نظریهٔ اعداد

متن درسی و منبعی از مسائل

اندرو ادلر، جان ای. کوری

ترجمهٔ باقر نشوادیان بخش

نظریهٔ اعداد، متن درسی و منبعی از مسائل

اندرو ادلر، جان ای. کوری

در این کتاب مفاهیم اصلی نظریهٔ کلاسیک اعداد، با تأکید بر سیر تکامل تاریخی این قضایا و چهره‌های برجسته‌ای که در آنها کار کرده‌اند عرضه می‌شود. هدف آن آشنا ساختن خواننده با برهانهای ریاضی است که به روشی ساده و روشن ارائه شده‌اند. این تنها کتاب درسی در نظریهٔ اعداد است که حل مفصل تقریباً ۸۰۰ مسأله را، با ذکر قضایای به‌کار رفته ارائه می‌دهد، به‌طوری‌که خواننده می‌تواند هر مرحله از استدلال را پیگیری کند. نویسندگان همچنین سعی کرده‌اند که مفاهیم مهم را در برهانها و تکنیکهای عددی مشخص سازند و هر جا ممکن باشد محاسبات میان‌بر را به خواننده نشان دهند.

مطالب مهم

- زمینه‌های تاریخی و زندگینامه‌یی در هر فصل
- الگوریتمها برای محاسبهٔ کارساز در مسائل عددی
- ۸۰۰ مسألهٔ حل‌شده
- مطالبی که در سایر کتابهای درسی یافت نمی‌شوند.

مؤلفان کتاب، اندرو ادلر و جان ای. کوری، هر دو استاد ریاضیات در دانشگاه بریتیش کلمبیا هستند.

نظریهٔ اعداد

متن درسی و منبعی از مسائل

اندرو ادلر، جان ای. کوری

ترجمهٔ دکتر باقر نشوادیان بخش

مرکز نشر دانشگاهی

بسم‌الله‌الرحمن‌الرحیم

فهرست

پیشگفتار مترجم

تدریس بیش از ۵۰ نیمسال درس نظریهٔ اعداد در دوره‌های کارشناسی نه تنها مرا دلزده نکرد بلکه بیشتر و بیشتر مرا دلباختهٔ این ملکهٔ ریاضیات می‌دیدم و از اینکه گوشهٔ چشمی به من داشته بسیار راضی بوده‌ام. به نظر من درک زیباییهای این ملکهٔ دلربا را می‌توان با حل بیشتر تمرینی آن میسر ساخت. کتاب نظریهٔ اعداد تألیف پروفسور ادلر و پروفسور کوری این منظور مرا برآورده ساخت، زیرا کتابی است خودکفا. علاوه بر سبک جالب در ارائه روشهای روشن و ساده برای برهانها و ارائه کامل مراجع برای قضیه‌ها، و مزایای دیگر، تنها کتابی است در نظریهٔ اعداد که حل مفصل و گام به گام حدود ۸۰۰ مسأله را عرضه می‌کند. همچنین دارای ۴۳۳ تمرین حل نشده است که بسیاری از آنها با راهنمایی همراه‌اند.

پیشگفتار و مقدمهٔ کتاب مطالب بسیار جالبی هستند و توصیه می‌شود خوانندهٔ محترم با دقت آنها را مطالعه کند.

لازم می‌دانم که از استاد ارجمندم زنده یاد دکتر محمدهادی شفیعیها که هم مشوق من در ترجمهٔ کتاب بوده‌اند و هم به من منت نهادند و ویرایش آن را به‌عهده گرفتند، تشکر کنم. در واقع انتشار این کتاب را مدیون بذل توجه ایشان هستم. روانش شاد.

پیشگفتار مؤلفان

در این کتاب مفاهیم اصلی نظریهٔ کلاسیک مقدماتی اعداد با تأکید بر بسط تاریخی این قضیه‌ها و چهره‌های برجسته‌ای که در آنها کار کرده‌اند عرضه می‌شود. در این کتاب همچنین بر آنیم که دانشجویان را با برهانهای ریاضی که به روشی ساده و روشن ارائه شده‌اند و حل گام‌به‌گام و کامل مسائل با چنان تفصیلی که عرضهٔ آن از خود دانشجو انتظار می‌رود آشنا سازیم. در سراسر کتاب، سعی کرده‌ایم که مفاهیم مهم در یک برهان یا تکنیکهای عددی را مشخص سازیم و هر جا ممکن باشد محاسبات میان‌بر را به دانشجو نشان دهیم.

احساس می‌کنیم که زمینه‌های تاریخی و راهنماییها نه‌تنها برای تجسم قضیه‌های مختلف مهم‌اند، بلکه علاقه‌مندی و قدرت تخیل دانشجویان را جلب می‌کنند و مطالب را مناسبتر می‌سازند. هنگامی که این کتاب را می‌نوشتیم سه هدف در ذهن داشتیم. اول از همه، می‌خواستیم که مطالب جذاب و به‌قدر کافی برای آموختن آسان باشند؛ بدین‌منظور، کاربردهای مطالب نظری را افزوده‌ایم (مثلاً، بحثی دربارهٔ تقویمها، چگونه روزی از هفته را با مفروض بودن یک تاریخ، تعیین «بهترین» تقریبهای گویای π، و آلگوریتمی برای تجزیهٔ اعداد بزرگ به حاصلضرب) پیدا کنیم. دوم، مطالب طوری مرتب شوند و برهانها و حلها به روشی نوشته شوند که تدریس این کتاب برای استاد بسیار آسان باشد. سرانجام، خواستیم که برهانها به‌قدر کافی شفاف و انگیزه‌دار باشند تا دانشجویان ماهیت برهان ریاضی ــ هم استدلالهای ساده و هم پیچیده ــ را بفهمند، و سرانجام بیاموزند که چگونه برهانهای منطقی و دقیق خود را بنا کنند.

از آنجا که بسیاری از مفاهیم پایه‌یی (اعداد اول، بخشپذیری، تجزیه) برای دانشجویان آشنا هستند، نظریهٔ اعداد روشی آرمانی برای آشنا کردن دانشجویان با برهانهای ریاضی است ــ در واقع، بهتر از یک درس در آنالیز مقدماتی، که در آن مفاهیم کمتر آشنا هستند و برهانها (مثلاً، استدلالهای ϵـδ) فهمیدنشان مشکلتر است. اما دانشجویان به نمونه‌های روشنی از چگونگی نوشتن برهانها و راه‌حلها نیاز دارند. امتیاز بی‌نظیر این کتاب در این است که حل تفصیلی تقریباً ۸۰۰ مسأله

را با اشارهٔ کامل به قضیه‌های به‌کاررفته ارائه می‌دهد تا دانشجو بتواند هر مرحله از استدلال را پیگیری کند. گردایهٔ فراوانی از مسائل بدون حل نیز در آخر هر فصل وجود دارند که می‌توانند برای تکلیف شب یا امتحانات به‌کار روند. با توجه به تجربهٔ ما، دانشجویانِ در این سطح تمرین کافی برای حل مسائل انجام نمی‌دهند، به‌ویژه وقتی که دورهٔ درس فقط برای یک ترم باشد (کما اینکه در حال حاضر در اغلب دانشگاهها چنین است). این مطلب به‌ویژه در مورد مسائلی که شامل برهان هستند، حتی برهانهای ساده، صادق است. ولی، اگر دانشجویان در هر مبحث تعداد زیادی مسأله را که به تفصیل حل شده‌اند ببینند، شانس زیادتری برای حل مسائل مشابه دارند. وقتی فقط پاسخی عددی یا خلاصه‌ای از حل ارائه شده باشد، دانشجویان اغلب نکات مهم برهان را درک نمی‌کنند، در نتیجه، ممکن است نتوانند مسائل دیگر از این نمونه را حل کنند که شباهت نزدیکی به اندک تمرینهای حل‌شده در متن را ندارند.

در واقع، مسائل حل‌شده زمینهٔ روشنی برای ادامهٔ کارند، به دانشجو نشان می‌دهند که چگونه نتایج قبلی را برای حل یک مسأله جدید با هم مربوط سازند و مشخص کنند که چه چیزهایی را باید در نظرگرفت و چه چیزهایی ضرورت ندارند، و تا کجا باید پیش رفت. گاهی برای یک مسأله چندین راه‌حل ارائه شده است تا تأکید کنیم که اغلب روشهای مختلفی برای ورود به یک حل وجود دارند.

سخنی در مورد برهانهای این کتاب. زحمات خاصی را متحمل شده‌ایم تا در حد امکان برهانها سرراست و واضح باشند، و وضوح را یا بر یک برهان کوتاه یا یک برهان «زیبا» مقدم داشته‌ایم. در تعدادی از موارد، برهانهای ارائه‌شده نااستانده و به‌طور قابل‌ملاحظه‌ای شفافتر از استدلالهای معمول هستند (مثلاً، قضیهٔ چهار مربع و قانون تقابل درجه دوم). فلسفهٔ کار تماماً در آن بوده است که ارائه برهان قضیه‌ها و حل مسائل در کلاس آسان باشد. وقت بسیار زیادی برای مرتب کردن مطالب صرف شده است، و اغلب با مراجعه به مثالهای واقعی یا کاربردها توجه ویژه‌ای به‌کار رفته است تا قضیه‌ها انگیزه‌دار شوند.

این کتاب به‌عنوان یک کتاب درسی در نظریهٔ مقدماتی اعداد برای یک یا دو ترم که معمولاً در کالجها یا دانشگاههای آمریکا و کانادا در سال سوم ارائه می‌شوند، در نظرگرفته شده است. معمولاً، این درس را دانشجویان سال سوم یا سال آخر می‌گیرند، اما بیشتر، دانشجویان سال دوم (از جمله دانشجویانِ کالجهای دوساله) این درس را انتخاب می‌کنند، و مفاد آن برای آنها کاملاً قابل فهم است. برای مطالب این کتاب پیش‌نیاز رسمی خیلی کمی مورد نیاز است؛ به‌ویژه، هیچ درس قبلی در جبر مجرد لازم نیست. دانشجویان بایستی با اثباتها از راه استقرا ریاضی آشنا باشند، و به‌کرات از این حقیقت استفاده خواهد شد که هر زیرمجموعهٔ ناتهی از اعداد صحیح مثبت یک کوچکترین عنصر دارد. ویژگیهای پایه‌یی حد دنباله‌های اعداد حقیقی در اثباتهای کمی به‌کار می‌روند؛ مثلاً،

دانشجویان باید بدانند که یک دنبالهٔ صعودی از اعداد حقیقی که از بالا کراندار است همگراست. سرانجام، مطالب فصل ۱۱ ــ که این روزها به‌ندرت در یک درس نظریه مقدماتی اعداد گنجانده می‌شود ــ آشنایی مختصری با اعداد مختلط را می‌طلبد.

قسمتهای مهم

این کتاب به‌صورت یک کتاب مستقل (خودکفا) برای یک درس در نظریهٔ مقدماتی اعداد و به‌عنوان یک کتاب منبع از مسائل حل‌شده در نظر گرفته شده است. این تنها کتاب منبع از مسائل در نظریهٔ اعداد است که دارای حل تفصیلی، گام‌به‌گام برای تمام مسائل است. از این‌رو، یک مرجعی است ارزشمند حتی اگر به‌عنوان کتاب درسی اصلی به‌کار نرود؛ مسائل حل‌شده برای تکمیل درسهای کلاس، تکالیف شب، امتحانات، و مرور آرمانی هستند. تمام مباحث استانده همراه با تعدادی از مطالب که در بسیاری از کتابهای جاری یافت نمی‌شوند، مثلاً، همنهشتیهای چندجمله‌یی، تجزیهٔ اعداد بزرگ، اعداد گاوسی و اعدادی از سایر هیئتهای درجهٔ دوم، ارائه شده‌اند. این مبحث اخیر امروزه در یک درس مقدماتی نظریه اعداد به‌ندرت تدریس می‌شود، اما تعدادی از مباحث فصلهای قبلی را به‌خوبی به‌یکدیگر پیوند می‌دهد و اثباتهای ساده‌ای برای بسیاری از قضیه‌ها عرضه می‌کند.

بحث کاملی از تقابل درجه دوم، ریشه‌های اولیه، نمایش اعداد صحیح به‌صورت مجموع دو مربع (از جمله استخراج فرمولی برای تعداد این نمایشها)، تقریب گویای اعداد گنگ، و معادلهٔ پل نیز گنجانده شده‌اند. از این‌رو، استادان می‌توانند به میل خود تغییراتی در یک درس بدهند تا نظرات خود و زمینهٔ درسی دانشجویان خود را تأمین کنند، مثلاً می‌توانند مطالب محاسبه‌یی بیشتری به مواد استانده اضافه نمایند.

فصلهای ۱ و ۲ شامل مفاهیم پایه‌یی هستند که در سرتاسر کتاب به‌کار می‌روند؛ مطالب پیشرفته‌تر (از جمله مواد اختیاری) در فصلهای بعد ظاهر می‌شوند. بجز چند استثنا، هر فصل با یک مقدمهٔ تاریخی شروع می‌شود، و در سرتاسر کتاب نظرات تاریخی و تاریخهایی که قضیه‌های خاص و توسط چه کسی ثابت شده‌اند، آمده‌اند. هر جا مناسبت داشته باشد نیز به مسائل حل‌نشده یا سؤالات قابل بحث اشاره شده است. به‌ویژه هر فصل به‌صورت زیر مرتب شده است:

قضیه‌های پایه‌یی و اثباتها. در بسیاری از موارد، اثباتهای جدید یا برهانهای بسیار ساده‌تر تهیه شده است. همچنین، مثالهایی که به تفصیل توضیح داده شده‌اند، کاربردها، یادداشتهای محاسبه‌یی، و بحثی از آلگوریتمها برای محاسبهٔ کارساز در مسائل عددی وجود دارند.

مسائل حل‌شده. در هر فصل تقریباً ۵۰ تا ۱۰۰ مسأله با حل تفصیلی و کامل آورده شده است، که تماماً به قضیه‌های کتاب ارجاع داده شده‌اند. این شکل کار در این کتاب منحصر به‌فرد است. مسائل

برحسب بحثهای فصل مرتب شده‌اند و دامنهٔ وسیعی از مهارتهای دشوار و محاسبه‌یی، از مسائل ساده و قابل‌فهم (یک محاسبهٔ عددی یا اثبات یک مرحله‌یی که با استفاده از یک قضیه نظری از کتاب) گرفته تا مسائل مبارزطلب (که مستلزم چند مرحله در برهان یا استخراج قضیه‌های دیگر است) را در برمی‌گیرند. مسائل بسیار مبارزطلب که در حاشیه با علامت ◁ نشان داده شده‌اند برای دانشجویان برتر در نظر گرفته شده‌اند. این مسائل عرصه‌های دیگر مطالب فصل را بسط می‌دهند و نظریه‌یی اضافی (مثلاً، نماد ژاکوبی در فصل ۵ و همگراهای درجهٔ دوم در فصل ۹) عرضه می‌کنند، یا یک اثبات جدید یا استثنایی از یک قضیهٔ رایج به‌دست می‌دهند. این مسائل مورد نیاز فصلهای بعد نیستند؛ در واقع، بجز چند استثناء، قضیه‌های کتاب از مسائل حل‌شده مستقل‌اند.

سرانجام، بسیاری از مسائل با راهنمایی همراه‌اند، و تعدادی به‌صورت «اثبات یا رد کنید» بیان شده‌اند تا دانشجویان را به تجربه‌کردن تشویق کنند و دربارهٔ صحت و سقم یک حکم به اندیشه وادارند.

تمرینها. هر فصل شامل تعداد زیادی مسائل بدون حل است، هر چند که بسیاری از آنها با راهنمایی همراه‌اند. این تمرینها شباهت زیادی به مسائل حل‌شده دارند و برای تکالیف شب، مسابقهٔ اطلاعات عمومی، و امتحانات آرمانی هستند.

یادداشتهای فصل. این یادداشتها مطالب کتاب را با ارائه روشهای متفاوت، قضیه‌های اضافی و سؤالات قابل بحث وسعت می‌بخشند. بعضی از این یادداشتها بحثهایی را مطرح می‌کنند که مباحث را به سطوح دیگر ریاضیات مربوط می‌سازند.

شرح کوتاهی از زندگینامه‌ها. شرح مختصری از زندگی و کارهای ریاضیدانان برگزیده‌تری که در نظریهٔ اعداد کار کرده‌اند ارائه شده است.

مآخذ حاشیه‌یی. این مآخذ با مشخص کردن جنبه‌های اختصاصی هر کتاب، منبعی از مطالب اضافی برای دانشجویان علاقه‌مند عرضه می‌کنند.

چگونگی استفاده از این کتاب

در این کتاب بیش از حد کفایت مطلب برای دو درس یک ترمی در نظریهٔ مقدماتی اعداد وجود دارد؛ در واقع، حتی اگر دو ترم نیز برقرار شود بایستی انتخابی از مطالب انجام گیرد. می‌توان سرفصلها را به روشهای مختلف دسته‌بندی کرد. در دانشگاه بریتیش کلمبیا، درس اصلی یک سال کاملِ ما در نظریهٔ اعداد در دو ترم برنامه‌ریزی شده است که هر ترم ۱۳ هفته طول می‌کشد. اولی پیش‌نیاز برای دومی است و ممکن است به‌تنهایی اختیار شود، هر چند که اغلب دانشجویان هر دو را انتخاب می‌کنند.

درس یک ترمی را می‌توان به طریق زیر برنامه‌ریزی کرد: فصلهای ۱، ۲، و ۳ بایستی فرا گرفته شوند، زیرا مطالب پایه‌یی در بخشپذیری، اعداد اول، آلگوریتم اقلیدسی، همنهشتیها، قضیهٔ باقیماندهٔ چینی، و قضیه‌های فرما، اویلر، و ویلسن در فصلهای بعد به‌کار می‌روند. مباحث فصل ۴ (همنهشتیهای چندجمله‌یی) اختیاری هستند و به‌طورکلی در بسیاری از درسهای مقدماتی نظریهٔ اعداد تدریس نمی‌شوند. به‌هر حال منبع خوبی برای مسائل محاسبه‌یی هستند. (در دانشگاه ما، معمولاً این قسمت با توجه به فصل ۵ حذف می‌شود.) در فصل ۵، قضیهٔ مانده‌های درجهٔ دوم و قانون تقابل درجه دوم گاوس بایستی تدریس شوند، حتی اگر اثبات قانون تقابل درجهٔ دوم ارائه نشود. اثباتی که ما ارائه می‌دهیم برهان استانده نیست (منتسب به آیزنشتاین)، و باور داریم که برای دانشجویان ریاضی سال سوم و چهارم بسیار قابل‌فهم است. قانون تقابل درجه دوم یکی از مهمترین قضیه‌ها در نظریهٔ کلاسیک اعداد است، و این مطلب یک منبع عالی از مسائل عددی و نظری است.

در دانشگاه ما، دومین درس یک ترمی معمولاً شامل مباحث زیر است: با مطالب فصل ۶ در ریشه‌های اولیه و اندیسها شروع می‌کنیم، اما می‌توان به آسانی بعضی از برهانهای وجودی را رها کرد یا به‌عنوان تکلیف خواندنی برای دانشجو گذاشت. این مطلب مخلوط زیبایی از نظریه و تکنیکهای محاسبه‌یی است. فصل ۷ اختیاری است، هر چند که بحث کلی اعداد اول و مطالب مربوط به اعداد تام و اعداد اول مِرسن در دوره‌ای که ما پیشنهاد می‌کنیم گنجانده شده است. بخش مربوط به اعداد فرما نیز خیلی کوتاه است و ما آن را نیز گنجانده‌ایم. مطالب فصل ۸ دربارهٔ سه‌تاییهای فیثاغورسی و مجموعهای دو مربع، همچنین بیان قضیهٔ چهار مربع است، با بحث در نمایشهای اولیه، اثبات قضیهٔ چهار مربع، و مسأله وِرینگ به‌عنوان مطالب اختیاری واگذار شده‌اند. در فصل ۹، اکثر قضیه‌های پایه‌یی درکسرهای مسلسل متناهی و نامتناهی ارائه شده‌اند، اما تعداد کمی برهان نیاز به ارائه دارند، زیرا بسیاری از آنها با استفاده از استقرا ثابت می‌شوند و کاملاً تکراری هستند. مطالب مربوط به تقریبهای گویا را می‌توان حذف کرد، اما هر دو مؤلف گنجاندن آن را ضروری می‌دانند زیرا کاربردی زیبا از تئوری و نیز منبع خوبی از مسائل عددی است. فصل ۱۰ (معادلهٔ پِل) یک کاربرد مهم از کسرهای مسلسل است و نیز مسائل عددی بسیاری را به‌وجود می‌آورد. در حالت کلی توقع داریم که هر دو معادلهٔ $x^2 - dy^2 = 1$ و $x^2 - dy^2 = -1$ مورد مطالعه قرار گیرند، گرچه به دلیل صرفه‌جویی در وقت یا ارائه مطلب در تجزیهٔ اعداد بزرگ (موضوعی که به نظر می‌رسد دانشجویان آن را واقعاً جالب بیابند) می‌توان دومی را حذف کرد. سرانجام، فصل ۱۱ دلخواه است و به‌ندرت ارائه می‌شود مگر آنکه مطالب دیگری (مثلاً، ریشه‌های اولیه یا معادلهٔ پِل) حذف شده باشند، که در این حالت، می‌توان مطالب اعداد اول گاوسی را ارائه

نمود که برای چند برهان ظریف از قضیه‌های فصلهای قبل، از جمله فرمول سه‌تاییهای فیثاغورسی و تعداد روشهای نمایش یک عدد صحیح به‌صورت مجموع دو مربع، به‌کار می‌آید.

یک توصیهٔ نهایی دربارهٔ مسائل حل‌شده و تمرینها. می‌توان گردایه‌ای از مسائل حل‌شده و تمرینها را به‌طور هفتگی یا حتی روزانه برای مطالعه به دانشجویان واگذار کرد، و یک امتحان ۲۰ یا ۲۵ دقیقه در هر هفته یا در این حدود با استفاده از مسائل حل‌شدهٔ دیگر یا سؤالاتی از تمرینها به عمل آورد. بدین‌ترتیب، ضرورت ندارد که وقت با ارزش کلاس برای حل تعدادی از مسائل به تفصیل (که می‌توانند خیلی وقت‌گیر باشند) گرفته شود.

مطالب پایانی و سپاسگزاریها

در سرتاسر بیست‌وپنج سال گذشته هر دو ما بارها درسهایی در نظریهٔ اعداد را تدریس کرده‌ایم. این کتاب و مسائل آن حاصل تجربه و علاقهٔ پایدار ما به این موضوع است. ما هر دو دریافتیم که بهترین روشِ تدریس نظریهٔ اعداد این است که قضیه‌های نظری را با تعداد زیادی مسأله که حل تفصیلی دارند کامل کنیم، به‌طوری که دانشجویان تکنیکهای مختلف را برای نوشتن اثباتهای خود فرا گیرند، سالهاست که این روند را در تدریسمان به‌کار برده‌ایم. از آنجا که هیچ کتاب منبعی از مسائل با حل گام‌به‌گام وجود نداشت، تصمیم گرفتیم که صدها مسأله‌ای را که در طول سالها جمع‌آوری کرده‌ایم مرتب کنیم و کتاب خود را بنویسیم.

مایلیم که دین خود را به کتابهای گ. ه. هاردی[1] و ا. م. رایت[2]، ایوان نیون[3] و هربرت زوکرمن[4]، و هرلد داونپورت[5] ادا کنیم. هر کدام به سهم خود نقش مهمی در رسیدن ما به نظریه اعداد و علاقهٔ ممتد ما به این موضوع ایفا کرده‌اند.

مایلیم که از پروفسور استیون چیس[6] و پروفسور دون ردمند[7] به خاطر مطالعهٔ نسخهٔ دست‌نویس و ارائه تعدادی پیشنهادات سودمند سپاسگزاری نماییم.

سرانجام ، پروفسور کوری مایل است سپاس خود را نسبت به ادوین هویت[8] و هربرت زوکرمن اظهار نماید، به اولی به خاطر هدایت زندگی ریاضی دیرینش و به دومی به جهت نشان دادن زیبایی نظریهٔ اعداد. او به‌شدت مدیون هر دو آنهاست.

وَنکوور، کانادا — اندرو ادلر
اکتبر ۱۹۹۴ — جان ای. کوری

1. G. H. Hardy 2. E. M. Wright 3. Ivan Niven 4. Herbert Zuckerman
5. Harold Davenport 6. Stephen Chase 7. Don Redmond 8. Edwin Hewitt

مقدمه

نظریهٔ اعداد، که گاهی حساب عالی خوانده می‌شود، یکی از قدیمی‌ترین عرصه‌های ریاضیات است، که به چند هزار سال قبل برمی‌گردد. قدیمی‌ترین مسائل مورد توجه، پایه‌ای در مفهوم شمارش و مفاهیم ابتدایی حساب داشتند، مفاهیمی که حتی قدیمی‌ترند و در لوحه‌های بابلیان حدود ۴۰۰۰ سال قبل پیدا شده‌اند. معماهای ریاضی و مسأله‌های لفظی، از دوران باستان، منابع دیگری برای تحقیق در نظریهٔ اعداد بوده‌اند. مسأله‌های لفظی در ریاضیات یونانی در آغاز سدهٔ اول میلادی و در ریاضیات چینی در سدهٔ پنجم میلادی پیدا شده‌اند. این مسائل در نوشته‌های ریاضیدانان هندی برهمگوپته (سدهٔ هفتم) و بهاسکره (سدهٔ دوازدهم)، و در کارهای ریاضیدان ایتالیایی فیبوناتچی (اوایل سدهٔ سیزدهم) نیز یافت شده‌اند.

نظریهٔ اعداد، به معنی وسیع کلمه، با ویژگیهای اعداد صحیح مثبت (یا اعداد طبیعی)، از جمله بخشپذیری، بزرگترین مقسوم‌علیه مشترک دو عدد صحیح، و مطالعهٔ اعداد اول و مرکب سروکار دارد. به‌طورکلی، مسأله‌ها و حدسیه‌ها در نظریه اعداد به بیان آسان هستند ولی اثبات آنها اغلب واقعاً دشوار است. یک مثال خوب از این نوع، حدسیهٔ گلدباخ است، که اظهار می‌دارد هر عدد صحیح زوج بزرگتر از ۲ مجموع دو عدد اول است. از ۱۷۴۲ که برای اولین بار این مسأله مطرح شده است تاکنون کارهای بسیاری در مورد آن انجام شده است، ولی حل‌نشده باقی مانده است. مثال دیگر دربارهٔ نمایش بعضی از اعداد صحیح مثبت به‌صورت مجموع دو مربع است. اگر چه دیوفانتوس در سدهٔ سوم درکتابش علم حساب به این مسأله پرداخته است، ولی سرانجام بعد از تقریباً ۱۵۰۰ سال این مسأله حل شد.

در ریاضیات یونان باستان به مسائلی از اعداد اول و بخشپذیری، یافتن مثلثهای قائم‌الزاویه با اضلاع صحیح، و بررسی اعداد تام (یعنی، اعدادی که با مجموع مقسوم‌علیه‌های کوچکتر از خودشان مساوی‌اند) پرداخته شده است. اگر از فیثاغورس در سدهٔ ششم قبل از میلاد شروع کنیم، این مسائل تا اندازه‌ای به تفصیل بررسی شده‌اند و معمولاً قضیه‌های آنها جنبهٔ نظری داشته‌اند.

در سدهٔ سوم قبل از میلاد، اقلیدس بسیاری از مطالب ریاضی را که بر یونانیان باستان معلوم بودند در کتاب اصول خود، که به احتمال قوی مهمترین اثر ریاضی است که تاکنون نوشته شده، گردآوری کرده است. علاوه بر بسط مشروح هندسه، کتاب اصول شامل بحثی در اعداد اول از جمله اثبات وجود بی‌نهایت عدد اول؛ روشی برای تولید اعداد تام؛ آلگوریتم معروف اقلیدسی برای یافتن بزرگترین مقسوم‌علیه مشترک دو عدد صحیح؛ و مقدماتی برای اثبات قضیهٔ اصلی علم حساب، که می‌گوید هر عدد صحیح بزرگتر از ۱ را می‌توان، صرف‌نظر از ترتیب عوامل، فقط به یک طریق به‌صورت حاصلضرب اعداد اول بیان کرد. (این قضیه را اول بار در ۱۸۰۱ کارل فریدریش گاوس بیان و اثبات کرد.) کمی بعد، اراتستن روش جالبی، به نام غربال اراتستن را، برای تعیین همهٔ اعداد اول کمتر از یک عدد صحیح مثبت مفروض ارائه داد. و در سدهٔ سوم میلادی دیوفانتوس اسکندرانی نخستین بحث نظام‌مندِ آن چیزی را ارائه داد که اکنون به معادلات دیوفانتی معروف‌اند، یعنی معادلات جبری که باید جوابهای صحیح (یا، به‌زعم دیوفانتوس، جوابهای گویا) برای آنها پیدا کرد. کتاب علم حساب او، که برای نخستین بار برای بیان معادلات از نمادها به‌جای واژه‌ها استفاده کرده است، شامل بیش از ۲۵۰ مسأله از این نوع و حل آنهاست.

از زمان دیوفانتوس تا سدهٔ سیزدهم، ریاضیدانان هندی، چینی و عرب[۱] آلگوریتمهای مختلفی (نظیر قضیهٔ باقیماندهٔ چینی) تولید کردند و برخی معادله‌های دیوفانتی را بررسی نمودند، از جمله معادلهٔ خطی $ax + by = c$ و معادلهٔ درجهٔ دوم $x^2 - dy^2 = 1$ را، که سرانجام به معادلهٔ پِل معروف شد. برهمگوپته و بهاسکره معادلهٔ آخر را به تفصیل بررسی نمودند و نتایجی به‌دست آوردند که تا سدهٔ هفدهم در اروپا بی‌مانند بود. صورتهای خاص معادلهٔ پِل توسط یونانیها نیز مطالعه شده بودند، زیرا این معادلات و مفاهیم بسیار مرتبط به آنها یعنی کسرهای مسلسل در مسأله یافتن تقریبهای گویای خوب برای اعداد گنگ $\sqrt{d}$ ظاهر می‌شوند. مثلاً، در سدهٔ سوم ق.م. ارشمیدس $\sqrt{3}$ را با ۲۶۵/۱۵۳ و ۱۳۵۱/۷۸۰ تقریب کرد، که به‌ترتیب تا چهار و شش رقم اعشاری دقت دارند. یکی از قدیمی‌ترین پیدایش معادلهٔ پِل در سدهٔ سوم در ارتباط با مسأله گِلهٔ ارشمیدس است، که به معادلهٔ $x^2 - 4729494y^2 = 1$ منجر می‌شود، کوچکترین جواب مثبت (که در سال ۱۸۸۰ پیدا شد) مقدار y آن ۴۱ رقم دارد.

تا سدهٔ دوازدهم، گسترش ریاضیات در اروپای سده‌های میانه بسیار کم بود. با استعدادترین ریاضیدان در اروپا در خلال سده‌های میانه لئوناردو پیسایی (حدود ۱۱۷۵ تا ۱۲۵۰)، مشهور به فیبوناتچی بود. او شمارهای عربی را در کتابش لیبرآباکی («کتاب حساب») معرفی کرد، و در کتاب مربعات، به تحقیق در حل بعضی از معادلات دیوفانتی شامل مربعها پرداخت. لیبرآباکی مسائل

۱. ایرانی.ـم.

لفظی بسیار دارد، از آن جمله «مسألهٔ خرگوشها»ی معروف فیبوناتچی است: با یک جفت خرگوش شروع می‌کنیم، در یک سال چند جفت خرگوش تولید می‌شود اگر هر جفت خرگوش در هر ماه جفت جدیدی تولید کند که از ماه دوم به بعد مولّد می‌شوند؟ جواب ۳۷۷ یعنی جملهٔ دوازدهم در دنبالهٔ فیبوناتچی

$$۲, ۳, ۵, ۸, ۱۳, ۲۱, \ldots, ۳۷۷, \ldots$$

است که در آن از جملهٔ سوم به بعد، هر جمله مساوی مجموع دو جملهٔ قبلی است. این دنباله ویژگیهای بسیار دارد. مثلاً، هر دو جملهٔ متوالی آن نسبت به هم اول‌اند، و نسبت دو جملهٔ متوالیِ به اندازهٔ کافی بزرگ تصادفاً به «نسبت زرین» $۲/(۱-\sqrt{۵})$، که مورد علاقهٔ یونانیهای باستان بوده نزدیک است.

با شروع سدهٔ دوازدهم در اروپای غربی، اصول اقلیدس و تعدادی از منابع نوشته‌شده به عربی به لاتین ترجمه شدند، معهذا اولین نسخهٔ چاپی اصول تا ۱۴۸۲ در دسترس قرار نگرفت. تقریباً یک سده بعد، یک ترجمهٔ لاتین از کتاب حساب دیوفانتوس به چاپ رسید، و به دنبال آن در ۱۶۲۱ با چاپ خیلی بهتری انتشار یافت. با دستیابی به این کتابها، کیفیت ریاضیات در اروپا به‌طور قابل‌ملاحظه‌ای پیشرفت کرد.

تا سدهٔ هفدهم، کارکردن به‌تنهایی، برای ریاضیدانان یک امر عادی بود و دستاوردهای خود را توسط نامه به یکدیگر انتقال می‌دادند. مارن مرسن[1] (۱۶۴۸ـ۱۵۸۸)، که راهبی از فرقهٔ فرانسیسیان بود، با بسیاری از دانشمندان زمان خود ارتباط داشت و به‌عنوان مرکز مبادلهٔ کارهای علمی آنها عمل می‌کرد. یکی از ریاضیدانانی که مرسن با او به‌طور مرتب تبادل‌نظر داشت پیرفرما (۱۶۶۵ـ۱۶۰۱) بود. ترجمهٔ کتاب علم حسابِ دیوفانتوس که در ۱۶۲۱ توسط باشه انجام شده بود، فرما را با مسائل نظریهٔ اعداد آشنا کرد. فرما، که بعدها سلطان آماتورها لقب گرفت (حرفهٔ او قضاوت بود)، آخرین ریاضیدان بزرگی است که ریاضیات برای او اساساً یک سرگرمی بود. بعد از فرماست که، تحقیقات ریاضی توسط ریاضیدانان حرفه‌یی در دانشگاهها و مراکز علمی به‌طور گسترده رهبری شده‌اند.

نظریهٔ اعداد به‌عنوان یک حوزهٔ نظام‌مند تحقیق، در حقیقت با کار فرما در سدهٔ هفدهم آغاز می‌شود. از زمان فیثاغورس، بسیاری از ریاضیدانان در این حوزه کارهایی انجام داده‌اند، اما این فقط فرما بود که مسائل و مطالب نظریهٔ اعداد را برجسته کرد تا در ۱۵۰ سال بعد مورد بررسی و تحقیق قرارگیرند. فرما به مفاهیم نظری که قضیه‌های عددی مجزا را به‌هم پیوند می‌دهند علاقه‌مند بود، و کار او طیف وسیعی از مسائل را می‌پوشانید: اعداد تام، بخشپذیری، اعداد اول، و انواع معادلات دیوفانتی، از جمله اولین بررسی جدیِ معادلهٔ پِل. فرما، بدون اثبات، بیان داشت که هر

1. Marin Mersenne

عدد اول به‌صورت $۴k+۱$ نمایش یکتایی به‌صورت مجموع دو مربع دارد، مسأله‌ای که از کارهای دیوفانتوس حاصل می‌شود. در دوران زندگیش، فرما برای تعداد کمی از احکامش برهان ارائه داده است؛ بسیاری از کارهایش در ارتباط با سایر ریاضیدانان، و اغلب به‌صورت یک چالش در حل مسائل خاص به‌وجود آمده‌اند. ولی، فرما برای اثبات بعضی از قضیه‌هایش از آنچه که او آن را روش نزول نامتناهی می‌نامد استفاده کرده است؛ این تکنیک اساساً با اصل استقرای ریاضی هم‌ارز است. معروفترین حکم ثابت‌نشدهٔ فرما، و یکی از مشهورترین مسائل حل‌نشده در تمام ریاضیات، بیان می‌کند که معادلهٔ $x^n+y^n=z^n$ به‌ازای $n \geq ۳$ جواب صحیح غیرصفر ندارد. این حدسیه، معروف به آخرین قضیهٔ فرما، برای مدت بیش از سه سده و نیم حل‌ناشدنی بود؛ سرانجام حل کامل آن در اکتبر ۱۹۹۴ ارائه شد.

لئونهارت اویلر (۱۷۸۳ـ۱۷۰۷) و ژوزف لویی لاگرانژ (۱۸۱۳ـ۱۷۳۶) جانشین این برجسته‌ترین چهره در نظریهٔ اعداد در سدهٔ هفدهم شدند. اویلر نامدارترین ریاضیدان سدهٔ هجدهم و نیز یکی از پرکارترین ریاضیدان تاریخ بود، که در دوران زندگیش تعداد فوق‌العاده زیادی مقاله منتشر کرد. او بسیاری از قضیه‌هایی را که فرما فقط بیان کرده بود به اثبات رسانید، از جمله اینکه هر عدد اول به‌صورت $۴k+۱$ تنها به یک طریق با مجموع دو مربع نشان داده می‌شود. تعدادی از قضیه‌های فرما را تعمیم داد و فرمولبندی کرد، در ۱۷۴۶ صورتی از قانون تقابل مربعی معروف را ارائه داد که حدود ۵۰ سال بعد توسط گاوس اثبات گردید. اویلر چیزی را نیز معرفی کرد که اکنون به تابع ϕی اویلر معروف است و اهمیت زیادی در نظریهٔ اعداد دارد، و نیز مفهوم همنهشتی و رده‌های مانده‌ها را ارائه داد که مجدداً توسط گاوس در اواخر همان سده احیا گردید.

ژوزف لویی لاگرانژ، تنها نظیر اویلر در شهرت ریاضی در سدهٔ هجدهم، جانشین اویلر در آکادمی برلین گردید وقتی که اویلر مقامی در سنت‌پترزبورگ پذیرفت. با اینکه بیشتر کارهای لاگرانژ در خارج از نظریهٔ اعداد بود، او اولین کسی بود که در ۱۷۷۰ ثابت کرد که می‌توان هر عدد صحیح مثبت را به‌صورت حداکثر مجموع چهار مربع بیان کرد، قضیه‌ای که حتی اویلر از اثبات آن سر باز زد. همچنین، لاگرانژ نخستین اثبات قضیهٔ ویلسن را در ۱۷۷۱ به چاپ رسانید و قضیهٔ مهمی در تعداد ریشه‌های برخی از همنهشتیهای چندجمله‌یی اثبات کرد. و در یک سری از مقاله‌ها که به آکادمی برلین در حدود سال ۱۷۷۰ ارائه داد، اولین بررسی دقیق معادلهٔ پِل را با بهره‌گیری از کسرهای مسلسل عرضه کرد (ادامهٔ راهی که اویلر در حدود ده سال جلوتر مورد توجه قرار داده بود).

برجسته‌ترین عالِم در نظریهٔ اعداد در سدهٔ نوزدهم کارل فردریش گاوس (۱۸۵۵ـ۱۷۷۷) بود. گاوس که توسط معاصرانش «امیر ریاضیات» لقب گرفته بود، مؤسس نظریهٔ جدید اعداد محسوب می‌شود و همراه با ارشمیدس و آیزک نیوتن بزرگترین ریاضیدان تاریخ به‌شمار می‌آید. با

انتشار کتاب دوران سازش «تحقیقات حسابی» در ۱۸۰۱، نظریهٔ اعداد را بر پایهٔ ریاضی استوار قرار داد. منظور گاوس از حساب، همان نظریهٔ اعداد است؛ در حقیقت، گاوس در مقدمهٔ کتابش عبارت «حساب عالی» را بدین‌منظور ساخته است، که شامل مطالب کلی‌تری از اعداد صحیح است، تا با آنچه که او «حساب مقدماتی» می‌خواند تمایزی قائل شود. گاوس در تحقیقات، بیشتر مفاهیم و نمادهایی را که هنوز امروزه به‌کار می‌روند ارائه داده است. او تعریف نوین همنهشتی و مانده‌ها را وارد کرده است، که محاسبات شامل اعداد صحیح را به‌طور وسیعی آسان کرده است، و نماد $\equiv$ را برای همنهشتی به‌کار برده است که تاکنون نیز به‌کار می‌رود. کتاب گاوس اولین اثبات کامل قانون تقابل مربعی (او سرانجام شش برهان برای این قضیه ارائه داده است)، و بحث مفصلی از همنهشتی‌های خطی، و بحث کاملی از ریشه‌های اولیه را نیز شامل می‌شود. علاوه بر این، تحقیقات اولین اثبات قضیهٔ اصلی حساب و بیان آن را دربر دارد.

گاوس قضیهٔ معروف اعداد اول را فرمولبندی کرده، اما اثبات نکرده است (اولین اثباتی که تا ۱۸۹۶، یعنی حدود ۴۰ سال بعد از درگذشت گاوس، ارائه نشده بود)، و بعدها در کارهایش بررسی مفصلی از ویژگیهای آنچه که اکنون به اعداد صحیح گاوسی موسوم‌اند (یعنی، اعداد مختلط $a + bi$، که a و b اعداد صحیح‌اند) انجام داده است. گاوس مفهوم اعداد اول را به اعداد گاوسی تعمیم داده و ثابت کرده است که می‌توان این اعداد را همانند اعداد صحیح معمولی به یک روش اصولی یکتا به حاصلضرب اعداد اول گاوسی تجزیه کرد.

در سرتاسر فعالیت برجسته و طولانی‌اش در بسیاری از حوزه‌های ریاضی و علوم، گاوس همواره علاقهٔ خاص به نظریه اعداد داشت. او ریاضیات را ملکه علوم و نظریه اعداد را ملکه ریاضیات می‌نامید. یکی از دلایلی که نظریه اعداد از زمانهای قدیم مورد توجه ریاضیدانان بوده این است که مطالب و مفاهیم (مثل، بخشپذیری، اعداد اول، و تجزیه به حاصلضرب) همگی کاملاً آشنا هستند. فرمولبندی و فهم بسیاری از حدسیه‌ها آسان است، حتی مطالبی نظیر قضیهٔ آخر فرما، که برای قرنها بدون اثبات مانده بود.

در ارتباط با مشکل اثبات قضیه‌هایی که بر پایهٔ ملاحظات عددی، کاملاً بدیهی به نظر می‌رسند یکبار گاوس گفته است که «دقیقاً همین نکته است که زیبایی سحرآمیز به حساب عالی می‌دهد، چیزی که آن را دانش محبوب بزرگترین ریاضیدانان ساخته است، صرف‌نظر از غنای پایان‌ناپذیری که برتری زیادی نسبت به سایر شاخه‌های ریاضیات به آن می‌دهد.»

۱

بخشپذیری، اعداد اول، و الگوریتم اقلیدسی

اولین بسط نظام‌مند نظریهٔ بخشپذیری را می‌توان در مقاله‌های VII_IX از اصول اقلیدس (تقریباً ۳۰۰ ق.م.) پیدا کرد. پیش از اقلیدس، گفته‌های نظام‌مندی از نظریهٔ پایه‌یی اعداد، مثلاً، توسط آرخوتاس[1] و ریاضیدان بزرگ ائودوکسوس[2] وجود داشته است. گرچه این گفته‌ها از بین رفته‌اند، ولی دلایلی وجود دارند تا باور کنیم که مقدار زیادی از نظریهٔ اقلیدسی اعداد از منابع پیشین به‌دست آمده است.

تعداد زیادی از محتویات نظری این فصل را می‌توان در اصول اقلیدس یافت. قضیهٔ تجزیهٔ یکتا را او بیان نکرده است، اما بعضی استدلال کرده‌اند که این قضیه اساساً در اصول اقلیدس آمده است. اقلیدس حل معادلهٔ $ax + by = c$ را در اعداد صحیح مورد بررسی قرار نداده است، با اینکه جواب آن به سادگی از الگوریتمش برای یافتن بزرگترین مقسوم‌علیه مشترک دو عدد به‌دست می‌آید.

1. Archytas 2. Eudoxus

روشهای یافتن جوابهای صحیح $ax + by = c$ در سدهٔ ششم در هند توسط آریبهطه[1] به‌دست آمده بودند و در سدهٔ هفتم توسط برهمگوپته[2] شسته‌ورفته شدند. روش آنها، که *kuttaka* (خردکننده) نامیده می‌شد، برای چندین سده نقش مهمی در ریاضیات هندی ایفا کرده است، این روش با روش جایگزینی پسرو که بعد از قضیهٔ ۲۳.۱ بیان شده است ارتباط نزدیک دارد.

به نظر می‌رسد که در اروپای غربی تنها در اوایل سدهٔ هفدهم به فهم کامل معادلهٔ $ax+by = c$ رسیده‌اند. کلود باشه دو مزیریاک[3] (۱۵۸۷ـ۱۶۳۸) در ۱۶۱۲ بحث کاملی ارائه داده است. روش او نیز ارتباط نزدیکی با الگورتیم اقلیدسی دارد. همانند ریاضیدانان قبلی در به‌کارگیری اعداد منفی اکراه داشته است. در سدهٔ هجدهم، لئونهارت اویلر[4] (۱۷۰۷ـ۱۷۸۳) و ژوزف لویی لاگرانژ[5] (۱۷۳۶ـ۱۸۱۳) تسلط فنی کاملی به موضوع پیدا کردند. در ۱۸۰۱، کارل فریدریش گاوس[6] (۱۷۷۷ـ۱۸۵۵) در تحقیقات حسابی‌اش[7] یک چارچوب نظری مناسب برای نظریهٔ اعداد ارائه داد.

قضیه‌هایی برای فصل ۱

بخشپذیری

(۱.۱) تعریف. فرض می‌کنیم a و b که a غیر صفر است دو عدد صحیح باشند. گوییم عدد a عدد b را می‌شمارد، یا b مضربی از a است، هرگاه عدد صحیحی مانند q وجود داشته باشد به‌طوری که $b = qa$. در این‌صورت، می‌نویسیم $a|b$ و گوییم که a یک مقسوم‌علیه b است. اگر عدد a عدد b را نشمارد، می‌نویسیم $a\nmid b$.

برهان قضیهٔ بعد نتیجهٔ مستقیم این تعریف است.

(۲.۱) قضیه. فرض کنیم a، b، و c اعداد صحیح باشند.

(i) اگر $a|b$، آنگاه به‌ازای هر عدد صحیح k، $a|kb$.

(ii) اگر $a|b$ و $b|a$، آنگاه $a = \pm b$.

(iii) اگر $a|b$ و $b|c$، آنگاه $a|c$.

(iv) اگر $a|b$ و $a|c$، آنگاه به‌ازای هر دو عدد صحیح s و t داریم $a|sb + tc$.

(v) به‌ازای هر عدد صحیح غیر صفر k، $a|b$ اگر و تنها اگر $ka|kb$.

نتیجهٔ آشنای زیر، که به **الگوریتم تقسیم** معروف است، ابزار مهمی در نظریهٔ اعداد است.

1. Aryabhata 2. Brahmagupta 3. Claude Bachet de Méziriac 4. Leonhard Euler
5. Joseph Louis Lagrange 6. Carl Friedrich Gauss 7. Disquisitiones Arithmeticae

صرف‌نظر از جزئیات، چنین می‌گوید که می‌توان عدد b را بر عدد a تقسیم کرد و باقیمانده‌ای کوچکتر از a به‌دست آورد. برهان قضیه ویژگی خوش‌ترتیبی زیر را که غالباً در این کتاب به‌کار می‌رود می‌طلبد:
ویژگی خوش‌ترتیبی: هر زیرمجموعهٔ ناتهی از اعداد صحیح مثبت یک کوچکترین عنصر دارد.

(۳.۱) قضیهٔ (الگوریتم تقسیم). فرض می‌کنیم a و b دو عدد صحیح باشند که a مثبت است. در این‌صورت، اعداد صحیح یکتای q و r وجود دارند به‌طوری که $b = qa + r$ و $0 \leq r < a$.

برهان. فرض کنیم S مجموعهٔ اعداد صحیح مثبت بزرگتر از b/a باشد. بنابر ویژگی خوش‌ترتیبی، S دارای یک کوچکترین عنصر مانند t است؛ بنابراین $t - 1 \leq b/a < t$. فرض کنیم $q = t - 1$، پس $qa \leq b < (q+1)a$. اگر قرار دهیم $r = b - qa$، آنگاه $b = qa + r$ و $0 \leq r < a$. عدد صحیح q خارج‌قسمت و r باقیمانده نامیده می‌شوند.

توضیح. واژهٔ الگوریتم از نام الخوارزمی ریاضیدان قرن نهم، کسی که در بیان دستگاه‌شمار هندی (یعنی، نمایش دهدهی اعداد صحیح که اکنون عمومیت دارد) کتابی نوشته، مشتق شده است. در اواخر قرون وسطی، کسانی که هنر محاسبه را با کاربرد نمایش دهدهی می‌دانستند حسابگر[1] نامیده می‌شدند. اینان به‌تدریج چرتکه‌کاران، یعنی کسانی را که با چرتکه اجدای محاسبه می‌کردند، روی کار آوردند.

الگوریتم به معنی روند محاسبهٔ مکانیکی آمده است. بدین معنی، در برهان قضیهٔ ۳.۱ یک الگوریتم ضمنی وجود دارد. مثلاً، اگر $b \geq 0$، عمل کم کردن a را از b تا آنجا ادامه می‌دهیم که آنچه می‌ماند کمتر از a باشد. روشن است که آنچه می‌ماند همان r است و تعداد دفعاتی که a را از b کم کرده‌ایم برابر q است. در حالت کلی، این الگوریتم فاقد کارایی است ــ روند آشنای «تقسیم طولانی» به مراتب بهتر است.

(۴.۱) تعریف. بزرگترین عدد صحیح مثبتی که هم a و هم b را می‌شمارد بزرگترین مقسوم‌علیه مشترک (بمعم) a و b خوانده می‌شود. آن را با (a, b) نشان می‌دهیم.

تعریف ۴.۱ تلویحاً الگوریتمی را برای محاسبهٔ بمعم دربر دارد. اگر a و b هر دو صفر باشند، بمعم وجود ندارد. اگر $a = 0$ و $b \neq 0$، بمعم برابر $|b|$ است. اگر a و b هر دو ناصفر باشند و $|b| \leq |a|$، همهٔ مقسوم‌علیه‌های مثبت a را ثبت می‌کنیم. بزرگترین آنها که b را نیز می‌شمارد همان بمعم است. در حالت کلی، این الگوریتم خیلی کارایی ندارد.

قضیهٔ بعد یک خصوصیت بسیار مفیدی از بمعم a و b را برحسب ترکیب خطی آنها، یعنی، مجموعه‌هایی به‌صورت $sa + tb$، که در آن s و t اعداد صحیح هستند، به‌دست می‌دهد. این

1. Algorist

قضیه غالباً در برهانهای بعدی این فصل بکار خواهد آمد.

(۵.۱) قضیه. فرض می‌کنیم a و b هر دو صفر نیستند، و $d = (a, b)$. در این‌صورت، d کوچکترین عدد صحیح مثبتی است که می‌توان آن را به‌صورت ترکیب خطی a و b بیان کرد.

برهان. چون روشن است که مجموعهٔ تمام ترکیبهای خطی a و b شامل اعداد صحیح مثبت (همچنین اعداد صحیح منفی و صفر) است. لذا شامل کوچکترین عنصر مثبتی است مانند m، مثلاً $m = sa + tb$. با استفاده از الگوریتم اقلیدسی می‌نویسیم $a = qm + r$، که $0 \leq r < m$. دراین‌صورت، $r = a - qm = a - q(sa + tb) = (1 - qs)a + (-qt)b$، و لذا r نیز یک ترکیب خطی از a و b است. اما $r < m$، بنابراین از تعریف m نتیجه می‌شود که $r = 0$. از این‌رو، $a = qm$، یعنی $m|a$؛ به طریق مشابه، $m|b$. لذا، m یک مقسوم‌علیه مشترک a و b است.

چون $d|a$ و $d|b$، لذا بنابر (iv.۲.۱)، هر ترکیب خطی آنها را می‌شمارد. بنابراین، $d|m$ و لذا $d \leq m$. چون d بزرگترین مقسوم‌علیه مشترک است، باید داشته باشیم $d = m$.

(۶.۱) فرع. اگر c یک مقسوم‌علیه مشترک a و b باشد، آنگاه $c|(a, b)$.

برهان. اگر $d = (a, b)$، می‌نویسیم $d = sa + tb$. چون $c|a$ و $c|b$، لذا (iv.۲.۱) ایجاب می‌کند که $c|d$.

توضیح. می‌توان بمعم a و b یعنی d را به‌ترتیب زیر نیز مشخص کرد: d عدد صحیح مثبت یکتایی است که (i) $d|a$ و $d|b$، و (ii) اگر $e|a$ و $e|b$، آنگاه $e|d$.

(۷.۱) قضیه. (i) به‌ازای هر عدد صحیح c، $(ca, cb) = c(a, b)$؛
(ii) اگر $d = (a, b)$، آنگاه $(a/d, b/d) = 1$.

برهان. برای اثبات (i) توجه کنید که کوچکترین عدد صحیح مثبتی که ترکیب خطی ca و cb باشد درست c برابر کوچکترین عدد صحیح مثبتی است که ترکیب خطی a و b باشد. اکنون از (۵.۱) استفاده کنید. قسمت (ii) از (i) با استفاده از a/d، b/d، و $c = d$ نتیجه می‌شود.

(۸.۱) تعریف. اعداد a و b را نسبت به هم اول خوانیم اگر $(a, b) = 1$، یعنی، اگر هیچ عامل (مثبت) مشترک جز ۱ نداشته باشند. اعداد m_1، m_2، ...، m_k را دو به دو نسبت به هم اول خوانیم اگر $i \neq j$ رابطهٔ $(m_i, m_j) = 1$ را ایجاب کند.

از (۵.۱) نتیجه می‌شود که اگر به‌ازای مقادیری از s و t، $sa+tb=1$، آنگاه a و b نسبت به هم اول‌اند. همچنین، اگر a و b هرکدام بر بمعم‌شان d تقسیم شوند، a/d و b/d نسبت به هم اول‌اند ((ii.۷.۱) را ببینید).

ویژگی زیر از اعداد صحیح نسبت به هم اول بسیار قابل استفاده است و نقش مهمی در اثبات قضیهٔ اصلی حساب (قضیهٔ ۱۶.۱) بازی می‌کند.

(۹.۱) قضیهٔ (اقلیدس). اگر $a|bc$ و $(a,b)=1$، آنگاه $a|c$.

برهان. از قضیهٔ (۷.۱) نتیجه می‌شود که $(ac,bc)=c(a,b)=c$. ملاحظه می‌کنید که a مقسوم‌علیهی از ac (به‌وضوح) و bc (بنا به فرض) است. بنابراین، از (۶.۱) نتیجه می‌شود که $a|c$.

(۱۰.۱) قضیهٔ (اقلیدس). فرض می‌کنیم a، b، و c اعداد صحیح باشند.

(i) اگر $(a,b)=(a,c)=1$، آنگاه $(a,bc)=1$.

(ii) اگر $a|c$، $b|c$، و $(a,b)=1$، آنگاه $ab|c$.

برهان. (i) بنابر (۵.۱) اعداد صحیحی چون s، t، u، و v وجود دارند که $sa+tb=1$ و $ua+vc=1$. در این‌صورت، $tb\cdot vc=(1-sa)(1-ua)=1-ma$، که در آن $m=s+u-sua$. لذا $ma+tv(bc)=1$، و قضیه از (۵.۱) به‌دست می‌آید.

(ii) فرض می‌کنیم $c=mb$. چون $a|mb$ و $(a,b)=1$، از (۹.۱) نتیجه می‌شود که $a|m$. اگر $m=na$، آنگاه $c=nab$ و لذا $ab|c$.

اکنون به تعریف مفهومی می‌پردازیم که تعریف بمعم دو عدد را کامل می‌کند. قضیهٔ (۱۳.۱) در زیر ارتباط بین آنها را نشان می‌دهد.

(۱۱.۱) تعریف. فرض می‌کنیم a و b دو عدد صحیح ناصفر باشند. کوچکترین عدد صحیح مثبتی که مضربی از a و b باشد کوچکترین مضرب مشترک a و b خوانده می‌شود. آن را با $[a,b]$ نشان می‌دهیم. کوچکترین مضرب مشترک a_1، a_2، ...، a_r به طریق مشابه با $[a_1,a_2,\ldots,a_r]$ نشان داده می‌شود.

(۱۲.۱) قضیه. اگر k مضرب مشترکی از a و b باشد، آنگاه $[a,b]|k$. لذا هر مضرب مشترک a و b به‌ازای عدد صحیحی مانند t به‌صورت $t[a,b]$ است.

برهان. فرض می‌کنیم $m=[a,b]$ و با استفاده از الگوریتم تقسیم می‌نویسیم $k=qm+r$، که $0\le r<m$. چون $a|k$ و $a|m$، داریم $a|r$؛ با استدلالی مشابه داریم، $b|r$. لذا r مضرب

مشترکی از a و b است که کمتر از m است. چون m کوچکترین مضرب مشترک است، در نتیجه $r = 0$، و از این‌رو $m|k$.

(۱۳.۱) قضیه. فرض می‌کنیم a و b اعداد صحیح مثبتی باشند. در این‌صورت $(a, b)[a, b] = ab$.

برهان. فرض کنیم $d = (a, b)$ و با استفاده از (۵.۱) می‌نویسیم $d = sa + tb$. چون $d|ab$، پس $m = ab/d$ عددی صحیح است. کافی است ثابت کنیم که $m = [a, b]$.

روشن است که m مضرب مشترکی از a و b است. همچنین، اگر n مضرب مشترک مثبت دلخواهی از a و b باشد، آنگاه $n/m = nd/ab = n(sa + tb)/ab = (n/b)s + (n/a)t$ عددی صحیح است. لذا $m|n$ و از این‌رو $m \leq n$. در نتیجه m کوچکترین مضرب مشترک a و b است.

اعداد اول

مطالعهٔ اعداد اول همیشه جزء مهمی از نظریهٔ اعداد بوده است، و قضیه‌های اولیه در این پهنه به یونانیها در سدهٔ چهارم قبل از میلاد مربوط می‌شود. در این بخش به ارائه مطالب پایه‌یی در اعداد اول می‌پردازیم. ویژگیهای عمیقتر اعداد اول در فصل ۷ بررسی خواهند شد. مطلب را با تعریف عدد اول آغاز می‌کنیم.

(۱۴.۱) تعریف. یک عدد اول عدد صحیحی است مانند $p > 1$ که هیچ مقسوم‌علیه مثبتی جز ۱ و خودش ندارد. (به عبارت دیگر، p هیچ مقسوم‌علیه سره ندارد.) هر عدد صحیح بزرگتر از ۱ که اول نباشد مرکب نامیده می‌شود. (عدد ۱ نه اول است و نه مرکب.)

به یک تعبیر، اعداد اول بلوکهای ساختمانی اعداد صحیح‌اند. قضیهٔ اصلی حساب حکم می‌کند که هر عدد صحیح مثبت بزرگتر از ۱ را می‌توان اساساً به یک طریق یکتا به‌صورت حاصلضرب اعداد اول (احتمالاً تکراری) نوشت. همهٔ ابزار لازم برای اثبات این قضیه در اصول اقلیدس آمده‌اند، ولی گاوس اولین کسی بود که در تحقیقات حسابی‌اش در ۱۸۰۱ این قضیه را بیان و ثابت کرد. به لم زیر نیاز داریم.

(۱۵.۱) لم. اگر p اول باشد و $p|ab$، آنگاه $p|a$ یا $p|b$. به‌طور کلی، اگر p حاصلضرب $a_1a_2 \ldots a_r$ را بشمارد، لااقل یکی از a_iها را می‌شمارد.

برهان. اگر $p|ab$ و $p\nmid a$، آنگاه $(p,a)=1$ و لذا (۹.۱) ایجاب می‌کند که $p|b$، حال، فرض کنیم $p|a_1a_2\dots a_r$. اگر $p\nmid a_1$، آنگاه $p|a_2\dots a_r$. اگر $p|a_2\dots a_r$ و $p\nmid a_2$، آنگاه $p|a_3\dots a_r$، و مانند آن، لذا، اگر p هیچ‌کدام از a_1، ...، a_{r-1} را نشمارد، آنگاه $p|a_r$.

(۱۶.۱) قضیهٔ اصلی حساب. هر عدد صحیح $n>1$ حاصلضربی از اعداد اول است. این نمایش، صرف‌نظر از ترتیب عوامل، یکتاست.

برهان. با استفاده از برهان خلف نشان می‌دهیم که n حداقل یک چنین نمایشی دارد. اگر عدد صحیحی بزرگتر از ۱ وجود داشته باشد که حاصلضرب اعداد اول نباشد، یک کوچکترین عدد صحیحی از این گونه اعداد، مانند m، وجود دارد، روشن است که m اول نیست. لذا می‌توانیم بنویسیم $m=rs$ با $1<r<m$ و $1<s<m$. از آنجا که r و s کوچکتر از m هستند، باید هر کدام حاصلضرب اعداد اول باشند، و لذا m نیز حاصلضرب اعداد اول است، که با تعریف m تناقض دارد. بنابراین، نتیجه می‌گیریم که هر عدد $n>1$ حاصلضرب اعداد اول (که لزوماً متمایز نیستند) است.

حال، فرض کنیم اعداد صحیحی بزرگتر از ۱ با دو تجزیهٔ متفاوت وجود داشته باشند؛ کوچکترین آنها را n می‌نامیم که به‌وضوح اول نیست. فرض می‌کنیم n اساساً دارای دو تجزیهٔ متفاوت $n=p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}=q_1^{b_1}q_2^{b_2}\dots q_s^{b_s}$ باشد، که در آن p_iها و q_jها اعداد اول متمایزند. چون p_1 طرف راست را می‌شمارد، از لم قبل نتیجه می‌شود که به‌ازای مقداری چون k، $p_1|q_k$؛ لذا $p_1=q_k$، زیرا هر دو اول‌اند. از تقسیم طرفین بر p_1 دو تجزیهٔ متفاوت از n/p_1 به‌دست می‌آوریم، که با تعریف n تناقض دارد، زیرا $1<n/p_1<n$. بنابراین، نتیجه می‌گیریم که صرف‌نظر از ترتیب عاملها، نمایش هر عدد بزرگتر از ۱ به‌صورت حاصلضرب اعداد اول یکتاست.

از قضیهٔ اصلی حساب نتیجه می‌شود که هر عدد صحیح بزرگتر از ۱ را می‌توان به‌صورت $p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$ نوشت، که در آن p_iها متمایز و نماها مثبت‌اند. این نمایش معمولاً تجزیهٔ n به عوامل اول خوانده می‌شود. برای نشان دادن $p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$، اغلب نماد $\prod_1^r p_i^{a_i}$، یا به‌طور ساده‌تر $\prod p_i^{a_i}$ را به‌کار می‌بریم.

قضیهٔ (۱۶.۱) روشی را برای یافتن بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک دو عدد نیز به‌دست می‌دهد. اگر لازم باشد با انتخاب بعضی نماها برابر صفر، می‌توان در تجزیهٔ دو عدد اعداد اول واحدی را به‌کار برد، مانند قضیهٔ زیر.

(۱۷.۱) قضیه. فرض کنیم $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ و $b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$، که در آنها a_iها و b_iها نامنفی هستند. به‌ازای $i = 1, 2, \dots, r$، m_i را مینیمم a_i و b_i و M_i را ماکسیمم a_i و b_i تعریف می‌کنیم. در این‌صورت

$$(a, b) = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r} \quad \text{و} \quad [a, b] = p_1^{M_1} p_2^{M_2} \dots p_r^{M_r}.$$

قضیهٔ (۱۷.۱) برهان خیلی آسانی از (۱۳.۱) را به‌دست می‌دهد: فقط ملاحظه کنید که $\min(m, n) + \max(m, n) = m + n$. به‌طور کلی، مسأله‌ای که فقط شامل حاصلضرب باشد (از جمله مفاهیم بخشپذیری، بزرگترین مقسوم‌علیه مشترک، و کوچکترین مضرب مشترک) معمولاً با کاربرد قضیهٔ اصلی حساب به طریقی ساده حل می‌شود.

اکنون که نشان دادیم هر عدد صحیح بزرگتر از ۱ یک مقسوم‌علیه اول دارد، در وضعیتی هستیم که ثابت کنیم تعداد اعداد اول نامتناهی است. برهان بی‌نهایت ساده است و در مقالهٔ IX از اصول اقلیدس آمده است.

(۱۸.۱) قضیهٔ (اقلیدس). بی‌نهایت عدد اول وجود دارد.

برهان. به‌ازای هر گردایهٔ متناهی از اعداد اول، نشان می‌دهیم که همواره می‌توان عدد اولی مانند q یافت که در گردایه نباشد. فرض کنیم p_1، p_2، ...، p_n اعداد اول مفروض باشند، و قرار می‌دهیم $N = p_1 p_2 \dots p_n + 1$. بنابر (۱۶.۱)، N مقسوم‌علیه اولی مانند q دارد (که ممکن است خود N باشد). اگر q یکی از p_iها باشد، آنگاه q حاصلضرب $p_1 p_2 \dots p_n$ را می‌شمارد، و چون $q|N$، در نتیجه q تفاضل آنها را می‌شمارد، یعنی $q|1$. این تناقض قضیه را ثابت می‌کند.

در حالی‌که بی‌نهایت عدد اول وجود دارد، به آسانی می‌توان نشان داد که فاصلهٔ بین دو عدد اول متوالی ممکن است اتفاقاً خیلی زیاد باشد. (مسأله ۲۸.۱ را ببینید.)

بعداً نشان می‌دهیم که تجزیهٔ به عواملِ اولِ یک عدد صحیح مثبت را چگونه می‌توان برای تعیین تعداد مقسوم‌علیه‌های مثبت و مجموع این مقسوم‌علیه‌ها به‌کار برد.

(۱۹.۱) تعریف. اگر n عدد صحیح مثبتی باشد، تعداد مقسوم‌علیه‌های مثبت n را با $\tau(n)$ نشان می‌دهیم، و مجموع همهٔ مقسوم‌علیه‌های مثبت آن را با $\sigma(n)$.

در قضیهٔ بعد، فرمولهایی برای $\tau(n)$ و $\sigma(n)$ برحسب تجزیهٔ n به اعداد اول به‌دست می‌آوریم.

(۲۰.۱) قضیه. فرض می‌کنیم $n > ۱$ و $n = p_۱^{n_۱} p_۲^{n_۲} \dots p_r^{n_r}$. در این صورت

$$\tau(n) = (n_۱ + ۱)(n_۲ + ۱) \cdots (n_r + ۱)$$

و

$$\sigma(n) = \frac{(p_۱^{n_۱+۱} - ۱)}{p_۱ - ۱} \frac{(p_۲^{n_۲+۱} - ۱)}{p_۲ - ۱} \cdots \frac{(p_r^{n_r+۱} - ۱)}{p_r - ۱}.$$

برهان. فرض کنیم $d = p_۱^{d_۱} p_۲^{d_۲} \dots p_r^{d_r}$ یک مقسوم‌علیه مثبت n باشد؛ در این‌صورت به‌ازای هر i، $d_i \le n_i$. تعداد $n_i + ۱$ انتخاب (یعنی، ۰، ۱، ...، n_i) برای d_i وجود دارد، و لذا می‌توان نماهای $d_۱$، ...، d_r را دقیقاً به $(n_۱ + ۱)(n_۲ + ۱) \cdots (n_r + ۱)$ طریق انتخاب کرد.

برای به‌دست آوردن $\sigma(n)$، ملاحظه می‌کنید که اگر جمله‌های حاصلضرب

$$P = (۱ + p_۱ + p_۱^۲ + \cdots + p_۱^{n_۱})(۱ + p_۲ + p_۲^۲ + \cdots + p_۲^{n_۲}) \cdots (۱ + p_r + p_r^۲ + \cdots + p_r^{n_r})$$

در هم ضرب شوند، مجموع تمام حاصلضربهای ممکن به‌صورت $p_۱^{a_۱} p_۲^{a_۲} \dots p_r^{a_r}$ حاصل می‌شود که در آن $۰ \le a_i \le n_i$. اما گردایهٔ چنین حاصلضربهایی دقیقاً همان مجموعهٔ تمام مقسوم‌علیه‌های مثبت n است، و لذا $\sigma(n) = P$. برای تکمیل برهان ملاحظه می‌کنیم که بنابر فرمول معمولِ جمع تصاعد هندسی، $۱ + p + p^۲ + \cdots + p^k = (p^{k+۱} - ۱)/(p - ۱)$. (برای اثبات این، $۱ + p + p^۲ + \cdots + p^k$ را در $p - ۱$ ضرب کنید.)

توضیح. توابع τ و σ مثالهایی از توابع حسابی هستند، و در یک ویژگی مهم شریک‌اند: τ و σ هر دو توابع ضربی هستند. یعنی، به‌ازای هر m و n که $(m, n) = ۱$ داریم

$$\tau(mn) = \tau(m)\tau(n) \quad \text{و} \quad \sigma(mn) = \sigma(m)\sigma(n)$$

به‌طور کلی، هر تابع f را که روی اعداد صحیح مثبت تعریف شده باشد ضربی خوانیم اگر $f(mn) = f(m)f(n)$ هر وقت که $(m, n) = ۱$. ضربی بودن τ و σ را با استفاده از فرمولهای به‌دست آمده در قضیهٔ (۲۰.۱) می‌توان به آسانی ثابت کرد. (مثال مهم دیگری از یک تابع ضربی تابع ϕی اویلر است، که در فصل ۳ معرفی خواهد شد.)

این بخش را با مطلب مهمی دربارهٔ تجزیه به اعداد اول فاکتوریلها خاتمه می‌دهیم.

(۲۱.۱) قضیهٔ (لژاندر). فرض کنیم p یک عدد اول باشد. بزرگترین توان p که $n!$ را می‌شمارد برابر است با $[n/p] + [n/p^2] + [n/p^3] + \cdots$، که در آن نماد $[x]$ جزء صحیح x را نشان می‌دهد.

برهان. می‌خواهیم تعداد عاملهای p را که در $n!$ ظاهر می‌شوند به‌دست آوریم. در بین اعداد ۱، ۲، ...، n، تعداد اعدادی که بر p بخشپذیرند درست برابر $[n/p]$ است. بعضی از این اعداد بر p^2 نیز بخشپذیرند و لذا در یک عامل اضافی p سهیم‌اند. به‌ویژه، دقیقاً تعداد $[n/p^2]$ وجود دارند که از n تجاوز نمی‌کنند و بر p^2 بخشپذیرند. همچنین، اعداد بخشپذیر بر p^3 در یک عامل اضافی دیگری سهیم‌اند و بر همین قیاس ... . لذا مجموع $[n/p] + [n/p^2] + \cdots$ تعداد کلی عاملهای p در $n!$ را به‌دست می‌دهد. توجه کنید که این مجموع فقط تعداد متناهی جملهٔ غیرصفر دارد، زیرا به‌ازای یک عدد مفروض n، اگر k به اندازهٔ کافی بزرگ باشد $n/p^k < 1$ و لذا $[n/p^k] = 0$.

الگوریتم اقلیدسی

اکنون به بیان الگوریتم اقلیدسی، روشی نظام‌مند و کارآمد برای محاسبهٔ بمعم دو عدد، می‌پردازیم. قضیهٔ VII.۲ یِ اصول اقلیدس این الگوریتم را بیان و اثبات می‌کند که با این روش بمعم محاسبه می‌شود، ولی احتمالاً این روشِ کار قبل از اقلیدس وجود داشته است.

لم زیرکلید فهم الگوریتم اقلیدسی است.

(۲۲.۱) لم. فرض می‌کنیم m و n هر دو ناصفر باشند. در این‌صورت به‌ازای هر t، $(m, n) = (n, m - tn)$.

برهان. اگر e یک مقسوم‌علیه مشترک m و n باشد، آنگاه بنابر (۲.۱)، $e|m - tn$، و لذا e یک مقسوم‌علیه مشترک n و $m - tn$ است. همچنین، اگر e یک مقسوم‌علیه مشترک دلخواه n و $m - tn$ باشد، آنگاه $e|m$، و لذا e یک مقسوم‌علیه مشترک m و n است. به‌ویژه، از اینجا نتیجه می‌شود که بزرگترین مقسوم‌علیه مشترک m و n همان بزرگترین مقسوم‌علیه مشترک $m - tn$ و n است، یعنی $(m, n) = (n, m - tn)$.

مفید بودن این لم را با مثال زیر روشن می‌سازیم.

مثال. فرض کنید می‌خواهیم (۹۹۶, ۲۳۴) را محاسبه کنیم. بنابر لم قبل و با $t = 1$ داریم (۲۳۴, ۹۹۶ − ۲۳۴) = (۹۹۶, ۲۳۴)؛ بمعم تغییر نکرده است، ولی یکی از اعداد کوچکتر شده است. می‌توانیم به این ترتیب ادامه دهیم، یعنی مرتباً عدد کوچکتر را از عدد

بزرگتر کم کنیم (این همان عبارت اقلیدس بوده است)، اما روش سریعتری وجود دارد. ۹۹۶ را بر ۲۳۴ تقسیم می‌کنیم، داریم $۹۹۶ = ۴ \times ۲۳۴ + ۶۰$. بنابر (۲۲.۱) با $t = ۴$ داریم $(۲۳۴, ۶۰) = (۲۳۴, ۹۹۶ - ۴ \times ۲۳۴) = (۹۹۶, ۲۳۴)$. حال، مجدداً این لم را برای $(۲۳۴, ۶۰)$ به‌کار می‌بریم. با تقسیم ۲۳۴ بر ۶۰ داریم $۲۳۴ = ۳ \times ۶۰ + ۵۴$؛ لذا $(۶۰, ۵۴) = (۲۳۴, ۶۰)$. یک‌بار دیگر (۲۲.۱) را با $t = ۱$ به‌کار می‌بریم، داریم $(۵۴, ۶) = (۶۰, ۵۴)$. یا با استفادهٔ مجدد از (۲۲.۱) رابطهٔ $(۶, ۰) = (۵۴, ۶)$ را به‌دست می‌آوریم، و یا اصلاً ملاحظه می‌کنیم که $(۵۴, ۶) = ۶$، زیرا $۶ | ۵۴$. (اگر محاسبات را دستی انجام می‌دهیم همین‌که به بمعم رسیدیم توقف می‌کنیم.)

چیزی که محاسبات فوق را عملی می‌سازد آن است که وقتی اعداد مورد نظر تغییر می‌کنند (در واقع، به سرعت نزول می‌کنند)، بمعمشان تغییر نمی‌کند. اکنون مسأله را در حالت کلی در نظر می‌گیریم. به‌ازای هر عدد صحیح c، مقسوم‌علیه‌های c دقیقاً همان مقسوم‌علیه‌های $-c$ هستند؛ لذا همواره داریم $(a, b) = (|a|, |b|)$. از این‌رو، برای محاسبهٔ (a, b)، می‌توانیم فرض کنیم که a و b نامنفی‌اند. بی‌آنکه به کلیت خللی وارد آید، فرض خواهیم کرد که $a \geq b > ۰$.

روند کاهش مشروح در مثال بالا را به‌طور مکرر به‌کار می‌بریم. اگر در مرحلهٔ معینی بخواهیم (m, n) را پیدا کنیم، که در آن $m \geq n$ و $n \neq ۰$، از تقسیم m بر n فرض می‌کنیم $m = qn + r$. در این‌صورت، $r = m - qn$ و لذا بنابر (۲۲.۱)، $(m, n) = (n, r)$. اگر $r \neq ۰$، مجدداً روند را برای دو عدد n و r به‌کار می‌بریم. اگر $r = ۰$، توقف می‌کنیم؛ در این حالت $(m, n) = n$.

روشن است که روند بالا باید پایانی داشته باشد، زیرا در هر مرحله کوچکترین عدد از دو عددی که در نظر می‌گیریم لااقل یک عدد کم می‌شود و از این‌رو باید حداکثر در b مرحله به ۰ برسد. در واقع الگوریتم اقلیدسی زودتر از آن به پایان می‌رسد.

(۲۳.۱) الگوریتم اقلیدسی. فرض می‌کنیم $a \geq b > ۰$. برای یافتن (a, b)، اول فرض می‌کنیم $m = a$ و $n = b$، و r باقیماندهٔ تقسیم m بر n باشد. اگر $r \neq ۰$، به‌جای m، n می‌گذاریم و به‌جای n، r سپس این فرایند را تکرار می‌کنیم. اگر $r = ۰$، آنگاه $(a, b) = n$.

اکنون نشان می‌دهیم که چگونه با استفاده از الگوریتم اقلیدسی اعداد صحیح x و y را محاسبه می‌کنیم به‌طوری که $ax + by = (a, b)$. برای سهولت در نمادگذاری، قرار می‌دهیم $r_۰ = a$ و $r_۱ = b$. در این‌صورت الگوریتم اقلیدسی را می‌توان به شرح زیر بیان کرد. فرض می‌کنیم $r_۲$

باقیماندهٔ تقسیم r_0 بر r_1، r_3 باقیماندهٔ تقسیم r_1 بر r_2، به همین قیاس باشد. مقداری از k، $k \geq 1$ وجود دارد که $r_{k+1} = 0$ و محاسبه خاتمه می‌یابد. در این‌صورت $(a, b) = r_k$. (r_k آخرین باقیماندهٔ ناصفر) اگر q_i خارج‌قسمت تقسیم r_{i-1} بر r_i باشد، داریم

$$\begin{aligned}
a = r_0 &= q_1 r_1 + r_2, & 0 < r_2 < r_1,\\
b = r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2,\\
r_2 &= q_3 r_3 + r_4, & 0 < r_4 < r_3,\\
&\vdots\\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= q_k r_k .
\end{aligned}$$

از معادلهٔ ماقبل آخر شروع می‌کنیم و r_k را برحسب r_{k-1} و r_{k-2} به‌دست می‌آوریم. سپس r_{k-1} را از معادلهٔ قبلی (یعنی دو معادله به آخر مانده) پیدا کرده در رابطه‌ای که به‌دست آورده‌ایم جانشین می‌کنیم. به همین ترتیب ادامه می‌دهیم و متوالیاً باقیمانده‌های r_{k-1}، r_{k-2}، ...، r_2 را حذف می‌کنیم. معادلهٔ آخر، r_k یعنی بمعم a و b را به‌صورت ترکیب خطی از a و b به‌دست می‌دهد. (تمرین ۳.۱ را ببینید.)

توضیح محاسبه‌یی. صورت دیگری از الگوریتم اقلیدسی، موسوم به الگوریتم اقلیدسی منبسط، وجود دارد که اعداد صحیح x و y را به‌طور همزمان به‌دست می‌دهد به گونه‌ای که $ax + by = (a, b)$. این روند کار مؤثر و انجام آن با کامپیوتر یا رایانه‌هایی که قابل برنامه‌ریزی باشند آسان است.

این الگوریتم را به‌گونه‌ای که در ۲۳.۱ گفته شد به‌کار می‌بریم. روشن است که، a و b ترکیبهای خطی a و b هستند. حال فرض کنیم m و n را به‌صورت ترکیبهای خطی از a و b، مثلاً $m = as + bt$ و $n = au + bv$ نوشته‌ایم. می‌نویسیم $m = qn + r$، که $0 \leq r < n$. اگر $r = 0$، آنگاه $n = (a, b)$، و لذا نمایشی از (a, b) به‌صورت یک ترکیب خطی از a و b یافته‌ایم. اگر $r \neq 0$، آنگاه $r = m - nq = as + bt - q(au + bv) = a(s - qu) + b(t - qv)$ یک ترکیب خطی از a و b است. از آنجا که (a, b) آخرین باقیماندهٔ ناصفر است، سرانجام نمایشی از (a, b) به‌صورت $ax + by$ به‌دست می‌آوریم.

معادلهٔ $ax + by = c$

در کارهای دیوفانتوس اسکندرانی (حدود ۲۵۰ بعد از میلاد) روشهای نظام‌مندی برای استخراج جوابهای گویای بعضی از معادلات آمده است. در ابتدا، عبارت معادلهٔ دیوفانتی[1] به معادله‌ای گفته می‌شده که جوابهایش به اعداد گویا محدود می‌شدند، اما اکنون در مورد معادلاتی به‌کار می‌رود که در آنها جوابهای صحیح جستجو می‌شوند. این معادله‌ها به تفصیل در فصل ۸ مورد مطالعه قرار می‌گیرند.

در این بخش، به بررسی جوابهای صحیح معادلهٔ $ax + by = c$ می‌پردازیم، زیرا وجود و شکل جوابهایش از قضیه‌های قبلی این فصل نتیجه می‌شوند. به‌ویژه، نشان خواهیم داد که اگر چنین معادله‌ای یک جواب در اعداد صحیح داشته باشد، بی‌نهایت جواب صحیح دارد.

(۲۴.۱) قضیه. معادلهٔ $ax + by = c$ جواب صحیح دارد اگر و تنها اگر $d|c$. اگر $d = (a, b)$، x^*، y^* یک جواب خصوصیِ این معادله باشد، همهٔ جوابها به‌صورت زیرند

$$x = x^* + (b/d)t \quad \text{و} \quad y = y^* - (a/d)t \qquad (۱)$$

که در آن t عدد صحیحی است دلخواه.

برهان. فرض می‌کنیم که $ax + by = c$ دارای جواب باشد؛ چون $d|a$ و $d|b$، بنابر (iv.۲.۱) باید داشته باشیم $d|c$. لذا جواب صحیح وجود ندارد مگر آنکه $d|c$.

حال، فرض کنیم $d|c$، و می‌نویسیم $c = kd$. بنابر (۵.۱)، اعداد صحیح r و s وجود دارند به‌طوری که $ra + sb = d$، و لذا $x^* = rk$، $y^* = sk$ یک جواب $ax + by = c$ است، روشن است که اگر x، y مانند (۱) تعریف شده باشند، آنگاه $ax + by = c$. بعکس، اگر x، y جوابی از این معادله باشند، آنگاه $ax + by = ax^* + by^* = c$، و لذا $a(x - x^*) = b(y^* - y)$. از تقسیم طرفین این رابطه بر d داریم $(a/d)(x - x^*) = (b/d)(y^* - y)$. از آنجا که a/d طرف راست را می‌شمارد و (بنابر (ii.۷.۱)) $(a/d, b/d) = ۱$، لذا بنابر (۹.۱)، a/d باید $y^* - y$ را بشمارد. بنابراین عدد صحیح t وجود دارد که $y^* - y = (a/d)t$، یعنی، $y = y^* - (a/d)t$. با گذاشتن این مقدار در $(a/d)(x - x^*) = (b/d)(y^* - y)$ خواهیم داشت $x - x^* = (b/d)t$، و لذا $x = x^* + (b/d)t$.

توضیح. بنابه تعریف، یک نقطهٔ مشبکه نقطه‌ای است مانند (x, y) در صفحه که x و y هر دو صحیح باشند. در این‌صورت (۲۴.۱) ایجاب می‌کند که اگر خط مستقیم $ax + by = c$ (با a، b، c اعداد صحیح) از یک نقطهٔ مشبکه بگذرد، از بی‌نهایت نقطهٔ مشبکه خواهد گذشت.

1. Diophantine equation

سرانجام، به دنبال شرایطی در a، b، و c هستیم که وجود جواب مثبت را تضمین کند، یعنی، جوابی با $x > ۰$ و $y > ۰$. در بررسی معادلهٔ $ax + by = c$، می‌توانیم فرض کنیم که $d = (a, b) = ۱$. (در غیر این‌صورت، معادلهٔ هم‌ارز $(a/d)x + (b/d)y = c/d$ را بررسی می‌کنیم که در آن $(a/d, b/d) = ۱$.)

(۲۵.۱) قضیه. فرض می‌کنیم a، b، و c اعداد صحیح مثبت باشند، با $(a, b) = ۱$، و فرض می‌کنیم x^*، y^* جواب دلخواهی از $ax + by = c$ باشد. در این‌صورت، تعداد جوابهای مثبت $ax+by = c$ برابر تعداد اعداد صحیح t است که $-x^*/b < t < y^*/a$. به‌ویژه، $ax+by = c$ دارای حداقل n جواب مثبت است هرگاه $c > nab$.

برهان. با قرار دادن $x > ۰$ و $y > ۰$ در صورت کلی جوابها داریم $-x^*/b < t < y^*/a$. (۱) لذا تعداد جوابهای مثبت معادله با تعداد اعداد صحیحی که در (۱) صدق می‌کنند برابر است. در نتیجه معادلهٔ $ax+by = c$ حداقل دارای n جواب مثبت است هرگاه $y^*/a-(-x^*/b) > n$. این نابرابری اخیر برقرار است اگر و تنها اگر $by^* + ax^* > nab$. چون $by^* + ax^* = c$، قضیه ثابت می‌شود.

فرض کنیم تعداد جوابهای مثبت $ax+by = c$ برابر N باشد. اگر c/ab عددی صحیح باشد، آنگاه $N = (c/ab) - ۱$. اگر c/ab عدد صحیح نباشد، N با $[c/ab]$ یا با $[c/ab] + ۱$ برابر است. از این‌رو تعداد جوابهای مثبت تقریباً، و نه کاملاً، با c/ab معین می‌شود. (مثلاً، معادله‌های $x + ۱۵y = ۲۳$ و $۳x + ۵y = ۲۳$ را در نظر بگیرید. معادلهٔ اول یک جواب دارد و معادلهٔ دوم دو جواب مثبت، اما در هر دو حالت، $c/ab = ۲۳/۱۵$.

مسأله‌ها و راه‌حلها

بخشپذیری، بزرگترین مقسوم‌علیه مشترک، کوچکترین مضرب مشترک، الگوریتم اقلیدسی

۱.۱ بمعم ۲۱۰ و ۴۹۵ را تعیین کنید، و آن را به‌صورت ترکیب خطی صحیح از ۲۱۰ و ۴۹۵ بیان کنید.

حل. با کاربرد الگوریتم اقلیدسی داریم: $۴۹۵ = ۲ \times ۲۱۰ + ۷۵$، $۲۱۰ = ۲ \times ۷۵ + ۶۰$، $۷۵ = ۱ \times ۶۰ + ۱۵$، $۶۰ = ۴ \times ۱۵$. لذا $(۴۹۵, ۲۱۰) = ۱۵$. همچنین،

$$۱۵ = ۷۵ - ۱ \times ۶۰ = ۷۵ - ۱(۲۱۰ - ۲ \times ۷۵) = ۳ \times ۷۵ - ۱ \times ۲۱۰$$
$$= ۳(۴۹۵ - ۲ \times ۲۱۰) - ۱ \times ۲۱۰ = ۳ \times ۴۹۵ - ۷ \times ۲۱۰$$

۲.۱ بمعم اعداد (الف) ۲۷۱ و ۳۳۷؛ (ب) ۱۱۲۸ و ۱۶۳۶؛ (ج) ۵۱۹ و ۱۷۳۰ را با استفاده از الگوریتم اقلیدسی به‌دست آورید.

حل. (الف) $۳۳۷ = ۲۷۱ + ۶۶$، $۲۷۱ = ۴ \times ۶۶ + ۷$، $۶۶ = ۹ \times ۷ + ۳$، $۷ = ۲ \times ۳ + ۱$؛ لذا $۱ = (۲۷۱, ۳۳۷)$، آخرین باقیماندهٔ غیرصفر.

(ب) $۵۰۸ = ۱۱۲۸ + ۵۰۸$، $۱۱۲۸ = ۲ \times ۵۰۸ + ۱۱۲$، $۱۱۲ = ۴ \times ۱۱۲ + ۶۰$، $۵۰۸ = ۴ \times ۱۱۲ + ۵۲$، $۶۰ = ۱ \times ۵۲ + ۸$، $۵۲ = ۶ \times ۸ + ۴$، $۸ = ۲ \times ۴ + ۰$؛ لذا $۴ = (۱۱۲۸, ۱۶۳۶)$.

(ج) $۱۷۳۰ = ۳ \times ۵۱۹ + ۱۷۳$، $۵۱۹ = ۳ \times ۱۷۳ + ۰$، و لذا $۱۷۳ = (۵۱۹, ۱۷۳۰)$.

۳.۱ بمعم ۱۷۶۹ و ۲۳۷۸ را به‌دست آورید و آن را به‌صورت ترکیب خطی از این دو عدد بیان کنید.

حل. $۶۰۹ = ۱ \times ۱۷۶۹ + ۶۰۹$، $۱۷۶۹ = ۲ \times ۶۰۹ + ۵۵۱$، $۵۵۱ = ۱ \times ۵۵۱ + ۵۸$، $۶۰۹ = ۱ \times ۵۵۱ + ۵۸$، $۵۸ = ۹ \times ۵۸ + ۲۹$، و $۲ = ۲ \times ۲۹ + ۰$. لذا $۲۹ = (۱۷۶۹, ۲۳۷۸)$. سپس

$$۲۹ = ۵۵۱ - ۹ \times ۵۸ = ۵۵۱ - ۹(۶۰۹ - ۵۵۱) = ۱۰ \times ۵۵۱ - ۹ \times ۶۰۹$$
$$= ۱۰(۱۷۶۹ - ۲ \times ۶۰۹) - ۹ \times ۶۰۹ = ۱۰ \times ۱۷۶۹ - ۲۹ \times ۶۰۹$$
$$= ۱۰ \times ۱۷۶۹ - ۲۹(۲۳۷۸ - ۱۷۶۹) = ۳۹ \times ۱۷۶۹ - ۲۹ \times ۲۳۷۸.$$

۴.۱ الگوریتم بمعم دوتایی را که در یادداشتهای آخر فصل بیان شده است برای یافتن سه جفت اعداد مسألهٔ ۲.۱ به‌کار برید.

حل. (الف)

$$(۲۷۱, ۳۳۷) = (۲۷۱, ۳۳۷ - ۲۷۱) = (۲۷۱, ۶۶) = (۲۷۱, ۳۳) = (۳۳, ۲۷۱ - ۳۳)$$
$$= (۳۳, ۲۳۸) = (۳۳, ۱۱۹) = (۳۳, ۱۱۹ - ۳۳) = (۳۳, ۸۶) = (۳۳, ۴۳) = ۱.$$

(ب)

$$(۱۱۲۸, ۱۶۳۶) = ۲(۵۶۴, ۸۱۸) = ۴(۲۸۲, ۴۰۹) = ۴(۱۴۱, ۴۰۹) = ۴(۱۴۱, ۲۶۸)$$
$$= ۴(۱۴۱, ۱۳۴) = ۴(۱۴۱, ۶۷) = ۴(۷۴, ۶۷) = ۴(۳۷, ۶۷) = ۴.$$

(ج)

$$(۵۱۹, ۱۷۳۰) = (۵۱۹, ۸۶۵) = (۵۱۹, ۳۴۶) = (۵۱۹, ۱۷۳) = (۳۴۶, ۱۷۳)$$
$$= (۱۷۳, ۱۷۳) = ۱۷۳$$

۵.۱ آیا دو عدد a و b وجود دارند که مجموعشان ۵۰۰ و بمعمشان ۷ باشد؟

حل. نه. اگر $(a, b) = ۷$، آنگاه $۷|a$ و $۷|b$، و لذا $۷|a + b$. اما ۵۰۰ بر ۷ قابل قسمت نیست.

۶.۱ فرض کنید a، b، c، و d اعداد صحیح مثبت باشند، که $b \neq d$. اگر $(a, b) = (c, d) = ۱$ ثابت کنید $a/b + c/d$ نمی‌تواند عدد صحیح باشد.

حل. برخلاف فرض می‌کنیم که $a/b + c/d = n$، که n عددی صحیح است. در این‌صورت، $ad + bc = bdn$، یعنی، $ad = b(dn - c)$. لذا $b|ad$، و چون $(a, b) = ۱$، پس $b|d$. به طریق مشابه می‌توانیم نشان دهیم که $d|b$. بنابراین $b = d$، که یک تناقض است.

۷.۱ ثابت کنید که n و $n + ۱$ همیشه نسبت به هم اول‌اند.

حل. هر مقسوم‌علیه مشترک n و $n + ۱$ باید $(n + ۱) - n = ۱$ را بشمارد.

۸.۱ نشان دهید که $n! + ۱$ و $(n + ۱)! + ۱$ نسبت به هم اول‌اند. (راهنمایی: عدد اولی را در $n + ۱$ ضرب کنید.)

حل. اگر $d > ۰$ یک مقسوم‌علیه مشترک این دو عدد باشد، آنگاه d ترکیب خطی $(n + ۱)(n! + ۱) - ((n + ۱)! + ۱)$ را که برابر n است، می‌شمارد. اما اگر $d|n$ و $d|n! + ۱$، آنگاه $d|۱$. لذا $d = ۱$.

۹.۱ اگر n فرد باشد، ثابت کنید n و $n - ۲$ نسبت به هم اول‌اند.

حل. اگر $d = (n, n - ۲)$، آنگاه $d|n - (n - ۲) = ۲$. اما چون n فرد است پس $d \neq ۲$، و لذا $d = ۱$.

۱۰.۱ اگر $(a, b) = ۱$، ثابت کنید $(a + b, a - b)$ برابر ۱ یا ۲ است.

حل. فرض کنیم $d = (a+b, a-b)$. لذا $d|(a+b) \pm (a-b)$، یعنی $d|2a$ و $d|2b$. لذا بنابر (i.۷.۱)، $d|(2a, 2b) = 2(a, b)$. پس d برابر ۱ یا ۲ است. اما اگر یکی از a و b فرد و دیگری زوج باشد، $a+b$ فرد است و در این حالت $d = 1$. در غیر این‌صورت، یعنی اگر a و b هر دو فرد باشند، $a+b$ زوج است و لذا $d = 2$. (حل با تغییراتی از مترجم).

۱۱.۱ اثبات یا رد کنید. به‌ازای هر $k \geq 1$، اعداد صحیح $6k+5$ و $7k+6$ نسبت به هم اول‌اند.

حل. این حکم برقرار است، زیرا $6(7k+6) - 7(6k+5) = 1$. لذا هر مقسوم‌علیه مشترک $6k+5$ و $7k+6$ باید ۱ را بشمارد.

۱۲.۱ اگر $(a, b) = 1$ و $c|a+b$، ثابت کنید که $(a, c) = (b, c) = 1$.

حل. فرض کنیم $d = (a, c)$. از $d|c$ نتیجه می‌شود که $d|a+b$، چون $d|a$، همچنین داریم $d|b$. لذا $d = 1$. استدلال مشابه نشان می‌دهد که $(b, c) = 1$.

۱۳.۱ اگر $(b, c) = 1$ و $m|b$، ثابت کنید $(m, c) = 1$.

حل. فرض کنیم $d = (m, c)$؛ لذا $d|c$ و $d|m$. چون $m|b$، پس $d|b$، و لذا d یک مقسوم‌علیه مشترک b و c است و چون $(b, c) = 1$ پس $d = 1$.

برهان دیگر: بنابر (۵.۱)، دو عدد صحیح r و s وجود دارند به‌طوری که $rb + sc = 1$. فرض می‌کنیم $b = mk$. در این‌صورت، $(rk)m + sc = 1$، و لذا $(m, c) = 1$.

۱۴.۱ اگر b مثبت باشد، نشان دهید که در دنبالهٔ اعداد n، $2n$، $3n$، ...، bn، دقیقاً تعداد (b, n) عدد وجود دارد که مضرب b هستند.

حل. فرض کنیم $d = (b, n)$، و می‌نویسیم $n = md$، $b = ad$. در این‌صورت، kn مضربی از b است اگر و تنها اگر km مضربی از a باشد. اما چون $(a, m) = 1$، این برقرار است اگر و تنها اگر k مضربی از a باشد. تعداد این‌گونه kها با شرط $1 \leq k \leq b$ برابر است با $b/a = d$.

◁ **۱۵.۱** مجموع دو عدد مثبت ۵۴۳۲ و کوچکترین مضرب مشترکشان ۲۲۳۰۲۰ است، آن دو عدد را بیابید.

حل. فرض کنیم a و b آن دو عدد باشند، لذا $a + b = 5432$ و $[a, b] = 223020$. اگر $(a, b) = d$، داریم $a = a'd$ و $b = b'd$ که $(a', b') = 1$ (۱). همچنین داریم

$[a,b]=ab/d$ بنابراین، $d(a',b')=۵۴۳۲$ و $a'b'd=۲۲۳۰۲۰$. اما با توجه به (۱)، داریم $(a'+b',a'b')=۱$. پس $(d(a'+b'),a'b'd)=d$ یا $d=(۵۴۳۲,۲۲۳۰۲۰)=۲۸$. در نتیجه $a'+b'=۱۹۴$ و $a'b'=۷۹۶۵$. بنابراین a' و b' دو عدد نسبت به هم اول هستند که در معادلهٔ $x^۲-۱۹۴x+۷۹۶۵=۰$ صدق می‌کنند. از حل این معادله داریم $a'=۱۳۵$ و $b'=۵۹$، سرانجام $a=۱۳۵\times۲۸=۳۷۸۰$ و $b=۵۹\times۲۸=۱۶۵۲$. (حل اصلی قدری تغییر داده شد. مترجم)

راه‌حل دیگر مسألهٔ ۱۵.۱:

فرض کنیم a و b آن دو عدد باشند؛ لذا $a+b=۵۴۳۲$ و $[a,b]=۲۲۳۰۲۰$. اگر p عدد اولی باشد که $[a,b]$ و $a+b$ را بشمارد، آنگاه چون $p|[a,b]$، پس p لااقل یکی از a و b را نیز می‌شمارد، و چون p عدد $a+b$ را نیز می‌شمارد، لذا p اعداد a و b هر دو را می‌شمارد. اکنون می‌توانیم a و b را بر p و $[a,b]$ را نیز بر p تقسیم کنیم. این عمل را آن‌قدر ادامه می‌دهیم تا دو عدد A و B که نسبت به هم اول‌اند را به‌دست آوریم. در مورد این مسأله، چون $۲۸=(۵۴۳۲,۲۲۳۰۲۰)$، داریم $a=۲۸A$ و $b=۲۸B$، $A+B=۵۴۳۲/۲۸=۱۹۴$، $[A,B]=۲۲۳۰۲۰/۲۸=۷۹۶۵$.

چون $(A,B)=۱$، از (۱۳.۱) نتیجه می‌شود که $[AB]=AB$. اکنون برای یافتن A و B معادلات $A+B=۱۹۴$ و $AB=۷۹۶۵$ را حل می‌کنیم. با جانشینی $B=۱۹۴-A$ در معادلهٔ دوم داریم $A^۲-۱۹۴A+۷۹۶۵=۰$. این معادله دارای جوابهای $A=۵۹$ و $A=۱۳۵$ است، که $B=۱۳۵$ یا $B=۵۹$ را نتیجه می‌دهد. از این‌رو اعداد مورد نظر عبارت‌اند از $۵۹\times۲۸=۱۶۵۲$ و $۱۳۵\times۲۸=۳۷۸۰$.

۱۶.۱ اگر $m\geq۱$، ثابت کنید $[ma,mb]=m[a,b]$.

حل. فرض کنیم $s=[ma,mb]$ و $t=[a,b]$؛ در این‌صورت mt مضربی از ma و mb است، و لذا $mt\geq s$. چون s نیز مضربی از ma و mb است، s/m مضربی از a و b است و لذا $s/m\geq t$، یعنی $s\geq mt$. بنابراین $s=mt$.

برهان دیگر: بنابر (۷.۱)، $(ma,mb)=m(a,b)$، و لذا (۱۳.۱) ایجاب می‌کند که $[ma,mb]=(ma)(mb)/(ma,mb)=mab/(a,b)=m[a,b]$. (با توجه به تجزیه به عوامل اول نیز می‌توانیم این قضیه را ثابت کنیم.)

۱۷.۱ اگر d و M اعداد صحیح مثبتی باشند، ثابت کنید که دو عدد صحیح a و b وجود دارند به‌طوری که $d=(a,b)$ و $M=[a,b]$ اگر و تنها اگر $d|M$.

حل. از آنجا که هر مقسوم‌علیه مشترک دو عدد کوچکترین مضرب مشترک آنها را می‌شمارد، شرط $d|M$ لازم است. پس فرض می‌کنیم $d|M$. با فرض $a = d$ و $b = M$، آشکار است که $(a, b) = d$ و $[a, b] = M$.

۱۸.۱ اگر x و y اعداد صحیح باشند، کوچکترین عدد گویای مثبتی را به‌دست آورید که بتوان آن را به‌صورت $x/۳۰ + y/۳۶$ نوشت.

حل. فرض کنیم $x/۳۰ + y/۳۶ = r$. پس $۳۶x + ۳۰y = (۳۰ \times ۳۶)r$. برای آنکه r مثبت و به‌قدر ممکن کوچک باشد، مقدار $۳۶x + ۳۰y$ را مثبت و به‌قدر ممکن کوچک می‌سازیم. کوچکترین مقدار مثبت $۳۶x + ۳۰y$ عبارت است از $۶ = (۳۶, ۳۰)$. لذا کوچکترین مقدار مثبت $x/۳۰ + y/۳۶$ عبارت است از $۱/۱۸۰ = ۶/(۳۰ \times ۳۶)$. (استدلال مشابه نشان می‌دهد که کوچکترین مقدار مثبت $x/a + y/b$ عبارت است از $۱/N$، که در آن N کوچکترین مضرب مشترک a و b است.)

◁ **۱۹.۱** یک صفحهٔ کاغذ به ارتفاع ۱۱ اینچ را با رسم ۲۱ خط موازی آبی‌رنگ به ۲۲ نوار با ارتفاعهای مساوی تقسیم می‌کنیم. حال، ۳۷ خط موازی قرمز رنگ رسم می‌کنیم به‌طوری که کاغذ را به ۳۸ نوار با ارتفاع مساوی تقسیم کند. کوچکترین فاصلهٔ بین یک خط آبی و یک خط قرمز چقدر است؟

حل. فرض کنیم $a = ۱۱/۲۲$ و $b = ۱۱/۳۸$. مقصود یافتن اعداد صحیح مثبت $x \leq ۲۱$ و $y \leq ۳۷$ است به‌طوری که $|x(۱۱/۲۲) - y(۱۱/۳۸)|$ به‌قدر ممکن کوچک باشد. این مقصود برآورده می‌شود هرگاه $|۱۱y - ۱۹x|$ به‌قدر ممکن کوچک باشد، روشن است که، کوچکترین مقدار ممکن برای $|۱۱y - ۱۹x|$ برابر ۱ است زیرا ۱۱ و ۱۹ نسبت به هم اول‌اند؛ این مقدار مثلاً، به‌ازای $x = ۴$ و $y = ۷$ حاصل می‌شود. در نتیجه فاصلهٔ مینیمم برابر $۱/۳۸$ است.

اعداد اول و تجزیه به عوامل اول

۲۰.۱ بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک $a = ۲^۳ \times ۳^۲ \times ۱۱^۴ \times ۳۷^۳$ و $b = ۲^۲ \times ۳ \times ۵^۲ \times ۷ \times ۱۱ \times ۲۹ \times ۳۷^۴$ را به‌دست آورید.

حل. بنابر (۱۷.۱) داریم $(a, b) = ۲^۲ \times ۳ \times ۱۱ \times ۳۷^۳$ و

$$[a, b] = ۲^۳ \times ۳^۲ \times ۵^۲ \times ۷ \times ۱۱^۴ \times ۲۹ \times ۳۷^۴$$

۲۱.۱ کوچکترین مضرب مشترک اعداد ۱، ۲، ...، ۳۰ چقدر است؟

حل. به‌ازای هر عدد اول p، بزرگترین توان p که کمم اعداد ۱، ۲، ...، ۳۰ را بشمارد بزرگترین توان p است که دست‌کم یکی از اعداد ۱، ۲، ...، ۳۰ را بشمارد. بنابراین، جواب عبارت است از $۲^۴ \times ۳^۳ \times ۵^۲ \times ۷ \times ۱۱ \times ۱۳ \times ۱۷ \times ۱۹ \times ۲۳ \times ۲۹$.

۲۲.۱ ثابت کنید که اگر $a^۳|b^۲$، آنگاه $a|b$. آیا $a^۲|b^۳$ مستلزم $a|b$؟

حل. به‌ازای هر عدد اول p فرض کنیم p^m و p^n بزرگترین توانهای p باشند که به‌ترتیب a و b را می‌شمارند. در این‌صورت $a^۳|b^۲$ ایجاب می‌کند که $۳m \leq ۲n$، و لذا $m \leq n$. در نتیجه $a|b$. اگر $a^۲|b^۳$، لازم نیست که $a|b$، مثلاً $a = ۸$ و $b = ۴$.

۲۳.۱ اگر $(a, b) = ۱۰$، کلیهٔ مقادیر ممکن برای $(a^۳, b^۴)$ را به‌دست آورید.

حل. بنابر (ii.۷.۱) می‌نویسیم $a = ۱۰A$ و $b = ۱۰B$ که در آن $(A, B) = ۱$. لذا $a^۳ = ۱۰۰۰A^۳$، $b^۴ = ۱۰۰۰۰B^۴$، و $(a^۳, b^۴) = ۱۰۰۰(A^۳, ۱۰B^۴)$. اعداد $A^۳$ و $B^۴$ نسبت به هم اول‌اند، زیرا اگر p عدد اولی باشد که $p|A^۳$ و $p|B^۴$، آنگاه $p|A$ و $p|B$ که با $(A, B) = ۱$ تناقض دارد. لذا هر مقسوم‌علیه مشترک $A^۳$ و $۱۰B^۴$ باید ۱۰ را بشمارد. روشن است که $۱۰B^۴$ و $A^۳$) یکی از اعداد ۱، ۲، ۵، یا ۱۰ است. لذا مقادیر ممکن برای $(a^۳, b^۴)$ عبارت‌اند از ۱۰۰۰، ۲۰۰۰، ۵۰۰۰، و ۱۰۰۰۰.

۲۴.۱ ثابت کنید که به‌ازای هر $n \geq ۱$، $(a^n, b^n) = (a, b)^n$. به‌ویژه، اگر $(a, b) = ۱$، آنگاه $(a^n, b^n) = ۱$.

حل. فرض کنید $a = \prod p_i^{a_i}$ و $b = \prod p_i^{b_i}$. بنابر (۱۷.۱)، $(a, b) = \prod p_i^{m_i}$، که در آن $m_i = \min(a_i, b_i)$؛ به طریق مشابه، $(a^n, b^n) = \prod p_i^{k_i}$، که $k_i = \min(na_i, nb_i)$. چون $k_i = n \times \min(a_i, b_i) = nm_i$، از اینجا نتیجه می‌شود که $(a^n, b^n) = \prod p_i^{nm_i} = (a, b)^n$.

۲۵.۱ اگر $a^n|b^n$، آیا $a|b$؟ (راهنمایی: از مسأله قبل استفاده کنید.)

حل. بله، زیرا $a^n|b^n$ ایجاب می‌کند که $(a^n, b^n) = a^n$. چون بنابر مسأله قبل، $(a^n, b^n) = (a, b)^n$، لذا $(a, b) = a$، یعنی $a|b$. (با نوشتن $a = \prod p_i^{a_i}$ و $b = \prod p_i^{b_i}$ نیز

می‌توان مسأله را ثابت کرد، با این توجه که $a^n|b^n$ ایجاب می‌کند $na_i \le nb_i$، یعنی، به‌ازای هر i، $a_i \le b_i$، لذا $a|b$.)

◁ **۲۶.۱** گیریم $n > 0$، و فرض می‌کنیم n دارای r مقسوم‌علیه اول متمایز است. ثابت کنید 2^r جفت مرتب (x, y) از اعداد صحیح مثبت متباین وجود دارند که $xy = n$.

حل. کافی است تعداد انتخابهای x را محاسبه کنیم، زیرا وقتی x انتخاب شد، y معین می‌شود. x را با تجزیهٔ آن به عوامل اول به‌دست می‌آوریم. r عدد اولی را که n را می‌شمارد یکی‌یکی بررسی می‌کنیم. برای یک چنین عدد اول p، نمی‌توانیم $p|x$ و نیز $p|y$ را داشته باشیم، لذا یا x شامل بزرگترین توان p است که n را می‌شمارد، یا ابداً هیچ عامل p ندارد. در نتیجه برای هر عدد اول دو انتخاب و در مجموع 2^r انتخاب وجود دارد. (یا با عبارتی هم‌ارز، می‌توانستیم بگوییم که x توسط مجموعهٔ عوامل اولش مشخص می‌شود. اما هر مجموعهٔ r عنصری دارای 2^r زیرمجموعه است.)

۲۷.۱ تمام اعداد اول p را به‌دست آورید که $17p + 1$ مربع باشد.

حل. فرض کنیم $17p + 1 = x^2$. از آنجا که ۱۷ و p اول هستند و $17p = x^2 - 1 = (x - 1)(x + 1)$، باید داشته باشیم $x - 1 = 17$، که به ما می‌دهد $p = x + 1 = 19$. ($x + 1 = 17$ قبول نیست زیرا ۱۵ اول نیست.)

۲۸.۱ اگر $n > 1$، نشان دهید که اعداد $n! + 2$، $n! + 3$، ...، $n! + n$ همگی مرکب هستند. (این نشان می‌دهد که دنباله‌های طولانی دلخواه از اعداد مرکب وجود دارند.)

حل. اگر $2 \le i \le n$، آنگاه $i|n!$، و لذا $i|n! + i$. چون $i < n! + i$، پس $n! + i$ مرکب است.

۲۹.۱ اگر p و $p + 2$ هر دو اول باشند و $p > 3$، نشان دهید $2p + 2$ بر ۱۲ بخشپذیر است.

حل. چون $2p + 2 = 2(p + 1)$، کافی است ثابت کنیم که $6|p + 1$. چون p فرد است، $p + 1$ زوج و لذا بر ۲ بخشپذیر است. همچنین، p به‌صورت $3k + 1$ یا $3k + 2$ است؛ اما اگر $p = 3k + 1$، آنگاه $p + 2 = 3(k + 1)$ بر ۳ بخشپذیر است و لذا اول نیست. در نتیجه $p = 3k + 2$ و لذا $3|p + 1$. چون ۲ و ۳ عدد $p + 1$ را می‌شمارند و $(2, 3) = 1$، در نتیجه $6|p + 1$.

۳۰.۱ ثابت کنید که هر عدد به‌صورت $4k + 3$ دارای عامل اولی به همین صورت است.

حل. (بنابرالگوریتم تقسیم) هر عدد صحیح را می‌توان به یکی از ۴ صورت $4k$، $4k + 1$، $4k + 2$، یا $4k + 3$ نوشت، و لذا هر عدد اول غیر از ۲ به‌صورت $4k + 1$ یا $4k + 3$ است. فرض می‌کنیم

$N = q_1 q_2 \dots q_r$، که در آن q_iها اعداد اول فرد (نه لزوماً متمایز) هستند. حاصلضرب دو عدد به‌صورت $4k+1$ نیز به همان صورت است، زیرا $(4m+1)(4n+1) = 4(mn+m+n)+1$. لذا، اگر تمام q_iها به‌صورت $4k+1$ باشند حاصلضربشان نیز به همان صورت خواهد بود، که با این فرض که N به‌صورت $4k+3$ است تناقض دارد.

◁ **۳۱.۱** ثابت کنید بی‌نهایت عدد اول به‌صورت $4k+3$ وجود دارد. (راهنمایی: عدد $N = 4p_1 p_2 \dots p_n - 1$ را که در آن p_1، p_2، ...، p_n اعداد اولی به‌صورت $4k+3$ هستند در نظر می‌گیریم و تمرین قبل را به‌کار می‌بریم.)

حل. توجه کنید که هر عدد اول فرد به‌صورت $4k+1$ یا $4k+3$ است. عدد N را همان‌گونه که در راهنمایی گفته شد تعریف می‌کنیم. بنابر تمرین قبل، N عامل اولی مانند q به‌صورت $4k+3$ دارد. عدد اول q یکی از p_iها نیست، زیرا در غیر این‌صورت، چون $q|N$ و $q|4p_1 \dots p_n$، خواهیم داشت $q|1$، که یک تناقض است. بنابراین نشان داده‌ایم که به‌ازای هر مجموعهٔ متناهی از اعداد اول به‌صورت $4k+3$، همواره می‌توان عدد اول متفاوتی از این نوع به‌دست آورد. از این‌رو، بی‌نهایت عدد اول از نوع $4k+3$ وجود دارد.

توضیح. با استدلال مشابه می‌توان نشان داد که بی‌نهایت عدد اول به‌صورت $3k+2$ وجود دارد، ولی این استدلال را برای اینکه نشان دهیم بی‌نهایت عدد اول به‌صورتهای $3k+1$ یا $4k+1$ وجود دارد نمی‌توانیم به‌کار بریم. این دو مورد در فصل ۵ بررسی می‌شوند.

۳۲.۱ فرض می‌کنیم $n = \prod p_i^{n_i}$ تجزیهٔ n به اعداد اول باشد. ثابت کنید که n یک مربع کامل است اگر و تنها اگر هر n_i زوج باشد.

حل. اگر هر n_i زوج باشد، مثلاً $n_i = 2c_i$، آنگاه $n = (\prod p_i^{c_i})^2$. حال، فرض می‌کنیم n مربع باشد، مثلاً $n = m^2$. اگر $m = \prod p_i^{m_i}$، آنگاه به‌ازای هر i، $n_i = 2m_i$.

۳۳.۱ اگر $(a,b) = 1$ و ab برابر عددی به توان k باشد، ثابت کنید هر کدام از a و b نیز عددی به‌توان k است.

حل. فرض کنیم $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ و $b = q_1^{b_1} \dots q_s^{b_s}$ تجزیه‌های a و b به اعداد اول باشند؛ چون $(a,b) = 1$، هیچ p_i برابر q_j نیست. اگر $ab = n^k$، روشن است که مقسوم‌علیه‌های اول n همان p_iها و q_jها هستند. می‌نویسیم $n = p_1^{c_1} \dots p_r^{c_r} \cdot q_1^{d_1} \dots q_s^{d_s}$؛ در این‌صورت

$ab = n^k$ ایجاب می‌کند که به‌ازای هر i، $a_i = kc_i$ و $b_i = kd_i$. لذا $a = (p_1^{c_1} \dots p_r^{c_r})^k$ و $b = (q_1^{d_1} \dots q_s^{d_s})^k$.

۳۴.۱ (الف) فرض کنیم a، b، و c اعداد صحیح مثبت باشند. اگر ab، ac، و bc مکعب کامل باشند، ثابت کنید a، b، و c نیز مکعب کامل‌اند.

(ب) اگر به‌جای «توان کامل»، «توان kام کامل» را بگذاریم چه اتفاقی می‌افتد؟

حل. (الف) از قضیهٔ تجزیهٔ یکتا استفاده می‌کنیم. به‌ازای هر عدد اول p، فرض کنیم p^{a_p} بزرگترین توانی از p باشد که a را می‌شمارد، و b_p و c_p را نیز همین گونه تعریف می‌کنیم. در این‌صورت، $a_p + b_p$، $a_p + c_p$، و $b_p + c_p$ بر ۳ بخشپذیرند. بنابراین، $3|a_p - c_p$؛ و چون $3|a_p + c_p$، پس $3|2a_p$ و لذا $3|a_p$. بنابراین a یک مکعب کامل است، و به قرینه، a و b نیز مکعب کامل هستند.

(ب) اگر «به جای توان سه»، «توان k» گذاشته شود، استدلال (الف) در حالت k فرد کارساز است. اما برای k زوج، استدلال فرو می‌ریزد، زیرا از $k|2a_p$ نمی‌توان نتیجه گرفت که $k|a_p$. در واقع، در حالت k زوج نتیجهٔ نادرست است. مثلاً فرض کنیم $k = 2m$ و $a = b = c = 2^m$.

۳۵.۱ فرض کنیم k و d اعداد صحیح مثبت باشند. با استفاده از قضیهٔ تجزیهٔ یکتا نشان دهید که اگر $\sqrt[k]{d}$ عددی گویا باشد، آنگاه به‌ازای عدد مثبتی مانند b داریم $d = b^k$. به‌ویژه، اگر d عدد مثبتی باشد که مربع کامل نیست، آنگاه $\sqrt{d}$ عددی است گنگ.

حل. فرض کنیم $\sqrt[k]{d} = r/s$، که در آن r و s مثبت هستند، داریم $ds^k = r^k$. به‌ازای هر عدد اول p، فرض کنیم p^{d_p} بزرگترین توان p باشد که d را می‌شمارد. s_p و r_p را به همین‌نحو تعریف می‌کنیم. با پیدا کردن توانهای متناظر p در معادلهٔ $ds^k = r^k$، داریم $d_p + ks_p = kr_p$. در نتیجه، به‌ازای هر p، $k|d_p$، و لذا d یک توان kام کامل است.

معادلهٔ $ax + by = c$

۳۶.۱ (الف) تمام جوابهای صحیح $15x + 7y = 210$ را به‌دست آورید. (ب) تعداد جوابهای مثبت را معین کنید.

حل. (الف) با تجسس، $x = 0$، $y = 30$ یک جواب است. چون ۱۵ و ۷ نسبت به هم اول‌اند، بنابر (۲۴.۱) تمام جوابها با $x = 7t$، $y = 30 - 15t$ ارائه می‌شوند، که در آن t روی تمام اعداد صحیح تغییر می‌کند.

(ب) چون $x > 0$، داریم $t \geq 1$، و چون $y > 0$، $t < 0$. لذا $t = 1$، و تنها یک جواب مثبت وجود دارد.

۳۷.۱ جوابهای معادلهٔ $91x + 221y = 1053$ را به‌دست آورید. آیا معادله جواب مثبت دارد؟

حل. چون هر ضریب به ۱۳ قابل قسمت است، معادلهٔ هم‌ارز $7x + 17y = 81$ است. با تجسس، $x = 14$، $y = -1$ یک جواب است. بنابراین جواب کلی عبارت است از $x = 14 + 17t$، $y = -1 - 7t$. برای آنکه y مثبت باشد، باید t منفی باشد، در این‌صورت x منفی می‌شود. لذا جواب مثبت وجود ندارد.

۳۸.۱ تمام جوابهای صحیح مثبت $11x + 7y = 200$ را به‌دست آورید.

حل. چون $(11, 7) = 1$، پس (۲۴.۱) وجود جواب را تضمین می‌کند. ملاحظه می‌کنید که $11 \times 2 - 7 \times 3 = 1$، لذا $11(2 \times 200) - 7(3 \times 200) = 200$. از این‌رو، $x = 400$، $y = -600$ یک جواب $11x + 7y = 200$ است، و لذا بنابر (۲۴.۱) تمام جوابها به‌صورت $x = 400 + 7t$، $y = -600 - 11t$ هستند. با فرض $x > 0$ و $y > 0$ داریم $-400/7 < t < -600/11$، و بنابراین، جوابهای مثبت به‌ازای $t = -55, -56, -57$ حاصل می‌شود. لذا تنها جوابهای مثبت عبارت‌اند از $x = 15$، $y = 5$؛ $x = 8$، $y = 16$؛ و $x = 1$، $y = 27$. (ملاحظه می‌کنید که برای مقادیر نزولی t، مقادیر x به مقدار ۷، که ضریب t در $x = 400 + 7t$ است، کم می‌شوند و مقادیر y به مقدار ۱۱، که ضریب t با علامت منفی در $y = -600 - 11t$ است اضافه می‌شوند.)

۳۹.۱ آیا بی‌نهایت جواب صحیح مثبت برای $10x - 7y = -17$ وجود دارد؟ توضیح دهید.

حل. بله، با تجسس می‌بینیم که $x = -1$، $y = 1$ یک جواب این معادله است. لذا تمام جوابها به‌صورت $x = -1 - 7t$، $y = 1 - 10t$، هستند. اگر $t < -1/7$ آنگاه $x > 0$، و اگر $t < 1/10$، آنگاه $y > 0$، و لذا به‌ازای هر عدد صحیح t که $t \leq -1$ یک جواب مثبت حاصل می‌شود.

۴۰.۱ کوچکترین عدد صحیح مثبت b را بیابید به‌طوری که $1111x + 704y = 15000 + b$ دارای جواب باشد.

حل. چون $(1111, 704) = 11$، از (۲۴.۱) نتیجه می‌شود که معادله جواب دارد اگر و تنها اگر $11 \mid 15000 + b$. لذا کوچکترین مقدار مثبت b عبارت است از ۴.

۴۱.۱ کوچکترین مقدار n را بیابید به‌طوری که $10x + 11y = n$ دقیقاً دارای ۹ جواب در اعداد صحیح نامنفی باشد.

حل. n هر چه باشد $x = -n$، $y = n$ یک جواب است، لذا جواب عمومی عبارت است از $x = -n + 11t$، $y = n - 10t$. با فرض $x \geq 0$ و $y \geq 0$ داریم $n/11 \leq t \leq n/10$. بازهٔ $[n/11, n/10]$ دارای طول $n/110$ است. لذا، اگر $n = 880$، آنگاه مقادیر مجاز t از ۸۰ تا ۸۸ خواهند بود، که ۹ مقدار برای t به‌دست می‌دهند، و چون هر دو سرِ بازه هم جزء جوابها بوده‌اند، هیچ مقدار کوچکتری برای n مناسب نیست.

۴۲.۱ به قضیهٔ ۲۵.۱ برمی‌گردیم. اگر $(a, b) = 1$ و $c \leq ab$، آیا نتیجه می‌شود که $ax + by = c$ هیچ جواب مثبت ندارد؟

حل. نه. مثلاً $8x + 9y = 43$ را در نظر بگیرید که دارای جواب مثبت $x = 2$، $y = 3$ است.

۴۳.۱ جوابهای صحیح مثبت دستگاه معادلات زیر را به‌دست آورید. $2x + 3y + 5z = 201$، $3x + 5y + 7z = 315$.

حل. یکی از متغیرها، مثلاً x، را حذف می‌کنیم؛ داریم $y - z = 27$. جواب عمومی این معادله عبارت است از $y = 27 + t$، $z = t$. با جایگذاری این مقادیر در معادلهٔ اول داریم $x = 60 - 4t$، برای به‌دست آوردن یک جواب مثبت، قرار می‌دهیم $x > 0$، $y > 0$، و $z > 0$، که در نتیجه به ما می‌دهد $0 \leq t \leq 14$.

۴۴.۱ همهٔ جوابهای معادلهٔ دیوفانتی $(6x + 15y)(8x + 7y) = 129$ را به‌دست آورید.

حل. قرار می‌دهیم $6x + 15y = a$ و $8x + 7y = b$، پس $ab = 129$؛ در این‌صورت، $39y = 4a - 3b$، و لذا $3 | a$. چون a مضرب ۳ است و $a | 129$ پس $a = \pm 129$ یا $a = \pm 3$. اگر $a = \pm 129$ و $b = \pm 1$، y عدد صحیح نمی‌شود، بنابراین تنها وقتی جواب داریم که $a = \pm 3$ و $b = \pm 43$؛ در نتیجه $x = 8$، $y = -3$ و $x = -8$، $y = 3$.

۴۵.۱ شخصی تعداد ۴۸ سیب و پرتقال را به قیمت ۵۶۸ تومان خریداری کرد. اگر قیمت یک کیلو سیب ۱۰ تومان بیشتر از قیمت یک پرتقال باشد و تعداد سیبها بیشتر از تعداد پرتقالها باشد، تعداد هر کدام را تعیین کنید.

حل. فرض کنیم x تعداد سیبها و y تعداد پرتقالهای خریداری‌شده باشد، و فرض می‌کنیم c قیمت یک پرتقال (به تومان) باشد. داریم $x+y=۴۸$، $x>y$، و $x(c+۱۰)+yc=۵۶۸$ (۱). با قرار دادن $y=۴۸-x$ در (۱) داریم $۱۰۰+۴۸c=۵۶۸$، یعنی، $۵x+۲۴c=۲۸۴$. با تجسس $c=۱$ و $x=۵۲$ یک جواب این معادله به‌دست می‌آید، لذا همهٔ جوابها با $x=۵۲+۲۴t$، $c=۱-۵t$ داده می‌شوند. چون $x<۴۸$، باید داشته باشیم $t<-۴/۲۴$؛ و چون $x+y=۴۸$ پس $x>۲۴$ و لذا $t>-۲۸/۲۴$. اما t عدد صحیح است، بنابراین $t=-۱$ تنها مقدار ممکن است. لذا تنها جواب عبارت است از $x=۲۸$، $y=۲۰$.

۴۶.۱ دهقانی تعداد ۱۲۰ رأس اسب، گاو، و گوسفند را به مبلغ ۴ میلیون تومان خریداری کرد. هر اسب ۵۰۰۰۰ تومان، هر گاو ۳۰۰۰۰ تومان، و هر گوسفند ۱۵۰۰۰ تومان قیمت دارد. اگر این دهقان از هر نوع حیوان حداقل یک رأس خریده باشد و تعداد اسبها بیشتر از تعداد گاوها باشد، کمترین تعداد گوسفندی را که دهقان می‌توانست بخرد چقدر است؟

حل. فرض کنیم x، y، و z به‌ترتیب تعداد اسبها، گاوها، و گوسفندها باشند. در این‌صورت داریم $x+y+z=۱۲۰$ و $۵۰۰۰۰x+۳۰۰۰۰y+۱۵۰۰۰x=۴۰۰۰۰۰۰$، یعنی $۱۰x+۶y+۳z=۸۰۰$. با حذف z داریم $۷x+۳y=۴۴۰$. چون $x=۵۰$، $y=۳۰$ یک جواب است، پس جواب عمومی عبارت است از $x=۵۰+۳t$، $y=۳۰-۷t$. لذا $z=۱۲۰-x-y=۴۰+۴t$. برای برقراری $x>y$، داریم $۵۰+۳t>۳۰-۷t$؛ یعنی $t\geq -۱$. تعداد گوسفندها، یعنی، $۴۰+۴t$ مینیمم خواهد بود هرگاه $t=-۱$؛ در نتیجه کمترین تعداد گوسفندی را که می‌توانسته بخرد ۳۶ است.

۴۷.۱ شخصی تعداد ۶۰ بسته شکلات و آدامس را روی‌هم ۱۹۲۶ تومان خرید. تعداد بسته‌های شکلات بیشتر از تعداد بسته‌های آدامس است. قیمت هر بسته آدامس بیشتر از ۲۰ تومان و قیمت هر بسته شکلات ۱۸ تومان بیشتر از قیمت هر بسته آدامس است. تعداد بسته‌های شکلات و تعداد بسته‌های آدامس و قیمت هر بسته شکلات را تعیین کنید.

حل. فرض کنیم x تعداد بسته‌های شکلات، y تعداد بسته‌های آدامس، و c قیمت هر بسته آدامس (به تومان) باشد. در این‌صورت، $x+y=۶۰$ و $(c+۱۸)x+cy=۱۹۲۶$، یعنی، $۱۸x+۶۰c=۱۹۲۶$. لذا $۳x+۱۰c=۳۲۱$؛ چون $x=۷$، $c=۳۰$ یک جواب این معادله است، جواب عمومی آن عبارت است از $x=۷+۱۰c$، $c=۳۰-۳t$. چون $x<y$، داریم $۳۰<x\leq ۶۰$ و لذا $۵٫۲\leq t<۲٫۳$. بنابراین، t برابر ۳، ۴، یا ۵ است، و چون $c>۲۰$،

تنها مقدار ممکن $t = ۳$. در نتیجه تعداد ۳۷ بسته شکلات، و ۲۳ بسته آدامس خریداری شده است، و قیمت هر بسته شکلات ۳۹ تومان است.

۴۸.۱ («مسألهٔ صد مرغ و خروس و جوجه»؛ از چانگ چین چیئن[1]، قرن پنجم.) یک خروس پنج چیئن ارزش دارد، یک مرغ سه چیئن، و سه جوجه یک چیئن[2]. با ۱۰۰ چیئن تعداد ۱۰۰ عدد از آنها را می‌خریم. تعداد هر کدام را به تفکیک تعیین کنید.

حل. فرض کنیم x تعداد خروسها باشد، y تعداد مرغها، و z تعداد جوجه‌ها. در این‌صورت، $x + y + z = ۱۰۰$ و $۱۵x + ۹y + z = ۳۰۰$. با حذف z داریم $۷x + ۹y = ۱۰۰$. با تجسس $x = ۰$، $y = ۲۵$ جوابی از این معادله است. لذا جواب عمومی معادله به‌صورت $x = ۴t$، $y = ۲۵ - ۷t$ است، و لذا $z = ۷۵ + ۳t$. همهٔ اینها باید نامنفی باشند، بنابراین مقادیر ممکن t عبارت‌اند از ۰، ۱، ۲، یا ۳.

۴۹.۱ یک تخم‌مرغ‌پز زمان‌سنج‌داری یک تخم‌مرغ را دقیقاً در ۵ دقیقه آب‌پز می‌کند، و تخم‌مرغ‌پز زمان‌سنج‌دار دیگر آن را دقیقاً در ۱۱ دقیقه آب‌پز می‌کند. چگونه می‌توانیم تخم‌مرغی را دقیقاً در ۳ دقیقه آب‌پز کنیم؟

حل. ملاحظه می‌کنید که $۳ = ۲ \times ۱۱ - ۵ \times ۵$. همزمان هر دو تخم‌مرغ‌پز را به‌کار می‌اندازیم، هر وقت که یکی از آنها متوقف شد، دوباره آن را به‌کار می‌اندازیم. وقتی تخم‌مرغ‌پز ۱۱ـدقیقه‌یی در دور دوم متوقف شد، تخم‌مرغ را سر بار می‌گذاریم، و وقتی دور پنجم تخم‌مرغ‌پز ۵ـدقیقه‌یی پایان پذیرفت، تخم‌مرغ را از سر بار برمی‌داریم. (با همین روش می‌توانیم هر تعداد صحیح دقیقه را با استفاده از یک زمان‌سنج a ـدقیقه‌یی و یک زمان‌سنج bـدقیقه‌یی اندازه بگیریم، به شرط آنکه a و b نسبت به هم اول باشند.)

۵۰.۱ فرض کنیم d و e اعداد صحیح مثبت باشند. نشان دهید که دو تصاعد عددی $a, a + d, a + ۲d, \ldots$، و $b, b + e, b + ۲e, \ldots$ یک عدد مشترک دارند اگر و تنها اگر $(d, e) | b - a$.

حل. این دو تصاعد دارای یک عنصر مشترک هستند اگر و تنها اگر اعداد مثبت r و s وجود داشته باشند به‌طوری که $a + rd = b + se$، یعنی، $rd - se = b - a$. و این امر مطمئناً اتفاق نمی‌افتد مگر آنکه $(d, e) | b - a$.

1. Chang Ch'in Chien 2. Ch'ien

اگر $(d,e)|b-a$، آنگاه بنابر (۲۴.۱)، معادلهٔ $dx-ey=b-a$ جواب دارد. فرمول معمولی جوابها نشان می‌دهد که به‌ازای xهای به‌قدر کافی بزرگ جوابهایی وجود دارند؛ اما اگر $x>(b-a)/d$، آنگاه y باید مثبت باشد. (از این‌رو، همچنین نشان داده‌ایم که اگر دو تصاعد حسابی یک عدد مشترک داشته باشند، بی‌نهایت عدد مشترک خواهند داشت.)

مسأله‌های گوناگون

۵۱.۱ اگر $n\geq ۲$، نشان دهید که آخرین رقمِ غیرِ صفرِ $n!$ همواره زوج است.

حل. از (۲۱.۱) پیداست که اگر ۲^a و ۵^b بزرگترین توانهای ۲ و ۵ باشند که $n!$ را بشمارند، آنگاه $a>b$. زیرا به‌ازای هر عدد طبیعی k و $[n/۲]<[n/۵]$ داریم $[n/۵^k]\leq n/۲^k]$. لذا می‌توانیم بنویسیم $n!=۲^a۵^bm$، که $(m,۱۰)=۱$. بنابراین بزرگترین توان ۱۰ که $n!$ را می‌شمارد برابر است با ۱۰^b، و چون $n!/۱۰^b=۲^{a-b}\cdot m$، پس حکم ثابت شده است.

۵۲.۱ بزرگترین توان ۱۵ را به‌دست آورید که $۶۰!$ را بشمارد.

حل. با استفاده از (۲۱.۱) برای تجزیهٔ ۱۵ به عوامل اول ۳ و ۵، روشن است که برای ۵ توان ماکسیممی کوچکتر از توان ماکسیمم ۳ به‌دست می‌آوریم، در واقع بزرگترین توان ۵ که $۶۰!$ را می‌شمارد برابر است با $[۶۰/۲۵]+[۶۰/۵]=۱۲+۲=۱۴$. در نتیجه $۱۵^{۱۴}$ بزرگترین توان ۱۵ است که $۶۰!$ را می‌شمارد.

۵۳.۱ $۱۶۹!$ به چند صفر ختم می‌شود؟

حل. این مسأله هم‌ارز یافتن بزرگترین توان ۱۰ است که $۱۶۹!$ را می‌شمارد. همانند مسألهٔ ۱۵.۱، کافی است (۲۱.۱) را برای عدد اول ۵ به‌کار بریم، داریم

$$[۱۶۹/۵]+[۱۶۹/۵^۲]+[۱۶۹/۵^۳]=۳۳+۶+۱=۴۰$$

لذا $۱۶۹!$ به ۴۰ صفر ختم می‌شود.

۵۴.۱ $۵۰۰!/۲۰۰!$ به چند صفر ختم شود؟

حل. بزرگترین توان ۱۰ که $۵۰۰!$ را می‌شمارد برابر است با

$$[۵۰۰/۵]+[۵۰۰/۲۵]+[۵۰۰/۱۲۵]=۱۲۴$$

(مسألهٔ ۵۱.۱ را ببینید)؛ همچنین بزرگترین توان ۱۰ که $۲۰۰!$ را می‌شمارد برابر است با

$۴۹ = [۲۰۰/۱۲۵] + [۲۰۰/۲۵] + [۲۰۰/۵]$. بنابراین $۲۰۰!/۵۰۰!$ به $۱۲۴ - ۴۹ = ۷۵$ صفر ختم می‌شود.

۵۵.۱ تمام اعداد صحیح مثبت n را به‌دست آورید که $n!$ دقیقاً به ۴۰ صفر ختم شود.

حل. (مترجم). ابتدا مطلب زیر را اثبات می‌کنیم: اگر p عدد اولی باشد و e بزرگترین توان p باشد که $p^e | n!$ آنگاه $e < n/(p-۱)$، زیرا داریم

$$e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^۲}\right] + \cdots + \left[\frac{n}{p^k}\right] \leq \frac{n}{p} + \frac{n}{p^۲} + \cdots + \frac{n}{p^k} < \sum_{i=۱}^{\infty} \frac{n}{p^i} = \frac{n}{p-۱}.$$

حال، به حل مسأله می‌پردازیم. با توجه به مسألهٔ (۶۶.۱)، $n!$ به ۴۰ صفر ختم می‌شود اگر و تنها اگر بزرگترین توان ۵ که $n!$ را می‌شمارد ۴۰ باشد. پس داریم $۴۰ < n/(۵-۱)$ یا $n > ۱۶۰$ چون ۱۶۰ جواب نیست، اعداد ۱۶۱، ...، ۱۶۴ نیز به‌دلیل آنکه مضرب ۵ نیستند جواب نخواهند بود. در مورد ۱۶۵ داریم

$$\left[\frac{۱۶۵}{۵}\right] + \left[\frac{۱۶۵}{۵^۲}\right] + \left[\frac{۱۶۵}{۵^۳}\right] = ۳۳ + ۶ + ۱ = ۴۰$$

پس مقادیر ممکن برای n عبارت‌اند از ۱۶۵، ۱۶۶، ۱۶۷، ۱۶۸، ۱۶۹.

راه‌حل دیگر مسألهٔ ۱ـ۵۵: عدد صحیح $n!$ دقیقاً به ۴۰ صفر ختم خواهد شد اگر و تنها اگر بزرگترین توان ۵ که $n!$ را عاد می‌کند $۵^{۴۰}$ باشد (مسألهٔ ۵۱.۱ را ببینید). از این‌رو، با کاربرد (۲۱.۱)، nی را لازم داریم که $M_n = ۴۰$، که $M_n = [n/۵] + [n/۲۵] + [n/۱۲۵] + \cdots$، اگر $n = ۱۲۵$، آنگاه $M_n = ۳۱$؛ اگر $n = ۲۰۰$، آنگاه $M_n = ۴۹$. از این‌رو، اگر $M_n = ۴۰$، آنگاه $۱۲۵ < n < ۲۰۰$. می‌نویسیم $n = ۱۲۵ + ۲۵s + ۵u + v$، که s برابر ۰، ۱، یا ۲، $۰ \leq u \leq ۴$، و $۰ \leq v \leq ۴$. در این‌صورت $M_n = ۱ + (۵ + s) + (۲۵ + ۵s + u) = ۳۱ + ۶s + u$؛ لذا $M_n = ۴۰$، اگر و تنها اگر $۶s + u = ۹$. چون $u \leq ۴$، داریم $s = ۱$ و $u = ۳$، و بنابراین

$$n = ۱۶۵ + v, \quad v = ۰, ۱, ۲, ۳, ۴.$$

لذا $n!$ دقیقاً به ۴۰ صفر ختم می‌شود هرگاه n یکی از اعداد ۱۶۵، ۱۶۶، ۱۶۷، ۱۶۸، و ۱۶۹ باشد.

۵۶.۱ آیا nی وجود دارد که $n!$ به ۲۴۷ صفر یا ۲۴۸ صفر ختم شود

حل. مانند مسألهٔ ۵۱.۱، کافی است بزرگترین توان ۵ که $n!$ را می‌شمارد بررسی کنیم، برای $n = ۱۰۰۰$ داریم $[۱۰۰۰/۶۲۵] + [۱۰۰۰/۱۲۵] + [۱۰۰۰/۲۵] + [۱۰۰۰/۵] = ۲۴۹$، اما مجموع نظیر برای $n = ۹۹۹$ عدد ۲۴۶ است. لذا $n!$ نمی‌تواند به ۲۴۷ یا ۲۴۸ صفر ختم شود.

حل. (مترجم). با توجه به مسألهٔ قبل و $p = ۵$، در مورد ۲۴۷ داریم $n/۴ > ۲۴۷$ یا $n > ۹۸۸$. پس ممکن است $n = ۱۰۰۰$ جواب باشد. اما

$$\left[\frac{۱۰۰۰}{۵}\right] + \left[\frac{۱۰۰۰}{۵^۲}\right] + \left[\frac{۱۰۰۰}{۵^۳}\right] + \left[\frac{۱۰۰۰}{۵^۴}\right] = ۲۰۰ + ۴۰ + ۸ + ۱ = ۲۴۹,$$

لذا در این حالت n وجود ندارد. در مورد ۲۴۸ نیز به همین طریق ثابت می‌شود که n وجود ندارد.

◁ **۵۷.۱** فرض کنید که $n!$ دقیقاً به M_n صفر ختم شود. ثابت کنید برای nهای بزرگ مقدار M_n تقریباً $n/۴$ است.

حل. استدلال به‌کاررفته در حل مسألهٔ ۵۱.۱ نشان می‌دهد که M_n با بزرگترین توان ۵ که $n!$ را عاد می‌کند برابر است. بنابر (۲۱.۱)، $M_n = [n/۵] + [n/۲۵] + [n/۱۲۵] + \cdots$؛ در این‌صورت، بیشتر از $\log_۵^n$ جملهٔ غیرصفر در مجموع وجود ندارد. فرض کنیم $s_n = n/۵ + n/۲۵ + n/۱۲۵ + \cdots$. با مقایسهٔ جمله‌به‌جملهٔ دو مجموع می‌بینیم که $۰ < s_n - M_n < \log_۵^n$. از طرفی s_n مجموع جمله‌های یک تصاعد هندسی است، و لذا $s_n = n/۴$. با تقسیم طرفین نامساوی بر n، داریم

$$\frac{۱}{۴} - \frac{۱}{n}\log_۵ n < \frac{۱}{n}M_n < \frac{۱}{۴}.$$

از آنجا که $\log_۵^n$ بسیار کندتر از n زیاد می‌شود، لذا می‌توان با انتخاب n به‌قدر کافی بزرگ، نسبت M_n/n را به‌دلخواه به ۱/۴ نزدیک کرد، و بدین معنی M_n تقریباً برابر $n/۴$ است.

حل. (مترجم). با توجه به مسألهٔ ۵۱.۱ (یا ۵۳.۱)، M_n بزرگترین توان ۵ است که $n!$ را می‌شمارد. یک عدد صحیح t وجود دارد که $۵^t \le n < ۵^{t+۱}$. لذا $M_n = [n/۵] + \cdots + [n/۵^t]$، که $t \le \log_۵^n$. فرض کنیم $s_n = \sum_{k=۱}^{\infty}(n/۵^k)$، داریم

$$۰ < s_n - M_n < \left(\frac{n}{۵} - \left[\frac{n}{۵}\right]\right) + \cdots + \left(\frac{n}{۵^t} - \left[\frac{n}{۵^t}\right]\right) + \frac{n}{۵^{t+۱}} + \cdots < \log_۵^n + \frac{۵}{۴}.$$

خلاصه: $0 < s_n - M_n < 5/4 + \log_5^n$ (۱)، از طرفی $s_n = n/4$. لذا با توجه به (۱) داریم

$$\frac{1}{4} - \frac{1}{n}\left(\frac{5}{4} + \log_5^n\right) < \frac{M_n}{n} < \frac{1}{4}.$$

چون $\lim(\log_5^n/n) = 0$، پس M_n/n به‌دلخواه به $1/4$ نزدیک می‌شود هرگاه n به‌قدر کافی بزرگ اختیار شود، و بدین معنی، M_n تقریباً برابر $n/4$ است.

◁ **۵۸.۱** (الف) به‌ازای هر دو عدد حقیقی x و y نشان دهید که $[x] + [y] \leq [x + y]$.

(ب) با استفاده از (الف) و (۲۱.۱) نشان دهید که $n!$ حاصلضرب n عدد صحیح مثبت متوالی را می‌شمارد. (راهنمایی: فرض کنید اعداد صحیح $m+1$، $m+2$، ... $m+n$، باشند از (الف) با $x = m/p^k$ و $y = n/p^k$ استفاده کنید.)

برهان. (الف) فرض می‌کنیم $x = a + s$ و $y = b + t$ که a و b اعداد صحیح هستند و $0 \leq s$ و $t < 1$. پس $[x] + [y] = a + b$. چون $x + y = a + b + s + t$، داریم $[x + y] \geq a + b$ و قضیه اثبات شده است.

(ب) حاصلضرب n عدد متوالی که با $(m+1)$ شروع شوند درست برابر است با $(m+n)!/m!$، یعنی $(m+1)\cdots(m+n) = (m+n)!/m!$. به‌ازای هر عدد اول p، فرض کنیم p^d بزرگترین توان p باشد که $n!$ را می‌شمارد و p^e بزرگترین توان p باشد که $(m+n)!/m!$ را می‌شمارد. برای اثبات (ب) کافی است ثابت کنیم که $d \leq e$. بنابراین (۲۱.۱) داریم

$$d = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots$$

$$e = \left(\left[\frac{m+n}{p}\right] + \left[\frac{m+n}{p^2}\right] + \cdots\right) - \left(\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots\right)$$

اگر در قسمت (الف) قرار دهیم $x = m/p^k$ و $y = n/p^k$، آنگاه به‌ازای هر k داریم $[n/p^k] \leq [(m+n)/p^k] - [m/p^k]$، و لذا $d \leq e$.

توضیح. با استفاده از ویژگیهای ضرایب دوجمله‌یی می‌توان برهان ساده‌یی برای (ب) ارائه داد. می‌دانیم $\binom{m+n}{n} = (m+n)!/m!n!$ عدد صحیح است، لذا $n!|(m+n)!/m!$. اما روشی که در حل (ب) به‌کار رفته کارسازتر است. چبیشف[1] با استفاده از روشی مشابه، در ۱۸۵۲، اولین تخمین مناسب برای تعداد اعداد اول کوچکتر از یک عدد مفروض x را به‌دست آورد.

1. Chebyshev

۵۹.۱ فرض کنید a، r، و s اعداد صحیحی باشند که s مثبت است. اگر $a < x < a + ۱$ ثابت کنید $[(x + r)/s] = [(a + r)/s]$.

حل. فرض کنیم $a + r = qs + t$، که $۰ \le t \le s - ۱$. در این‌صورت $qs+t < x+r < qs+t+۱$ لذا $q \le q+t/s < (x+r)/s < q+(t+۱)/s \le q+۱$. بنابراین $[(x + r)/s] = q = [(a + r)/s]$.

◁ **۶۰.۱** بین ۵۰۰ و ۲۰۰۰ دقیقاً چند عدد صحیح بر ۳ و ۷ بخشپذیرند و چند عدد بر ۳ یا ۷؟

حل. تعداد اعداد صحیح نابیشتر از ۵۰۰ که بر ۲۱ بخشپذیرند برابراست با $۲۳ = [۵۰۰/۲۱]$؛ همچنین، تعداد $۹۵ = [۲۰۰۰/۲۱]$ عدد صحیح که از ۲۰۰۰ نابیشترند وجود دارند که مضرب ۲۱ هستند. (توجه کنید که ۲۰۰۰ یکی از آنها نیست.) لذا دقیقاً تعداد $۷۲ = ۲۳ - ۹۵$ عدد صحیح وجود دارند که بین ۵۰۰ و ۲۰۰۰ قرار دارند و بر ۳ و ۷ (هر دو) بخشپذیرند.

حال، فرض کنیم N تعداد اعداد صحیحی باشند که دقیقاً بین ۵۰۰ و ۲۰۰۰ قرار دارند و بر ۳ یا ۷ (یا هر دو) بخشپذیرند. اگر M_k معرف تعداد اعداد صحیح مثبت نابیشتر از k باشد که بر ۳ یا ۷ بخشپذیرند، آنگاه $M_k = [k/۳] + [k/۷] - [k/۲۱]$. (دلیل کم کردن آخرین جمله آن است که مضربهای ۲۱ دو بار حساب شده‌اند، یکی به‌عنوان مضرب ۳ و بار دیگر به‌عنوان مضرب ۷.) لذا $N = M_{۱۹۹۹} - M_{۵۰۰} = ۸۵۶ - ۲۱۴ = ۶۴۲$.

۶۱.۱ تعداد اعداد صحیح بین ۵۰۰ و ۲۰۰۰ را تعیین کنید که بر ۳ یا ۷ قابل قسمت نباشند. (تمرین قبل را ملاحظه کنید.)

حل. بین ۵۰۰ و ۲۰۰۰ تعداد ۱۴۹۹ عدد صحیح وجود دارد. بنابر مسألهٔ قبل، ۶۴۲ تای آنها بر ۳ یا ۷ (یا هر دو) بخشپذیرند. لذا فاصلهٔ مفروض شامل $۸۵۷ = ۶۴۲ - ۱۴۹۹$ عدد صحیح است که نه بر ۳ بخشپذیرند و نه بر ۷.

۶۲.۱ رد یا اثبات کنید. هیچ عدد صحیح مربعی به‌صورت $۳k + ۲$ نیست.

حل. درست است. بنابر الگوریتم تقسیم، هر عدد صحیح n را می‌توان به‌صورت $۳k$، $۳k + ۱$، یا $۳k + ۲$ نوشت. اگر $n = ۳k$، آنگاه $n^۲$ نیز به همین صورت است. اگر $n = ۳k + ۱$، آنگاه $n^۲ = ۳K + ۱$، که $K = ۳k^۲ + ۲k$. اگر $n = ۳k + ۲$، آنگاه $n^۲ = ۳K + ۱$، که $K = ۳k^۲ + ۴k + ۱$.

۶۳.۱ فرض کنید N عدد صحیحی باشد که بسط دهدهی آن متشکل از 3^n رقم یکسان است. به استقرا نشان دهید که $3^n|N$.

حل. قضیه به‌ازای $n = 0$ برقرار است. اگر به‌ازای $n = k$ برقرار باشد، نشان می‌دهیم که برای $k + 1$ نیز برقرار است. کافی است حالتی را در نظر بگیریم که تمام ارقام ۱ باشند بنابراین فرض می‌کنیم که بسط دهدهی n متشکل از 3^{k+1} رقم ۱ باشد. در این‌صورت $N = Ma$، که در آن M دارای 3^k رقم ۱ است و $a = 1 + 10^{34} + 10^{2\times 3^k}$. بنابر فرض استقرا $3^k|M$ و روشن است که $3|a$، لذا $3^{k+1}|N$.

۶۴.۱ در چه صورتی حاصلضرب ۴ عدد صحیح متوالی یک مربع است؟ (راهنمایی: ملاحظه کنید که $(x(x+1)(x+2)(x+3) + 1 = (x(x+3) + 1)^2$.)

حل. اتحاد ارائه‌شده در راهنمایی، که با محاسبهٔ مستقیم به‌سادگی برقراری آن ثابت می‌شود، مسأله را خیلی آسان می‌سازد. زیرا اگر P حاصلضرب چهار عدد صحیح متوالی باشد، آنگاه $P + 1$ مربع است، لذا P نمی‌تواند یک مربع باشد مگر آنکه $P = 0$.

توضیح. این مسأله که آیا حاصلضرب ۲ یا چند عدد صحیح متوالی می‌تواند یک مربع، یا به‌طور کلی‌تر، یک توان کامل باشد، داستانی طولانی دارد. پاول اِردوش[1] در ۱۹۳۹ ثابت کرده است که نمی‌تواند مربع باشد. در ۱۹۷۵، اِردوش و سلفریج[2] ثابت کردند که به‌ازای هر $m \geq 2$ نمی‌تواند توانی از m باشد. (برای یک برهان، کتاب مسائل کلاسیک در نظریهٔ اعداد نوشتهٔ نارکیدویچ[3] را ببینید.)

۶۵.۱ ثابت کنید هر عدد صحیح به‌صورت $8^n + 1$ عددی است مرکب. (راهنمایی: اگر k فرد باشد. آنگاه $(x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots - x + 1)$.)

حل. با استفاده از فرمول بالا داریم $(8^n+1) = (2^n+1)|((2^n)^3+1)$. چون $2^n+1 \geq 3$، $8^n + 1$ مرکب است.

◁ **۶۶.۱** نشان دهید که $e = \sum_0^\infty 1/n!$ گنگ است. (راهنمایی: فرض کنید $e = p/q$ که p و q اعداد صحیح مثبت‌اند. نشان دهید $q!e$ و $q!\sum_0^q 1/n!$ هر دو عدد صحیح‌اند.)

حل. فرض کنیم $S_q = \sum_0^q 1/n!$ و $R_q = \sum_{q+1}^\infty 1/n!$. داریم $q!e = q!S_q + q!R_q$.

1. Paul Erdös 2. Selfridge 3. *Classical Problems in Number Theory*, by Narkiewicz

آشکار است که $q!S_q$ عدد صحیح است. اگر $q!e$ عدد صحیح باشد، آنگاه $q!R_q$ نیز عدد صحیح می‌شود. نشان می‌دهیم که $q!R_q < ۱$، و لذا $q!R_q$ نمی‌تواند عدد صحیح باشد.

توجه کنید که: $q!R_q = ۱/(q+۱)+۱/(q+۱)(q+۲)+۱/(q+۱)(q+۲)(q+۳)+\cdots$

لذا $۱ = ۱/۲ + ۱/۴ + ۱/۸ + \cdots$، و قضیه نتیجه می‌شود. $q!R_q < ۱/۲$

◁ **۶۷.۱** اگر $n > ۱$، ثابت کنید $۱ + ۱/۲ + ۱/۳ + \cdots + ۱/n$ عدد صحیح نیست.

حل. قرار می‌دهیم $S = ۱ + ۱/۲ + ۱/۳ + \cdots + ۱/n$. فرض کنیم m بزرگترین عدد صحیحی باشد که $۲^m \le n$ و فرض می‌کنیم P حاصلضرب تمام اعداد فردی باشد که از n تجاوز نمی‌کنند. در این‌صورت تمام جمله‌های حاصلضرب $۲^{m-۱}PS$ بجز $۲^{m-۱}P(۱/۲^m)$ عدد صحیح هستند. لذا S نمی‌تواند عدد صحیحی باشد.

تعداد و مجموع مقسوم‌علیه‌ها

۶۸.۱ $\tau(۵۱۱۲)$ و $\sigma(۵۱۱۲)$ را محاسبه کنید.

حل. داریم $۵۱۱۲ = ۲^۳ \times ۳^۲ \times ۷۱$. بنابر قضیهٔ (۲۰.۱)، $\tau(۵۱۱۲) = ۴ \times ۳ \times ۲ = ۲۴$ و $\sigma(۵۱۱۲) = (۱۵/۱) \times (۲۶/۲) \times ۷۲ = ۱۴۰۴۰$.

۶۹.۱ پیدا کنید (الف) $\tau(۵۰۹)$؛ (ب) $\tau(۹!)$؛ (ج) $\tau(۱۱۲۸)$.

حل. بنابر قضیهٔ (۲۰.۱) داریم، (الف) $\tau(۵۰۹) = ۲$ زیرا ۵۰۹ اول است.
(ب) چون $۹! = ۲^۷ \times ۳^۴ \times ۵ \times ۷$ پس $\tau(۹!) = ۸ \times ۵ \times ۲ \times ۲ = ۱۶۰$.
(ج) $\tau(۱۱۲۸) = \tau(۲^۳ \times ۳ \times ۴۷) = ۴ \times ۲ \times ۲ = ۱۶$.

۷۰.۱ مطلوب است محاسبهٔ (الف) $\sigma(۵۰۹)$، (ب) $\sigma(۹!)$؛ (ج) $\sigma(۱۱۲۸)$.

حل. (الف) $\sigma(۵۰۹) = ۵۱۰$، زیرا ۵۰۹ اول است. (ب) بنابر (۲۰.۱)،

$$\sigma(۹!) = \sigma(۲^۷ \times ۳^۴ \times ۵ \times ۷) = \frac{۲۵۵}{۱} \times \frac{۲۴۲}{۲} \times \frac{۲۴}{۴} \times \frac{۴۸}{۶} = ۱۴۸۱۰۴۰$$

(ج) $\sigma(۱۱۲۸) = \sigma(۲^۳ \times ۳ \times ۴۷) = (۱۵/۱)(۸/۲)(۴۸) = ۲۸۸۰$ (چون ۴۷ اول است، روشن است که $\sigma(۴۷) = ۱ + ۴۷ = ۴۸$؛ و نیازی به استفاده از عبارت $(۴۷^۲ - ۱)/۴۶$ نیست.)

۷۱.۱ فرض کنید N حاصلضرب ۷ نخستین عدد اول باشد. $\tau(N)$ و $\sigma(N)$ را محاسبه کنید.

حل. چون N دارای ۷ عامل اول با توان یک است، (۲۰.۱) ایجاب می‌کند که $\tau(N) = ۲^۷ = ۱۲۸$،

$$\sigma(N| = \sigma(۲ \times ۳ \times ۵ \times ۷ \times ۱۱ \times ۱۳ \times ۱۷) = (۳/۱)(۸/۲)(۲۴/۴)(۴۸/۶)$$
$$(۱۲۰/۱۰)(۱۶۸/۱۲)(۲۸۸/۱۶) = ۱۷۴۱۸۲۴$$

۷۲.۱ به‌ازای چه مقادیر صحیح n، $\tau(n)$ فرد است؟

حل. اگر $n = p_۱^{n_۱} \times p_۲^{n_۲} \times \cdots \times p_r^{n_r}$، آنگاه (۲۰.۱) ایجاب می‌کند $\tau(n) = (n_۱ + ۱)(n_۲ + ۱)\ldots(n_r + ۱)$. لذا $\tau(n)$ فرد است اگر و تنها اگر هر عامل $n_i + ۱$ فرد باشد، یعنی، اگر و تنها اگر هر n_i زوج باشد. بنابراین $\tau(n)$ فرد است اگر و تنها اگر n مربع کامل باشد.

برهان دیگر. به‌ازای هر d، $d|n$ اگر و تنها اگر $n/d|n$. اگر $d < \sqrt{n}$ یک مقسوم‌علیه n باشد، با n/d یک جفت تشکیل می‌دهد. اگر n مربع کامل نباشد، تمام مقسوم‌علیه‌های مثبت n عنصرهای یک جفت هستند، لذا $\tau(n)$ زوج است. اگر n یک مربع کامل باشد، آنگاه تمام مقسوم‌علیه‌های n بجز $\sqrt{n}$ عناصر یک جفت هستند، لذا $\tau(n)$ فرد است.

۷۳.۱ به‌ازای چه مقادیر صحیح n، $\sigma(n)$ فرد است؟

حل. از (۲۰.۱) استفاده می‌کنیم. اگر $n = p_۱^{n_۱} p_۲^{n_۲} \ldots p_r^{n_r}$، آنگاه $\sigma(n) = P_۱P_۲ \ldots P_r$، که در آن نوشتن $P_i = ۱ + p_i + \cdots + p_i^{n_i}$ (به‌جای $P_i = (p_i^{n_i+۱} - ۱)/p_i - ۱$) مناسبتر است. اگر $p_i = ۲$، آنگاه P_i فرد است. اگر p_i عدد اول فرد باشد، آنگاه P_i فرد است اگر و تنها اگر P_i دارای تعداد فردی جمله در عبارت فوق باشد. لذا برای آنکه P_i فرد باشد باید n_i زوج باشد. از آنجا که $\sigma(n)$ فرد است اگر و تنها اگر هر P_i فرد باشد، نتیجه می‌شود که باید n حاصلضرب $۲^k (k \geq ۰)$ و یک مربع کامل باشد.

برهان دیگر. ملاحظه می‌کنید که مقسوم‌علیه‌های زوج فرد بودن یا زوج بودن مجموع را تغییر نمی‌دهند، بنابراین فقط مقسوم‌علیه‌های فرد n اهمیت دارند. اگر بنویسیم $n = ۲^k m$، که در آن m فرد است، مقسوم‌علیه‌های فرد n و m یکی می‌شوند. اگر $d < \sqrt{m}$ یک مقسوم‌علیه مثبت (لزوماً فرد) از m باشد، d را با $m/d > \sqrt{m}$ جفت می‌کنیم. مجموع $d + m/d$ زوج است. اگر m مربع کامل نباشد، تمام مقسوم‌علیه‌های مثبت m را به‌حساب آورده‌ایم، و لذا $\sigma(m)$ زوج

است. اگر m مربع کامل باشد، تمام مقسوم‌علیه‌های m بجز $\sqrt{m}$ را حساب کرده‌ایم، و بنابراین $\sigma(m)$ فرد است. لذا $\sigma(n)$ فرد است اگر و تنها اگر به‌صورت $2^k N^2$ باشد.

۷۴.۱ مطلوب تعیین اعداد صحیح مثبتی است که دقیقاً دارای (الف) دو مقسوم‌علیه مثبت؛ (ب) سه مقسوم‌علیه مثبت؛ (ج) چهار مقسوم‌علیه مثبت باشند.

حل. (الف) فرض کنیم $n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$. از (۲۰.۱) آشکار است که $\tau(n) = 2$ اگر و تنها اگر $r = 1$ و $n_1 = 1$، یعنی اگر و تنها اگر n یک عدد اول باشد.

(ب) با استدلال مشابه، اگر $\tau(n) = 3$، آنگاه $(n_1 + 1) \dots (n_r + 1) = 3$، و لذا باید داشته باشیم $r = 1$ و $n_1 = 2$. از این‌رو n باید مربع یک عدد اول باشد.

(ج) سرانجام، $\tau(n) = 4$ ایجاب می‌کند که یا $n_1 + 1 = 4$ و $n_2 + 1 = 1$، یا $n_2 + 1 = n_1 + 1 = 2$. به عبارت دیگر، n باید به‌صورت p^3 یا به‌صورت pq باشد، که در آن p و q اعداد اول متمایزند.

۷۵.۱ فرض کنید $n > 1$، ثابت کنید که حاصلضرب مقسوم‌علیه‌های مثبت n برابر $n^{\tau(n)/2}$ است. (راهنمایی: مقسوم‌علیه مفروض d را با n/d جفت کنید.)

حل. با هر مقسوم‌علیه d از n که $d \neq n/d$، مقسوم‌علیه n/d را مربوط می‌سازیم. حاصلضرب این جفت n است. اگر n مربع کامل نباشد، آنگاه تمام مقسوم‌علیه‌های مثبت n به حساب گرفته می‌شوند، و $\tau(n)/2$ جفت وجود دارد؛ لذا حاصلضرب مقسوم‌علیه‌های مثبت n برابر $n^{\tau(n)/2}$ است. اگر n مربع کامل باشد، مثلاً $n = m^2$، آنگاه $(\tau(n) - 1)/2$ جفت وجود دارد، با عامل m که جفت نمی‌شود. بنابراین حاصلضرب مقسوم‌علیه‌ها مثبت n عبارت است از $n^{(\tau(n)-1)/2} \times n^{1/2} = n^{\tau(n)/2}$.

حل. (مترجم). اگر d_1، d_2، ...، $d_{\tau(n)}$ کلیهٔ مقسوم‌علیه‌های متمایز n باشند، آنگاه n/d_1، ...، $n/d_{\tau(n)}$ نیز تمام مقسوم‌علیه‌های متمایز n هستند. لذا اگر $P(n)$ حاصلضرب مقسوم‌علیه‌های n باشد. داریم $P(n) = d_1 \times \dots \times d_{\tau(n)}$ و $P(n) = n/d_1 \times \dots \times n/d_{\tau(n)}$. لذا $[P(n)]^2 = n^{\tau(n)}$.

۷۶.۱ اثبات یا رد کنید: n اول است اگر و تنها اگر $\sigma(n) = n + 1$.

حل. اگر n اول باشد، مقسوم‌علیه‌های مثبت n فقط ۱ و n هستند، و لذا $\sigma(n) = n + 1$.

برعکس، اگر n اول نباشد، آنگاه دارای یک مقسوم‌علیه واقعی d است. لذا

$$\sigma(n) \geq n + d + ۱ > n + ۱$$

۷۷.۱ اثبات یا رد کنید: به‌ازای $k > ۱$، تعداد نامتناهی عدد صحیح وجود دارند که دقیقاً k مقسوم‌علیه مثبت دارند.

حل. درست است. فرض کنیم $n = p^{k-۱}$، که p یک عدد اول است. لذا بنابر (۲۰.۱)، $\tau(n) = k$.

۷۸.۱ آیا عدد صحیحی مانند k وجود دارد به‌طوری که معادلهٔ $\sigma(n) = k$ برای n بی‌نهایت جواب داشته باشد؟

حل. نه. اگر $n > ۱$، روشن است که $\sigma(n) \geq n + ۱$. لذا اگر $\sigma(n) = k$، باید $n \leq k - ۱$، و بنابراین معادلهٔ $\sigma(n) = k$ حداکثر $k - ۱$ جواب دارد.

۷۹.۱ همهٔ اعداد $n < ۱۰۰$ را بیابید به‌طوری که $\tau(n) = ۱۲$.

حل. اگر $n = p_۱^{n_۱} \dots p_r^{n_r}$، می‌خواهیم $(n_۱ + ۱) \dots (n_r + ۱) = ۱۲$. با تجزیهٔ ۱۲ به‌صورت $۱۲ = ۴ \times ۳$ داریم $n_۱ = ۳$ و $n_۲ = ۲$؛ لذا $n = p_۱^۳ p_۲^۲$. چون $n < ۱۰۰$، پس در این حالت فقط $۷۲ = ۳^۲ \times ۲^۳$ جواب است. اگر $۱۲ = ۲ \times ۲ \times ۳$ را در نظر بگیریم، آنگاه $n_۱ = n_۲ = ۱$ و $n_۳ = ۲$؛ لذا $n = p_۱ p_۲ p_۳^۲$. مقادیر ممکن در این حالت عبارت‌اند از $۶۰ = ۲^۲ \times ۵ \times ۳$، $۸۴ = ۲^۲ \times ۳ \times ۷$، و $۹۰ = ۳^۲ \times ۵ \times ۲$. تجزیهٔ ۱۲ به‌صورت $۱۲ = ۶ \times ۲$ به ما می‌دهد $n = p_۱^۵ p_۲$، و $۹۶ = ۳ \times ۲^۵$ تنها جواب ممکن در این حالت است. سرانجام، $۱ \times ۱۲ = ۱۲$ هیچ مقداری برای n کمتر از ۱۰۰ به‌دست نمی‌دهد. بنابراین اعداد $n < ۱۰۰$ که در $\tau(n) = ۱۲$ صدق می‌کنند عبارت‌اند از ۶۰، ۷۲، ۸۴، ۹۰، و ۹۶.

۸۰.۱ عدد n را بیابید به‌طوری که $\sigma(n) = ۳۶$.

حل. اگر $n = p_۱^{n_۱} \dots p_r^{n_r}$، آنگاه $\sigma(n) = P_۱ \dots P_r$، که در آن $P_i = ۱ + p_i + \dots p_i^{n_i}$ (برهان ۲۰.۱) را ببینید). اگر $\sigma(n) = ۳۶$، باید هر p_i عدد ۳۶ را بشمارد. اگر به مقسوم‌علیه‌های ۳۶ توجه کنیم، آشکار است که ۱، ۲، ۳، و ۳۶ را نمی‌توانیم به‌صورت P_i بیان کنیم، اما $۲ + ۱ = ۳$، $۳ + ۱ = ۴$، $۵ + ۱ = ۶$، $۱۱ + ۱ = ۱۲$، و $۱۷ + ۱ = ۱۸$، و هر یک از اینها تنها

یک نمایش به‌صورت P_i دارد. اکنون تمام راههای ممکن برای بیان ۳۶ به‌صورت حاصلضرب را امتحان می‌کنیم. تنها تجربه‌ای که منجر به جواب می‌شود $۳۶ = ۳ \times ۱۲$ است، که در این حالت $p_۱ = ۲$، $n_۱ = ۱$ و $p_۲ = ۱۱$، $n_۲ = ۱$، لذا $n = ۲ \times ۱۱ = ۲۲$ تنها جواب است.

۸۱.۱ همهٔ مقادیر n را که در تساوی $\sigma(n) = ۷۲$ صدق می‌کنند پیدا کنید.

حل. مانند مسألهٔ قبل استدلال می‌کنیم، مقسوم‌علیه‌هایی از ۷۲ که نمایشی به‌صورت $۱ + p + \cdots + p^k$ ندارند عبارت‌اند از ۱، ۲، ۹، و ۳۶. لذا تجزیه‌هایی از ۷۲ که به جواب منجر می‌شوند عبارت‌اند از ۱۸×۴، ۲۴×۳، ۱۲×۶، و ۷۲×۱، که به‌ترتیب جوابهای $۵۱ = ۱۷ \times ۳$، $۴۶ = ۲۳ \times ۲$، $۵۵ = ۱۱ \times ۵$، و ۷۱ را به‌دست می‌دهند.

۸۲.۱ آیا مقادیری از n وجود دارند که برای آنها $\sigma(n) = ۵۱$؟ توضیح دهید.

حل. نه. اعداد ۱۷ و ۵۱ به‌صورت $۱ + p \cdots + p^k$ نیستند (p اول)، و ۳×۱۷ تنها تجزیهٔ واقعی ۵۱ است. لذا nی وجود ندارد که $\sigma(n) = ۵۱$.

۸۳.۱ همهٔ مقادیر n را بیابید به‌طوری که (الف) $\sigma(n) = ۴۲$؛ (ب) $\sigma(n) = ۹۱$.

حل. (الف) درمیان مقسوم‌علیه‌های ۴۲ اعداد ۳، ۶، ۷، و ۱۴ نمایشی به‌صورت $۱ + p + \cdots + p^k$ دارند، که p عدد اول است (حل مسألهٔ ۸۰.۱ را ملاحظه کنید). لذا تجزیه‌هایی از ۴۲ که به جواب منجر می‌شوند عبارت‌اند از ۱۴×۳، که $n = ۲ \times ۱۳ = ۲۶$، و ۷×۶، که $n = ۵ \times ۲^۲ = ۲۰$ (زیرا $۱ + ۲ + ۲^۲ = ۷$) را به‌دست می‌دهند.

(ب) چون نمی‌توان ۹۱ را به‌صورت $۱ + p + \cdots + p^k$ بیان کرد، باید فقط تجزیهٔ $۱۳ \times ۷ = ۹۱$ را بررسی کرد. داریم $۱ + ۲ + ۲^۲ = ۷$ و $۱ + ۳ + ۳^۲ = ۱۳$. لذا $n = ۲^۲ \times ۳^۲ = ۳۶$.

۸۴.۱ (اقلیدس، قضیهٔ IX.۳۶.) فرض می‌کنیم p و $۲^p - ۱$ هر دو اول باشند، و قرار می‌دهیم $n = ۲^{p-۱}(۲^p - ۱)$. ثابت کنید $\sigma(n) = ۲n$. (اعداد صحیح n که در $\sigma(n) = ۲n$ صدق کنند اعداد تام نامیده می‌شوند. در فصل ۷ این اعداد به تفصیل بررسی می‌شوند.)

حل. قرار می‌دهیم $q = ۲^p - ۱$. آنگاه تمام مقسوم‌علیه‌های مثبت n به‌صورت ۲^k یا $۲^k q$ هستند که $۰ \le k \le p - ۱$. لذا

$$\begin{aligned}\sigma(n) &= ۱ + ۲ + ۲^۲ + \cdots + ۲^{p-۱} + q + ۲q + ۲^۲q + \cdots + ۲^{p-۱}q \\ &= (q+۱)(۱+۲+۲^۲+\cdots+۲^{p-۱}) = (q+۱)(۲^p-۱) = ۲^p(۲^p-۱) = ۲n\end{aligned}$$

برهان دیگر. چون σ ضربی است و $(۲^{p-۱}, ۲^p - ۱) = ۱$، داریم

$$\sigma(n) = \sigma(۲^{p-۱}q) = \sigma(۲^{p-۱})\sigma(q) = (۲^p - ۱)(q+۱) = q\,۲^p = ۲n$$

حل. (مترجم). قرار می‌دهیم $q = ۲^p - ۱$. چون q اول است پس $۲^{p-۱}q$ تجزیهٔ n به عوامل اول است و لذا بنابر قضیهٔ (۲۰.۱) داریم

$$\sigma(n) = \frac{۲^p - ۱}{۲ - ۱} \times \frac{q^۲ - ۱}{q - ۱} = (۲^p - ۱)(q+۱) = (۲^p - ۱)۲^p = ۲n.$$

تمرینهایی برای فصل ۱

۱. اثبات یا رد کنید: اگر $(m, n) = ۱$، آنگاه $(m+n, mn) = ۱$.

۲. فرض کنید $(m, ۶) = (n, ۶) = ۳$. ثابت کنید $(m+n, ۶) = ۶$.

◁ ۳. فرض کنید $(m, n) = ۱$. ثابت کنید که بمعم $m + ۲n$ و $n + ۲m$ یا ۱ یا ۳ است.

۴. همهٔ اعداد صحیح مثبت m و n را بیابید که $(m, n) = ۸$ و $[m, n] = ۲۰۰$.

۵. در چه شرایطی $(m, n) = [m, n]$؟

۶. فرض کنید p اول باشد. عبارت $p^\alpha || a$ بدین معنی است که $p^\alpha | a$ و $p^{\alpha+۱} \nmid a$. (الف) اگر $p^\alpha || a$ و $p^\beta || b$، نشان دهید $p^{\alpha+\beta} || ab$.

(ب) اگر $p^\alpha || a$ و $p^\beta || b$، که $\alpha < \beta$، ثابت کنید $p^\alpha || a+b$. اگر $\alpha = \beta$، آیا قضیه برقرار است؟

۷. فرض می‌کنیم $(r, s) = ۱$. مقادیر ممکن برای $(r+s, r^۲ + s^۲)$ را تعیین کنید.

۸. ثابت کنید که به‌ازای هر $k \geq ۱$، $(۷k + ۱۶, ۳k + ۷) = ۱$.

۹. فرض می‌کنیم k عدد صحیح مثبتی باشد. مقدار $(۵k + ۴, ۹k - ۷)$ چقدر است؟

۱۰. اگر $(a, b) = ۱$، ثابت کنید $(a^۲ - b^۲, ۲ab)$ برابر ۱ یا ۲ است.

۱۱. اگر $ab' - a'b = ۱$، ثابت کنید $(a + a', b + b') = ۱$.

۱۲. اگر $r | u$ و $s | v$، آیا $r + s | u + v$؟ توضیح دهید.

۱۳. اثبات یا رد کنید: اگر p و q دو عدد اول متمایز باشند و $pq | k^۲$، آنگاه $pq | k$.

۱۴. اعداد اول p را تعیین کنید که $۷p + ۴$ مربع کامل باشد.

۱۵. آیا عدد اولی مانند p، و اعداد صحیحی مانند m و n وجود دارند که $p = m^۴ - n^۴$؟

۱۶. هفت عدد صحیح مثبت متوالی پیدا کنید که همهٔ آنها مرکب باشند.

۱۷. اگر $a = ۲^۳ \times ۵^۲ \times ۱۳^۳ \times ۱۷$، $b = ۲ \times ۷^۳ \times ۱۳ \times ۱۷^۲$ را (a,b) و $[a,b]$ محاسبه کنید.

۱۸. آیا چهار عدد صحیح وجود دارند که هیچ عامل مشترک بزرگتر از ۱ نداشته باشند ولی هیچ دوتای آنها نسبت به هم اول نباشند؟

۱۹. به استقرا ثابت کنید که به‌ازای هر $n \geq ۱$، $۷ | n^۷ - n$.

۲۰. اثبات یا رد کنید: اگر $r | s+t$ و $(s,t) = ۱$، آنگاه $(r,s) = (r,t) = ۱$.

۲۱. اثبات یا رد کنید: اگر $(r,s) = (u,v) = ۱$ و $r/s + u/v$ عدد صحیحی باشد، آنگاه $s = \pm v$.

۲۲. کوچکترین مقدار n را بیابید به‌طوری که $۷^۳ | n!$ ولی $۷^۴ \not| n!$.

۲۳. ۸۳! به چند صفر ختم می‌شود؟

۲۴. به‌ازای چه مقادیری از n، $n!$ به ۲۶ صفر ختم می‌شود؟

۲۵. آیا nی وجود دارد که $n!$ دقیقاً به ۳۵ صفر ختم شود؟

۲۶. بزرگترین توان ۱۱ را که $(۱۱^۷ - ۱)!$ را بشمارد به‌دست آورید.

۲۷. $۱۰۰!/۲۵!$ به چند صفر ختم می‌شود؟

۲۸. بزرگترین توان ۷ را که $۵۰۰!$ را می‌شمارد پیدا کنید.

۲۹. تعداد اعداد صحیحی را پیدا کنید که دقیقاً بین ۲۰۰۰ و ۴۰۰۰ قرار دارند و نه بر ۵ بخشپذیرند و نه بر ۷.

◁ ۳۰. آیا $۶^k + ۲۱ \times ۱$ به‌ازای هر $k \geq ۱$ عدد مرکب است؟

۳۱. با استفاده از الگوریتم اقلیدسی بمعم ۴۱۹۹ و ۳۸۴۳۷ را به‌دست آورید. بمعم را به‌صورت ترکیب خطی از ۴۱۹۹ و ۳۸۴۳۷ بیان کنید.

۳۲. شخصی تعداد ۱۰۰ کارت ۳۳ ریالی، ۳۹ ریالی، و ۴۷ ریالی را به قیمت ۳۹۹۸ ریال خریداری می‌کند. اگر تعداد کارتهای ۳۹ ریالی بین ۳۵ و ۴۰ باشد، تعیین کنید که از هر کارت چه تعداد خریده است.

۳۳. کودکی ۴۵۵۰ ریال متشکل از سکه‌های ۱۰۰ ریالی و ۲۵۰ ریالی دارد. تعداد ترکیبهای ممکن چقدر است؟

۳۴. بلیطهای یک نمایش به قیمت ۸۷ تومان، ۷۳ تومان، یا ۵۷ تومان است. در یک نمایش ۴۹۰۰ نفر شرکت‌کننده مبلغ ۳۵۵۰۴۲ تومان پرداختند. اگر تعداد بلیطهای ۸۷ تومانی کمتر از ۲۰۰۰ و بلیطهای ۷۳ تومانی کمتر از ۱۰۰۰ باشد، تعداد بلیطهای هر نوع را تعیین کنید.

۳۵. آیا ترکیبی از ۵۰ سکهٔ ۱۰، ۱۰۰، ۲۵۰ ریالی وجود دارد که مجموع مقادیرشان ۷۵۰۰ ریال باشد؟

۳۶. شخصی تعدادی تمبر ۲۰ ریالی و ۵۰ ریالی به مبلغ ۹۹۰ ریال می‌خرد، تعداد ترکیبهای ممکن را تعیین کنید.

۳۷. (ازکتاب باشه[1] با عنوان مسائلی مطبوع و دلنشین که از اعداد ساخته می‌شوند[2] (۱۶۱۲). گروهی متشکل از ۴۱ زن و مرد و کودک در یک مهمانخانه غذا صرف کردند و صورتحساب ۴۰ سو[3] شد. اگر سهم هر مرد ۴ سو، زن ۳ سو، و هر سه کودک یک سو باشد، تعداد مردها، زنها، و بچه‌ها را تعیین کنید.

۳۸. (از جبر اویلر (۱۷۷۰).) کشاورزی مبلغ ۱۷۷۰ کرون[4] برای خرید تعدادی اسب و گاو نر می‌پردازد. اگر قیمت هر اسب ۳۱ کرون و قیمت هر گاو ۲۱ کرون باشد، تعداد اسبها و تعداد گاوها را تعیین کنید.

۳۹. (از جبر اویلر) یک شیلینگ به دوستم بدهکارم و با خودم فقط سکه‌هایی داریم که هر یک ۲۱ شیلینگ ارزش دارند. همراه دوستم نیز سکه‌هایی است که هرکدام ۱۷ شیلینگ ارزش دارند. چگونه بدهی خود را بپردازم؟

۴۰. (بهاسکره[5]) دو ثروتمند با ثروت متساوی وجود دارند. یکی از آنها دارای ۵ یاقوت قرمز، ۸ یاقوت کبود، ۷ مروارید و ۹۰ سکهٔ طلاست. دیگری ۷ یاقوت قرمز، ۹ یاقوت کبود، ۶ مروارید، و ۶۲ سکهٔ طلا دارد. قیمت هر یک از گوهرها را برحسب سکهٔ طلا حساب کنید.

۴۱. تمام جوابهای $۶۳x - ۳۶y = ۳$ را به‌دست آورید. آیا جواب مثبت وجود دارد؟ اگر چنین است، چه تعداد؟

۴۲. بمعم $۲^{۳۲} + ۱$ و $۲^{۸} + ۱$ را به‌دست آورید. بمعم را به‌صورت ترکیب خطی این اعداد بنویسید.

۴۳. آیا اعداد صحیح a و b وجود دارند به‌طوری که $a/۲۹ + b/۳۷ = ۳۹/۳۲۱۹$؟

۴۴. ترکیبی خطی از ۲۹ و ۳۱۳ به‌دست آورید که برابر ۱ باشد.

۴۵. ۱ را به‌صورت ترکیب خطی از اعداد متباین ۱۸۹۵ و ۱۸۰۱ بنویسید.

۴۶. فرض کنید $d = (۲۰۷۸۵, ۴۴۳۵۰)$. x و y را پیدا کنید که $۲۰۷۸۵x + ۴۴۳۵۰y = d$.

۴۷. آیا می‌توان ۲۱ را به‌صورت ترکیب خطی ۵۲۷۸ و ۴۵۰۸ نوشت؟

۴۸. معادلهٔ $۱۰۱x + ۹۹y = ۳۰۰۰۰$ چه تعداد جواب مثبت دارد؟

۴۹. فرض کنید a و b اعداد صحیح مثبت، و $d = (a, b)$. نشان دهید که اعداد مثبت u و v وجود دارند به‌طوری که $au - bv = d$.

---

1. Bachet 2. *Problèmes plaisants et dèlectables quis se font par les nombres.*
3. sou 4. crown (سکهٔ پنج شیلینگی) 5. Bhāskara

۵۰. همهٔ جوابهای صحیح دستگاه معادلات زیر را به‌دست آورید

$$۲x + ۵y - ۱۱z = ۱$$
$$x - ۱۲y + ۷z = ۲۰$$

۵۱. (الف) بمعم ۷۹۱ و ۱۲۴۳ رابه‌دست آورید.

(ب) آیا معادلهٔ دیوفانتی $۷۹۱x + ۱۲۴۳y = ۲۸۲۵$ جوابی دارد؟ اگر چنین است، جواب عمومی آن را به‌دست آورید.

۵۲. $\tau(۸۵۷۵۰۰)$ و $\sigma(۸۵۷۵۰۰)$ را محاسبه کنید.

۵۳. $\tau(۱۳!)$ و $\sigma(۱۳!)$ را محاسبه کنید.

۵۴. فرض کنید n عدد صحیح مثبتی باشد. چه تعداد جفت مرتب (x, y) از اعداد مثبت در معادلهٔ $۱/x + ۱/y = ۱/۱۲۰۰$ صدق می‌کنند؟ (راهنمایی: نشان دهید که این معادله با معادلهٔ $(x - ۱۲۰۰)(y - ۱۲۰۰) = (۱۲۰۰)^۲$ هم‌ارز است.)

۵۵. اثبات یا رد کنید: اگر $\sigma(n)$ اول باشد، آنگاه n توانی از یک عدد اول است.

◁ **۵۶.** ثابت کنید به‌ازای هر $n \geq ۱$، $\tau(n) \leq ۲\sqrt{n}$.

۵۷. $\sigma(۳۳۰)$، $\sigma(۲۴۵۰۰)$، و $\sigma(۱۰!)$ را محاسبه کنید.

◁ **۵۸.** فرض کنید m و n دو عدد صحیح مثبت باشند. ثابت کنید $\tau(mn) \leq \tau(m)\tau(n)$. (راهنمایی: ابتدا حالتی را در نظر بگیرید که m و n توانهایی از عدد اول واحدی هستند.)

۵۹. اثبات یا رد کنید: n حاصلضرب k عدد اول متمایز است اگر و تنها اگر $\tau(n) = ۲^k$.

۶۰. عدد صحیح مثبتی بیابید که $\sigma(n) = \sigma(n + ۱)$.

۶۱. اعدادی را پیدا کنید که بر ۱۲ بخشپذیر باشند و دقیقاً ۱۴ مقسوم‌علیه مثبت داشته باشند.

ملاحظاتی برای فصل ۱

۱. الگوریتم کوچکترین باقیماندهٔ مطلق. الگوریتمی که اقلیدس در قضیهٔ VII ۲۰ی اصول بیان کرده خیلی نزدیک به روندی است که در این فصل بیان شده است. تنها تفاوت در این است که به‌جای تقسیم a بر b، اقلیدس پیوسته b را از a کم می‌کند تا جایی که نتیجه کمتر از a شود. پیچیدگی مختصری وجود دارد و آن این است که برای اقلیدس ۱ عدد نیست.

الگوریتم اقلیدس، با وجود قدمت قابل احترامش، هنوز هم یکی از کارآمدترین روشهای شناخته‌شده برای یافتن بزرگترین مقسوم‌علیه مشترک است، اما روند نسبتاً سریعتری وجود دارد که بعداً شرح می‌دهیم.

یادآور می‌شویم که الگوریتم اقلیدسی کارساز است زیرا $(m,n)=(n,m-tn)=(n,s)$، که در آن $s=m-tn$، اگر مانند (۲۳.۱)، فرض کنیم s باقیماندهٔ تقسیم m بر n باشد، آنگاه متوالیاً بمعم اعداد کوچکتر و کوچکتر را جستجو می‌کنیم، تا جایی که مسأله بدیهی شود. انتخاب مناسب دیگر برای s عددی است به‌صورت $m-tn$ که کوچکترین قدرمطلق را داشته باشد. مطابق معمول m را بر n تقسیم می‌کنیم و فرض می‌کنیم باقیمانده r باشد، که $0<r\leq|n|$. اگر $r\leq|n|/2$، s را برابر r می‌گیریم؛ در غیر این‌صورت، فرض می‌کنیم $s=r-|n|$. در این‌صورت $|s|\leq|n|/2$.

به آسانی معلوم می‌شود که این صورت دیگر الگوریتم اقلیدس بزرگترین مقسوم‌علیه مشترک را تولید می‌کند. مانند الگوریتم اقلیدسی، می‌توان آن را برای یافتن x و y به‌طوری که $ax+by=(a,b)$ به‌کار برد. به‌طور شهودی پذیرفته شده است، و در واقع درست است، که الگوریتم کوچکترین باقیماندهٔ مطلق هرگز مراحل تقسیم بیشتری را از الگوریتم اقلیدسی طلب نمی‌کند، و به‌طور قابل ملاحظه‌ای می‌تواند بهتر باشد. مثلاً، برای محاسبهٔ (۹۸۷، ۱۵۹۷) الگوریتم اقلیدسی ۱۵ مرحله دارد، در حالی‌که الگوریتم کوچکترین باقیماندهٔ مطلق فقط از ۸ مرحله استفاده می‌کند.

۲. الگوریتم بزرگترین مقسوم‌علیه مشترک دوتایی. این الگوریتم بر یک فکر کاملاً متفاوت بنا شده است. فرض کنیم m و n مثبت باشند.

(i) اگر m و n هر دو زوج باشند، آنگاه $(m,n)=2(m/2,n/2)$.

(ii) اگر m و n هر دو فرد باشند، آنگاه با فرض $m>n$، $(m,n)=(m-n,n)$.

(iii) اگر یکی از m و n (مثلاً m) زوج و دیگری فرد باشد، آنگاه $(m,n)=(m/2,n)$.

(iv) اگر $m=n$، آنگاه $(m,n)=m$.

چون $m-n$ زوج است وقتی که m و n فرد هستند، پس عمل تقسیم بر ۲ را حداقل در هر دو مرحله انجام می‌دهیم، لذا الگوریتم با سرعت زیاد به پایان می‌رسد. بمعم دوتایی به‌ویژه در رایانهٔ دودویی کارآمد است. تقسیم یک عمل نسبتاً کند است، و در تقسیمها بیشتر وقت صرف کاربرد الگوریتم اقلیدسی می‌شود. ولی، در یک رایانهٔ دودویی تقسیم بر ۲ سریع صورت می‌گیرد (فقط ۰ پایانی را در نمایش دودویی عدد حذف می‌کنیم).

در یک روش سرراست می‌توان الگوریتم بمعم دوتایی را برای تولید x و y به‌طوری که $ax+by=(a,b)$ توسعه داد. (این دید ممکن است جدید باشد، مثلاً کنوث[1] و کوبلیتس[2]، هر دو مدعی هستند که الگوریتم به‌این روش بسط نمی‌یابد. منابع انتهای فصل را ملاحظه کنید.)

1. Knuth 2. Koblitz

بدون آنکه به کلیت استدلال خللی وارد آید، می‌توانیم فرض کنیم که a و b هر دو زوج نیستند، زیرا اگر هر دو زوج باشند، مکرراً (i) را به‌کار می‌بریم تا سرانجام یکی فرد شود و اعداد a' و b' به‌دست آیند. آشکار است که اگر $a'x + b'y = (a', b')$، آنگاه $ax + by = (a, b)$.

اگر (ii) را به‌کار بریم و اعداد s، t، u، و v را محاسبه کنیم به‌طوری که $as + bt = m$ و $au + bv = n$، آنگاه $m - n = a(s - u) + b(t - v)$.

بالاخره، فرض می‌کنیم که (iii) را به‌کار برده و u و v را یافته‌ایم به‌طوری که $au + bv = m$. می‌خواهیم که $m/۲$ را به‌صورت ترکیبی خطی از a و b بنویسیم. اگر u و v زوج باشند این عمل پیش‌پا افتاده است، لذا فرض کنیم لااقل یکی از آنها فرد باشد. یک بررسی ساده از حالتها نشان می‌دهد که $u + b$ و $v - a$ زوج هستند. لذا می‌توانیم $m/۲$ را به‌صورت یک ترکیب خطی از a و b بنویسیم، یعنی، $m/۲ = a((u + b)/۲) + b((v - a)/۲)$.

۳. قضیهٔ اصلی حساب. اولین بیان صریح و اثبات این قضیه در تحقیقات حسابی گاوس[1] آمده است، اما اغلب این نتیجه را به اقلیدس، حدود ۲۰۰۰ سال پیشتر، نسبت می‌دهند. لم اصلی (۱۵.۱) اساساً قضیهٔ ۳۰ از مقالهٔ VII است. ولی نزدیکترین کار اقلیدس به قضیهٔ اصلی (به زبان امروزی) آن است که نشان دهد اگر N کوچکترین عددی باشد که به اعداد اول $p_۱$، $p_۲$، ...، p_k بخشپذیر است، آنگاه N به عدد اول دیگری بخشپذیر نیست.

احتمالاً قضیهٔ اصلی به صراحت بیان نشده است زیرا تجربهٔ ما در تجزیه آن را بسیار بدیهی‌تر از آنچه که بخواهیم به آن بپردازیم می‌سازد. اینکه گاوس دریافت که این قضیه احتیاج به اثبات دارد ستایشی از بینش و دقت زیاد اوست. در اواسط سدهٔ نوزدهم، ریاضیدانان سرگرم کشف دستگاههای عدد صحیح‌گونه بودند که در آنها مشابه قضیهٔ اصلی برقرار نباشد. بعضی از اینها در فصل ۱۱ بررسی شده‌اند.

اینک مثالی توضیحی، منتسب به داوید هیلبرت[2] (۱۹۴۳ـ۱۸۶۲)، ارائه می‌دهیم که نشان می‌دهد قضیهٔ تجزیهٔ یکتا به آن وضوحی که به نظر می‌رسد نیست. فرض کنیم H مجموعهٔ تمام اعداد صحیح به‌صورت $۴k + ۱$ باشد. به آسانی دیده می‌شود که حاصلضرب عناصر H نیز در H قرار دارند. اگر $m > ۱$ عنصری از H باشد، m یک Hـپریم خوانده می‌شود اگر m هیچ مقسوم‌علیه مثبتی در H جز ۱ و خودش نداشته باشد. از این‌رو، مثلاً، ۲۱ عنصری از H است که به معنی معمول عدد مرکب است اما یک Hـپریم است. (درست است که $۳ \times ۷ = ۲۱$، اما ۳ و ۷ عناصر H نیستند.)

اگر m عنصری از H بزرگتر از ۱ باشد، اثبات اینکه می‌توان m را به‌صورت حاصلضرب Hـپریمها

1. *Gauss's Disquisitiones Arithmeticae* 2. David Hilbert

بیان کرد مشکل نیست. اما این نمایش لزوماً یکتا نیست؛ مثلاً، $۴۴۱ = ۹ \times ۴۹ = ۲۱ \times ۲۱$ که در آنها ۹، ۴۹، و ۲۱ همگی Hـپریم‌اند.

اگر بررسی بیشتری انجام دهیم، می‌بینیم که تعدادی از قضیه‌های اصلی ما برقرار نیستند. Hـبمعم دو عنصر a و b از H را به‌عنوان بزرگترین عنصری از H که a و b را می‌شمارد تعریف می‌کنیم. اگر Hـبمعم a و b برابر d باشد و e یک مقسوم‌علیه مشترک a و b باشد، لزوماً $e|d$ برقرار نیست. مثلاً، ۲۱ برابر Hـبمعم $a = ۳^۲ \times ۷ \times ۱۱$ و $b = ۳^۳ \times ۷$ است، اما ۹ نیز یک مقسوم‌علیه مشترک a و b است.

شرح مختصری از زندگینامه‌ها

آریبهطه در سال ۴۷۶ و احتمالاً در شهری که اکنون شهر هندی پاتنا[1] نامیده می‌شود به دنیا آمد. همانند اکثر هندیان پیشین که سهمی در ریاضیات داشته‌اند، او نیز اصولاً یک منجم بود. آریبهطه و اخلافش بهاسکره و برهمگوپته یک نجومِ ریاضی خیلی پیچیده را توسعه دادند که در آن حل معادلات دیوفانتی نقش داشت. آریبهطه، مانند سلف یونانیش بطلمیوس[2]، مقدار دقیقی برای π به‌دست داد (در این مورد ۳٫۱۴۱۶)، و جدولی از سینوسها را تهیه کرد. مشهورترین کار او کتاب آریبهطیه[3] است، که ۳۳ شعر آن به ریاضیات، ۲۵ شعر به محاسبهٔ زمان و مدلهای حرکت سیاره‌ای، و ۵۰ تا به مطالعهٔ خسوف و کسوف اختصاص دارد. (در هندوستان سنت چنین بوده است که حتی کارهای فنی را نیز به شعر می‌نوشته‌اند.) به نظر می‌رسد که آریبهطه اولین کسی باشد که معادلات دیوفانتی خطی را با روش نظام‌مندی (اساساً الگوریتم اقلیدسی) حل کرده است.

اقلیدس احتمالاً در حدود ۳۰۰ ق.م. شکوفا شد. امکان دارد که ریاضیات را در آتن زیر نظر اخلاف افلاطون آموخته باشد، گمان می‌رود که او مؤسس مدرسهٔ بزرگ ریاضیات در اسکندریه بوده است، زیرا شهر اسکندریه در دوران باستان دارای کتابخانهٔ بسیار بزرگ و موزه و مرکز دانش‌پژوهی بوده است. علاوه بر کتاب اصول، اقلیدس کتابهایی در قطوع مخروطی (که اکنون وجود ندارد)، نور، نجوم ریاضی، و موسیقی داشته است.

امکان دارد که قسمت عمده‌ای از اصول یک گردآوری و نظام‌بخشی از کار ریاضیدانان پیشین، به‌ویژه تئاتیتوس[4] و ائودوکسوس باشد؛ سرنخهایی وجود دارد که به سال ۵۰۰ ق.م. و فیثاغوریان اولیه برمی‌گردد. منتخباتی از مشکلترین و جالبترین قسمتهای اصول اساس ساختمان ریاضیات

1. Patna 2. Ptolemy 3. Aryabhatiya 4. Theaetetus

پیشرفته تا سدهٔ هجدهم بوده است. از صورتهای ساده‌شدهٔ قسمتهایی از اصول تا سدهٔ بیستم کاملاً در دبیرستانها استفاده می‌شده است.

مراجع

Thomas L. Heath. *The Thirteen Books of Euclid's Elements, Volume II*, Cambridge University Press, Cambridge, England, 1926.

این کتاب چاپ انگلیسی استانده از اصول اقلیدس است. به‌ویژه، جلد II شامل مقاله‌های حسابی IX_VII است. هیث شرح و تفسیرهای فنی جامعی بر کتاب اقلیدس آورده است. این کتاب بسیار ناموزون است، به‌طوری که از برهان کلاسیک نامتناهی بودن اعداد اول گرفته تا یک بحث خشک، در ۱۳ قضیه، از ویژگیهای پیش‌پا افتادهٔ اعداد زوج و فرد تغییر می‌کند.

Donald E. Knuth. *The Art of Computer Programming, Volume* 2 (Second Edition), Addison-Wesley, Reading, Massachusetts, 1981.

این یک کتاب منبع ضروری برای هر کسی است که بخواهد در مورد برنامه‌های رایانه‌یی نظریه‌یی اعداد مطلب بنویسد. یک تحلیل تفصیلی زیبا از الگوریتم اقلیدسی و یک گنجینه از سایر اطلاعات را شامل می‌شود. مطالب از مقدماتی به دشوار مرتب و تماماً با یک سبک توضیحی استادانه مورد بحث واقع شده‌اند.

Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

کتاب بر آن قسمتهایی از نظریهٔ اعداد تکیه دارد که مورد نیاز کارهای جدید در راهنمای عمومی رمزنویسی است. توجه زیادی به الگوریتمهای نظریهٔ اعداد، به‌ویژه الگوریتمهای تجزیه و آزمونهای اساسی شده است. بعضی از مطالب کتاب کاملاً پیشرفته هستند، ولی کتاب یک مقدمهٔ بسیار خوب نیز برای نظریهٔ مقدماتی اعداد ارائه می‌دهد.

۲

همنهشتیها

در بخش آغازین تحقیقات حسابی، گاوس نظریهٔ همنهشتیهایش را چنین معرفی کرده است:

> اگر عدد a تفاضل دو عدد b و c را بشمارد، آنگاه b و c نسبت به a همنهشت خوانده می‌شوند؛ اگر نشمارد، b و c ناهمنهشت هستند. عدد a پیمانه نامیده می‌شود.

در کار با همنهشتیها، گاوس فقط به باقیماندهٔ تقسیم یک عدد بر عدد دیگر توجه داشت. نماد همنهشتی که او معرفی کرده است فرمولبندی قضیه‌های مربوط به ویژگیهای بخشپذیری و انجام محاسبات ضروری را بسیار آسانتر می‌سازد.

مفهوم همنهشتی در نظریهٔ نوین اعداد بنیادی است، اما مفاهیم زیربنایی آن به سده‌ها جلوتر از کار گاوس برمی‌گردند. در هندوستان، آریبهطه ریاضیدان و منجم سدهٔ ششم چگونگی حل آنچه را که ما امروزه دستگاه دو همنهشتی خطی می‌نامیم نشان داده است. برهمگوپته ریاضیدان سدهٔ هفتم به مسائل مربوط به گاهنامه‌ها می‌پرداخت چون که آنها به چرخشهای سیاره‌ای مربوط

می‌شوند؛ این نیز به مسائل پیچیده‌ای منجر می‌شد که با استفاده از روشهای این فصل حلپذیرند. در اواسط سدهٔ دوازدهم، بهاسکره تحلیل کاملی از دستگاههای همنهشتیهای خطی به‌دست داد. همنهشتیها به‌ویژه در مسائل گاهشماری، مثلاً، تعیین روز عید پاک یا پیدا کردن روزی از هفته برای یک تاریخ به‌خصوص، مفید است.

مسائلی نیز در آثار ریاضی چین باستان یافت می‌شوند که متضمن پیدا کردن اعدادی هستند که در تقسیم بر مجموعهٔ مفروضی از اعداد صحیح باقیمانده‌های مشخصی داشته باشند. (مسألهٔ ۴۳.۲ را ببینید.) تکنیک به‌کار رفته برای حل آنها در زبان چینی به‌قانون تاین معروف است. یک سنت طولانی از چنین مسائلی وجود دارد، که از سون‌ـتسو[1] در سدهٔ سوم شروع می‌شود و در کارهای چئین چیو‌ـشائو[2] در ۱۲۴۷ به اوج خود می‌رسد. این قضیهٔ اصلی اکنون به قضیهٔ باقیماندهٔ چینی معروف شده است. اولین بیان و اثبات این قضیه با زبان کم‌وبیش امروزی به لئونهارت اویلر (۱۷۰۷ـ۱۷۸۳) منسوب است.

قضیه‌هایی برای فصل ۲

(۱.۲) تعریف. فرض کنیم m عدد صحیح مثبتی باشد. اگر m تفاضل $a-b$ از دو عدد صحیح را بشمارد، گوییم که a همنهشت با b به پیمانهٔ m است و می‌نویسیم $a \equiv b (\mathrm{mod}\, m)$. (در غیر این‌صورت، گوییم که a همنهشت با b به پیمانه m نیست و می‌نویسیم $a \not\equiv b (\mathrm{mod}\, m)$) عدد m پیمانه خوانده می‌شود.

اگر $a \equiv b (\mathrm{mod}\, m)$، آنگاه b ماندهٔ a به پیمانهٔ m خوانده می‌شود (و برعکس). هرگاه $0 \leq b \leq m-1$، b کوچکترین ماندهٔ نامنفی a به پیمانهٔ m نامیده می‌شود.

توضیح. امروزه معمول است که کوچکترین ماندهٔ نامنفی a به پیمانهٔ m را با $a \bmod m$ نشان می‌دهند. لذا a همنهشت با b به پیمانهٔ m است اگر و تنها اگر $a \bmod m = b \bmod m$. هر چند که این نماد یقیناً مفید است، به‌ویژه در برنامه‌های رایانه‌یی، ولی در آنچه می‌آید ما آن را به‌کار نخواهیم برد.

یک طریق هم‌ارز تعریف $a \equiv b (\mathrm{mod}\, m)$ عبارت از این است که بگوییم تفاوت a و b در مضربی از m است، یعنی، عدد صحیحی مانند k وجود دارد به‌طوری که $a+b=km$. پیش از گاوس، به جای نوشتن «$a \equiv b (\mathrm{mod}\, m)$»، ریاضیدانان می‌نوشتند «a به‌صورت $km+b$ است». هنوز هم معمول است که مثلاً به جای استفاده از نماد همنهشتی $a \equiv ۱ (\mathrm{mod}\, ۴)$ بگوییم

1. Sun-Tzu 2. Ch'in Chiu-Shao

a به‌صورت $۴k + ۱$ است.

در حالت خاص که a مضربی از m باشد، داریم $a \equiv ۰ \pmod m$. به‌طور کلی، به‌ازای عدد صحیح مفروض a، اگر r کوچکترین عدد صحیح نامنفی باشد که همنهشت با a به پیمانه m است، r همان باقیماندهٔ تقسیم a بر m است. بنابراین، دو عدد همنهشت به پیمانهٔ m هستند اگر و تنها اگر در تقسیم بر m باقیماندهٔ واحدی داشته باشند. از آنجا که تقسیم بر m یکی از اعداد ۰، ۱، ۲، ...، $m - ۱$ را به‌عنوان باقیمانده به ما می‌دهد، نتیجه می‌شود که هر عدد صحیح همنهشت به پیمانهٔ m با یکی از این m عدد است. بنابراین، باقیمانده برای عدد مفروض a کوچکترین ماندهٔ نامنفی a به پیمانهٔ m است. مجموعهٔ $\{۰, ۱, \ldots, m - ۱\}$ مثالی از یک دستگاه کامل مانده‌ها به پیمانهٔ m است، یعنی گردایه‌ای از m عدد ناهمنهشت به پیمانهٔ m به‌طوری که هر عدد دقیقاً با یکی از اعداد گردایه همنهشت است. روشن است که می‌توان به‌جای هر عنصر در یک دستگاه کامل مانده‌ها هر عددِ همنهشت به پیمانهٔ m با آن، را گذارد. (مثلاً، $\{۱۰, -۴, ۷, ۳, ۲۴\}$ یک دستگاه کامل مانده‌ها به پیمانهٔ ۵ است.) معمولاً با دستگاه کامل مانده‌های $\{۰, ۱, \ldots, m - ۱\}$ کار می‌کنیم. در اینجا توجه می‌کنیم که هر m عدد صحیح متوالی یک دستگاه کامل مانده‌ها به پیمانهٔ m تشکیل می‌دهند، زیرا باقیمانده‌های تقسیم این اعداد صحیح بر m دقیقاً همان اعداد ۰، ۱، ...، $m - ۱$ هستند.

مطالب پایه‌یی زیر در مورد همنهشتیها نظیر مطالب مربوط به مطالبی هستند که برای معادله‌های معمولی صادق‌اند.

(۲.۲) قضیه. فرض کنیم m عدد صحیح مثبتی باشد

(i) اگر $a \equiv b \pmod m$، آنگاه $b \equiv a \pmod m$.

(ii) اگر $a \equiv b \pmod m$ و $b \equiv c \pmod m$، آنگاه $a \equiv c \pmod m$.

(iii) اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$، آنگاه $a \pm c \equiv b \pm d \pmod m$.

(iv) اگر $a \equiv b \pmod m$، آنگاه به‌ازای هر c، $ca \equiv cb \pmod m$.

(v) به‌ازای هر مقسوم‌علیه مشترک a، b، و m مانند c، $a \equiv b \pmod m$ اگر و تنها اگر $a/c \equiv b/c \pmod{m/c}$.

(vi) اگر $ca \equiv cb \pmod m$، آنگاه $a \equiv b \pmod{m/(c, m)}$، به‌ویژه اگر c و m نسبت به هم اول باشند، آنگاه $ca \equiv cb \pmod m$ ایجاب می‌کند $a \equiv b \pmod m$.

برهان. اثبات قسمتهای (i) تا (v) مستقیماً از تعریف همنهشتی نتیجه می‌شود. برای اثبات (vi)،

فرض می‌کنیم $ca \equiv cb(\mathrm{mod}\, m)$؛ لذا عدد صحیحی مانند k وجود دارد که $(a-b)c = km$. اگر $d = (c, m)$، آنگاه $(a-b)c/d = km/d$. چون عدد صحیح m/d طرف راست را می‌شمارد، پس باید طرف چپ را نیز بشمارد. اما بنابر (ii.۷.۱)، c/d و m/d نسبت به هم اولند، لذا m/d عدد $a-b$ را می‌شمارد، یعنی $a \equiv b(\mathrm{mod}\, m/d)$.

توضیح. در حالت کلی نمی‌توانیم طرفین یک همنهشتی را بر عددی تقسیم کنیم بدون آنکه پیمانه را تغییر دهیم. مثلاً، از تقسیم طرفین همنهشتی درست $۱۵ \equiv ۵ (\mathrm{mod}\, ۱۰)$ بر ۵ همنهشتی $۳ \equiv ۱ (\mathrm{mod}\, ۱۰)$ حاصل می‌شود که نادرست است. همنهشتی صحیح عبارت است از $۳ \equiv ۱ (\mathrm{mod}\, ۲)$.

(۳.۲) قضیه. فرض کنیم m مثبت، و a، b، c، و d اعداد صحیح دلخواه باشند.

(i) اگر $a \equiv b(\mathrm{mod}\, m)$ و $c \equiv d(\mathrm{mod}\, m)$، آنگاه $ac \equiv bd(\mathrm{mod}\, m)$.

(ii) اگر $a \equiv b(\mathrm{mod}\, m)$، آنگاه به‌ازای هر عدد مثبت n، $a^n \equiv b^n(\mathrm{mod}\, m)$.

(iii) اگر $f(x)$ هر چند جمله‌یی با ضرایب صحیح باشد و $a \equiv b(\mathrm{mod}\, m)$، آنگاه $f(a) \equiv f(b)(\mathrm{mod}\, m)$.

برهان. برای اثبات (i) توجه داریم که بنابر (iv.۲.۲)، $ac \equiv bc(\mathrm{mod}\, m)$، و مجدداً بنابر همان (iv.۲.۲)، $bc \equiv bd(\mathrm{mod}\, m)$. قسمت (ii) از (i) با ضرب مکرر $a \equiv b(\mathrm{mod}\, m)$ در خودش به‌دست می‌آید. قسمت (iii) از (ii) با کاربرد (iii.۲.۲) و (iv.۲.۲) نتیجه می‌شود.

(۴.۲) قضیه. فرض کنیم m عدد صحیحی مثبت باشد.

(i) فرض کنیم $d|m$ و $d > ۰$. اگر $a \equiv b(\mathrm{mod}\, m)$، آنگاه $a \equiv b(\mathrm{mod}\, d)$.

(ii) اگر $a \equiv b(\mathrm{mod}\, m_۱)$ و $a \equiv b(\mathrm{mod}\, m_۲)$، آنگاه $a \equiv b(\mathrm{mod}\, [m_۱, m_۲])$.

(iii) به‌طور کلی، $a \equiv b(\mathrm{mod}\, m_i)$ $(i = ۱, ۲, \ldots r)$ اگر و تنها اگر $a \equiv b(\mathrm{mod}\, m)$، که در آن $m = [m_۱, m_۲, \ldots, m_r]$.

برهان. قسمت (i) از تعریف همنهشتی واضح است؛ (ii) از این مطلب نتیجه می‌شود که اگر $r|k$ و $s|k$، آنگاه کوچکترین مضرب مشترکشان $[r, s]$ نیز k را می‌شمارد. برای اثبات (iii)، ملاحظه می‌کنیم که اگر $m|a-b$، آنگاه به‌ازای هر i، $m_i|a-b$. برعکس، اگر به‌ازای هر i، $m_i|a-b$، آنگاه بنابر (۱۲.۱) $[m_۱, m_۲, \ldots, m_r]|a-b$.

اگر $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ تجزیهٔ m به عوامل اول باشد، آنگاه همنهشتی $a \equiv b (\mathrm{mod}\, m)$ هم‌ارز دستگاه همنهشتیهای $a \equiv b (\mathrm{mod}\, p_i^{k_i})$ $(i = 1, 2, \dots, r)$ است. از این‌رو، مثلاً برای حل همنهشتی $ax + b \equiv 0 (\mathrm{mod}\, m)$، کافی است جوابهای x_i از $ax + b = 0 (\mathrm{mod}\, p_i^{k_i})$ را به‌ازای $i = 1, 2, \dots, r$ به‌دست آوریم و سپس جوابی از همنهشتی اصلی را با کاربرد قضیهٔ باقیماندهٔ چینی، که به‌زودی از آن صحبت خواهیم کرد، تولید کنیم.

آزمونهای بخشپذیری

قدری تأمل می‌کنیم تا کاربردی از همنهشتی را به‌دست دهیم. گاوس در انتهای بخش ۱ در تحقیقات حسابی دریافت که می‌توان همنهشتیها را برای بررسی بخشپذیری بر بعضی اعداد به‌کار برد. از نظر تاریخی، آزمونهایی از این قبیل را می‌توان در کارهای خوارزمی ریاضیدان قرن نهم یافت؛ این قضیه‌ها در قرون وسطی در اروپا اشاعه یافت. لئوناردو پیسایی[1] (حدود ۱۲۵۰–۱۱۷۵)، که به‌عنوان فیبوناتچی[2] بهتر شناخته می‌شود، آزمونهایی برای بخشپذیری بر ۷، ۹، و ۱۱ در کتاب حسابش[3] ارائه می‌دهد.

(۵.۲) قضیه. فرض کنیم $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$ بسط اعشاری عدد مثبت n باشد. (لذا a_k اولین، یا رقم پیشرو n، a_{k-1} دومین، ...، و a_0 آخرین رقم است.)

(i) n بر 2^r بخشپذیر است اگر و تنها اگر عددی که از r رقم آخر n تشکیل شده است بر 2^r بخشپذیر باشد.

(ii) n بر ۳ بخشپذیر است اگر و تنها اگر مجموع ارقام n بر ۳ بخشپذیر باشد، یعنی: $3 | a_k + \dots + a_0$.

(iii) n بر ۹ بخشپذیر است اگر و تنها اگر مجموع ارقام n بر ۹ بخشپذیر باشد.

(iv) n بر ۱۱ بخشپذیر است اگر و تنها اگر مجموع‌واری a_k $a_0 - a_1 + a_2 - \dots + (-1)^k a_k$ بر ۱۱ بخشپذیر باشد.

برهان. (i) روشن است که برای $j \geq 2$ داریم $10^j = 0 (\mathrm{mod}\, 4)$، لذا $n \equiv 10 a_1 + a_0 (\mathrm{mod}\, 4)$ همچنین، اگر $j \geq 3$، آنگاه $10^j \equiv 0 (\mathrm{mod}\, 8)$، لذا $n \equiv 100 a_2 + 10 a_1 + a_0 (\mathrm{mod}\, 8)$. برای توانهای بالاتر از ۲ اثبات کاملاً همین‌گونه است.

برای اثبات (ii) و (iii) ملاحظه می‌کنیم که $10 \equiv 1 (\mathrm{mod}\, 9)$. لذا به‌ازای هر عدد مثبت j داریم $10^j \equiv 1 (\mathrm{mod}\, 9)$. با جایگذاری این رابطه در بسط اعشاری n داریم

1. Leonardo of Pisa 2. Fibonacci 3. Liber Abaci

$n \equiv a_k + a_{k-1} + \cdots + a_0 \pmod 9$ یعنی، باقیماندهٔ تقسیم n و مجموع a_jها بر ۹ و ۳ برابرند.

اثبات قسمت (iv) از این مطلب نتیجه می‌شود که به‌ازای هر عدد مثبت j، $10^j \equiv (-1)^j \pmod{11}$. اکنون با جایگذاری این رابطه در بسط اعشاری n داریم $n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k \pmod{11}$.

توضیحات. ۱. آزمون واضحی برای بخشپذیری بر ۵ وجود دارد، یعنی، باید رقم آخر عدد ۰ یا ۵ باشد. همچنین، یک عدد بر ۱۰ بخشپذیر است اگر و تنها اگر به ۰ ختم شود.

۲. قسمت (iii) پایهٔ تکنیک معروف به طرح نُه‌نُه است، روشی که برای امتحان صحت محاسبات توسط مقایسهٔ باقیمانده‌ها به پیمانهٔ ۹ به‌کار می‌رود. برهان (iii) نشان می‌دهد که می‌توان باقیماندهٔ تقسیم n بر ۹ را توسط مجموع رقمهای n به پیمانه ۹ به‌دست آورد.

۳. با ترکیب آزمونهای بالا می‌توان بخشپذیری بر سایر اعداد را امتحان کرد. مثلاً، برای اینکه ببینیم عددی بر ۶ بخشپذیر است یا نیست، بخشپذیری بر ۲ و ۳ را امتحان می‌کنیم، برای ۱۵، ۳ و ۵ را. مادام که پیمانه‌های مختلف دوبه‌دو نسبت به هم اول باشند این روند کارساز است.

۴. زمانی آزمونهای بخشپذیری تکنیکی عملی برای بررسی صحت نتایج محاسبات بودند. به نظر می‌رسد که در این عصرِ حسابگرها و رایانه‌ها وابستگی به آنها کم شده است. اما ابزارهای محاسبه، و حتی دیسکتهای فشرده، اشکال پیچیدهٔ آزمونهای بخشپذیری قدیمی را به‌کار می‌برند، از بررسیهای قیاسی ساده گرفته تا کدهای خطاتصحیح کن پیچیده. دومی اغلب بر مفاهیم نظریِ عددیِ دقیق بنا شده است.

همنهشتیهای خطی

ابتدا به بررسی حل همنهشتی خطی $ax \equiv b \pmod m$ می‌پردازیم. برخلاف معادلهٔ خطی $ax = b$، که با شرط $a \neq 0$ همواره دارای یک جواب یکتای حقیقی است، همنهشتی $ax \equiv b \pmod m$ ممکن است بیش از یک جواب (ناهمنهشت) داشته باشد، یا اصلاً جواب نداشته باشد، حتی اگر $a \not\equiv 0 \pmod m$. مطلب را با تعریف جواب یک همنهشتی خطی شروع می‌کنیم.

(۶.۲) تعریف. عدد صحیح s را یک جواب $ax \equiv b \pmod m$ خوانیم هرگاه $as \equiv b \pmod m$. آشکار است که اگر s یک جواب باشد و $s \equiv t \pmod m$، آنگاه نیز یک جواب است. در این‌صورت s و t را به‌عنوان یک جواب در نظر می‌گیریم، و می‌گوییم که

$x \equiv s(\bmod m)$ یک جواب $ax \equiv b(\bmod m)$ است.

با توجه به این تعریف، برای حل یک همنهشتی خطی، کافی است که عناصر یک دستگاه کامل مانده‌ها، مثلاً $\{0, 1, \ldots, m-1\}$ را جایگذاری (امتحان) کنیم.

قضیهٔ زیر یک مشخصه از همنهشتیهای خطی را که دارای جواب هستند، و همچنین بیان کاملی از جوابها را به‌دست می‌دهد.

(۷.۲) قضیه. فرض کنیم $d = (a, m)$. همنهشتی $ax \equiv b(\bmod m)$ حلپذیر است اگر و تنها اگر $d|b$. اگر جواب داشته باشد، دقیقاً d جواب ناهمنهشت به پیمانهٔ m به‌صورت زیر دارد

$$x \equiv x^* + (m/d)t \ (\bmod m) \qquad (t = 0, 1, \ldots, d-1)$$

که در آن x^* یک جواب همنهشتی

$$(a/d)x \equiv b/d \qquad (\bmod m/d)$$

است.

برهان. اگر $ax \equiv b(\bmod m)$، آنگاه عدد صحیحی چون k وجود دارد که $ax = b + km$. چون $b = ax - km$ و a، d و m را می‌شمارد پس $d|b$. برعکس، فرض کنیم $d|b$. بنابر (۲۴.۱) ترکیبی خطی از a و m وجود دارد که با b برابر است، مثلاً $ax + my = b$. این رابطه ایجاب می‌کند که $ax \equiv b(\bmod m)$. لذا ثابت کرده‌ایم که جواب وجود دارد اگر و تنها اگر b مضربی از d باشد.

حال فرض کنیم که $ax \equiv b(\bmod m)$ حلپذیر است؛ پس $d|b$، و از این‌رو $(a/d)x \equiv b/d(\bmod m/d)$ نیز حلپذیر است. اگر x^* جوابی از همنهشتی دوم باشد، عدد صحیحی چون k وجود دارد که $(a/d)x^* = b/d + km/d$؛ از این‌رو $ax^* - mk = b$، و لذا x^*، k جوابی از $ax - my = b$ است. بنابر (۲۴.۱)، جوابهای این معادله مقادیر x را به‌صورت $x = x^* + (m/d)t$ به ما می‌دهد، که t دلخواه است. اما $x^* + (m/d)t_1 \equiv x^* + (m/d)t_2(\bmod m)$ اگر و تنها اگر $(m/d)t_1 \equiv (m/d)t_2(\bmod m)$. از تقسیم طرفین بر m/d، شرط هم‌ارز $t_1 \equiv t_2(\bmod d)$ را به‌دست می‌آوریم ((v.۲.۲) را ببینید).

لذا، جوابهای ناهمنهشت به پیمانهٔ m با انتخاب $t_1 \not\equiv t_2(\bmod d)$ به‌دست می‌آیند. در این‌صورت، آشکار است که تمام جوابهای ناهمنهشت بافرض $t = 0, 1, \ldots, d-1$ حاصل می‌شوند.

(۸.۲) نتیجه. اگر $(a,m) = ۱$، به‌ازای هر مقدار b همنهشتی $ax \equiv b(\bmod m)$ جواب یکتا دارد.

در نظریهٔ همنهشتیها جوابهای همنهشتی $ax \equiv ۱(\bmod m)$ به‌ویژه مهم هستند. این مطلب در تعریف زیر آمده است.

(۹.۲) تعریف. اگر a' جوابی از همنهشتی $ax \equiv ۱(\bmod m)$ باشد، a' یک وارون (ضربی) a به پیمانهٔ m خوانده می‌شود.

بنابر (۷.۲)، a دارای وارون ضربی به پیمانهٔ m است اگر و تنها اگر a و m نسبت به هم اول باشند، و وارون a، در صورت وجود، یکتا به پیمانهٔ m است.

توجه کنید که وارون a به پیمانهٔ m خیلی زیاد شبیه وارون معمولی رفتار می‌کند. به‌ویژه، اگر a' وارون a به پیمانهٔ m باشد، آنگاه $x = a'b$ جوابی از $ax \equiv b(\bmod m)$ است. این مطلب قویاً با این حقیقت که در حساب معمولی $b(۱/a)$ جواب معادلهٔ $ax = b$ است شباهت دارد. اویلر و گاوس هر دو نماد $۱/a$ را برای جواب همنهشتی $ax \equiv ۱(\bmod m)$ به‌کار برده‌اند. به دلیل خطر اشتباه شدن با وارون، این نماد دیگر به‌کار نمی‌آید.

تکنیکهای حل $ax \equiv b(\bmod m)$

اکنون به این مسأله می‌پردازیم که اگر همنهشتی خطی $ax \equiv b(\bmod m)$ دارای جواب باشد، جوابها را چگونه به‌دست آوریم. در مسأله‌های این فصل روشهای متعددی به‌کار گرفته شده‌اند، که می‌توان آنها را به اجمال در زیر بیان کرد.

۱. بنابر (۲۴.۱) و اینکه $(a,m)|b$، می‌توان الگوریتم اقلیدسی را برای یافتن اعداد r و s به‌طوری که $ar + ms = b$ به‌کار برد. از این معادله فوراً نتیجه می‌شود که $ar \equiv b(\bmod m)$.

۲. می‌توان به‌جای a یا b (یا هر دو) اعدادی را که با آنها به پیمانهٔ m همنهشت هستند گذاشت و یک همنهشتی به‌دست آورد که بتوان طرفینش را بر عامل مشترکی تقسیم کرد. معمولاً تکرار این روند یک همنهشتی تولید خواهد کرد که حل آن بسیار آسانتر است و جوابش جوابی از همنهشتی اصلی است. اگر پیمانه بسیار بزرگ نباشد این تکنیک بهترین کارایی را دارد.

۳. اگر پیمانه عدد اولی مانند p باشد، می‌توان همنهشتی x را در نزدیکترین عدد صحیح به p/a ضرب کرد تا یک همنهشتی هم‌ارز به‌دست آید. اگر ضریب x را ماندهٔ کوچکترین قدرمطلق، مثلاً a' بگیریم، آنگاه $|a'| < |a|/۲$. با تکرار این روند، جواب درکمتر از n مرحله به‌دست می‌آید، که $n = \log_۲ a$.

به‌طور کلی، می‌توان این روش را برای پیمانهٔ غیر اول به‌کار برد، ولی ممکن است جوابهای

خارجی پیدا شود که باید جداجدا امتحان شوند. ولی، اگر این روش فقط منجر به یک جواب شود، این تنها جواب همنهشتی اصلی است. همچنین، اگر این تکنیک جوابی تولید نکند، همنهشتی اصلی حلپذیر نیست.

توضیح. می‌توان هر یک از این تکنیکها را برای حل معادلهٔ $ax + by = c$ به‌کار برد. ابتدا جوابی مانند r از $ax \equiv c \pmod{b}$ را پیدا می‌کنیم؛ لذا $c - ar$ بر b بخشپذیر است. اگر قرار دهیم $s = (c - ar)/b$، آنگاه $ar + bs = c$.

(۱۰.۲) مثالها. ابتدا الگوریتم اقلیدسی را برای حل همنهشتی $۱۱x \equiv ۲۸ \pmod{۱۹۴۳}$ به‌کار می‌بریم. این الگوریتم نشان می‌دهد که $۱ = (۱۱, ۱۹۴۳)$، و جایگزینی پَسرو نتیجه می‌دهد $۱ = ۳ \times ۱۹۴۳ - ۵۳۰ \times ۱۱$.[۱] با ضرب این رابطه در ۲۸ داریم $۲۸ = ۸۴ \times ۱۹۴۳ - ۱۴۸۴۰ \times ۱۱$، و لذا $۱۱x \equiv ۲۸ \pmod{۱۹۴۳}$ تنها جواب $x \equiv ۱۴۸۴۰ \equiv ۱۲۳۹ \pmod{۱۹۴۳}$ است.

برای توضیح تکنیک دوم، همنهشتی $۱۴۳x \equiv ۴ \pmod{۳۱۵}$ را در نظر می‌گیریم. اگر به‌جای ۴، ۳۱۹ بگذاریم و طرفین معادلهٔ حاصل را بر ۱۱ تقسیم کنیم، داریم $۱۳x \equiv ۲۹ \pmod{۳۱۵}$. چون $-۲۸۶ \equiv ۲۹ \pmod{۳۱۵}$، از تقسیم بر ۱۳ داریم $x \equiv -۲۲ \equiv ۲۹۳ \pmod{۳۱۵}$. (این تنها جواب است، زیرا $۱ = (۱۴۳, ۳۱۵)$.)

بالاخره، با کاربرد تکنیک سوم معادله $۵۱۹x \equiv ۳۱۱ \pmod{۱۹۶۷}$ را حل می‌کنیم. ابتدا طرفین را در نزدیکترین عدد صحیح به $۱۹۶۷/۵۱۹$ یعنی ۴ ضرب می‌کنیم، و پس از ساده کردن به پیمانه ۱۹۶۷ داریم $۱۰۹x \equiv -۷۲۳ \pmod{۱۹۶۷}$. از آنجا که $۱۹۶۷/۱۰۹ = ۱۸٫۰۴۰۰$، اکنون در ۱۸ ضرب می‌کنیم و $-۵x \equiv ۷۵۵ \pmod{۱۹۶۷}$ را به‌دست می‌آوریم. لذا $x \equiv -۱۵۱ \equiv ۱۸۱۶ \pmod{۱۹۶۷}$ جواب یکتای همنهشتی اصلی است.

توضیح. همان‌گونه که در بالا اشاره رفت، هر یک از این تکنیکها را می‌توان برای بیان بزرگترین

---

۱. با توجه به مطلب بعد از (۲۳.۱)، و مانند مسألهٔ ۳.۱ داریم

$۳ \times ۱ = ۱ \times ۳ + ۱,۳ = ۱ \times ۴ + ۳,۴ = ۱ \times ۷ + ۴,۷ = ۱ \times ۱۱ + ۷,۱۱ = ۱ \times ۱۷۶ + ۷ = ۱۹۴۳$ لذا $۱ = (۱۹۴۳, ۱۱)$ و بنابراین داریم

$$\begin{aligned} ۱ &= ۴ - ۳ = ۴ - (۷ - ۴) = ۲ \times ۴ - ۷ = ۲(۱۱ - ۷) - ۷ = ۲ \times ۱۱ - ۳ \times ۷ \\ &= ۲ \times ۱۱ - ۳(۱۹۴۳ - ۱۱ \times ۱۷۶) = ۲ \times ۱۱ - ۳ \times ۱۹۴۳ + ۱۱ \times ۵۳۸ \\ &= ۱۱ \times ۵۳۰ - ۳ \times ۱۹۴۳ \end{aligned}$$

(مترجم).

مقسوم‌علیه مشترک a و m به‌صورت ترکیب خطی از این دو عدد به‌کار برد. مثلاً، به آسانی دیده می‌شود که $(۵۱۹, ۱۹۶۷) = ۱$. اگر تکنیک سوم را برای $۵۱۹x \equiv ۱ (\mathrm{mod}\ ۱۹۶۷)$ به‌کار بریم، به‌ترتیب داریم $۱۰۹x \equiv ۴ (\mathrm{mod}\ ۱۹۶۷)$ و $-۵x \equiv ۷۲ \equiv -۱۸۹۵ (\mathrm{mod}\ ۱۹۶۷)$؛ لذا $x \equiv ۳۷۹ (\mathrm{mod}\ ۱۹۶۷)$ تنها جواب است. در نتیجه به‌ازای اعداد صحیحی مانند s داریم $۱ + ۱۹۶۷s = ۵۱۹ \times ۳۷۹$، و به‌وضوح دیده می‌شود $s = (۵۱۹ \times ۳۷۹ - ۱)/۱۹۶۷ = ۱۰۰$. لذا $(۵۱۹, ۱۹۶۷) = ۱ = ۵۱۹ \times ۳۷۹ - ۱۹۶۷ \times ۱۰۰$.

قضیهٔ باقیماندهٔ چینی

اکنون به مسأله یافتن جواب مشترک یک دستگاه از همنهشتیهای خطی که پیمانه‌هایشان دوبه‌دو نسبت به هم اول هستند می‌پردازیم. هم گاوس و هم ریاضیدان سوئیسی لئونهارت اویلر (۱۷۰۷ـ۱۷۸۳) روشی را که بعداً توضیح می‌دهیم به‌کار بردند، ولی طرح این روش، که به قضیهٔ باقیماندهٔ چینی معروف است، خیلی جلوتر در قرن سوم در نوشته‌های ریاضیدان چینی سون‌تسو ظاهر می‌شود.

(۱۱.۲) قضیهٔ باقیماندهٔ چینی. فرض کنیم $m_۱$، $m_۲$، ...، m_r اعداد صحیح مثبتی باشند که دوبه‌دو نسبت به هم اول‌اند، یعنی اگر $i \neq j$ آنگاه $(m_i, m_j) = ۱$، در این‌صورت، به‌ازای اعداد صحیح دلخواه $a_۱$، $a_۲$، ...، a_r همنهشتیهای

$$x \equiv a_i \pmod{m_i} \qquad (i = ۱, ۲, \ldots, r)$$

یک جواب مشترک دارند، و هر دو جواب به پیمانه $m_۱ m_۲ \ldots m_r$ همنهشت‌اند.

برهان. فرض کنیم $m = m_۱ m_۲ \ldots m_r$؛ در این‌صورت عدد صحیح m/m_i با m_i متباین است ((۹.۱) و (ii.۷.۱) را به‌کار برید). لذا بنابر (۸.۲) اعداد صحیح b_i وجود دارند به‌طوری که $(m/m_i)b_i \equiv ۱ (\mathrm{mod}\, m_i)$؛ آشکار است که به‌ازای $j \neq i$ داریم $(m/m_i)b_i \equiv ۰ (\mathrm{mod}\, m_j)$. قرار می‌دهیم

$$x^* = (m/m_۱)b_۱a_۲ + (m/m_۲)b_۲a_۲ + \cdots + (m/m_r)b_r a_r$$

در این‌صورت به‌ازای هر i، $x^* \equiv (m/m_i)b_i a_i \equiv a_i (\mathrm{mod}\, m_i)$، و لذا x^* یک جواب مشترک همنهشتیهای مفروض است.

اگر x^* و y^* هر دو جوابهای مشترک دستگاه همنهشتیها باشند، آنگاه به‌ازای $i = ۱, ۲, \ldots, r$ داریم $x^* \equiv y^* (\mathrm{mod}\, m_i)$. لذا بنابر (۴.۲) $x^* \equiv y^* (\mathrm{mod}\, m)$؛ به عبارت دیگر، تفاوت هر دو جواب مشترک مضربی است از m.

مثال. قضیهٔ باقیماندهٔ چینی را برای یافتن همهٔ اعداد صحیح مثبت کمتر از ۵۰۰۰ که در تقسیم بر ۹، ۱۰، و ۱۱ به‌ترتیب دارای باقیمانده‌های ۲، ۴، و ۸ هستند به‌کار می‌بریم. لذا باید دستگاه همنهشتیهای $x \equiv ۲ (\mathrm{mod}\, ۹)$، $x \equiv ۴ (\mathrm{mod}\, ۱۰)$، و $x \equiv ۸ (\mathrm{mod}\, ۱۱)$ را حل کنیم. ابتدا $b_۱$، $b_۲$، $b_۳$ را پیدا می‌کنیم به‌طوری که $۱۱۰ b_۱ \equiv ۱ (\mathrm{mod}\, ۹)$، $۹۹ b_۲ \equiv ۱ (\mathrm{mod}\, ۱۰)$، و $۹۰ b_۳ \equiv ۱ (\mathrm{mod}\, ۱۱)$، یا $۲ b_۱ \equiv ۱ (\mathrm{mod}\, ۹)$، $-b_۲ \equiv ۱ (\mathrm{mod}\, ۱۰)$، و $۲ b_۳ \equiv ۱ (\mathrm{mod}\, ۱۱)$. لذا می‌توانیم بگیریم $b_۱ = ۵$، (یا ۹) $b_۲ = -۱$، و $b_۳ = ۶$. بنابراین از برهان (۱۱.۲) نتیجه می‌شود که

$$x^* = ۱۱۰(۵)(۲) + ۹۹(-۱)(۴) + ۹۰(۶)(۸) = ۵۰۲۴$$

یک جواب این دستگاه است. در این مثال $m = ۹ \times ۱۰ \times ۱۱ = ۹۹۰$. از آنجا که $۵۰۲۴ \equiv ۷۴ (\mathrm{mod}\, ۹۹۰)$، تمام جوابهای دستگاه به‌صورت $۹۹۰t + ۷۴$ ارائه می‌شوند، که در آن t عدد صحیح دلخواهی است. لذا تنها جوابهای بین ۱ و ۵۰۰۰ عبارت‌اند از ۷۴، ۱۰۶۴، ۲۰۵۴، ۳۰۴۴، و ۴۰۳۴.

یک کاربرد: یافتنِ روزِ هفته

تقویم یولیانی[1] یا تقویم قیصری، که در سال ۴۶ ق.م. معمول شده بود تا سال ۱۵۸۲ ب. م. در میان ملل غرب به‌کار می‌رفت. در این تقویم، که سال ۳۶۵ شبانه‌روز حساب می‌شد، لازم بود هر چهار سال یک‌شبانه روز به ۳۶۵ افزوده شود اما با این عمل در هر ۱۲۸ سال یک روز می‌بایست بر سال افزوده شود. در ۱۵۸۲، پاپ گرگوری[2] سیزده با حذف ۱۰ روز خطاهای متراکم‌شده تقویم را اصلاح کرد. سالهایی که بر ۴ بخشپذیرند سالهای کبیسه هستند، بجز آن سالهایی که بر ۱۰۰ بخشپذیرند ولی بر ۴۰۰ بخشپذیر نیستند. بیشتر اروپا تقویم گرگوری را فوراً پذیرفتند، اما انگلستان و متصرفاتش، با مستعمرات امریکا، تا ۱۷۵۲ تقویم خود را عوض نکردند. لذا در انگلستان و امریکا تا قبل از ۱۴ سپتامبر ۱۷۵۲، تاریخها با تقویم قیصری حساب می‌شدند؛ برای بیشتر کشورهای دیگر که تقویم قیصری را پذیرفتند، تغییر از روزِ بعد از چهارم اکتبر ۱۵۸۲ صورت گرفت.

(۱۲.۲) روز هفته. می‌توانیم همنهشتیهای به پیمانهٔ ۷ را برای تعیین روز هفته برای یک تاریخ مفروض به‌کار بریم. ترتیبِ رمزنگاری زیر را به‌کار می‌بریم: شنبه = ۰، یکشنبه = ۱، دوشنبه = ۲، ...،

1. Julian 2. Gregory

جمعه = ۶. به رمز ماهها نیز احتیاج داریم؛ برای ژانویه تا دسامبر، این رمزها به‌ترتیب عبارت‌اند از

$$۱۴۴ - ۰۲۵ - ۰۳۶ - ۱۴۶.$$

(برای سهولت، رمزها درگروههای سه‌تایی ارائه شده‌اند؛ توجه کنید که اتفاقاً سه گروه اول مربع کامل‌اند، و آخرین گروه شباهت نزدیکی با اولی دارد.) برای شروع، فرض می‌کنیم که تاریخ ما سدهٔ بیستم، مثلاً ۱۹ مه ۱۹۴۵ باشد. خارج‌قسمت تقسیم دو رقم آخرِ مربوط به سال، یعنی ۴۵ را بر ۴ پیدا می‌کنیم؛ در اینجا ۱۱ به‌دست می‌آید، که همنهشت با ۴ به پیمانهٔ ۷ است. ۴۵ را با ۴ جمع نموده و به پیمانهٔ ۷ تحویل می‌کنیم، ۰ به‌دست می‌آید. اکنون ۰ را با روز مربوط به ماه، ۱۹، و رمز ماه مه، که ۲ است، جمع می‌کنیم، ۰ به پیمانهٔ ۷ حاصل می‌شود. لذا نوزدهم مه ۱۹۴۵ روز شنبهٔ ما می‌شود.

برای تاریخهای واقع در ژانویه یا فوریه در یک سال کبیسه (یعنی، سالِ بعد از ۱۹۰۰ که دو رقم آخرش بر ۴ بخشپذیر است)، بایستی در محاسباتمان ۱ واحد کم کنیم.

توجیه الگوریتم مشکل نیست. برای گذر از یک سال به سال بعد، روز هفته برای یک تاریخ مفروض یکی به جلو می‌رود، مگر از روز کبیسه یعنی ۲۹ فوریه عبور کنیم، که در این حالت دو روز به جلو می‌رود. (این مطلب از این واقعیت که $۳۶۵ \equiv ۱ \pmod ۷$ و $۳۶۶ \equiv ۲ \pmod ۷$ نتیجه می‌شود.) مثلاً، در مقایسه با روز هفته برای ۱۹ مه ۱۹۰۰، ۱۹ مه ۱۹۴۵ به تعداد ۴۵ روز بعلاوه یک ۱۱ روز دیگر به دلیل دخالت ۱۱ سال کبیسه، به جلو رفته است. (به آسانی دیده می‌شود که تعداد سالهای کبیسه در اینجا خارج‌قسمت تقسیم ۴۵ بر ۴، یعنی، ۱۱ است).

بنابراین، کافی است که با تاریخهای واقع در ۱۹۰۰ کار کنیم، سپس مانند بالا برای هر سال دیگر تنظیم کنیم. (ملاحظه می‌کنید که ۱۹۰۰ سال کبیسه نبود) اولِ ژانویهٔ ۱۹۰۰ را که بر دوشنبه منطبق است، روز مبدأ می‌گیریم. اگر روش قبل را برای ۱۹۰۰ به‌کار بریم، ۰ بعلاوهٔ خارج‌قسمت ۰ بر ۴، یعنی ۰ حاصل می‌شود، به این عدد تاریخ، ۱، و رمز ماه برای ژانویه، که آن را x می‌نامیم، اضافه می‌کنیم و مجموع $x + ۱$ را به‌دست می‌آوریم. چون رمز دوشنبه ۲ است، بایستی داشته باشیم $x + ۱ = ۲$، یعنی $x = ۱$، رمزهای سایر ماهها به طریق زیر مشخص می‌شوند. درگذر از یک تاریخ در ژانویه ــ مثلاً، نوزدهم ــ به همان تاریخ در فوریه، ۳۱ روز فاصله افتاده است؛ چون $۳۱ \equiv ۳ \pmod ۷$، آشکار است که ۱۹ فوریه در هفته سه روز دیرتر از نوزدهم ژانویه است، لذا رمز ماه برای فوریه بایستی سه روز بیشتر از رمز ماه برای ژانویه، یعنی ۴ باشد. اگر به همین روند ادامه دهیم تمام رمزهای ماههای ارائه‌شده در بالا را به‌دست می‌آوریم.

سرانجام، اشاره می‌کنیم که می‌توانیم این الگوریتم را برای سایر قرنها، گذشته یا آینده، به‌کار بریم. برای تاریخهای واقع در سدهٔ بیست‌ویکم، یک واحد کم می‌کنیم؛ برای تاریخهای (گرگوری) واقع

در سدهٔ نوزدهم ۲ واحد جمع می‌کنیم؛ در سدهٔ هجدهم، ۴ اضافه می‌کنیم؛ در سدهٔ هفدهم، ۶ اضافه می‌کنیم؛ و در سدهٔ شانزدهم، از ۱۵ اکتبر ۱۵۸۲ تا ۳۱ دسامبر ۱۵۹۹، ۰ اضافه می‌کنیم. تنها احتیاط آن است که مطمئن باشید تاریخ مفروض برای تقویم گرگوری است؛ در غیر این‌صورت روش ما نتیجهٔ نادرست به‌دست می‌دهد.

برای محاسبهٔ روز هفته برای یک تاریخ در تقویم یولیایی، تصحیحِ ۱۸ منهای دو رقم اول سال را به‌کار می‌بریم (فرض می‌کنیم که هر سال با چهار رقم نوشته شده است). مثلاً یک تاریخ در سدهٔ شانزدهم به تصحیح $۳ = ۱۵ - ۱۸$ نیاز دارد، در حالی‌که یک تاریخ در سدهٔ نهم به تصحیح $۱۰ = ۸ - ۱۸$، یا ۳ به پیمانهٔ ۷، احتیاج دارد.

برای مثالهایی که این الگوریتم به‌کار می‌رود، مسأله‌های ۴۹.۲ تا ۵۵.۲ را ببینید.

مسأله‌ها و راه‌حلها

توضیح. اگر بخواهید با استفاده از ماشین‌حساب باقیماندهٔ تقسیم a بر m را به‌دست آورید، ابتدا a را بر m تقسیم کنید و سپس جزء صحیح نتیجه را از آن کم کنید تا عدد اعشاری کمتر از ۱ به‌دست آید. اکنون این عدد را در m ضرب کنید. نتیجه همان باقیمانده تقسیم a بر m است. البته، پاسخ باید یک عدد صحیح نامنفی باشد، زیرا نشانگر باقیمانده است، ولی به دلیل عمل گِرد کردن در ماشین‌حساب، مثلاً ممکن است اعداد ۴۷٫۹۹۹۹۹۹۹ یا ۴۸٫۰۰۰۰۰۰۱ را به‌جای ۴۸ به‌دست آورید.

همنهشتیهای عمومی

۱.۲ باقیماندهٔ تقسیم $۱۷^{۱۷}$ را بر ۷ به‌دست آورید

حل. $۱۷ \equiv ۳ \pmod ۷$، لذا بنابر (۳.۲)، $۱۷^{۱۷} \equiv ۳^{۱۷} \pmod ۷$. برای یافتن $۳^{۱۷}$ به پیمانهٔ ۷ داریم $۹ \equiv ۲ \pmod ۷$، $۳^{۲} \equiv$، لذا $۴ \pmod ۷ \equiv (۳^{۲})^{۲} \equiv ۳^{۴}$. از این‌رو $۳^{۱۷} \equiv ۳ \times ۳^{۱۶} \equiv ۱۲ \equiv ۵ \pmod ۷$، و سرانجام $۳^{۱۶} \equiv ۴ \pmod ۷$، $۳^{۸} \equiv ۱۶ \equiv ۲ \pmod ۷$ بنابراین، باقیماندهٔ $۱۷^{۱۷}$ بر ۷ برابر ۵ است.

۲.۲ باقیماندهٔ تقسیم $۴^{۳۰}$ بر ۲۳ را به‌دست آورید.

حل. چون $۴۳ = ۶۴ \equiv -۵ \pmod{۲۳}$، داریم $۴^{۳۰} \equiv (-۵)^{۲} \equiv ۲ \pmod{۲۳}$. بنابراین $۴^{۳۰} \equiv ۲^{۵} \equiv ۹ \pmod{۲۳}$. لذا باقیماندهٔ برابر ۹ است.

۳.۲ نشان دهید که $۲^{۳۷} - ۱$ مضربی از ۲۲۳ است.

حل. چون $۲^۸ \equiv ۳۳ (\mathrm{mod}\ ۲۲۳)$، داریم $۲^{۱۶} \equiv (۳۳)^۲ \equiv -۲۶ (\mathrm{mod}\ ۲۲۳)$؛ لذا $۲^{۳۲} \equiv (-۲۶)^۲ \equiv ۷ (\mathrm{mod}\ ۲۲۳)$. بنابراین

$$۲^{۳۷} \equiv ۲^{۳۲} \times ۲^۵ \equiv ۷ \times ۳۲ \equiv ۱ (\mathrm{mod}\ ۲۲۳)$$

۴.۲ مطلوب است کوچکترین ماندهٔ مثبت (الف) $۳^{۵۰۰}$ به پیمانه ۱۳؛ (ب) !۱۲ به پیمانهٔ ۱۳؛ (ج) $۵^{۱۶}$ به پیمانهٔ ۱۷؛ (د) $۵^{۵۰۰}$ به پیمانهٔ ۱۷.

حل. (الف) چون $۳^۳ \equiv ۱ (\mathrm{mod}\ ۱۳)$، داریم $(۳^۳)^{۱۶۶} \equiv ۱ (\mathrm{mod}\ ۱۳)$. لذا $۳^{۴۹۸} \equiv ۹ (\mathrm{mod}\ ۱۳)$
$۳^{۵۰۰} \equiv ۳^{۴۹۸} \times ۳^۲ \equiv ۱ \times ۹ \equiv ۹ (\mathrm{mod}\ ۱۳)$

(ب)

$$۱۲! = (۲ \times ۳ \times ۴)(۵ \times ۶)(۷ \times ۸)(۹ \times ۱۰)(۱۱ \times ۱۲)$$
$$\equiv (-۲)(۴)(۴)(-۱)(۲) \equiv ۱۲ (\mathrm{mod}\ ۱۳)$$

(ج) $۵^۲ \equiv ۸ (\mathrm{mod}\ ۱۷)$ ایجاب می‌کند $۵^۴ \equiv ۸^۲ \equiv -۴ (\mathrm{mod}\ ۱۷)$. لذا $۵^۸ \equiv ۱۶ \equiv -۱ (\mathrm{mod}\ ۱۷)$ و بنابراین $۵^{۱۶} \equiv ۱ (\mathrm{mod}\ ۱۷)$.

(د) بنابر (ج)، $۵^{۱۶} \equiv ۱ (\mathrm{mod}\ ۱۷)$، لذا $۵^{۴۹۶} = (۵^{۱۶})^{۳۱} \equiv ۱^{۳۱} (\mathrm{mod}\ ۱۷)$. از این‌رو $۵^{۵۰۰} = ۵^{۴۹۶} \times ۵^۴ \equiv ۱ \times ۵^۴ \equiv ۱۳ (\mathrm{mod}\ ۱۷)$.

۵.۲ باقیماندهٔ تقسیم $۳^{۴۰}$ و $۴۳^{۳۷}$ را بر ۱۱ به‌دست آورید.

حل. چون $۳^۲ \equiv -۲ (\mathrm{mod}\ ۱۱)$، داریم $۳^۴ \equiv ۴ (\mathrm{mod}\ ۱۱)$ و لذا $۳^۸ \equiv ۵ (\mathrm{mod}\ ۱۱)$، و از این رابطه $۳^{۱۶} \equiv ۳ (\mathrm{mod}\ ۱۱)$، سپس $۳^{۳۲} \equiv -۲ (\mathrm{mod}\ ۱۱)$، و لذا $۳^{۴۰} = ۳^{۳۲} \times ۳^۸ \equiv (-۲)(۵) \equiv ۱ (\mathrm{mod}\ ۱۱)$. همچنین، چون $۴۳ \equiv -۱ (\mathrm{mod}\ ۱۱)$، داریم $(۴۳)^{۳۷} \equiv (-۱)^{۳۷} \equiv -۱ \equiv ۱۰ (\mathrm{mod}\ ۱۱)$. بنابراین، باقیمانده‌های تقسیم $۳^{۴۰}$ و $(۴۳)^{۳۷}$ بر ۱۱ به ترتیب برابر ۱ و ۱۰ است.

۶.۲ نشان دهید که $۲^{۴۸} - ۱$ بر ۹۷ قابل‌قسمت است.

حل. $۲^۸ \equiv ۶۲ \equiv -۳۵ (\mathrm{mod}\ ۹۷)$ ایجاب می‌کند که

$$۲^{۱۶} \equiv (-۳۵)^۲ \equiv ۶۱ \equiv -۳۶ (\mathrm{mod}\ ۹۷)$$

بنابراین $۲^{۳۲} \equiv (-۳۶)^۲ \equiv ۳۵ (\mathrm{mod}\ ۹۷)$، و لذا

$$۲^{۴۸} = ۲^{۳۲} \times ۲^{۱۶} \equiv ۳۵(-۳۶) \equiv -۹۶ \equiv ۱ (\mathrm{mod}\ ۹۷)$$

پس ۹۷ عدد $۲^{۴۸} - ۱$ را می‌شمارد.

۷.۲ نشان دهید که ۴۷ عدد $۵^{۲۳} + ۱$ را می‌شمارد.

حل. چون $۵^۴ \equiv ۱۴ (\mathrm{mod}\ ۴۷)$، نتیجه می‌شود که $۵^۸ \equiv ۸ (\mathrm{mod}\ ۴۷)$ و $۵^{۱۶} \equiv ۱۷ (\mathrm{mod}\ ۴۷)$. بنابراین $۵^{۲۴} = ۵^{۱۶} \times ۵^۸ \equiv ۱۷ \times ۸ \equiv -۵$، و لذا $۵^{۲۴} + ۵$ بر ۴۷ بخشپذیر است. چون $۵(۵^{۲۳} + ۱) = ۵^{۲۴} + ۵$ و $(۵, ۴۷) = ۱$، نتیجه می‌گیریم که ۴۷ عدد $۵^{۲۳} + ۱$ را می‌شمارد.

۸.۲ آیا ۴۱ عدد $۳^{۲۰} \times ۷ + ۶$ را می‌شمارد؟

حل. از $۳^۴ \equiv -۱ (\mathrm{mod}\ ۴۱)$ نتیجه می‌شود که $۳^{۲۰} \equiv (-۱)^۵ \equiv -۱ (\mathrm{mod}\ ۴۱)$. از این‌رو $۳^{۲۰} \times ۷ + ۶ \equiv ۷(-۱) + ۶ \equiv -۱ (\mathrm{mod}\ ۴۱)$. لذا ۴۱ عدد $۳^{۲۰} \times ۷ + ۶$ را نمی‌شمارد. (در واقع، باقیماندهٔ $۳^{۲۰} \times ۷ + ۶$ بر ۴۱ برابر ۴۰ است.)

۹.۲ اگر k فرد باشد ثابت کنید $۱۳^{۲k} + ۱۷^{۲k}$ بر ۲۲۹ بخشپذیر است. اگر k زوج باشد چطور؟

حل. اگر $n = ۱۳^{۲k} + ۱۷^{۲k} = (۱۶۹)^k + (۲۸۹)^k$، آنگاه

$$n \equiv (-۶۰)^k + (۶۰)^k (\mathrm{mod}\ ۲۲۹)$$

لذا اگر k فرد باشد، $n \equiv ۰ (\mathrm{mod}\ ۲۲۹)$. این نتیجه برای هر k زوج برقرار نیست، زیرا در این‌صورت خواهیم داشت $n \equiv ۲ \times ۶۰^k (\mathrm{mod}\ ۲۲۹)$، و به وضوح ۲۲۹ عدد n را نمی‌شمارد. (زیرا در غیر این‌صورت $۲۲۹ | ۶۰^k$ و چون ۲۲۹ اول است پس $۲۲۹ | ۶۰$ که ممکن نیست.)

۱۰.۲ کوچکترین ماندهٔ نامنفی $۱! + ۲! + ۳! + \cdots + ۱۰۰!$ به پیمانهٔ ۴۵ را به‌دست آورید.

حل. اگر $n \geq ۶$، آنگاه چون $۴۵ | ۶!$ پس $۴۵ | n!$. لذا

$$۱! + ۲! + \cdots + ۱۰۰! \equiv ۱ + ۲! + \cdots + ۵! \equiv ۱۸ (\mathrm{mod}\ ۴۵)$$

۱۱.۲ اگر $p \geq 5$ اول باشد، ثابت کنید $p^2 + 2$ عدد مرکب است.

حل. اگر $p > 3$ اول باشد، آنگاه $p \equiv \pm 1 \pmod 3$، و لذا $p^2 + 2 \equiv 0 \pmod 3$. چون $p^2 + 2$ مضربی از ۳ و بزرگتر از ۳ است نمی‌تواند اول باشد.

۱۲.۲ ثابت کنید به‌ازای هر عدد صحیح مثبت n، $2^{2^n} + 5$ عدد مرکب است.

حل. فرض کنیم $N = 2^{2^n} + 5$؛ در این‌صورت به‌ازای $n = 1$ داریم $N = 9$ و $n = 2$ ایجاب می‌کند $N = 21$. لذا حدس می‌زنیم که N مضربی از ۳ باشد. برای اثبات، توجه می‌کنیم که $2 \equiv -1 \pmod 3$ و چون 2^n زوج است پس $2^{2^n} \equiv 1 \pmod 3$ و لذا $2^{2^n} + 5 \equiv 6 \equiv 0 \pmod 3$.

۱۳.۲ فرض کنید p_i معرف عدد اول iام باشد. نشان دهید که $p_1 p_2 \cdots p_n + 1$ هرگز توان دوم عددی نیست. (راهنمایی: نشان دهید که این مجموع به‌صورت $4k + 3$ است.)

حل. حاصلضرب $p_1 p_2 \cdots p_n$ دو برابر یک عدد فرد است، لذا همنهشت ۲ به پیمانهٔ ۴ است. بنابراین $p_1 p_2 \cdots p_n + 1 \equiv 3 \pmod 4$ و نمی‌تواند مربع باشد، زیرا تمام مربعها همنهشت ۰ یا ۱ به پیمانهٔ ۴ هستند. (حتی نمی‌تواند مجموع دو مربع باشد.)

۱۴.۲ فرض کنید q_1، ...، q_n اعداد اول فرد باشند. آیا $N = (q_1 q_2 \ldots q_n)^2 + 1$ می‌تواند مکعب کامل باشد؟

حل. هر عدد اول فرد به یکی از دو صورت $4k+1$ یا $4k+3$ است، لذا $q_i \equiv \pm 1 \pmod 4$؛ در نتیجه $N \equiv 2 \pmod 4$. لذا 2^1 بزرگترین توانی از ۲ است که N را می‌شمارد، و بنابراین به‌ازای هر $k > 1$، N نمی‌تواند توان kام کامل باشد.

۱۵.۲ ثابت کنید که هر عدد صحیح x لااقل در یکی از همنهشتیهای زیر صدق می‌کند: $x \equiv 0 \pmod 2$، $x \equiv 0 \pmod 3$، $x \equiv 1 \pmod 4$، $x \equiv 3 \pmod 8$، $x \equiv 7 \pmod{12}$، و $x \equiv 23 \pmod{24}$.

حل. هر پیمانه مذکور در فوق ۲۴ را می‌شمارد، لذا کافی است برای $0 \leq x \leq 23$، نشان دهیم که x لااقل در یکی از همنهشتیها صدق می‌کند. همهٔ xها بجز ۷و ۱۱، ۱۹، و ۲۳ در سه همنهشتی اول صدق می‌کنند. ۱۱ و ۱۹ در همنهشتی چهارم صدق می‌کنند، ۷ در پنجم صدق می‌کند و ۲۳ در آخری.

توضیح. فرض کنید $m_1 < m_2 < \cdots < m_k$، و دستگاه همنهشتیهای $x \equiv a_i \pmod{m_i}$ $(i = 1, 2, \ldots, k)$ را در نظر می‌گیریم. اگر عدد صحیحی مانند x لااقل در یکی از همنهشتیهای دستگاه صدق کند، دستگاه یک دستگاه پوششی نامیده می‌شود. پل اردش[1] جایزهٔ قابل‌توجهی برای اثبات اینکه دستگاههای پوششی با m_1 به اندازهٔ کافی بزرگ وجود دارند پیشنهاد کرده است (و جایزهٔ کوچکتری برای اثبات درست نبودن این مطلب).

۱۶.۲ ثابت کنید که $1 + 2 + \cdots + n$ بر n بخشپذیر است وقتی که n فرد باشد و بر $n + 1$ قابل‌قسمت است هرگاه n زوج باشد.

حل. ابتدا فرض می‌کنیم n فرد باشد. مجموع با $1 + 2 + \cdots + (n - 1)$ همنهشت به پیمانهٔ n است. توجه کنید که مجموع جمله‌های اول و آخر، همین‌طور مجموع جمله‌های دوم و یکی به آخر مانده، و مانند آن برابر n است. تعداد $n - 1/2$ این چنین جفت که مجموعشان n است وجود دارند، و لذا مجموع همنهشت با ۰ به پیمانهٔ n است. اگر n زوج باشد، استدلال بالا را برای عدد صحیح فرد $n + 1$ به‌کار برید تا نتیجه بگیرید که $n + 1$ مجموع $1 + 2 + \cdots + n$ را می‌شمارد.

۱۷.۲ نشان دهید که حاصلضرب سه عدد صحیح متوالی مضربی از ۶ است.

حل. فرض کنیم $N = (n - 1)n(n + 1)$ حاصلضرب سه عدد صحیح متوالی باشد. حداقل یکی از این سه عدد زوج است، پس $2|N$. چون (دقیقاً) یکی از این سه عدد مضرب ۳ است پس $3|N$. (برای اثبات این مطلب سه حالت $n \equiv 0, 1, 2 \pmod 3$ را در نظر بگیرید.) چون ۲ و ۳ نسبت به‌هم اول‌اند بنابر قضیهٔ (۱۰.۱) $6 = 3 \times 2$ عدد N را می‌شمارد.

۱۸.۲ ثابت کنید که مجموع هر سه عدد مکعب متوالی مضربی از ۹ است.

حل. فرض کنیم $N = (n-1)^3 + n^3 + (n+1)^3$؛ روشن است $N = 3n^3 + 6n = 3n(n^2 + 2)$. سه حالت اتفاق می‌افتد. اگر $n \equiv 0 \pmod 3$، آنگاه N دو عامل ۳ دارد و لذا $9|N$. اگر $n \equiv \pm 1 \pmod 3$، آنگاه $n^2 + 2 \equiv (\pm 1)^2 + 2 \equiv 0 \pmod 3$، و مجدداً N دو عامل ۳ دارد.

۱۹.۲ نشان دهید که هیچ عدد صحیح به‌صورت $4k + 3$ مجموع دو مربع نیست.

حل. هر عدد صحیح همنهشت با ۰، ۱، ۲، یا ۳ به پیمانهٔ ۴ است، و لذا مربع هر عدد صحیح همنهشت با 0^2، 1^2، 2^2، یا 3^2، یعنی با ۰ یا ۱ به پیمانهٔ ۴ است. بنابراین مجموع دو مربع

1. Paul Erdös

همنهشت با ۰، ۱، یا ۲ به پیمانهٔ ۴ است. در حالی‌که روشن است که هر عدد صحیح به‌صورت $4k+3$ همنهشت ۳ به پیمانهٔ ۴ است.

◁ **۲۰.۲** ثابت کنید که هیچ عدد صحیح به‌صورت $8k+7$ مجموع سه مربع نیست. با استفاده از این مطلب نشان دهید هیچ عدد صحیح به‌صورت $4^m(8k+7)$ مجموع سه مربع نیست.

حل. هر عدد صحیح همنهشت با ۰، ± 1، ± 2، ± 3، یا ۴ به پیمانهٔ ۸ است، زیرا گردایهٔ $\{-3,-2,-1,0,1,2,3,4\}$ یک دستگاه کامل مانده‌ها به پیمانهٔ ۸ است. لذا مربع هر عدد همنهشت با مربع یکی از اعداد بالا، یعنی ۰، ۱، یا ۴ به پیمانهٔ ۸ است. مجموع هر ترکیب سه‌تایی انتخابی از اعداد ۰، ۱، یا ۴ ناهمنهشت با ۷ پیمانهٔ ۸ است، و لذا هیچ عدد صحیح به‌صورت $8k+7$ مجموع سه مربع نیست.

فرض می‌کنیم عدد $m \geq 1$ وجود داشته باشد به‌طوری که $N = 4^m(8k+7) = x^2+y^2+z^2$. چون $N \equiv 0 \pmod 4$ و چون هر مربع همنهشت با ۰ یا ۱ به پیمانهٔ ۴ است، نتیجه می‌شود که هرکدام از x^2، y^2، و z^2 همنهشت با ۰ به پیمانهٔ ۴ هستند، و لذا x، y، و z زوج هستند. اگر $x=2r$، $y=2s$، $z=2t$، آنگاه $N/4 = r^2+s^2+t^2$. تکرار این روند سرانجام نشان می‌دهد که $8k+7$ مجموع سه مربع است، که با استدلال قسمت اول تناقض دارد.

۲۱.۲ با استفاده از همنهشتیها نشان دهید که معادلهٔ $x^2 - 2y^2 = 10$ جواب صحیح ندارد.

حل. از پیمانهٔ ۵ استفاده می‌کنیم. اگر $u \not\equiv 0 \pmod 5$، به آسانی معلوم می‌شود که $u^2 \equiv \pm 1 \pmod 5$، اگر هیچ کدام از x و y بخشپذیر بر ۵ نباشند، بررسی حالتهای مختلف نشان می‌دهد که $x^2 - 2y^2 \not\equiv 0 \pmod 5$. لذا اگر $x^2 - 2y^2 \equiv 0 \pmod 5$، آنگاه لااقل یکی از x و y بر ۵ بخشپذیر است. در نتیجه x و y هر دو بر ۵ بخشپذیرند، و لذا $x^2 - 2y^2$ بر ۲۵ بخشپذیر است. به‌ویژه نمی‌توانیم داشته باشیم $x^2 - 2y^2 = 10$.

۲۲.۲ ثابت کنید که به‌ازای هر n عدد $N = n^3 + 11n + 1$ بر اولین ۴ عدد اول بخشپذیر نیست.

حل. چون $n \equiv 0 \pmod 2$ یا $n \equiv 1 \pmod 2$، $n^3 \equiv 0$ یا $1 \pmod 2$ و لذا در هر حالت $N \equiv 1 \pmod 2$، یعنی $2 \not| N$. به طریق تشابه، از $n \equiv 0, 1 \pmod 3$ نتیجه می‌شود $n^3 \equiv 0, 1 \pmod 3$ و در هر حال $N \equiv 1 \pmod 3$، لذا $3 \not| N$. اگر $n \equiv 0, \pm 1, \pm 2 \pmod 5$، آنگاه $n^3 \equiv 0, \pm 1, \pm 2 \pmod 5$؛ لذا $N \equiv \pm 1, -2 \pmod 5$،

یعنی $5 \nmid N$. سرانجام $n \equiv 0, \pm 1, \pm 2, \pm 3 \pmod 7$ ایجاب می‌کند $n^3 \equiv 0, \pm 1 \pmod 7$؛ لذا $N \equiv \pm 1, -2, \pm 3 \pmod 7$ و بنابراین $7 \nmid N$.

۲۳.۲ با استفاده از $5 \times 2^7 = 640$ ثابت کنید که عدد فرمای $1 + 2^{32}$ بر ۶۴۱ بخشپذیر است.

حل. چون $5 \times 2^7 \equiv -1 \pmod{641}$، داریم $5^4 \times 2^{28} \equiv 1 \pmod{641}$. از طرفی $5^4 = 625 \equiv -16 \pmod{641}$، لذا $5^4 \times 2^{28} \equiv 1 \pmod{641}$ یا $-2^4 \times 2^{28} \equiv -1 \pmod{641}$، $2^{32} \equiv -1 \pmod{641}$، یعنی $1 + 2^{32}$ بر ۶۴۱ بخشپذیر است.

۲۴.۲ نشان دهید که مجموع ارقام یک عدد مربع (در دستگاه اعشاری) با ۰، ۱، ۴، یا ۷ به پیمانهٔ ۹ همنهشت است.

حل. ابتدا ملاحظه می‌کنیم که n هر عددی باشد مجموع ارقام n همنهشت با n به پیمانهٔ ۹ است. لذا اگر a^2 یک عدد مربع باشد، کافی است باقیماندهٔ a^2 به پیمانهٔ ۹ را حساب کنیم. داریم $a \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4 \pmod 9$، لذا $a^2 \equiv 0, 1, 4, 9, 16 \equiv 0, 1, 4, 7 \pmod 9$.

۲۵.۲ ثابت کنید که به‌ازای هر عدد صحیح مثبت n عدد $n(n-1)(2n-1)$ بر ۶ بخشپذیر است.

حل. یک راه حل «ترکیبیاتی» ساده یادآوری رابطهٔ

$$1^2 + 2^2 + \cdots + (n-1)^2 = (n)(n-1)(2n-1)/6$$

است. راه حل ساده دیگر استفاده از استدلال همنهشتی است. آشکار است که $n(n-1)$ بر ۲ بخشپذیر است. برای اینکه نشان دهیم $n(n-1)(2n-1)$ بر ۳ بخشپذیر است یا می‌توان حالتهای $n \equiv 0, 1, -1 \pmod 3$ را جداگانه در نظر گرفت، و یا چون $2 \equiv -1 \pmod 3$ پس $2n - 1 \equiv -(n+1) \pmod 3$ و لذا $n(n-1)(2n-1) \equiv -(n-1)n(n+1) \pmod 3$، و اینکه دقیقاً یکی از ۳ عدد صحیح متوالی بر ۳ بخشپذیر است.

همچنین می‌توانیم مسأله را به استقرا اثبات کنیم. فرض کنیم $f(n) = n(n-1)(2n-1)$. چون $f(1) = 0$، $f(1)$ مضربی از ۶ است. حال نشان می‌دهیم که به‌ازای هر عدد صحیح k، اگر $f(k)$ بر ۶ بخشپذیر باشد، آنگاه $f(k+1)$ بر ۶ بخشپذیر است. $f(k+1) - f(k)$ را در نظر می‌گیریم. یک محاسبهٔ ساده نشان می‌دهد که این تفاضل برابر $6k^2$ است. لذا چون $f(k+1) = f(k) + 6k^2$، اگر $f(k)$ بر ۶ بخشپذیر باشد $f(k+1)$ نیز بر ۶ بخشپذیر است.

همنهشتیهای خطی

۲۶.۲ معادلهٔ $۴۲x \equiv ۹۰ (\mathrm{mod}\ ۱۵۶)$ را حل کنید.

حل. از (۷.۲) استفاده می‌کنیم. چون $d = (۴۲, ۱۵۶) = ۶$ و $۶|۹۰$، پس معادلهٔ ۶ جواب ناهمنهشت به پیمانهٔ ۱۵۶ دارد. همنهشتی را به $۷x \equiv ۱۵ (\mathrm{mod}\ ۲۶)$ بدل می‌کنیم. این همنهشتی جواب یکتای $x \equiv -۹ (\mathrm{mod}\ ۲۶)$ دارد. لذا بنابر ۷.۲، همهٔ جوابهای همنهشتی اصلی عبارت‌اند از

$$x \equiv -۹ + \frac{۱۵۶}{۶} t \equiv -۹ + ۲۶t (\mathrm{mod}\ ۱۵۶) \qquad t = -۲, -۱, ۰, ۱, ۲, ۳$$

یا

$$x \equiv -۶۱, -۳۵, -۹, ۱۷, ۴۳, ۶۹ (\mathrm{mod}\ ۱۵۶)$$

یا

$$x \equiv ۱۷, ۴۳, ۶۹, ۹۵, ۱۲۱, ۱۴۷ (\mathrm{mod}\ ۱۵۶)$$

۲۷.۲ همهٔ جوابهای $۸۷x \equiv ۵۷ (\mathrm{mod}\ ۱۰۵)$ را به‌دست آورید.

حل. چون $۳ = (۸۷, ۱۰۵)$ و $۳|۵۷$، همنهشتی سه جواب دارد. همنهشتی را به $۲۹x \equiv ۱۹ (\mathrm{mod}\ ۳۵)$ تبدیل می‌کنیم. جواب یکتای این همنهشتی عبارت است از $x \equiv -۹ (\mathrm{mod}\ ۳۵)$. لذا بنابر (۷.۲) تمام جوابهای همنهشتی اصلی عبارت‌اند از

$$x \equiv -۹ + ۳۵t (\mathrm{mod}\ ۱۰۵) \qquad t = -۱, ۰, ۱$$

یا $x \equiv -۴۴, -۹, ۲۶ (\mathrm{mod}\ ۱۰۵)$. یا $x \equiv ۲۶, ۶۱, ۹۶ (\mathrm{mod}\ ۱۰۵)$.

۲۸.۲ تمام جوابهای $۶۴x \equiv ۸۹۷ (\mathrm{mod}\ ۱۰۰۱)$ را به‌دست آورید.

حل. چون $۸۹۷ \equiv -۱۰۴ (\mathrm{mod}\ ۱۰۰۱)$ پس همنهشتی فوق هم‌ارز است با $۶۴x \equiv -۱۰۴ (\mathrm{mod}\ ۱۰۰۱)$ (۱)، و چون $۱ = (۸, ۱۰۰۱)$ پس (۱) نیز هم‌ارز است با $۸x \equiv -۱۳ (\mathrm{mod}\ ۱۰۰۱)$ (۲). جواب یکتای این همنهشتی (و لذا همنهشتی اصلی) عبارت است از $x \equiv -۳۷۷ (\mathrm{mod}\ ۱۰۰۱)$، و یا (چون ۱۳ و ۱۰۰۱ فرد هستند، می‌توانیم همنهشتی (۲) را به روش زیر حل کنیم، داریم $۹۸۸ \equiv -۱۳ (\mathrm{mod}\ ۱۰۰۱)$ پس (۲) هم‌ارز است با $۹۸۸ \equiv ۸x (\mathrm{mod}\ ۱۰۰۱)$ و این نیز هم‌ارز است با $۲x \equiv ۲۴۷ (\mathrm{mod}\ ۱۰۰۱)$، مجدداً $-۷۵۴ \equiv ۲x (\mathrm{mod}\ ۱۰۰۱)$ و این هم‌ارز است با $x \equiv -۳۷۷ (\mathrm{mod}\ ۱۰۰۱)$. (این روش در حل همنهشتی $ax \equiv b (\mathrm{mod}\ m)$، هر وقت که a توانی از ۲ باشد، کارایی دارد).

۲۹.۲ از اندیشه به‌کار رفته در مسألهٔ قبل برای حل $x \equiv ۱ (\mathrm{mod}\ ۸۱۸۰)$ $۳^۶ x \equiv ۱ (\mathrm{mod}\ ۸۱۸۰)$ پیروی کنید.

حل. چون $۸۱۸۱ \equiv ۱ (\mathrm{mod}\ ۸۱۸۰)$، با جایگزینی ۸۱۸۱ به‌جای ۱ و تقسیم طرفین همنهشتی بر $۳^۴$ همنهشتی $۳^۲ x \equiv ۱۰۱ (\mathrm{mod}\ ۸۱۸۰)$ را که با همنهشتی اصلی هم‌ارز است به‌دست می‌آوریم. اکنون $۸۱۸۰ \times ۲ + ۱۰۱ \equiv ۱۰۱ (\mathrm{mod}\ ۸۱۸۰)$. لذا همنهشتی آخر هم‌ارز است با $۳^۲ x \equiv ۱۶۴۶۱ (\mathrm{mod}\ ۸۱۸۰)$ و از آنجا $x \equiv ۱۸۲۹ (\mathrm{mod}\ ۸۱۸۰)$ جواب همنهشتی است.

۳۰.۲ اعداد صحیح مثبت کمتر از ۱۵ به پیمانهٔ ۱۵ را که وارون دارند تعیین کرده و وارون آنها را به‌دست آورد.

حل. بنابه تعریف، a به پیمانهٔ ۱۵ وارون دارد اگر و تنها اگر همنهشتی $ax = ۱ (\mathrm{mod}\ ۱۵)$ حلپذیر باشد. در نتیجه بنابر (۷.۲)، اگر و تنها اگر $|۱| = (a, ۱۵)$، و لذا اگر و تنها اگر $۱ = (a, ۱۵)$، یعنی a, ۱۵ نسبت به هم اول باشند بنابراین a یکی از اعداد ۱، ۲، ۴، ۷، ۸، ۱۱، ۱۳، یا ۱۴ است. به پیمانهٔ ۱۵ داریم $۱ \equiv ۱، ۱ \equiv ۸ \times ۲، ۱ \equiv ۴ \times ۴، ۱ \equiv ۱۳ \times ۷، ۱ \equiv ۱۱ \times ۱۱$، و $۱ \equiv ۱۴ \times ۱۴$. لذا ۱، ۴، ۱۱، و ۱۴ وارون خود هستند. همچنین، ۲ و ۸، و ۷ و ۱۳ وارونهای یکدیگر هستند.

۳۱.۲ تعداد جوابهای ممکن برای $ax \equiv b (\mathrm{mod}\ ۲۰)$ چقدر است؟

حل. بنابر (۷.۲)، اگر معادله جواب داشته باشد، تعداد $d = (a, ۲۰)$ جواب ناهمنهشت به پیمانهٔ ۲۰ دارد. چون $d | ۲۰$ پس مقادیر ممکن برای d عبارت‌اند از ۱، ۲، ۴، ۵، ۱۰، و ۲۰. اما همنشتیهای $۲x \equiv ۱، x \equiv ۱، ۲x \equiv ۲، ۲x \equiv ۴، ۴x \equiv ۴، \ldots$، و $۲۰x \equiv ۲۰$ (همگی به پیمانهٔ ۲۰) به‌ترتیب ۰، ۱، ۲، ۴، ۵، ۱۰، و ۲۰ جواب دارند. لذا مقادیر به‌دست آمده برای d همان مقادیر ممکن هستند.

۳۲.۲ (الف) معادلهٔ $۱۷۹x \equiv ۲۸۳ (\mathrm{mod}\ ۳۱۳)$ را حل کنید. (۳۱۳ اول است.)
(ب) ۲۸۳ را به‌صورت ترکیب خطی از ۱۷۹ و ۳۱۳ بنویسید. (توجه قبل از (۱۰.۲) را ببینید.)

حل. (الف) از شیوهٔ حاصلضرب که در تکنیک ۳ قبل از (۱۰.۲) بیان شد استفاده می‌کنیم. نزدیکترین عدد صحیح به ۳۱۳/۱۷۹ عدد ۲ است، لذا از ضرب همنهشتی در ۲ داریم $۳۵۸x \equiv ۵۶۶ (\mathrm{mod}\ ۳۱۳)$ که این هم‌ارز است با $-۴۵x \equiv -۶۰ (\mathrm{mod}\ ۳۱۳)$، یا $۳x \equiv -۴ (\mathrm{mod}\ ۳۱۳)$. مجدداً نزدیکترین عدد صحیح به ۳۱۳/۳ عدد ۱۰۴ است. از ضرب همنهشتی اخیر در ۱۰۴ و ساده کردن آن داریم $x \equiv ۱۰۳ (\mathrm{mod}\ ۳۱۳)$.

(ب) بنابر قسمت الف $۳۱۳k + ۲۸۳ = ۱۰۳ \times ۱۷۹$، و روشن است که

$$k = (۱۷۹ \times ۱۰۳ - ۲۸۳)/۳۱۳ = ۵۸$$

لذا $۱۰۳ \times ۱۷۹ - ۳۱۳ \times ۵۸ = ۲۸۳$.

۳۳.۲ جواب یکتای $۲۵۱x \equiv ۱۲۵ (\mathrm{mod}\, ۵۲۱)$ را به‌دست آورید (۵۲۱ اول است.)

حل. مجدداً تکنیک حاصلضرب را به‌کار می‌بریم. نزدیکترین عدد صحیح به $۵۲۱/۲۵۱$ برابر ۲ است؛ از ضرب همنهشتی در ۲ و تحویل آن به پیمانهٔ ۵۲۱ داریم $-۱۹x \equiv ۲۵۰ (\mathrm{mod}\, ۵۲۱)$ (۱). به همین ترتیب، از ضرب همنهشتی (۱) در نزدیکترین عدد صحیح به $۵۲۱/۱۹$ یعنی ۲۷ داریم $۸x \equiv ۴۹۸ \equiv -۲۳ (\mathrm{mod}\, ۵۲۱)$. (۲) نزدیکترین عدد صحیح به $۵۲۱/۸$ برابر ۶۵ است. از ضرب (۲) در ۶۵ و ساده کردن آن داریم $x \equiv -۶۸ (\mathrm{mod}\, ۵۲۱)$ یا $x \equiv ۴۵۳ (\mathrm{mod}\, ۵۲۱)$ که جواب یکتای همنهشتی اصلی است.

مسألهٔ بعد تکنیکی را برای تحویل یک همنهشتی مفروض به یک همنهشتی با پیمانهٔ کوچکتر به‌دست می‌دهد. در صورت لزوم، با تکرار این روند یک همنهشتی به‌دست می‌آید که جوابش به آسانی تعیین می‌شود. سپس با عمل از آخر، جواب همنهشتی اصلی را از این جواب به‌دست می‌آوریم.

۳۴.۲ فرض کنید y^* یک جواب همنهشتی $my \equiv -b (\mathrm{mod}\, a)$ باشد. ثابت کنید $(my^* + b)/a$ یک جواب $ax \equiv b (\mathrm{mod}\, m)$ است.

حل. اگر $my^* \equiv -b (\mathrm{mod}\, a)$، آنگاه یک عدد صحیح k وجود دارد به‌طوری که $my^* + b = ka$. لذا $ak \equiv b (\mathrm{mod}\, m)$، و از آنجا $k = (my^* + b)/a$ یک جواب $ax \equiv b (\mathrm{mod}\, m)$ است.

توضیح. روند تحویلی بالا را می‌توان تکرار کرد، ولی چون پیمانه، ضریب مجهول، و مقدار ثابت سمت راست همگی در کاربردهای متوالی تغییر می‌کنند، به خاطر داشتن جایگذاری مقادیر مناسب a، b، و m در هر مرحله مهم است. این تکنیک در حل مسألهٔ زیر نشان داده شده است.

۳۵.۲ تمام جوابهای $۱۰۸x \equiv ۱۷۱ (\mathrm{mod}\, ۵۲۹)$ را به‌دست آورید.

حل. چون $(۱۰۸, ۵۲۹) = ۱$، پس معادله فقط یک جواب دارد. با استفاده از الگوریتم اقلیدسی ۱ را به‌صورت ترکیب خطی از ۱۰۸ و ۵۲۹ می‌نویسیم، یعنی $۱۰۸(-۲۴۰) + ۵۲۹ \times ۴۹ = ۱$.

(بررسی کنید!). لذا $۱۰۸(-۲۴۰) \equiv ۱(\bmod ۵۲۹)$، و از این‌رو،

$$۱۰۸(-۲۴۰ \times ۱۷۱) \equiv ۱۷۱(\bmod ۵۲۹)$$

چون $-۲۴۰ \times ۱۷۱ \equiv ۲۲۲(\bmod ۵۲۹)$، لذا $x \equiv ۲۲۲(\bmod ۵۲۹)$ تنها جواب این همنهشتی است.

روش دیگر، تکنیک به‌کار رفته در مسألهٔ قبل را به‌کار می‌بریم. اگر $ax \equiv b(\bmod m)$ مفروض باشد، ابتدا $my \equiv -b(\bmod a)$ را حل می‌کنیم؛ در اینجا، داریم $۵۲۹y \equiv -۱۷۱(\bmod ۱۰۸)$، یعنی، $-۱۱y \equiv -۱۷۱(\bmod ۱۰۸)$ که هم‌ارز است با $۱۱y \equiv ۶۳(\bmod ۱۰۸)$. مجدداً همنهشتی تحویلی $۱۰۸z \equiv -۶۳(\bmod ۱۱)$ یا $۲z \equiv ۸(\bmod ۱۱)$ را در نظر می‌گیریم. از اینجا جواب $z_۰ = ۴$ به‌دست می‌آید. لذا $y_۰ = (mz_۰ + b)/a = (۱۰۸ \times ۴ + ۶۳)/۱۱ = ۴۵$. (توجه کنید که در مرحلهٔ دوم تحویل، با نوشتن $۱۱y \equiv ۶۳(\bmod ۱۰۸)$ به‌صورت $az \equiv b(\bmod m)$ مقادیر $m = ۱۰۸$، $b = ۶۳$، و $a = ۱۱$ به‌دست آمده‌اند.) سرانجام،

$$x_۰ = (my_۰ + b)/a = (۵۲۹ \times ۴۵ + ۱۷۱)/۱۰۸ = ۲۲۲$$

به‌دست می‌آید، زیرا در همنهشتی اصلی داریم $m = ۵۲۹$، $b = ۱۷۱$، و $a = ۱۰۸$.

۳۶.۲ تمام جوابهای مشترک دو همنهشتی $۳x - ۷y \equiv ۴(\bmod ۱۹)$، و

$$۷x - ۳y \equiv ۱(\bmod ۱۹)$$

را به‌دست آورید.

حل. فقط به یک جرح و تعدیل جزئی از روش معمول در حل دو معادلهٔ خطی دومجهولی نیاز داریم. چون $(۷, ۱۹) = ۱$، همنهشتی اول با همنهشتی $۷(۳x - ۷y) \equiv ۷ \times ۴(\bmod ۱۹)$، یعنی، $۲۱x - ۴۹y \equiv ۲۸(\bmod ۱۹)$ هم‌ارز است. با استدلال مشابه، همنهشتی $۷x - ۳y \equiv ۱(\bmod ۱۹)$ با $۲۱x - ۴۹y \equiv ۳(\bmod ۱۹)$ هم‌ارز است. از تفریق دو همنهشتی داریم $-۴۰y \equiv ۲۵(\bmod ۱۹)$ یا هم‌ارز با آن $-۲y \equiv ۶(\bmod ۱۹)$، لذا $y \equiv -۳(\bmod ۱۹)$. با گذاشتن این مقدار در همنهشتی اول $x \equiv ۷(\bmod ۱۹)$ را به‌دست می‌آوریم. لذا جواب دستگاه عبارت است از $x \equiv ۷(\bmod ۱۹)$، $y \equiv ۱۶(\bmod ۱۹)$.

۳۷.۲ تمام جوابهای دستگاه همنهشتیهای $۳x - ۷y \equiv ۴(\bmod ۱۵)$، $۷x - ۳y \equiv ۱(\bmod ۱۵)$ را به‌دست آورید.

حل. همانند مسأله قبل، همنهشتی اول با $21x - 49y \equiv 28 \pmod{15}$ هم‌ارز است. همنهشتی دوم ایجاب می‌کند $21x - 96 \equiv 3 \pmod{15}$ (در اینجا هم‌ارزی نداریم، زیرا ۳ و ۱۵ نسبت به هم اول نیستند). اما مانند قبل، اگر دو همنهشتی مفروض برقرار باشند، آنگاه $-40y \equiv 25 \pmod{15}$ یا $5y \equiv 10 \pmod{15}$، و لذا $y \equiv 2 \pmod{3}$. بنابراین مقادیر ممکن به پیمانهٔ ۱۵ برای y تنها عبارت‌اند از ۲، ۵، ۸، ۱۱، و ۱۴. با جایگزین کردن این مقادیر در $7x - 3y \equiv 1 \pmod{15}$، به‌ترتیب مقادیر 4 و $7 \pmod{15}$ و $x \equiv 1, 13, 10, 7$ به‌دست می‌آید.

قضیهٔ باقیماندهٔ چینی

۳۸.۲ تمام اعداد صحیح بین ۳۰۰۰ و ۵۰۰۰ را که در تقسیم آنها بر ۷، ۱۱، و ۱۳ باقیمانده‌ها به‌ترتیب ۱، ۳، و ۵ می‌شوند، به‌دست آورید.

حل. قضیهٔ باقیماندهٔ چینی را در مورد دستگاه $x \equiv 1 \pmod{7}$، $x \equiv 3 \pmod{11}$، $x \equiv 5 \pmod{13}$ به‌کار می‌بریم. اعداد b_1، b_2، b_3 را پیدا می‌کنیم به‌طوری که $143b_1 \equiv 1 \pmod{7}$، $91b_2 \equiv 1 \pmod{11}$، و $77b_3 \equiv 1 \pmod{13}$، یا $3b_1 \equiv 1 \pmod{7}$، $3b_2 \equiv 1 \pmod{11}$، و $-b_3 \equiv 1 \pmod{13}$. لذا می‌توانیم مقادیر $b_1 = 5$، $b_2 = 4$، و $b_3 = -1$ را اختیار کنیم. در نتیجه جواب دستگاه عبارت است از

$$x^* \equiv 143(5)(1) + 91(4)(3) + 77(-1)(5) \equiv 1422 \pmod{1001}$$

چون جوابها به‌صورت $1001t + 1422$ (t عدد صحیح) هستند، آشکار است که جوابهای بین ۳۰۰۰ و ۵۰۰۰ عبارت است از $1001 \times 2 + 1422 = 3424$ و $1001 + 3424 = 4425$.

۳۹.۲ اعداد صحیح $0 < x < 140$ را تعیین کنید که در همنهشتیهای $x \equiv 1 \pmod{4}$، $2x \equiv 3 \pmod{5}$، و $4x \equiv 5 \pmod{7}$ صدق می‌کنند.

حل. ابتدا همنهشتیها را به‌صورت $x_i \equiv a_i \pmod{m_i}$ در می‌آوریم، سپس قضیهٔ باقیماندهٔ چینی را به‌کار می‌بریم. همنهشتی اول خود به همین صورت است؛ از حل $2x \equiv 3 \pmod{5}$ به‌دست می‌آوریم $x \equiv 3 \pmod{5}$؛ و از حل $4x \equiv 5 \pmod{7}$ خواهیم داشت $x \equiv 3 \pmod{7}$. اکنون b_1، b_2، b_3 را به‌دست می‌آوریم به‌طوری که $5 \times 7b_1 \equiv 1 \pmod{4}$، $4 \times 7b_2 \equiv 1 \pmod{5}$، و $4 \times 5b_3 \equiv 1 \pmod{7}$. از حل این همنهشتیها داریم $b_1 = -1$، $b_2 = 2$، و $b_3 = -1$. لذا جواب دستگاه عبارت است از

$$x^* \equiv 35 \times -1 \times 1 + 28 \times 2 \times 4 + 20 \times -1 \times 3 \equiv 129 \pmod{140}$$

چون $۱۴۰ = ۷ \times ۵ \times ۴$ در نتیجه ۱۲۹ تنها جوابی از دستگاه است که در شرط $۰ < x < ۱۴۰$ صدق می‌کند.

در سه مسأله بعد از دستگاه $x \equiv a_i (\mathrm{mod}\, m_i)$ $(i = ۱, ۲, \ldots, r)$ بحث می‌شود که در آن m_iها لزوماً دوبه‌دو متباین نیستند. می‌توان نشان داد که این دستگاه جواب دارد اگر و تنها اگر به‌ازای $i \neq j$، $(m_i, m_j) | a_j - a_i$. برهان در حالت کلیِ r کمی دشوار است (تعدادی برهانهای نادرست وجود دارند)، لذا فقط در حالت $r = ۲$ مسأله را به‌طور کامل بررسی می‌کنیم.

۴۰.۲ نشان دهید که قضیهٔ (۱۱.۲) در حالتی که پیمانه‌ها دوبه‌دو نسبت به هم اول نباشند لزوماً برقرار نیست.

حل. مثلاً، فرض کنید $m_۱ = ۲$، $m_۲ = ۴$، $a_۱ = ۱$، و $a_۲ = ۲$. آشکار است که دستگاه همنهشتیهای $x_i \equiv a_i (\mathrm{mod}\, m_i)$ $(i = ۱, ۲)$ جواب ندارد.

۴۱.۲ دستگاه $x \equiv a (\mathrm{mod}\, m)$، $x \equiv b (\mathrm{mod}\, n)$ را که در آن m و n لزوماً نسبت به هم اول نیستند در نظر می‌گیریم. اگر $(m, n) | b - a$، ثابت کنید دستگاه جواب دارد.

حل. قرار می‌دهیم $d = (m, n)$ و فرض می‌کنیم $d | b - a$. بنابر (۲۴.۱) اعداد صحیح u و v وجود دارند به‌طوری که $mu + nv = b - a$. فرض کنیم $x = a + mu$؛ در این‌صورت روشن است که $x \equiv a (\mathrm{mod}\, m)$. همچنین، $x = a + mu = a + (b - a) - nv = b - nv$، و لذا $x \equiv b (\mathrm{mod}\, n)$.

۴۲.۲ فرض کنید دستگاه $x \equiv a_i (\mathrm{mod}\, m_i)$ $(i = ۱, ۲, \ldots, r)$ جواب دارد. نشان دهید به‌ازای $i \neq j$، $(m_i, m_j) | a_j - a_i$. همچنین اگر s جوابی از دستگاه باشد، نشان دهید که همهٔ جوابها همنهشت با s به پیمانهٔ $[m_۱, \ldots, m_r]$ هستند.

حل. فرض کنیم $i \neq j$ و قرار می‌دهیم $d = (m_i, m_j)$. اگر s جوابی از دستگاه باشد، آنگاه $s \equiv a_i (\mathrm{mod}\, m_i)$. لذا $m_i | s - a_i$، و از این‌رو $d | s - a_i$؛ با استدلالی مشابه، $d | s - a_j$. در نتیجه، $d | (s - a_i) - (s - a_j) = a_j - a_i$. لذا دستگاه جواب ندارد مگر اینکه به‌ازای $i \neq j$، $(m_i, m_j) | a_j - a_i$.

عدد x جوابی از دستگاه است اگر و تنها اگر به‌ازای هر i، $x \equiv a_i (\mathrm{mod}\, m_i)$، یعنی، اگر و تنها اگر به‌ازای هر i، $x \equiv s (\mathrm{mod}\, m_i)$. اما بنابر (iii.۴.۲) این رابطه دقیقاً وقتی برقرار است که $x \equiv s (\mathrm{mod}\, [m_۱, m_۲, \ldots, m_r])$.

۴۳.۲ (چین‌چیو شائو، سدهٔ سیزدهم) سه کشاورز محصول برنجی را که درو کرده‌اند به تساوی بین خود تقسیم می‌کنند. یکی از آنها به مغازه‌ای می‌رود که وزنهٔ ۸۳ پوندی به‌کار می‌برد، دیگری به مغازه‌ای که وزنهٔ ۱۱۰ پوندی دارد، و سومی به مغازه‌ای که از وزنهٔ ۱۳۵ پوندی استفاده می‌کند. هر کشاورز تا آنجا که می‌تواند برنج خود را به فروش می‌رساند. وقتی سه‌تایی به خانه برمی‌گردند، از برنج اولی ۳۲ پوند، از برنج دومی ۷۰ پوند، و از برنج سومی ۳۰ پوند باقی مانده است. مقدار کل برنجی را که به بازار برده‌اند تعیین کنید.

حل. فرض کنیم x مقدار برنجی باشد که هر کشاورز به بازار برده است؛ در این‌صورت $x \equiv ۳۲ (\mathrm{mod}\, ۸۳)$، $x \equiv ۷۰ (\mathrm{mod}\, ۱۱۰)$، و $x \equiv ۳۰ (\mathrm{mod}\, ۱۳۵)$. در اینجا مسأله این است که ۸۳، ۱۱۰، و ۱۳۵ دوبه‌دو متباین نیستند، زیرا $(۱۱۰, ۱۳۵) = ۵$.

چون $۱۱ \times ۵ \times ۲ = ۱۱۰$ و $۲۷ \times ۵ = ۱۳۵$، دو همنهشتی آخر با همنهشتیهای زیر هم‌ارزند: $x \equiv ۰ (\mathrm{mod}\, ۲)$، $x \equiv ۰ (\mathrm{mod}\, ۵)$، $x \equiv ۴ (\mathrm{mod}\, ۱۱)$، و $x \equiv ۳ (\mathrm{mod}\, ۲۷)$. قضیهٔ باقیماندهٔ چینی را در مورد این چهار همنهشتی و همنهشتی $x \equiv ۳۲ (\mathrm{mod}\, ۸۳)$ به‌کار می‌بریم. داریم $m_۱ = ۲$، $m_۲ = ۵$، $m_۳ = ۱۱$، $m_۴ = ۲۷$، $m_۵ = ۸۳$ و $a_۱ = ۰$، $a_۲ = ۰$، $a_۳ = ۴$، $a_۴ = ۳$، $a_۵ = ۳۲$. چون $a_۱ = a_۲ = ۰$، فقط به محاسبهٔ مقادیر $b_۳$، $b_۴$، و $b_۵$ که در برهان قضیهٔ ماندهٔ چینی آمده بود نیاز داریم. لذا باید معادله‌های $۱ (\mathrm{mod}\, ۱۱) \equiv ۸۳b_۳ \times ۲۷ \times ۵ \times ۲$، $۱ (\mathrm{mod}\, ۲۷) \equiv ۸۳b_۴ \times ۱۱ \times ۵ \times ۲$، و $۱ (\mathrm{mod}\, ۸۳) \equiv ۲۷b_۵ \times ۱۱ \times ۵ \times ۲$ یا هم‌ارز آنها $۱ (\mathrm{mod}\, ۱۱) \equiv ۳b_۳$، $۱ (\mathrm{mod}\, ۲۷) \equiv ۴b_۴$ و $۱ (\mathrm{mod}\, ۸۳) \equiv ۶۵b_۵$ را حل کنیم. در اولین همنهشتی به‌جای عدد ۱ عدد ۱۲ می‌گذاریم و دو طرف را بر ۳ تقسیم می‌کنیم و به‌دست می‌آوریم $b_۳ = ۴$ (یا می‌توانستیم از $b_۳ = -۷$ استفاده کنیم)؛ در همنهشتی دوم به‌جای ۱ عدد ۲۸ را قرار می‌دهیم و طرفین را بر ۴ تقسیم می‌کنیم و به‌دست می‌آوریم $b_۴ = ۷$ (یا $b_۴ = -۲۰$). در سومی به‌جای ۶۵ عدد -۱۸ و به‌جای ۱ عدد ۸۴ را می‌گذاریم و طرفین را بر ۶ تقسیم می‌کنیم و به‌دست می‌آوریم $-۳b_۵ \equiv ۱۴ (\mathrm{mod}\, ۸۳)$؛ حال به‌جای ۱۴ عدد -۶۹ می‌گذاریم و طرفین را بر ۳ تقسیم می‌کنیم و به‌دست می‌آوریم $b_۵ = ۲۳$. (ملاحظه می‌کنیم که در همهٔ این تقسیمها، پیمانه تغییر نمی‌کند، زیرا عددی که بر آن تقسیم می‌کنیم نسبت به پیمانه اول است). اکنون مقادیر مناسب را در عبارت مربوط به x^* که در برهان (۱۱.۲) ارائه شده است قرار می‌دهیم. با استفاده از $b_۳ = -۷$، $b_۴ = -۲۰$ (به این دلیل که مجموع کلی کوچکتر شود)، $b_۵ = ۲۳$، $x^* = ۱۰۱۰۶۴۰$ را به‌دست می‌آوریم. در اینجا $m = ۲ \times ۵ \times ۱۱ \times ۲۷ \times ۸۳ = ۲۴۶۵۱۰$، لذا کمترین ماندهٔ نامنفی x^* به پیمانهٔ m برابر است با ۲۴۶۰۰. چون کوچکترین جواب بعدی

عبارت است از $x^* + m = ۲۴۶۰۰ + ۲۴۶۵۱۰ = ۲۷۱۱۱۰$، که می‌توان گفت از حد معمول زیادتر است، در نتیجه هر کشاورز ۲۴۶۰۰ پوند برنج به بازار می‌برد، و لذا مقدار کل برنج $۳ \times ۲۴۶۰۰ = ۷۳۸۰۰$ پوند بوده است.

۴۴.۲ (بهاسکره I، سدهٔ ششم؛ همچنین الهیثم، سدهٔ یازدهم؛ فیبوناتچی، اوایل سدهٔ سیزدهم) اگر تخم‌مرغهای یک سبد را ۲تا ۲تا، ۳تا ۳تا، ۴تا ۴تا، ۵تا ۵تا، و ۶تا ۶تا خارج کنیم، به‌ترتیب ۱، ۲، ۳، ۴، و ۵ تخم‌مرغ در سبد باقی می‌ماند. در صورتی‌که آنها را ۷تا ۷تا برداریم هیچ تخم‌مرغی باقی نمی‌ماند. کمترین تعداد تخم‌مرغی را که می‌تواند در سبد باشد تعیین کنید.

حل. یک عدد صحیح مثبت x را لازم داریم به‌طوری‌که $x \equiv ۱ (\mathrm{mod}\ ۲)$، $x \equiv ۲ (\mathrm{mod}\ ۳)$، $x \equiv ۳ (\mathrm{mod}\ ۴)$، $x \equiv ۴ (\mathrm{mod}\ ۵)$، $x \equiv ۵ (\mathrm{mod}\ ۶)$، و $x \equiv ۰ (\mathrm{mod}\ ۷)$. اما، چون پیمانه‌ها دوبه‌دو متباین نیستند (مثلاً ۲ و ۴ یا ۳ و ۶)، نمی‌توان مستقیماً قضیهٔ باقیماندهٔ چینی را به‌کار برد. ولی به دلیل ماهیت خاص همنهشتیها، راه‌حل آسانی وجود دارد.

توجه می‌کنیم که پنج همنهشتی اول را می‌توان به‌صورت $x \equiv -۱ (\mathrm{mod}\ ۲, ۳, ۴, ۵, ۶)$ نوشت. بنابر (iii.۴.۲) جواب این دستگاه فوراً به‌دست می‌آید و آن $x \equiv -۱ (\mathrm{mod}\ ۶۰)$ است (۶۰ کوچکترین مضرب مشترک این پیمانه‌هاست). لذا کافی است دستگاه $x \equiv -۱ (\mathrm{mod}\ ۶۰)$ و $x \equiv ۰ (\mathrm{mod}\ ۷)$ را حل کنیم. با فرض $x = ۷y$، حل دستگاه هم‌ارز $۷y \equiv -۱ (\mathrm{mod}\ ۶۰)$ است. بنابر الگوریتم اقلیدسی (یا با تجسس)، $y = ۱۷$ یک جواب است، لذا $x = ۱۱۹$ جوابی از دستگاه اصلی است. چون اختلاف جوابها مضربی است از $۶۰ \times ۷ = ۴۲۰$، پس $x = ۱۱۹$ کوچکترین جواب است.

۴۵.۲ کوچکترین عدد صحیح مثبت x را بیابید به‌طوری که $x \equiv ۵ (\mathrm{mod}\ ۱۲)$، $x \equiv ۱۷ (\mathrm{mod}\ ۲۰)$، و $x \equiv ۲۳ (\mathrm{mod}\ ۴۲)$.

حل. چون پیمانه‌ها دوبه‌دو متباین نیستند، قضیهٔ باقیماندهٔ چینی مستقیماً به‌کار نمی‌آید. ابتدا دستگاه مفروض را به دستگاهی با پیمانه‌های دوبه‌دو متباین بدل می‌کنیم. بنابر (iii.۴.۲)، $x \equiv ۵ (\mathrm{mod}\ ۱۲)$ با $x \equiv ۵ (\mathrm{mod}\ ۳)$ و $x \equiv ۵ (\mathrm{mod}\ ۴)$، یعنی $x \equiv ۲ (\mathrm{mod}\ ۳)$ و $x \equiv ۱ (\mathrm{mod}\ ۴)$ هم‌ارز است. به دلیل تشابه، $x \equiv ۱۷ (\mathrm{mod}\ ۲۰)$ با $x \equiv ۱ (\mathrm{mod}\ ۴)$ و $x \equiv ۲ (\mathrm{mod}\ ۵)$ هم‌ارز است. (توجه: اگر در این قسمت مثلاً $x \equiv ۲ (\mathrm{mod}\ ۴)$ به‌دست آمده بود، این با $x \equiv ۱ (\mathrm{mod}\ ۴)$ که قبلاً به‌دست آمده بود ناسازگار می‌شد، لذا دستگاه اصلی جواب نمی‌داشت.) به همین ترتیب، $x \equiv ۲۳ (\mathrm{mod}\ ۴۲)$ با $x \equiv ۱ (\mathrm{mod}\ ۲)$، $x \equiv ۲ (\mathrm{mod}\ ۳)$،

و $x \equiv ۲(\bmod ۷)$ هم‌ارز است. چون $x \equiv ۱(\bmod ۴)$ همنهشتی $x \equiv ۱(\bmod ۲)$ را ایجاب می‌کند، دستگاه مبدل عبارت است از $x \equiv ۱(\bmod ۴)$، $x \equiv ۲(\bmod ۳)$، $x \equiv ۲(\bmod ۵)$، و $x \equiv ۲(\bmod ۷)$. اکنون می‌توانیم روش ماشینی بیان‌شده در برهان (۱۱.۲) را به‌کار بریم. اما آسانتر آن است که توجه کنیم سه همنهشتی آخر با $x \equiv ۲(\bmod ۱۰۵)$ هم‌ارز است و اینکه $۱(\bmod ۴) \equiv (۱۰۵ - ۲)$. لذا -۱۰۳ یک جواب همنهشتی است، و $۱۰۵ \times ۴ + ۱۰۳ - = ۳۱۷$ کوچکترین جواب مثبت است.

۴۶.۲ کوچکترین عدد صحیح مثبتی را پیدا کنید که در تقسیم بر ۱۰، ۹، ...، ۳، ۲ باقیمانده‌ها به‌ترتیب ۹، ۸، ...، ۲، ۱ شوند.

حل. مطلوب یافتن xی است که $x \equiv ۱(\bmod m)$ $(m = ۱۰, ۹, \ldots, ۲)$. در نگاه اول وسوسه می‌شویم که قضیهٔ باقیماندهٔ چینی را به‌کار بریم، ولی برای یافتن جواب راه آسانتری وجود دارد. $x = -۱$ یک جواب است که متأسفانه مثبت نیست. ولی، بنابر (iii.۴.۲) این دستگاه با $x \equiv -۱(\bmod m)$ که m کوچکترین مضرب مشترک ۲، ۳، ...، ۱۰ است هم‌ارز است. لذا هر جواب به‌صورت $mt - ۱$ است که t عدد صحیحی است. بنابراین کوچکترین جواب مثبت $m - ۱$ است که در آن $m = ۲^۳ \times ۳^۲ \times ۵ \times ۷$.

توضیح. استدلال بالا با تعویض -۱ با هر عدد صحیح کارساز است، آنچه مهم است آن است که طرف راست هر همنهشتی یکی است.

۴۷.۲ دستگاه همنهشتیهای زیر را حل کنید: $x^۲ \equiv ۲(\bmod ۷)$، $x^۲ \equiv ۳(\bmod ۱۱)$، $x^۲ \equiv ۴(\bmod ۱۳)$. (راهنمایی: ابتدا هر همنهشتی را برای x حل کنید.)

حل. در همنهشتی اول، ۲ را با ۹ عوض می‌کنیم تا $x \equiv \pm ۳(\bmod ۷)$ را به‌دست آوریم؛ در دومی، ۲۵ را جایگزین ۳ می‌کنیم تا $x \equiv \pm ۵(\bmod ۱۱)$ به‌دست آید، در سومی، روشن است که $x \equiv \pm ۲(\bmod ۱۳)$. اکنون قضیهٔ باقیماندهٔ چینی را در مورد دستگاه $x \equiv a(\bmod ۷)$، $x \equiv b(\bmod ۱۱)$، $x \equiv c(\bmod ۱۳)$ به‌کار می‌بریم که در آن $a = \pm ۳$، $b = \pm ۵$، و $c = \pm ۲$. لذا $۸ = ۲ \times ۲ \times ۲$ دستگاه مختلف وجود دارند که باید مورد بررسی قرار گیرند. بهتر آن است که صورت جوابها را برحسب a، b، c به‌دست آوریم، سپس مقادیر مختلف را جایگزین کنیم. به اعداد $b_۱$، $b_۲$، $b_۳$ نیاز داریم به‌طوری که $۱۴۳b_۱ \equiv ۱(\bmod ۷)$، $۳b_۱ \equiv ۱(\bmod ۱۱)$، $۹۱b_۲ \equiv ۱(\bmod ۱۳)$، و $۷۷b_۳ \equiv ۱(\bmod ۷)$، یعنی،

$3b_2 \equiv 1 \pmod{11}$، و $-b_3 \equiv 1 \pmod{13}$. مقادیر $b_1 = -2$، $b_2 = 4$، $b_3 = -1$ را اختیار می‌کنیم. در این‌صورت جواب عمومی عبارت است از

$$x^* \equiv 143(-2)a + 91(4)b + 77(-1)c \pmod{7 \times 11 \times 13}$$

با استفاده از این حقیقت که سه‌تایی (a, b, c) در چهار جفت با علامت مخالف ظاهر می‌شوند، مقادیر a، b، و c را جایگزین می‌کنیم. در نتیجه دستگاه اصلی همنهشتیها دارای جوابهای زیر است

$$\pm 115, \pm 171, \pm 193, \quad \text{و} \quad \pm 479 \pmod{1001}$$

◁ **۴۸.۲** کوچکترین عدد صحیح مثبت n را بیابید به‌طوری که $n/3$ یک مکعب کامل، $n/5$ یک توان پنجم کامل، و $n/7$ یک توان هفتم کامل باشد.

حل. چون n بر ۳، ۵، و ۷ بخشپذیر است، می‌توانیم n را به‌صورت $3^a 5^b 7^c$ اختیار کنیم. چون $n/3 = 3^{a-1} 5^b 7^c$ یک مکعب کامل است، لذا باید $a - 1$، b، و c بر ۳ بخشپذیر باشند، یعنی $a \equiv 1 \pmod 3$، $b \equiv 0 \pmod 3$، و $c \equiv 0 \pmod 3$. به دلیل مشابه، $n/5 = 3^a 5^{b-1} 7^c$ یک توان پنجم کامل است، در نتیجه به پیمانهٔ ۵ داریم $a \equiv 0$، $b \equiv 1$، و $c \equiv 0$. همچنین از اینکه $n/7 = 3^a 5^b 7^{c-1}$ یک توان هفتم کامل است نتیجه می‌شود که به پیمانهٔ ۷، $a \equiv 0$، $b \equiv 0$، و $c \equiv 1$. از سه همنهشتی مربوط به a کوچکترین جوابِ مثبت a برابر ۷۰ است (زیرا a مضربی از ۳۵ و همنهشت با ۱ به پیمانهٔ ۳ است). کوچکترین جوابِ مثبتِ b از سه همنهشتی مربوط به آن ۲۱ است (زیرا b مضربی از ۲۱ و همنهشت با ۱ به پیمانهٔ ۵ است). و کوچکترین مقدار c برابر ۱۵ است. لذا $n = 3^{70} \times 5^{21} \times 7^{15}$.

روز هفته

در حل مسائل زیر برای تعیین روز هفته در یک تاریخِ مفروض از الگوریتمی استفاده می‌شود که به تفصیل در (۱۲.۲) بیان شده است.

۴۹.۲ در الگوریتم بیان‌شده در (۱۲.۲)، رمز سال با $y + [y/4]$ ارائه شده است، که در آن y عدد صحیحی متشکل از دو رقم آخرِ مربوط به آن سال است. می‌توان این رمز را به طریق زیر نیز محاسبه کرد. اگر $y = 12k + r$، که $0 \le r \le 11$، آنگاه رمز سال با $k + r + [r/y]$ ارائه می‌شود. (مثلاً اگر سال ۱۹۴۵ باشد، رمز برابر است با تعداد ۱۲ها در ۴۵ (یعنی، ۳)، به‌علاوه باقیماندهٔ تقسیم ۴۵ بر ۱۲، یعنی ۹، به‌علاوه تعداد ۴ها در ۹، یعنی $2 + 9 + 3$، یا ۰

به پیمانهٔ ۷.) ثابت کنید که این‌دو بیان همواره یک نتیجه را به‌دست می‌دهند؛ یعنی، ثابت کنید که $u + [y/۴] \equiv k + r + [r/۴] (\mathrm{mod}\, ۷)$.

حل. اگر $y = ۱۲k + r$، آنگاه

$$y + [y/۴] = ۱۲k + r + [۳k + r/۴]$$
$$= ۱۲k + r + ۳k + [r/۴] = ۱۵k + r + [r/۴] \equiv k + r + [r/۴] (\mathrm{mod}\, ۷)$$

این مطلب را به‌کار بردیم که اگر n عدد صحیحی باشد، آنگاه، $[n + x] = n + [x]$. (این تساوی از تعریفِ $[x]$ فوراً نتیجه می‌شود.)

توضیح. کاربرد روش بالا برای یافتن رمز سال آسانتر است هرگاه بخواهید محاسبه را ذهنی انجام دهید. ولی، اگر الگوریتم برای چیزی پیچیده‌تر از یافتن روز هفته برای یک تاریخِ مفروض به‌کار رود، آنگاه طریقِ اصلی محاسبهٔ رمز سال (یعنی، $y + [y/۴]$) غالباً مناسبتر است. (مسألهٔ ۵۴.۲ را ببینید.)

۵۰.۲ ثابت کنید که در سدهٔ بیستم، روز اول مارس ۱۹۰۰ بر هر روز از هفته بیفتد در ۲۸ سال بعد هم بر همان روز از هفته خواهد افتاد.

حل. کافی است ثابت کنیم که رمز سال در هر ۲۸ سال یکی است، یعنی

$$y' + [y'/۴] \equiv y + [y/۴] (\mathrm{mod}\, ۷)$$

که در آن $y' = y + ۲۸k$. این رابطه از

$$[y'/۴] = [y/۴ + ۷k] = [y/۴] + ۷k \equiv [y/۴] (\mathrm{mod}\, ۷)$$

فوراً نتیجه می‌شود. (توجه کنید که تاریخهای واقع در ژانویه یا فوریه ۱۹۰۰ استثنا شده‌اند، زیرا ۱۹۰۰ یک سال کبیسه نبوده است).

◁ **۵۱.۲** (جمعهٔ سیزدهم) بیان کنید که چرا هر سال لااقل یک جمعهٔ سیزدهم دارد و بیشتر از سه جمعه ندارد. اگر سال دارای سه جمعهٔ سیزدهم باشد، اول سال نو به چه روزی از هفته می‌افتد؟

حل. فرض کنیم سیزدهم ژانویه روز x از هفته در یک سال مفروض باشد؛ لذا $x = ۰.۱.۲, \ldots, ۶$. (توجه کنید که شنبه، هفتمین روزِ هفته متناظر با ۰ است.) برای بررسی دو

حالت وجود دارد. ابتدا فرض می‌کنیم که در یک سالِ کبیسه نباشیم. چون ژانویه ۳۱ روز دارد و $۳۱ \equiv ۳ \pmod ۷$، روز هفته برای سیزدهم فوریه روز $x + ۳$ هفته است. چون فوریه ۲۸ روز دارد و $۲۸ \equiv ۰ \pmod ۷$، روز هفته برای سیزدهم مارس با روز هفته برای سیزدهم فوریه یکی، یعنی $x + ۳$ می‌شود. اگر این روش را ادامه دهیم، روزهای هفتهٔ زیر را برای هر ماه به‌دست می‌آوریم: x، $x + ۳$، $x + ۳$، $x + ۶$، $x + ۱$، $x + ۴$، $x + ۶$، $x + ۲$، $x + ۵$، x، $x + ۳$، $x + ۵$. قطع نظر از مقدار x، فهرست بالا همواره شامل یک دستگاه کامل مانده‌ها به پیمانهٔ ۷ است، لذا به‌ازای هر x، حداقل یکی از این اعداد همنهشت با ۶ است، که جمعه را نمایش می‌دهد. این امر ثابت می‌کند که یک جمعهٔ سیزدهم در هر سال غیرکبیسه وجود دارد.

چون در فهرست بالا $x + ۳$ سه‌بار آمده است، سال دارای دقیقاً سه جمعهٔ سیزدهم است هرگاه $x + ۳ = ۶$، یعنی $x = ۳$. بنابه تعریفِ x، این بدان معنی است که سیزدهم ژانویه بایستی سومین روز هفته، یعنی سه‌شنبه باشد. لذا نتیجه می‌گیریم که در یک سال غیرکبیسه، روز سال نو به سه‌شنبه می‌افتد اگر سال دارای سه جمعهٔ سیزدهم باشد. به آسانی بررسی می‌شود که در این‌صورت جمعهٔ سیزدهم در فوریه، مارس، و نوامبر (ماههای متناظر با $x + ۳$) ظاهر می‌شوند.

سرانجام، فرض می‌کنیم که در یک سال کبیسه هستیم. تحلیل مسأله دقیقاً مانند بالاست، بجز اینکه حالا فوریه ۲۹ روز دارد. فهرستِ سیزدهم هر ماه عبارت است از x، $x + ۳$، $x + ۴$، $x + ۷$، $x + ۵$، $x + ۳$، $x + ۶$، $x + ۱$، $x + ۴$، $x + ۶$، که مجدداً شامل یک دستگاه کامل مانده‌ها به پیمانهٔ ۷ است. اما اکنون سال دارای دقیقاً سه جمعهٔ سیزدهم خواهد بود وقتی که $x = ۶$ (زیرا x روزی است که سه بار ظاهر می‌شود). لذا اگر سه جمعهٔ سیزدهم در یک سالِ کبیسه وجود داشته باشد، سیزدهم ژانویه $(= x)$ بایستی جمعه باشد، و لذا روز سال نو به یکشنبه می‌افتد. در این حالت، سه جمعهٔ سیزدهم در ژانویه، آوریل، و ژوئیه ظاهر می‌شوند.

۵۲.۲ نبرد هستینگز[1] در چهاردهم اکتبر ۱۰۶۶ اتفاق افتاده است. این روز کدام روز از هفته بوده است؟

حل. رمز سال عبارت است از $۵ \pmod ۷ \equiv [۶۶/۴] + ۶۶$، رمز ماه ۱ است، و تصحیح برای سدهٔ یازدهم عبارت است از $۱ \pmod ۷ \equiv ۸ = ۱۰ - ۱۸$. چون $۵ + ۱ + ۱۴ + ۱ \equiv ۰ \pmod ۷$ نبرد در شنبه اتفاق افتاده است.

◁ **۵۳.۲** در ۱۹۹۱، روز تولد شخصی به روز شکرگزاری امریکاییها (چهارمین پنجشنبهٔ نوامبر) افتاده است. اولین‌بار که اتفاق افتاده، او سه‌ساله بوده است؛ دفعهٔ بعد که اتفاق افتاده، سنش بین ۱۳

1. Hastings

تا ۱۹ بوده است. اگر فرض کنیم که این شخص در ۱۹۹۱ بالای ۲۰ و کمتر از ۵۰ سال داشته باشد، تولدش در چه روزی بوده است؟

حل. فرض کنیم d روز تولد در نوامبر باشد. رمز ماه برای نوامبر ۴ است، و رمز سال برای ۱۹۹۱ عبارت است از $۹۱+[۹۱/۴]+۲۲ \equiv ۱ \pmod ۷$. چون روز تولد در ۱۹۹۱ به پنجشنبه (پنجمین روز هفته) افتاده است، داریم $d \equiv ۰ \pmod ۷$. یعنی، $۵ \pmod ۷ \equiv d+۱+۴$. لذا $d = ۲۸$، زیرا روز تولد چهارمین پنجشنبه در نوامبر بوده است. آشکار است که اگر روز تولد به پنجشنبه بیفتد، آن پنجشنبه بایستی روز شکرگزاری باشد.

سپس تعیین می‌کنیم در چه سالهایی از این سده بیست و هشتم نوامبر به پنجشنبه می‌افتد. سال را با $y+۱۹۰۰$ نشان می‌دهیم. می‌نویسیم $y = ۴k+r$، با r برابر ۰، ۱، ۲، یا ۳؛ لذا رمز سال $y+[y/۴] = ۴k+r+k = ۵k+r$ است. چون بیست‌وهشتم نوامبر بایستی به پنجشنبه بیفتد، لازم است که $۵k+r \equiv ۱ \pmod ۷$. به‌ازای $r = ۰$، داریم $k \equiv ۳ \pmod ۷$، یعنی، به‌ازای یک عدد صحیح مثبت t، $k = ۷t+۳$. لذا $y = ۴(۷t+۳)+r = ۲۸t+۱۲$، و این جوابهای ۱۹۱۲، ۱۹۴۰، ۱۹۶۸، و ۱۹۹۶ را به‌دست می‌دهد. با استدلالی مشابه، اگر $r = ۱$، آنگاه $k \equiv ۰ \pmod ۷$ را به‌دست می‌آوریم، که ۱۹۰۰ ۱۹۲۸ ۱۹۵۶، و ۱۹۸۴ را ارائه می‌دهد؛ اگر $r = ۲$، آنگاه $k \equiv ۴ \pmod ۷$، که از آن ۱۹۱۸، ۱۹۴۶، و ۱۹۷۴ به‌دست می‌آید؛ و $r = ۳$ ایجاب می‌کند $k \equiv ۱ \pmod ۷$، که ۱۹۰۷، ۱۹۳۵، ۱۹۶۳، و ۱۹۹۱ را ارائه می‌دهد.

از آنجا که سنِ آن شخص در ۱۹۹۱ بالای ۲۰ و کمتر از ۵۰ بوده است، سالهای ممکن تولد عبارت‌اند از ۱۹۴۳، ۱۹۵۳، ۱۹۶۰، و ۱۹۶۵. در سه حالت آخر سن آن شخص بین ۱۳ تا ۱۹ نخواهد بود تا روز تولدش برای بار دوم به روز شکرگزاری بیفتد. لذا نتیجه می‌گیریم که آن شخص در بیست‌وهشتم نوامبر ۱۹۴۳ متولد شده است.

۵۴.۲ تمام سالهای سدهٔ بیستم را بیابید که در آنها کریسمس به یکشنبه بیفتد.

حل. رمزهای ماه و روز برای بیست‌وپنجم دسامبر $۳ \pmod ۷ \equiv ۲۵+۶$ را به‌دست می‌دهند. لذا اگر بخواهید کریسمس به یکشنبه بیفتد، رمز سال بایستی همنهشت با ۵ به پیمانهٔ ۷ باشد. سال را با $y+۱۹۰۰$ نشان می‌دهیم، و می‌نویسیم $y = ۴k+r$، که در آن r برابر ۰، ۱، ۲، یا ۳ است. سپس، همانند مسألهٔ قبل، رمز سال برابر است با $y+[y/۴] = ۵k+r$. از این‌رو لازم داریم که $۵k+r \equiv ۵ \pmod ۷$. برای $r = ۰$، داریم $k \equiv ۱ \pmod ۷$، که جوابهای ۱۹۰۴، ۱۹۳۲، ۱۹۶۰، و ۱۹۸۸ را به‌دست می‌دهد. برای $r = ۱$، به‌دست می‌آوریم $۵k \equiv ۴ \pmod ۷$،

یعنی، $k \equiv ۵ (\mathrm{mod}\ ۷)$، و این ۱۹۲۱، ۱۹۴۹، و ۱۹۷۷ را ارائه می‌دهد. اگر $r = ۲$، آنگاه $k \equiv ۲ (\mathrm{mod}\ ۷)$، که ۱۹۱۰، ۱۹۳۸، ۱۹۶۶، و ۱۹۹۴ را به ما می‌دهد؛ و $r = ۳$ ایجاب می‌کند $k \equiv ۶ (\mathrm{mod}\ ۷)$، که ۱۹۲۷، ۱۹۵۵، و ۱۹۸۳ را به ما می‌دهد.

۵۵.۲ هانری[1] هشتم با آن بولین[2] مخفیانه در بیست‌وپنجم ژانویه ۱۵۳۳ ازدواج کرده است. ازدواج آنها در چه روزی از هفته بوده است؟

حل. رمز سال برابر است با $۶ (\mathrm{mod}\ ۷) \equiv ۴۱ = [۳۳/۴] + ۳۳$، رمز ماه برای ژانویه ۱ است، و تصحیح برای قرن شانزدهم $۳ = ۱۵ - ۱۸$ است. چون $۰ (\mathrm{mod}\ ۷) \equiv ۳ + ۲۵ + ۱ + ۶$، پس ازدواج آنها روز شنبه بوده است.

مسائل گوناگون

آزمونهای بخشپذیری در قضیهٔ (۵.۲) در حل سه مسألهٔ بعد به‌کار می‌روند.

۵۶.۲ یک صورتحساب قدیمی که قسمتی از آن ناخواناست نشان می‌دهد که ۳۶ متر پارچه به قیمت $x۷۳۹y$ تومان خریداری شده است. با فرض آنکه قیمت هر متر پارچه کمتر از صد تومان باشد، ارقام مجهول را پیدا کنید.

حل. چون $x۷۳۹y$ ریال بر ۳۶ بخشپذیر است، $۴ | x۷۳۹y$ و $۹ | x۷۳۹y$. لذا، بنابر (i.۵.۲)، $۹ | ۹y$ و بنابراین y برابر ۲ یا ۶ است. همچنین (ii.۵.۲) ایجاب می‌کند که $۰ (\mathrm{mod}\ ۹) \equiv x+۷+۳+۹+y$. یعنی، $x + y \equiv ۸ (\mathrm{mod}\ ۹)$. چون x و y رقم هستند، داریم $x + y = ۸$. اگر $y = ۲$، آنگاه $x = ۶$، و قیمت هر متر پارچه $\frac{۶۷۳۹٫۲}{۳۶} = ۱۸۷٫۲$ تومان می‌شود که بیشتر از صد تومان است. بنابراین، $y = ۶$ و $x = ۲$ تنها جواب است و قیمت هر متر پارچه $\frac{۲۷۳۹٫۶}{۳۶} = ۷۶٫۱$ تومان بوده است.

۵۷.۲ عدد ۷ رقمی $n = ۷۲x۲۰y۲$ بر ۷۲ بخشپذیر است. x و yهای ممکن را به‌دست آورید.

حل. چون n و ۱۰۰۰ بر ۸ بخشپذیرند، داریم $۰ (\mathrm{mod}\ ۸) \equiv ۱۰y + ۲$، که از آن دو جواب $y = ۳$ یا $y = ۷$ به‌دست می‌آید. چون $۹ | n$، پس مجموع ارقام n بر ۹ بخشپذیر است، لذا $۰ (\mathrm{mod}\ ۹) \equiv x + y + ۴$. اگر $y = ۳$، آنگاه $x = ۲$، و اگر $y = ۷$، آنگاه $x = ۷$.

۵۸.۲ عدد صحیح $n = ۱۳xy۴۵z$ بر ۷۹۲ بخشپذیر است. ارقام x، y، و z را پیدا کنید.

1. Henry 2. Anne Boleyn

حل. داریم $۱۱ \times ۹ \times ۸ = ۷۹۲$. چون $۸|n$، بنابر (۵.۲) داریم $۸|۴۵z$ ، و لذا $z = ۶$. با استدلالی مشابه از $۹|n$ منجر می‌شود $x + y \equiv ۸ (\mathrm{mod}\ ۹)$، و $۱۱|n$ ایجاب می‌کند که $x+y = ۸$.$x - ۶ \equiv ۸ (\mathrm{mod}\ ۱۱)$، یعنی $۱ - ۳ + x - y + ۴ - ۵ + ۶ \equiv ۰ (\mathrm{mod}\ ۱۱)$ لذا و $x - y = ۸$، پس $x = ۸$، $y = ۰$.

مسألهٔ زیر آزمونی نسبتاً ساده برای بخشپذیری بر ۷ به‌دست می‌دهد. شیوهٔ محاسبهٔ چندجمله‌یی که در حل مسأله آمده است معمولاً به روش هورنر[1] موسوم است. این شیوه محاسبه به‌مراتب کارآمدتر از روند ضعیف محاسبهٔ توانهای x، ضرب در ضرایب، و جمع کردن است.

◁ **۵۹.۲** فرض می‌کنیم $N \geq ۱۰$ عددی طبیعی باشد. اولین رقم سمت چپ N را در ۳ ضرب، به پیمانهٔ ۷ ساده، رقم دوم (از سمت چپ) را با آن جمع می‌کنیم. نتیجه را در ۳ ضرب، به پیمانهٔ ۷ ساده، با رقم سوم جمع می‌کنیم. عمل را به این ترتیب ادامه می‌دهیم تا جایی که اولین رقم سمت راست را جمع کنیم. نشان دهید که عدد به‌دست آمده همنهشت با N به پیمانهٔ ۷ است.

حل. فرض کنیم $P(x) = b_۰ x^n + b_۱ x^{n-۱} + \cdots + b_n$. قرار می‌دهیم $y_۰ = b_۰$، $y_۱ = y_۰ x + b_۱$، $y_۲ = y_۱ x + b_۲$، و مانند آن. اثبات تساوی $y_n = P(x)$ دشوار نیست.

اکنون فرض می‌کنیم N دارای بسط دهدهی $a_n ۱۰^n + \cdots + a_۰$ باشد. قرار می‌دهیم $P(x) = a_n x^n + \cdots + a_۰$. در این‌صورت $N = P(۱۰)$، و چون $۱۰ \equiv ۳ (\mathrm{mod}\ ۷)$، لذا بنابر (iii.۳.۲)، $N \equiv P(۳) (\mathrm{mod}\ ۷)$. سرانجام، توجه کنید که روش مذکور در صورت مسأله به آسانی $P(۳)$ را به پیمانهٔ ۷ محاسبه می‌کند.

۶۰.۲ ثابت یا رد کنید: مجموعهٔ $۱^۲$، $۲^۲$، ...، $m^۲$ یک دستگاه کامل مانده‌ها به پیمانهٔ m است.

حل. به آسانی دیده می‌شود که فقط وقتی یک دستگاه کامل مانده‌ها به‌دست می‌آوریم که m مساوی ۱ یا ۲ باشد، زیرا اگر $m > ۲$، آنگاه ۱ همنهشت با $m - ۱$ به پیمانهٔ m نیست، اما $۱^۲ \equiv (m-۱)^۲ (\mathrm{mod}\ m)$. از این‌رو لااقل دو تا از اعداد $۱^۲$، $۲^۲$، ...، $m^۲$، همنهشت با یکدیگرند و بنابراین مجموعه نمی‌تواند دستگاه کامل مانده‌ها باشد.

۶۱.۲ فرض می‌کنیم $r_۱$، ...، r_m یک دستگاه کامل مانده‌ها به پیمانهٔ m باشد. اگر $(a, m) = ۱$، ثابت کنید $ar_۱$، ...، ar_m نیز یک دستگاه کامل مانده‌ها به پیمانهٔ m است.

حل. کافی است ثابت کنیم که هر دو عنصر از مجموعهٔ $\{ar_۱, ar_۲, \ldots, ar_m\}$ به پیمانهٔ m ناهمنهشت هستند. اما اگر $ar_i \equiv ar_j (\mathrm{mod}\ m)$، بنابر (vi.۲.۲) داریم $r_i \equiv r_j (\mathrm{mod}\ m)$،

1. Horner (1786-1837)

و این ممکن نیست مگر $r_i = r_j$ (زیرا r_iها یک دستگاه کامل مانده‌ها به پیمانه m تشکیل می‌دهند).

۶۲.۲ فرض می‌کنیم $(a, m) = ۱$. با کاربرد مسأله قبل نشان دهید که همنهشتی خطی $ax \equiv b \pmod m$ جواب یکتا دارد.

حل. بنابر مسأله قبل $\{۰, a, ۲a, \dots, (m-۱)a\}$ یک دستگاه کامل مانده‌هاست. لذا b با یکی و تنها یکی از عناصر این دستگاه همنهشت است، یعنی یک r یکتا بین ۰ و $m - ۱$ وجود دارد به‌طوری که $ar \equiv b \pmod m$.

۶۳.۲ اگر $a \equiv b \pmod m$، نشان دهید $(a, m) = (b, m)$. آیا عکس این حکم برقرار است؟

حل. اگر $a \equiv b \pmod m$، آنگاه عدد صحیح k وجود دارد به‌طوری که $a = b + km$. لذا بنابر (۲۲.۱)، $(a, m) = (b + km, m) = (b, m)$. عکس مطلب برقرار نیست، مثلاً $(۳, ۵) = ۱ = (۲, ۵)$، ولی $۲ \not\equiv ۳ \pmod ۵$.

در مسأله بعد با ضریبهای دوجمله‌ای سروکار داریم. یادآوری می‌شود که

$$\binom{n}{k} = \frac{n!}{k!(n-۱)!} = \frac{n(n-۱)\cdots(n-k+۱)}{k!}$$

۶۴.۲ فرض می‌کنیم p اول، و $۰ \le n < p$. نشان دهید که $\binom{n+p}{p}$ همنهشت با ۱ به پیمانهٔ p است.

حل. قرار می‌دهیم $N = \binom{n+p}{p}$. با توجه به نکتهٔ بالا

$$n!N = (n+p)(n+p-۱)\cdots(p+۱)$$

اما $n + p \equiv n \pmod p$، $n + p - ۱ \equiv n - ۱ \pmod p$، ... و لذا $(n+p)(n+p-۱)\cdots(p+۱) \equiv n! \pmod p$. در نتیجه $n!N \equiv n! \pmod p$. اما چون $n < p$ و p اول است، $n! \not\equiv ۰ \pmod p$. پس می‌توانیم طرفین همنهشتی را بر $n!$ تقسیم کنیم و لذا $N \equiv ۱ \pmod p$ به‌دست می‌آید.

۶۵.۲ اگر p اول باشد، نشان دهید $\binom{۲p}{p} \equiv ۲ \pmod p$.

حل. اگر $N = \binom{۲p}{p}$، آنگاه $p!N = (۲p)(۲p-۱)\cdots(p+۱)$، یا

$$(۲-۱)!N = ۲(۲p-۱)\cdots(p+۱)$$

داریم $۲p-۱ \equiv p-۱ (\mathrm{mod}\, p)$، $۲p-۲ \equiv p-۲$، ... . در نتیجه

$$(p-۱)!N \equiv ۲(p-۱)! (\mathrm{mod}\, p)$$

یا $N \equiv ۲ (\mathrm{mod}\, p)$.

◃ **۶۶.۲** پیمانهٔ A دقیقاً گنجایش a اونس، و پیمانهٔ B دقیقاً گنجایش b اونس مایع را دارند. a و b نسبت به هم اولند و $a < b$. ظرفی پُر از شربت در اختیار داریم. نشان دهید که به کمک پیمانهٔ A می‌توان تعداد صحیح $x \leq b$ اونس شربت در B پیمانه کرد.

حل. ابتدا نشان می‌دهیم که به‌ازای هر $r < a$، می‌توانیم r اونس پیمانه کنیم. چون q وجود دارد به‌طوری که $x = aq + r$ و $۰ \leq r \leq a-۱$، در نتیجه می‌توان x اونس پیمانه کرد.

روند کار مرحله به مرحله انجام می‌گیرد. فرض کنیم در مرحله‌ای x_k اونس شربت در پیمانهٔ A داشته باشیم. پیمانهٔ B را از ظرف پُر می‌کنیم و پیمانهٔ A را از پیمانهٔ B لبریز می‌کنیم، سپس محتوای A را داخل ظرف شربت می‌ریزیم. به پُرکردنِ A از B و تخلیهٔ A در ظرف ادامه می‌دهیم. پس از مدتی، مقدار باقیمانده در B برای پُرکردن A کافی نیست، با وجود این آن را در A می‌ریزیم. این مقدار را $x_{k+۱}$ می‌نامیم. در این‌صورت آشکار است که به‌ازای nی $b = (a-x_k) + na + x_{k+۱}$. لذا $x_{k+۱} \equiv x_k + b (\mathrm{mod}\, a)$. بنابراین، اگر با وقتی که A خالی است شروع کنیم، مقادیر واقع در A پس از مراحل ۱، ۲، ... با $۱ \times b$، $۲b$، ... به پیمانهٔ a همنهشت خواهند بود. چون a و b نسبت به هم اولند، مجموعهٔ $\{۰ \times b, ۱ \times b, \ldots, (a-۱)b\}$ یک دستگاه کامل مانده‌ها به پیمانهٔ a است. لذا دنبالهٔ $x_۰$، $x_۱$، ...، $x_{a-۱}$ به ترتیبی اعداد ۰، ۱، ...، $a-۱$ را طی می‌کند.

◃ **۶۷.۲** فرض می‌کنیم n عدد صحیح مثبتی غیر از ۱، ۲، ۳، ۴، یا ۶ باشد. ثابت کنید اعداد صحیح a و b با $۱ < a < n-۱$ و $۱ < b < n-۱$ وجود دارند به‌طوری که $ab \equiv -۱ (\mathrm{mod}\, n)$.

حل. کافی است a با $۱ < a < n-۱$ را پیدا کنیم به‌طوری که $(a, n) = ۱$، زیرا در این‌صورت بنابر (۷.۲) همنهشتی $ax \equiv -۱ (\mathrm{mod}\, n)$ جوابی مانند b دارد، و b نمی‌تواند همنهشت ۱ یا $n-۱$ به پیمانهٔ n باشد. اگر $n > ۳$ فرد باشد می‌توان a را برابر ۲ اختیار کرد. اگر $n \geq ۶$ زوج باشد، دو عدد $n-۲$ و $n-۴$ را در نظر می‌گیریم. اگر اعداد $n-۲$ و $n-۴$ هر دو به‌صورت توانی از ۲ باشند، آنگاه $n = ۶$، که خلاف فرض است. لذا لااقل یکی از اعداد صحیح $n-۲$ یا $n-۴$ به‌صورت توانی از ۲ نیست. فرض کنیم $n-۲$ به‌صورت توانی از ۲ نباشد. اگر p مقسوم‌علیه اول فردی از $n-۲$ باشد، آنگاه واضح است که $(p, n) = ۱$. بنابراین p مقدار مناسبی برای a است. با دلیلی مشابه اگر $n-۴$ به‌صورت توانی از ۲ نباشد و p مقسوم‌علیه

اول فردی از $n-۴$ باشد، $(p,۱)=۱$). لذا در این حالت نیز مقدار مناسبی برای a به‌دست می‌آید. (در فصل ۳ که خصوصیتهای اساسی تابع ϕی اویلر بسط داده شد، می‌توان برهان بسیار آسانتری برای این مسأله ارائه داد.)

تمرینهایی برای فصل ۲

۱. یک دستگاه کامل مانده‌ها به پیمانهٔ ۱۱ به‌دست آورید به‌طوری که (الف) عناصرش همگی زوج باشند؛ (ب) همهٔ عناصرش فرد باشند.

۲. آیا $\{۱۱,-۱,۱۲,۸,۳۴,-۳\}$ یک دستگاه کامل مانده‌ها به پیمانهٔ ۶ است؟

۳. کوچکترین ماندهٔ نامنفی $۱!+۲!+\cdots+۵۰۰!$ به پیمانهٔ ۱۸۹ را به‌دست آورید.

۴. باقیماندهٔ $۳۶!/۲۶!$ بر ۱۳ را به‌دست آورید.

۵. کوچکترین ماندهٔ مثبت $۲۶^{۱۰۰۰}$ به پیمانهٔ ۲۹ را به‌دست آورید.

۶. دو رقم سمت راست $۹^{۹۹۹}$ را به‌دست آورید. (به پیمانهٔ $۱۰^۲$ محاسبه کنید.)

۷. سه رقم سمت راست $۷^{۴۹۳}$ را معین کنید. (به پیمانهٔ $۱۰^۳$ محاسبه کنید و نشان دهید $۷^{۲۰}\equiv ۱(\bmod ۱۰۰۰)$.)

۸. نشان دهید $۳^{۹۹۹}-۱)/۲\equiv ۱۳(\bmod ۲۶)$.

۹. درستی یا نادرستی احکام زیر را بررسی کنید: (الف) $۲۲۷|۳^{۳۲}+۸$، (ب) عدد $۵^{۵۳}-۱$ بر ۱۱۷ بخشپذیر است.

۱۰. ثابت کنید $(۳۲۳)^{۱۶۹}+(۱۶۹)^{۳۲۳}$ مضربی از ۱۲ است.

۱۱. باقیماندهٔ $(۲۲)^{۱۵}+(۱۵)^{۲۳}$ را بر ۳۳۰ به‌دست آورید. (راهنمایی: به پیمانهٔ ۲، ۳، ۵، و ۱۱ عمل کنید، سپس قضیهٔ باقیماندهٔ چینی را به‌کار برید.)

۱۲. ثابت کنید به‌ازای هر $n\geq ۱$، $۵^{۲n+۱}+۲^{۸n+۹}$ مضربی از ۱۱ است.

۱۳. حکم زیر را اثبات یا رد کنید: به‌ازای هر $n\geq ۱$، $۳^{۲n+۵}+۲^{۴n+۱}$ مضرب ۷ است.

۱۴. ثابت کنید به‌ازای هر $n\geq ۰$، $۴^{۲n+۱}+۳^{n+۲}\equiv ۰(\bmod ۱۳)$.

۱۵. ثابت کنید به‌ازای هر $n\geq ۱$، $n(۱۳n^۲-۱)$ بر ۶ بخشپذیر است.

۱۶. آیا عدد صحیح مثبتی مانند n وجود دارد به‌طوری که $۷n^۳-۱$ مربع کامل باشد؟

۱۷. اثبات یا رد کنید: عدد اولی مانند $p>۵$ وجود دارد به‌طوری که نه $p^۲-۱$ بر ۱۰ بخشپذیر است و نه $p^۲+۱$.

۱۸. ثابت کنید که حاصلضرب چهار عدد صحیح متوالی بر ۲۴ بخشپذیر است.

۱۹. اگر $۳a^۲-۲b^۲=۱$، نشان دهید که $a^۲-b^۲$ بر ۴۰ بخشپذیر است.

۲۰. رقم مجهول را پیدا کنید $۱۹۲۹۲۱x۵۰۶۴ = ۱۱۰۱۲ \times ۱۷۵۱۹۲۲$.

۲۱. اگر $۵۳x۰y۷۴z$ بر ۲۶۴ بخشپذیر باشد، ارقام x، y، و z را تعیین کنید.

۲۲. وارونهای زیر را پیدا کنید (الف) ۷ به پیمانهٔ ۲۶؛ (ب) ۱۳ به پیمانهٔ ۳۷؛ (ج) ۵ به پیمانهٔ ۳۱.

۲۳. همهٔ جوابهای $۵۱x \equiv ۶۶ \pmod{۱۰۵}$ را به‌دست آورید.

۲۴. کلیهٔ جوابهای $۴۴x \equiv ۷۶ \pmod{۱۰۴}$ را به‌دست آورید.

۲۵. شیوهٔ ضرب بیان‌شده در تکنیک ۳ قبل از (۱۰.۲) را برای حل $۲۶۳x \equiv ۳۱۷۵ \pmod{۹۹۰۱}$ به‌کار برید. (۹۹۰۱ اول است.)

۲۶. به‌ازای چه مقادیر صحیح مثبت a کمتر از ۱۰۸ همنهشتی $۳۰x \equiv a \pmod{۱۰۸}$ حلپذیر است؟

۲۷. همنهشتیهای زیر را حل کنید: (الف) $۳۷x \equiv ۲۰ \pmod{۷۳}$؛ (ب) $۱۹x \equiv ۲ \pmod{۹۷}$؛ (ج) $۲۴x \equiv ۳۰ \pmod{۵۴}$.

۲۸. به‌ازای چه مقادیر صحیح مثبت m همنهشتی $۲۵ \equiv ۹۷ \pmod{m}$ برقرار است؟

۲۹. در صورت وجود، همهٔ جوابهای $۲۸x \equiv ۶ \pmod{۷۰}$ را به‌دست آورید.

۳۰. کمترین ماندهٔ مثبت همهٔ جوابهای زیر را به‌دست آورید،

(الف) $۱۱x \equiv ۳ \pmod{۳۲}$؛

(ب) $۷x \equiv ۱۹ \pmod{۳۷}$؛

(ج) $۱۸x \equiv ۱۲ \pmod{۹۰}$.

۳۱. کوچکترین دو عدد صحیح مثبتی را پیدا کنید که در تقسیم آنها بر ۷، ۱۱، و ۱۳ باقیمانده‌هایشان به‌ترتیب ۲، ۳، و ۴ باشند.

۳۲. باکاربرد قضیهٔ باقیماندهٔ چینی جوابی از همنهشتیهای زیر به‌دست آورید: $x \equiv ۲ \pmod{۶}$، $x \equiv ۶ \pmod{۱۱}$، $x \equiv ۴ \pmod{۱۷}$.

۳۳. کوچکترین دو عدد صحیح مثبتی را پیدا کنید که در تقسیم بر ۴، ۷، و ۹ به‌ترتیب دارای باقیمانده‌های ۲، ۵، و ۶ باشند.

۳۴. همهٔ جوابهای دستگاه زیر را پیدا کنید: $x \equiv ۳۴ \pmod{۱۰۵}$، $x \equiv ۷۹ \pmod{۳۳۰}$.

۳۵. کوچکترین چهار عدد صحیح مثبتی را پیدا کنید که در تقسیم بر ۹، ۱۰، و ۱۱ به‌ترتیب دارای باقیمانده‌های ۳، ۵، و ۷ باشند.

۳۶. دستگاه همنهشتهای زیر را حل کنید: $۵x \equiv ۲ \pmod{۹}$، $۲x \equiv ۵ \pmod{۱۳}$، $۳x \equiv ۷ \pmod{۱۷}$.

۳۷. با استفاده از قضیهٔ باقیماندهٔ چینی $۲۹x \equiv ۷ \pmod{۱۴۳۰}$ را حل کنید.

۳۸. (چین ۱۳۷۲ میلادی) تعدادی سکه را می‌توان به‌صورت ۷۸ حلقه (گروه) با اندازه‌های برابر مرتب کرد. برای آنکه ۷۷ حلقه با اندازه‌های برابر به‌دست آوریم به ۵۰ سکهٔ دیگر نیاز داریم. کمترین تعداد سکهٔ مورد نیاز چقدر است؟

۳۹. فرض کنید r تعداد عوامل اول متمایز m باشد. نشان دهید دقیقاً 2^r عدد صحیح x وجود دارند به‌طوری که $0 \leq x < m$ و $x^2 \equiv x \pmod{m}$.

۴۰. فرض کنید که حاصلضرب دو عدد فرد متوالی n باشد. مقادیر ممکن برای آخرین «رقم» n در نمایش آن در مبنای ۱۶ چه هستند؟ معمولاً در مبنای ۱۶ ارقام به‌صورت ۰، ۱، ۲، ...، ۹، A، B، C، D، E، F هستند . (راهنمایی: فرض کنید اعداد فرد بر صورت $2k-1$ و $2k+1$ باشند، و به پیمانهٔ ۱۶ عمل کنید.)

۴۱. نشان دهید که معادلهٔ $x^2 + xy - y^2 = 3$ جواب صحیح ندارد. (راهنمایی: معادله را نسبت به x حل کنید، و نشان دهید عبارت زیر علامت ریشهٔ دوم نمی‌تواند مربع باشد.)

۴۲. اگر a و b دو عدد صحیح مثبت و نسبت به هم اول باشند، آنگاه معادلهٔ $ax+by=1$ جواب دارد. این مطلب را با تکمیل زیر به تفصیل ثابت کنید (اویلر، ۱۷۶۰)؛ وقتی $x = 0, 1, 2, \ldots, b-1$) $1 + ax$ بر b تقسیم شود باقیمانده‌های متمایز ارائه می‌شوند، لذا باقیمانده‌ها به‌ترتیبی عبارت‌اند از ۰، ۱، ...، $b-1$. لذا x با $0 \leq x \leq b-1$ وجود دارد به‌طوری که $b \mid 1 + ax$.

۴۳. کریستف کلمب[1] در دوازدهم اکتبر ۱۴۹۲ در دنیای جدید[2] پیاده شد. این کار در چه روزی از هفته صورت گرفته است؟ (توجه کنید که تاریخ ارائه‌شده در تقویم یولیایی است.)

۴۴. کارل فریدریش گاوس در سی‌ام آوریل ۱۷۷۷ به دنیا آمد، و پیر فرما در هفدهم اوتِ ۱۶۰۱، این تاریخها در چه روزی از هفته بوده‌اند؟

۴۵. آبراهام لینکلن[3] در شب چهاردهم آوریل ۱۸۶۵ در تئاتر فورد مورد اصابت گلوله قرار گرفت و صبح روز بعد درگذشت. ثابت کنید که لینکلن در شنبه فوت کرده است.

۴۶. مگنا کارتا[4] (فرمان مشروطیت در انگلستان) در پانزدهم ژوئن ۱۲۱۵ امضا شد. معین کنید که در چه روزی از هفته اتفاق افتاده است.

ملاحظاتی برای فصل ۲

یک روند جبری در همنهشتیها. فرض کنیم m یک عدد صحیح مثبت ثابتی باشد. علامت $\equiv$ که گاوس آن را به‌عنوانِ اختصاری برای «همنهشت است با» انتخاب کرده است ما را وادار می‌کند

1. Christopher Columbus 2. New World 3. Abraham Lincoln 4. Magna Carta

تا به همنهشتی به پیمانهٔ m به‌عنوان نوعی تساوی بنگریم. از آنجا که در این بحث m ثابت خواهد بود، به‌جای $a \equiv b(\bmod m)$ می‌نویسیم $a \equiv b$ تا ارتباط نزدیک بین همنهشتی و تساوی را با وضوح بیشتری به‌دست دهیم.

اکنون اگر به (i.۲.۲) تا (iv.۲.۲) برگردیم، می‌توانیم دریابیم که این روابط حاکی از آن هستند که همنهشتی به پیمانهٔ m واجد بسیاری از خصوصیتهای آشنای تساوی است. اما در حالی‌که بی‌نهایت عدد صحیح وجود دارد، تنها m عدد صحیح واقعاً «متفاوت» به پیمانهٔ m وجود دارند. در محاسباتی که شامل جمع و ضرب به پیمانهٔ m هستند، می‌توان عدد صحیح b را جانشین عدد صحیح a کرد به شرطی که $a \equiv b(\bmod m)$.

چون هر عدد صحیح با یکی از اعداد ۰، ۱، ...، $m-1$ همنهشت به پیمانهٔ m است، یک مجموعهٔ مناسب اسامی برای m شیء متفاوت عبارت است از $[0]_m$، $[1]_m$، ...، $[m-1]_m$. این نمادها بسیار بد قواره هستند؛ یک مجموعه از اسامی بهتر ۰، ۱، ...، $m-1$ است. در این نمادگذاری ساده خطراتی وجود دارد. مثلاً، $[4]_3$ واجد ویژگیهایی است که با ویژگیهای $[5]_3$ بسیار تفاوت دارند، لذا اگر هر دو را ۳ بخوانیم مشکلات جدی ایجاد می‌شود. به‌ویژه، اگر همزمان در حال کار با چند پیمانه باشیم، این نمادگذاری سردرگمی وحشتناکی ایجاد می‌کند. اما اگر فقط به یک پیمانهٔ m سروکار داشته باشیم، این نمادگذاری مزایایی دارد.

درگردایهٔ $\{0, 1, \ldots, m-1\}$ از اشیاء مجرد، دو عمل «جمع» و «ضرب» را چنین تعریف می‌کنیم: «مجموع» i و j باقیماندهٔ عدد $i+j$ بر m است و «حاصلضرب» i و j باقیماندهٔ ij بر m. اغلب این دو عمل جمع به پیمانهٔ m و ضرب به پیمانهٔ m نامیده می‌شوند.

مثلاً، حالت $m = 12$ را در نظر می‌گیریم؛ لذا $3 + 8 = 7 + 8 = 0$، $4 + 8 = 2$، $10 \times 5 = 0$، 4×3، و مانند آن. گاهی محاسبه به پیمانهٔ ۱۲ «حساب ساعت» نامیده می‌شود. اگر عقربهٔ ساعت‌شمار ابتدا ۷ ساعت و سپس ۸ ساعت حرکت کند نتیجهٔ نهایی آن ۳ ساعت حرکت کردن است اگر به تعداد ۱۰ بار و هر بار ۵ ساعت به جلو برده شود نتیجهٔ نهایی آن ۲ ساعت جلو بردن است.

جمع و ضرب به پیمانهٔ m تعدادی ویژگی مشترک با جمع و ضرب معمولی دارند. در آنچه می‌آید، $+$ نشانگر جمع به پیمانهٔ m، و $\times$ نشانگر ضرب به پیمانهٔ m است. (معمولاً نقطه حذف می‌شود.) متغیرهای x، y، و z مجموعهٔ $\{0, 1, \ldots, m-1\}$ را اختیار می‌کنند.

(i) به‌ازای هر x، y، و z، $x + (y + z) = (x + y) + z$.

(ii) یک شیء n، که همان جمعی نامیده می‌شود، وجود دارد به‌طوری که به‌ازای هر x، $x + n = n + x = x$. (روشن است که ۰ همان خود شیء است.)

(iii) به‌ازای هر x، یک y وجود دارد به‌طوری که $x + y = y + x = ۰$. این y وارون جمعی x خوانده می‌شود. روشن است که وارون جمعی ۰ برابر ۰ است، و اگر $۰ < x < m$، وارون جمعی x برابر $m - x$ است.

هر مجموعهٔ G با یک عمل جمع $+$ که در ویژگیهای (i)، (ii)، و (iii) صدق کند یک گروه نامیده می‌شود. مثلاً، مجموعهٔ $\{۰, ۱, \ldots, m - ۱\}$ یک گروه نسبت به عمل جمع به پیمانهٔ m است. یک مثال دیگر نظریهٔ اعدادی $\{r_۱, r_۲, \ldots, r_k\}$ است که در آن r_iها اعدادی در بازهٔ $۰ \leq x < m$ هستند که با m متباینند و عمل همان ضرب به پیمانهٔ m است. بررسی ویژگیهای (i) و (ii) آسان است، و ویژگی (iii) از (۸.۲) نتیجه می‌شود. مثالهای گروهی مهمی در تقریباً هر زمینهٔ ریاضی وجود دارند.

اشیاء ۰، ۱، ۲، ...، $m - ۱$ در عمل جمع به پیمانهٔ m در ویژگی زیر نیز صدق می‌کنند:

(iv) به‌ازای هر x و y، $x + y = y + x$.

گروههایی که در ویژگی (iv) صدق کنند، به نام ریاضیدان نروژی قرن نوزدهم نیلس آبل[1] (۱۸۲۹ـ۱۸۰۲)، گروههای آبلی نامیده می‌شوند.

ضرب به پیمانهٔ m با ضرب معمولی دارای ویژگیهای مشترک زیر است:

(v) به‌ازای هر x، y، و z، $(xy)x = x(yz)$.

(vi) به‌ازای هر x، y، و z، $x(y + z) = xy + xz$، و $(y + z)x = yx + zx$. یک مجموعهٔ R با جمع و ضربی که در ویژگیهای (i)ـ(iv) صدق کند یک حلقه نامیده می‌شود. علاوه بر این اگر

(vii) شییء e در R، که همانی ضربی نامیده می‌شود، وجود داشته باشد به‌طوری که به‌ازای هر x، $ex = xe = x$ و

(viii) به‌ازای هر x و y، $xy = yx$،

آنگاه R یک حلقهٔ تعویضپذیر واحددار خوانده می‌شود.

به‌ازای هر $m > ۱$ مجموعهٔ $\{۰, ۱, \ldots, m - ۱\}$ نسبت به اعمال جمع و ضرب به پیمانهٔ m یک حلقهٔ تعویضپذیر است. (شییء به‌کار رفته در (vii) همان شییء ۱ است.)

فرض کنیم R یک حلقهٔ تعویضپذیر واحددار باشد. اگر به‌ازای هر عنصر $x \neq ۰$ یک شییء y وجود داشته باشد به‌طوری که $xy = e$، آنگاه R یک میدان خوانده می‌شود. شییء (یکتای) y به‌طوری که $xy = e$ وارون ضربی x نامیده می‌شود. یک مثال آشنا و مهم برای میدان مجموعهٔ اعداد حقیقی، با جمع و ضرب معمولی است؛ در اینجا وارون x عدد $۱/x$ است. مثالهای دیگر

1. Niels Abel

شامل اعداد گویا و اعداد مختلط هستند.

در حالت کلی اشیاء ۰، ۱، ...، $m-1$ نسبت به اعمال جمع و ضرب به پیمانهٔ m تشکیل میدان نمی‌دهند، زیرا اگر $0 < x < m$، آنگاه لزوماً yی وجود ندارد که $xy = 1$ (یعنی $xy \equiv 1 \pmod{m}$). در واقع، چنین yی دقیقاً همان چیزی است که به‌عنوان وارون x به پیمانهٔ m تعریف کردیم، و اگر $(x, m) > 1$، آنگاه وارون x به پیمانهٔ m وجود ندارد. مجموعهٔ $\{0, 1, \ldots, m-1\}$ نسبت به اعمال جمع و ضرب به پیمانهٔ m یک میدان است اگر و تنها اگر m اول باشد.

شرح مختصری از زندگینامه‌ها

چین چیوشائو در ۱۲۰۲ در ناحیهٔ تسه‌چوان[1] متولد شد، بعد از تحصیلاتش در نجوم، به یک شغل نظامی گماشته شد. پس از آن، علی‌رغم اتهامات مکرر به رشوه‌خواری، یک رشته شغلهای اجرایی پذیرفت. چین به بسیاری از چیزها علاقه داشت ــ نجوم، ریاضیات، شعر، تیراندازی، شمشیربازی.

در ۱۲۴۷، شو-شو چیو-چانگ[2] را به چاپ رساند («رسالهٔ ریاضی در نه بخش»). این کتاب شامل یک رشته مسائل حل شده است، که بسیاری از آنها پیچیدگی قابل توجه دارند. چین دستگاههای معادلات خطی را به آسانی بررسی می‌کند و می‌داند که چگونه تقریبهای خوب به صفر چندجمله‌ییها را محاسبه کند. چین ده مسأله طرح و حل نموده است که به دستگاههای همنهشتیهای خطی یک متغیره منجر می‌شوند. وجود این قبیل مسائل در نوشته‌های چینی به زمان سون-تسو[3] (سدهٔ سوم) برمی‌گردد. اما گردایهٔ چین به‌درستی خارج از مسائل مطرح‌شده به‌وسیلهٔ پیشینیانش است. راه‌حلهایش روشن می‌سازند که وی صاحب یک روش کلی بوده است.

چین چیوشائو، احتمالاً در ۱۲۶۱، در ایالت کوانگ‌تونگ[4] درگذشته است.

کارل فردریش گاوس. در ۱۷۷۷ در شهر آلمانی برونسویک (براوفشوایک) متولد شد. گرچه با تنگدستی نسبی بزرگ شد، ولی به‌زودی استعدادهای ذهنی عظیم او آشکار شد. در ۱۷۹۵، قضیهٔ اعداد اول و قانون تقابل مربعی را حدس زده و روش کمترین مربعات را کشف کرده بود، در ۱۷۹۶، با مشخص کردن چندضلعیهای منتظمی که می‌توان آنها را با ستاره و پرگار رسم کرد، تکلیف یک مسألهٔ ۲۰۰۰ ساله را تعیین کرد. در ۱۷۹۸، اولین اثبات قضیهٔ اصلی جبر (اینکه هر چندجمله‌یی غیرثابت با ضرایب مختلط دارای یک صفر در اعداد مختلط است) را ارائه داد. در ۱۸۰۱ کتاب تحقیقات حسابی او پدید آمد. علاوه بر معرفی مفهوم همنهشتی و نشان دادن

1. Szechwan 2. Shu-shu chiu-chang 3. Sun-Tzu 4. Kuangtung

سودمندی آن در نظریهٔ مقدماتی اعداد، کتاب اولین اثبات قانون تقابل مربعی و پیشرفتهای اساسی در تحلیل صورتهای درجهٔ دوم را ارائه می‌دهد.

در ۱۸۰۱، گاوس مدار سیارک سِرس[1] را، که به مدت کوتاهی مشاهده و سپس ناپدید شده بود، محاسبه کرد. با استفاده از محاسبات گاوس مجدداً سرس را در ۱۸۰۲ یافتند، و این موفقیت بزرگ به گاوس شهرت جهانی بخشید. در ۱۸۰۷، گاوس استاد نجوم و مدیر رصدخانهٔ گوتینگن گردید. در آنجا به خلق آثار بنیادی در نظریهٔ اعداد، آنالیز، نظریهٔ احتمال و بسیاری از شاخه‌های دیگر ریاضی پرداخت. همزمان، به انجام کارهای بزرگ در نجوم، مکانیک سماوی، الکترومغناطیس، نورشناسی، مکانیک و زمین‌سنجی مشغول بود.

گاوس در ۲۳ فوریه ۱۸۵۵ در گوتینگن بدرود حیات گفت. به اعتراف تمامی جهانیان، او بزرگترین ریاضیدان زمان خود، و بلکه تمام اعصار بوده است.

لئوناردو پیسایی (فیبوناتچی). در ۱۱۷۵ در شهر پیسا (در ایتالیا) متولد شد. در حدود سال ۱۱۹۲، پدرش به پایگاه تجارتی در الجزیره فرستاده شد. لئوناردو به او پیوست و در آنجا آموخت که چگونه با نمادهای هندی ـ عربی محاسبه کند. در سفرهای تجارتی بعدی به مصر، سوریه، سیسیل و جاهای دیگر، تماسهای زیادی با دانشمندان مسلمان داشت. در ۱۲۰۲، لیبرآباکی (کتاب حساب) را به چاپ رساند. این کتاب شامل شرحی از نمادهای هندسی ـ عربی است، و نیز شامل تعداد زیادی معماست، از جمله مسألهٔ مشهور خرگوشها که به پیدایش دنباله‌ای که اکنون دنبالهٔ فیبوناتچی نامیده می‌شود منجر شد. لئوناردو تعداد دیگری کتاب نوشت. از دیدگاه ریاضی، عمیقترین آنها لیبر کوادراتورم (کتاب مجذورات) (۱۲۲۵) است، که قضیه‌های جالبی در معادلات دیوفانتی درجهٔ دوم دارد.

در ۱۲۴۰، پیسا از فرزند مشهورش قدردانی کرد و یک مقرری سالانه به لئوناردو دانشمند بزرگ «Master Leonardo Bigallo» اعطا کرد. بعد از این تاریخ چیزی دربارهٔ لئوناردو معلوم نیست.

مراجع

Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke, Yale University Press, New Haven, Connecticut, 1966.

اثرگذارترین کتاب در نظریهٔ اعداد که تا آن زمان نوشته شده بود در سال ۱۸۰۱ به چاپ رسید، وقتی که مؤلف ۲۴ ساله بود. در تحقیقات (کتاب تحقیقات حسابی) گاوس تعریف نوین همنهشتی و مانده‌ها و نیز نماد $\equiv$ را معرفی می‌کند. این کتاب اولین بیان و اثبات قضیهٔ اصلی حساب، بحث

1. Ceres

مفصلی از همنهشتیهای خطی، نخستین برهان کامل قانون تقابل مربعی، (که در فصل ۵ به آن اشاره می‌کنیم) و بحث جامعی از ریشه‌های اولیه (رک. فصل ۶) را در بردارد. تمام این مطالب در ربع اول کتاب قرار دارند. بیشتر مطالب باقیمانده به یک بررسی تفصیلی و عمیق از صورتهای درجهٔ دوم اختصاص دارد.

گاوس مباحث پایه‌یی را موجز و دقیق تنظیم کرده است، و مطالعهٔ قسمت اول کتاب به‌طور شگفت‌آوری ساده نوشته شده است.

Donald E. Knuth, *The Art of Computer Programming Volume 2.*

(فصل اول را ببینید)

Ulrich Libbrecht, *Chinese Mathematics in the Thirteenth Century*, The MIT Press, Cambridge, Massachusetts, 1973.

این کتاب اصولاً در مورد کتاب بسیار با نفوذ شوـشو چیوـچانگ از چین چیوشائو بحث می‌کند. لیبرخت در حدود ۲۰۰ صفحه را به تاریخچهٔ قضیهٔ باقیماندهٔ چینی، با توجه خاص به سهم چینیها، اختصاص داده است.

۳

قضیه‌های فرما، اویلر، و ویلسن

اولین اشاره به قضیهٔ فرما در نوشته‌های اروپایی در ژوئن ۱۶۴۰ در نامه‌ای از پییر فرما[1] به مارَن مِرسِن[2]، راهب فرقهٔ فرانسیسیان[3] بود. در آن نامه، فرما ادعا می‌کند که اگر p عدد اولی باشد، $۲^p - ۲$ مضربی از $۲p$ است، و اگر q مقسوم‌علیه اولی از $۲^p - ۱$ باشد، $q - ۱$ مضربی از p است. فرما در نامه‌ای به تاریخ ۱۸ اکتبر ۱۶۴۰ به فِرنیکل دو بِسی[4] (۱۶۷۵ـ۱۶۰۵)، پاریسی علاقه‌مند به اعداد، ادعا می‌کند که اگر p عددی اول و a عددی طبیعی باشد، عدد صحیحی مانند n وجود دارد به‌طوری که p عدد $a^n - ۱$ را می‌شمارد، و کوچکترین مقدار n که در این شرط صدق کند عدد $p - ۱$ را می‌شمارد.

فرما در نامه‌اش به فرنیکل می‌نویسد که اثباتی در نظر دارد و اگر نگران طولانی شدن آن نباشد آن را برای او خواهد فرستاد. متأسفانه، فرما اصولاً برهان قضیه‌های خود را افشا نمی‌کرد. برای این نوع رفتار یک سنت طولانی وجود داشت؛ ریاضیدانان یکدیگر را در مسائل به چالش می‌طلبیدند

1. Pierre Fermat 2. Marin Mersenne 3. Franciscan 4. Frenicle de Bessy

و بنابراین از افشای روش خاصی که ممکن بود یافته باشند تنفر داشتند. این رسم در زمان فرما در حال از بین رفتن بود، و چند سال بعد، ظهور مجله‌های علمی شروع شد.

حوالی سال ۱۶۸۰ لایپنیتس[1] قضیهٔ فرما را اثبات کرد، ولی این اثبات در میان دستنوشته‌هایش رها شده بود تا اینکه در ۱۸۶۳ آشکار شد. پس از فرما، نظریهٔ اعداد دستخوش یک دورهٔ طولانی توقف قرارگرفت. در ۱۷۳۰ به همت اویلر[2] نظریهٔ اعداد دوباره احیا شد، اویلر مجدداً قضیهٔ فرما را کشف کرد، اثباتی بر پایهٔ قضیهٔ دوجمله‌یی برای آن در ۱۷۳۶ انتشار داد، و در ۱۷۵۸ برهان جبری‌تری که خود آن را ترجیح می‌داد به چاپ رسانید، اثباتی که به سرعت به تعمیم قضیه برای پیمانه‌های مرکب منجر شد که ما آن را قضیهٔ اویلر می‌نامیم.

قضیهٔ ویلسن[3] می‌گوید که اگر p اول باشد، $(p-1)!+1$ بر p بخشپذیر است. قضیهٔ ویلسن برای اولین بار در ۱۷۷۰ توسط ریاضیدان انگلیسی ادوارد وئرینگ[4] (۱۷۹۸ـ۱۷۳۴) به چاپ رسید. او به دانشجوی سابق خود جان ویلسن اعتبار بخشید، اگر چه در واقع این قضیه یک صد سال جلوتر در نوشته‌های لایپنیتس منعکس شده بود. لایپنیتس اظهار می‌دارد که اگر p اول باشد، p عدد $(p-2)!-1$ را می‌شمارد، اما به آسانی می‌توان نشان داد که این دو صورت هم‌ارزند.

وئرینگ نوشته است که او نتوانسته است این قضیه را ثابت کند و اثبات بایستی خیلی مشکل باشد زیرا نمادی برای اعداد اول وجود ندارد. منظور او این بوده است که چون «فرمولی» برای اعداد اول وجود ندارد، او نتوانسته است برهانی ارائه دهد؛ تنها اثباتی که او می‌توانسته تصور کند کارهای نمادی بوده است. (گاوس[5] با بیان گزنده‌ای نوشته است که حقایق از این نوع بایستی از مفاهیم استنباط شوند نه از نمادها.) اولین اثباتی را که به چاپ رسیده لاگرانژ[6] در ۱۷۷۱ داده است. برهان لاگرانژ شامل کارهای نسبتاً پیچیده‌ای روی چندجمله‌یی $(x+1)(x+2)\dots(x+p-1)$ است. در ۱۷۷۳، اویلر اثباتی با کاربرد ریشه‌های اولیه ارائه داده است. یک برهان ساده‌تر ادراکی (که اساساً با برهان چاپ‌شدهٔ لایپنیتس یکی است) توسط گاوس در تحقیقات حسابی بنیادی داده شده است.

قضیه‌هایی برای فصل ۳

قضیهٔ فرما و قضیهٔ ویلسن

برهان قضیهٔ فرما را که در (۶.۳) ارائه می‌دهیم منتسب به دیریکله است. این اثبات صورت ضعیفی از برهان گاوس از قضیهٔ ویلسن است و این برتری را دارد که همزمان اثباتهای قضیهٔ فرما، قضیهٔ ویلسن، و اطلاعاتی در مورد همنهشتی $x^2 \equiv a \pmod{p}$ را که در فصل ۵ به‌طور نظام‌مند به آن می‌پردازیم، به‌دست می‌دهد. به لم زیر نیاز داریم.

1. Leibniz 2. Euler 3. Wilson 4. Edward waring 5. Gauss 6. Lagrange

(۱.۳) لم. فرض می‌کنیم p عدد اول فردی باشد و $p \nmid a$. اگر عددی مانند b وجود داشته باشد به‌طوری که $b^2 \equiv a \pmod{p}$، آنگاه همنهشتی $x^2 \equiv a \pmod{p}$ دقیقاً دو جواب ناهمنهشت به پیمانهٔ p دارد.

برهان. حداقل دو جواب ناهمنهشت وجود دارد، زیرا $(-b)^2 \equiv a \pmod{p}$ و چون $p \neq 2$، $b \not\equiv -b \pmod{p}$. برای آنکه نشان دهیم فقط دو جواب ناهمنهشت وجود دارد، فرض می‌کنیم $x^2 \equiv a \pmod{p}$. در این‌صورت $x^2 \equiv b^2 \pmod{p}$، لذا $p \mid x^2 - b^2$، و بنابراین $p \mid (x-b)(x+b)$. لذا $p \mid x-b$ یا $p \mid x+b$. در حالت اول $x \equiv b \pmod{p}$، و در حالت دوم $x \equiv -b \pmod{p}$.

به‌طور غیررسمی، (۱.۳) می‌گوید که اگر p عدد اول فردی باشد و عدد a یک «ریشهٔ دوم» به پیمانهٔ p داشته باشد، آنگاه a دقیقاً دو ریشهٔ دوم به پیمانهٔ p دارد.

(۲.۳) قضیهٔ (دیریکله، ۱۸۲۸). فرض کنیم p اول باشد، و فرض می‌کنیم $1 \leq a \leq p-1$. اگر همنهشتی $x^2 \equiv a \pmod{p}$ دارای جواب نباشد، آنگاه $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$. اگر همنهشتی جواب داشته باشد، آنگاه $(p-1)! \equiv -a^{(p-1)/2} \pmod{p}$.

برهان. برای $p = 2$ قضیه واضح است، لذا فرض می‌کنیم p فرد باشد. اگر $1 \leq m \leq p-1$، آنگاه بنابر (۸.۲) عدد یکتای n وجود دارد به‌طوری که $1 \leq n \leq p-1$ و $mn \equiv a \pmod{p}$. m و n را اعداد متناظر می‌نامیم. اگر $x^2 \equiv a \pmod{p}$ جوابی نداشته باشد، آنگاه برای اعداد متناظر m و n داریم $m \neq n$. بنابراین می‌توانیم اعداد ۱ تا $p-1$ را به‌صورت $(p-1)/2$ جفت متناظر تبدیل کنیم. حاصلضرب جفتهای متناظر از یک طرف همنهشت با $a^{(p-1)/2}$ به پیمانهٔ p است و از طرف دیگر آشکارا برابر است با $(p-1)!$. لذا $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$.

اگر $x^2 \equiv a \pmod{p}$ حلپذیر باشد، جوابی مانند b دارد به‌طوری که $1 \leq b \leq p-1$. تنها جواب دیگر در این فاصله $p-b$ است. $p-3$ عدد باقیمانده از ۱ تا $p-1$ را به‌صورت جفتهای متناظر مرتب می‌کنیم؛ در این‌صورت حاصلضربشان همنهشت با $a^{(p-3)/2} \pmod{p}$ است. حاصلضرب دو عدد باقیمانده یعنی b و $p-b$ همنهشت با $-a \pmod{p}$ است. لذا $(p-1)! \equiv (-a)a^{(p-3)/2} = -a^{(p-1)/2} \pmod{p}$.

یک نتیجهٔ مهم قضیهٔ دیریکله قضیهٔ ویلسن است. لاگرانژ اثبات تا اندازه‌ای پیچیده‌ای را در ۱۷۷۱ ارائه داده است، ولی قضیهٔ ویلسن به آسانی از (۲.۳) نتیجه می‌شود.

(۳.۳) قضیهٔ ویلسن. اگر p اول باشد، آنگاه $(p-1)! \equiv -1 \pmod{p}$.

برهان. در (۲.۳) قرار می‌دهیم $a = ۱$. مسلماً $x^۲ \equiv ۱ (\mathrm{mod}\, p)$ جواب دارد، لذا $(p-۱)! \equiv -۱^{(p-۱)/۲} \equiv -۱ (\mathrm{mod}\, p)$.

توضیح. عکس قضیهٔ ویلسن نیز برقرار است (مسألهٔ ۳ـ۲۲ را ببینید). بنابراین قضیهٔ ویلسن یک آزمون اول بودن را ارائه می‌دهد، هر چند که قویاً غیر عملی است. اگر n عدد بزرگی مثلاً به بزرگی تقریبی $۱۰^{۱۰۰}$ باشد، به نظر می‌رسد که هیچ روند معقولی برای محاسبهٔ مستقیم باقیماندهٔ تقسیم $(n-۱)!$ بر n وجود نداشته باشد.

به‌عنوان نتیجهٔ آسانی از (۲.۳) و قضیهٔ ویلسن، مشخصهٔ مفید زیر را برای وقتی که همنهشتی $x^۲ \equiv a (\mathrm{mod}\, p)$ دارای جواب باشد داریم.

(۴.۳) ملاک اویلر. فرض کنیم p اول و $p \nmid a$. در این‌صورت $x^۲ \equiv a (\mathrm{mod}\, p)$ حلپذیر است یا حلپذیر نیست برحسب آنکه $a^{(p-۱)/۲} \equiv ۱ (\mathrm{mod}\, p)$ یا $a^{(p-۱)/۲} \equiv -۱ (\mathrm{mod}\, p)$.

برهان. فرض می‌کنیم همنهشتی دارای جوابی باشد. بنابر (۲.۳) و قضیهٔ ویلسن. $-a^{(p-۱)/۲} (\mathrm{mod}\, p) \equiv -۱$، و از ضرب طرفین در -۱ نتیجه به‌دست می‌آید. اگر همنهشتی هیچ جواب نداشته باشد استدلال به همین صورت است.

قضیهٔ مهم زیر نتیجهٔ بلافصل ملاک اویلر است.

(۵.۳) قضیه. فرض کنیم p یک عدد اول فرد باشد. همنهشتی $x^۲ \equiv -۱ (\mathrm{mod}\, p)$ جواب دارد اگر p به‌صورت $۴k+۱$ و جواب ندارد هر گاه p به‌صورت $۴k+۳$ باشد.

اکنون به بیان قضیهٔ فرما می‌پردازیم. این قضیه یکی از قضیه‌هایی اساسی نظریهٔ مقدماتی اعداد است و اغلب در برهانها و محاسبات آتی به‌کار خواهد رفت.

(۶.۳) قضیهٔ فرما. اگر p اول و $p \nmid a$، آنگاه $a^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$. یا هم‌ارز با آن، اگر a هر عدد صحیحی باشد، آنگاه $a^p \equiv a (\mathrm{mod}\, p)$.

برهان. بنابر ملاک اویلر $a^{(p-۱)/۲} \equiv \pm ۱ (\mathrm{mod}\, p)$. طرفین همنهشتی را به توان ۲ می‌رسانیم. صورت دیگر قضیهٔ فرما اگر $a \equiv ۰ (\mathrm{mod}\, p)$ بدیهی است و در غیر این‌صورت از ضرب a در $a^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$ به‌دست می‌آید.

توضیح ۱. یک روش مستقیم‌تر برای قضیهٔ فرما کاربرد استدلالی است که در برهان قضیهٔ اویلر (۱۳.۳) به‌کار می‌رود. بنابراین اغلب قضیهٔ فرما را نتیجهٔ بلافصل قضیهٔ اویلر می‌شمارند برای

اثبات قضیهٔ فرما توسط اویلر در ۱۷۵۸ به توضیح ۲ در انتهای این فصل مراجعه کنید.

توضیح ۲. عکس قضیهٔ فرما برقرار نیست: حتی اگر $a^{m-1} \equiv 1 \pmod{m}$ به‌ازای هر a که با m متباین است برقرار باشد لزومی ندارد که m اول باشد (مسائل ۳۹.۳ و ۴۰.۳ را ببینید). یک عکس صحیح از قضیهٔ فرما در مسألهٔ ۵۵.۳ و نیز در فصل ۶ آمده است (قضیهٔ ۹.۶ را ببینید).

می‌توانیم به‌طور حدسی دلیل فرما را برای این ادعا که $2p \mid 2^p - 2$ بازسازی کنیم. در زمانی جلوتر، شاید در ۱۶۳۶، فرما اتحادی برای ضرایب دوجمله‌یی کشف کرده بود که می‌توان آن را به زبان امروزی چنین نوشت $n\binom{n+m-1}{m-1} = m\binom{n+m-1}{m}$. این اتحاد نتیجهٔ سادهٔ فرمول ضرایب دوجمله‌یی برحسب فاکتوریلهاست، اما پاسکال ضرایب دوجمله‌ای را تا ۱۶۵۴ به‌طور نظام‌مند کشف نکرده بود. بنابر اتحاد فرما می‌توان به استقرا ثابت کرد که اگر p اول و $1 \le k \le p-1$، آنگاه $p \mid \binom{p}{k}$. بنابر قضیهٔ دوجمله‌یی داریم

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p-1} + 1,$$

و در نتیجه $2^p - 2$ بر p بخشپذیر است. از آنجا که $2^p - 2$ بر ۲ نیز بخشپذیر است، قضیهٔ فرما برای اعداد اول فرد p ثابت می‌شود.

می‌توان استدلال مشابه را برای اثبات اینکه اگر p اول باشد، آنگاه $a^p - a$ بر p بخشپذیر است به‌کار برد (مسألهٔ ۱۴.۳ را ببینید)، اما طرز بیان گزارهٔ اصلی فرما از قضیه‌اش اشاره بر آن دارد که ممکن است از یک روش ادراکی‌تر نظیر آنچه که اویلر در ۱۷۵۸ در اثبات قضیهٔ فرما به‌کار برد، استفاده کرده باشد. (به توضیحات انتهای این فصل برای یک توضیح مختصر مراجعه کنید.)

در قضیه‌های ۸.۳ و ۹.۳ باقی ادعای سال ۱۶۴۰ فرما را اثبات می‌کنیم. ابتدا به یک لم نیاز داریم که در جاهای دیگر نیز کاربرد دارد.

(۷.۳) لم. فرض کنیم a، u، و v اعداد صحیح باشند به‌طوری که $u > 0$ و $v > 0$، و فرض می‌کنیم $(u,v) = d$ و $m > 0$. اگر $a^u \equiv 1 \pmod{m}$ و $a^v \equiv 1 \pmod{m}$، آنگاه $a^d \equiv 1 \pmod{m}$.

برهان. بنابر (۵.۱) می‌توان d را به‌صورت یک ترکیب خطی از u و v نوشت، مثلاً $d = su + tv$. یکی از اعداد s و t مثبت خواهد بود. بدون آنکه به کلیت استدلال خللی وارد آید فرض می‌کنیم $t \le 0$، لذا $su = d + |t|v$. پس $(a^u)^s = a^d (a^v)^{|t|}$. چون $a^u \equiv a^v \equiv 1 \pmod{m}$، در نتیجه $a^d \equiv 1 \pmod{m}$.

(۸.۳) قضیه. فرض کنیم q یک عامل اول $۲^p - ۱$ باشد که در آن p عدد اولی است فرد. در این‌صورت q به‌صورت $۲kp + ۱$ است.

برهان. بنابر قضیهٔ فرما $۲^{q-۱} \equiv ۱ (\mathrm{mod}\, p)$، و بنابه فرض $۲^p \equiv ۱ (\mathrm{mod}\, p)$. لذا، اگر $d = (p, q-۱)$، آنگاه بنابر (۷.۳)، $۲^d \equiv ۱ (\mathrm{mod}\, q)$. اما چون p اول است پس یا $d = ۱$ یا $d = p$. اگر $d = ۱$، آنگاه $۲^۱ \equiv ۱ (\mathrm{mod}\, q)$ که یک تناقض است. پس $d = p$، و لذا $p|q-۱$. از طرفی چون $۲^p - ۱$ فرد است پس q نیز فرد و لذا $q - ۱$ زوج است. در نتیجه $۲p|q-۱$، و بنابراین $q \equiv ۱ (\mathrm{mod}\, ۲p)$، یعنی q به‌صورت $۲kp + ۱$ است.

قضیهٔ بالا را می‌توان برای بررسی اول بودن $۲^p - ۱$ به‌کار برد (فصل ۷، مسائل ۱۵.۷ و ۱۹.۷ را ببینید).

(۹.۳) قضیه. فرض می‌کنیم p اول باشد $p \nmid a$. اگر n کوچکترین عدد طبیعی باشد به‌طوری که $p|a^n - ۱$ (بنابر قضیهٔ فرما چنین nی وجود دارد.) آنگاه $n|p-۱$.

برهان. بنابر قضیهٔ فرما $a^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$. اگر $d = (n, p-۱)$، آنگاه بنابر (۳.۷)، $a^d \equiv ۱ (\mathrm{mod}\, p)$. چون n کوچکترین عدد طبیعی است که $p|a^n - ۱$، در نتیجه $d = n$ و لذا $n|p-۱$.

قضیهٔ اویلر و تابع ϕی اویلر

طبیعی است که سؤال شود آیا مشابه قضیهٔ فرما برای وقتی که پیمانه اول نیست برقرار است؟ پاسخ آری است. اویلر یک تعمیم مناسب پیدا کرده و در ۱۷۶۰ اثباتی از آن را به چاپ رسانده است. در همان مقاله، اویلر به بررسی ویژگیهای اساسی تابع ϕ، که کلید تنظیم این تعمیم است، پرداخته است.

(۱۰.۳) تعریف. اگر $m > ۱$، $\phi(m)$ را تعداد اعداد طبیعی کوچکتر از m و متباین با m می‌گیریم. $\phi(۱)$ را برابر ۱ تعریف می‌کنیم. تابع ϕ که به این ترتیب تعریف می‌شود معمولاً تابع ϕی اویلر نامیده می‌شود.

آشکار است که به‌ازای هر $m \geq ۱$، $\phi(m) \leq m - ۱$. همچنین، $\phi(m) = m - ۱$ اگر و تنها اگر m اول باشد. (تمرین ۵۹.۳ را ببینید.)

(۱۱.۳) تعریف. فرض کنیم m عددی طبیعی باشد. یک دستگاه مخفف مانده‌ها به پیمانهٔ m مجموعه‌ای از اعداد صحیح است به‌طوری که هر عددِ متباین با m با یک عنصر یکتا از مجموعه

همنهشت به پیمانهٔ m است. در آنچه می‌آید د.م.م را به‌عنوان مختصر دستگاه مخفف مانده‌ها به‌کار می‌بریم.

از آنجا که هر دو دستگاه مخفف مانده‌ها به پیمانهٔ m دارای یک تعداد عنصر هستند، همهٔ آنها $\phi(m)$ عنصر دارند. معمولاً (ولی نه همیشه) عناصر یک دستگاه مخفف مانده‌ها به پیمانهٔ m را اعداد طبیعی کوچکتر از m که با m متباین هستند اختیار می‌کنیم. به ویژه، اگر p اول باشد، مجموعهٔ ۱، ۲، ...، $p-1$ یک دستگاه مخفف مانده‌ها به پیمانهٔ p است.

(۱۲.۳) لم. اگر r_1، r_2، ...، r_k یک د.م.م به پیمانهٔ m باشد و $(a,m)=1$، آنگاه ar_1، ar_2، ...، ar_k نیز یک د.م.م به پیمانهٔ m است.

برهان. باید نشان دهیم که هیچ دو عنصر از دنبالهٔ ar_1، ar_2، ...، ar_k با هم به پیمانهٔ m همنهشت نیستند و اینکه به‌ازای $1 \le i \le k$، $(ar_i, m)=1$. فرض کنیم که اعداد i و j وجود داشته باشند به‌طوری که $i \neq j$ و $ar_i \equiv ar_j \pmod m$. چون $(a,m)=1$ بنابر (vi.۲.۲) داریم $r_i \equiv r_j \pmod m$ و این با تعریف r_1، r_2، ...، r_k به‌عنوان یک د.م.م تناقض دارد. همچنین، چون به‌ازای هر i، $(r_i,m)=1$ و $(a,m)=1$، در نتیجه بنابر (۱۰.۱) داریم $(ar_i,m)=1$. بنابراین ar_1، ar_2، ...، ar_k مجموعه‌ای از k عدد صحیح تا همنهشت که هر یک نسبت به m اول است، و لذا یک د.م.م به پیمانهٔ m می‌سازند.

اکنون برای اثبات قضیهٔ اویلر مهیا هستیم. برهان ارائه‌شدهٔ در بالا برای قضیهٔ فرما را می‌توان تعدیل کرد تا برای پیمانهٔ مرکب کارساز باشد، ولی استدلال زیر شسته‌ورفته‌تر است. این برهان در ابتدا توسط آیوری[1] در ۱۸۰۴ برای اثبات قضیهٔ فرما به‌کار رفته است و در ۱۸۲۶ هورنر آن را تعدیل کرده تا قضیهٔ اویلر را به‌دست آورد.

(۱۳.۳) قضیهٔ اویلر. اگر m عددی طبیعی و $(a,m)=1$، آنگاه $a^{\phi(m)} \equiv 1 \pmod m$.

برهان. فرض کنیم r_1، r_2، ...، $r_{\phi(m)}$ یک د.م.م به پیمانهٔ m باشد. بنابر لم قبل ar_1، ar_2، ...، $ar_{\phi(m)}$ نیز یک د.م.م به پیمانهٔ m است. لذا داریم

$$(ar_1)(ar_2)\dots(ar_{\phi(m)}) \equiv r_1 r_2 \dots r_{\phi(m)} \pmod m .$$

از آنجا که ar_1، ar_2، ...، $ar_{\phi(m)}$ یک د.م.م به پیمانهٔ m است هریک از عناصرش به ترتیبی با یکی از عناصر r_1، r_2، ...، $r_{\phi(m)}$ همنهشت است. لذا

1. Ivory

$(r_i, m) = ۱$ چون به‌ازای هر r_i داریم $a^{\phi(m)} r_۱ r_۲ \dots r_{\phi(m)} \equiv r_۱ r_۲ \dots r_{\phi(m)} (\mathrm{mod}\, m)$. پس $(r_۱ r_۲ \dots r_{\phi(m)}, m) = ۱$ و در نتیجه بنابر (vi.۲.۲)، $a^{\phi(m)} \equiv ۱ (\mathrm{mod}\, m)$.

توضیح. از قضیهٔ اویلر به آسانی نتیجه می‌شود که اگر $(a, m) = ۱$، آنگاه $a^{\phi(m)-۱}$ وارون ضربی a به پیمانهٔ m است.

در استفاده از قضیهٔ اویلر، ابتدا بایستی $\phi(m)$ را مشخص کنیم. اگر تجزیهٔ m به عوامل اول معلوم باشد، یک روش مؤثر برای محاسبهٔ $\phi(m)$ کاربرد این حقیقت است که ϕ ضربی است. در این‌صورت به‌دست آوردن یک فرمول برای $\phi(m)$ برحسب تجزیهٔ m مطلب آسانی است.

ابتدا نشان می‌دهیم که ϕ یک تابع ضربی است. برهان کاربرد قشنگی از قضیهٔ باقیماندهٔ چینی است.

(۱۴.۳) قضیه. اگر $(m, n) = ۱$، آنگاه $\phi(mn) = \phi(m)\phi(n)$.

برهان. برای $۰ \le x < mn$، فرض کنیم x_m باقیماندهٔ تقسیم x بر m و x_n باقیماندهٔ تقسیم x بر n باشند. اعداد متمایز در فاصلهٔ ۰ تا $mn - ۱$ دارای جفت باقیمانده‌های متمایز هستند. زیرا اگر $x_m = y_m$ و $x_n = y_n$، آنگاه $x \equiv y (\mathrm{mod}\, m)$ و $x \equiv y (\mathrm{mod}\, n)$؛ و چون $(m, n) = ۱$. پس $x \equiv y (\mathrm{mod}\, mn)$ و این ممکن نیست زیرا اعداد ۰ تا $mn - ۱$ یک د.ک.م. به پیمانهٔ mn است. لذا برای هر $۰ \le x < mn$ یک جفت یکتا x_m و x_n متناظر است. اما mn عدد در فاصلهٔ $۰ \le x < mn$ و mn جفت a، b با $۰ \le a < m$ و $۰ \le b < n$ وجود دارند. لذا هر جفت a، b به‌ازای xی برابر جفت x_m و x_n است.

چون $x \equiv x_m (\mathrm{mod}\, m)$، پس $(x, m) = (x_m, m)$. با استدلالی مشابه $(x, n) = (x_n, n)$. لذا، بنابر (۱۰.۱)، $(x, mn) = ۱$ اگر و تنها اگر $(x_m, m) = ۱$ و $(x_n, n) = ۱$. چون $\phi(m)\phi(n)$ طریق برای انتخاب جفت a، b با $(a, m) = (b, n) = ۱$ و $\phi(mn)$ طریق برای انتخاب $x_{a,b}$ که با mn متباین باشد (بنابر تعریف ϕ) وجود دارند، در نتیجه $\phi(mn) = \phi(m)\phi(n)$.

توضیح. بند اول برهان بالا نشان می‌دهد که اگر $(m, n) = ۱$، آنگاه به‌ازای هر a، b، یک x یکتا در فاصلهٔ $۰ \le x < mn$ وجود دارد به‌طوری که $x \equiv a (\mathrm{mod}\, m)$ و $x \equiv b (\mathrm{mod}\, n)$، که اثبات قضیهٔ باقیماندهٔ چینی برای یک جفت همنهشتی است. قضیهٔ باقیماندهٔ چینی برای k همنهشتی را دقیقاً به همین روش می‌توان با ملاحظهٔ kـتاییهای باقیمانده اثبات کرد. ولی، اثبات

ارائه‌شده در فصل ۲ آموزنده‌تر است، زیرا یک روش عملی برای یافتن جواب یک دستگاه از همنهشتیهای خطی را به‌دست می‌دهد.

(۱۵.۳) لم. اگر p اول باشد، آنگاه برای هر $k \geq ۱$ داریم

$$\phi(p^k) = p^k - p^{k-۱} = p^{k-۱}(p-۱) = p^k\left(۱ - \frac{۱}{p}\right)$$

برهان. فرض کنیم $a < p^k$ و a با p^k متباین نباشد؛ در این‌صورت a بر p بخشپذیر است و لذا $a = mp$، که در آن $۱ \leq m \leq p^{k-۱}$. آشکار است که دقیقاً $p^{k-۱}$ انتخاب برای a وجود دارد. لذا $p^k - p^{k-۱}$ عدد صحیح کمتر از p^k و متباین با آن وجود دارد.

(۱۶.۳) قضیه. اگر $m = p_۱^{m_۱}p_۲^{m_۲}\cdots p_r^{m_r}$. آنگاه

$$\begin{aligned}\phi(m) &= (p_۱^{m_۱} - p_۱^{m_۱-۱})(p_۲^{m_۲} - p_۲^{m_۲-۱})\cdots(p_r^{m_r} - p_r^{m_r-۱}) \\ &= p_۱^{m_۱-۱}p_۲^{m_۲-۱}\cdots p_r^{m_r-۱}(p_۱-۱)(p_۲-۱)\cdots(p_r-۱) \\ &= m(۱ - ۱/p_۱)(۱ - ۱/p_۲)\cdots(۱ - ۱/p_r)\end{aligned}$$

برهان. چون ϕ ضربی است و $p_i^{m_i}$ها دوبه‌دو متباین هستند، معادلهٔ اول از (۱۵.۳) نتیجه می‌شود. دو معادلهٔ دیگر صورتهای سادهٔ اولی هستند.

مسأله‌ها و راه‌حلها

قضیهٔ فرما و قضیهٔ ویلسن

۱.۳ عدد n، $۰ \leq n \leq ۱۶$، را بیابید به‌طوری که $n \equiv ۳^{۱۰۰} \pmod{۱۷}$.

حل. بنابر قضیهٔ فرما $۳^{۱۶} \equiv ۱ \pmod{۱۷}$. لذا $۳^{۱۰۰} = ۳^{۹۶} \times ۳^۴ \pmod{۱۷}$. اما $۳^۴ \equiv ۱۳ \pmod{۱۷}$، پس $n = ۱۳$.

۲.۳ باقیماندهٔ تقسیم اعداد زیر را بر ۳۷ به‌دست آورید: (الف) $۲^{۵۲}$، (ب) $۲^{۷۰}$.

حل. (الف) بنابر قضیهٔ فرما $۲^{۳۶} \equiv ۱ \pmod{۳۷}$، لذا $۲^{۵۲} = ۲^{۳۶} \times ۲^{۱۶} \equiv ۲^{۱۶} \pmod{۳۷}$. اکنون کافی است $۲^{۱۶}$ را به پیمانهٔ ۳۷ با مربع‌کردنهای مکرر به پیمانهٔ ۳۷ محاسبه کنیم.

$$۲^۲ \equiv ۴, ۲^۴ \equiv ۱۶, ۲^۸ \equiv (۱۶)^۲ \equiv -۳, ۲^{۱۶} \equiv ۹ \pmod{۳۷},$$

لذا باقیماندهٔ $۲^{۵۲}$ بر ۳۷ برابر ۹ است.

(ب) با استفاده از (الف) و قضیهٔ فرما داریم

$$۲^{۷۰} = ۲^{۳۶} \times ۲^{۳۴} \equiv ۲^{۳۴} \equiv ۲^{۳۲} \times ۲^{۲} \equiv (۲^{۱۶})^{۲} \times ۴ \equiv ۹^{۲} \times ۴ \equiv ۷ \times ۴ (\mathrm{mod}\ ۳۷),$$

لذا باقیماندهٔ $۲^{۷۰}$ بر ۳۷ برابر ۲۸ است.

۳.۳ باقیماندهٔ $۵۵^{۱۴۲}$ بر ۱۴۳ چقدر است؟

حل. داریم $۱۳ \times ۱۱ = ۱۴۳$، پس ۵۵ و ۱۴۳ نسبت به هم اول نیستند و لذا نمی‌توان از ابتدا به پیمانهٔ ۱۴۳ از قضیهٔ اویلر استفاده کرد. روشن است که داریم $۵۵^{۱۴۲} \equiv ۰ (\mathrm{mod}\ ۱۱)$ (۱) از طرفی $۵۵ \equiv ۳ (\mathrm{mod}\ ۱۳)$ و لذا بنابر قضیهٔ فرما

$$(۵۵)^{۱۴۲} \equiv ۳^{۱۴۲} \equiv (۳^{۱۲})^{۱۱} \times ۳^{۱۰} \equiv ۳^{۱۰} (\mathrm{mod}\ ۱۳)$$

اما

$$۳^{۲} \equiv ۹ \equiv -۴, ۳^{۴} \equiv ۱۶ \equiv ۳, ۳^{۸} \equiv ۹ \equiv -۴, ۳^{۱۰} \equiv ۱۶ \equiv ۳ (\mathrm{mod}\ ۱۳)$$

لذا $(۵۵)^{۱۴۲} \equiv ۳ (\mathrm{mod}\ ۱۳)$ (۲). حال، با توجه به (۱) و (۲) به کوچکترین عدد طبیعی نیاز داریم که مضرب ۱۱ بوده و باقیمانده‌اش بر ۱۳ برابر ۳ باشد. با تجسس یا کاربرد قضیهٔ باقیماندهٔ چینی جواب ۵۵ است.

۴.۳ باقیماندهٔ تقسیم $۱۲^{۴۵} \times ۱۳$ را بر ۴۷ به‌دست آورید.

حل. بنابر قضیهٔ فرما $۱۲^{۴۶} \equiv ۱ (\mathrm{mod}\ ۴۷)$. با ضرب دو طرف این همنهشتی در ۴ و با توجه به $۴۸ \equiv ۱ (\mathrm{mod}\ ۴۷)$، داریم $(۱۲)^{۴۵} \equiv ۴ (\mathrm{mod}\ ۴۷)$. در نتیجه $۱۲^{۴۵} \times ۱۳ \equiv ۵۲ \equiv ۵ (\mathrm{mod}\ ۴۷)$. پس باقیماندهٔ مورد نظر برابر ۵ است.

۵.۳ نشان دهید $(۵۵۵۵)^{۲۲۲۲} + (۲۲۲۲)^{۵۵۵۵}$ بر ۷ بخشپذیر است.

حل. $۵۵۵۵ \equiv ۴ (\mathrm{mod}\ ۷)$، $۲۲۲۲ \equiv ۳ (\mathrm{mod}\ ۷)$. پس کافی است ثابت کنیم $۴^{۲۲۲۲} + ۳^{۵۵۵۵}$ بر ۷ بخشپذیر است. از طرفی باقیمانده‌های ۲۲۲۲ و ۵۵۵۵ بر ۶ به ترتیب ۲ و ۵ است. پس بنابر قضیهٔ فرما $۴^{۲۲۲۲} + ۳^{۵۵۵۵} = ۴^{۲} + ۳^{۵} (\mathrm{mod}\ ۷)$ اما

$$۴^{۲} \equiv ۱۶ \equiv ۲, ۳^{۲} \equiv ۹ \equiv ۲, ۳^{۴} \equiv ۴, ۳^{۵} \equiv ۱۲ \equiv ۵ (\mathrm{mod}\ ۷)$$

لذا $۴^{۲} + ۳^{۵} \equiv ۲ + ۵ = ۰ (\mathrm{mod}\ ۷)$.

۶.۳ ثابت کنید به‌ازای هر عدد صحیح نامنفی n، عبارت $۳^{۶n} - ۲^{۶n}$ مضرب ۳۵ است.

حل. بنابر قضیهٔ فرما یا هر روش دیگر داریم $(۳^۶)^n \equiv ۱ (\mathrm{mod}\, ۷)$ و $(۲^۶)^n \equiv ۱ (\mathrm{mod}\, ۷)$، لذا $۷ | ۳^{۶n} - ۲^{۶n}$. چون $-۳ \equiv -۳ (\mathrm{mod}\, ۵) \equiv ۲$، پس $۳^{۶n} \equiv (-۳)^{۶n} \equiv ۲^{۶n} (\mathrm{mod}\, ۵)$ لذا $۵ | ۳^{۶n} - ۲^{۶n}$ و چون $(۵, ۷) = ۱$، داریم $۳۵ | ۳^{۶n} - ۲^{۶n}$.

۷.۳ ثابت کنید به‌ازای هر عدد طبیعی n، عدد $۱^n + ۲^n + ۳^n + ۴^n$ مضرب ۵ است اگر و تنها اگر n مضرب ۴ نباشد.

حل. فرض کنیم $n = ۴q + r$ که در آن $۰ \leq r \leq ۳$. اگر $a \not\equiv ۰ (\mathrm{mod}\, ۵)$، آنگاه بنابر قضیهٔ فرما داریم $a^n = (a^۴)^q a^r \equiv a^r (\mathrm{mod}\, ۵)$. لذا

$$۱^n + ۲^n + ۳^n + ۴^n \equiv ۱^r + ۲^r + ۳^r + ۴^r (\mathrm{mod}\, ۵)$$

اگر n مضربی از ۴ باشد، آنگاه $r = ۰$ و $۱^r + ۲^r + ۳^r + ۴^r = ۴$، و لذا ۵ عدد $۱^n + ۲^n + ۳^n + ۴^n$ را نمی‌شمارد. اگر $۴ \nmid n$، آنگاه $r = ۱, ۲$ یا ۳. اکنون به‌ازای این مقادیر r به آسانی ثابت می‌شود که $۱^r + ۲^r + ۳^r + ۴^r$ بر ۵ بخشپذیر است.

۸.۳ فرض کنید $S_k = ۱^k + ۲^k + \cdots + (p-۱)^k$، که در آن p عدد اولی است فرد. اگر $p - ۱ | k$، ثابت کنید $S_k \equiv -۱ (\mathrm{mod}\, p)$.

حل. بنابر قضیهٔ فرما به‌ازای $۱ \leq t \leq p - ۱$ داریم $t^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$، و چون $p - ۱ | k$، پس $t^k \equiv ۱ (\mathrm{mod}\, p)$. لذا به پیمانه p، مجموع $p - ۱$ عدد ۱ است.

۹.۳ اگر n عددی صحیح باشد، ثابت کنید $n^۵/۵ + n^۳/۳ + ۷n/۱۵$ نیز عددی صحیح است.

حل. داریم $n^۵/۵ + n^۳/۳ + ۷n/۱۵ = (۳n^۵ + ۵n^۳ + ۷n)/۱۵$. لذا کافی است ثابت کنیم که به‌ازای جمیع مقادیر n، $۳n^۵ + ۵n^۳ + ۷n$ بر ۳ و ۵ و در نتیجه بر ۱۵ بخشپذیر است. با استفاده از قضیهٔ فرما داریم $n^۵ \equiv n (\mathrm{mod}\, ۵)$، لذا $۳n^۵ \equiv ۳n (\mathrm{mod}\, ۱۵)$؛ $n^۳ \equiv n (\mathrm{mod}\, ۳)$، لذا $۵n^۳ \equiv ۵n (\mathrm{mod}\, ۱۵)$. در نتیجه

$$۳n^۵ + ۵n^۳ + ۷n \equiv ۳n + ۵n + ۷n \equiv ۰ (\mathrm{mod}\, ۱۵)$$

۱۰.۳ با استفاده از قضیهٔ فرما همنهشتی $x^{۳۵}+۵x^{۱۹}+۱۱x^{۳}\equiv ۰ \pmod{۱۷}$ را حل کنید.

حل. بنابر قضیهٔ فرما به‌ازای هر x، $x^{۱۷}\equiv x \pmod{۱۷}$، و لذا

$$x^{۳۵}\equiv x(x^{۱۷})^{۲}\equiv x^{۳} \pmod{۱۷}$$

با استدلالی مشابه، $۵x^{۱۹}\equiv ۵x^{۳} \pmod{۱۷}$. لذا به‌ازای هر x، داریم

$$x^{۳۵}+۵x^{۱۹}+۱۱x^{۳}\equiv ۱۷x^{۳}\equiv ۰ \pmod{۱۷}$$

بنابراین معادلهٔ اصلی به‌ازای هر x برقرار است.

۱۱.۳ همنهشتی $۳۰۴x^{۳۰۳}+۲۰۴x^{۲۰۲}-۱۰۴x^{۱۰۱}\equiv ۰ \pmod{۱۰۱}$ را به یک همنهشتی درجهٔ ۳ بدل کرده و همهٔ جوابهای آن را پیدا کنید. (توجه کنید که ۱.۱ اول است.)

حل. بنابر قضیهٔ فرما به‌ازای هر x، $x^{۱۰۱}\equiv x \pmod{۱۰۱}$. لذا معادلهٔ اصلی به معادلهٔ هم‌ارز $x^{۳}+۲x^{۲}-۳x\equiv ۰ \pmod{۱۰۱}$ یا $x(x-۱)(x+۳)\equiv ۰ \pmod{۱۰۱}$ بدل می‌شود. بنابراین همهٔ جوابها اعدادی هستند همنهشت با ۰، ۱، یا -۳ به پیمانهٔ ۱۰۱.

۱۲.۳ فرض کنید p اول و $a^{p}+b^{p}=c^{p}$. ثابت کنید $p|a+b-c$.

حل. بنابر قضیهٔ فرما، $a^{p}+b^{p}-c^{p}\equiv a+b-c \pmod{p}$. لذا اگر $a^{p}+b^{p}=c^{p}$، $a+b-c\equiv ۰ \pmod{p}$.

۱۳.۳ فرض کنید p و q دو عدد اول فرد باشند به‌طوری که $p-۱|q-۱$. اگر $(a,pq)=۱$، ثابت کنید $a^{q-۱}\equiv ۱ \pmod{pq}$.

حل. بنابر قضیهٔ فرما $a^{q-۱}\equiv ۱ \pmod{q}$ (۱). باید نشان دهیم که $a^{q-۱}\equiv ۱ \pmod{p}$ نیز برقرار است. چون p و q نسبت به هم اول‌اند، در نتیجه $a^{q-۱}\equiv ۱ \pmod{pq}$. فرض می‌کنیم $q-۱=k(p-۱)$. در این‌صورت $a^{q-۱}=(a^{p-۱})^{k}\equiv ۱^{k} \pmod{p}$.

◁ **۱۴.۳** فرض کنید p اول باشد. به کمک بسط دوجمله‌یی $(a+b)^{p}$، نشان دهید که $(a+b)^{p}\equiv a^{p}+b^{p} \pmod{p}$. از قضیهٔ فرما استفاده نکنید.

حل. بنابر قضیهٔ دوجمله‌یی داریم $(a+b)^{p}=\sum_{k=۰}^{p}\binom{p}{k}a^{p-k}b^{k}$. لذا

$$(a+b)^{p}-(a^{p}+b^{p})=\sum_{k=۱}^{p-۱}\binom{p}{k}a^{p-k}b^{k}$$

اما $\binom{p}{k}$ برای $1 \le k \le p-1$ مضرب p است. زیرا مثلاً $k!(p-k)!\binom{p}{k} = p!$ روشن است که p طرف چپ را می‌شمارد و چون هیچ‌کدام از $(p-k)!$ و $k!$ بر p بخشپذیر نیستند، پس $p|\binom{p}{k}$. در نتیجه $(a+b)^p - (a^p + b^p)$ مجموع جمله‌هایی است که هر یک بر p بخشپذیر است، و لذا اثبات مسأله تمام می‌شود.

توضیح. در مسألهٔ فوق فرض می‌کنیم $b = 1$. در این صورت $(a+1)^p \equiv a^p + 1 \pmod p$. لذا اگر قبلاً می‌دانستیم که $a^p \equiv a \pmod p$، نتیجه می‌گرفتیم که $(a+1)^p \equiv a+1 \pmod p$. این تساوی مرحلهٔ استقرائی را در نخستین برهان منتشر شده قضیهٔ فرما را به‌دست می‌دهد (اویلر، ۱۷۳۶).

۱۵.۳ با استفاده از قضیهٔ فرما ثابت کنید که هر عدد اول $p > 5$ تعداد نامتناهی عدد به‌صورت ۹۹ ... ۹۹۹ را می‌شمارد.

حل. هم‌ارز با این مسأله چنین است: به‌ازای هر عدد اول $p > 5$، رابطهٔ $10^n \equiv 1 \pmod p$ برای تعداد نامتناهی n برقرار است. چون ۱۰ و p نسبت به‌هم اول‌اند، داریم $10^{p-1} \equiv 1 \pmod p$، لذا هر عدد طبیعی n که مضرب $p-1$ باشد دارای ویژگی مورد نظر است.

◁ **۱۶.۳** اگر $n|2^n - 1$، ثابت کنید $n = 1$. (راهنمایی: اگر $n > 1$، فرض کنید p کوچکترین مقسوم‌علیه اول n باشد، و (۷.۳) را به‌کار برید.)

حل. فرض کنید $n > 1$ و $n|2^n - 1$، و فرض می‌کنیم p کوچکترین مقسوم‌علیه اول n باشد. بنابر قضیهٔ فرما داریم $2^{p-1} \equiv 1 \pmod p$. چون $p|n$ و $n|2^n - 1$ پس $2^n \equiv 1 \pmod p$. فرض کنیم $d = (n, p-1)$. اگر $d > 1$، آنگاه n مقسوم‌علیهی بزرگتر از ۱ و کوچکتر از p دارد و این با انتخاب p تناقض دارد. پس $d = 1$. اما بنابر (۷.۳)، $2^d \equiv 1 \pmod p$، یا $2^1 \equiv 1 \pmod p$ که ممکن نیست.

۱۷.۳ (الف) اعداد ۲، ۳، ...، ۱۷ را به‌صورت جفتهای $\{x, y\}$ مرتب کنید به‌طوری که $xy \equiv 1 \pmod{19}$. (ب) با استفاده از (الف) کوچکترین باقیماندهٔ تقسیم ۱۸! بر ۱۹ را به‌دست آورید.

حل. (الف) این جفتها عبارت‌اند از $\{2, 10\}$، $\{17, 9\}$، $\{3, 13\}$، $\{16, 6\}$، $\{4, 5\}$، $\{15, 14\}$، $\{7, 11\}$، و $\{12, 8\}$. (جفتهای $\{x, y\}$ و $\{19-x, 19-y\}$ درکنار هم قرار داده شده‌اند، زیرا با ملاحظهٔ اینکه $ab \equiv 1$ ایجاب می‌کند $(-a)(-b) \equiv 1$ کار را می‌توان نصف کرد.)

(ب) با توجه به (الف) و حاصلضرب جفتها که برابر با ۱ همنهشت ۱۹ هستند داریم $۱۸! \equiv ۱۸ (\mathrm{mod}\ ۱۹)$

۱۸.۳ اگر p عدد اول فردی باشد، ثابت کنید $۲(p-۳)! \equiv -۱ (\mathrm{mod}\, p)$. باقیماندهٔ تقسیم $۵۶!$ را بر ۵۹ به‌دست آورید.

حل. بنابر قضیهٔ ویلسن

$$-۱ \equiv (p-۱)! \equiv (p-۱)(p-۲)(p-۳)! \equiv (-۱)(-۲)(p-۳)! (\mathrm{mod}\, p)$$

به‌ویژه $۲(۵۶)! \equiv -۱ \equiv ۵۸ (\mathrm{mod}\, ۵۹)$، و لذا باقیمانده برابر ۲۹ است.

۱۹.۳ باقیماندهٔ تقسیم $۹۰!$ بر ۹۷ را به‌دست آورید.

حل. بنابر قضیهٔ ویلسن داریم $۹۶! \equiv -۱ (\mathrm{mod}\ ۹۷)$. به جای اینکه از ۱ به جلو برویم از ۹۶ به عقب می‌رویم. برای اینکه اعداد را کوچک نگاه داریم از واقعیت $-x \equiv ۹۷ - x (\mathrm{mod}\ ۹۷)$ استفاده می‌کنیم. لذا

$$۹۶ \times ۹۵ \times \cdots \times ۹۱ \times ۹۰! \equiv (-۱)(-۲) \cdots (-۶) \times ۹۰! (\mathrm{mod}\ ۹۷) \equiv -۱ (\mathrm{mod}\ ۹۷)$$

اما $۶!$. لذا $۵۶! \equiv ۴۱ \equiv -۵۶ (\mathrm{mod}\ ۹۷)$. حال اگر باقیماندهٔ تقسیم $۹۰!$ بر ۹۷ برابر x باشد داریم $۹۰! \equiv x (\mathrm{mod}\ ۹۷)$. لذا $۵۶x \equiv ۵۶ \times ۹۰! \equiv ۱ (\mathrm{mod}\ ۹۷)$. بالاخره از حل این معادله از راه الگوریتم اقلیدسی $x = ۲۶$ به‌دست می‌آید.

۲۰.۳ اگر $y = ۸۲!/۲۱$، باقیماندهٔ تقسیم y بر ۸۳ را به‌دست آورید.

حل. بنابه قضیهٔ ویلسن $۲۱y = ۸۲! \equiv -۱ (\mathrm{mod}\, ۸۳)$. لذا $۸۴y \equiv -۴ (\mathrm{mod}\, ۸۳)$ یا $y \equiv -۴ (\mathrm{mod}\, ۸۳)$. پس باقیماندهٔ تقسیم y بر ۸۳ برابر -۴ یا ۷۹ است.

۲۱.۳ باقیماندهٔ تقسیم $۱۸!$ را بر ۴۳۷ به‌دست آورید. (ابتدا ۴۳۷ را تجزیه کنید.)

حل. داریم $۴۳۷ = ۱۹ \times ۲۳$. چون $۱۸! \equiv -۱ (\mathrm{mod}\ ۱۹)$ پس کافی است باقیماندهٔ $۱۸!$ بر ۲۳ را حساب کنیم. بنابر قضیهٔ ویلسن داریم $۲۲! \equiv -۱ (\mathrm{mod}\ ۲۳)$. اما

$$۲۲ \times ۲۱ \times ۲۰ \times ۱۹ \equiv -۱(-۲)(-۳)(-۴) \equiv ۲۴ \equiv ۱ (\mathrm{mod}\ ۲۳)$$

لذا $۱۸! \equiv -۱ (\mathrm{mod}\ ۲۳)$. در نتیجه $۱۸! \equiv -۱ (\mathrm{mod}\ ۴۳۷)$. پس باقیمانده برابر -۱ یا ۴۳۶ است.

۲۲.۳ عکس قضیهٔ ویلسن را ثابت کنید: اگر $m > ۱$ و m اول نباشد، آنگاه $(m-۱)! \not\equiv -۱ (\mathrm{mod}\, m)$.

حل. چون m اول نیست پس مقسوم‌علیهی مانند t دارد که $۱ < t < m$. واضح است که $t|(m-۱)!$. حال اگر $(m-۱)! \equiv -۱ (\mathrm{mod}\, m)$، آنگاه $t|-۱$ که ممکن نیست.

توضیح. می‌توانیم قضیهٔ قویتری را ثابت کنیم. ملاحظه می‌کنیم که $(۱-۴)! \equiv ۲ (\mathrm{mod}\, ۴)$. حال ثابت می‌کنیم که اگر $m > ۴$ مرکب باشد، آنگاه $(m-۱)! \equiv ۰ (\mathrm{mod}\, m)$. چون m مرکب است پس مثلاً $m = pq$ به‌طوری که $۱ < p \le q < m$. دو حالت در نظر می‌گیریم. حالت اول $p < q$ در این‌صورت به‌وضوح $p, q|(m-۱)!$ و لذا $m|(m-۱)!$. حالت دوم $m = p^۲$ و $p \neq ۲$. در این حالت $۱ < p < ۲p < m$ و بنابراین $m = p^۲|(m-۱)!$.

◁ **۲۳.۳** همهٔ اعداد صحیح $n > ۱$ را پیدا کنید به‌طوری که $n(n+۱)|(n-۱)!$. (راهنمایی: توضیح قبل را در نظر بگیرید.)

حل. اگر n اول باشد، آنگاه بنابر قضیهٔ ویلسن $(n-۱)! \equiv -۱ (\mathrm{mod}\, n)$، لذا به‌ویژه $n \not| (n-۱)!$. اگر $n+۱$ اول باشد، آنگاه $n! \equiv -۱ (\mathrm{mod}\, n+۱)$. اما

$$n! = n(n-۱)! \equiv -(n-۱)! (\mathrm{mod}\, n+۱)$$

لذا $(n-۱)! \equiv ۱ (\mathrm{mod}\, n+۱)$ و از این‌رو $n+۱ \not| (n-۱)!$. تا اینجا تمام اعداد اول n یا تمام اعداد n که یک واحد کمتر ازعدد اولی هستند کنار گذاشته شدند. روشن است که عدد ۴ کنار گذاشته شده است (زیرا $۱ - ۵ = ۴$). حال چون $(n, n+۱) = ۱$ کافی است ثابت کنیم اعداد مرکب $n > ۴$ و $n+۱ > ۴$ هر کدام $(n-۱)!$ را می‌شمارند. بنابر توضیح بالا $n! \equiv ۰ (\mathrm{mod}\, n)$، یعنی $n|(n-۱)!$؛ همچنین بنابر همان توضیح $n! \equiv ۰ (\mathrm{mod}\, n+۱)$ یعنی $n+۱|n!$ و چون $(n, n+۱) = ۱$ پس $n+۱|(n-۱)!$.

۲۴.۳ ثابت کنید که به‌ازای هر عدد اول p و هر عدد صحیح a، عدد $a^p + (p-۱)!a$ بر p بخشپذیر است.

حل. بنابر قضیهٔ فرما داریم $a^p \equiv a (\mathrm{mod}\, p)$، لذا

$$a^p + (p-۱)!a \equiv a(۱ + (p-۱)!) (\mathrm{mod}\, p)$$

اما بنابر قضیهٔ ویلسن $(p-۱)! + ۱ \equiv ۰ (\mathrm{mod}\, p)$.

توضیح. قضیهٔ بالا قضیهٔ ویلسن را «در بر دارد» (a را برابر ۱ اختیار کنید). قضیهٔ فرما را نیز «در بر دارید». زیرا از $(p-1)!+1 \equiv 0 \pmod p$ و $a^p + (p-1)!a \equiv 0 \pmod p$ نتیجه می‌شود $a^p - a \equiv 0 \pmod p$.

۲۵.۳ (الف) فرض می‌کنیم r_1، r_2، ...، r_{p-1} و s_1، s_2، ...، s_{p-1} در دستگاه مخفف مانده‌ها به پیمانهٔ عدد اول فرد p باشند. ثابت کنید که r_1s_1، r_2s_2، ...، $r_{p-1}s_{p-1}$ نمی‌تواند یک د.م.م[1] به پیمانهٔ p باشد. (راهنمایی: از قضیهٔ ویلسن استفاده کنید.)

(ب) فرض می‌کنیم r_1، r_2، ...، r_p و s_1، s_2، ...، s_p دو د.ک.م[2] به پیمانهٔ عدد اول فرد p باشند. ثابت کنید r_1s_1، r_2s_2، ...، r_ps_p نمی‌تواند یک د.ک.م به پیمانهٔ p باشد.

حل. (الف). چون ۱، ۲، ...، $p-1$ یک د.م.م به پیمانهٔ p است، لذا اگر r_1، ...، r_{p-1} هر دستگاه مخفف مانده‌ها به پیمانهٔ p باشد، آنگاه هر یک از عناصر این دستگاه با عنصری از دستگاه اول همنهشت به پیمانهٔ p است، لذا $p-1$ همنهشتی به‌دست می‌آید که از ضرب آنها داریم $r_1r_2\cdots r_{p-1} \equiv (p-1)! \equiv -1 \pmod p$. به همین دلیل $s_1s_1\cdots s_{p-1} \equiv -1 \pmod p$. در نتیجه $(r_1s_1)\cdots(r_{p-1}s_{p-1}) \equiv 1 \pmod p$ (۱). حال اگر r_1s_1، ...، $r_{p-1}s_{p-1}$ یک د. م .م به پیمانهٔ p باشد، داریم

$$(r_1s_1)\cdots(r_{p-1}s_{p-1}) \equiv -1 \pmod p$$

از این رابطه و (۱)، $1 \equiv -1 \pmod p$ به‌دست می‌آید که ممکن نیست.

توضیح. چون r_1، r_2، ...، r_{p-1} و s_1، s_2، ...، s_{p-1} هرکدام د. م .م به پیمانهٔ p هستند. لذا

$$(r_i, p) = (s_i, p) = 1 \quad i = 1, 2, \ldots, p-1$$

در نتیجه به‌ازای هر $1 \le i \le p-1$، داریم $(r_is_i, p) = 1$، لذا از اینکه r_1s_1، ...، $r_{p-1}s_{p-1}$ نمی‌تواند یک د. م. م به پیمانهٔ p باشد نتیجه می‌گیریم که اعداد i و j وجود دارند که $r_is_i \equiv r_js_j \pmod p$.

(ب) بدون آنکه به کلیت استدلال خللی وارد آید می‌توانیم فرض کنیم $r_p \equiv 0 \pmod p$. دو حالت در نظر می‌گیریم، حالت اول: $s_p \equiv 0 \pmod p$. در این‌صورت r_1، ...، r_{p-1} و s_1، ...، s_{p-1} هرکدام یک د.م.م به پیمانهٔ p هستند و بنابر (الف) در بالا، r_1s_1، ...، $r_{p-1}s_{p-1}$

۱. یعنی دستگاه مخفف مانده‌ها.
۲. یعنی دستگاه کامل مانده‌ها.

نمی‌تواند یک د. م. م به پیمانهٔ p باشد. لذا با توجه به توضیح بالا r_1s_1، ...، r_ps_p نمی‌تواند یک د. ک. م به پیمانه p باشد. حالت دوم: $s_p \not\equiv 0 \pmod p$ در این‌صورت $j \neq p$ وجود دارد که $s_j \equiv 0 \pmod p$. بنابراین $r_ps_p \equiv r_js_j \equiv 0 \pmod p$. لذا در این حالت نیز r_1s_1، ...، r_ps_p د. ک. م نیست.

◁ **۲۶.۳** (برهانی برای قضیهٔ (۵.۳) از طریق قضیهٔ ویلسن) فرض کنید p عدد اولی به‌صورت $4k+1$ باشد. ثابت کنید که $(\frac{p-1}{2})!$ یک جواب $x^2 \equiv -1 \pmod p$ است. (راهنمایی: به‌ازای $1 \leq x \leq \frac{p-1}{2}$، $p - x \equiv -x \pmod p$.)

حل. فرض کنیم $p = 4k+1$. وقتی x از ۱ تا $2k$ تغییر کند، $p-x$ از $4k$ تا $2k+1$ نزول می‌کند. بنابراین $4k(4k-1)\cdots(2k+1) \equiv (-1)^{2k}(2k)! \equiv (2k)! \pmod p$، و لذا $(4k)! \equiv ((2k)!)^2 \pmod p$. اما $4k! \equiv -1 \pmod p$، بنابراین $((2k)!)^2 \equiv -1 \pmod p$.

۲۷.۳ به کمک تمرین ۲۶.۳ جوابهایی برای معادله‌های $x^2 \equiv -1 \pmod{37}$ و $x^2 \equiv -1 \pmod{41}$ به‌دست آورید.

حل. ۳۷ و ۴۱ هر دو به‌صورت $4k+1$ هستند، لذا بنابر تمرین قبل $18!$ و $20!$ به‌ترتیب در معادله‌ها صدق می‌کنند. ولی بهتر است که کوچکترین ماندهٔ مثبت را پیدا کنیم. با کمی کار خواهیم داشت $18! \equiv 31 \pmod{37}$ و $20! \equiv 9 \pmod{41}$. (البته برای اعداد اول بزرگ p، این روش محاسبه برای حل $x^2 \equiv -1 \pmod p$ عملی نیست.)

◁ **۲۸.۳** فرض می‌کنیم p عدد اول فردی باشد. ثابت کنید

$$[1 \times 3 \times 5 \times \cdots \times (p-2)]^2 \equiv [2 \times 4 \times 6 \times \cdots \times (p-1)]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

حل. وقتی x تعداد $\frac{p-1}{2}$ عدد صحیح زوج از ۲ تا $p-1$ را اختیار می‌کند، $p-x$ اعداد فرد از $p-2$ تا ۱ را به سمت پایین اختیار خواهد کرد. لذا با توجه به اینکه $p - x \equiv -x \pmod p$ داریم

$$2 \times 4 \times \cdots \times (p-1) \equiv (-1)^{\frac{p-1}{2}}[1 \times 3 \times \cdots \times (p-2)] \pmod p \qquad (1)$$

اگر طرفین (۱) را به توان ۲ برسانیم روشن است که داریم

$$[1 \times 3 \times 5 \times \cdots \times (p-2)]^2 \equiv [2 \times 4 \times 6 \times \cdots \times (p-1)]^2 \pmod p$$

حال، بنابر قضیهٔ ویلسن داریم

$$-۱ \equiv (p-۱)! = [۱ \times ۳ \times \cdots \times (p-۲)][۲ \times ۴ \times \cdots \times (p-۱)] \equiv -۱ (\mathrm{mod}\, p)$$

لذا با توجه به (۱)

$$-۱ \equiv (-۱)^{\frac{p-۱}{۲}} [۱ \times ۳ \times ۵ \times \cdots \times (p-۲)]^۲ (\mathrm{mod}\, p)$$

یا

$$[۱ \times ۳ \times ۵ \times \cdots \times (p-۲)]^۲ \equiv (-۱)^{\frac{p+۱}{۲}} (\mathrm{mod}\, p)$$

۲۹.۳ (الف) نشان دهید که تعداد نامتناهی اعداد صحیح n وجود دارند که به‌ازای آنها $n! - ۱$ مرکب است.

(ب) تعداد نامتناهی اعداد صحیح n وجود دارند که به‌ازای آنها $n! + ۱$ مرکب است.

حل. (الف) فرض می‌کنیم p عدد اولی بزرگتر از ۵ باشد. قرار می‌دهیم $n = p - ۲$. بنابر قضیهٔ ویلسن داریم $(p-۲)! \equiv -۱ (\mathrm{mod}\, p)$ و چون $(p-۱) \equiv -۱ (\mathrm{mod}\, p)$، پس $(p-۲)! \equiv ۱ (\mathrm{mod}\, p)$ لذا $p | n! - ۱$ و چون $p > ۵$، داریم $(p-۲)! - ۱ > p$، پس $n! - ۱$ مرکب است.

(ب) فرض می‌کنیم p عدد اولی باشد. قرار می‌دهیم $n = p - ۱$. بنابر قضیهٔ ویلسن $p | n! + ۱$ و بجز وقتی $p = ۲$ داریم $n! + ۱ > p$.

◁ **۳۰.۳** به استقرا بر s نشان دهید که اگر p اول باشد و $۱ \leq s \leq p$، آنگاه

$$(۱) \quad (s-۱)!(p-s)! \equiv (-۱)^s (\mathrm{mod}\, p)$$

حل. این قضیه می‌گوید اگر یک واحد بر s افزوده شود عبارت $(s-۱)!(p-s)!$ به پیمانهٔ p تغییر علامت می‌دهد. همین امر موجب می‌شود که برهان از راه استقرا صورت گیرد. به‌ازای $s = ۱$ رابطه (۱) همان قضیهٔ ویلسن است. فرض کنیم $s \geq ۱$ و (۱) برقرار باشد، گوییم (۱) با $s + ۱$ به جای s نیز برقرار است یعنی $s!(p-s-۱)! \equiv (-۱)^{s+۱} (\mathrm{mod}\, p)$ (۲) قرار می‌دهیم $A = (s-۱)!(p-s)!$ و $B = s!(p-s-۱)!$. به آسانی دیده می‌شود که $As = B(p-s)$، لذا $As \equiv -Bs (\mathrm{mod}\, p)$ یا $B \equiv -A (\mathrm{mod}\, p)$. در نتیجه (۲) برقرار است.

اعداد اول p و q اعداد اول توأمان نامیده می‌شوند هرگاه تفاضل آنها برابر ۲ باشد. قویاً گمان می‌رود که تعداد نامتناهی اعداد اول توأمان وجود دارند، ولی تاکنون دلیلی برای آن ارائه نشده است.

۳۱.۳ اگر n و $n+۲$ هر دو اول باشند، نشان دهید که $۴[(n-۱)!+۱]+n \equiv ۰ \pmod{n(n+۲)}$ (عکس مطلب نیز برقرار است.) (راهنمایی: $n(n+۱) \equiv (-۲)(-۱) \pmod{(n+۲)}$).

حل. اگر n اول باشد، بنابر قضیهٔ ویلسن $(n-۱)! + ۱ \equiv ۰ \pmod{n}$، و لذا

$$۴[(n-۱)! + ۱] + n \equiv ۰ \pmod{n}$$

اگر $n+۲$ اول باشد، آنگاه $(n+۱)!+۱ \equiv ۰ \pmod{n+۲}$. اما چون $n+۱ \equiv -۱ \pmod{n+۲}$ و $n \equiv -۲ \pmod{n+۲}$، داریم

$$۴[(n-۱)! + ۱] + n \equiv ۲(n+۱)! + ۲ + n + ۲ \equiv ۰ \pmod{n+۲}$$

چون $(n, n+۲) = ۱$ داریم $۴[(n-۱)! + ۱] + n \equiv ۰ \pmod{n(n+۲)}$.

◁ **۳۲.۳** (لیوویل، ۱۸۵۶). اگر p یکی از اعداد اول ۲، ۳، یا ۵ باشد، آنگاه $(p-۱)! + ۱$ توانی از یک عدد اول است. رئوس برهان برای صحیح نبودن این مطلب به‌ازای $p > ۵$ در زیر آمده است آن را به تفصیل بنویسید.

(الف) اگر $p > ۵$، آنگاه $(p-۱)^۲ | (p-۱)!$.

(ب) اگر $(p-۱)! + ۱$ توانی از یک عدد اول باشد، آنگاه توانی از عدد اول p است.

(ج) اگر $(p-۱)! + ۱ = p^k$، آنگاه $p - ۱ | p^{k-۱} + \cdots + ۱$. این حالت فقط وقتی اتفاق می‌افتد که $p - ۱ | k$، اما در این‌صورت $(p-۱)! + ۱ = p^k$ غیرممکن است.

حل. (الف) چون p فرد است، $p-۱$ بر ۲ و $\frac{p-۱}{۲}$ بخشپذیر است و چون $p > ۵$ داریم $۲ < \frac{p-۱}{۲} < p-۱$. لذا $(p-۱)^۲ | (p-۱)!$.

(ب) بنابر قضیهٔ ویلسن، $p | (p-۱)! + ۱$؛ لذا اگر قرار باشد $(p-۱)! + ۱$ توانی از یک عدد اول باشد، p همان عدد است.

(ج) اگر $(p-۱)! + ۱ = p^k$، آنگاه $(p-۱)! = p^k - ۱ = (p-۱)(p^{k-۱} + \cdots + p + ۱)$. بنابراین از (الف) نتیجه می‌شود که $p - ۱ | p^{k-۱} + \cdots + ۱$. اما

$$p^{k-۱} + \cdots + ۱ \equiv k \pmod{p-۱}$$

زیرا $p \equiv ۱ (\mathrm{mod}\, p-۱)$؛ بنابراین $p-۱|k$. در این‌صورت $p^k \geq p^{p-۱}$، و چون $p^{p-۱} > (p-۱)! + ۱$، لذا $p^k = (p-۱)! + ۱$ برقرار نیست.

توضیح. لایپنیتس در ۱۶۸۰ یک برهان نادرست ارائه داد که اگر n اول نباشد، عدد $۲^n - ۲$ را نمی‌شمارد. نخستین عدد مرکب n که برای آن $۲^n \equiv ۲ (\mathrm{mod}\, n)$، ۳۴۱ است. لذا شگفت‌آور نیست که عقیده پیدا کرده بودند که این همنهشتی یک آزمون اول بودن را به ما می‌دهد.

اگر n عدد مرکبی باشد ولی $a^{n-۱} \equiv ۱ (\mathrm{mod}\, n)$، آنگاه n را یک شبه اول یا اول نما در پایهٔ a می‌خوانیم. مسأله بعد مثالهایی از اعداد شبه اول در پایهٔ ۲ ارائه می‌دهد. علاوه بر این، هر عدد فرمای $۲^{۲^n} + ۱$ و هر عدد مرسن $۲^p - ۱$ که در آن p اول‌است، یا اول است یا شبه اول در پایهٔ ۲ است. (هفت مسأله زیر را ملاحظه کنید.)

۳۳.۳ اگر p و q اعداد اول متمایز باشند به‌طوری که $۲^p \equiv ۲ (\mathrm{mod}\, q)$ و $۲^q \equiv ۲ (\mathrm{mod}\, p)$، ثابت کنید $۲^{pq} \equiv ۲ (\mathrm{mod}\, pq)$. نشان دهید $p = ۱۱$، $q = ۳۱$؛ $p = ۱۹$، $q = ۷۳$؛ و $p = ۱۷$، $q = ۲۵۷$ در شرایط مسأله صدق می‌کنند. (در نتیجه، در هر حالت، pq یک شبه اول در پایهٔ ۲ است.)

حل. بنابر قضیهٔ فرما داریم $۲^{pq} = (۲^p)^q \equiv ۲^q \equiv ۲ (\mathrm{mod}\, q)$ و با استدلالی مشابه $۲^{pq} \equiv ۲ (\mathrm{mod}\, p)$، لذا $۲^{pq} \equiv ۲ (\mathrm{mod}\, pq)$. محاسبات عددی روشن هستند. مثلاً،

$$۲^{۱۷} = ۲ \times ۲^۸ \times ۲^۸ \equiv ۲(-۱)^۲ \equiv ۲ (\mathrm{mod}\, ۲۵۷)$$

همین‌طور، $۲^{۲۵۷} = ۲(۲^۴)^{۶۴} \equiv ۲ (\mathrm{mod}\, ۱۷)$.

۳۴.۳ (ادوارد لوکا[1]، ۱۸۷۷.) اگر $n = ۳۷ \times ۷۳$، نشان دهید که $۲^{n-۱} \equiv ۱ (\mathrm{mod}\, n)$.

حل. کافی است نشان دهیم $۲^{n-۱} \equiv ۱ (\mathrm{mod}\, ۳۷)$ و $۲^{n-۱} \equiv ۱ (\mathrm{mod}\, ۷۳)$، زیرا $n - ۱ = ۲۷۰۰$. بنابر قضیهٔ فرما $۲^{۳۶} \equiv ۱ (\mathrm{mod}\, ۳۷)$ و چون $۳۶|۲۷۰۰$، لذا $۲^{n-۱} \equiv ۱ (\mathrm{mod}\, ۳۷)$. با استدلالی مشابه داریم $۲^{۷۲} \equiv ۱ (\mathrm{mod}, ۷۳)$. چون $۷۲ \not| ۲۷۰۰$ نمی‌توان به‌راحتی بالا عمل کرد. ولی در واقع $۲^{۳۶} \equiv ۱ (\mathrm{mod}\, ۷۳)$، راههای مختلفی برای پی بردن به آن وجود دارد، ولی محاسبهٔ مستقیم دشوار نیست. زیرا، مثلاً داریم

$$۲^۶ \equiv -۹, ۲^{۱۲} \equiv ۸۱ \equiv ۸, ۲^{۱۸} \equiv -۹ \times ۸ \equiv ۱ (\mathrm{mod}\, ۷۳)$$

در نتیجه، چون $۱۸|۲۷۰۰$، پس $۲^{n-۱} \equiv ۱ (\mathrm{mod}\, ۷۳)$.

1. Edward Lucas

۳۵.۳ اگر $n = ۱۶۱۰۳۸$، ثابت کنید $n | ۲^n - ۲$. (این سؤال، که آیا عدد زوجی مانند n وجود دارد به‌طوری که $n | ۲^n - ۲$ تا سال ۱۹۵۰، که د. ه. لیمر[1] این مثال را پیدا کرد، بی‌جواب بود.)

حل. داریم $n = ۲ \times ۷۳ \times ۱۱۰۳$. لذا کافی است ثابت کنیم هر یک از اعداد ۷۳ و ۱۱۰۳ عدد $۲^{n-۱} - ۱$ را می‌شمارند. داریم $n - ۱ = ۳^۲ \times ۲۹ \times ۶۱۷$. از طرفی $۷۳ \times ۷ = ۲^۹ - ۱$، و چون $۲^{n-۱} - ۱$ بر $۲^۹ - ۱$ بخشپذیر است پس $۲^{n-۱} - ۱ | ۷۳$. همچنین داریم

$$۲^{۱۰} \equiv -۷۹, ۲^{۲۰} \equiv ۷۲۶, ۲^{۲۹} \equiv ۱ (\mathrm{mod}\ ۱۱۰۳)$$

و چون $۲^{n-۱} - ۱$ بر $۲^{۲۹} - ۱$ نیز بخشپذیر است پس $۲^{n-۱} - ۱ | ۱۱۰۳$. بنابراین $۲^n - ۲$ بر ۲ و ۳۷ و ۱۱۰۳ و بنابراین بر n بخشپذیر است.

۳۶.۳ فرض می‌کنیم $۲^{n-۱} \equiv ۱ (\mathrm{mod}\ n)$. اگر $N = ۲^n - ۱$، ثابت کنید $۲^{N-۱} \equiv ۱ (\mathrm{mod}\ N)$. (راهنمایی: فرض کنید $۲^{n-۱} - ۱ = nk$.)

حل. اگر $۲^{n-۱} - ۱ = nk$، آنگاه $N = ۲nk + ۱$، و لذا

$$۲^{N-۱} = (۲^n)^{۲k} = (۱ + N)^{۲k} \equiv ۱ (\mathrm{mod}\ N)$$

توضیح. اگر p اول باشد، بنابر قضیهٔ فرما داریم $۲^{p-۱} \equiv ۱ (\mathrm{mod}\ p)$. لذا نشان داده‌ایم که اگر $N = ۲^p - ۱$، آنگاه یا N اول است یا یک شبه اول در پایهٔ ۲ است.

◁ **۳۷.۳** با استفاده از مسألهٔ قبل نشان‌دهید که تعداد نامتناهی اعداد شبه اول در پایهٔ ۲ وجود دارد. (راهنمایی: فرض کنید $n_۱ = ۲^{۱۱} - ۱$، $n_۲ = ۲^{n_۱} - ۱$، و مانند آن.)

حل. $n_۱$ و $n_۲$ را همان‌گونه که راهنمایی کردیم انتخاب می‌کنیم. بنابر قضیهٔ فرما $۲^{۱۰} \equiv ۱ (\mathrm{mod}\ ۱۱)$، و لذا بنابر مسألهٔ قبل، $۲^{n_۱ - ۱} \equiv ۱ (\mathrm{mod}\ n_۱)$. با استدلالی مشابه، چون $۲^{n_۱ - ۱} \equiv ۱ (\mathrm{mod}\ n_۱)$، مسألهٔ قبل نشان می‌دهد که $۲^{n_۲ - ۱} \equiv ۱ (\mathrm{mod}\ n_۲)$. اگر این روش را ادامه دهیم، می‌بینیم که به‌ازای هر $k \geq ۱$، $۲^{n_k - ۱} \equiv ۱ (\mathrm{mod}\ n_k)$.

برای تکمیل برهان نشان می‌دهیم که به‌ازای هر $k \geq ۱$ عدد n_k مرکب است. عدد $n_۱ = ۲۰۴۷$ مضرب ۲۳ است. اما به‌طور کلی، اگر n مرکب باشد، $۲^n - ۱$ مرکب است، زیرا اگر $n = rs$، آنگاه $۲^{rs} - ۱ | ۲^r - ۱$. از این‌رو، چون $n_۱$ مرکب است، در نتیجه $n_۲$ مرکب است، و قس علی‌هذا.

---

1. D. H. Lehmer

◁ **۳۸.۳** اگر $F_k = ۲^{۲^k} + ۱$، نشان دهید $۲^{F_k} \equiv ۲ (\mathrm{mod}\, F_k)$. (راهنمایی: از $۲^k | F_k - ۱$ استفاده کنید، و مانند مسأله ۳۶.۳ استدلال کنید.)

حل. $F_k - ۱ = ۲^k \times ۲^{۲^k - k}$، و به‌ازای هر k داریم $۲^k > k$. لذا $F_k = ۱ + ۲^k m$ که در آن m زوج است. بنابراین $۲^{F_k} = ۲(۲^{۲^k})^m \equiv ۲(-۱)^m \equiv ۲ (\mathrm{mod}\, F_k)$.

توضیح. نشان داده‌ایم که هر F_k یا عدد اول است یا یک شبه اول در پایهٔ ۲ است. شاید همین قضیه موجب شد که فرما حدسیهٔ اشتباه خود را که هر F_k اول است ابراز دارد. اویلر در ۱۷۳۰ با اثبات اینکه $۶۴۱ | F_۵$ این حدسیه را رد کرد. این مطلب اولین قضیهٔ اویلر در نظریهٔ اعداد است.

۳۹.۳ ثابت کنید که به‌ازای هر a که با ۵۶۱ متباین باشد $a^{۵۶۰} \equiv ۱ (\mathrm{mod}\, ۵۶۱)$. (۵۶۱ اول نیست.)

حل. چون $۵۶۱ = ۳ \times ۱۱ \times ۱۷$، کافی است که نشان دهیم اگر $(a, ۵۶۱) = ۱$، آنگاه $a^{۵۶۰} \equiv ۱ (\mathrm{mod}\, ۳, ۱۱, ۱۷)$. اگر $(a, ۵۶۱) = ۱$، آنگاه $(a, ۳) = (a, ۱۱) = (a, ۱۷) = ۱$. لذا، بنابر قضیهٔ فرما $a^۲ \equiv ۱ (\mathrm{mod}\, ۳)$، $a^{۱۰} \equiv ۱ (\mathrm{mod}\, ۱۱)$، و $a^{۱۶} \equiv ۱ (\mathrm{mod}\, ۱۷)$ اما ۵۶۰ مضربی از ۲، ۱۰، و ۱۶ است، و لذا $a^{۵۶۰} \equiv ۱ (\mathrm{mod}\, ۳, ۱۱, ۱۷)$.

توضیح. اگر n عدد مرکبی باشد و به‌ازای هر a که با n متباین است، $a^{n-۱} \equiv ۱ (\mathrm{mod}\, n)$، آنگاه n یک عدد کارمایکل[1] خوانده می‌شود. لذا یک عدد کارمایکل مانند n یک عدد شبه اول در هر پایهٔ متباین با n است. مسألهٔ قبل نشان می‌دهد که ۵۶۱ یک عدد کارمایکل است. برای مدتی طولانی معلوم نبود که آیا تعداد نامتناهی عدد کارمایکل وجود دارد. سرانجام در ۱۹۹۳ تکلیف مسأله روشن شد، هنگامی که و. ر. آلفورد[2]، اندرو گرانویل[3]، و کارل پومرانس[4] قضیهٔ قوی‌تری را ثابت کردند. آنها نشان دادند که اگر x به‌قدر کافی بزرگ باشد، تعداد $x^{۲/۷}$ عدد کارمایکل کمتر از x وجود دارد. مثلاً به‌طور دقیق ۱۰۵۲۱۲ عدد کارمایکل کمتر از $۱۰^{۱۵}$ وجود دارد.

۴۰.۳ ثابت کنید که $۶۶۰۱ = ۷ \times ۲۳ \times ۴۱$ یک عدد کارمایکل است.

حل. اگر a با ۶۶۰۱ متباین باشد، باید نشان دهیم $a^{۶۶۰۰} \equiv ۱ (\mathrm{mod}\, ۶۶۰۱)$. بنابر قضیهٔ فرما داریم $a^۶ \equiv ۱ (\mathrm{mod}\, ۷)$، $a^{۲۲} \equiv ۱ (\mathrm{mod}\, ۲۳)$، و $a^{۴۰} \equiv ۱ (\mathrm{mod}\, ۴۱)$. چون ۶، ۲۲، و ۴۰ هرکدام ۶۶۰۰ را می‌شمارند، در نتیجه $a^{۶۶۰۰}$ همنهشت با ۱ به پیمانهٔ ۷، ۲۳، و ۴۱ است، و لذا $a^{۶۶۰۰} \equiv ۱ (\mathrm{mod}\, ۶۶۰۱)$.

1. Carmichael 2. W. R. Alford 3. Andrew Granville 4. Carl Pomerance

قضیهٔ اویلر

توضیح. برای حل بعضی از مسائل باید مقدار $\phi(n)$ حساب شود. این کار را می‌توان با استفاده از هر یک از نمایشهای $\phi(n)$ که در قضیهٔ ۱۶.۳ داده شده انجام داد.

۴۱.۳ درست یا نادرست: رقم یکان توان چهار هر عددی که بر ۲ و ۵ بخشپذیر نباشد عدد ۱ است.

حل. این سؤال هم‌ارز است با اینکه سؤال شود آیا $(a, ۱۰) = ۱$ ایجاب می‌کند $a^۴ \equiv ۱ (\mathrm{mod}\ ۱۰)$؟ چون $\phi(۱۰) = ۴$، بنابر قضیهٔ اویلر جواب مثبت است. با محاسبهٔ مستقیم نیز می‌توان این کار را انجام داد، کافی است بررسی کنیم که رقم یکان توان ۴ اعداد ۱، ۳، ۷، و ۹ همگی برابر ۱ هستند.

۴۲.۳ باقیمانده‌های ممکن تقسیم $a^{۱۰۰}$ بر ۱۲۵ را به‌دست آورید.

حل. $\phi(۱۲۵) = ۱۰۰$، لذا اگر $(۵, a) = ۱$، آنگاه $a^{۱۰۰} \equiv ۱ (\mathrm{mod}\ ۱۲۵)$. در غیر این‌صورت $۵|a$، و روشن است که $۱۲۵|a^{۱۰۰}$. لذا باقیمانده‌های ممکن ۱ و ۰ هستند.

۴۳.۳ ارقام یکان و دهگان عدد $۹^{۹^۹}$ را به‌دست آورید. (راهنمایی: نشان دهید که $۹^{۹^۹} \equiv ۹^۹ (\mathrm{mod}\ ۱۰۰)$.)

حل. چون $\phi(۱۰۰) = ۴۰$، ابتدا باقیماندهٔ تقسیم توان $۹^۹$ را بر ۴۰ به‌دست می‌آوریم. داریم $۹ \equiv +۱ (\mathrm{mod}\ ۸)$ و $۹ \equiv -۱ (\mathrm{mod}\ ۵)$، لذا $۹^۹ \equiv ۱ (\mathrm{mod}\ ۸)$ و $۹^۹ \equiv -۱ (\mathrm{mod}\ ۵)$؛ یا $۹^۹ \equiv ۹ (\mathrm{mod}\ ۸)$ و $۹^۹ \equiv -۹ (\mathrm{mod}\ ۵)$. در نتیجه $۹^۹ \equiv ۹ (\mathrm{mod}\ ۴۰)$. بنابراین $۹^{۹^۹} \equiv ۹^۹ (\mathrm{mod}\ ۱۰۰)$. $۹^{۹^۹} \equiv ۹^{۹+۴۰k} \equiv ۹^۹ \times (۹^{۴۰})^k$ کافی است باقیماندهٔ تقسیم $۹^۹$ را بر ۱۰۰ پیدا کنیم. این کار به روشهای گوناگون انجام می‌شود. مثلاً

$$۹^{۱۰} = (۱۰ - ۱)^{۱۰} \equiv ۱ \equiv -۹۹ (\mathrm{mod}\ ۱۰۰)$$

لذا $۹^۹ \equiv -۱۱ \equiv ۸۹ (\mathrm{mod}\ ۱۰۰)$. از این‌رو باقیمانده برابر ۸۹ است. یعنی رقم یکان و دهگان عدد $۹^{۹^۹}$ به‌ترتیب ۹ و ۸ است.

۴۴.۳ اگر a بر ۲ و ۵ بخشپذیر نباشد، ثابت کنید سه رقم آخر a و $a^{۱۰۱}$ برابرند. (در اینجا قرارداد می‌کنیم که مثلاً ۲۱ به ۰۲۱ «ختم» می‌شود.)

حل. کافی است ثابت کنیم $a^{۱۰۱} \equiv a (\mathrm{mod}\ ۱۰۰۰)$. داریم $(a, ۱۲۵) = (a, ۸) = ۱$. چون

$\phi(۱۲۵)=۱۰۰$، لذا بنابر قضیهٔ اویلر $a^{۱۰۰}\equiv ۱(\bmod ۱۲۵)$ (۱). همچنین $\phi(۸)=۴|۱۰۰$، پس $a^{۱۰۰}\equiv ۱(\bmod ۸)$. از این (۱) $a^{۱۰۰}\equiv ۱(\bmod ۱۰۰۰)$ و در نتیجه

$$a^{۱۰۱}\equiv a(\bmod ۱۰۰۰)$$

۴۵.۳ اگر $(n,۷۲)=۱$، قضیهٔ اویلر را به‌کار برید و ثابت کنید $n^{۱۲}\equiv ۱(\bmod ۷۲)$.

حل. فرض کنیم $(n,۷۲)=۱$. چون $\phi(۸)=۴$، $\phi(۹)=۶$، و ۱۲ مضربی از ۴ و مضربی از ۶ است، قضیهٔ اویلر ایجاب می‌کند که $n^{۱۲}\equiv ۱$ به پیمانهٔ ۸ و به پیمانهٔ ۹، و لذا به پیمانهٔ ۷۲.

۴۶.۳ آیا عدد صحیح $n>۱$ وجود دارد به‌طوری که ۱۷۲۹ عدد $n^{۳۶}-۱$ را بشمارد؟ آیا تعداد نامتناهی از این اعداد وجود دارند؟

حل. آشکار است که اگر $n=۱(\bmod ۱۷۲۹)$، آنگاه $۱۷۲۹|n^{۳۶}-۱$. از اینجا به‌ازای $k\geq ۱$ بی‌نهایت جواب $n=۱+۱۷۲۹k$ به‌دست می‌آید. در واقع جوابهای خیلی زیادتری وجود دارند: چون $۱۷۲۹=۷\times ۱۳\times ۱۹$ و به‌ازای $p=۷,۱۳,۱۹$ داریم $p-۱|۱۷۲۹$، قضیهٔ فرما ایجاب می‌کند که به‌ازای هر n متباین با ۱۷۲۹، $n^{۳۶}\equiv ۱(\bmod ۱۷۲۹)$.

۴۷.۳ با استفاده از قضیهٔ اویلر نشان دهید که به‌ازای هر n، $۴۰۸۰|n^{۲۰}-n^{۴}$.

حل. $۴۰۸۰=۲^{۴}\times ۳\times ۵\times ۱۷$، و $n^{۲۰}-n^{۴}=n^{۴}(n^{۱۶}-۱)$. فرض کنیم $p=۳,۵,۷$. اگر $p\nmid n$، آنگاه چون $\phi(p)|۱۶$، لذا $p|n^{۱۶}-۱$، و اگر $p|n$ آنگاه $p|n^{۴}$؛ از این‌رو، $p|n^{۲۰}-n^{۴}$. اکنون $۲^{۴}$ را در نظر می‌گیریم. اگر n فرد باشد $۲^{۴}|۲^{۱۶}-۱$ زیرا $\phi(۲^{۴})=۸$؛ اگر n زوج باشد، آنگاه $۲^{۴}|n^{۴}$. در نتیجه $n^{۲۰}-n^{۴}$ بر اعداد $۲^{۴}$، ۳، ۵، و ۷ و لذا بر ۴۰۸۰ بخشپذیر است.

۴۸.۳ اگر $(m,n)=۱$، ثابت کنید $m^{\phi(n)}+n^{\phi(m)}\equiv ۱(\bmod mn)$.

حل. بنابر قضیهٔ اویلر $m^{\phi(n)}\equiv ۱(\bmod n)$، و روشن است که $n^{\phi(m)}\equiv ۰(\bmod n)$، لذا $m^{\phi(n)}+n^{\phi(m)}\equiv ۱(\bmod n)$. به قرینه، همین رابطه برای پیمانهٔ m نیز برقرار است و چون $(m,n)=۱$ بنابر (۴.۲) مجموع همنهشت با ۱ به پیمانهٔ mn است.

۴۹.۳ کلیهٔ اعداد بین ۰ و ۴۴ را که در همنهشتی $۵x^{۱۳}+۳x^{۳}+۲\equiv ۰(\bmod ۴۵)$ صدق می‌کنند پیدا کنید. (برای ساده کردن محاسبات از قضیهٔ فرما و قضیهٔ اویلر استفاده کنید.)

حل. معادلهٔ فوق با دستگاه معادلات $۵x^{۱۳}+۳x^{۳}+۲\equiv ۰(\bmod ۵)$ (۱) و $۳x^{۳}+۲\equiv ۰(\bmod ۹)$ (۲) هم‌ارز است. روشن است که (۱) با $۵x^{۱۳}+۳x^{۳}+۲\equiv ۰(\bmod ۵)$ هم‌ارز است. با تجسس $x^{۳}-۱\equiv ۰(\bmod ۵)$ یا $-۲x^{۳}+۲\equiv ۰(\bmod ۵)$ تنها جواب معادله آخر و لذا تنها جواب (۱) است. حال به حل (۲) می‌پردازیم. بدیهی است که در (۲)، $(x,۳)=۱$ و لذا بنابر قضیهٔ اویلر $x^{۶}\equiv ۱(\bmod ۹)$. در نتیجه (۲) با $۳x^{۳}+۵x+۲\equiv ۰(\bmod ۹)$ (۴) هم‌ارز است. اگر x جوابی از (۴) باشد، آنگاه $۵x+۲\equiv ۰(\bmod ۳)$ یا $x\equiv -۱(\bmod ۳)$. لذا $x+۱=۳k$ و به کمک بسط دوجمله‌یی $x^{۳}\equiv -۱(\bmod ۹)$. در نتیجه (۴) به $۵x-۱\equiv ۰(\bmod ۹)$ بدل می‌شود. از اینجا $x\equiv ۲(\bmod ۹)$ (۵) به‌دست می‌آید. بالاخره از حل دستگاه متشکل از (۳) و (۵)، مثلاً قضیهٔ باقیماندهٔ چینی جواب $x\equiv ۱۱(\bmod ۴۵)$ برای همنهشتی اصلی حاصل می‌شود. بدیهی است که ۱۱ تنها جواب بین ۰ و ۴۴ است.

۵۰.۳ (الف) اگر p اول و $p\nmid a$، نشان دهید که $ba^{p-۲}$ جوابی از همنهشتی $ax\equiv b(\bmod p)$ است. این روش را برای حل همنهشتی $۵x\equiv ۴(\bmod ۱۷)$ به‌کار برید.

(ب) با کاربرد مناسب ایدهٔ (الف) جوابی از همنهشتی $ax\equiv b(\bmod m)$ که در آن $(a,m)=۱$ و m لزوماً اول نیست به‌دست آورید. از فرمول حاصل برای حل همنهشتی $۵x\equiv ۴(\bmod ۴۲)$ استفاده کنید.

حل. (الف) بنابر قضیهٔ فرما $a(ba^{p-۲})=ba^{p-۱}\equiv b(\bmod p)$. لذا در مثال عددی داریم $x\equiv ۴\times ۵^{۱۵}(\bmod ۱۷)$. این جواب است، ولی اگر کوچکترین ماندهٔ مثبت را بخواهیم، قدری محاسبه لازم است. داریم $۵^{۲}\equiv ۸(\bmod ۱۷)$، لذا $۵^{۴}\equiv -۴(\bmod ۱۷)$، $۵^{۸}\equiv -۱(\bmod ۱۷)$، و از این‌رو

$$۵^{۱۵}=۵^{۱}\times ۵^{۲}\times ۵^{۴}\times ۵^{۸}\equiv ۵(-۸)(-۴)(-۱)\equiv ۷(\bmod ۱۷)$$

بنابراین، $x\equiv ۱۱(\bmod ۱۷)$.

(ب) با کاربرد قضیهٔ اویلر، درست همانند (الف) $x=ba^{\phi(m)-۱}$ را به‌عنوان جوابی از همنهشتی به‌دست می‌آوریم. لذا در مثال عددی داریم $x\equiv ۴\times ۵^{۱۱}(\bmod ۴۲)$. از حُسن اتفاق، $۵^{۳}\equiv -۱(\bmod ۴۲)$، لذا $۴\times ۵^{۱۱}\equiv ۴(-۱)^{۳}(۵^{۲})\equiv ۲۶(\bmod ۴۲)$.

توضیح. برای اعداد اول بزرگ p و اعداد بزرگ a، تکنیک توصیف‌شده در (الف) می‌تواند تقریباً به همان سرعت الگوریتم اقلیدسی باشد هرگاه یک روش مؤثر، نظیر روش مربع‌سازی مکرر،

برای یافتن توانها به پیمانهٔ p به‌کار بریم. برای pهای بزرگ و اعداد کوچک a، الگوریتم اقلیدسی کارسازتر است، زیرا بعد از یک مرحله با اعداد کوچک سروکار داریم. تکنیک قسمت (ب) تقریباً همیشه یک روش ناکارآمد برای حل همنهشتیهای خطی است، زیرا برای محاسبهٔ $\phi(m)$ به تجزیهٔ m نیاز داریم که یک مسألهٔ محاسبه‌ای بسیار دشوار است.

۵۱.۳ (بونیاکوفسکی[1]، ۱۸۳۱)، فرض می‌کنیم a، b دو عدد طبیعی متباین باشند. ثابت کنید

$$x = ca^{\phi(b)-1}, \quad y = -\frac{c}{b}\left(a^{\phi(b)} - 1\right)$$

جواب معادلهٔ $ax + by = c$ است.

حل. چون $a^{\phi(b)} \equiv 1 \pmod{b}$، پس $b | a^{\phi(b)} - 1$، و لذا y عدد صحیح، یعنی قضیهٔ اویلر برقرار است. داریم

$$ax + by = ca^{\phi(b)} - ca^{\phi(b)} + c = c$$

۵۲.۳ فرض می‌کنیم $(a, m) = 1$ و عدد صحیح t وجود داشته باشد به‌طوری که $n | t\phi(m) + 1$. ثابت کنید $x^n \equiv a \pmod{m}$ دارای جواب یکتای a^k است، که در آن $k = (t\phi(m) + 1)/n$.

حل. بنابر قضیهٔ اویلر، $(a^k)^n = a^{t\phi(m)+1} = (a^{\phi(m)})^t a \equiv a \pmod{m}$. برای اثبات یکتایی فرض می‌کنیم $s^n \equiv a \pmod{m}$. در این‌صورت بنابر قضیهٔ اویلر داریم $s \equiv (s^{\phi(m)})^t s = s^{t\phi(m)+1} = (s^n)^k \equiv a^k \pmod{m}$.

۵۳.۳ به کمک مسألهٔ قبل معادلات زیر را حل کنید: (الف) $x^{11} \equiv 3 \pmod{68}$؛ (ب) $x^{13} \equiv 7 \pmod{68}$؛ (ج) $x^{23} \equiv 5 \pmod{68}$.

حل. (الف) $\phi(68) = \phi(2^2 \times 17) = 2 \times 16 = 32$؛ از این‌رو $11 | \phi(68) + 1$. لذا جواب عبارت است از $x \equiv 3^{33/11} \equiv 27 \pmod{68}$.

(ب) چون $13 | 2\phi(68) + 1$، پس جواب چنین است $x \equiv 7^{65/13} \equiv 11 \pmod{68}$.

(ج) $23 | 5\phi(68) + 1$، لذا $x \equiv 5^{161/23} \equiv 61 \pmod{68}$ تنها جواب معادلهٔ $x^{23} \equiv 5 \pmod{68}$.

◁ **۵۴.۳** (قضیهٔ باقیماندهٔ چینی از طریق قضیهٔ اویلر.) فرض می‌کنیم اعداد طبیعی m_1، m_2، ...، m_k دوبه‌دو نسبت به‌هم اول باشند، و a_1، a_2، ...، a_k اعداد صحیح. فرض

1. Bunyakovskii

می‌کنیم $m = m_1 m_2 \cdots m_k$. ثابت کنید دستگاه همنهشتیهای $x \equiv a_1 (\mathrm{mod}\, m_1)$، ...، $x \equiv a_k (\mathrm{mod}\, m_k)$ جوابی به‌صورت زیر دارد

$$x = a_1 \left(\frac{m}{m_1}\right)^{\phi(m_1)} + a_2 \left(\frac{m}{m_2}\right)^{\phi(m_2)} + \cdots + a_k \left(\frac{m}{m_k}\right)^{\phi(m_k)}$$

حل. به قرینه، کافی است ثابت کنیم که جواب ارائه‌شده در $x \equiv a_1 (\mathrm{mod}\, m_1)$ صدق می‌کند. اگر $i > 1$، آنگاه $m_1 | m/m_1$، لذا $x \equiv a_1 (m/m_1)^{\phi(m_1)} (\mathrm{mod}\, m_1)$ (۱). از طرفی $(m_1, m/m_1) = 1$، لذا بنابر قضیهٔ اویلر $(m/m_1)^{\phi(m_1)} \equiv 1 (\mathrm{mod}\, m_1)$ (۲). پس، از (۱) و (۲) داریم $x \equiv a_1 (\mathrm{mod}\, m_1)$.

موضوع مسأله بعد در باب عکس جزئی از قضیهٔ فرماست که لوکا در ۱۸۷۸ ارائه داده است.

۵۵.۳ (الف) فرض می‌کنیم m عدد مرکبی باشد و $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$، که در آن $a \not\equiv 1 (\mathrm{mod}\, m)$. با استفاده از قضیهٔ اویلر و (۷.۳) نشان دهید که یک مقسوم‌علیه سره از $m - 1$ مانند d وجود دارد به‌طوری که $a^d \equiv (\mathrm{mod}\, m)$.

(ب) با استفاده از (الف) ثابت کنید اگر aای وجود داشته باشد به‌طوری که $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$. ولی به‌ازای هر عامل اول $m - 1$ مانند p، $a^{\frac{m-1}{p}} \not\equiv 1 (\mathrm{mod}\, m)$، آنگاه m اول است.

حل. (الف) فرض کنیم $d = (\phi(m), m - 1)$. بنابر قضیهٔ اویلر $a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$ و بنابر فرض $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$، لذا (۷.۳) ایجاب می‌کند که $a^d \equiv 1 (\mathrm{mod}\, m)$. چون $a \not\equiv 1 (\mathrm{mod}\, m)$، در نتیجه $d \neq 1$؛ همچنین، چون m مرکب است $\phi(m) < m - 1$، و بنابراین $d \neq m - 1$. لذا d یک مقسوم‌علیه سرهٔ $m - 1$ است.

(ب) فرض کنیم بعکس، m مرکب باشد (فرض خلف). چون بنابر (الف) dی تولیدشدهٔ یک مقسوم‌علیه سرهٔ $m - 1$ است، در نتیجه $(m - 1)/d$ بر عدد اولی مانند p بخشپذیر است. فرض کنیم $(m - 1)/d = kp$؛ در این‌صورت $a^{(m-1)/p} = (a^d)^k \equiv 1 (\mathrm{mod}\, m)$. که با فرض تناقض دارد.

◁ **۵۶.۳** (کِرله[1]، ۱۸۲۹) فرض می‌کنیم m عددی طبیعی باشد که بر ۲ و ۵ بخشپذیر نیست. نشان دهید که تعداد نامتناهی N به‌صورت ۱۴۷...۱۴۷۱۴۷۱۴۷ وجود دارد به‌طوری که $m | N$. (به جای ۱۴۷ می‌توان هر دنباله از ارقام و با هر طول قرار داد.)

1. Crelle

حل. فرض می‌کنیم N عددی باشد که در آن دستهٔ ارقام ۱۴۷ به تعداد k بار، که k بعداً انتخاب خواهد شد، تکرار شده است. بنابراین داریم

$$N = ۱۴۷(۱ + ۱۰^{۳} + \cdots + ۱۰^{۳(k-۱)}) = ۱۴۷((a^k - ۱)/(a - ۱))$$

که در آن $a = ۱۰^{۳}$. چون $(a, m) = ۱$، با انتخاب k به‌صورت مضربی از $\phi(m)$ می‌توانیم مطمئن باشیم که $m|a^k - ۱$. ولی، به دلیل بودن $a - ۱$ در مخرج، این کافی نیست. بنابراین فرض می‌کنیم k مضربی از $\phi(m(a-۱))$ باشد؛ در این‌صورت، بنابر قضیهٔ اویلر $a^k \equiv ۱ (\mathrm{mod}\, m(a-۱))$. لذا $m(a-۱)$ عدد $a^k - ۱$ را می‌شمارد، و از این‌رو $m|(a^k - ۱)/(a - ۱)$. برای هر دنباله از ارقام نیز اثبات به همین نحو است.

تابع ϕ اویلر

توضیح. در بقیهٔ مسائل این فصل به ویژگیهای تابع اویلر پرداخته خواهد شد. اکثر آنها را می‌توان با استفاده از یکی از فرمولهای اویلر که در (۱۶.۳) داده شده است، حل کرد.

۵۷.۳ $\phi(۵۰۴۰)$ و $\phi(۴۹۶۱۲۵)$ را محاسبه کنید.

حل. $۵۰۴۰ = ۲^{۴} \times ۳^{۲} \times ۵ \times ۷$. پس، بنابر (۱۶.۳) داریم

$$\begin{aligned}\phi(۵۰۴۰) &= \phi(۱۶)\phi(۹)\phi(۵)\phi(۷) \\ &= (۲^{۴} - ۲^{۳})(۳^{۲} - ۳)(۵ - ۱)(۷ - ۱) = ۸ \times ۶ \times ۴ \times ۶ = ۱۱۵۲\end{aligned}$$

همچنین، چون $۴۹۶۱۲۵ = ۳^{۴} \times ۵^{۳} \times ۷^{۲}$، لذا

$$\phi(۴۹۶۱۲۵) = (۳^{۴} - ۳^{۳})(۵^{۳} - ۵^{۲})(۷^{۲} - ۷) = ۲۲۶۸۰۰$$

۵۸.۳ اگر $n \geq ۳$، ثابت کنید $\phi(n)$ زوج است.

حل. اگر n هیچ عامل فرد نداشته باشد، آنگاه n به‌صورت ۲^k است که در آن $k \geq ۲$. در این‌صورت $\phi(n) = ۲^{k-۱}$ که روشن است عددی زوج است. اگر n عامل اول فرد مانند p داشته باشد می‌توانیم بنویسیم $n = p^{\alpha}q$ که $\alpha \geq ۱$ و $q \geq ۱$ و $(p, q) = ۱$. در این حالت $\phi(n) = p^{\alpha-۱}(p - ۱)\phi(q)$، و لذا زوج است.

۵۹.۳ فرض می‌کنیم $m > ۱$. ثابت کنید $\phi(m) = m - ۱$ اگر و تنها اگر m اول باشد.

حل. اگر m اول باشد، روشن است که اعداد ۱، ۲، . . .، $m - ۱$ همگی نسبت به m اول‌اند، و لذا از تعریف نتیجه می‌شود که $\phi(m) = m - ۱$. بعکس، اگر m اول نباشد، m یک مقسوم‌علیه سَرِه مانند d دارد، که نمی‌تواند با m متباین باشد. لذا حداقل یک عدد صحیح مثبت کوچکتر از m وجود دارد که با m متباین نیست، و از این‌رو $\phi(m) \leq m - ۲$.

۶۰.۳ به‌ازای چه مقادیری از n تساوی $\phi(n) = n - ۲$ برقرار است؟

حل. روشن است که، تمام اعداد ۱، ۲، . . .، $n - ۱$ بجز یکی باید با n متباین باشند. لذا n دقیقاً باید یک مقسوم‌علیه سَرِه داشته باشد، و در نتیجه عدد اول p وجود دارد که $n = p^۲$. لذا $\phi(n) = p(p - ۱)$. از مساوی قرار دادن این عبارت با $p^۲ - ۱$ خواهیم‌داشت $p = ۲$. بنابراین $n = ۴$.

۶۱.۳ ثابت یا رد کنید اگر $d|n$، آنگاه $\phi(d)|\phi(n)$.

حل ۱. آشکار است که

$$\phi(d) = d\prod_{p|d}\left(۱ - \frac{۱}{p}\right) \Big| n\prod_{p|n}\left(۱ - \frac{۱}{p}\right) = \phi(n)$$

حل ۲. اگر p_i عامل اولی از d باشد، فرض می‌کنیم $p_i^{n_i}$ و $p_i^{d_i}$ بزرگترین توان p_i باشند که به‌ترتیب n و d را عاد می‌کنند. بنابر (۱۶.۳)، $p_i^{n_i}$ عامل $(p_i - ۱)p_i^{n_i - ۱}$ را در عبارت $\phi(n)$، و $p_i^{d_i}$ عامل $(p_i - ۱)p_i^{d_i - ۱}$ را در عبارت $\phi(d)$ تولید می‌کنند. چون $d_i \leq n_i$، نتیجه حاصل می‌شود.

۶۲.۳ فرض می‌کنیم که $a = ۲^k b$ و b فرد باشد. اگر $\phi(x) = a$، ثابت کنید که x حداکثر k عامل اول فرد دارد.

حل. اگر p عامل اول فردی از x باشد، $p - ۱$ در عبارت $\phi(x)$ ظاهر می‌شود. چون بنابه فرض، $\phi(x)$ دقیقاً k عامل ۲ دارد، پس x نمی‌تواند بیش از k عامل اول فرد داشته باشد. البته x می‌تواند کمتر از k عامل اول فرد داشته باشد. مثلاً، اگر $b = ۱$ و $x = ۲^{k+۱}$، آنگاه x هیچ عامل اول فرد ندارد.

۶۳.۳ با استفاده از مسألهٔ ۶۲.۳ اعداد n را تعیین کنید به‌طوری که $\phi(n)$ بر ۴ بخشپذیر نباشد.

حل. مقصود یافتن nهایی است که $\phi(n) = ۲b$ یا $\phi(n) = b$ که b فرد است. لذا بنابر مسألهٔ قبل، n حداکثر یک عامل اول فرد دارد. اگر $n = ۲^\alpha$ داریم $\phi(n) = ۲^{\alpha-۱}$، پس $\alpha = ۱$ یا $\alpha = ۲$: در این حالت، $n = ۲$ یا $n = ۴$. اگر $n = ۲^\alpha p^k$، داریم $\phi(n) = \phi(۲^\alpha)\phi(p^k)$. اما $\phi(p^k) = p^{k-۱}(p-۱)$. در این‌صورت $p-۱$ زوج است و چون $۴ \nmid \phi(n)$ پس p به‌صورت $۴q+۳$ می‌تواند باشد. از طرفی، چون $۲|\phi(p^k)$ پس $\phi(۲^\alpha)$ فقط ۱ را اختیار می‌کند، لذا $\alpha = ۰$ یا $\alpha = ۱$. در نتیجه کلیه مقادیر ممکن برای n عبارت‌اند از ۱، ۲، ۴، و اعداد به‌صورت p^k یا $۲p^k$ که p عدد اول به‌صورت $۴q+۳$ است.

۶۴.۳ ثابت کنید $\phi(۲n) = \phi(n)$ اگر و تنها اگر n فرد باشد.

حل. اگر n فرد باشد، داریم $(n, ۲) = ۱$ و لذا $\phi(۲n) = \phi(۲)\phi(n) = \phi(n)$. بعکس، فرض کنیم $n = ۲^k m$، که m فرد است. اگر $k \geq ۱$ داریم

$$\phi(n) = \phi(۲^k)\phi(m) = ۲^{k-۱}\phi(m)$$

و $\phi(۲n) = ۲^k\phi(m)$؛ از آنجا، $\phi(۲n) = ۲\phi(n) \neq \phi(n)$. لذا، $k = ۰$ و بنابراین n فرد است.

۶۵.۳ فرض می‌کنیم n زوج باشد، ثابت کنید $\phi(n) = n/۲$ اگر و تنها اگر $n = ۲^k$ که در آن $k \geq ۱$.

حل. اگر $n = ۲^k$ با $k \geq ۱$، آنگاه $\phi(n) = ۲^{k-۱} = n/۲$. حال، فرض کنیم $n = ۲^k m$ که در آن m فرد است. داریم $\phi(n) = ۲^{k-۱}\phi(m)$. لذا، اگر $\phi(n) = n/۲$، آنگاه $\phi(m) = ۱$، پس $m = ۱$. در نتیجه $n = ۲^k$.

۶۶.۳ فرض می‌کنیم n عدد طبیعی ثابتی باشد. ثابت کنید فقط تعداد متناهی x وجود دارد به‌طوری که $\phi(x) = n$. (در واقع، ممکن است هیچ xی یافت نشود.)

حل. اگر $x = \prod p^\alpha$، آنگاه $\phi(x) = n$ ایجاب می‌کند که $n = \prod_{p|x}(p^\alpha - p^{\alpha-۱})$ چون فقط یک تعداد متناهی روش برای تجزیهٔ n به‌صورت حاصلضرب اعداد صحیح وجود دارند، لذا حداکثر تعداد متناهی x وجود دارند که معادلهٔ $\phi(x) = n$ را حل کنند.

۶۷.۳ کلیهٔ اعداد صحیح n را بیابید به‌طوری که (الف) $\phi(n) = ۱۸$؛ (ب) $\phi(n) = ۸۰$.
(راهنمایی: برای قسمت (الف) از مسألهٔ ۶۳.۳ استفاده کنید.)

حل. (الف) چون ۱۸ فقط یک عامل ۲ دارد، مسألهٔ ۶۳.۳ ایجاب می‌کند که $n = p^k$ یا $n = ۲p^k$، که در آن p عددی است اول و $p \equiv ۳ (\mathrm{mod}\ ۴)$. اگر $n = p^k$ یا $n = ۲p^k$، آنگاه $\phi(n) = p^{k-۱}(p-۱)$. اگر $k > ۱$، آنگاه $p = ۳$، و n یکی از اعداد ۲۷ یا ۵۴ است. اگر $k = ۱$، آنگاه $p = ۱۹$، و n برابر ۱۹ یا ۳۸ است.

(ب) فرض کنیم $n \prod p^a$. چون n به‌صورت توانی از ۲ نیست، عدد اول فردی مانند p وجود دارد که n را می‌شمارد. اگر $p^۲|n$ به‌ازای یک عدد فرد اول p، آنگاه $p|\phi(n)$ ((۱۶.۳) را ببینید). بنابراین، اگر به‌ازای عدد اول فردی مانند p، $p^۲|n$، آنگاه $p = ۵$ و $n = ۲۵m$، که در آن $(m, ۵) = ۱$ و لذا $\phi(m) = ۸۰/۲۰ = ۴$. به آسانی دیده می‌شود که m با $۲^۳$ یا ۳×۲^۲ برابر است، و از این‌رو $n = ۲۰۰$ یا $n = ۳۰۰$. اگر به‌ازای هر عدد اول فرد p، $p^۲ \nmid n$، آنگاه عامل ۵ در $\phi(n)$ از $p - ۱$ حاصل می‌شود، که در آن p عدد اول فردی است که n را می‌شمارد. بنابراین، $p - ۱ = ۲^j \times ۵$، که $۱ \le j \le ۴$. به آسانی دیده می‌شود که فقط برای $j = ۱$ و $j = ۳$ عدد p اول است. اگر $j = ۱$، آنگاه $p = ۱۱$ و $n = ۱۱m$، و لذا $\phi(m) = ۸$. به آسانی می‌توان دید که مقادیر m عبارت‌اند از $۲^۴$، ۳×۲^۳، ۵×۲^۲، $۵ \times ۳ \times ۲$، یا ۵×۳. این ایجاب می‌کند که n برابر باشد با ۱۷۶، ۲۶۴، ۲۲۰، ۳۳۰، یا ۱۶۵. اگر $j = ۳$، آنگاه $p = ۴۱$، و $n = ۴۱m$ به‌طوری که $\phi(m) = ۲$؛ لذا n برابر است با ۱۶۴، ۱۲۳، یا ۲۴۶. در نتیجه کلیهٔ مقادیر n که در $\phi(n) = ۸۰$ صدق می‌کنند عبارت‌اند از ۱۲۳، ۱۶۴، ۱۶۵، ۱۷۶، ۲۰۰، ۲۲۰، ۲۴۶، ۲۶۴، ۳۰۰، و ۳۳۰.

۶۸.۳ (الف) نشان دهید که هیچ عدد صحیح n وجود ندارد که $\phi(n) = ۱۴$.
(ب) اگر $e \ge ۱$ ثابت کنید هیچ عدد صحیح n وجود ندارد که $\phi(n) = ۲ \times ۷^e$. (راهنمایی: نشان دهید که $۱ + ۷^e \times ۲$ هیچ‌گاه اول نخواهد بود.)
(ج) حالتهایی را بیابید که در آنها دو برابر یک عدد صحیح فرد برابر هیچ $\phi(n)$ی نشود.

حل. روشن است که (الف) حالت خاصی از (ب) است. چون ۲×۷^e بر ۲ بخشپذیر است ولی بر ۴ بخشپذیر نیست، لذا بنابر مسألهٔ ۶۳.۳، از $\phi(n) = ۲ \times ۷^e$ نتیجه می‌شود که n به‌صورت p^k یا $۲p^k$ است که p به‌صورت $۴t + ۳$ است. در هر دو حالت $\phi(n) = p^{k-۱}(p-۱)$ و لذا با توجه به $\phi(n) = ۲ \times ۷^e$ داریم $k = ۱$ و $p - ۱ = ۲ \times ۷^e$. یعنی $p = ۱ + ۲ \times ۷^e$.

ولی، چون $۷^e \equiv ۱ (\mathrm{mod}\ ۳)$، پس $۱ + ۷^e \times ۲$ بر ۳ بخشپذیر است و لذا اگر $e \geq ۱$ آنگاه $p = ۲ \times ۷^e + ۱$ اول نیست.

(ج) دقیقاً همان استدلال کارساز است اگر به جای ۷ هر عدد اول به‌صورت $۳t + ۱$ گذاشته شود، یا اگر به جای ۷ عدد $p^۲$ گذاشته شود که p به‌صورت $۳t + ۲$ است، از این‌رو، مثلاً nی وجود ندارد به‌طوری که $\phi(n) = ۲ \times ۱۳^e$ یا $\phi(n) = ۲ \times ۱۱^{۲e}$. همین‌طور، به جای ۷^e می‌توانیم $۳^{۴e+۳}$ را به‌کار بریم، زیرا $۱ + ۳^{۴e+۳} \times ۲$ همواره بر ۵ بخشپذیر است. با اندکی تغییر در برهان، می‌توانیم ۱۳×۷ را به جای ۷ نیز به‌کار بریم.

۶۹.۳ اگر $\phi(n) | n - ۱$، ثابت کنید n خالی از مربع است (یعنی، n بر هیچ عدد صحیح مربع بزرگتر از ۱ بخشپذیر نیست).

حل. اگر n خالی از مربع نباشد، آنگاه عدد اول p وجود دارد که $p^۲ | n$. از طرفی با توجه به (۱۶.۳)، $p | \phi(n)$. لذا اگر $\phi(n) | n - ۱$، آنگاه $p | n - ۱$ لذا p اعداد n و $n - ۱$ را می‌شمارد که ممکن نیست.

توضیح. یک حدسیه خیلی قدیمی می‌گوید که اگر $n > ۱$ و $\phi(n) | n - ۱$، آنگاه n اول است.

◁ **۷۰.۳** ثابت کنید $\phi(mn) = m\phi(n)$ اگر و تنها اگر هر عدد اول که m را می‌شمارد عدد n را نیز بشمارد. به‌ویژه، به‌ازای هر $e \geq ۱$، $\phi(n^e) = n^{e-۱}\phi(n)$.

حل. فرض کنیم $P_k = \prod_{p|k}(۱ - ۱/p)$. اگر هر عدد اول که m را می‌شمارد عدد n را نیز بشمارد، آنگاه روشن است که $P_{mn} = P_n$. لذا بنابر (۱۶.۳) داریم

$$\phi(mn) = mnP_{mn} = m(nP_n) = m\phi(n)$$

بعکس فرض می‌کنیم $\phi(mn) = m\phi(n)$. در این‌صورت بنابر (۱۶.۳) داریم $P_{mn} = P_n$. اگر عدد اولی مانند p وجود داشته باشد که m را بشمارد ولی n را نشمارد، آنگاه جملهٔ $(۱ - ۱/p)$ در حاصلضرب P_{mn} ظاهر می‌شود ولی در P_n ظاهر نمی‌شود، در حالی‌که برای هر عدد اول q که n را بشمارد، $۱ - ۱/q$ در هر دو حاصلضرب ظاهر می‌شود. لذا $P_{mn} \leq (۱ - ۱/p)P_n$، که با $P_{mn} = P_n$ تناقض دارد.

توضیح. حالت خاص مستقلاً و به آسانی ثابت می‌شود. داریم

$$\phi(n^e) = n^e \prod_{p|n}\left(۱ - \frac{۱}{p}\right) = n^{e-۱} \times n\prod_{p|n}\left(۱ - \frac{۱}{p}\right) = n^{e-۱}\phi(n)$$

۷۱.۳ ثابت کنید $\phi(m)/m = \phi(n)/n$ اگر و تنها اگر m و n دارای عاملهای اول واحدی (احتمالاً با توانهای متفاوت) باشند.

حل. قرار می‌دهیم $P_k = \prod_{p|k}(1 - 1/p)$؛ لذا بنابر (۱۶.۳)، $\phi(k) = kP_k$. اگر m و n عاملهای اول واحدی داشته باشند، آنگاه روشن است $P_m = P_n$، و لذا $\phi(m)/m = \phi(n)/n$. (رابطهٔ اخیر از مسألهٔ قبل نیز نتیجه می‌شود، زیرا فرض اینکه m و n دارای عاملهای اول واحدی هستند ایجاب می‌کند که $\phi(mn) = m\phi(n)$ و نیز $\phi(mn) = n\phi(m)$ بنابراین $\phi(m)/m = \phi(n)/n$.)

بعکس، فرض می‌کنیم $\phi(m)/m = \phi(n)/n$. لذا $P_m = P_n$. فرض می‌کنیم $p_1, \ldots, p_s$ عوامل اول m و $q_1, \ldots, q_t$ عوامل اول n هر دو به ترتیب صعودی باشند. از $P_m = P_n$ نتیجه می‌شود که

$$q_1 q_2 \cdots q_t(p_1 - 1) \cdots (p_s - 1) = p_1 \cdots p_s(q_1 - 1) \cdots (q_t - 1)$$

فرض می‌کنیم $q_t \geq p_s$. چون q_t طرف چپ معادلهٔ فوق را می‌شمارد و چون بزرگتر از هر جملهٔ طرف راست به استثنای احتمالاً p_s است از اینجا نتیجه می‌شود که $q_t = p_s$. حال جملات شامل q_t و p_s را از دو طرف حذف می‌کنیم (اگر $p_s > q_t$، استدلال به همین گونه است.) اگر این روند را ادامه دهیم، می‌بینیم که $s = t$ و به‌ازای هر i، $p_i = q_i$.

۷۲.۳ فرض می‌کنیم $n \geq 2$. ثابت کنید که مجموع تمام اعداد طبیعی کوچکتر از n که با n متباین‌اند برابر است با $\frac{1}{2}n\phi(n)$ (راهنمایی: اگر $(a, n) = 1$، نشان دهید $(n - a, n) = 1$.)

حل. مشاهده می‌کنیم که a نسبت به n اول است اگر و تنها اگر $n - a$ نسبت به n اول باشد (۲۲.۱ را ببینید). هر $a \leq n/2$ را که با n متباین است با $n - a$ جفت می‌کنیم. جز در حالت $n = 2$، که نتیجه بدیهی است، داریم $(n/2, n) \neq 1$. لذا a هرگز با خودش جفت نمی‌شود. از آنجا که دقیقاً $\phi(n)/2$ این چنین جفتها که مجموع هر جفت برابر n است وجود دارند، نتیجه حاصل می‌شود.

◁ **۷۳.۳** فرض می‌کنیم P حاصلضرب مقسوم‌علیه‌های اول متمایز (m, n) باشد (حاصلضرب تهی را برابر ۱ تعریف می‌کنیم). ثابت کنید که $\phi(mn)/\phi(m)\phi(n) = P/\phi(P)$. به‌ویژه، اگر $(m, n) > 1$، نشان دهید $\phi(m, n) > \phi(m)\phi(n)$.

حل. می‌توانیم فرض کنیم که دقیقاً اعداد اول واحدی m و n را می‌شمارند. زیرا اگر p عدد

m را بشمارد ولی n را نشمارد، فرض کنیم p^e بزرگترین توانی از p باشد که m را می‌شمارد، و قرار می‌دهیم $m' = m/p^e$. در این‌صورت $\phi(mn) = \phi(m'n)\phi(p^e)$، و

$$\phi(m)\phi(n) = \phi(m')\phi(p^e)\phi(n)$$

بنابراین، اگر m با m' تعویض شود، نسبت $\phi(mn)/(\phi(m)\phi(n))$ تغییر نمی‌کند.

لذا فرض می‌کنیم $m = \prod p_i^{a_i}$ و $n = \prod p_i^{b_i}$؛ در این‌صورت (m,n) بر هر p_i بخشپذیر است. بنابر (۱۶.۳)، $\phi(mn)$ حاصلضرب جمله‌هایی به‌صورت $p^{a+b-1}(p-1)$ است که p روی p_iها تغییر می‌کند. جملهٔ متناظر در $\phi(m)\phi(n)$ عبارت است از $p^{b-1}(p-1)p^{a-1}(p-1)$، لذا نسبت این جمله‌ها $p/(p-1)$ می‌شود، که دقیقاً همان سهمی است که p در نسبت $P/\phi(P)$ پدید می‌آورد.

سرانجام، اگر $(m,n) > 1$، آنگاه $P > 1$ و لذا $P/\phi(P) > 1$، زیرا به‌ازای هر $k \geq 2$، $\phi(k) \leq k-1$. لذا بنابر استدلال قبلی، داریم $\phi(mn)/(\phi(m)\phi(n)) > 1$، یعنی، $\phi(mn) > \phi(m)\phi(n)$.

◁ **۷۴.۳** اگر $n \geq 1$، ثابت کنید $\sum_{d|n} \phi(d) = n$.

حل. فرض می‌کنیم N دستگاه کامل مانده‌های $\{0, 1, 2, \ldots, n-1\}$ باشد. اگر d یک مقسوم‌علیه n باشد، فرض می‌کنیم N_d متشکل از همهٔ عناصر $k \in N$ باشد به‌طوری که $(k,n) = n/d$. لذا N_d متشکل از عناصر N به‌صورت $e(n/d)$ است، که $1 \leq e \leq d$ و $(e,d) = 1$؛ به‌ویژه، مجموعهٔ N_d دارای $\phi(d)$ عنصر است. آشکار است که اگر $d \neq d'$، آنگاه $N_d \neq N_{d'}$. وقتی d مقسوم‌علیه‌های n را اختیار می‌کند، n/d نیز مقسوم‌علیه‌های n را اختیار می‌کند، و لذا هر عنصر N به یک N_d یکتای معین تعلق دارد. چون N دارای n عنصر و هر N_d دارای $\phi(d)$ عنصر است، نتیجه می‌شود که $n = \sum_{d|n} \phi(d)$.

تمرینهایی برای فصل ۳

۱. باقیماندهٔ تقسیم $24!$ را بر ۲۹ پیدا کنید.

۲. باقیماندهٔ تقسیم $3(26i)$ بر ۲۹ چقدر است؟

۳. آیا درست است که $1991! \equiv 1 \pmod{1993}$؟ آیا از این نتیجه می‌شود که ۱۹۹۳ عددی است اول؟

۴. کوچکترین ماندهٔ مثبت $53!$ به پیمانهٔ ۵۹ چقدر است؟

۵. قضیهٔ ویلسن را برای یافتن باقیماندهٔ تقسیم !۲۷ بر ۸۹۹ بکار برید. (راهنمایی: ابتدا ۸۹۹ را تجزیه کنید.)

۶. اگر p اول باشد، قضیهٔ ویلسن را برای اثبات $(p-1)! \equiv p-1 (\mathrm{mod}\, p(p-1))$ بکار برید.

۷. باقیماندهٔ تقسیم !۱۵ بر ۳۲۳ را بدست آورید.

۸. آیا $۷! + ۷۷! \times ۱۶$ مضرب ۷۹ است؟

◁ ۹. قضیهٔ ویلسن را برای یافتن باقیماندهٔ تقسیم !۴۲ بر ۲۰۲۱ بکار برید.

۱۰. قضیهٔ اویلر را برای یافتن آخرین دو رقم (رقمهای یکان و دهگان) $۷^{۲۰۰}$ بکار برید.

۱۱. آیا $۶۹^{۶۷} + ۵۴^{۱۰۳}$ مضرب ۱۳ است؟

۱۲. همنهشتی $x^{۲۰۰} - ۲۰۰x \equiv ۰ (\mathrm{mod}\, ۱۹۹)$ را حل کنید. (۱۹۹ اول است.)

۱۳. بازای کدام اعداد اول p، $۲^p + ۱$ بر p بخشپذیر است؟

۱۴. اثبات یا رد کنید: اگر p عدد اول فردی باشد، آنگاه $n^{۲p-۱} \equiv n (\mathrm{mod}\, ۲p)$.

۱۵. فرض کنید p و q دو عدد اول فرد با $q > p$ باشند. اگر $q-۱$ بر $p-۱$ بخشپذیر باشد، ثابت کنید $۴^{q-۱} - ۱$ مضرب pq است.

۱۶. قضیهٔ اویلر را برای یافتن سه رقم آخر $۳^{۹۶۱۰}$ بکار برید.

۱۷. کوچکترین ماندهٔ مثبت $۳^{۷۲۵}$ به پیمانهٔ ۶۷۵ چقدر است؟

۱۸. باقیماندهٔ تقسیم $۱۱^{۱۹۶}$ بر ۱۴۴ را بدست آورید.

۱۹. باقیماندهٔ تقسیم $۳^{۱۰۰۰۰}$ بر ۳۵ را بدست آورید. (محاسبات را توجیه کنید.)

۲۰. کوچکترین ماندهٔ مثبت $۷^{۴۴۳}$ به پیمانهٔ ۱۴۴، و $۱۱^{۴۸۴}$ به پیمانهٔ ۲۸۸ چقدر است؟

۲۱. باقیماندهٔ تقسیم $۱۱۷۷^{۱۱۷۷}$ بر ۹ چقدر است؟

۲۲. آخرین دو رقم صحیح $۷^{۸۹}$ را تعیین کنید.

۲۳. ثابت کنید بازای هر عدد فرد n، $n^{۲۵} - n$ مضرب ۵۴۶۰ است.

۲۴. ثابت کنید که بازای هر عدد فرد n، $n^{۵۰} - n^۲$ بر ۱۲۲۴۰ بخشپذیر است.

۲۵. ثابت کنید که بازای همهٔ اعداد صحیح m و n متباین با ۱۳۳ عدد $m^{۱۸} - n^{۱۸}$ بر ۱۳۳ بخشپذیر است.

۲۶. ثابت کنید که بازای هر دو عدد صحیح m و n عدد $mn(m^{۶۰} - n^{۶۰})$ بر ۵۶۷۸۶۷۳۰ بخشپذیر است.

۲۷. آیا درست است که بازای هر n، $n^{۳۷} - n$ بر ۵۴ بخشپذیر است؟

۲۸. ثابت کنید بازای هر n، $n^{۱۳} - n$ بر ۲۷۳ بخشپذیر است.

◁ **۲۹.** با استفاده از قضیهٔ اویلر ثابت کنید که $x^{۸۹} \equiv ۳ (\mathrm{mod}\ ۲۲۰۰)$ جوابی یکتا دارد، و این جواب را پیدا کنید.

۳۰. (الف) با استفاده از قضیهٔ فرما همنهشتی $۱۸x \equiv ۲۳ (\mathrm{mod}\ ۳۷)$ را حل کنید.

(ب) برای حل $۷x \equiv ۳۹ (\mathrm{mod}\ ۵۴)$ از قضیهٔ اویلر استفاده کنید.

(ج) همنهشتیهای قسمتهای (الف) و (ب) را با استفاده از الگوریتم اقلیدسی حل کنید.

۳۱. فرض کنید m عدد صحیح مثبتی باشد که با $a(a-۱)$ متباین است. نشان دهید $۱ + a + a^۲ + \cdots + a^{\phi(m)-۱} \equiv ۰ (\mathrm{mod}\ m)$.

۳۲. آیا عدد صحیح مثبتی مانند m وجود دارد که در تقسیم عدد ۲^m بر m باقیمانده ۱ شود؟

۳۳. $\phi(۳۳۰)$ و $\phi(۸۵۷۵۰۰)$ را به‌دست آورید.

۳۴. $\phi(۱۲!)$ و $\phi(۱۷!)$ را محاسبه کنید.

۳۵. ثابت کنید $\phi(۴۱۵۸۰۰)$ مضرب ۱۶ است.

۳۶. تعداد اعداد گویای مثبت تحویل‌یافتهٔ r/s را بیابید به‌طوری که $r/s < ۱$ و $۱ \le s \le ۱۰$.

۳۷. تمام اعداد صحیح مثبت کوچکتر از n را بیابید به‌طوری که $\phi(n) | n$.

۳۸. آیا درست است که $\phi(n) \ge \sqrt{n}/۲$؟

۳۹. ثابت یا رد کنید: $\phi(۱۲^k) = ۱۲^{k-۱}\phi(۱۲)$.

۴۰. آیا تعداد نامتناهی عدد صحیح مثبت n وجود دارد به‌طوری که $n = ۳\phi(n)$؟

۴۱. آیا تعداد نامتناهی n وجود دارد به‌طوری که $\phi(n) = n/۴$.

۴۲. فرض کنید p عدد اول فردی باشد که $۲p + ۱$ مرکب است. ثابت کنید عدد صحیح مثبتی مانند n وجود ندارد به‌طوری که $\phi(n) = ۲p$.

۴۳. به‌ازای چه مقدار n، $\phi(۲n) > \phi(n)$؟

۴۴. اثبات یا رد کنید: فقط برای تعداد متناهی عدد فرد n، $\phi(n)$ مربع کامل است.

۴۵. اگر $n > ۱$ و $\phi(n)$ عدد $۱ - n$ را بشمارد، ثابت کنید که n حاصلضرب اعداد اول متمایز است.

۴۶. شش مقدار از n بیابید به‌طوری که $\phi(n) = \phi(n + ۲)$.

◁ **۴۷.** فرض کنید a و b دو عدد صحیح مثبت متباین باشند، و فرض می‌کنیم p عدد اول فردی باشد. ثابت کنید که بزرگترین مقسوم‌علیه مشترک $a + b$ و $(a^p + b^p)/(a + b)$ یا ۱ است یا p. (راهنمایی: فرض کنید $c = a + b$؛ پس $a^p + b^p = (c - b)^p + b^p$. با استفاده از قضیهٔ دوجمله‌یی $(c - b)^p$ را بسط دهید.)

ملاحظاتی برای فصل ۳

۱. قضیهٔ فرما یک قضیهٔ بنیادی در نظریهٔ مقدماتی اعداد است، لذا پی بردن به انگیزه‌ای که ممکن است فرما را به آن هدایت کرده باشد جالب خواهد بود. در سالهای ۱۶۳۰، ریاضیدانان پاریسی، از جمله فِرنیکل، مِرسن، و حتی دکارتِ گوشه‌گیر، به دنبال مسائلی بودند که با «اعداد تام» و «اول بودن» آنچه اکنون به اعداد مرسن معروف‌اند، ارتباط داشت.

در زمان فرما، اول بودن عدد مرسن $M_p = ۲^p - ۱$ به‌ازای $p = ۲, ۳, ۵, ۷, ۱۳, ۱۷, ۱۹$ و مرکب بودن آن به‌ازای $p = ۱۱, ۲۳$ شناخته شده بود: $M_{۱۱}$ حاصلضرب ۲۳ در ۸۹ است، و $M_{۲۳}$ مضرب ۴۷ است (مطلبی که توسط فرما کشف شد). امکان دارد که صورت این مقسوم‌علیه‌های $M_{۱۱}$ و $M_{۲۳}$ فرما را به این حدسیه که هر مقسوم‌علیه M_p به‌صورت $۲kp + ۱$ است راهنمایی کرده باشد (قضیهٔ (۸.۳) را ببینید).

می‌توان قضیهٔ اصلی فرما را ــ یعنی اینکه $۲^p - ۲$ از عدد اول p است ــ به‌عنوان نتیجه‌ای از (۸.۳) به‌دست آورد، زیرا (۸.۳) ایجاب می‌کند که تمام مقسوم‌علیه‌های $۲^p - ۱$ به‌صورت $۲kp + ۱$ باشند (چون که هر مقسوم‌علیه اول به این صورت است)؛ به‌ویژه، خودِ $۲^p - ۱$ به این صورت است، و لذا $۲^p - ۲$ مضربی از p است.

۲. اکنون اثباتِ سال ۱۷۵۸ اویلر از قضیهٔ فرما را که در مقدمه ذکر شد به اختصار شرح می‌دهیم. استدلال از نظر تاریخی مهم است، زیرا نشانه‌ای از یک قضیهٔ پایه‌یی از شاخهٔ جدید ریاضیات است که نظریهٔ گروهها نامیده می‌شود.

فرض کنیم a بزرگتر از یک است و بر p بخشپذیر نیست، و باقیمانده‌های تقسیم $۱, a, a^۲, \ldots, a^{p-۱}$ بر p را در نظر می‌گیریم. حداکثر $p - ۱$ باقیماندهٔ ممکن وجود دارد، اما این فهرست p عضو دارد، لذا حداقل دو تا از باقیمانده‌ها برابرند. از این‌رو، i و j با $۰ \le i < j \le p - ۱$ وجود دارند به‌طوری که $a^i \equiv a^j \pmod p$. چون a و p نسبت به هم اول‌اند، می‌توانیم همنهشتی را i بار بر a تقسیم کنیم و $a^{j-i} \equiv ۱ \pmod p$ را به‌دست آوریم. لذا یک عدد n با $۱ \le n \le p - ۱$ وجود دارد به‌طوری که $a^n \equiv ۱ \pmod p$.

اکنون ثابت می‌کنیم که اگر n کوچکترین عدد صحیح مثبتی باشد که $a^n \equiv ۱ \pmod p$، آنگاه عدد n عدد $p - ۱$ را می‌شمارد. این مطلب بلافاصله نتیجه می‌دهد که $a^{p-۱} \equiv ۱ \pmod p$.

فرض می‌کنیم S معرف مجموعهٔ $\{۱, a, a^۲, \ldots, a^{n-۱}\}$ باشد. این توانهای a همگی به پیمانهٔ p ناهمنهشت‌اند؛ در غیر این‌صورت، مانند بالا، می‌توانیم عددی مانند m با $۱ \le m < n$ به‌دست آوریم به‌طوری که $a^m \equiv ۱ \pmod p$. اکنون اعداد $۱, ۲, \ldots, p - ۱$ را به خانواده‌هایی تقسیم می‌کنیم به این ترتیب که x و y به یک خانواده تعلق دارند اگر $s \in S$ وجود داشته باشد

به‌طوری که $y \equiv sx \pmod{p}$. می‌توان نشان داد که خانوادهٔ هر x دقیقاً n عضو دارد، یعنی، باقیمانده‌های تقسیم x، ax، ...، $a^{n-1}x$ بر p بخشپذیر. لذا اگر f تعداد خانواده‌ها باشد، آنگاه $nf = p-1$؛ در نتیجه n عدد $p-1$ را می‌شمارد.

۳. قضیهٔ فرما و قضیهٔ اویلر کار یافتن کوچکترین ماندهٔ (یعنی، باقیمانده) نامنفی را بسیار آسان می‌سازند وقتی که یک عدد با توان بزرگ بر یک عدد صحیح مثبت (اول یا غیر آن) تقسیم می‌شود. روشهای محاسبه در حل مسائل ۱.۳، ۲.۳، ۵.۳، و ۴۳.۳ بایستی به دقت بررسی شوند.

نکات مهم عبارت‌اند از: ابتدا با برداشتن هر تعداد ممکن مضرب $p-1$، اگر p اول باشد، یا در حالت کلی m، هر تعداد مضرب $\phi(m)$ اگر محاسبهٔ $\phi(m)$ آسان باشد، از توان آن را تقلیل می‌دهیم. (این عمل دقیقاً به معنای یافتن کوچکترین مانده‌های نامنفی از توان به‌ترتیب ، به پیمانهٔ $p-1$ یا $\phi(m)$ است.) حاصل کار عبارتی به‌صورت a^k با $0 \le k < \phi(m)$ است، که بایستی به پیمانهٔ m بدل شود. در بسیاری از حالتها، مقرون به‌صرفه است که به‌طور جداگانه با توانهای اولِ تجزیهٔ m عمل کنیم و سپس با استفاده از قضیهٔ باقیماندهٔ چینی کار را جمع‌وجور کنیم.

برای مقادیر بزرگِ k، اغلب مناسبترین کار آن است که ابتدا k را به‌صورت مجموع توانهای متمایز ۲ بنویسیم. (مثلاً، اگر $k = ۲۹$، آنگاه $k = ۱۶+۸+۴+۱$؛ لذا $a^{۲۹} = a^{۱۶}a^{۸}a^{۴}a^{۱}$.) می‌توان مانده‌های به پیمانهٔ m از توانهای a، $a^۲$، $a^۴$، ... را با تکرار مربع کردن و تبدیل به پیمانهٔ m به‌دست آورد (مسألهٔ ۲.۳ را ببینید). سرانجام، کوچکترین ماندهٔ نامنفی خود a^k از ضرب کوچکترین مانده‌های نامنفی توانهای مناسب a و (در صورت لزوم) تبدیل به پیمانهٔ m در هر مرحله، به‌دست می‌آید.

۴. شبه اولهای در پایهٔ ۲ بسیار کمیاب‌تر از اعداد اول هستند. مثلاً ۴۵۵۰۵۲۵۱۲ عددِ اولِ کمتر از $۱۰^{۱۰}$ وجود دارند اما فقط ۱۴۸۸۴ شبه اول در پایهٔ ۲. اگر یک عددِ بزرگِ n (مثلاً، عددی با ۱۰۰ رقم) در همنهشتی $۲^{n-۱} \equiv ۱ \pmod{n}$ صدق کند، به سختی احتمال دارد که n واقعاً اول باشد. هنری کوهن[1] یک عدد $n > ۱$ را یک «عدد اول از درجهٔ صنعتی» خوانده است اگر $۲^{n-۱} \equiv ۱ \pmod{n}$. می‌توان آنها را در کاربردهایی که اعدادِ اول خیلی بزرگ مورد نیازند، نظیر رمزنگاری یا تولید اعداد شبه‌تصادفی مطمئن به‌کار برد.

اگر به‌ازای چند مقدار a، مثلاً ۲، ۳، و ۵، $a^{n-۱} \equiv ۱ \pmod{n}$، و n حدود ۱۰۰ رقم داشته باشد، آنگاه احتمال اینکه n اول نباشد بسیار کمتر است از، مثلاً احتمال اینکه یک سیارک رایانه‌ای را که محاسبات را انجام می‌دهد از بین ببرد.

۵. روش رمزی‌سازی RSA. این روند، که در ابتدا توسط ر. ل. ریوست[2]، آ. شمیر[3]، و

1. Henri Cohen 2. R. L. Rivest 3. A. Shamir

ل. م. آدلمن[1]، بیان شد، اولین کاربرد مهم مالی نظریهٔ اعداد است. با استفاده از روش RSA، شما می‌توانید به مخاطب بگویید که چگونه پیامهای سری که برای شما فرستاده شده بایستی به‌صورت رمز درآورید. به‌رغم این، برای هرکس جز خود شما بی‌نهایت مشکل است که این پیامها را رمزگشایی کند.

می‌توانیم نمادهای صفحه‌کلید (رایانه) را با استفاده از اعداد صحیح دو رقمی به رمز درآوریم. با تکه‌تکه کردن مناسبِ پیام، می‌توانیم فرض کنیم که پیامها از اعداد k رقمی، مثلاً $k = ۱۵۰$، ساخته شده‌اند. حال دو عدد اول p و q را انتخاب می‌کنیم که هر یک لااقل دارای ۱۰۰ رقم باشند، و قرار می‌دهیم $n = pq$. همچنین یک شاخص رمزسازی e انتخاب می‌کنیم که با $\phi(n)$ متباین و نسبتاً بزرگ باشد؛ مثلاً e می‌تواند عدد اولی بزرگتر از p یا q باشد. شما جفت (e, n) را به مخاطب می‌گویید، اما p و q را به او نمی‌گویید.

کسی که بخواهد پیام ۱۵۰ رقمی x را برای شما بفرستد، y، باقیماندهٔ تقسیم x^e بر n را محاسبه و y را به شما منتقل می‌کند. با استفاده از روش مربع کردن مکرر محاسبهٔ y را می‌توان کاملاً سریع انجام داد. احتمال آنکه p یا q عدد n را بشمارد بسیار ناچیز است، لذا می‌توانیم فرض کنیم که x با n متباین است. حال نشان می‌دهیم که چگونه x را از y به‌دست می‌آوریم.

با آگاهی از p و q دارید، $\phi(n) = (p - ۱)(q - ۱)$ را محاسبه می‌کنید و سپس عدد صحیح یکتای d با $۰ < d < \phi(n)$ را پیدا می‌کنید به‌طوری که $de \equiv ۱ (\mathrm{mod}\, \phi(n))$. این عدد صحیح d شاخص رمزگشایی خوانده می‌شود. فرض می‌کنیم $de = ۱ + t\phi(n)$. سپس بنابر قضیهٔ اویلر،

$$y^d \equiv (x^e)^d = x \cdot (x^{\phi(n)})^t \equiv x \pmod{n}$$

و لذا x باقیماندهٔ تقسیم y^d بر n است. لذا با داشتن شاخص رمزگشایی d و عدد پیام رمزی y، به آسانی می‌توانیم x را پیدا کنیم.

پذیرفته شده است که روش رمزی‌سازی RSA قطعی است. به نظر نمی‌رسد که راهی برای رمزگشایی پیامهای رمزی‌سازی‌شدهٔ RSA بدون یافتن تجزیهٔ n وجود داشته باشد، و به نظر می‌رسد که تجزیهٔ اعداد صحیح ۲۰۰ رقمی خارج از دسترس الگوریتمهای امروزی باشد. گونه‌های مختلف روش RSA به‌طور گسترده به‌کار می‌روند و موجب علاقهٔ جدیدی در یافتن الگوریتمهای کارآمد برای تعیین اعداد اول و تجزیه شده‌اند. برای جزئیات بیشتر، کتابهایی را که D. Bressoud، P. Giblin، N. Koblitz، و H. Riesel نوشته‌اند و در کتابنامه فهرست شده‌اند ببینید.

1. L. M. Adleman

شرح مختصری از زندگینامه‌ها

پییر سیمون دو فرما در ۱۶۰۱ در فرانسه به دنیا آمد. حقوقدانی، که در زندگی خود نسبتاً دیر به ریاضیات وارد شد ــ بعد از سن ۳۰ سالگی ــ و ریاضیات را به‌عنوان سرگرمی در ایام فراغت دنبال می‌کرد. شاید به‌عنوان آخرین ریاضیدانِ بزرگِ «حرفه‌یی»، با بسیاری از شخصیتهای ریاضی طراز اول زمان خود مکاتبه داشت، آنها را (چنان که رسم شده بود) برای حل مسائلی که مطرح می‌کرد به چالش می‌طلبید.

یادداشتهای ریاضی فرما مرتب نبودند، شاید به این دلیل که هرگز قصد چاپ آنها وجود نداشت. (در واقع، فرما در دوران زندگی‌اش، هیچ‌یک از قضیه‌های خود در نظریهٔ اعداد را چاپ نکرد.) یادداشتهایش اغلب در حاشیهٔ کتابهایش نوشته می‌شدند، چشمگیرترین آنها نسخه‌ای از کتاب علم حساب دیوفانتوس است، که حاشیه‌اش «متأسفانه بسیار باریک» بود و برای اثبات آخرین قضیهٔ معروفش جا نداشت.

فرما مبانی هندسهٔ تحلیلی را حدود ده سال قبل از اینکه دکارت کارش را منتشر کند پایه‌ریزی کرد، و در مکاتباتش با پاسکال او را در پی‌ریزی مفاهیم ریاضی نظریهٔ احتمال یاری کرد. همچنین، روش او در یافتن مماس در نقاط یک منحنی الهام‌بخش نیوتون در بسط حساب دیفرانسیل شد. اما شاید برجسته‌تر از همه، با بررسیهایش در اعداد اول، بخشپذیری، مجموعهای مربعات، و معادلات دیوفانتی، از جمله روش نزول نامتناهی. مخترع نظریهٔ نوین اعداد شناخته شده است. فرما در ۱۲ ژانویهٔ ۱۶۶۵ درگذشت.

لئونهارت اویلر در ۱۷۰۷ در شهر بال سوئیس به دنیا آمد. در دانشگاه، اویلر تصمیم گرفت که فراگیری الهیات را دنبال نکند و در عوض به تحصیل ریاضیات به سرپرستی یاکوب برنولی بپردازد. اویلر بیشتر عمر خود را در برلین و سن‌پترزبورگ گذراند. بر خلافِ فرما، اویلر در بیان چگونگی دستیابی به قضیه‌هایش خیلی دست و دل باز بود. گرچه در ۱۷ سال آخر عمرش نابینا بود، با وجود این پرکارترین ریاضیدان در طول تاریخ بوده است. انتظار می‌رود که کارهای گردآوری شده‌اش ــ نزدیک به ۹۰۰ کتاب و مقاله ــ به ۷۵ مجلد برسد.

بسیاری از نمادهای جدید ریاضی از اویلر است (مثلاً، $f(x)$ به‌عنوان نماد تابع و $\sum$ برای علامت مجموعیابی). او کاشف نظریهٔ تحلیلی اعداد است و اولین کسی است که مانده‌های توانی را به‌طور نظام‌مند بررسی کرده است. اویلر همچنین در معادلات دیوفانتی کار کرده است، برای بسیاری از قضیه‌های فرما برهانی آورده است، و یک بررسی نظام‌مند از کسرهای مسلسل ارائه داده است. اویلر در بسیاری از زمینه‌های دیگر نیز سهیم است، از جمله مکانیک، حساب تغییرات،

هیدرودینامیک، معادلات دیفرانسیل، و نظریهٔ توابع ــ و چهار کتاب به چاپ رساند که یک معرفی وحدت‌بخش از حساب دیفرانسیل و انتگرال ارائه می‌دهند.

اویلر در ۱۸ سپتامبر ۱۷۸۳ در سن ۷۶ سالگی درگذشت.

مراجع

David M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

در این کتاب از موضوعاتی بحث می‌شود که در سالهای اخیر بسیار مهم شده‌اند، زیرا مطالب مبتنی بر نظریهٔ اعداد به‌طور وسیعی در رمزنویسی به‌کار می‌روند. یک بحث کامل از اعداد شبه‌اول و اعداد کارمایکل، و قضیه‌های فرما و اویلر نقش مهمی را ایفا می‌کنند. مؤلف مقدار زیادی از توجه خود را به موضوعات محاسبه‌یی معطوف داشته و الگوریتمهای رایانه‌یی مفصل ارائه می‌دهد.

Leonard Eugene Dickson, *History of the Theory of Numbers* (3 volumes), Chelsea, New York, 1952 (originally published in 1919).

مطالب مرتبط با این فصل را می‌توان در مجلد I پیدا کرد. بررسی دیکسن جامع ولی خیلی رمزی و سربسته است و ابداً تحلیلی نیست. شرح خلاصه‌ای بدون توضیح از یک برهان را ارائه می‌دهد یا اصلاً برهانی نمی‌آورد، و بین قضیه‌های مهم و معماها آشکارا تمیز قائل نمی‌شود. اینها کتابهایی شگفت‌انگیز برای تورّق، و در مقدار قابل استفاده اندک هستند.

André Weil, *Number Theory: An approach through history form Hammurapi to Legendre*, Birkhäuser, Boston, 1984.

این کتاب یک بررسی تحلیلی توسط یکی از استادان نظریه نوین اعداد است، که به مهمترین مطالب کارهای فرما، اویلر، لاگرانژ، و لژاندار مربوط می‌شود. هر بخش دانش نسبتاً پیشرفته‌ای از نظریه اعداد را طلب می‌کند، زیرا از دیدگاههای خیلی نوین به تاریخ وارد می‌شود، اما بسیاری از مطالبِ مربوط به فرما و اویلر را در دسترس خواننده قرار می‌دهد.

۴

همنهشتیهای چندجمله‌یی

در این فصل به بررسی همنهشتی چندجمله‌یی $f(x) \equiv 0 \pmod{m}$ می‌پردازیم که $f(x)$ یک چندجمله‌یی با ضرایب صحیح است. تقریباً تمام مطالب این فصل را می‌توان به‌صورتی در نوشته‌های لاگرانژ پیدا کرد، و کار لاگرانژ درست قبل از آنکه گاوس مفهوم همنهشتی را تعریف کند انجام شده بود. گاوس در تحقیقات حسابی خود دو حالت خاص را بررسی کرده است و اولین کسی بوده که مسألهٔ یافتن جوابهای همنهشتیهای چندجمله‌یی با پیمانهٔ غیر اول را مورد توجه قرار داده است. ساده‌ترین حالت، که به تفصیل در فصل ۲ بررسی شد، همنهشتی خطی $ax \equiv b \pmod{m}$ است، که در آن $f(x) = ax - b$ یک چندجمله‌یی از درجهٔ ۱ است. همنهشتیهای چندجمله‌یی درجهٔ دوم، در فصل ۵ به تفصیل خواهند آمد، و بعضی از همنهشتیهای از درجات بالاتر در فصل ۶ بررسی می‌شوند.

قضیه‌هایی برای فصل ۴

در قضیه‌های اصلی این فصل به بررسی تعداد جوابهای همنهشتی چندجمله‌یی کلی $f(x) \equiv ۰ (\mathrm{mod}\, p)$، که در آن p عددی است اول، می‌پردازیم. در بخش بعدی مسألهٔ یافتن یک جواب به پیمانهٔ p^k را از یک جواب به پیمانهٔ p بررسی می‌کنیم.

همنهشتیهای چندجمله‌یی کلی

از این به بعد، چندجمله‌ییهای مورد نظر دارای ضرایب صحیح هستند. موضوع را با یک تعریف شروع می‌کنیم.

(۱.۴) تعریف. یک جواب همنهشتی چندجمله‌یی $f(x) \equiv ۰ (\mathrm{mod}\, m)$ عدد صحیحی مانند c است به‌طوری که $f(c) = ۰ (\mathrm{mod}\, m)$. در این حالت، (به قیاس با ریشهٔ یک معادلهٔ چندجمله‌یی معمولی)، c یک ریشهٔ $f(x)$ به پیمانهٔ m نیز خوانده می‌شود.

توضیح. فرض می‌کنیم $a \equiv b (\mathrm{mod}\, m)$. بنابر (۳.۲)، $f(a) \equiv ۰ (\mathrm{mod}\, m)$ اگر و تنها اگر $f(b) \equiv ۰ (\mathrm{mod}\, m)$، لذا اگر داشته باشیم $a \equiv b (\mathrm{mod}\, m)$، a و b را جوابهای متمایز تلقی نمی‌کنیم.

از آنجا که هر عدد صحیح دقیقاً با یکی از عناصر دستگاه کامل مانده‌های $۰, ۱, \ldots, m-۱$ همنهشت است، لذا هر جواب $f(x) \equiv ۰ (\mathrm{mod}\, m)$ بایستی با یکی از این m عدد همنهشت باشد. به‌ویژه، یک همنهشتی چندجمله‌یی به پیمانهٔ m می‌تواند حداکثر m جواب ناهمنهشت داشته باشد، که می‌توان آنها را با امتحان اعداد $۰, ۱, \ldots, m-۱$ یکی‌یکی به‌دست آورد. (اغلب آسانتر است که اعداد صحیح x را که $-m/۲ < x \leq m/۲$ امتحان کنیم.) اگر m بزرگ باشد هیچ‌یک از دو روش کارساز نیست.

برای یافتن جواب در حالت کلی، فرض می‌کنیم $m = p_۱^{a_۱} p_۲^{a_۲} \cdots p_r^{a_r}$. چون به‌ازای هر i، $p_i^{a_i} | m$، آشکار است که هر ریشهٔ $f(x)$ به پیمانهٔ m یک ریشهٔ $f(x)$ به پیمانهٔ $p_i^{a_i}$ برای $i = ۱, ۲, \ldots, r$ نیز هست. بعکس، فرض می‌کنیم به‌ازای هر i، $f(c_i) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$. چون $p_i^{a_i}$ها دوبه‌دو متباین‌اند، با استفاده از قضیهٔ باقیماندهٔ چینی می‌توانیم عدد c را (که به پیمانهٔ m یکتاست) بیابیم به‌طوری که به‌ازای هر i، $c \equiv c_i (\mathrm{mod}\, p_i^{a_i})$؛ لذا $f(c) \equiv ۰ (\mathrm{mod}\, m)$. بنابراین قضیهٔ زیر را ثابت کرده‌ایم.

(۲.۴) قضیه. فرض می‌کنیم $m = p_۱^{a_۱} p_۲^{a_۲} \cdots p_r^{a_r}$. اگر c یک جواب $f(x) \equiv ۰ (\mathrm{mod}\, m)$

باشد، آنگاه به‌ازای هر $i = ۱, ۲, \ldots, r$ عدد c یک جواب $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ است. بعکس، اگر به‌ازای هر i، c_i جوابی از $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ باشد، آنگاه دقیقاً یک جواب c از $f(x) \equiv ۰ (\mathrm{mod}\, m)$ وجود دارد به‌طوری که به‌ازای هر $i = ۱, ۲, \ldots, r$، $c \equiv c_i (\mathrm{mod}\, p_i^{a_i})$.

از (۲.۴) نتیجه می‌شود که هر مجموعهٔ متمایز از جوابهای همنهشتیهای چندجمله‌یی $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ با یک جواب $f(x) \equiv ۰ (\mathrm{mod}\, m)$ متناظر است. فرض می‌کنیم $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ دارای t_i جواب ناهمنهشت باشد. در این‌صورت، با توجه به نمادگذاری در (۲.۴)، $t_۱$ انتخاب برای $c_۱$، $t_۲$ انتخاب برای $c_۲$، و هکذا وجود دارند. بنابراین، دقیقاً $t_۱ t_۲ \cdots t_r$ ریشه برای $f(x) \equiv ۰ (\mathrm{mod}\, m)$ وجود دارد. آشکار است که اگر حتی یکی از همنهشتیهای $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ جواب نداشته باشد (لذا $t_i = ۰$)، آنگاه $f(x) \equiv ۰ (\mathrm{mod}\, m)$ جواب نخواهد داشت. بنابراین قضیهٔ زیر را داریم:

(۳.۴) قضیه. فرض می‌کنیم $m = p_۱^{a_۱} p_۲^{a_۲} \cdots p_r^{a_r}$. اگر t_i معرف تعداد جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, p_i^{a_i})$ باشد، آنگاه تعداد جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, m)$ دقیقاً برابر با $t_۱ t_۲ \cdots t_r$ است.

با توجه به (۲.۴)، برای یافتن جوابهای یک همنهشتی چندجمله‌یی، کافی است حالتی را در نظر بگیریم که پیمانه به‌صورت p^a است. از آنجا که هر جواب $f(x) \equiv ۰ (\mathrm{mod}\, p^a)$ بایستی جوابی از $f(x) \equiv ۰ (\mathrm{mod}\, p)$ باشد، لذا تمام ریشه‌های $f(x)$ به پیمانهٔ m را می‌توان از میان اعداد صحیح x که $f(x) \equiv ۰ (\mathrm{mod}\, p)$ به‌دست آورد. در قضیهٔ ۱۰.۴ روشی را برای یافتن جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, p^a)$ از جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, p)$ ارائه خواهیم داد.

یادآور می‌شویم که $f(x) = a_n x^n + a_{n-۱} x^{n-۱} + \cdots + a_۱ x + a_۰$ از درجهٔ n خوانده می‌شود هرگاه $a_n \neq ۰$. برای چندجمله‌یی صفر درجه‌یی تعیین نمی‌شود. می‌دانیم که درجهٔ حاصلضرب $f(x)g(x)$ از دو چندجمله‌یی مجموع درجه‌های $f(x)$ و $g(x)$ است. (یک دلیل اینکه برای چندجمله‌یی صفر درجه‌یی تعیین نمی‌شود این است که دیگر این قضیه همواره برقرار نخواهد بود.)

اغلب، در بحث مربوط به همنهشتیهای به پیمانهٔ m، تعریف معمولی درجه قدری تغییر کرده است. چندجمله‌یی $f(x) = a_n x^n + a_{n-۱} x^{n-۱} + \cdots + a_۱ x + a_۰$ را از درجهٔ k به پیمانهٔ m خوانیم اگر k بزرگترین عدد صحیحی باشد که $m \nmid a_k$. اگر تمام ضرایب $f(x)$ بر m بخشپذیر باشند، درجه به پیمانهٔ m تعریف نمی‌شود. اثر این تعریف در آن است که وقتی همنهشتیهای چندجمله‌یی به پیمانهٔ m را بررسی می‌کنیم، می‌توان با ضرایبی که بر m بخشپذیرند به‌عنوان صفر

برخورد کرد. در این کتاب مفهوم درجه به پیمانهٔ m مورد نیاز نیست، و لذا، درجه به معنای درجهٔ معمولی خواهد بود.

در قضیهٔ بعد روند آشنای تقسیم یک چندجمله‌یی بر دیگری بررسی می‌شود. اگر به روش معمول $f(x)$ بر $g(x)$ تقسیم شود، لزومی ندارد که ضرایب خارج‌قسمت و باقیمانده عدد صحیح باشند حتی اگر ضرایب $f(x)$ و $g(x)$ اعداد صحیح باشند، لذا فرض می‌کنیم که ضریب پیشرو در $g(x)$ برابر ۱ باشد. حال فرض می‌کنیم که $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$، که در آن $a_n \neq 0$، و $g(x)$ دارای درجهٔ $m \leq n$ باشد. قرار می‌دهیم $f_1(x) = f(x) - a_n x^{n-m} g(x)$؛ در این‌صورت یا $f_1(x)$ چندجمله‌یی صفر است یا درجه‌یی کمتر از n دارد. اگر برای b و kی مناسب به کم کردن جمله‌های به‌صورت $bx^k g(x)$ ادامه دهیم، سرانجام یا به چندجمله‌یی صفر می‌رسیم یا به یک چندجمله‌یی از درجهٔ کمتر از m می‌رسیم. این روند دقیقاً همانند الگوریتم «تقسیم طولانی» معمولی برای چندجمله‌ییهاست. بنابراین قضیهٔ زیر را داریم:

(۴.۴) قضیهٔ (الگوریتم تقسیم برای چندجمله‌ییها). فرض کنیم $f(x)$ و $g(x)$ چندجمله‌ییهایی با ضرایب صحیح باشند، و فرض می‌کنیم ضریب جملهٔ پیشرو در $g(x)$ برابر ۱ باشد. در این‌صورت چندجمله‌ییهای $q(x)$ و $r(x)$، هر کدام با ضرایب صحیح، وجود دارند به‌طوری که $f(x) = q(x)g(x) + r(x)$، که در آن یا درجهٔ $r(x)$ از درجهٔ $g(x)$ کمتر است یا $r(x)$ چندجمله‌یی صفر است.

از آنجاکه بررسی همنهشتیهای چندجمله‌یی برای یک پیمانهٔ کلی به حالتی که پیمانه عدد اول است تبدیل می‌شود، ابتدا به بررسی ماهیّت جوابهای $f(x) \equiv 0 \pmod p$، که p اول است می‌پردازیم. به‌عنوان نتیجه‌ای از قضیهٔ فرما، می‌توانیم فرض کنیم که درجهٔ $f(x)$ کمتر از p است. زیرا اگر $f(x)$ چندجمله‌یی دلخواهی باشد، بنابر الگوریتم تقسیم داریم $f(x) = q(x)(x^p - x) + r(x)$، که در آن یا درجهٔ $r(x)$ کمتر از p است یا $r(x)$ چندجمله‌یی صفر است. چون به‌ازای هر x داریم $x^p - x \equiv 0 \pmod p$، آشکار است که ریشه‌های $r(x)$ همان ریشه‌های $f(x)$ است.

به روش دیگر، x^n را که در آن n عدد طبیعی است در نظر می‌گیریم، و می‌نویسیم $n - 1 = k(p-1) + r$، که $0 \leq r < p - 1$. اگر $x \not\equiv 0 \pmod p$، آنگاه بنابر قضیهٔ فرما $x^{p-1} \equiv 1 \pmod p$ و لذا $x^{n-1} \equiv (x^{p-1})^k x^r \equiv x^r \pmod p$. بنابراین، اگر $x \not\equiv 0 \pmod p$، آنگاه $x^n \equiv x^{r+1} \pmod p$. آشکار است که $x^n \equiv x^{r+1} \pmod p$ برای $x \equiv 0 \pmod p$ نیز برقرار است. چون $r + 1 \leq p - 1$، می‌توانیم $f(x)$ را با یک چندجمله‌یی $g(x)$ از درجهٔ نابیشتر از $p - 1$ جانشین کنیم به‌طوری که به‌ازای هر x، $f(x) \equiv g(x) \pmod p$.

به‌ویژه، چندجمله‌ییهای $f(x)$ و $g(x)$ دقیقاً ریشه‌های واحدی به پیمانهٔ p دارند. (مسألهٔ ۱۹.۴ را ببینید.)

بنابراین می‌رسیم به اینکه جوابهای $f(x) \equiv 0 \pmod p$ را که در آن درجهٔ $f(x)$ مساوی با $p-1$ یا کمتر از آن است مورد بررسی قرار دهیم. قضیهٔ اصلی، که در ۱۷۶۸ توسط لاگرانژ ثابت شد، بیان می‌دارد که برای یک پیمانهٔ اول یک همنهشتی چندجمله‌یی از درجهٔ n حداکثر n جواب دارد. لم زیر را لازم داریم.

(۵.۴) لم. فرض می‌کنیم p عددی اول باشد، و $f(x)$ یک چندجمله‌یی از درجهٔ n. اگر a یک ریشهٔ $f(x)$ به پیمانهٔ p باشد، آنگاه $f(x) = (x-a)q(x) + c$، به‌طوری که $p|c$ و $q(x)$ یک چندجمله‌یی از درجهٔ $n-1$ و با ضرایب صحیح است.

برهان. بنابر (۴.۴)، یک چندجمله‌یی $q(x)$ و یک عدد ثابت c وجود دارند به‌طوری که $f(x) = q(x)(x-a) + c$. اگر $x = a$ را در این تساوی قرار دهیم، آنگاه $c = f(a)$ و لذا $p|c$. آشکار است که $q(x)$ از درجهٔ $n-1$ است.

توضیح. لازم نیست که فرض کنیم پیمانه اول است؛ دقیقاً همین استدلال برای یک پیمانهٔ دلخواه m نیز کارساز است. می‌توان استدلال مشابهی را به‌کار برد و ثابت کرد اگر $f(x)$ یک چندجمله‌یی با ضرایب حقیقی باشد و $f(a) = 0$، آنگاه $(x-a)|f(x)$.

(۶.۴) قضیهٔ لاگرانژ. فرض کنیم p اول باشد، و فرض می‌کنیم $f(x)$ یک چندجمله‌یی از درجهٔ n باشد که همهٔ ضرایبش بر p بخشپذیر نیستند. در این‌صورت همنهشتی $f(x) \equiv 0 \pmod p$ نمی‌تواند بیش از n جواب ناهمنهشت داشته باشد.

برهان. اثبات به استقرا بر n یعنی روی درجهٔ $f(x)$ است. اگر $f(x)$ دارای درجهٔ 0 باشد، آنگاه $f(x)$ چندجمله‌یی ثابت a_0 است. چون $p \nmid a_0$، همنهشتی $f(x) \equiv 0 \pmod p$ جوابی ندارد.

اکنون فرض می‌کنیم که قضیه برای چندجمله‌ییهای از درجهٔ $n-1$ برقرار باشد، و فرض می‌کنیم $f(x)$ یک چندجمله‌یی از درجهٔ n باشد. یا $f(x) \equiv 0 \pmod p$ جوابی ندارد (که در این حالت قضیه برقرار است) یا حداقل جوابی مانند a دارد؛ لذا $f(a) \equiv 0 \pmod p$. فرض کنیم $q(x)$ مانند لم قبل باشد؛ سپس بررسی اینکه هر ضریب $q(x)$ بر p بخشپذیر نیست آسان است.

اگر b جواب دیگری از $f(x) \equiv 0 \pmod p$ باشد که ناهمنهشت با a به پیمانهٔ p است، آنگاه (۵.۴) ایجاب می‌کند که $0 \equiv f(b) \equiv (b-a)q(b) \pmod p$؛ چون $a \not\equiv b \pmod p$،

داریم $q(b) \equiv ۰ \pmod p$. لذا هر جواب $f(x) \equiv ۰ \pmod p$ که با a متمایز باشد جوابی از $q(x) \equiv ۰ \pmod p$ است، که بنابر فرض استقرا بیش از $n-۱$ جواب ناهمنهشت ندارد. بنابراین $f(x) \equiv ۰ \pmod p$ حداکثر n جواب ناهمنهشت دارد.

توضیحات. ۱. اگر k بزرگترین عدد صحیحی باشد که $p \nmid a_k$، آنگاه بنابر قضیهٔ لاگرانژ $f(x) \equiv ۰ \pmod p$ نمی‌تواند بیش از k جواب ناهمنهشت داشته باشد.

۲. اگر پیمانه عدد اول نباشد، آنگاه ممکن است یک همنهشتی از درجهٔ n بیشتر از n جواب داشته باشد؛ مثلاً، همنهشتی $x^۲ - ۱ \equiv ۰ \pmod ۸$ دارای چهار جواب ۱، ۳، ۵، و ۷ است. دلیل اینکه برهان قضیهٔ لاگرانژ در این مورد به‌کار نمی‌آید این است که اگر $m > ۱$ اول نباشد، آنگاه از $uv \equiv ۰ \pmod m$ نمی‌توان نتیجه گرفت که یا u همنهشت با صفر به پیمانهٔ m است یا v.

۳. برهان قضیهٔ لاگرانژ که در بالا ارائه شد اساساً با برهان معمولی که یک چندجمله‌یی از درجهٔ n با ضرایب حقیقی بیشتر از n ریشهٔ حقیقی ندارد یکی است.

تحت شرایطی، می‌توانیم ثابت کنیم که یک چندجمله‌یی $f(x)$ از درجهٔ n درست n ریشه به پیمانهٔ p دارد. اگر $f(x)$ یک چندجمله‌یی از درجهٔ n باشد که ضریب پیشرو آن یعنی a_n همنهشت با ۰ به پیمانهٔ p نباشد، آنگاه عدد صحیح c وجود دارد به‌طوری که $a_n c \equiv ۱ \pmod p$. فرض می‌کنیم $f_۱(x)$ چندجمله‌یی به‌دست آمده از تعویض ضریب پیشرو $cf(x)$ با ۱ باشد. لذا به‌ازای هر x، $f_۱(x) \equiv cf(x) \pmod p$، و بنابراین $f_۱(x)$ همان ریشه‌های به پیمانهٔ p را دارد که $f(x)$ دارد.

(۷.۴) قضیهٔ (چبیشف، ۱۸۴۹). فرض می‌کنیم p اول باشد، و فرض می‌کنیم چندجمله‌یی $f(x)$ دارای درجهٔ n، با $n \le p$، و ضریب پیشرو ۱ باشد. با استفاده از الگوریتم تقسیم داریم $x^p - x = q(x)f(x) + r(x)$، که در آن $r(x)$ یا چندجمله‌یی صفر است یا درجهٔ $r(x)$ کمتر از n است. در این‌صورت $f(x)$ دقیقاً n ریشهٔ به پیمانهٔ p دارد اگر و تنها اگر هر ضریب $r(x)$ بر p بخشپذیر باشد.

برهان. فرض کنیم هر ضریب $r(x)$ بر p بخشپذیر باشد. در این‌صورت ریشه‌های $q(x)f(x)$ به پیمانهٔ p همان ریشه‌های $x^p - x$ هستند. اما بنابر قضیهٔ فرما، $x^p - x$ دارای p ریشه به پیمانهٔ p است. لذا $q(x)f(x)$ نیز p ریشه دارد، و چون p اول است، هر یک از این p ریشه بایستی یا یک ریشهٔ $q(x)$ یا $f(x)$ (یا هر دو) باشد. اما چون $q(x)$ از درجهٔ $p-n$ و ضریب پیشرو ۱ است، لذا بنابر قضیهٔ لاگرانژ بیشتر از $p-n$ ریشه ندارد. بنابراین $f(x)$ حداقل n ریشه و لذا درست n ریشه دارد.

اکنون فرض می‌کنیم که $f(x) \equiv ۰ \pmod p$ دقیقاً دارای n جواب باشد. بنابر قضیهٔ فرما، به‌ازای هر x داریم $x^p - x \equiv ۰ \pmod p$. لذا هر ریشه $f(x)$ به پیمانهٔ p ریشه‌ای از $r(x)$ به پیمانهٔ p نیز هست، و بنابراین $r(x)$ حداقل n ریشه دارد. یا $r(x)$ چندجمله‌یی صفر است (و چیزی برای اثبات وجود ندارد) یا درجهٔ $r(x)$ کمتر از n است، که در این حالت قضیهٔ لاگرانژ ایجاب می‌کند که هر ضریب $r(x)$ بر p بخشپذیر باشد.

(۸.۴) فرع. اگر p عددی اول و $d|p-۱$، آنگاه همنهشتی چندجمله‌یی $x^d - ۱ \equiv ۰ \pmod p$ درست d جواب ناهمنهشت دارد.

برهان. اگر $p - ۱ = kd$، آنگاه

$$x^p - x = (x^{p-۱} - ۱)x = (x^d - ۱)(x^{d(k-۱)} + x^{d(k-۲)} + \cdots + x^d + ۱)x\,.$$

لذا وقتی $x^p - x$ بر $x^d - ۱$ بخشپذیر باشد باقیمانده ۰ است، و نتیجه از (۷.۴) حاصل می‌شود.

حل همنهشتی $f(x) \equiv ۰ \pmod{p^k}$

اکنون به مسألهٔ تعیین جوابهایی از $f(x) \equiv ۰ \pmod p$ می‌پردازیم که در $f(x) \equiv ۰ \pmod{p^k}$ نیز صدق می‌کنند. همان‌گونه که در خلاصه و مثال (۱۲.۴) بعد از آن شرح داده شده، روند کلی با انتخاب ریشه‌ای به پیمانهٔ p و استفاده از آن برای تولید یک ریشه (یا ریشه‌هایی) به پیمانهٔ $p^۲$ شروع می‌شود. با استفاده از همین تکنیک، ریشه‌های به پیمانه $p^۳$، $p^۴$ و مانند آن را تولید می‌کنیم، تا سرانجام ریشه‌ای (یا ریشه‌هایی) برای پیمانهٔ اصلی p^k به‌دست آوریم.

لم زیر را لازم داریم، در این بخش، $f'(x)$ معرف مشتق چندجمله $f(x)$ است.

(۹.۴) لم. فرض کنیم p عددی اول باشد و k عددی طبیعی. به‌ازای هر انتخاب x و t داریم:

$$f(x + p^k t) \equiv f(x) + f'(x)p^k t \pmod{p^{k+۱}}\,.$$

برهان. اثبات به استقرا بر درجهٔ $f(x)$ است. اگر درجهٔ $f(x)$ صفر باشد نتیجه نمایان است. فرض می‌کنیم که قضیه برای چندجمله‌ییهای از درجهٔ n برقرار باشد، و فرض می‌کنیم $f(x)$ دارای درجهٔ $n+۱$ باشد. در این‌صورت $f(x) = a + xg(x)$، که در آن a عدد ثابتی است و $g(x)$ دارای درجهٔ n است. بنابه فرض استقرا

$$g(x + p^k t) \equiv g(x) + g'(x)p^k t \pmod{p^{k+۱}}$$

لذا

$$f(x+p^k t) = a + (x+p^k t)g(x+p^k t) \equiv a + (x+p^k t)(g(x)+g'(x)p^k t)$$
$$\equiv a + xg(x) + (xg'(x)+g(x)p^k t \pmod{p^{k+1}}.$$

چون $a + xg(x) = f(x)$ و $xg'(x) + g(x) = f'(x)$، برهان کامل می‌شود.

ملاحظه می‌کنید که هر ریشهٔ $f(x)$ به پیمانهٔ p^{k+1} به‌وضوح ریشه‌ای از $f(x)$ به پیمانهٔ p^k است. فرض می‌کنیم ریشه‌های $f(x)$ به پیمانهٔ p^k با r_1، r_2، ...، r_n داده شده باشند، و فرض می‌کنیم S ریشه‌ای به پیمانهٔ p^{k+1} باشد؛ در این‌صورت یک i وجود دارد که $S \equiv r_i \pmod{p^k}$. بنابراین تمام جوابهای $f(x) \equiv 0 \pmod{p^{k+1}}$ از جوابهای $f(x) \equiv 0 \pmod{p^k}$ تولید می‌شوند. اکنون نشان می‌دهیم که چگونه ریشه‌های $f(x)$ به پیمانهٔ p^{k+1} را از ریشه‌های به پیمانهٔ p^k به‌وجود آوریم.

(۱۰.۴) قضیه. فرض می‌کنیم p عددی اول باشد و k عدد طبیعی دلخواه، و فرض می‌کنیم s یک جواب $f(x) \equiv 0 \pmod{p^k}$ باشد.

(الف) اگر $p \nmid f'(s)$، آنگاه دقیقاً یک جواب s_{k+1} از $f(x) \equiv 0 \pmod{p^{k+1}}$ وجود دارد به‌طوری که $s_{k+1} \equiv s \pmod{p^k}$. جواب s_{k+1} با $s_{k+1} = s + p^k t$ ارائه می‌شود، که در آن t جواب یکتای $f'(s)t \equiv -f(s)/p^k \pmod{p}$ است.

(ب) اگر $p | f'(s)$ و $p^{k+1} | f(s)$، آنگاه $f(x) \equiv 0 \pmod{p^{k+1}}$ دارای p جواب همنهشت با s به پیمانهٔ p^k است، که با $s + p^k j$ به‌ازای $j = 0, 1, \ldots, p-1$ ارائه می‌شوند.

(ج) اگر $p | f'(s)$ و $p^{k+1} \nmid f(s)$، آنگاه $f(x) \equiv 0 \pmod{p^{k+1}}$ هیچ جوابی ندارد که با s به پیمانهٔ p^k همنهشت باشد.

برهان. فرض می‌کنیم S یک جواب $f(x) \equiv 0 \pmod{p^{k+1}}$ باشد به‌طوری که $S \equiv s \pmod{p^k}$؛ در این‌صورت عدد صحیحی چون t وجود دارد به‌طوری که $S = s + p^k t$. لذا مسأله به یافتن مقادیری از t برمی‌گردد به‌طوری که $s + p^k t$ یک ریشهٔ $f(x) \equiv 0 \pmod{p^{k+1}}$ باشد، یعنی، اعداد صحیح t که به‌ازای آنها $f(s + p^k t) \equiv 0 \pmod{p^{k+1}}$. لذا با توجه به لم قبل، به tای نیاز داریم به‌طوری که

$$f(s) + f'(s)p^k t \equiv 0 \pmod{p^{k+1}}. \qquad (1)$$

از آنجا که $f(s) \equiv ۰ \pmod{p^k}$، پس $f(s)/p^k$ عددی صحیح است، و لذا می‌توانیم طرفین (۱) را بر p^k تقسیم کنیم و معادله زیر را به‌دست آوریم:

$$f'(s)t \equiv -\frac{f(s)}{p^k} \pmod{p}. \qquad (۲)$$

بنابر (۸.۲)، همنهشتی اخیر جوابی یکتا دارد هرگاه $(f'(s), p) = ۱$ یا، هم‌ارز با آن، اگر $p \nmid f'(s)$. اگر $p|f'(s)$، آنگاه طرف چپ (۲) همنهشت با ۰ به پیمانهٔ p است، و لذا سمت راست (۲) نیز بایستی همنهشت با ۰ باشد. لذا بایستی داشته باشیم $f(s)/p^k \equiv \pmod{p}$، یعنی، $p^{k+۱}|f(s)$، در این حالت هر مقدار t در یک دستگاه کامل مانده‌ها (به پیمانهٔ p) یک جواب خواهد بود (مثلاً $t = ۰, ۱, \ldots, p-۱$)، سرانجام، اگر $p|f'(s)$ ولی $p^{k+۱} \nmid f(s)$، آنگاه سمت راست (۲) به پیمانهٔ p همنهشت با ۰ نخواهد بود، و لذا tای وجود ندارد که همنهشتی را حل کند. این مطلب برهان قضیه را کامل می‌کند.

از آنجا که هر ریشهٔ $f(x)$ به پیمانهٔ p^k ریشه‌ای به پیمانهٔ p است، از اینجا نتیجه می‌شود که اگر $f(x) \equiv ۰ \pmod{p}$ جوابی نداشته باشد، به‌ازای هر $k \geq ۱$ هیچ جوابی برای $f(x) \equiv ۰ \pmod{p^k}$ وجود ندارد.

(۱۱.۴) فرع. فرض می‌کنیم p عددی اول باشد و k عدد طبیعی دلخواه. اگر $s_۱$ یک جواب $f(x) \equiv ۰ \pmod{p}$ باشد و $p \nmid f'(s_۱)$، آنگاه دقیقاً یک جواب s_k از $f(x) \equiv ۰ \pmod{p^k}$ وجود دارد به‌طوری که $s_k \equiv s_۱ \pmod{p}$.

برهان. چون $p \nmid f'(s_۱)$، می‌توانیم با استفاده از (۱۰.۴الف) جواب یکتای $s_۲$ از $f(x) \equiv ۰ \pmod{p^۲}$ را به‌دست آوریم به‌طوری که $s_۲ \equiv s_۱ \pmod{p}$. چون $s_۲ \equiv s_۱ \pmod{p}$ و $f'(s_۱) \not\equiv ۰ \pmod{p}$، از (۳.۲) نتیجه می‌شود که $f'(s_۲) \not\equiv ۰ \pmod{p}$. لذا می‌توانیم (۱۰.۴الف) را برای $s_۲$ به‌کار بریم و ریشهٔ یکتای $s_۳$ از $f(x) \equiv ۰ \pmod{p^۳}$ را به‌دست آوریم به‌طوری که $s_۳ \equiv s_۲ \pmod{p^۲}$. روشن است که از $s_۳ \equiv s_۲ \pmod{p^۲}$ نتیجه می‌شود $s_۳ \equiv s_۲ \pmod{p}$؛ چون $s_۲ \equiv s_۱ \pmod{p}$، داریم $s_۳ \equiv s_۱ \pmod{p}$. لذا اگر به همین ترتیب ادامه دهیم یک ریشهٔ s_k از $f(x) \equiv ۰ \pmod{p^k}$ به‌دست می‌آید به‌طوری که $s_k \equiv s_۱ \pmod{p}$.

خلاصه. روند کلی یافتن تمام جوابهای $f(x) \equiv ۰ \pmod{p^k}$ را می‌توان به‌ترتیب زیر خلاصه نمود:

۱. ابتدا تمام جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, p)$ را به‌دست می‌آوریم.

۲. یکی از جوابها، مثلاً $s_۱$ را انتخاب می‌کنیم، در این‌صورت بنابر (۱۰.۴)، ۰، ۱، یا p جواب از $f(x) \equiv ۰ (\mathrm{mod}\, p^۲)$ همنهشت با $s_۱$ به پیمانهٔ p وجود دارند؛ اگر جوابهایی وجود داشته باشند، آنها از حل همنهشتی خطی $f'(s_۱)t \equiv -f(s_۱)/p (\mathrm{mod}\, p)$ به‌دست می‌آیند. اگر هیچ جوابی وجود نداشته باشد، مجدداً با $s_۱$ دیگری کار را آغاز می‌کنیم.

۳. اگر $f(x) \equiv ۰ (\mathrm{mod}\, p^۲)$ دارای جواب باشد، یکی از آنها، مثلاً $s_۲$، را انتخاب کرده و ریشه‌های متناظر $f(x)$ به پیمانهٔ $p^۳$ را با حل همنهشتی $f(s_۲)t \equiv -f(s_۲)/p^۲ (\mathrm{mod}\, p)$ به‌دست می‌آوریم. این کار را برای تمام ریشه‌های $f(x)$ به پیمانهٔ $p^۲$ انجام می‌دهیم. توجه کنید چون $s_۲ \equiv s_۱ (\mathrm{mod}\, p)$ پس $f'(s_۲) \equiv f'(s_۱) (\mathrm{mod}\, p)$، لذا به محاسبهٔ $f'(s_۲)$ نیاز نداریم.

۴. اگر به همین ترتیب ادامه دهیم، سرانجام تمام جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, p^k)$ را به‌دست می‌آوریم.

توضیح. بجاست که تأکید کنیم اگر در هر مرحلهٔ این روند جوابهای چندگانه به‌دست آوریم (یعنی اگر $p | f'(s)$ و $p^{k+۱} | f(s)$، حالت (ب) از قضیهٔ ۱۰.۴)، آنگاه بایستی روند بالا را برای هر جواب به‌کار بریم.

(۱۲.۴) مثال. ما وارد جزئیات این تکنیک می‌شویم و تمام جوابهای همنهشتی چندجمله‌یی $۱۳x^۷ - ۴۲x + ۶۷۴ \equiv ۰ (\mathrm{mod}\, ۱۳۲۳)$ را به‌دست می‌آوریم.

فرض می‌کنیم $f(x) = ۱۳x^۷ - ۴۲x + ۶۷۴$. چون $۱۳۲۳ = ۳^۳ \times ۷^۲$، ابتدا تمام جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, ۳^۳)$ و $f(x) \equiv ۰ (\mathrm{mod}\, ۷^۲)$ را پیدا می‌کنیم، سپس با استفاده از قضیهٔ باقیماندهٔ چینی تمام جوابهای همنهشتی اصلی را به‌دست می‌آوریم. برای حل $f(x) \equiv ۰ (\mathrm{mod}\, ۳^۳)$، ابتدا $f(x) \equiv ۰ (\mathrm{mod}\, ۳)$ را در نظر می‌گیریم. چون ۰ جواب نیست، پس برای هر $x \not\equiv ۰$ بنابر قضیهٔ فرما داریم $x^۲ \equiv ۱ (\mathrm{mod}\, ۳)$، و لذا $x^۷ \equiv x (\mathrm{mod}\, ۳)$. بنابراین $f(x) \equiv ۰ (\mathrm{mod}\, ۳)$ به $-۲۹x + ۶۷۴ \equiv ۰$ بدل می‌شود، یعنی، $x + ۲ \equiv ۰ (\mathrm{mod}\, ۳)$. تنها جواب این همنهشتی $s_۱ = ۱$ است. (در واقع، در اینجا جواب بدیهی است، ولی این تکنیک برای اعداد اول بزرگتر مفید است.)

ملاحظه می‌کنید که به‌ازای هر جواب x، $f'(x) = ۹۱x^۶ - ۴۲ \equiv x^۶ = (x^۲)^۳ \equiv ۱ (\mathrm{mod}\, ۳)$ و لذا $f'(۱) \not\equiv ۰ (\mathrm{mod}\, ۳)$. بنابراین (۱۱.۴) تضمین می‌کند که $f(x) \equiv ۰ (\mathrm{mod}\, ۹)$ و $f(x) \equiv ۰ (\mathrm{mod}\, ۲۷)$ هر کدام دقیقاً یک جواب دارند، و این جوابها بایستی با ۱ به پیمانهٔ ۳

همنهشت باشند. به دنبال یافتن جواب $f(x) \equiv 0 \pmod 9$ که به‌صورت $s_1 + 3t = 1 + 3t$ است می‌رویم؛ لذا، بنابر (۱۰.۴الف) به tای نیاز داریم که $f'(1)t \equiv -f(1)/3 \pmod 3$، یعنی $t \equiv 1 \pmod 3$، زیرا $f(1) \equiv 6 \pmod 9$. بنابراین $t = 1$ و لذا $s_2 = 1 + 3t = 4$ جواب یکتای $f(x) \equiv 0 \pmod 9$ است.

سپس ریشهٔ یکتای $f(x)$ به پیمانهٔ ۲۷ را به‌دست می‌آوریم، که بایستی به‌صورت $4 + 9t$ باشد زیرا ریشهٔ $f(x)$ به پیمانهٔ ۲۷ ریشهٔ به پیمانهٔ ۹ نیز خواهد بود. بنابر (۱۰.۴الف)، بایستی t در $f'(4)t \equiv -f(4)/9 \pmod 3$ صدق کند. چون به‌ازای هر جواب x داریم $f'(x) \equiv 1 \pmod 3$، لذا $f'(4) \equiv 1 \pmod 3$. برای ساده کردن محاسبهٔ $f(4)/9$ ملاحظه می‌کنیم که $f(x) \equiv 13x^7 + 12x - 1 \pmod{27}$؛ لذا $f(4) \equiv 9 \pmod{27}$. از این‌رو، بنابر (v.۲.۲)، $f(4)/9 \equiv 1 \pmod 3$، و لذا $t \equiv -f(4)/9 \pmod 3$ به $t \equiv -1 \pmod 3$ بدل می‌شود، که دارای جواب یکتای $t = 2$ است. لذا $s_3 = 4 + 9t = 22$ جواب یکتای $f(x) \equiv 0 \pmod{27}$ است.

همین‌طور، قضیهٔ فرما را برای تبدیل $f(x) \equiv 0 \pmod 7$ به $-29x + 674 \equiv 0 \pmod 7$، یعنی، $-x + 2 \equiv 0 \pmod 7$ به‌کار می‌بریم، که دارای جواب یکتای $s_1 = 2$ است. بنابراین به جستجوی ریشهٔ $f(x)$ به پیمانهٔ ۴۹ که به‌صورت $2 + 7t$ است می‌پردازیم، که $f'(2)t \equiv -f(2)/7 \pmod 7$. چون به‌ازای هر x داریم $f'(x) = 91x^6 - 42 \equiv 0 \pmod 7$، $7 | f'(2)$؛ همچنین، $49 | f(2) = 2254$، لذا (۱۰.۴ب) ایجاب می‌کند که هر مقدار $t = 0, 1, \ldots 6$ جوابی از $f(x) \equiv 0 \pmod{49}$ را تولید کند. لذا $f(x) \equiv 0 \pmod{49}$ دارای ۷ ریشهٔ ۲، ۹، ۱۶، ۲۳، ۳۰، ۳۷، و ۴۴ است.

اکنون قضیهٔ باقیماندهٔ چینی را برای حل $x \equiv 22 \pmod{27}$ و $x \equiv a \pmod{49}$، که a یکی از هفت جواب $f(x)$ به پیمانهٔ ۴۹ است، به‌کار می‌بریم. در استفاده از قضیهٔ باقیماندهٔ چینی تنها برای یک بار به محاسبهٔ b_iها نیاز داریم و سپس مقادیر مختلف a را در عبارت x^* قرار می‌دهیم. (برهان (۱۱.۲) را ببینید.) لذا تمام جوابهای $f(x) \equiv 0 \pmod{1323}$ با $x^* \equiv 49 + 540a \pmod{1323}$، یعنی ۱۸۴، ۳۷۳، ۵۶۲، ۷۵۱، ۹۴۰، ۱۱۲۹، و ۱۳۱۸ داده می‌شوند.

همنهشتی $x^2 \equiv a \pmod{p^k}$

بالاخره، نوع خاصی از همنهشتی چندجمله‌یی، یعنی، همنهشتی درجهٔ دوم $x^2 \equiv a \pmod{p^k}$ را که در آن p عدد اولی است بررسی می‌کنیم. این همنهشتیها نقش مهمی در نظریهٔ کلی همنهشتیهای

درجه دوم، که در فصل بعد عرضه خواهند شد، بازی می‌کنند. (همان‌گونه که از نامش پیداست، یک همنهشتی چندجمله‌یی درجهٔ دوم یک همنهشتی است که چندجمله‌یی آن از درجهٔ ۲ است.)

(۱۳.۴) قضیه. فرض می‌کنیم p یک عدد اول فرد باشد و فرض می‌کنیم $k \geq ۱$. اگر $(a,p) = ۱$، آنگاه $x^۲ \equiv a \pmod{p^k}$ یا جواب ندارد یا دقیقاً دو جواب دارد، برحسب آنکه $x^۲ \equiv a \pmod{p}$ حلپذیر باشد یا نباشد.

برهان. اگر $x^۲ \equiv a \pmod{p}$ جوابی نداشته باشد، آنگاه $x^۲ \equiv a \pmod{p^k}$ جوابی ندارد. اکنون فرض کنیم $x^۲ \equiv a \pmod{p}$ جوابی مانند s داشته باشد؛ در این‌صورت $-s$ نیز جواب است. چون s و $-s$ به پیمانهٔ p ناهمنهشت هستند، لذا بنابر (۶.۴)، اینها تنها ریشه‌های $x^۲ - a$ به پیمانهٔ p هستند. آشکار است که s بر p بخشپذیر نیست، زیرا $(a,p) = ۱$. از این‌رو اگر $f(x) = x^۲ - a$، آنگاه $f'(s) = ۲s$ بر p بخشپذیر نیست، و لذا قضیه از (۱۰.۴الف) نتیجه می‌شود. (به‌ویژه، ریشه‌های s و $-s$ به پیمانهٔ p هرکدام دقیقاً یک ریشه به پیمانهٔ p^k برای هر $k \geq ۱$ تولید می‌کنند.)

(۱۴.۴) قضیه. فرض می‌کنیم a عدد صحیحی باشد. در این‌صورت

(الف) $x^۲ \equiv a \pmod{۲}$ همواره حلپذیر است و دقیقاً یک جواب دارد،

(ب) $x^۲ \equiv a \pmod{۴}$ حلپذیر است اگر و تنها اگر $a \equiv ۱ \pmod{۴}$، در این حالت دقیقاً دو جواب وجود دارد،

(ج) $x^۲ \equiv a \pmod{۲^k}$ با $k \geq ۳$، حلپذیر است اگر و تنها اگر $a \equiv ۱ \pmod{۸}$، در این حالت دقیقاً چهار جواب وجود دارد. به‌ویژه، اگر s جوابی باشد، آنگاه تمام جوابها به‌صورت $\pm s$ و $\pm s + ۲^{k-۱}$ هستند.

برهان. قسمتهای (الف) و (ب) واضح هستند. حال فرض کنیم $k \geq ۳$. اگر $۲^{k-۳}$ عدد فرد از ۱ تا $۲^{k-۲}$ را مربع کنیم، هیچ دو مربعی به پیمانهٔ ۲^k همنهشت نیستند. زیرا اگر $a^۲ \equiv b^۲ \pmod{۲^k}$، با $a > b$ و a و b فرد، آنگاه $۲^k | (a-b)(a+b)$. اما دقیقاً یکی از $a-b$ و $a+b$ همنهشت با ۲ به پیمانهٔ ۴ است و لذا فقط یک عامل ۲ دارد. از این‌رو دیگری بایستی بر $۲^{k-۱}$ بخشپذیر باشد، که ممکن نیست، زیرا $a-b$ و $a+b$ هر دو کمتر از $۲^{k-۱}$ هستند.

مربع یک عدد فرد همنهشت با ۱ به پیمانهٔ ۸ است، و دقیقاً $۲^{k-۳}$ عدد طبیعی کمتر از ۲^k وجود دارد که همنهشت با ۱ به پیمانهٔ ۸ هستند. در نتیجه مربع $۲^{k-۳}$ عدد فردِ از ۱ تا $۲^{k-۲}$، به‌ترتیبی، همنهشت به پیمانهٔ ۲^k با اعداد صحیح مثبتی هستند که کمتر از ۲^k و همنهشت با ۱ به

پیمانهٔ ۸ می‌باشند. لذا، اگر $a \equiv ۱ (\mathrm{mod}\, ۸)$، روشن است که همنهشتی $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ جوابی مانند s دارد که $۱ \leq s < ۲^{k-۲}$. آشکار است که اگر a فرد و $a \not\equiv ۱ (\mathrm{mod}\, ۸)$ جوابی وجود ندارد.

اگر s یک جواب $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ باشد، آنگاه مربع $-s$ و $\pm s + ۲^{k-۱}$ به پیمانهٔ ۲^k نشان می‌دهد که اینها نیز جواب هستند؛ با اختیارکمترین مانده‌های مثبت، می‌توانیم فرض کنیم که تمام جوابها مثبت و کمتر از ۲^k هستند. به آسانی می‌توان بررسی کرد که هیچ دو تا از این اعداد همنهشت به پیمانهٔ ۲^k نیستند. لذا اگر $a \equiv ۱ (\mathrm{mod}\, ۸)$، همنهشتی $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ دست‌کم چهار جواب دارد. این به دلیل $۲^{k-۱} = ۴ \times ۲^{k-۳}$ عدد فردی است که کمتر از ۲^k هستند، یعنی، همهٔ آنها. در نتیجه اگر $a \equiv ۱ (\mathrm{mod}\, ۸)$، همنهشتی $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ دقیقاً چهار جواب دارد.

توضیح. قضیه‌های دیگر دربارهٔ همنهشتیهای $x^۲ \equiv a (\mathrm{mod}\, p^k)$ و $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ در مسائل ۳۷.۴ تا ۴۷.۴ داده شده‌اند.

مسأله‌ها و راه‌حلها

۱.۴ همهٔ جوابهای $x^۴ + ۲x + ۳۶ \equiv ۰ (\mathrm{mod}\, ۸۷۵)$ را به‌دست آورید.

حل. فرض می‌کنیم $f(x) = x^۴ + ۲x + ۳۶$. ملاحظه می‌کنید که $۸۷۵ = ۵^۳ \times ۷$؛ لذا ابتدا تمام جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۳)$ و $f(x) \equiv ۰ (\mathrm{mod}\, ۷)$ را به‌دست می‌آوریم، سپس با استفاده از قضیهٔ باقیماندهٔ چینی تمام جوابهای همنهشتی اصلی را پیدا می‌کنیم. به‌سادگی معلوم می‌شود که تنها جوابهای $f(x) \equiv ۰ (\mathrm{mod}\, ۷)$ عبارت‌اند از $x \equiv -۱, ۲ (\mathrm{mod}\, ۷)$؛ همچنین، $f(x) \equiv ۰ (\mathrm{mod}\, ۵)$ دارای جواب یکتای $x \equiv -۱ (\mathrm{mod}\, ۵)$ است.

چون $f'(x) = ۴x^۳ + ۲$ و از این‌رو $f'(-۱) \not\equiv ۰ (\mathrm{mod}\, ۵)$، (۱۱.۴) تضمین می‌کند که $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۳)$ دقیقاً یک جواب دارد (و این جواب لزوماً با -۱ به پیمانهٔ ۵ همنهشت است). فرض کنیم $s_۱ = -۱$؛ سپس به دنبال یافتن جواب $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۲)$ که به‌صورت $-۱ + ۵t$ است می‌رویم؛ لذا، بنابر (۱۰.۴الف)، tای را لازم داریم که $f'(-۱)t \equiv -f(-۱)/۵ (\mathrm{mod}\, ۵)$. چون $f(-۱) = ۳۵$ و $f'(-۱) = -۲$، این همنهشتی به $-۲t \equiv -۷ (\mathrm{mod}\, ۵)$ بدل می‌شود، که دارای جواب یکتای ۱ است. لذا $s_۲ = -۱ + ۵t = ۴$ تنها جواب $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۲)$ است.

اکنون جواب $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۳)$ را که به‌صورت $۲۵t + ۴$ است پیدا می‌کنیم؛ بنابر

(۴.۱۰الف)، t بایستی در $f'(۴)t \equiv -f(۴)/۲۵ (\mathrm{mod}\, ۵)$ صدق کند، چون $f(۴) \equiv ۵۰ (\mathrm{mod}\, ۱۲۵)$ و $f'(۴) \equiv f'(-۱) \equiv -۲ (\mathrm{mod}\, ۵)$، این همنهشتی به $-۲t \equiv -۲ (\mathrm{mod}\, ۵)$ بدل می‌شود، که دارای جواب یکتای $t = ۱$ است. لذا $s_۳ = ۴ + ۲۵t = ۲۹$ تنها جواب $f(x) \equiv ۰ (\mathrm{mod}\, ۵^۳)$ است.

سرانجام، برای حل $x \equiv ۲۹ (\mathrm{mod}\, ۱۲۵)$ و $x \equiv -۱۲ (\mathrm{mod}\, ۷)$، قضیهٔ باقیماندهٔ چینی را به‌کار می‌بریم و جوابهای ۲۷۹ و ۷۷۹ را برای همنهشتی اصلی $f(x) \equiv ۰ (\mathrm{mod}\, ۸۷۵)$ به‌دست می‌آوریم.

۲.۴ تمام جوابهای همنهشتی $x^۶ - ۲x^۵ - ۳۵ \equiv ۰ (\mathrm{mod}\, ۶۱۲۵)$ را به‌دست آورید.

حل. فرض می‌کنیم $f(x) = x^۶ - ۲x^۵ - ۳۵$؛ در این‌صورت $f'(x) = ۶x^۵ - ۱۰x^۴$. چون $۶۱۲۵ = ۵^۳ \times ۷^۲$، بایستی ریشه‌های $f(x)$ به پیمانه‌های ۱۲۵ و ۴۹ را پیدا کنیم. بنابر قضیهٔ فرما، همنهشتی $f(x) \equiv ۰ (\mathrm{mod}\, ۵)$ به $x^۲ - ۲x \equiv ۰ (\mathrm{mod}\, ۵)$ بدل می‌شود که دارای دو جواب ۰ و ۲ است. چون $۵ | f'(۰) = ۰$ و $۲۵ \nmid f(۰) = -۳۵$، لذا ریشهٔ ۰ هیچ ریشه‌ای به پیمانهٔ ۲۵ و از این‌رو هیچ ریشه‌ای به پیمانهٔ ۱۲۵ را تولید نمی‌کند. چون $۵ \nmid f'(۲) = ۳۲$، ریشه‌ای یکتا به پیمانهٔ ۲۵ به‌صورت $۵t + ۲$ وجود دارد که t در $۳۲t \equiv -f(۲)/۵ (\mathrm{mod}\, ۵)$، یعنی در $۲t \equiv ۲ (\mathrm{mod}\, ۵)$ صدق می‌کند. لذا $t = ۱$ و بنابراین $۷ = ۱ \times ۵ + ۲$ ریشه به پیمانهٔ ۲۵ است. حال ریشهٔ به پیمانهٔ ۱۲۵ را که به‌صورت $۲۵t + ۷$ است پیدا می‌کنیم. چون $f(۷) \equiv ۰ (\mathrm{mod}\, ۱۲۵)$، فعلاً ۷ یک ریشه به پیمانهٔ ۱۲۵ است. چون $f'(۲) \not\equiv ۰ (\mathrm{mod}\, ۵)$، $x \equiv ۷ (\mathrm{mod}\, ۱۲۵)$ تنها ریشهٔ به پیمانهٔ ۱۲۵ است. [(۱۱.۴) را ببینید.]

به‌ازای هر x داریم $f(x) \equiv x^۵(x - ۲) (\mathrm{mod}\, ۷)$؛ لذا ریشه‌های $f(x)$ به پیمانه ۷ اعداد ۰ و ۲ هستند. چون $۷ | f'(۰) = ۰$ ولی $۴۹ \nmid f(۰) = -۳۵$، پس ۰ ریشهٔ به پیمانهٔ ۴۹ تولید نمی‌کند. چون $۷ \nmid f'(۲) = ۳۲$، لذا ۲ یک ریشهٔ یکتا به پیمانهٔ ۴۹ تولید می‌کند، که به‌صورت $۷t + ۲$ است و t در $۳۲t \equiv -f(۲)/۷ (\mathrm{mod}\, ۷)$، یعنی در $۴t \equiv ۵ (\mathrm{mod}\, ۷)$ صدق می‌کند. لذا $t = ۳$ و $۷ \times ۳ + ۲ = ۲۳$ تنها ریشهٔ $f(x)$ به پیمانهٔ ۴۹ است.

بالاخره با استفاده از قضیهٔ باقیماندهٔ چینی در مورد دستگاه $x \equiv ۷ (\mathrm{mod}\, ۱۲۵)$ و $x \equiv ۲۳ (\mathrm{mod}\, ۴۹)$، عدد ۳۲۵۷ به‌عنوان تنها جواب $f(x) \equiv ۰ (\mathrm{mod}\, ۶۱۲۵)$ به‌دست می‌آید.

۳.۴ همنهشتی $x^۲ - ۳۱x - ۱۲ \equiv ۰ (\mathrm{mod}\, ۳۶)$ را حل کنید.

حل. فرض می‌کنیم $f(x) = x^۲ - ۳۱x - ۱۲$؛ در این‌صورت $f'(x) = ۲x - ۳۱$.

آشکار است که ۰ و ۳ تنها جوابهای به پیمانهٔ ۴ هستند. همچنین ریشه‌های $f(x)$ به پیمانهٔ ۳ عبارت‌اند از ۰ و ۱. به جستجوی جواب به پیمانهٔ ۹ می‌رویم که به‌صورت $3t + 0 = 3t$ است و $f'(0)t \equiv -f(0)/3 \pmod 3$، یعنی، $2t \equiv 1 \pmod 3$. از آنجا $t = 2$، و لذا ۰ ریشهٔ $2 \times 3 + 0 = 6$ به پیمانهٔ ۹ را تولید می‌کند. به همین قیاس، ریشهٔ ۱ به پیمانهٔ ۳ ریشهٔ $3t + 1$ به پیمانهٔ ۹ را تولید می‌کند، که $f'(1)t \equiv -f(1)/3 \pmod 3$، یعنی $-29t \equiv 14 \pmod 3$. از این‌رو $t = 2$ و لذا تنها ریشهٔ دیگر به پیمانهٔ ۹ عبارت است از $2 \times 3 + 7 = 1$.

اکنون قضیهٔ باقیماندهٔ چینی را برای حل $x \equiv a \pmod 4$ و $x \equiv b \pmod 9$ به‌کار می‌بریم، که a برابر ۰ یا ۳ و b برابر ۶ یا ۷ است. لذا $f(x)$ به پیمانهٔ ۳۶ دارای چهار جواب ۷، ۱۵، ۱۶، و ۲۴ است.

توضیح. در فصل ۵ یک روش خیلی بهتری را برای حل همنهشتیهای درجهٔ دوم، با استفاده از یک تغییر روند آشنای تکمیل مربع بیان خواهیم کرد.

۴.۴ تمام جوابهای $x^7 - 14x - 2 \equiv 0 \pmod{27}$ را به‌دست آورید.

حل. فرض می‌کنیم $f(x) = x^7 - 14x - 2$. ابتدا $f(x) \equiv 0 \pmod 3$ را حل می‌کنیم. از راه تجسس احتیاج داریم تنها اعداد -1، ۰، و ۱ را بیازماییم. معلوم می‌شود که ۱ تنها جواب است. داریم $f'(1) \not\equiv 0 \pmod 3$، زیرا $f'(x) = 7x^6 - 14$. لذا بنابر (۱۱.۴) $f(x) \equiv 0 \pmod 9$ و $f(x) \equiv 0 \pmod{27}$ هر یک دقیقاً یک جواب دارند (و این جوابها همنهشت با ۱ به پیمانهٔ ۳ هستند). حال جواب $f(x) \equiv 0 \pmod 9$ را که به‌صورت $s_1 + 3t = 1 + 3t$ است جستجو می‌کنیم؛ بنابر (۱۰.۴الف)، t در $f'(1)t \equiv -f(1)/3 \pmod 3$ یا در $-7t \equiv 15/3 \pmod 3$ صدق کند. از آنجا $t = 1$ و لذا $s_2 = 1 + 3t = 4$ تنها جواب $f(x) \equiv 0 \pmod 9$ است.

بالاخره جواب یکتای $f(x) \equiv 0 \pmod{27}$ را که به‌صورت $9t + 4$ است به‌دست می‌آوریم (توجه داریم که هر جواب $f(x)$ به پیمانهٔ ۲۷ به پیمانهٔ ۹ نیز هست). بنابر (۱۰.۴الف)، t در $f'(4)t \equiv -f(4)/9 \pmod 3$ صدق می‌کند. از آنجا با توجه به $f(4) \equiv 18 \pmod{27}$ و $f'(4) \equiv f'(1) \equiv 2 \pmod 3$. این همنهشتی به $2t \equiv -2 \pmod 3$ بدل می‌شود که دارای جواب $t = 2$ است. لذا $s_3 = 4 + 9t = 22$ تنها جواب $f(x) \equiv 0 \pmod{27}$ است.

۵.۴ تمام جوابهای $x^7 - 14x - 2 \equiv 0 \pmod{49}$ را به‌دست آورید.

حل. فرض می‌کنیم $f(x) = x^7 - 14x - 2$. با استفاده از قضیهٔ فرما همنهشتی $f(x) \equiv 0 \pmod 7$ به $x - 2 \equiv 0 \pmod 7$ بدل می‌شود، که به‌وضوح دارای جواب $s_1 = 2$

است. حال ریشه‌های $f(x)$ به پیمانهٔ ۴۹ را به‌دست می‌آوریم که به‌صورت $7t+2$ هستند و $f'(2)t \equiv -f(2)/7 \pmod 7$. چون $7 \mid f'(2) = 434$ و $49 \mid f(2) = 98$، (۴۹، (۱۰.۴ب) ایجاب می‌کند که هر مقدار از $t = 0, 1, \ldots, 6$ جوابی از $f(x) \equiv 0 \pmod{49}$ را ارائه دهد. لذا $f(x)$ به پیمانهٔ ۴۹ دارای هفت ریشهٔ ۲، ۹، ۱۶، ۲۳، ۳۰، ۳۷، و ۴۴ است.

۶.۴ گیریم p عددی اول باشد، و فرض می‌کنیم $f(x) \equiv 0 \pmod p$ دارای k جواب a_1، a_2، ...، a_k است. ثابت کنید چندجمله‌یی $q(x)$ از درجهٔ $n-k$ با همان ضریب جملهٔ پیشرو در $f(x)$ وجود دارد به‌طوری که به‌ازای هر x،

$$f(x) \equiv (x-a_1)(x-a_2)\cdots(x-a_k)q(x) \pmod p$$

(راهنمایی: $f(x)$ را بر $(x-a_1)(x-a_2)\cdots(x-a_k)$ تقسیم کنید.)

حل. فرض می‌کنیم $g(x) = (x-a_1)(x-a_2)\cdots(x-a_k)$. دراین‌صورت $g(x)$ از درجهٔ k و دارای ضریب جملهٔ پیشرو ۱ است. بنابر الگوریتم تقسیم داریم $f(x) = q(x)g(x)+r(x)$. آشکار است که $q(x)$ دارای درجهٔ $n-k$ و دارای همان ضریب جملهٔ پیشرو در $f(x)$ است. چون a_1، a_2، ...، a_k ریشه‌های $f(x)$ و $g(x)$ به پیمانهٔ p هستند، لذا ریشه‌های $r(x)$ نیز می‌باشند. اما چون یا $r(x)$ چندجمله‌یی صفر است یا درجه‌ای کمتر از k دارد، از قضیهٔ لاگرانژ نتیجه می‌شود که تمام ضرایب $r(x)$ بر p بخشپذیرند، و لذا به‌ازای هر x $f(x) \equiv q(x)g(x) \pmod p$.

۷.۴ فرض می‌کنیم $f(x)$ و $g(x)$ هم‌درجه و دقیقاً دارای ریشه‌های واحدی به پیمانهٔ p باشند. آیا از اینجا نتیجه می‌شود که به‌ازای هر x، $f(x) \equiv g(x) \pmod p$؟ اگر $f(x)$ و $g(x)$ دارای ضریب جملهٔ پیشرو واحدی باشند چه می‌شود؟

حل. در هر دو مورد جواب منفی است. فرض کنیم $p = 5$، $f(x) = 3(x-1)$ و $g(x) = 4(x-1)$. در این‌صورت f و g هر دو دارای ریشهٔ یکتای ۱ هستند، ولی تنها وقتی، $f(x) \equiv g(x) \pmod 5$ برقرار است که $x \equiv 1 \pmod 5$. می‌توان $f(x)$ و $g(x)$ را نیز طوری تعریف کرد که ضریب جملهٔ پیشرو واحدی داشته باشند. مثلاً، فرض کنیم $p = 5$، $f(x) = x(x^2-2)$، و $g(x) = x(x^2-3)$. چون یک مربع هرگز با ۲ یا ۳ به پیمانهٔ ۵ همنهشت نیست، $f(x)$ و $g(x)$ هرکدام دارای ریشهٔ یکتای ۰ هستند. اما آشکار است که تنها وقتی $f(x) \equiv g(x) \pmod 5$ برقرار است که $x \equiv 0 \pmod 5$.

۸.۴ فرض می‌کنیم $f(x)$ و $g(x)$ هر کدام از درجهٔ n و دارای n ریشهٔ متمایز، و یک ضریب جملهٔ پیشرو باشند. اکنون آیا به‌ازای هر x، $f(x) \equiv g(x) \pmod{p}$ برقرار است؟

حل. بله. چندجمله‌یی $D(x) = f(x) - g(x)$ را در نظر می‌گیریم. کافی است نشان دهیم به‌ازای هر x، $D(x) \equiv ۰ \pmod{p}$. برای این کار نشان می‌دهیم که هر یک از ضرایب $D(x)$ بر p بخشپذیر است.

هر ریشهٔ مشترک $f(x)$ و $g(x)$ به پیمانهٔ p ریشه‌ای از $D(x)$ به پیمانهٔ p است. لذا $D(x)$ دست‌کم n ریشه دارد. اما ضریب x^n در $D(x)$ برابر ۰ است، لذا یا $D(x)$ چندجمله‌یی صفر است یا درجه‌اش کمتر از n است. لذا بنابر قضیهٔ لاگرانژ، هر ضریب $D(x)$ بر p بخشپذیر است، و قضیه حاصل می‌شود.

۹.۴ با استفاده از قضیهٔ فرما ثابت کنید که به‌ازای هر x،

$$x^{p-۱} - ۱ \equiv (x-۱)(x-۲)\cdots(x-(p-۱)) \pmod{p}$$

(راهنمایی: از مسألهٔ ۸.۴ استفاده کنید.)

حل. فرض می‌کنیم $f(x) = x^{p-۱} - ۱$ و $g(x) = (x-۱)(x-۲)\cdots(x-(p-۱))$. بدون آنکه به کلیت استدلال خللی وارد آید، می‌توانیم فرض کنیم که تمام ریشه‌ها در دستگاه کامل مانده‌های $\{۰, ۱, \ldots, p-۱\}$ قرار دارند. در این‌صورت قضیهٔ فرما ایجاب می‌کند که $f(x) \equiv ۰ \pmod{p}$ دقیقاً $p-۱$ جواب داشته باشد، یعنی ۱، ۲، ...، $p-۱$. آشکار است که همنهشتی $g(x) \equiv ۰ \pmod{p}$ دقیقاً همان جوابها را دارد. اما $f(x)$ و $g(x)$ دارای ضریب جملهٔ پیشرو ۱ هستند، لذا بنابر مسأله ۸.۴، به‌ازای هر x، $f(x) \equiv g(x)$. (در واقع می‌توانیم نتیجه بگیریم که ضرایب متناظر $f(x)$ و $g(x)$ به پیمانهٔ p نظیر هم هستند.)

۱۰.۴ با مقایسهٔ جمله‌های ثابت در طرفین همنهشتی مسألهٔ قبل قضیهٔ ویلسن را ثابت کنید.

حل. اگر p اول باشد، از مسألهٔ ۹.۴ نتیجه می‌شود که به‌ازای هر x

$$x^{p-۱} - ۱ \equiv (x-۱)(x-۲)\cdots(x-(p-۱)) \pmod{p}$$

با انتخاب $x = ۰$ داریم $(p-۱)! \equiv (-۱)^{p-۱}(-۱) \equiv -۱$. اگر $p \neq ۲$، آنگاه $(-۱)^{p-۱} = ۱$، و اگر $p = ۲$، آنگاه $(p-۱)! \equiv -۱ \pmod{p}$. لذا نتیجه می‌گیریم $(p-۱)! \equiv -۱ \pmod{p}$ که همان قضیهٔ ویلسن است.

توضیح. به نظر می‌رسد که چبیشف اولین کسی باشد که با استدلال بالا قضیهٔ ویلسن را ثابت کرده است. در برهان اصلی لاگرانژ نیز چندجمله‌ییها به‌کار رفته‌اند، اما به طریق خیلی پیچیده‌تر.

۱۱.۴ به مسألهٔ ۹.۴ برمی‌گردیم، اگر p عدد اول فردی باشد، از مقایسهٔ ضرایب x^{p-2} در دو طرف همنهشتی چه چیزی می‌توان به‌دست آورد؟

حل. ضریب x^{p-2} در $x^{p-1}-1$ برابر 0 است، در حالی‌که ضریب x^{p-2} در $(x-1)(x-2)\cdots(x-(p-1))$ برابر $-S$ است، که $S=1+2+\cdots+(p-1)$. طبق تبصرهٔ انتهای راه‌حل مسألهٔ ۹.۴ ضرایب متناظر به پیمانهٔ p نظیر هم هستند. لذا $S\equiv 0 \pmod p$.

نتیجهٔ مسألهٔ قبل را می‌توان تعمیم داد. فرض می‌کنیم p عدد اول فردی باشد. با محاسبهٔ حاصلضرب $(x-1)(x-2)\cdots(x-(p-1))$، و تعریف a_1، a_2، ...، a_{p-1} با

$$(x-1)(x-2)\cdots(x-(p-1))=x^{p-1}+a_1x^{p-2}+\cdots+a_{p-1}. \qquad (3)$$

داریم

$$a_{p-1}=(-1)^{p-1}(p-1)!=(p-1)! \quad \text{و} \quad a_1=-(1+2+\cdots+(p-1))$$

۱۲.۴ فرض می‌کنیم p عدد اول فردی باشد، و فرض می‌کنیم a_1، a_2، ...، a_{p-1} مانند (۱) (در بالا) تعریف شوند. اگر $1\le k\le p-2$، نشان دهید $a_k\equiv 0 \pmod p$. (مسألهٔ ۱۰.۴ را ببینید.)

حل. ضریب x^k در $x^{p-1}-1$ صفر است، در حالی‌که ضریب x^k در

$$(x-1)(x-2)\cdots(x-(p-1))$$

برابر a_k است. لذا دقیقاً مانند مسألهٔ ۱۰.۴ نتیجه می‌گیریم که $a_k\equiv 0 \pmod p$.

◁ **۱۳.۴** (۱۸۶۲ وُلستینهولم[1]). فرض می‌کنیم p عدد اولی بزرگتر از ۳ باشد. نشان دهید $a_{p-2}\equiv 0 \pmod{p^2}$، که a_{p-2} همان است که در فرمول (۱) در بالا تعریف شد. (راهنمایی: در فرمول قرار دهید $x=p$ و مسألهٔ ۱۲.۴ را به‌کار برید.)

حل. با قرار دادن p به‌جای x در (۱) داریم

$$(p-1)!=p^{p-1}+a_1p^{p-2}+\cdots+a_{p-2}p+a_{p-1}.$$

1. Wolstenholme

توجه داریم که $a_{p-1} = (p-1)!$. با حذف و تعدیل معادلهٔ

$$-a_{p-2} = p^{p-2} + a_1 p^{p-3} + \cdots + a_{p-3} p$$

را به‌دست می‌آوریم. چون $p \geq 5$، از مسألهٔ ۱۲.۴ نتیجه می‌شود که $p | a_{p-2}$. لذا هر جملهٔ سمت راست معادله بر p^2 بخشپذیر است، و در نتیجه $a_{p-2} \equiv 0 \pmod{p^2}$.

توضیح. اگر p عدد اول فردی باشد، مجموع $1 + 1/2 + \cdots + 1/(p-1)$ را در نظر می‌گیریم. اگر $(p-1)!$ مخرج مشترک این مجموع باشد، صورت آن دقیقاً $-a_{p-2}$ است.

۱۴.۴ تعداد جوابهای $x^3 + x^2 + 2 \equiv 0 \pmod{3^7 \times 7^3}$ را پیدا کنید.

حل. آشکار است که همنهشتی هیچ جواب به پیمانه ۳ و در نتیجه به پیمانهٔ 3^7 ندارد. لذا بنابر (۳.۴)، همنهشتی اصلی جوابی ندارد.

۱۵.۴ تعداد جوابهای $x^2 - 3 \equiv 0 \pmod{11^4 \times 23^3}$ را به‌دست آورید.

حل. جوابهای همنهشتی به پیمانهٔ ۱۱ عبارت‌اند از ۵ و -5. چون نه $f'(5)$ بر ۱۱ بخشپذیر است و نه $f'(-5)$، لذا (۱۱.۴) تضمین می‌کند که ۵ و -5 هرکدام یک جواب یکتا به پیمانهٔ 11^4 تولید می‌کنند. با استدلالی مشابه، دو جواب ۷ و -7 به پیمانهٔ ۲۳ وجود دارند، و ۲۳ نه $f'(7)$ را می‌شمارد و نه $f'(-7)$ را. لذا دو جواب به پیمانهٔ 23^3 وجود دارد. لذا بنابر (۳.۴) نتیجه می‌شود که همنهشتی اصلی $2 \times 2 = 4$ جواب دارد.

۱۶.۴ تعداد جوابهای $x^3 - 2x^2 - 4x - 17 \equiv 0 \pmod{25}$ را به‌دست آورید.

حل. دو جواب ۲ و۳ به پیمانهٔ ۵ وجود دارند. چون $f'(x) = 3x^2 - 4x - 4$ داریم $f'(2) = 0$ و $f(2) = -25$، لذا (۱۰.۴ب) ایجاب می‌کند که ۲، تعداد ۵ جواب به پیمانهٔ ۲۵ تولید کند، با استدلالی مشابه، $5 \nmid f'(3)$، و لذا بنابر (۱۰.۴الف) ریشهٔ ۳ یک جواب یکتا به پیمانهٔ ۲۵ تولید می‌کند. بنابراین همنهشتی اصلی دقیقاً شش جواب به پیمانهٔ ۲۵ دارد.

۱۷.۴ فرض می‌کنیم p اول باشد. فرض می‌کنیم $f(x)$ دارای r ریشهٔ x_1، x_2، ...، x_r به پیمانهٔ p باشد و به‌ازای هر i، $p \nmid f'(x_i)$. ثابت کنید که به‌ازای هر عدد طبیعی k، $f(x)$ دقیقاً r ریشه به پیمانهٔ p^k دارد.

حل. از (۱۱.۴) نتیجه می‌شود که $f(x) \equiv ۰ (\mathrm{mod}\, p^k)$ به‌ازای هر i دقیقاً یک جواب دارد که با x_i به پیمانهٔ p همنهشت است. لذا $f(x) \equiv ۰ (\mathrm{mod}\, p^k)$ دقیقاً r جواب دارد.

۱۸.۴ تعداد جوابهای $x^۳ - ۱۸x^۲ + ۷۲ \equiv ۰ (\mathrm{mod}\, ۱۱۲۵)$ را پیدا کنید.

حل. فرض می‌کنیم $f(x) = x^۳ - ۱۸x^۲ + ۷۲$، داریم $۱۱۲۵ = ۹ \times ۱۲۵$. به آسانی معلوم می‌شود که ۰ تنها ریشهٔ $f(x)$ به پیمانهٔ ۳ است. چون $۳ \nmid f'(۰)$ و $۹ \mid f(۰)$، (۱۰.۴ب) ایجاب می‌کند که $f(x)$ سه ریشه به پیمانهٔ ۹ داشته باشد. به همین ترتیب، $f(x)$ دارای یک ریشهٔ یکتای ۱ به پیمانهٔ ۵ است. چون $۵ \nmid f'(۱)$، از (۱۱.۴) نتیجه می‌شود که به‌ازای هر $k \geq ۱$، $f(x)$ یک ریشهٔ یکتا به پیمانهٔ ۵^k دارد. لذا بنابر (۳.۴)، $f(x)$ دقیقاً ۳ ریشه به پیمانهٔ ۱۱۲۵ دارد. (همین استدلال نشان می‌دهد که دقیقاً سه ریشه به پیمانهٔ $۵^k \times ۹$ به‌ازای هر $k \geq ۱$، وجود دارد.)

۱۹.۴ به‌ازای هر چندجمله‌یی $f(x)$ و پیمانه p، یک چندجمله‌یی $g(x)$ از درجهٔ کمتر از p پیدا کنید به‌طوری که به‌ازای هر x، $f(x) \equiv g(x) (\mathrm{mod}\, p)$:

(الف) $p = ۷$ و $f(x) = x^{۱۶} + ۵x^۴ - ۳x^۲ + ۱$؛

(ب) $p = ۱۱$ و $f(x) = x^{۴۰} + x^{۳۹} + \cdots + x + ۱$.

حل. (الف) بنابر قضیهٔ فرما، به‌ازای هر x داریم $x^۷ \equiv x (\mathrm{mod}\, ۷)$ و لذا به‌ازای هر x، $x^{۱۶} = (x^۷)^۲ x^۲ \equiv x^۴ (\mathrm{mod}\, ۷)$. بنابراین $g(x) = ۶x^۴ - ۳x^۲ + ۱$.

(ب) مجدداً، بنابر قضیهٔ فرما به‌ازای هر x داریم

$$x^{۱۱} \equiv x (\mathrm{mod}\, ۱۱), x^{۱۲} \equiv x^۲ (\mathrm{mod}\, ۱۱), \ldots, x^{۲۰} \equiv x^{۱۰} (\mathrm{mod}\, ۱۱)$$

این الگو را چهار بار تکرار می‌کنیم، و لذا به‌ازای هر x داریم

$$f(x) \equiv ۴(x^{۱۰} + x^۹ + \cdots + x) + ۱ (\mathrm{mod}\, ۱۱).$$

۲۰.۴ تعداد جوابهای $x^{۳۶۱} - ۱ \equiv ۰ (\mathrm{mod}\, ۳^j \times ۵^k)$ را که در آن j و k اعداد طبیعی هستند پیدا کنید.

حل. روشن است که ۱ تنها ریشه به پیمانهٔ ۳ است، زیرا $(-۱)^{۳۶۱} \equiv -۱ (\mathrm{mod}\, ۳)$. چون $۳ \nmid f'(۱) = ۳۶۱$، (۱۱.۴) ایجاب می‌کند که به‌ازای هر $j \geq ۱$ دقیقاً یک ریشه به پیمانهٔ ۳^j وجود داشته باشد. به همین ترتیب، چون ۰ یک ریشه به پیمانهٔ ۵ نیست، پس قضیهٔ فرما ایجاب

می‌کند که به‌ازای هر ریشهٔ s به پیمانه ۵، $s^4 \equiv 1 \pmod 5$. از آنجا $s^{360} \equiv 1 \pmod 5$، و لذا همنهشتی اصلی به $x - 1 \equiv 0 \pmod 5$ بدل می‌شود. بنابراین ۱ تنها ریشه به پیمانهٔ ۵ است. چون $f'(1) \not\equiv 0 \pmod 5$، لذا از (۱۱.۴) نتیجه می‌شود که $x^{361} - 1 \equiv 0 \pmod{5^k}$ تنها یک جواب دارد. اکنون با استفاده از (۳.۴) نتیجه می‌شود که به‌ازای هر انتخاب در k همنهشتی اصلی دقیقاً یک جواب دارد.

۲۱.۴ اگر عدد فرد m دقیقاً r عامل اول متمایز داشته باشد، نشان دهید که همنهشتی $x^2 \equiv 1 \pmod m$ دقیقاً 2^r جواب دارد.

حل. اگر $m = 1$، آنگاه $r = 0$ و تعداد جوابها ۱ است، یعنی 2^0. اکنون فرض می‌کنیم $m = \prod p_i^{a_i}$. در این‌صورت به‌ازای هر i، همنهشتی $x^2 \equiv 1 \pmod{p_i^{a_i}}$ دقیقاً دو جواب دارد. (آشکارا یک جواب دارد؛ لذا بنابر (۱۳.۴) دارای دو جواب ± 1 است.) برای یافتن جواب همنهشتی اصلی از طریق قضیهٔ باقیماندهٔ چینی، به‌ازای هر i دو انتخاب داریم، و لذا 2^r جواب وجود دارد.

۲۲.۴ (الف) با استفاده از مسألهٔ قبل کوچکترین عدد فرد m را بیابید به‌طوری که همنهشتی $x^2 \equiv 1 \pmod m$ دارای ۱۶ جواب باشد. (ب) کوچکترین عدد زوج m که دارای این ویژگی باشد چقدر است؟

حل. (الف) بنابر مسألهٔ قبل m دارای چهار عامل اول متمایز است. لذا کوچکترین عدد فرد m عبارت است از $3 \times 5 \times 7 \times 11 = 1155$.

(ب) فرض کنیم $m = 2^k n$ که n فرد است. همنهشتی $x^2 \equiv 1 \pmod{2^k}$ دارای یک جواب است اگر $k = 1$، دو جواب است اگر $k = 2$، و چهار جواب هرگاه $k \geq 3$ (۱۴.۴ را ببینید). به آسانی دیده می‌شود که کوچکترین انتخاب برای m عدد $8 \times 3 \times 5 = 120$ است.

۲۳.۴ تعداد جوابهای $10x^4 + 4x + 1 \equiv 0 \pmod{27}$ را بیابید.

حل. چون بنابر قضیهٔ فرما $x^4 \equiv x^2 \pmod 3$، لذا هر جواب همنهشتی اصلی در $x^2 + x + 1 \equiv 0 \pmod 3$ صدق می‌کند، که ۱ تنها جواب آن است. توجه می‌کنیم که $f'(x) = 40x^3 + 4$. چون $f'(1) \equiv 2 \pmod 3$، از (۱۱.۴) نتیجه می‌شود که ۱ جواب یکتایی به پیمانهٔ ۲۷ تولید می‌کند. بنابراین همنهشتی اصلی دقیقاً یک جواب دارد.

۲۴.۴ تعداد جوابهای $7x^2 - 17x - 2 \equiv 0 \pmod{128}$ را به‌دست آورید.

حل. ۰ و ۱ ریشه‌های به پیمانهٔ ۲ هستند. چون نه $f'(0)$ بر ۲ بخشپذیر است و نه $f'(1)$، لذا (۱۱.۴) ایجاب می‌کند که همنهشتی اصلی دقیقاً دو جواب به پیمانهٔ ۱۲۸ داشته باشد.

۲۵.۴ تعداد جوابهای $7x^5 - 3x^3 + 2x - 5 \equiv 0 \pmod{49 \times 25 \times 27}$ را پیدا کنید.

حل. بنابر قضیهٔ فرما داریم $x^3 \equiv x \pmod 3$. لذا همنهشتی به $x - 3x + 2x - 5 \equiv 0$ بدل می‌شود که به‌وضوح ممکن نیست. لذا همنهشتی اصلی جواب ندارد.

۲۶.۴ تعداد جوابهای $3x^3 + x + 1 \equiv 0 \pmod{125}$ را به‌دست آورید.

حل. $f(x) \equiv 0 \pmod 5$ دارای جوابهای ۱ و ۳ است. $5 \nmid f'(3)$، لذا بنابر (۱۱.۴)، $f(x) \equiv 0 \pmod{125}$ تنها یک جواب دارد. $5 \mid f'(1)$ ولی $25 \nmid f(1)$، لذا بنابر (۱۰.۴ج) $f(x) \equiv 0 \pmod{125}$ جواب ندارد. در نتیجه همنهشتی اصلی تنها یک جواب دارد.

۲۷.۴ تعداد جواب همنهشتیهای زیر را بیابید: (الف) $x^2 \equiv 49 \pmod{53^3 \times 61^4}$؛ (ب) $x^2 \equiv 851 \pmod{(5)^2(7)^3(11)^4}$، و (ج) $x^2 \equiv -1 \pmod{5^3 \times 7^2}$.

حل. (الف) به آسانی ثابت می‌شود که ۷ و ۷− جوابهای به پیمانه‌های ۵۳ و ۶۱ هستند. لذا بنابر (۱۱.۴) برای هرکدام از پیمانه‌های $(53)^3$ و $(61)^4$ دو جواب وجود دارد. اکنون (۳.۴) نشان می‌دهد که همنهشتی اصلی $2 \times 2 \times 2 = 8$ جواب دارد.

(ب) ابتدا ملاحظه می‌کنیم که $x^2 \equiv 851 \equiv 1 \pmod 5$، $x^2 \equiv 851 \equiv 4 \pmod 7$، و $x^2 \equiv 851 \equiv 4 \pmod{11}$. چون هر طرف راست یک مربع است، از (۱۱.۴) و (۳.۴) نتیجه می‌شود که همنهشتی اصلی $2 \times 2 \times 2 = 8$ جواب دارد.

(ج) هر جواب x از همنهشتی باید در $x^2 \equiv -1 \pmod 7$ صدق کند. به آسانی ثابت می‌شود که این همنهشتی جواب ندارد. لذا همنهشتی اصلی جواب ندارد.

۲۸.۴ فرض کنیم p عدد اولی باشد که نه a را می‌شمارد و نه n را. ثابت کنید که به‌ازای هر عدد طبیعی k، همنهشتی $x^n \equiv a \pmod{p^k}$ جواب دارد اگر و تنها اگر $x^n \equiv a \pmod p$ جواب داشته باشد.

حل. آشکار است که اگر $x^n \equiv a \pmod{p^k}$ جواب داشته باشد، آنگاه $x^n \equiv a \pmod p$ نیز جواب دارد. بعکس، فرض کنیم $x^n \equiv a \pmod p$ جوابی مانند s داشته باشد. چون $(a, p) = 1$ پس $(s, p) = 1$. اگر فرض کنیم $f(x) = x^n - a$، آنگاه $f'(x) = nx^{n-1}$. چون p نه n را

می‌شمارد و نه s را، پس $p \nmid f'(s)$. لذا بنابر (۱۱.۴)، s جوابی از $x^n \equiv a \pmod{p^k}$ را تولید می‌کند، و درنتیجه همنهشتی دارای یک جواب است. (درواقع، دو همنهشتی یک تعداد جواب دارند.)

۲۹.۴ نشان دهید که به‌ازای هر عدد اول p، چندجمله‌یی $f(x)$ از درجهٔ p با ضریب پیشرو ۱ وجود دارد به‌طوری که $f(x) \equiv ۰ \pmod{p}$ جواب ندارد.

حل. فرض می‌کنیم $f(x) = x^p - x + ۱$. بنابر قضیهٔ فرما، به‌ازای هر x داریم $x^p - x \equiv ۰ \pmod{p}$، و لذا به‌ازای هر x، $f(x) \equiv ۱ \pmod{p}$.

۳۰.۴ فرض می‌کنیم k عددی طبیعی باشد. ثابت کنید $x^۲ + x + a \equiv ۰ \pmod{۲^k}$ جوابی ندارد اگر a فرد، و دو جواب دارد هرگاه a زوج باشد.

حل. اگر a فرد باشد، آشکار است که همنهشتی به پیمانهٔ ۲ جواب ندارد زیرا ۰ و ۱ در آن صدق نمی‌کنند، لذا به‌ازای هر عدد طبیعی k، همنهشتی اصلی نیز جواب ندارد. اگر a زوج باشد، ۰ و ۱ جوابهای همنهشتی به پیمانهٔ ۲ هستند. اگر فرض کنیم $f(x) = x^۲ + x - a$، آنگاه $f'(x) = ۲x + ۱$، $f'(۰) \nmid ۲$ و $f'(۱) \nmid ۲$، لذا بنابر (۱۱.۴) به‌ازای هر k هرکدام از ۰ و ۱ جوابی یکتا برای همنهشتی اصلی تولید می‌کنند.

۳۱.۴ آیا یک عدد پنج رقمی x وجود دارد به‌طوری که پنج رقم آخر $x^۲$ همان ارقام متناظر در x باشند؟

حل. چنین xی باید در $x^۲ \equiv x \pmod{۱۰^۵}$ یا در هم‌ارز آن $x(x-۱) \equiv ۰ \pmod{۱۰^۵}$ صدق کند. چون x و $x-۱$ همواره نسبت به هم اولند و $۱۰^۵ = ۲^۵ \times ۵^۵$، لذا x در دستگاههای زیر صدق می‌کند

$$\begin{cases} x \equiv ۰ \pmod{۳۲} \\ x \equiv ۱ \pmod{۳۱۲۵} \end{cases} \quad \text{و} \quad \begin{cases} x \equiv ۱ \pmod{۳۲} \\ x \equiv ۰ \pmod{۳۱۲۵} \end{cases}$$

(جوابهای نمایان $x = ۰$ یا $x = ۱$ را در نظر نگرفتیم.) از حل دستگاههای بالا توسط باقیماندهٔ چینی دو جواب ۹۳۷۶ و ۹۰۶۲۵ به‌دست می‌آید که دومی در شرایط مسأله صدق می‌کند.

۳۲.۴ اگر $f(x) = x^{۹۹} + x^{۹۸} + \cdots + x + ۱$، آنگاه $f(x) \equiv ۰ \pmod{۱۰۱}$ چند جواب دارد؟

حل. بنابر فرمول معمولی تصاعد هندسی، یا از ضرب مستقیم داریم $(x-1)f(x) = x^{۱۰۰} - ۱$ چون ۱۰۱ اول است، بنابر قضیهٔ فرما $x^{۱۰۰} - ۱ \equiv ۰ \pmod{۱۰۱}$ دارای ۱۰۰ جواب است، یعنی ۱، ۲، ۳، ...، ۱۰۰. اگر $x \not\equiv ۱ \pmod{۱۰۱}$ و $x^{۱۰۰} - ۱ \equiv ۰ \pmod{۱۰۱}$، آنگاه $f(x) \equiv ۰ \pmod{۱۰۱}$. لذا $f(x) \equiv ۰ \pmod{۱۰۱}$ دستکم ۹۹ جواب دارد. اما $f(x)$ از درجهٔ ۹۹ است، لذا همنهشتی دقیقاً ۹۹ جواب دارد.

برهان دیگر. داریم $x(x-۱)f(x) = x^{۱۰۱} - x$. چون $f(x)$ از درجهٔ ۹۹ است، از (۷.۴) نتیجه می‌شود که $f(x) \equiv ۰ \pmod{۱۰۱}$ دقیقاً ۹۹ جواب دارد.

۳۳.۴ فرض می‌کنیم p عدد اول فرد باشد و $(a,p) = ۱$. ثابت کنید که به‌ازای هر عدد طبیعی k، $x^۲ \equiv a \pmod{p^k}$ دارای جواب است اگر و تنها اگر $x^۲ \equiv a \pmod{p^{k+۱}}$ جواب داشته باشد.

حل. فرض می‌کنیم $f(x) = x^۲ - a$. آشکار است که هر ریشهٔ $f(x)$ به پیمانهٔ $p^{k+۱}$ ریشه‌ای به پیمانهٔ p^k نیز هست. بعکس، فرض می‌کنیم s ریشه‌ای به پیمانهٔ p^k باشد؛ چون $(a,p) = ۱$، $p \nmid s$. لذا $p \nmid f'(s) = ۲s$، و از آنجا بنابر (۱۰.۴الف)، $f(x)$ ریشه‌ای به پیمانهٔ $p^{k+۱}$ دارد.

۳۴.۴ فرض می‌کنیم p عدد اول فرد باشد و $(a,p) = ۱$. اگر $k \geq ۱$ وجود داشته باشد به‌طوری که $x^۲ \equiv a \pmod{p^k}$ حلپذیر باشد، مستقیماً (بدون استفاده از (۱۰.۴)) ثابت کنید که $x^۲ \equiv a \pmod{p^{k+۱}}$ حلپذیر است و دقیقاً دو جواب دارد. (راهنمایی: اگر s جوابی به پیمانهٔ p^k باشد، جواب به پیمانهٔ $p^{k+۱}$ را که به‌صورت $s + tp^k$ است پیدا کنید.)

حل. فرض می‌کنیم $s^۲ \equiv a \pmod{p^k}$؛ در این‌صورت یک عدد صحیح m وجود دارد که $s^۲ = a + mp^k$. به دنبال جوابهای $x^۲ \equiv a \pmod{p^{k+۱}}$ می‌گردیم که به‌صورت $s+tp^k$ هستند. لذا می‌خواهیم که $(s+tp^k)^۲ \equiv a \pmod{p^{k+۱}}$، یعنی $s^۲ + ۲stp^k \equiv ۰ \pmod{p^{k+۱}}$. با قرار دادن $s^۲ = a + mp^k$، داریم $mp^k + ۲stp^k \equiv ۰ \pmod{p^{k+۱}}$، یعنی $۲st \equiv -m \pmod{p}$. بنابر (۸.۲)، این همنهشتی جوابی یکتا دارد. در نتیجه هر جواب به پیمانهٔ p^k جواب یکتایی به پیمانهٔ $p^{k+۱}$ تولید می‌کند.

سرانجام نشان می‌دهیم که $x^۲ \equiv a \pmod{p^{k+۱}}$ دقیقاً دو جواب دارد. اگر u جوابی باشد، آشکار است که $-u$ نیز یک جواب است. ملاحظه می‌کنیم که چون $(a,p) = ۱$، پس $(u,p) = ۱$. اگر v هر جوابی از همنهشتی باشد، آنگاه $v^۲ \equiv u^۲ \equiv a \pmod{p^{k+۱}}$، و لذا $p^{k+۱} | (v-u)(v+u)$. اما p نمی‌تواند $v-u$ و $v+u$ هر دو را بشمارد، زیرا در غیر این‌صورت

$p|u$، که با $(u,p)=1$ تناقض دارد. لذا p^{k+1} دقیقاً یکی از مقادیر $v-u$ و $v+u$ را می‌شمارد، و لذا $v=u(\bmod p^{k+1})$ یا $v\equiv -u(\bmod p^{k+1})$.

۳۵.۴ فرض می‌کنیم p عدد اول فرد باشد و $k\geq 1$. ثابت کنید $x^2\equiv 0(\bmod p^k)$ دقیقاً p^m جواب دارد، که در آن $m=k/2$ اگر k زوج باشد و $m=(k-1)/2$ اگر k فرد باشد.

حل. فرض می‌کنیم s یک جواب باشد و می‌نویسیم $s=p^n t$، که $(t,p)=1$. می‌توانیم فرض کنیم که $0\leq s<p^k$؛ لذا $n\leq k-1$. چون $p^k|s^2$، داریم $2n\geq k$. لذا تمام جوابها بین 0 و p^k به‌صورت $p^r t$ هستند، که در آن $r=k/2$ اگر k زوج باشد، و $r=(k+1)/2$ اگر k فرد باشد، و $t=0,1,2,\ldots,p^{k-r}-1$. بنابراین، p^{k-r} جواب وجود دارد، و چون در هر دو حالت $k-r=m$، قضیه حاصل می‌شود.

◁ **۳۶.۴** فرض می‌کنیم m عددی طبیعی، $f(x)$ یک چندجمله‌یی با ضرایب صحیح، و a ریشه‌ای از $f(x)$ به پیمانهٔ m باشد. با استفاده از الگوریتم تقسیم $f(x)$ را به‌صورت $q(x)(x-a)^2+r(x)$ بنویسید، که در آن $r(x)$ چندجمله‌یی صفر یا یک چندجمله‌ایی از درجهٔ کمتر از ۱ یا مساوی با ۱ است. ثابت کنید $f'(a)\equiv 0(\bmod m)$ اگر و تنها اگر هر ضریب $r(x)$ بر m بخشپذیر باشد.

حل. داریم $f'(x)=2(x-a)q(x)+q'(x)(x-a)^2+r'(x)$. اگر هرضریب $r(x)$ بر m بخشپذیر باشد، آنگاه به‌ازای هر x، $r'(x)\equiv 0(\bmod m)$. از آنجا $f'(a)\equiv 0(\bmod m)$.

بعکس، فرض می‌کنیم $f'(a)\equiv 0(\bmod m)$. اگر $r(x)$ را بر $x-a$ تقسیم کنیم داریم $r(x)=b(x-a)+c$ که b و c اعداد ثابت هستند. چون $f(a)\equiv 0(\bmod m)$ پس روشن است که $r(a)\equiv 0(\bmod m)$، و لذا $c\equiv 0(\bmod m)$. از $f'(a)\equiv 0(\bmod m)$ نیز نتیجه می‌شود $r'(a)\equiv 0(\bmod m)$، و لذا $b\equiv 0(\bmod m)$. بنابراین هر ضریب $r(x)$ بر m بخشپذیر است.

توضیح. در جبر معمولی چندجمله‌یها، عدد حقیقی a یک ریشهٔ چندگانهٔ $f(x)$ خوانده می‌شود هرگاه $(x-a)^2|f(x)$، و به آسانی نشان داده می‌شود که این شرط برقرار است اگر و تنها اگر $f'(a)=0$. این مسأله نشان می‌دهد که نتیجهٔ مشابه برای همنهشتیها نیز برقرار است.

همنهشتی $x^2\equiv a(\bmod 2^k)$

۳۷.۴ ثابت کنید که $x^2\equiv 0(\bmod 2^k)$ دقیقاً 2^m جواب دارد، که در آن $m=k/2$ اگر k زوج باشد و $m=(k-1)/2$ اگر k فرد باشد. جوابها به‌ترتیب عبارت‌اند از $2^m t$ و 2^{m+1}، که $0\leq t\leq 2^m-1$.

حل. فرض می‌کنیم s یک جواب $x^۲ \equiv ۰ \pmod{۲^k}$ باشد، به‌طوری که $۰ \le s < ۲^k$. اگر $k = ۲m$، آنگاه $۲^{۲m} | s^۲$، یعنی $s = ۲^m t$، که $۰ \le t \le ۲^m - ۱$. بنابراین، چون هر چنین sی یک جواب است، دقیقاً ۲^m جواب وجود دارد. حال فرض می‌کنیم $k = ۲m + ۱$ یعنی، $m = (k-۱)/۲$. چون بزرگترین توانی از ۲ که یک مربع را بشمارد زوج است، داریم $۲^{۲m+۲} | s^۲$، و لذا $۲^{m+۱} | s$. بنابراین $s = ۲^{m+۱} t$، که $۰ \le t \le ۲^m - ۱$. چون هر چنین sی یک جواب است، دقیقاً ۲^m جواب وجود دارد.

۳۸.۴ فرض می‌کنیم a زوج و $a \not\equiv ۰ \pmod{۲^k}$، و فرض می‌کنیم ۲^b بزرگترین توانی از ۲ باشد که a را می‌شمارد. اگر b فرد باشد، ثابت کنید همنهشتی $x^۲ \equiv a \pmod{۲^k}$ به‌ازای هر مقدار k حلپذیر نیست.

حل. ملاحظه می‌کنیم که $b \le k - ۱$. اگر یک عدد صحیح s وجود داشته باشد به‌طوری که $a - s^۲ | ۲^k$، آنگاه $۲^b | s^۲$ و لذا $۲^{b+۱} | s^۲$. اما b فرد است و لذا $۲^{b+۱} | a$. بنابراین $۲^{b+۱} | a$ که با تعریف b تناقض دارد.

◁ **۳۹.۴** فرض می‌کنیم $a \not\equiv ۰ \pmod{۲^k}$، و فرض می‌کنیم $a = ۲^b c$ که c فرد است. اگر b زوج باشد، مثلاً $b = ۲t$، احکام زیر را ثابت کنید:

(الف) اگر $b \le k-۳$، آنگاه $x^۲ \equiv a \pmod{۲^k}$ حلپذیر است اگر و تنها اگر $c \equiv ۱ \pmod{۸}$، در این حالت دقیقاً $۲^{t+۲}$ جواب وجود دارد که به‌صورت $۲^t s + ۲^{k-t} j$ هستند که در آن $j = ۰, ۱, \ldots, ۲^t - ۱$ و s روی چهار جواب $y^۲ \equiv c \pmod{۲^{k-b}}$ تغییر می‌کند.

(ب) اگر $b = k-۲$، آنگاه $x^۲ \equiv a \pmod{۲^k}$ حلپذیر است اگر و تنها اگر $c \equiv ۱ \pmod{۴}$، در این حالت دقیقاً $۲^{t+۱}$ جواب وجود دارد که به‌صورت $\pm ۲^t + ۲^{t+۲} j$ هستند به‌طوری که $j = ۰, ۱, \ldots, ۲^t - ۱$.

(ج) اگر $b = k - ۱$ آنگاه برای هر عدد فرد c معادلهٔ $x^۲ \equiv a \pmod{۲^k}$ دقیقاً ۲^t جواب دارد که به‌صورت $j ۲^{t+۱} + ۱$ هستند به‌طوری که $j = ۰, ۱, \ldots, ۲^t - ۱$.

حل. اگر $b = ۰$، این همان قضیهٔ (۱۴.۴) است. فرض کنیم s یک جواب $x^۲ \equiv a \pmod{۲^k}$ باشد؛ می‌توانیم فرض کنیم که $۰ < s < ۲^k - ۱$. چون $a - s^۲ | ۲^k$ و $۲^b | a$، در نتیجه $۲^b | s^۲$ و لذا $۲^t | s$. از تقسیم طرفین $s^۲ \equiv a \pmod{۲^k}$ بر ۲^b همنهشتی هم‌ارز $(s/۲^t)^۲ \equiv c \pmod{۲^{k-b}}$ را به‌دست می‌آوریم.

(الف) چون c فرد است، (۱۴.۴) ایجاب می‌کند که به‌ازای $k - b \ge ۳$، این همنهشتی

حلپذیر است اگر و تنها اگر $c \equiv ۱ \pmod ۸$، در این حالت دقیقاً چهار جواب مثلاً $s_۱$، $s_۲$، $s_۳$، $s_۴$ وجود دارد. لذا $s/۲^t = s_i + ۲^{k-t}j$ و از آنجا $s = s^t s_i + ۲^{k-t}j$، که در آن $j = ۰, ۱, ۲, \ldots, ۲^t - ۱$. بنابراین همنهشتی اصلی $۴ \times ۲^t = ۲^{t+۲}$ جواب ناهمنهشت دارد.

(ب) اگر $b = k - ۲$، همنهشتی هم‌ارز $(s/۲^t)^۲ \equiv c \pmod ۴$ را به‌دست می‌آوریم؛ لذا جوابهایی وجود دارند اگر و تنها اگر $c \equiv ۱ \pmod ۴$. در این حالت، داریم $s/۲^t = \pm ۱ + ۴j$ و لذا $s = \pm ۲^t + ۲^{t+۲}j$، که $j = ۰, ۱, \ldots, ۲^t - ۱$. بنابراین $۲ \times ۲^t = ۲^{t+۱}$ جواب وجود دارد.

(ج) سرانجام، اگر $b = k - ۱$، چون c فرد است داریم $(s/۲^t)^۲ \equiv c \equiv ۱ \pmod ۲$. از این‌رو $s/۲^t = ۱ + ۲j$ و لذا $s = ۲^t + ۲^{t+۱}j$، که $j = ۰, ۱, \ldots, ۲^t - ۱$. بنابراین، در این حالت دقیقاً ۲^t جواب وجود دارد.

۴۰.۴ با استفاده از مسألهٔ ۳۷.۴ تعداد جوابهای همنهشتیهای زیر را پیدا کنید.
(الف) $x^۲ \equiv ۰ \pmod{۵۱۲}$؛ (ب) $x^۲ \equiv ۰ \pmod{۱۰۲۴}$؛ (ج) $x^۲ \equiv ۰ \pmod{۲^{۱۵}}$.

حل. (الف) چون $۲^۸ = ۵۱۲$، $۱۶ = ۲^۴$ وجود دارد. (ب) چون $۲^{۱۰} = ۱۰۲۴$، $۳۲ = ۲^۵$ وجود دارد. (ج) چون $۷ = ۲/(۱ - ۱۵)$، $۱۲۸ = ۲^۷$ جواب وجود دارد.

۴۱.۴ جوابهای همنهشتیهای زیر را به‌دست آورید. (الف) $x^۲ \equiv ۱۷ \pmod{۵۱۲}$؛ (ب) $x^۲ \equiv ۷ \pmod{۳۲}$؛ (ج) $x^۲ = -۱ \pmod{۱۲۸}$؛ (د) $x^۲ \equiv ۹ \pmod{۲۵۶}$.

حل. بنابر (۱۴.۴ج)، هر همنهشتی دارای ۰ یا ۴ جواب است.

(الف) اگر به‌جای ۱۷ بنویسیم $۵۲۹ = ۲۳^۲ = ۵۱۲ + ۱۷$ روشن است که دارای جوابهایی هستیم و دقیقاً چهار جواب داریم؛ یعنی ± ۲۳، و $۲۳ \pm ۲^۸ +$، یا ۲۳، ۱۰۵، ۱۵۱، و ۲۳۳.

(ب) اگر $s^۲ \equiv ۷ \pmod{۳۲}$ آنگاه $s^۲ \equiv ۷ \equiv ۳ \pmod ۴$، که جوابی ندارد. پس همنهشتی اصلی جوابی ندارد.

(ج) چون $-۱ \not\equiv ۱ \pmod ۸$ پس این همنهشتی نیز جواب ندارد.

(د) چون $۹ \equiv ۱ \pmod ۸$، پس معادله دقیقاً ۴ جواب دارد. جوابها عبارت‌اند از ± ۳، ۳ ± ۲^۷ یا ۳، ۱۲۵، ۱۳۱، و ۲۵۳.

۴۲.۴ با استفاده از مسأله‌های ۳۸.۴ و ۳۹.۴ تعداد جوابهای (الف) $x^۲ \equiv ۲ \pmod{۱۲۸}$؛ (ب) $x^۲ \equiv ۴۸ \pmod{۲۵۶}$؛ و (ج) $x^۲ \equiv ۱۶۴ \pmod{۵۱۲}$ پیدا کنید.

حل. (الف) با نمادگذاری مسألهٔ ۳۸.۴، b فرد است و لذا جوابی وجود ندارد.

(ب) می‌نویسیم $۳ \times ۲^۴ \equiv ۴۸$. لذا با نمادگذاری مسألهٔ ۳۹.۴ داریم $b = ۴$ پس یا ۰ یا ۴ جواب وجود دارد. با تقسیم طرفین بر ۱۶ یک همنهشتی به‌صورت $y^۲ \equiv ۳ \pmod{۱۶}$ به‌دست می‌آوریم که جواب ندارد، زیرا $y^۲ \equiv ۳ \pmod{۴}$ جوابی ندارد. لذا $x^۲ \equiv ۴۸ \pmod{۲۵۶}$ جوابی ندارد.

(ج) می‌نویسیم $۴۱ \times ۲^۲ = ۱۶۴$؛ با نمادگذاری مسألهٔ ۳۹.۴ داریم $b = ۲$، $t = ۱$، $c = ۱$، و $k = ۹$. لذا $۲^۳ = ۸$ جواب وجود دارد.

۴۳.۴ تمام جوابهای (الف) $x^۲ \equiv ۰ \pmod{۶۴}$؛ (ب) $x^۲ \equiv ۰ \pmod{۱۲۸}$ را به‌دست آورید. (راهنمایی: به مسألهٔ ۳۷.۴ مراجعه کنید.)

حل. (الف) چون $۲^۶ = ۶۴$ و b زوج است، $۲^۳ = ۸$ جواب وجود دارد، که تماماً مضارب ۸ هستند، یعنی، ۰، ۸، ۱۶، ۲۴، ۳۲، ۴۰، ۴۸، و ۵۶.

(ب) داریم $۲^۷ = ۱۲۸$، لذا (با نمادگذاری مسألهٔ ۳۷.۴) $m = ۳$ و بنابراین $۲^۳ = ۸$ جواب وجود دارد. چون $۲/(k+۱) = ۴$)، تمام جوابها به‌صورت مضارب $۲^۴ = ۱۶$ ارائه می‌شوند، یعنی ۰، ۱۶، ۳۲، ۴۸، ۶۴، ۸۰، ۹۶، و ۱۱۲.

۴۴.۴ تمام جوابهای معادلات زیر را به‌دست آورید. (الف) $x^۲ \equiv ۲۵ \pmod{۲۵۶}$؛ (ب) $x^۲ \equiv ۲۱ \pmod{۳۲}$؛ و (ج) $x^۲ \equiv ۴۱ \pmod{۱۲۸}$.

حل. از (۱۴.۴) استفاده می‌کنیم. (الف) روشن است که ۵ یک جواب است، لذا تمام جوابها عبارت‌اند از $۵\pm$، و $۱۲۸ + ۵\pm$، یا ۵، ۱۲۳، ۱۳۳، و ۲۵۱.

(ب) همنهشتی مفروض ایجاب می‌کند که $x^۲ \equiv ۲۱ \equiv ۵ \pmod{۸}$ و این جواب ندارد زیرا مربع هر عدد فرد همنهشت با ۱ به پیمانهٔ ۸ است. لذا همنهشتی اصلی جواب ندارد.

(ج) با قرار دادن $۱۳^۲ = ۱۲۸ + ۴۱$ به جای ۴۱ معلوم می‌شود که ۱۳ یک جواب است. بنابراین (۱۴.۴ج) ایجاب می‌کند که جوابها $۱۳\pm$، و $۶۴ + ۱۳\pm$ یا ۱۳، ۵۱، ۷۷، و ۱۱۵ هستند.

۴۵.۴ با استفاده از مسأله‌های ۳۸.۴ و ۳۹.۴ جوابهای همنهشتیهای زیر را پیدا کنید: (الف) $x^۲ \equiv ۲۴ \pmod{۵۱۲}$؛ (ب) $x^۲ \equiv ۱۴۴ \pmod{۲۵۶}$.

حل. (الف) می‌نویسیم $۳ \times ۲^۳ = ۲۴$. چون توان ۳ فرد است، مسألهٔ ۳۸.۴ ایجاب می‌کند که جوابی وجود نداشته باشد. به روش دیگر، اگر $x^۲ \equiv ۲۴ \pmod{۵۱۲}$، آنگاه x زوج است،

مثلاً $x = ۲y$، لذا $y^۲ \equiv ۶ (\mathrm{mod}\ ۱۲۸)$، که ممکن نیست، زیرا این همنهشتی ایجاب می‌کند که $y^۲ \equiv ۲ (\mathrm{mod}\ ۴)$.

(ب) می‌نویسیم $۹ \times ۲^۴ = ۱۴۴$؛ برحسب نمادگذاری مسألهٔ ۳۹.۴ داریم $b = ۴$، $t = ۲$، $c = ۹$، و $k = ۸$. لذا همنهشتی $۲^{۲+۲} = ۱۶$ جواب دارد. با تقسیم طرفین به $۲^۴$، همنهشتی هم‌ارز $(x/۴)^۲ \equiv ۹ (\mathrm{mod}\ ۱۶)$ را به‌دست می‌آوریم، که دارای جوابهای ± ۳ و ± ۵ است. از حل مسألهٔ ۳۹.۴ نتیجه می‌شود که تمام جوابهای همنهشتی اصلی با $۶۴j + ۳ \times ۴ \pm$ و $۶۴j + ۵ \times ۴ \pm$ ارائه می‌شوند که در آن $j = ۰, ۱, ۲, ۳$. لذا ۱۶ جواب عبارت‌اند از (امتحان کنید!) ± ۱۲، ± ۲۰، ± ۴۴، ± ۵۲، ± ۷۶، ± ۸۴، ± ۱۰۸، و ± ۱۱.

بدون توسل به مسألهٔ ۳۹.۴ نیز می‌توانیم جوابها را به‌دست آوریم. اگر $s^۲ \equiv ۱۴۴ (\mathrm{mod}\ ۲۵۶)$، آنگاه $(s/۴)^۲ \equiv ۹ (\mathrm{mod}\ ۱۶)$ و لذا $s/۴ \equiv \pm ۳, \pm ۵ (\mathrm{mod}\ ۱۶)$. بنابراین $s \equiv \pm ۱۲, \pm ۲۰ (\mathrm{mod}\ ۶۴)$، و لذا تمام جوابهای $x^۲ \equiv ۱۴۴ (\mathrm{mod}\ ۲۵۶)$ عبارت‌اند از α، $\alpha + ۶۴$، $\alpha + ۱۲۸$، و $\alpha + ۱۹۲$، که $\alpha = \pm ۱۲, \pm ۲۰$.

۴۶.۴ فرض می‌کنیم s یک جواب همنهشتی $x^۲ \equiv a (\mathrm{mod}\ ۲^k)$ است، که در آن a فرد است و $k \geq ۳$. نشان دهید که دقیقاً یکی از s و $s + ۲^{k-۱}$ جوابی از $x^۲ \equiv a (\mathrm{mod}\ ۲^{k+۱})$ است. (راهنمایی: $(s + ۲^{k-۱})^۲ - s^۲$ را ملاحظه کنید.)

حل. داریم $(s + ۲^{k-۱})^۲ - s^۲ = s ۲^k + ۲^{۲k-۲}$. چون s فرد است داریم $s ۲^k \equiv ۲^k (\mathrm{mod}\ ۲^{k+۱})$. همچنین، چون $k \geq ۳$ داریم $۲k - ۲ \geq k + ۱$؛ لذا

$$(s + ۲^{k-۱})^۲ - s^۲ \equiv ۲^k (\mathrm{mod}\ ۲^{k+۱})$$

قرار می‌دهیم $s^۲ = a + t ۲^k$. اگر t زوج باشد، آنگاه $s^۲ \equiv a (\mathrm{mod}\ ۲^{k+۱})$، و

$$(s + ۲^{k-۱})^۲ \equiv a + ۲^k (\mathrm{mod}\ s^{k+۱})$$

لذا s یک جواب $x^۲ \equiv a (\mathrm{mod}\ ۲^{k+۱})$ است و $s + ۲^{k-۱}$ جواب نیست. اگر t فرد باشد، $s + ۲^{k-۱}$ جواب است و s جواب نیست.

توضیح. برهان قضیهٔ (۱۴.۴) نشان می‌دهد که جواب وجود دارد ولی یک الگوریتم عملی محاسباتی برای یافتن جواب وقتی که پیمانه بزرگ است ارائه نمی‌دهد. به شباهت روندی که در برهان (۱۰.۴) آمده توجه شود.

۴۷.۴ به آسانی دیده می‌شود که ۲۳ یک جواب $x^۲ \equiv ۱۷ (\mathrm{mod}\, ۵۱۲)$ است، یک جواب $x^۲ \equiv ۱۷ (\mathrm{mod}\, ۲۰۴۸)$ را به‌دست آورید. (راهنمایی: مسألهٔ قبل را ببینید.)

حل. در مسألهٔ قبل نشان داده شد که اگر $k \geq ۳$ و s جوابی از $x^۲ \equiv a (\mathrm{mod}\, ۲^k)$ باشد، آنگاه یکی از s یا $s + ۲^{k-۱}$ جوابی از $x^۲ \equiv a (\mathrm{mod}\, ۲^{k+۱})$ است. در اینجا $a = ۱۷$، $k = ۹$ و $s = ۲۳$. بنابراین یکی از دو عدد ۲۳ یا $۲۵۶ + ۲۳$ جوابی است از $x^۲ \equiv ۱۷ (\mathrm{mod}\, ۱۰۲۴)$. به آسانی دیده می‌شود که ۲۳ جواب نیست؛ لذا ۲۷۹ جواب است. حال فرض کنیم $a = ۱۷$، $s = ۲۷۹$، و $k = ۱۰$. در این‌صورت یکی از دو عدد ۲۷۹ یا $۵۱۲ + ۲۷۹$ جوابی از $x^۲ \equiv ۱۷ (\mathrm{mod}\, ۲۰۴۸)$ است. محاسبه نشان می‌دهد که ۲۷۹ جواب است. (یک محاسبهٔ مشابه نشان می‌دهد که ۲۷۹ جواب همنهشتی با پیمانه ۴۰۹۶ نیز هست. اگر پیمانه ۸۱۹۲ باشد، آنگاه $۲۰۴۸ + ۲۷۹$ جواب است.)

تمرینهایی برای فصل ۴

۱. برای هر یک از چندجمله‌ییها و پیمانه‌های p در زیر، یک چندجمله‌یی $g(x)$ از درجهٔ کمتر از p پیدا کنید به‌طوری که به‌ازای هر x، $f(x) \equiv g(x) (\mathrm{mod}\, p)$:

(الف) $p = ۱۳$ و $f(x) = ۲x^{۲۹} - x^{۱۷} + ۳x^{۱۳} - ۴$؛

(ب) $p = ۵$ و $f(x) = x^{۱۶} + x^{۱۵} + \cdots + x + ۱$.

۲. تعداد جوابهای $۶x^۳ + ۱۳x^۲ + x - ۲ \equiv ۰ (\mathrm{mod}\, ۲۵)$ را به‌دست آورید.

۳. تعداد جوابهای $۶۴x^۳ + ۲۶x^۲ + ۱۰۸ \equiv ۰ (\mathrm{mod}\, ۱۱۲۵)$ را پیدا کنید.

۴. همنهشتی $۴x^۴ + ۷x + ۱۱ \equiv ۰ (\mathrm{mod}\, ۲۷)$ چند جواب دارد؟

۵. تعداد جوابهای $۱۰x^۵ - ۹x^۳ + ۱۱x + ۱ \equiv ۰ (\mathrm{mod}\, ۳^۳ \times ۵^۲ \times ۱۱^۴)$ را تعیین کنید.

۶. تعداد جوابهای $x^۲ - ۳۹x - ۴۶ \equiv ۰ (\mathrm{mod}\, ۱۲۸)$ را به‌دست آورید.

۷. تمام جوابهای $۷x^۲ - x + ۲۴ \equiv ۰ (\mathrm{mod}\, ۳۶)$ را به‌دست آورید.

۸. جوابهای $۱۴x^۳ + ۱۱x - ۱۳ \equiv ۰ (\mathrm{mod}\, ۲۷)$ را پیدا کنید.

۹. همنهشتی $۱۰x^۷ - ۲۱x - ۱۳ \equiv ۰ (\mathrm{mod}\, ۱۳۲۳)$ را حل کنید.

۱۰. جوابهای $x^۴ + ۱۷۷x - ۱۳۹ \equiv ۰ (\mathrm{mod}\, ۸۷۵)$ را پیدا کنید.

۱۱. $۷x^۷ + ۱۰x + ۱۳ \equiv ۰ (\mathrm{mod}\, ۲۷)$ را حل کنید.

۱۲. تعداد جوابهای $x^{۷۱} - ۱ \equiv ۰ (\mathrm{mod}\, ۷^j \times ۱۱^k)$ را که در آن j و k اعداد طبیعی هستند پیدا کنید.

۱۳. همنهشتی $x^۲ \equiv ۴ (\mathrm{mod}\, ۴۷۲۵)$ چند جواب دارد؟

۱۴. تعداد جوابهای $۴x^۳ + ۴۳x - ۸۲ \equiv ۰ (\mathrm{mod}\, ۱۲۵)$ را پیدا کنید.

۱۵. تعداد جوابهای همنهشتیهای زیر را به‌دست آورید.
(الف) $x^۲ \equiv ۲۵ (\mathrm{mod}\ ۳۷^۲ \times ۵۹^۳)$؛
(ب) $x^۲ \equiv ۷۶۴ (\mathrm{mod}\ ۵^۳ \times ۱۱^۲ \times ۱۳^۵)$؛
(ج) $x^۲ \equiv ۳ (\mathrm{mod}\ ۴۲۷)$.

۱۶. همنهشتی $x^{۳۵} + x^{۳۴} + \cdots + x + ۱ \equiv ۰ (\mathrm{mod}\ ۳۷)$ چند جواب دارد؟

۱۷. تعداد جوابهای (الف) $x^۲ \equiv ۰ (\mathrm{mod}\ ۷^۳)$؛ (ب) $x^۲ \equiv ۰ (\mathrm{mod}\ ۷^۶)$ را پیدا کنید.

۱۸. تعداد جوابهای (الف) $x^۲ \equiv ۱۱ (\mathrm{mod}\ ۳۲)$؛ (ب) $x^۲ \equiv ۳۳ (\mathrm{mod}\ ۲۵۶)$؛ (ج) $x^۲ \equiv ۲۵ (\mathrm{mod}\ ۵۱۲)$ را پیدا کنید.

۱۹. از (۱۴.۴ج) برای یافتن تمام جوابهای (الف) $x^۲ \equiv ۴۹ (\mathrm{mod}\ ۱۲۸)$؛ (ب) $x^۲ \equiv ۱۳۹ (\mathrm{mod}\ ۲۵۶)$؛ (ج) $x^۲ \equiv ۱۱۳ (\mathrm{mod}\ ۵۱۲)$ استفاده کنید.

۲۰. با استفاده از مسألهٔ ۳۵.۴، جوابهای (الف) $x^۲ \equiv ۰ (\mathrm{mod}\ ۳^۴)$؛ (ب) $x^۲ \equiv ۰ (\mathrm{mod}\ ۳^۵)$ را بیابید.

۲۱. از مسألهٔ ۳۷.۴ برای یافتن جوابهای (الف) $x^۲ \equiv ۰ (\mathrm{mod}\ ۶۴)$؛ (ب) $x^۲ \equiv ۰ (\mathrm{mod}\ ۱۲۸)$ استفاده کنید.

۲۲. مسأله‌های ۳۸.۴ و ۳۹.۴ را برای محاسبهٔ جوابهای همنهشتیهای زیر به‌کار برید:
(الف) $x^۲ \equiv ۲۲۴ (\mathrm{mod}\ ۵۱۲)$؛ (ب) $x^۲ \equiv ۶۴ (\mathrm{mod}\ ۱۲۸)$؛ (ج) $x^۲ \equiv ۶۴ (\mathrm{mod}\ ۲۵۶)$؛ (د) $x^۲ \equiv ۲۷۲ (\mathrm{mod}\ ۱۰۲۴)$.

۲۳. فرض می‌کنیم $x^۲ \equiv a (\mathrm{mod}\ p^k)$ حلپذیر است. آیا $x^۲ \equiv a (\mathrm{mod}\ p^{k+۱})$ حلپذیر است؟

۲۴. تمام جوابهای $۷x^۴ - ۵x + ۱ \equiv ۰ (\mathrm{mod}\ ۲۷)$ را پیدا کنید.

۲۵. همنهشتی $۶x^۴ - ۲۳x^۳ + ۱۳x - ۱۶ \equiv ۰ (\mathrm{mod}\ ۳۵)$ را حل کنید.

۲۶. جوابهای $۳x^۷ + ۷x - ۶ \equiv ۰ (\mathrm{mod}\ ۴۹)$ را به‌دست آورید.

۲۷. جوابهای $۶۴x^۴ - ۵۱x^۳ - ۳x - ۱۳ \equiv ۰ (\mathrm{mod}\ ۲۲۵)$ را پیدا کنید.

۲۸. همنهشتی $x^۷ - ۱۴x - ۲ \equiv ۰ (\mathrm{mod}\ ۱۳۲۳)$ را حل کنید.

۲۹. فرض می‌کنیم p عدد اولی فرد باشد، a عدد صحیح، و k عددی طبیعی. جوابهای $x^{p^k} \equiv a (\mathrm{mod}\ p)$ را تعیین کنید.

ملاحظاتی برای فصل ۴

۱. معمول است که قضیهٔ تیلر یا قضیهٔ دوجمله‌یی را برای اثبات لم (۹.۴) و لذا قضیهٔ (۱۰.۴) به‌کار می‌برند. در مورد یک چندجمله‌یی $f(x)$ از درجهٔ n، قضیهٔ تیلر به‌صورت زیر بدل می‌شود

$$f(x+y)=f(x)+y^{۲}f'(x)+y^{۳}f''(x)/۲!+\cdots+y^{n}f^{(n)}(x)/n!$$

که در آن f'، f''، ...، $f^{(n)}$ به‌ترتیب مشتقات متوالی f را نشان می‌دهند. ما یک روشِ قدری متفاوت انتخاب کرده‌ایم تا استقرا روانتر به پیش برود.

۲. مفهوم معمولی همنهشتی به پیمانهٔ m را می‌توان از اعداد صحیح برای چندجمله‌ییها گسترش داد. فرض می‌کنیم $f(x)$ و $g(x)$ چندجمله‌ییهایی با ضرایب صحیح باشند، و m عدد صحیح مثبتی باشد. چندجمله‌یی $f(x)$ را با $g(x)$ همنهشت به پیمانهٔ m گوییم اگر تمام ضرایب تفاضل $f(x)-g(x)$ بر m بخشپذیر باشند. اگر $f(x)$ با $g(x)$ همنهشت به پیمانهٔ m باشد، طبق معمول می‌نویسیم $f(x)\equiv g(x)(\bmod m)$. در این نمادگذاری یک احتمال خطر وجود دارد، زیرا ما نماد $f(x)\equiv ۰(\bmod m)$ را در ارتباط با همنهشتی چندجمله‌یی که بایستی برحسب x حل شود، به‌کار برده‌ایم. اگر به ۰ به‌عنوان چندجمله‌یی صفر نگاه کنیم، آنگاه می‌توان چنین تلقی کرد که $f(x)\equiv ۰(\bmod m)$ نیز می‌گوید که چندجمله‌ییهای $f(x)$ و ۰ همنهشت به پیمانهٔ m هستند، یعنی، تمام ضرایب $f(x)$ بر m بخشپذیرند. اینها دو مفهوم هستند کاملاً متفاوت و استفاده از یک نماد برای هر دو اصلاً خطرناک است. ولی، عملاً ابهام به‌ندرت بروز می‌کند.

اگر $f(a)\equiv g(a)(\bmod m)$، به‌ازای هر عدد صحیح a، $f(a)\equiv g(a)(\bmod m)$. نکتهٔ مهم این است که بدانیم عکس این مطلب برقرار نیست. یعنی اگر به‌ازای هر a، $f(a)\equiv g(a)(\bmod m)$، لزوماً نتیجه نمی‌شود که $f(x)\equiv g(x)(\bmod m)$. مثلاً، فرض می‌کنیم p یک عدد اول باشد و $f(x)=x^{p}$، $g(x)=x$. در این‌صورت $f(x)\not\equiv g(x)(\bmod p)$، زیرا تمام ضرایب چندجمله‌یی $x^{p}-x$ بر p بخشپذیر نیستند. ولی بنابر قضیهٔ فرما، به‌ازای هر عدد صحیح a، $f(a)\equiv g(a)(\bmod p)$. بنابراین، چندجمله‌ییهای اساساً به ظاهر متفاوت، نظیر x^{p} و x، می‌توانند، به پیمانهٔ p، توابع واحدی را نشان دهند. وقتی مثلاً روی اعداد حقیقی محاسبه می‌کنیم، این اتفاق نمی‌افتد. اگر به‌ازای هر عدد حقیقی a، $f(a)=g(a)$، آنگاه $f(x)$ و $g(x)$ یک چندجمله‌یی هستند.

مراجع

Trygve Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.
کتاب ناگل کتابی عالی در نظریهٔ پایه‌یی اعداد است. به‌ویژه، خیلی بیشتر از معمول به تحلیل همنهشتیهای چندجمله‌یی می‌پردازد. کتاب اثبات «مقدماتی» سلبرگ (ولی دشوار) از قضیهٔ اعداد اول را نیز در بردارد.

۵

همنهشتیهای درجهٔ دوم و قانون تقابل مربعی

در حالی‌که هیچ روش کارآمدی برای حل همنهشتیهای چندجمله‌یی در حالت کلی، یا حتی اظهارنظر دربارهٔ وجود یا عدم وجود جواب در دست نیست، ولی دربارهٔ حالتِ خاصِ همنهشتیهای درجهٔ دوم خیلی بیشتر می‌توان صحبت کرد. در فصل حاضر این مطالب به تفصیل بررسی خواهند شد. به‌ویژه، با کاربرد قانون تقابل مربعی گاوس، تکنیکی برای تعیین حلپذیری همنهشتیهای درجهٔ دوم عرضه خواهیم کرد. اما، مسألهٔ تعیین جوابها که چه وقتی وجود دارند، هنوز مشکل است، هر چند که روشهایی وجود دارند که می‌توان در بعضی موارد آنها را ارائه داد.

قانون تقابل مربعی یکی از مشهورترین قضیه‌ها در نظریهٔ اعداد است. اولین بار در مقاله‌ای از اویلر در ۱۷۸۳ صحبت از آن به میان آمده، اما او قادر به اثبات آن نبوده است. (در واقع اویلر یک قضیهٔ هم‌ارز با آن را خیلی جلوتر در ۱۷۴۶ حدس زده بوده است.) در ۱۷۸۵، آدرین‌ـماری لژاندر[1] (۱۸۳۳ـ۱۷۵۲) قضیه را به‌صورتی که در (۱۸.۵) ارائه شده بیان کرده است، اما برهانش چندین

1. Adrien-Marie Legendre

رخنه داشته است. (لژاندر فرض کرده بود که بی‌نهایت عدد اول در هر تصاعد عددی به‌صورت $ak+b$ که $(a,b)=1$، وجود دارد. این همان قضیهٔ دیریکله است، که تا سال ۱۸۳۷ اثبات نشده بود. اما حتی با این قضیه، استدلال لژاندر فقط در بعضی حالتها کارساز است.) لژاندر اولین کسی است که به این قضیه به‌عنوان یک «قانون تقابل» اشاره دارد، و در ۱۷۹۸، در کتابش رساله‌ای در نظریهٔ اعداد[1] برهان دیگری ارائه داده است، اما آن نیز متضمن یک اشتباه است. اولین اثباتِ کاملِ قانون تقابل مربعی در ۱۷۹۶ توسط گاوس ارائه گردید و پنج سالِ بعد در تحقیقات حسابی او منتشر شد. سرانجام گاوس شش برهان از این قضیه را ارائه داد، و از آن پس، بیش از ۱۰۰ برهان منتشر شده است. برهانی که در این فصل ارائه می‌دهیم استناد به قضیه‌ای (معروف به لم گاوس) دارد که گاوس در ۱۸۰۸ کشف کرده و به یک برهان نسبتاً ساده از قانون تقابل منجر می‌شود.

قضیه‌هایی برای فصل ۵

همان‌گونه که در فصل ۴ اشاره شد، می‌توان بررسی همنهشتیهای چندجمله‌یی را به حالتی که پیمانه توانِ یک عددِ اولِ p است بدل کرد. حالتهای $p=2$ و p فرد به‌طور جداگانه بررسی می‌شوند. (این امر ضرورت دارد زیرا همنهشتیهای درجهٔ دوم را بررسی می‌کنیم. مثلاً، عدد اولِ ۵ بایستی برای همنهشتیهای چندجمله‌یی از درجهٔ ۵ طور دیگری بررسی شود.)

همنهشتیهای درجهٔ دومِ کلی

اگر p فرد باشد، مطالعهٔ همنهشتیهای درجهٔ دوم به پیمانهٔ p^m به حالتی که پیمانه فقط p است بدل می‌شود. [(۱۰.۴) و (۱۱.۴) را ببینید.] بنابراین همنهشتی درجهٔ دوم عام

$$ax^2+bx+c\equiv 0 \pmod p$$

را در نظر می‌گیریم، که در آن p عدد اول فرد و $p\nmid a$، مسأله را مانند حالت معادلات درجهٔ دوم معمولی، با کامل کردن مربع در سمت چپ همنهشتی شروع می‌کنیم. (اتفاقاً این روش همان روش معمولی برای به‌دست آوردن فرمول معروف درجهٔ دوم است.) چون $(a,p)=1$ ایجاب می‌کند $(4a,p)=1$، همنهشتی را در $4a$ ضرب می‌کنیم تا همنهشتی هم‌ارز

$$(2ax)^2+4abx+4ac\equiv 0 \pmod p$$

را به‌دست آوریم، یعنی

$$(2ax+b)^2\equiv b^2-4ac \pmod p$$

1. Essai sur la théorie des nombres

چون جوابهای این همنهشتی دقیقاً همان جوابهای همنهشتی اصلی است، قضیهٔ زیر را اثبات کرده‌ایم.

(۱.۵) قضیه. فرض می‌کنیم p یک عدد اول فرد باشد و $(a,p)=۱$. در این‌صورت، همهٔ جوابهای همنهشتی $ax^۲+bx+c\equiv ۰ (\mathrm{mod}\, p)$ را می‌توان از حل رشتهٔ همنهشتیهای زیر به‌دست آورد

$$y^۲\equiv b^۲-۴ac \pmod p, \quad ۲ax\equiv y-b \pmod p$$

لذا، برای حل یک همنهشتی درجهٔ دوم کلی پیمانهٔ عددِ اولِ فرد p، کافی است که یک همنهشتی به‌صورت $x^۲\equiv a (\mathrm{mod}\, p)$ را حل کنیم. مثال زیر تکنیک این راه‌حل را نشان می‌دهد.

(۲.۵) مثال. می‌خواهیم جوابهای $۱۱x^۲+۵x+۱۸\equiv ۰ (\mathrm{mod}\, ۲۹)$ را پیدا کنیم. با کامل کردن مربع داریم $(۲۲x+۵)^۲\equiv b^۲-۴ac\equiv ۱۶ (\mathrm{mod}\, ۲۹)$؛ لذا $۲۲x+۵\equiv \pm ۴ (\mathrm{mod}\, ۲۹)$. از حل $۲۲x+۵\equiv ۴ (\mathrm{mod}\, ۲۹)$ داریم $x=۲۵$، و $۲۲x+۵\equiv -۴ (\mathrm{mod}\, ۲۹)$ جواب $x=۲۲$ را به‌دست می‌دهد. بدین‌ترتیب ۲۲ و ۲۵ تنها جوابهای همنهشتی اصلی هستند.

حال $ax^۲+bx+c\equiv ۰ (\mathrm{mod}\, ۲^m)$ را در نظر می‌گیریم. از آنجا که ۴ و ۲ نسبت به‌هم اول نیستند، بایستی استدلال قبل را کمی تغییر دهیم. باز می‌توانیم در $۴a$ ضرب کنیم، ولی برای به‌دست آوردن یک همنهشتی با همان جوابها، بایستی پیمانه را در توان مناسبی از ۲ ضرب کنیم.

(۳.۵) قضیه. فرض می‌کنیم $a=۲^r s$، که s فرد است. در این‌صورت تمام جوابهای همنهشتی $ax^۲+bx+c\equiv ۰ (\mathrm{mod}\, ۲^m)$ را می‌توان از حل رشتهٔ همنهشتیهای زیر به‌دست آورد

$$y^۲\equiv b^۲-۴ac \pmod{۲^{m+r+۲}}, \quad ۲ax\equiv y-b \pmod{۲^{m+r+۲}}$$

برهان. از ضرب همنهشتی اصلی در s همنهشتی هم‌ارز آن:

$$s(ax^۲+bx+c)\equiv ۰ (\mathrm{mod}\, ۲^m)$$

را به‌دست می‌آوریم. تغییر پیمانه لازم نیست، زیرا $(s,۲^m)=۱$. اکنون در $۲^r\times ۴$ ضرب می‌کنیم؛ این بار، برای به‌دست آوردن یک همنهشتی هم‌ارز، بایستی پیمانه را نیز در $۲^r\times ۴$ ضرب کنیم. خلاصه آنکه در $۴a$ ضرب کنیم، و همنهشتی هم‌ارز زیر را به‌دست آوریم

$$(۲ax+b)^۲\equiv b^۲-۴ac \pmod{۲^{m+r+۲}}$$

آشکار است که این با رشتهٔ همنهشتیهای بیان‌شده در صورت قضیه هم‌ارز است.

همنهشتی $x^2 \equiv a \pmod m$

هم‌اکنون دیدیم که اگر s فرد باشد، می‌توان همنهشتی $x^2 \equiv a \pmod s$ را به بررسی $x^2 \equiv a \pmod p$، که در آن p یک عدد اول فرد است، بدل کرد. لذا با توجه به (۱.۵) و (۳.۵)، بررسی یک همنهشتی درجهٔ دوم کلی $ax^2 + bx + c \equiv 0 \pmod m$ به بررسی همنهشتیهای زیر تبدیل می‌شود

$$x^2 \equiv a \pmod{2^k} \quad \text{و} \quad x^2 \equiv a \pmod p \quad (p \text{ یک عدد اول فرد}).$$

به‌طورکلی، سعی می‌کنیم اعداد صحیحی را تعیین کنیم که «مربع‌کامل» به پیمانهٔ 2^k و پیمانهٔ p هستند.

برای این کار باید دو مسأله را در نظر بگیریم. اول، چه وقت برای این همنهشتیها جواب وجود دارد؟ دوم، اگر این همنهشتیها حلپذیرند، چه تعداد جواب وجود دارد؟ برای یک عدد اول فرد p جواب سؤال اول بسیار مشکل است؛ برای $p = 2$، پاسخ در (۱۴.۴) آمده است. سؤال دوم، که خیلی آسانتر از اولی است، در (۱۳.۴) و (۱۴.۴) مطرح شده است. جهت تکمیل، قضیه‌های مربوطه را در اینجا بیان می‌کنیم.

(۴.۵) قضیه. (i) اگر $(a, p) = 1$، آنگاه $x^2 \equiv a \pmod{p^k}$ جوابی ندارد هرگاه $x^2 \equiv a \pmod p$ حلپذیر نباشد و دقیقاً دو جواب دارد اگر $x^2 \equiv a \pmod p$ حلپذیر باشد.

(ii) فرض می‌کنیم a فرد باشد. اگر همنهشتی $x^2 \equiv a \pmod{2^k}$ حلپذیر باشد، آنگاه دارای ۱، ۲، یا ۴ جواب است برحسب آنکه k مساوی ۱، ۲، یا $k \geq 3$.

می‌توان این قضیه‌ها را با (۳.۴) ترکیب کرد و تعداد جوابهای $x^2 \equiv a \pmod m$ را که در آن m یک عدد صحیح مثبت دلخواهی است، به‌دست آورد.

(۵.۵) قضیه. فرض می‌کنیم $m = 2^k p_1^{k_1} \cdots p_r^{k_r}$، و $(a, m) = 1$. در این‌صورت همنهشتی $x^2 \equiv a \pmod m$ حلپذیر است اگر و تنها اگر $x^2 \equiv a \pmod{2^k}$ و

$$(i = 1, 2, \ldots, r)\ x^2 \equiv a \pmod{p_i^{k_i}}$$

حلپذیر باشند. اگر $x^2 \equiv a \pmod m$ حلپذیر باشد، آنگاه به‌ازای $k = 0$ یا $k = 1$ تعداد 2^r جواب، برای $k = 2$، تعداد 2^{r+1} جواب، و برای $k \geq 3$ تعداد 2^{r+2} جواب وجود دارد.

مانده‌های درجهٔ دوم

در بحث قبل قسمت اعظم تکیهٔ ما بر تعداد جوابهای $x^2 \equiv a \pmod{p^k}$ بود، که در آن p اول است. اکنون توجه خود را به مسأله وجود جوابها برمی‌گردانیم. وقتی که $p = 2$، (۱۴.۴)

پاسخ کاملی به‌دست داده است. اگر p فرد باشد و $p|a$، می‌توان مسأله را خیلی ساده به حالت $(a,p)=۱$ تبدیل کرد.

بنابراین از حالا به بعد فرض خواهیم کرد که p یک عدد اول فرد است و $(a,p)=۱$. اگر $f(x)=x^۲-a$، آنگاه $f'(x)=۲x$. اگر s ریشه‌ای از $f(x)$ به پیمانهٔ p باشد، آنگاه $p\nmid s$، زیرا $(a,p)=۱$. لذا $f'(s)=۲s$ بر p بخشپذیر نیست، و بنابراین از (۱۱.۴) نتیجه می‌شود که برای هر $k\geq ۱$، $f(x)$ یک ریشه به پیمانهٔ p^k دارد.

بنابراین می‌توانیم توجه خود را به‌وجود جواب برای $x^۲\equiv a(\bmod p)$، که در آن p عدد اول فردی است، معطوف کنیم. این حالت یک روش بسیار دقیقتر از حالت $p=۲$ را طلب می‌کند، و سرانجام قانون تقابل مربعی، یکی از مهمترین قضیه‌ها در نظریهٔ اعداد، را به‌کار می‌بریم.

مطلب را با تعریف مهم شروع می‌کنیم.

(۶.۵) تعریف. فرض می‌کنیم m یک عدد صحیح بزرگتر از ۱ باشد، و $(a,m)=۱$. در این‌صورت a یک ماندهٔ درجهٔ دومِ m خوانده می‌شود اگر $x^۲\equiv a(\bmod m)$ دارای جواب باشد. اگر جواب وجود نداشته باشد، a یک نامانده‌ٔ درجهٔ دومِ m نامیده می‌شود.

توضیحات. ۱. اگر $a\equiv b(\bmod m)$، آنگاه آشکار است که a یک ماندهٔ درجهٔ دومِ m است اگر و تنها اگر b یک ماندهٔ درجهٔ دومِ m باشد.

۲. از آنجا که اگر a با m متباین باشد، هر جوابِ $x^۲\equiv a(\bmod m)$ بایستی با m متباین باشد، می‌توان تمام مانده‌های درجهٔ دومِ m را با مربع کردن عناصر یک دستگاه مخفف مانده‌ها به پیمانهٔ m پیدا کرد. به‌ویژه، در مورد یک پیمانهٔ اول p کافی است که ± ۱، ± ۲، ...، $\pm(p-۱)/۲$ را مربع کنیم. به آسانی دیده می‌شود که هر دو عنصر ۱، ۲، ...، $(p-۱)/۲$ به پیمانهٔ p ناهمنهشت‌اند.

چون اگر p اول باشد، در هر دستگاه مخفف مانده‌ها به پیمانهٔ p دقیقاً $p-۱$ عنصر وجود دارد، قضیهٔ زیر را داریم.

(۷.۵) قضیه. اگر p یک عدد اول فرد باشد، دقیقاً $(p-۱)/۲$ ماندهٔ درجهٔ دوم ناهمنهشت از p و دقیقاً $(p-۱)/۲$ نامانده‌ٔ درجهٔ دوم از p داریم.

نماد لژاندر، که بعداً تعریف می‌شود، توسط لژاندر در ۱۷۹۸ در کتابش، رساله‌ای در نظریهٔ اعداد، معرفی شد، این کتاب نخستین کار مهم (صرف‌نظر از ترجمه‌های دیوفانتوس و کتاب مربعات، فیبوناتجی) بود که تماماً به نظریهٔ اعداد اختصاص دارد.

(۸.۵) تعریف. اگر p یک عدد اول فرد باشد و $(a,p) = ۱$، آنگاه لژاندر که با (a/p) نشان داده می‌شود برابر ۱ است اگر a یک ماندهٔ درجهٔ دوم p باشد و -۱ است اگر a یک نامانده درجهٔ دوم p باشد.

قابل ذکر است که نماد لژاندر، (a/p) فقط وقتی تعریف می‌شود که p یک عدد اول فرد باشد و $p \nmid a$.

قضیهٔ بعد یک بیان دیگر ملاک اویلر (قضیهٔ ۴.۳) است، و (۱۰.۵) یک نتیجهٔ ساده آن.

(۹.۵) ملاک اویلر. فرض می‌کنیم p یک عدد اول فرد باشد، و $(a,p) = ۱$. در این‌صورت $(a/p) \equiv a^{(p-۱)/۲} (\mathrm{mod}\, p)$.

(۱۰.۵) قضیه. فرض می‌کنیم که p یک عدد اول فرد باشد. در این‌صورت

(i) $a \equiv b (\mathrm{mod}\, p)$ ایجاب می‌کند $(a/p) = (b/p)$؛

(ii) $(ab/p) = (a/p)(b/p)$؛

(iii) $(a^۲/p) = ۱$؛

(iv) $(a^۲b/p) = (b/p)$.

توضیح. قسمت (ii) از (۱۰.۵) را می‌توان به طریق زیر نیز بیان کرد: حاصلضرب دو ماندهٔ درجهٔ دوم (یا دو نامانده درجهٔ دوم) مجدداً یک ماندهٔ درجهٔ دوم است، در حالی‌که حاصلضرب یک ماندهٔ درجهٔ دوم در یک نامانده درجهٔ دوم یک نامانده p است.

اگر a را در (۹.۵) برابر -۱ اختیار و توجه کنیم که $(p-۱)/۲$ زوج است اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۴)$، بیانی برای اعداد اول فردی که برای آنها -۱ یک ماندهٔ درجهٔ دوم است به‌دست می‌آوریم.

(۱۱.۵) قضیه. فرض می‌کنیم p یک عدد اولِ فرد باشد. در این‌صورت $(-۱/p) = ۱$ اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۴)$.

فرما از این حقیقت آگاهی داشت که $x^۲ \equiv -۱ (\mathrm{mod}\, p)$ حلپذیر است اگر و تنها اگر p به‌صورت $۴k + ۱$ باشد، قضیه‌ای که برای نخستین‌بار توسط اویلر حدود ۱۷۵۰ ثابت شد. (ملاک اویلر حدود پنج سال بعد ثابت شد.) وقتی که همنهشتی حلپذیر است، جوابها با $\pm(۲k)!$ داده می‌شوند، که در آن $p = ۴k + ۱$. (مسألهٔ ۲۶.۳ را ببینید.) این طریق یک طریق شدنی از لحاظ محاسبه برای حل همنهشتی به‌ازای اعداد اولِ بزرگ p نیست. اما می‌توان جوابی از

$x^۲ \equiv -۱ (\mathrm{mod}\, p)$ را از هر ماندهٔ درجهٔ دوم p به توان $(p-۱)/۴$ پیدا کرد. (این مطلب بلافاصله از ملاک اویلر نتیجه می‌شود).

برای استفاده از قانون تقابل مربعی، همچنین لازم داریم که یک رده‌بندی در اعداد اولی که عدد ۲ یک ماندهٔ درجهٔ دوم آنهاست انجام دهیم. به‌جای استفاده از لم گاوس برای به‌دست آوردن این رده‌بندی، برهان زیر از ملاک اویلر را به‌کار می‌بریم.

(۱۲.۵) قضیه. فرض می‌کنیم p یک عدد اول فرد باشد. در این‌صورت ۲ یک ماندهٔ درجهٔ دوم p است اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۸)$ و یک ماندهٔ درجهٔ دوم p است اگر $p \equiv \pm ۳ (\mathrm{mod}\, ۸)$.

برهان. اگر $p \equiv ۵ (\mathrm{mod}\, ۸)$ یا $p \equiv ۱$، به آسانی دیده می‌شود که

$$۲^{(p-۱)/۲} \left(\frac{p-۱}{۲}\right)! = ۲ \times ۴ \times ۶ \cdots (p-۱)$$

$$\equiv ۲ \times ۴ \times ۶ \cdots \frac{p-۱}{۲} \times \left(-\frac{p-۳}{۲}\right) \cdots (-۵)(-۳)(-۱)$$

$$\equiv (-۱)^{(p-۱)/۴} \left(\frac{p-۱}{۲}\right)! \pmod{p}$$

اگر هر دو طرف را بر $!((p-۱)/۲)$ تقسیم کنیم خواهیم داشت

$$۲^{(p-۱)/۲} \equiv (-۱)^{(p-۱)/۴} (\mathrm{mod}\, p)$$

لذا بنابر ملاک اویلر $(p-۱)/۴$، $(۲/p) = (-۱)^{(p-۱)/۴}$. لذا $(۲/p)$ مساوی -۱ یا $+۱$ است برحسب اینکه $p \equiv ۵ (\mathrm{mod}\, ۸)$ یا $p \equiv ۱$.

با استدلالی مشابه، اگر $p \equiv ۷ (\mathrm{mod}\, ۸)$ یا $p \equiv ۳$، به‌سادگی دیده می‌شود که

$$۲^{(p-۱)/۲} \left(\frac{p-۱}{۲}\right)! = ۲ \times ۴ \times ۶ \cdots \frac{p-۳}{۲} \left(-\frac{p-۱}{۲}\right) \cdots (-۵)(-۳)(-۱)$$

$$= (-۱)^{(p+۱)/۴} \left(\frac{p-۱}{۲}\right)! \pmod{p}$$

از تقسیم طرفین بر $!((p-۱)/۲)$ داریم $۲^{(p-۱)/۲} \equiv (-۱)^{(p+۱)/۴} (\mathrm{mod}\, p)$. لذا، بنابر ملاک اویلر، $(۲/p)$ مساوی ۱ یا -۱ است برحسب آنکه $p \equiv ۷ (\mathrm{mod}\, ۸)$ یا $p \equiv ۳$.

قضیهٔ بعد برای بسیاری از مسأله‌های این فصل مفید است. برهانها را می‌توان در مسأله‌های ۴۹.۵، ۵۱.۵، ۵۲.۵، و ۵۳.۵ پیدا کرد.

(۱۳.۵) قضیه. فرض می‌کنیم p یک عدد اول فرد باشد. در این‌صورت

(i) ۲− یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv ۱, ۳ (\mathrm{mod}\, ۸)$؛

(ii) ۳ یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۱۲)$؛

(iii) ۳− یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۶)$؛

(iv) ۵ یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۵)$.

قانون تقابل مربعی

گرچه برهانهای بسیاری برای قانون تقابل مربعی وجود دارد، برهانی که ارائه می‌دهیم شاید ساده‌ترین آنها باشد. دو قضیهٔ زیر نقش کلیدی در برهان دارند. اولی، که توسط گاوس در ۱۸۰۸ ثابت شده، ملاکی است برای اینکه یک عدد صحیح ماندهٔ درجهٔ دوم عدد اول p باشد. به شباهت بین برهان آن و برهان قضیهٔ اویلر توجه کنید.

(۱۴.۵) لم گاوس. فرض می‌کنیم p یک عدد اول فرد باشد و $(a, p) = ۱$. کوچکترین مانده‌های مثبت اعداد a، $۲a$، ...، $\frac{p-۱}{۲}a$ نسبت به پیمانهٔ p را در نظر می‌گیریم. اگر تعداد این مانده‌ها که بزرگتر از $p/۲$ هستند برابر N باشد، آنگاه $(a/p) = (-۱)^N$.

برهان. اعداد صحیح a، $۲a$، ...، $\frac{p-۱}{۲}a$ نسبت به p اول‌اند و به پیمانهٔ p ناهمنهشت. فرض می‌کنیم $u_۱$، $u_۲$، ...، u_N کوچکترین مانده‌های مثبت این اعداد باشند که از $p/۲$ بزرگترند، و $v_۱$، $v_۲$، ...، v_M کوچکترین مانده‌های مثبت این اعداد باشند که از $p/۲$ کوچکترند؛ در این‌صورت $N + M = (p-۱)/۲$.

اعداد $p - u_۱$، $p - u_۲$، ...، $p - u_N$ مثبت، کمتر از $p/۲$، و نسبت به p اول‌اند و هیچ دو تا از آنها همنهشت به پیمانهٔ p نیستند. همچنین، هیچ $p - u_i$ مساوی یک v_j نیست. زیرا فرض کنیم $p - u_i = v_j$؛ گیریم $u_i \equiv ra (\mathrm{mod}\, p)$ و $v_j \equiv sa (\mathrm{mod}\, p)$، که در آنها r و s در عدد صحیح متمایز بین ۱ و $(p-۱)/۲$ هستند. پس $p \equiv a(r+s) (\mathrm{mod}\, p)$، و چون $(a, p) = ۱$، بایستی داشته باشیم $p | r+s$، که یک تناقض است زیرا $۰ < r+s < p$.

بنابراین، $p - u_۱$، $p - u_۲$، ...، $p - u_N$، $v_۱$، $v_۲$، ...، v_M گردایه‌ای از $(p-۱)/۲$ عدد صحیح ناهمنهشت است که مثبت و کمتر از $p/۲$ هستند. لذا، به ترتیبی، برابر با ۱، ۲، ...، $(p-۱)/۲$ هستند، و لذا

$$(p-u_۱)(p-u_۲)\cdots(p-u_N)v_۱v_۲\cdots v_M = ((p-۱)/۲)!$$

یعنی،

$$(-۱)^N u_۱ u_۲ \cdots u_N v_۱ v_۲ \cdots v_M \equiv ((p-۱)/۲)! \pmod p$$

اما از طرفی $u_۱$، $u_۲$، ...، u_N، $v_۱$، $v_۲$، ...، v_M به‌ترتیبی با a، $۲a$، ...، $\frac{p-۱}{۲}a$ همنهشت‌اند، و لذا

$$\begin{aligned}\left(\frac{p-۱}{۲}\right)! &\equiv (-۱)^N a \times ۲a \cdots \frac{p-۱}{۲}a \\ &= (-۱)^N a^{(p-۱)/۲} \left(\frac{p-۱}{۲}\right)! \pmod p\end{aligned}$$

چون در $((p-۱)/۲)!$ هر عامل با p متباین است، می‌توانیم طرفین همنهشتی آخر را بر $((p-۱)/۲)!$ تقسیم کنیم و $a^{(p-۱)/۲} \equiv (-۱)^N \pmod p$ را به‌دست آوریم. اکنون نتیجهٔ لم از ملاک اویلر به‌دست می‌آید.

(۱۵.۵) مثال. از آنجا که لم گاوس برای اثبات (۱۶.۵) است، دقت جزءبه‌جزء یک مثال آموزنده است. از لم گاوس برای تعیین آن اعداد اول p که ۵ یک ماندهٔ درجهٔ دوم آنهاست استفاده می‌کنیم. اگر $P = (p-۱)/۲$، آنگاه تمام اعداد صحیح ۵، ۱۰، ...، $۵P$ کمتر از $۵p/۲$ هستند. لذا تنها اعدادی که کوچکترین ماندهٔ مثبت آنها بزرگتر از $p/۲$ هستند عبارت‌اند از اعداد صحیح $۵j$ که در بازهٔ $(p/۲, p)$ یا $(۳p/۲, ۲p)$ قرار دارند. به دلایلی که به‌زودی روشن خواهد شد، می‌نویسیم $p = ۲۰k + r$، که r مساوی ۱، ۳، ۷، ۹، ۱۱، ۱۳، ۱۷، یا ۱۹ است. (برای مقادیر دیگر r، p اول نیست.) سپس می‌خواهیم عددی مانند j بیابیم به‌طوری که $p/۲ < ۵j < p$ یا $۳p/۲ < ۵j < ۲p$. از نابرابری اول داریم $p/۵ < j < p/۱۰$، و لذا $۲k+r/۱۰ < j < ۴k+r/۵$؛ به روشی مشابه، از نابرابری دوم به‌صورت $۲p/۵ < j < ۳p/۱۰$ می‌شود، و لذا $۶k + ۳r/۱۰ < j < ۸k + ۲r/۵$.

توجه دارید که همپایگی[1] (یعنی زوج یا فرد بودن) تعداد اعداد صحیحی که در هر یک از این نابرابریها صدق می‌کنند با افزودن اعداد صحیح زوج (که لزومی به برابری آنها نیست) به دو طرف نابرابری تغییر نمی‌کند. این مطلب از این حقیقت ناشی می‌شود که اختلافِ تعداد اعداد صحیح در بازهٔ جدید با تعداد اعداد صحیح در بازهٔ اصلی یک عدد زوج است. دقیقتر بگوییم، اگر $n(a,b)$ معرف تعداد اعداد صحیح در بازهٔ (a,b) باشد، آنگاه $n(a,b) = n(a+۲k, b+۲k)$، زیرا فقط بازه را $۲k$ انتقال داده‌ایم؛ همچنین، $n(a+۲k, b+۴k) = n(a, ۲k, b+۲k) + ۲k$،

1. parity

زیرا بازهٔ $(a+2k, b+2k)$ را به اندازهٔ $2k$ بسط داده‌ایم تا $(a+2k, b+4k)$ حاصل شود. لذا می‌توانیم $2k$ و $4k$ را از نابرابری اول در بالا و $6k$ و $8k$ را از نابرابری دوم حذف کنیم. (دلیل نوشتن $20k+r$ به‌صورت p این است که اعداد صحیح زوج نظیر $2k$، $4k$، $6k$، و $8k$ را در این نابرابریها به‌دست آوریم.) در این‌صورت نابرابریهای $r/10 < j < r/5$ و $3r/10 < j < 2r/5$ برای ما می‌ماند. اکنون این امتحان که اگر، مثلاً r برابر ۱ باشد، یک چنین jای وجود ندارد، کار ساده‌ای است؛ اگر $r = 3$، یک چنین jای وجود دارد (هیچ jای در نابرابری اول صدق نمی‌کند و یکی در دومی صدق می‌کند)؛ اگر $r = 17$، سه مقدار j وجود دارد (دو عدد صحیح که در نابرابری اول صدق می‌کنند و یکی که در دومی صدق می‌کند)؛ و هکذا به همین قیاس.

بنابراین اگر N تعداد کوچکترین مانده‌های مثبت ۵، ۱۰، ۱۵، ...، $5P$ باشد که از $p/2$ بزرگترند، آنگاه N زوج است اگر و تنها اگر r مساوی ۱، ۹، ۱۱، یا ۱۹ باشد. لذا از لم گاوس نتیجه می‌شود که ۵ یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv \pm 1, \pm 9 \pmod{20}$.

توضیح. از این مثال روشن می‌شود که مقدار $(5/p)$ فقط به باقیمانده تقسیم p بر $5 \times 4 = 20$ بستگی دارد؛ لذا اگر باقیمانده‌های تقسیم دوعدد اول p و q بر ۲۰ یکی باشند، آنگاه $(5/q) = (5/p)$. استدلال مشابه نشان می‌دهد که مقدار $(3/p)$ فقط به باقیماندهٔ تقسیم p بر $3 \times 4 = 12$ بستگی دارد، مقدار $(6/p)$ فقط به باقیماندهٔ تقسیم p بر $6 \times 4 = 24$، مقدار $(7/p)$ فقط به باقیماندهٔ تقسیم p بر $7 \times 4 = 28$، و مانند اینها. حکم مشابه برای $(2/p)$ نیز صادق است؛ (۱۲.۵ را ببینید).

بر اساس این‌گونه مثالهای عددی، منطقی است که برقراری این حکم در حالت کلی زیر سؤال برده شود. قضیهٔ بعد، که با قانون تقابل درجهٔ دوم هم‌ارز است، در ابتدا توسط اویلر بیان شده (ولی اثبات نشده) است. در واقع این قضیه نشان می‌دهد که ماهیت درجهٔ دوم a به پیمانهٔ p کاملاً با باقیماندهٔ تقسیم p بر $4a$ مشخص می‌شود. به‌ویژه، اگر باقیمانده‌های تقسیم دو عدد اول بر $4a$ یکی باشد، یا a یک ماندهٔ درجهٔ دوم از هر دو عدد اول یا یک نامانده درجهٔ دوم از هر دو است.

(۱۶.۵) قضیه. گیریم p و q دو عدد اولِ فردِ متمایز باشند، و فرض می‌کنیم $(a,p) = (a,q) = 1$، که a یک عدد صحیح مثبت است. اگر $q \equiv p \pmod{4a}$ یا $q \equiv -p \pmod{4a}$، آنگاه $(a/q) = (a/p)$.

برهان. گیریم $S = \{a, 2a, 3a, \ldots, Pa\}$، که در آن $P = (p-1)/2$. تعداد عنصرهای S را که کوچکترین مانده‌های مثبت آنها بزرگتر از $p/2$ است با N نشان می‌دهیم؛ در این‌صورت

بنابر لم گاوس $(a/p) = (-1)^N$. برای یافتن N، مانند مثال بالا، بایستی تعداد عنصرهای S را که در بازه‌های $(p/2, p)$، $(p, 3p/2)$، $(3p/2, 2p)$، $(5p/2, 3p)$، ... واقع می‌شوند تعیین کنیم، زیرا کوچکترین ماندهٔ مثبت $ja (1 \le j \le P)$ از $p/2$ تجاوز می‌کند اگر و تنها اگر ja در یکی از این بازه‌ها قرار گیرد. به‌روشنی دیده می‌شود که، فقط تعداد متناهی بازه برای امتحان کردن وجود دارند؛ آخرین بازه را با $((c - 1/2)p, cp)$ نشان می‌دهیم. (چون $Pa < (a/2)p$، به آسانی دیده می‌شود که $c = a/2$ اگر a زوج و $c = (a-1)/2$ اگر a فرد باشد.) توجه می‌کنید که عناصر S نمی‌توانند نقاط انتهایی این بازه‌ها باشند، زیرا اگر $ja = mp$ (یا $ja = (m/2)p$)، آنگاه $p|ja$ و چون $(a, p) = 1$ لذا $p|j$؛ که ممکن نیست زیرا $0 < j < p$.

اگر یک عنصر ja از S در اولین بازه قرار گیرد، آنگاه $p/2 < ja < p$، یعنی، $p/2a < j < 2p/a$. با بیانی مشابه، اگر ja در بازهٔ دوم باشد، آنگاه $3p/2a < j < 2p/a$، و هکذا. بنابراین N تعداد کل اعداد صحیح در بازه‌های

$$\left(\frac{p}{2a}, \frac{p}{a}\right), \quad \left(\frac{3p}{2a}, \frac{2p}{a}\right), \ldots, \left(\frac{(2c-1)p}{2a}, \frac{cp}{a}\right) \qquad (1)$$

است. اکنون فرض می‌کنیم $q \equiv p \pmod{4a}$؛ پس یک عدد صحیح m وجود دارد که $q = 4am + p$. اگر M تعداد عناصر a، $2a$، $3a$، ...، $((p-1)/2)a$ باشد که کوچکترین مانده‌های مثبت آنها از $q/2$ بزرگترند، آنگاه $(a/q) = (-1)^M$. اگر مانند بالا استدلال کنیم، نتیجه می‌شود که M درست تعداد اعداد صحیح واقع در بازه‌های زیر است

$$\left(\frac{q}{2a}, \frac{q}{a}\right), \quad \left(\frac{3q}{2a}, \frac{2q}{a}\right), \ldots, \left(\frac{(2c-1)q}{2a}, \frac{cq}{a}\right) \qquad (2)$$

چون $q = 4am + p$، می‌توان این گردایه را به‌صورت زیر نوشت

$$\left(2m + \frac{p}{2a}, 4m + \frac{p}{a}\right), \quad \left(6m + \frac{3p}{2a}, 8m + \frac{2p}{a}\right), \ldots,$$
$$\left(2(2c-1)m + \frac{(2c-1)p}{2a}, 4cm + \frac{cp}{a}\right) \qquad (3)$$

همان‌گونه که در مثال ۱۵.۵ نشان دادیم، همپایگی M تغییر نمی‌کند اگر اعداد صحیح زوج، که ممکن است منفی هم باشند، به دو سر بازه اضافه کنیم. می‌توان اعداد صحیح متفاوت برای سر سمت چپ و سر سمت راست به‌کار برد. با کم کردن $2m$ و $4m$ از دو سر بازهٔ اول در (۳)، $6m$ و $8m$ از دو سر بازهٔ دوم، و مانند آن، خواهیم داشت

$$\left(\frac{p}{2a}, \frac{p}{a}\right), \quad \left(\frac{3p}{2a}, \frac{2p}{a}\right), \ldots, \left(\frac{(2c-1)p}{2a}, \frac{cp}{a}\right)$$

از آنجا که این همان گردایهٔ بازه‌ها در (۱) است، M و N همپایگی واحدی دارند، و لذا بنابر لم گاوس $(a/p) = (a/q)$.

حال فرض می‌کنیم $q \equiv -p \pmod{۴a}$؛ پس یک m وجود دارد که $q = ۴am - p$. با گذاشتن این مقدار q در (۲)، گردایهٔ زیر از بازه‌های مجزا را به‌دست می‌آوریم:

$$\left(۲m - \frac{p}{۲a}, ۴m - \frac{p}{a}\right), \left(۶m - \frac{۳p}{۲a}, ۸m - \frac{۲p}{a}\right), \ldots, \left(۲(۲c-۱)m - \frac{(۲c-۱)p}{۲a}, ۴cm - \frac{cp}{a}\right) \tag{۴}$$

اگر M تعدادِ کل اعداد صحیح در این بازه‌ها باشد، آنگاه $(a/q) = (-۱)^M$، فرض کنیم $n(u,v)$ معرف تعداد اعداد صحیح در بازهٔ (u,v) باشد. اگر بازهٔ اول در (۴) را در نظر بگیریم، می‌توانیم $۲m$ را از دو سر آن کم کنیم تا به‌دست آوریم

$$n(۲m - p/۲a, ۴m - p/a) = n(-p/۲a, ۲m - p/a)$$

اگر منعکس این بازهٔ آخر را نسبت به نقطهٔ ۰ پیدا کنیم، خواهیم داشت

$$n(۲m - p/۲a, ۴m - p/a) = n(p/a - ۲m, p/۲a)$$

اجتماع بازه‌های $(p/a - ۲m, p/۲a)$ و $(p/۲a, p/a)$ بازهٔ $(p/a - ۲m, p/a)$ منهای نقطهٔ $p/۲a$ است؛ باید توجه کرد که نقطهٔ حذف‌شدهٔ $p/۲a$ نمی‌تواند یک عدد صحیح باشد، زیرا $(a,p) = ۱$. لذا

$$n(p/a - ۲m, p/۲a) + n(p/۲a, p/a) = n(p/a - ۲m, p/a)$$

از آنجا که بازهٔ $(p/a - ۲m, p/a)$ شامل $۲m$ عدد صحیح است و دو سر بازه اعداد صحیح نیستند، $n(p/a - ۲m, p/۲a)$ و $n(p/۲a, p/a)$ یک همپایگی دارند، و لذا $n(۲m - p/۲a, ۴m - p/a)$ و $n(p/۲a, p/a)$ یک همپایگی دارند.

استدلال مشابه برای هر بازه در (۱) و بازهٔ نظیر در (۴) کارساز است. در نتیجه M و N یک همپایگی دارند، و لذا بنابر لم گاوس $(a/p) = (a/q)$. که برهان کامل می‌شود.

حال آماده‌ایم که قانون تقابل مربعی را ثابت کنیم. بیان ارائه‌شده در (۱۷.۵) ابتدا توسط لژاندر در ۱۷۸۵ به‌عنوان یک حدسیه بیان شد. اولین اثبات کامل این قضیه توسط گاوس در ۱۸۰۱ در تحقیقات حسابی ارائه گردید.

(۱۷.۵) قانون تقابل مربعی گاوس. فرض می‌کنیم p و q دو عدد اول فردِ متمایز باشند. پس
$(p/q) = (q/p)$ اگر حداقل یکی از دو عدد p و q به‌صورت $4k+1$ باشد، و
$(p/q) = -(q/p)$ اگر p و q هر دو به‌صورت $4k+3$ باشند.

برهان. ابتدا فرض می‌کنیم که $q \equiv p \pmod 4$؛ پس عدد صحیحی چون m وجود دارد به‌طوری که $q = p + 4m$. از (۱۰.۵) نتیجه می‌شود که

$$(q/p) = ((p+4m)/p) = (4m/p) = (m/p)$$

به همین طریق، $(p/q) = ((q-4m)/q) = (-4m/q) = (-1/q)(m/q)$. لم قبل ایجاب می‌کند که $(m/p) = (m/q)$، و لذا $(q/p)(p/q) = (-1/q)$. لذا بنابر (۱۱.۵)، این حاصلضرب برابر ۱ است اگر p و بنابراین q به‌صورت $4k+1$ باشند، و -1 است اگر هر دو به‌صورت $4k+3$ باشند.

حال فرض کنیم $q \equiv -p \pmod 4$؛ پس یکی از دو عدد p و q به‌صورت $4k+1$ و دیگری به‌صورت $4k+3$ است. فرض می‌کنیم $q = -p + 4m$. اگر مانند بالا استدلال کنیم، داریم $(q/p) = (m/q)$ و $(p/q) = (m/q)$. از (۱۶.۵) نتیجه می‌شود که $(m/q) = (m/p)$، و لذا $(q/p) = (p/q)$.

بیان هم‌ارز زیر از قانون تقابل نتیجهٔ سادهٔ (۱۷.۵) است، که بیان می‌کند که نمای $\frac{p-1}{2} \times \frac{q-1}{2}$ فرد است اگر و تنها اگر هر دو عدد اول به‌صورت $4k+3$ باشند.

(۱۸.۵) قانون تقابل مربعی. فرض می‌کنیم که p و q دو عدد اولِ فردِ متمایز باشند. پس

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

اهمیت قانون تقابل مربعی در این واقعیت نهفته است که می‌توان به‌جای هر نماد مفروض لژاندر (با استفاده از ۱۰.۵) یک حاصلضرب از نمادهای لژاندر با «مخرج» کوچکتر (لزوماً اول) قرار دارد. ولی، این روند تبدیل، تجزیه به اعداد اول صورت در نماد لژاندر را طلب می‌کند، و لذا اگر اعداد صحیحِ مفروض بزرگ باشند این کار عملی نیست. یک روش بسیار کارآمدتر، استفاده از نماد ژاکوبی است، که تعریف و ویژگیهایش قبل از مسائل ۶۷.۵ تا ۷۱.۵ ارائه شده‌اند.

توضیحات. ۱. فرض می‌کنیم a عدد صحیحی بزرگتر از ۱ باشد. چون a حاصلضربی از توانهای اول است، می‌توانیم (ii.۱۰.۵) را برای نوشتن (a/p) به‌صورت حاصلضرب نمادهای لژاندر (q^k/p)، که q یک عدد اول (احتمالاً ۲) است به‌کار بریم. از (iv.۱۰.۵) نتیجه می‌شود که

اگر q اول باشد و $(q,p) = ۱$)، آنگاه

$$(q^k/p) = (q/p) \text{ وقتی } k \text{ زوج باشد و } (q^k/p) = ۱ \text{ هرگاه } k \text{ فرد باشد.}$$

(اگر a منفی باشد، ملاحظه می‌کنید که $(a/p) = (-۱/p)(|a|/p)$). لذا برای محاسبهٔ هر نماد لژاندر (a/p)، کافی است که بدانیم چگونه $(-۱/p)$، $(۲/p)$، و (q/p) را، که q یک عدد اول فرد است، محاسبه کنیم. (۱۱.۵) و (۱۲.۵) را برای محاسبهٔ $(-۱/p)$ و $(۲/p)$ به‌کار می‌بریم، و از قانون تقابل مربعی برای وارون (q/p) استفاده می‌کنیم. بنابر (i.۱۰.۵)، می‌توانیم (p/q) را به‌صورت (b/q) بنویسیم، که در آن $b \equiv p \pmod q$ و $b < p$. اکنون b را به‌صورت حاصلضرب توانهای اول بیان نموده و این روند را تکرار می‌کنیم. می‌توانیم قانون تقابل را آنقدر که لازم است به‌کار بریم تا نمادهای لژاندر را که مقادیرشان بدیهی است به‌دست آوریم. برای مثالهایی از این تکنیک مسألهٔ ۴۶.۵ را ببینید.

۲. ملاک اویلر در واقع یک روش خیلی کارآمد برای محاسبهٔ (a/p) است و وقتی p اول باشد خیلی سریعتر از کاربرد قانون تقابل مربعی به نتیجه می‌رسد. (برای استفاده از قانون تقابل، بایستی صورت نماد لژاندر را به عوامل اول تجزیه کنیم، و هیچ روش شناخته‌شده‌ای برای تجزیهٔ سریع اعداد بزرگ وجود ندارد.) ولی، وقتی p بزرگ نیست، قانون تقابل مربعی می‌تواند خیلی سریع ما را به جواب برساند.

یکی از کاربردهای مهم قانون تقابل درجهٔ دوم تعیین حلپذیری $x^۲ \equiv a \pmod p$ است، که در آن p یک عدد اول فرد مفروض است، اما مورد استعمال نظری اصلی آن مشخص کردن اعداد اولی است که یک عدد صحیح مفروض ماندهٔ درجهٔ دوم آنها باشد. (۲۰.۵ را ببینید.) یکی از موارد استعمال نسبتاً شگفت‌انگیز قانون تقابل اثبات وجود بی‌نهایت عدد اول در بعضی تصاعدهای عددی است (مثلاً، بی‌نهایت عدد اول به‌صورت $۵k - ۱$، $۶k + ۱$، $۸k + ۳$، $۸k - ۱$، و مانند اینها ــ مسأله‌های ۲۳.۵، ۴۸.۵، ۵۰.۵، و ۵۴.۵ را ببینید).

تمام این کاربردها به تفصیل در مسأله‌ها بحث می‌شوند. فعلاً، برای نحوهٔ استفاده از قانون تقابل برای تعیین وجود جواب در یک همنهشتی چندجمله‌یی مفروض مثالی می‌آوریم.

(۱۹.۵) مثال. حلپذیری همنهشتی $۱۸x^۲ - ۷۴x + ۳۷ \equiv ۰ \pmod{۳۱۱}$ را بررسی کنید (۳۱۱ اول است).

حل. بنابر (۱.۵)، کافی است حلپذیری $y^۲ \equiv b^۲ - ۴ac \equiv ۳۰ \pmod{۳۱۱}$ را بررسی کنیم. (در اینجا، $y = ۲ax + b = ۳۶x - ۷۴$، اما چون فقط می‌خواهیم وجود جواب را بررسی کنیم، فقط احتیاج داریم که ببینیم $b^۲ - ۴ac$ یک ماندهٔ درجهٔ دوم ۳۱۱ هست یا نه.) چون

$۵ \times ۳ \times ۲ = ۳۰$، داریم $(۳۰/۳۱۱) = (۲/۳۱۱)(۳/۳۱۱)(۵/۳۱۱)$. توجه می‌کنید که ۳۱۱ به‌صورت $۸k + ۷$ است، لذا (۱۲.۵) ایجاب می‌کند که $(۲/۳۱۱) = ۱$. چون ۳ و ۳۱۱ هر دو به‌صورت $۴k + ۳$ هستند، (۱۷.۵)، (i.۱۰.۵)، و (۱۲.۵) را به‌کار می‌بریم تا

$$(۳/۳۱۱) = -(۳۱۱/۳) = -(۲/۳) = ۱$$

را به‌دست آوریم. (توجه می‌کنید که $(۲/۳) = -۱$ زیرا ۳ به‌صورت $۸k + ۳$ است.) همچنین با استفاده از (۱۷.۵) نتیجه می‌گیریم که $(۵/۳۱۱) = (۳۱۱/۵) = (۱/۵) = ۱$. از این‌رو، $(۳۰/۳۱۱) = ۱ \times ۱ \times ۱ = ۱$، و لذا همنهشتی مفروض حلپذیر است. در واقع، زیرا $b^۲ - ۴ac \not\equiv ۰ \pmod{۳۱۱}$، مسأله دارای دو جواب است (مسأله ۲.۵ را ببینید).

سرانجام، اگر q یک عدد اول فرد باشد، می‌توان قضیهٔ کلی زیر را برای تعیین تمام اعداد اولی که q ماندهٔ درجهٔ دوم آنهاست به‌کار برد. (مسائل ۴۵.۵ و ۵۳.۵ را ببینید.)

(۲۰.۵) قضیه. فرض کنیم q یک عدد اول فرد باشد. پس اعدادِ اول فرد p که q یک ماندهٔ درجه دوم آنهاست چنین داده می‌شوند:

$$p = ۴qk \pm a,\ \text{که در آن}\ ۰ < a < ۴q\ \text{و}\ a \equiv ۱ \pmod{۴}\ \text{و}\ (a/q) = ۱$$

اعداد صحیح a که در این شرایط صدق می‌کنند فقط کوچکترین مانده‌های مثبت به پیمانهٔ $۴q$ از $۱^۲$، $۳^۲$، $۵^۲$، ...، $(q-۲)^۲$ هستند.

برهان. می‌نویسیم $p = ۴qm + r$، که در آن r فرد و $۰ < r < ۴q$. اگر $r \equiv ۱ \pmod{۴}$، قرار می‌دهیم $k = m$ و $a = r$. اگر $r \equiv ۳ \pmod{۴}$، فرض می‌کنیم $k = m + ۱$ و $a = ۴q - r$. لذا، در هر حالت داریم $p = ۴qk \pm a$، که $۰ < a < ۴q$ و $a \equiv ۱ \pmod{۴}$.

اگر $p \equiv a \pmod{۴q}$، آنگاه $p \equiv ۱ \pmod{۴}$. لذا (۱۷.۵) و (i.۱۰.۵) ایجاب می‌کنند که $(q/p) = (p/q) = (a/q)$. اگر $p \equiv -a \pmod{۴q}$، آنگاه $p \equiv ۳ \pmod{۴}$ و لذا بنابر (ii.۱۰.۵) و (۱۱.۵) داریم $(q/p) = -(p/q) = -(-a/q) = (a/q)$. لذا در هر دو حالت داریم $(q/p) = (a/q)$.

حال فرض کنیم $(a/q) = ۱$؛ لذا یک عدد صحیح s وجود دارد به‌طوری که $s^۲ \equiv a \pmod{q}$. می‌توانیم فرض کنیم که s فرد است (در غیر این‌صورت، از جواب $q - s$ استفاده کنید). چون $a \equiv ۱ \pmod{۴}$، نتیجه می‌شود که $s^۲ \equiv a \pmod{۴}$، و لذا بنابر (ii.۴.۲)، $s^۲ \equiv a \pmod{۴q}$.

مسأله‌ها و راه‌حلها

همنهشتیهای درجه دوم کلی و $x^2 \equiv a \pmod{m}$

۱.۵ $ax^2 + bx + c \equiv 0 \pmod{m}$ را که در آن $(2a, m) = 1$ در نظر می‌گیریم. ثابت کنید که یافتن جوابهای این همنهشتی به یافتن جوابهای همنهشتی $y^2 \equiv d \pmod{m}$ بدل می‌شود.

حل. استدلال اساساً مشابه استدلال (۱.۵) است. همنهشتی مفروض با همنهشتی

$$4a(ax^2 + bx + c) \equiv 0 \pmod{m}$$

هم‌ارز است، زیرا $(2a, m) = 1$ و لذا $(4a, m) = 1$. اما همنهشتی دوم را می‌توان به‌صورت $(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}$ نیز نوشت. لذا برای یافتن تمام جوابها، همنهشتی $y^2 \equiv b^2 - 4ac \pmod{m}$ را حل می‌کنیم، و برای هر جواب y، همنهشتی خطی $2ax \equiv y - b \pmod{m}$ را حل می‌کنیم.

برای معادلهٔ درجهٔ دوم $ax^2 + bx + c = 0$ (که در آن a، b، و c اعداد حقیقی هستند)، فرمول درجهٔ دوم معروف $x = (-b \pm \sqrt{b^2 - 4ac})/2a$ را ارائه می‌دهد. لذا تعداد جوابها ۰، ۱، یا ۲ است برحسب آنکه مقدار $b^2 - 4ac$، که مبین نامیده می‌شود، منفی، صفر، یا مثبت باشد. نتیجهٔ مشابه برای همنهشتیهای درجهٔ دوم برقرار است.

۲.۵ $ax^2 + bx + c \equiv 0 \pmod{p}$ را که در آن p یک عدد اول فرد و $p \nmid a$ در نظر می‌گیریم. قرار می‌دهیم $D = b^2 - 4ac$. ثابت کنید که این همنهشتی، (الف) جواب ندارد هرگاه D یک ناماندهٔ درجهٔ دوم p باشد؛ (ب) یک جواب یکتا دارد اگر $p|D$؛ و (ج) دقیقاً دو جواب دارد اگر D یک ماندهٔ درجهٔ دوم p باشد.

حل. این حکم از (۱.۵) نتیجه می‌شود. (الف) اگر D یک ماندهٔ درجهٔ دوم p نباشد، آنگاه $y^2 \equiv D \pmod{p}$ جوابی ندارد، و لذا دستگاه همنهشتیهای (۱.۵) جواب ندارد. (ب) توجه کنید که $y^2 \equiv 0 \pmod{p}$ جواب یکتای $y = 0$ را دارد، و همنهشتی $2ax \equiv -b \pmod{p}$ یک جواب یکتا دارد. (ج) همنهشتی $y^2 \equiv D \pmod{p}$ دارای دو جواب است. اگر $2ax \equiv y - b \pmod{p}$ را حل کنیم، دو جواب همنهشتی اصلی به‌دست می‌آیند.

۳.۵ فرض می‌کنیم $(a/p) = 1$، که در آن p عددِ اولی به‌صورت $4k + 3$ است. ثابت کنید که جوابهای $x^2 \equiv a \pmod{p}$ با $\pm a^{k+1}$ داده می‌شوند.

حل. چون $(p-1)/2 = 2k+1$، ملاک اویلر ایجاب می‌کند که $a^{2k+1} \equiv 1 \pmod{p}$. لذا $(\pm a^{k+1})^2 = a^{2k+1}a \equiv a \pmod{p}$.

توضیح. می‌توان از این قضیه برای تعیین حلپذیری $x^2 \equiv a \pmod{p}$ استفاده کرد. اگر جوابهایی وجود داشته باشند، بایستی $\pm a^{k+1}$ باشند؛ لذا کافی است بررسی کنیم که این مقادیر جواب هستند یا نیستند. در واقع، می‌توان با استدلال مشابه نشان داد که اگر $\pm a^{k+1}$ جوابهای $x^2 \equiv a \pmod{p}$ نباشند، جوابهای $x^2 \equiv -a \pmod{p}$ هستند.

۴.۵ از مسألهٔ قبل برای یافتن جوابهای (الف) $x^2 \equiv 46 \pmod{59}$؛ (ب) $9x^2 - 24x + 13 \equiv 0 \pmod{59}$ استفاده کنید. (می‌توانید فرض کنید که این همنهشتیها حلپذیرند.)

حل. (الف) بر طبق مسألهٔ قبل، جوابها با $\pm 46^{15}$ یا با هم‌ارز آنها $\mp 13^{15}$ داده می‌شوند. به پیمانهٔ ۵۹ داریم $13^2 \equiv -8$، $13^4 \equiv 5$، $13^8 \equiv 25$، $13^{12} \equiv 5 \times 25 \equiv 7$، $13^{14} \equiv 7(-8) \equiv 3$، و $13^{15} \equiv 39$. لذا جوابها عبارت‌اند از ± 39، یعنی ۲۰ و ۳۹ به پیمانهٔ ۵۹.

(ب) با کامل کردن مربع همانند (۱.۵) داریم

$$(18x - 24)^2 \equiv b^2 - 4ac = 108 \equiv -10 \pmod{59}$$

این همنهشتی حلپذیر است زیرا همنهشتی اصلی حلپذیر است. لذا جوابها از

$$18x - 24 \equiv \pm 10^{15} \pmod{59}$$

به‌دست می‌آیند. امتحان کنید که $\pm 10^{15} \equiv \pm 7 \pmod{59}$. اکنون از حل $18x - 24 \equiv \pm 7 \pmod{59}$، جوابهای ۵ و ۳۷ برای همنهشتی اصلی حاصل می‌شود.

۵.۵ تعیین کنید که آیا همنهشتیهای زیر حلپذیرند؟

(الف) $42x^2 - 51x + 91 \equiv 0 \pmod{311}$؛

(ب) $42x^2 - 51x + 91 \equiv 0 \pmod{622}$.

حل. (الف) با توجه به (۱.۵) کافی است که ببینیم آیا

$$b^2 - 4ac = 51^2 - 4(42)(91) \equiv 64 \pmod{311}$$

یک ماندهٔ درجهٔ دوم است؟ روشن است که $(64/311) = 1$ زیرا $64 = 8^2$، و لذا همنهشتی

مفروض حلپذیر است. (در واقع، بنابر مسألهٔ ۲.۵، دقیقاً دو جواب دارد.)

(ب) برای آنکه این همنهشتی دارای جواب باشد، بایستی به پیمانهٔ ۲ و پیمانهٔ ۳۱۱ دارای جواب باشد. روشن است که جوابی به پیمانهٔ ۲ دارد، زیرا همنهشتی به $x+1 \equiv 0 \pmod 2$ تبدیل می‌شود. بنابر (الف) به پیمانهٔ ۳۱۱ نیز جواب دارد. لذا همنهشتی (ب) جواب دارد.

۶.۵ اثبات یا رد کنید: اگر $x^2 \equiv a \pmod p$ و $x^2 \equiv a \pmod q$ حلپذیر نباشند، آنگاه $x^2 \equiv a \pmod{pq}$ حلپذیر است.

حل. درست نیست. اگر $x^2 \equiv a \pmod{pq}$ حلپذیر باشد، آنگاه $x^2 \equiv a \pmod p$ نیز حلپذیر خواهد بود، زیرا $x^2 \equiv a \pmod{pq}$ ایجاب می‌کند که $x^2 \equiv a \pmod p$.

۷.۵ از (۱.۵) برای تبدیل هر یک از همنهشتیهای زیر به‌صورت $y^2 \equiv d \pmod p$ استفاده کنید: (الف) $11x^2 - 7x + 12 \equiv 0 \pmod{29}$؛ (ب) $5x^2 + 9x - 21 \equiv 0 \pmod{23}$.

حل. در (الف) $(2ax+b)^2 \equiv b^2 - 4ac \pmod p$ به $(22x-7)^2 \equiv 14 \pmod{29}$ بدل می‌شود. در (ب) به‌دست می‌آوریم $18 \equiv (10x+9)^2 \pmod{23}$.

۸.۵ همهٔ جوابهای $x^2 \equiv 8 \pmod{287}$ را به‌دست آورید.

حل. توجه می‌کنید که $287 = 7 \times 41$. همنهشتی $x^2 \equiv 8 \pmod 7$ دارای جوابهای ± 1 است، و همنهشتی $x^2 \equiv 8 \equiv 49 \pmod{41}$ دارای جوابهای ± 7. لذا بنابر قضیهٔ باقیماندهٔ چینی، $x^2 \equiv 8 \pmod{287}$ دارای چهار جواب ± 34 و ± 48 است.

۹.۵ ثابت کنید که همنهشتی $x^2 \equiv 1 \pmod m$ فقط دارای جوابهای ± 1 است اگر و تنها اگر m مساوی ۲، ۴، p^n، یا $2p^n$ باشد، که p عدد فردی است اول.

حل. اگر m مساوی ۲ یا ۴ باشد، آشکار است که تنها جوابهای $x^2 \equiv 1 \pmod m$ عبارت‌اند از ± 1. (توجه می‌کنید که به‌ازای $m = 2$، جوابهای ۱ و -1 همنهشت‌اند.) اگر p یک عدد اول فرد و $m = p^n$ یا $m = 2p^n$، آنگاه قضیه از (۵.۵) به‌دست می‌آید.

بعکس، فرض می‌کنیم که $x^2 \equiv 1 \pmod m$ فقط دارای دو جواب ± 1 است. اگر $m > 2$، فرض می‌کنیم $m = 2^k p_1^{k_1} \cdots p_r^{k_r}$ تجزیهٔ m به عاملهای اول باشد. از (۵.۵) نتیجه می‌شود که، در حالت اول $k = 0$ یا $k = 1$ و $r = 1$، که در این حالت $m = p^n$ یا $m = 2p^n$، حالت دوم $k = 2$ و $r = 0$، در این حالت $m = 4$.

◁ **۱۰.۵** تعمیم گاوس از قضیهٔ ویلسن را ثابت کنید: فرض کنید $m > ۲$، و P حاصلضرب اعداد صحیح مثبت کمتر از m باشد که با m متباین‌اند. پس $P \equiv -۱ (\mathrm{mod}\, m)$ هرگاه m مساوی ۴، p^n، یا $۲p^n$ باشد، که p عدد فردی است اول، و در غیر این‌صورت $P \equiv ۱ (\mathrm{mod}\, m)$. (راهنمایی: با $a = ۱$ از برهان (۲.۳) پیروی کنید، و (۵.۵) را به‌کار برید.)

حل. فرض می‌کنیم $۱ \le x \le m - ۱$، با $(x, m) = ۱$ و $x^۲ \not\equiv ۱ (\mathrm{mod}\, m)$. عدد x را با عدد یکتای y به‌طوری که $۱ \le y \le m - ۱$ و $xy \equiv ۱ (\mathrm{mod}\, m)$ (وارون x) جفت می‌کنیم. آشکار است که حاصلضرب تمام اعدادی که به‌صورت یک جفت در می‌آیند همنهشت با ۱ به پیمانهٔ m است، لذا $P \equiv Q (\mathrm{mod}\, m)$، که Q حاصلضرب تمام اعداد x است به‌طوری که $۱ \le x \le m - ۱$ و $x^۲ \equiv ۱ (\mathrm{mod}\, m)$.

اکنون نوع دیگری از جفت کردن را در نظر می‌گیریم. اگر $x^۲ \equiv ۱ (\mathrm{mod}\, m)$، x را با $m - x$ جفت می‌کنیم. روشن است که، $m - x^۲ \equiv ۱ (\mathrm{mod}\, m)$، $m - x \not\equiv x (\mathrm{mod}\, m)$ و $x(m - x) \equiv -۱ (\mathrm{mod}\, m)$. لذا $Q \equiv (-۱)^{N/۲} (\mathrm{mod}\, m)$، که N تعداد جوابهای همنهشتی $x^۲ \equiv ۱ (\mathrm{mod}\, m)$ است. بنابر (۵.۵)، اگر m مساوی ۴، p^n، یا $۲p^n$، که p عدد اول فردی است، آنگاه $N = ۲$، در این حالت $Q \equiv -۱ (\mathrm{mod}\, m)$. برای هر m دیگر، داریم $Q \equiv ۱ (\mathrm{mod}\, m)$، زیرا N بر ۴ بخشپذیر است.

مانده‌های درجهٔ دوم

۱۱.۵ اگر p عدد اول فردی باشد، ثابت کنید $(۲/p) = (-۱)^{(p^۲-۱)/۸}$.

حل. از (۱۲.۵) استفاده کنید، با این توجه که $(p^۲ - ۱)/۸$ زوج است اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۸)$، و فرد است هرگاه $p \equiv \pm ۳ (\mathrm{mod}\, ۸)$.

۱۲.۵ فرض می‌کنیم a یک ماندهٔ درجهٔ دوم عدد اول فرد p باشد. ثابت کنید $-a$ نیز یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۴)$.

حل. $(-۱/p) = (-۱/p)(a/p) = (-a/p)$، زیرا $(a/p) = ۱$. لذا $-a$ یک ماندهٔ درجهٔ دوم p است اگر و تنها اگر -۱ یک ماندهٔ درجهٔ دوم p باشد، یعنی اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۴)$، بنابر (۱۱.۵).

۱۳.۵ اگر p عدد اول فردی باشد ثابت کنید $(۱/p) + (۲/p) + \cdots + ((p-۱)/p) = ۰$.

حل. بنابر (۷.۵)، $(p-1)/2$ مانده‌های درجهٔ دوم و $(p-1)/2$ نامانده‌ٔ درجهٔ دوم از p وجود دارند. لذا نیمی از جمله‌های این مجموع ۱ هستند و نیم دیگر ۱−.

۱۴.۵ گیریم p یک عدد اولی است فرد، و فرض می‌کنیم q کوچکترین نامانده‌ٔ درجهٔ دومِ مثبتِ p باشد. نشان دهید که q اول است.

حل. بنابر (ii.۱۰.۵) حاصلضرب مانده‌های درجهٔ دوم یک مانده‌ٔ درجهٔ دوم است. لذا اگر $q = ab$ با $1 < a < q$، آنگاه یکی از دو عدد صحیح a و b باید یک نامانده‌ٔ درجهٔ دومِ p باشد. این مطلب با این فرض که q کوچکترین نامانده‌ٔ درجهٔ دومِ p است تناقض دارد.

◁ **۱۵.۵** فرض می‌کنیم p یک عدد اول فرد باشد، و q کوچکترین نامانده‌ٔ درجهٔ دوم مثبتِ p باشد. نشان دهید که $q < \sqrt{p} + 1$. (راهنمایی: نشان دهید که q، $2q$، ...، $(q-1)q$ هر کدام از p کوچکترند.)

حل. فرض کنیم k کوچکترین عدد صحیح مثبتی باشد که $kq > p$، و فرض می‌کنیم r باقیماندهٔ تقسیم kq بر p باشد. چون $(k-1)q < p$، در نتیجه $r < q$، و لذا r (و از این‌رو kq) یک مانده‌ٔ درجهٔ دوم p است. بنابراین $k \geq q$، زیرا اگر $k < q$ آنگاه $k \leq 1$، یک مانده‌ٔ درجهٔ دوم p است، و لذا، بنابر (ii.۱۰.۵)، kq یک نامانده‌ٔ درجهٔ دوم p است. بنابراین $(q-1)q < p$، و در نتیجه $q < \sqrt{p} + 1$، زیرا در غیر این‌صورت، $(q-1)q \geq \sqrt{p}(\sqrt{p}+1) > p$.

◁ **۱۶.۵** فرض کنید p یک عدد اول فرد باشد. ثابت کنید که

$$((1 \times 2)/p) + ((2 \times 3)/p) + \cdots + (((p-2)(p-1))/p) = -1$$

(راهنمایی: ابتدا نشان دهید که $(a(a+1)/p) = ((a^*+1)/p)$، که $aa^* \equiv 1 \pmod{p}$.)

حل. فرض می‌کنیم $(a,p) = 1$، و فرض می‌کنیم a^* چنان باشد که $aa^* \equiv 1 \pmod{p}$. (وجود a^* از (۷.۲) نتیجه می‌شود.) در این‌صورت بنابر (۱۰.۵)،

$$(a(a+1)/p) = (a(a+aa^*)/p) = \left(a^2(1+a^*)/p\right) = ((1+a^*)/p)$$

توجه می‌کنید که وقتی a از ۱ تا $p-2$ تغییر می‌کند، کوچکترین مانده‌ٔ مثبت a^*+1 از ۲ تا $p-1$ تغییر می‌کند. لذا مجموع بالا با $((p-1)/p) + \cdots + (3/p) + (2/p)$ یکی است، که بنابر مسألهٔ قبل برابر است با $-(1/p) = -1$.

◁ **۱۷.۵** فرض می‌کنیم $p > 5$ اول باشد. با استفاده از مسألهٔ قبل ثابت کنید که همواره اعداد صحیح

متوالی وجود دارند که مانده‌های درجهٔ دوم p هستند و اعداد صحیح متوالی که نامانده‌های درجهٔ دوم p هستند.

حل. فرض می‌کنیم که هیچ دو عدد متوالی که مانده‌های درجهٔ دوم p باشند وجود نداشته باشند؛ پس به‌ازای هر a، $(a/p)((a+1)/p) = -1$. لذا به‌ازای هر a،

$$(a(a+1)/p) = (a/p)((a+1)/p) = -1$$

که با توجه به مسألهٔ قبل نمی‌تواند اتفاق بیفتد. استدلال مشابه برای وقتی که فرض کنیم هیچ دو ناماندهٔ درجهٔ دوم متوالی از p وجود ندارد کارساز است، زیرا در این حالت نیز، $(a/p)((a+1)/p) = -1$.

۱۸.۵ فرض می‌کنیم $p > 5$ اول باشد. نشان دهید که حداقل یکی از ۳ عدد صحیح ۲، ۵، یا ۱۰ یک مانده درجهٔ دوم p است. از این مطلب نتیجه بگیرید که همواره اعداد صحیح متوالی وجود دارند که مانده‌های درجهٔ دوم p باشند. سپس نشان دهید که همواره اعداد صحیح متوالی وجود دارند که نامانده درجهٔ دوم p هستند.

حل. اگر ۲ یک ماندهٔ درجهٔ دوم p باشد، ۱ و ۲ مانده‌های درجهٔ دوم متوالی p هستند. همچنین، اگر ۵ یک مانده باشد، ۴ و ۵ مانده‌های متوالی هستند. اگر ۲ و ۵ هر دو مانده‌های درجهٔ دوم p باشند، حاصلضربشان ۱۰ یک ماندهٔ درجهٔ دوم p است، و لذا q و ۱۰ مانده‌های متوالی هستند.

حال نامانده‌های درجهٔ دوم را بررسی می‌کنیم. اگر ۲ و ۳ هر دو نامانده باشند، کار تمام است. در غیر این‌صورت، حداقل سه تا از اعداد صحیح ۱، ۲، ۳، و ۴ مانده هستند. اگر، در بازهٔ $1 \le x \le p-1$، هیچ‌وقت دو نامانده درجهٔ دوم متوالی نداشته باشیم، آنگاه به‌ازای هر چنین xی، تعداد مانده‌ها در بازهٔ از ۱ تا x همواره بیشتر از تعداد نامانده‌ها خواهد بود. اما این ممکن نیست، زیرا دقیقاً همان تعداد مانده در بازهٔ از ۱ تا $p-1$ وجود دارد که نامانده‌اند.

۱۹.۵ کوچکترین مانده‌های مثبتِ مانده‌های درجهٔ دوم ۲۹ را تعیین کنید.

حل. کوچکترین مانده‌های مثبت 1^2، 2^2، 3^2، ...، $((29-1)/2)^2$ به پیمانهٔ ۲۹ را پیدا می‌کنیم. داریم ۱، ۴، ۹، ۱۶، ۲۵، ۷، ۲۰، ۶، ۲۳، ۱۳، ۵، ۲۸، ۲۴، و ۲۲.

۲۰.۵ آیا $x^2 \equiv -2 \pmod{263}$ حلپذیر است؟ (۲۶۳ اول است.)

حل. $-1 = (+1)(-1) = (2/263)(-1/263) = (-2/263)$، زیرا ۲۶۳ به‌صورت $4k+3$ و $8k+7$ است.

◁ **۲۱.۵** فرض می‌کنیم p یک عدد اول فرد باشد. ثابت کنید که حاصلضرب مانده‌های درجهٔ دوم p همنهشت با -۱ یا $+۱$ به پیمانهٔ p است، برحسب آنکه $p \equiv ۱ \pmod ۴$ یا $p \equiv ۳ \pmod ۴$. (راهنمایی: توجه کنید که اگر $ab \equiv ۱ \pmod p$، آنگاه $(a/p) = (b/p)$.)

حل. هر ماندهٔ درجهٔ دوم a غیر از ۱ و -۱ را با وارون ضربیش a^* جفت می‌کنیم، که در آن $aa^* \equiv ۱ \pmod p$. اگر $a \not\equiv \pm ۱ \pmod p$، آنگاه $a^* \not\equiv a \pmod p$. حاصلضرب هر جفت همنهشت با ۱ است. لذا حاصلضرب مانده‌های درجهٔ دوم p همنهشت با -۱ به پیمانهٔ p است اگر -۱ یک ماندهٔ درجهٔ دوم p باشد (یعنی، اگر $p \equiv ۱ \pmod ۴$) و همنهشت با ۱ در غیر این‌صورت.

۲۲.۵ فرض می‌کنیم $p > ۳$ یک عدد اول فرد باشد. ثابت کنید که S مجموع مانده‌های درجهٔ دوم p در بازهٔ $۱ \le x \le p - ۱$ بر p بخشپذیر است. (راهنمایی: فرمول

$$۱^۲ + ۲^۲ + \cdots + n^۲ = n(n+۱)(۲n+۱)/۶$$

را به‌کار برید.)

حل. مانده‌های درجهٔ دوم p با $۱^۲$، $۲^۲$، ...، $((p-۱)/۲)^۲$ همنهشت‌اند؛ از این‌رو $۶S = ((p-۱)/۲)((p+۱)/۲)p \equiv ۰ \pmod p$، و لذا $p|۶S$. چون p نه ۲ است و نه ۳، در نتیجه $p|S$.

۲۳.۵ ثابت کنید که بی‌نهایت عدد اول به‌صورت $۴k+۱$ وجود دارد. (راهنمایی: فرض کنید $p_۱$، $p_۲$، ...، p_n اعدادِ اولِ به این‌صورت باشند، و $N = (۲p_۱p_۲ \cdots p_n)^۲ + ۱$ را در نظر بگیرید.)

حل. فرض می‌کنیم p (لزوماً فرد) یک عامل اول N باشد؛ پس

$$(۲p_۱p_۲ \cdots p_n)^۲ \equiv -۱ \pmod p$$

و لذا بنابر (۱۱.۵)، بایستی p به‌صورت $۴k+۱$ باشد. آشکار است که p یکی از p_iها نیست. لذا به‌ازای هر گردایهٔ متناهی عدد اول به‌صورت $۴k+۱$، می‌توانیم عدد اولی به این‌صورت پیدا کنیم. بنابراین بی‌نهایت عدد اول به‌صورت $۴k+۱$ وجود دارد.

◁ **۲۴.۵** فرض می‌کنیم $p > ۳$ عدد اولی به‌صورت $۴k+۳$ باشد، و N تعداد نامانده‌های درجهٔ دوم p بین ۱ و $p/۲$. ثابت کنید که $((p-۱)/۲)! \equiv (-۱)^N$. (راهنمایی: فرض کنید $P = (p-۱)/۲$! و نشان دهید که $P! \equiv \pm ۱ \pmod p$.)

حل. اگر $P=(p-1)/2$، آشکار است که $(P!/p)=(1/p)(2/p)\cdots(P/p)=(-1)^N$.
بنابر قضیهٔ ویلسن داریم

$$\begin{aligned}-1 \equiv (p-1)! &= 1\times 2\times\cdots\times P(P+1)\cdots(p-2)(p-1)\\ &\equiv 1\times 2\times\cdots\times P(-P)\cdots(-2)(-1)\\ &= (-1)^P(P!)^2 = -(P!)^2 \pmod p\end{aligned}$$

ازاین‌رو $(P!)^2\equiv 1 \pmod p$، ولذا $P!\equiv \pm 1 \pmod p$. بنابر (۱۱.۵)، اگر $P!\equiv 1 \pmod p$، آنگاه $(P!/p)=(1/p)=1$، واگر $P!\equiv -1 \pmod p$، آنگاه $(P!/p)=(-1/p)=-1$.
لذا در هر دو حالت داریم $(P!/p)\equiv P! \pmod p$، و قضیه ثابت می‌شود.

۲۵.۵ تعداد جوابهای همنهشتیهای زیر را به‌دست آورید:

(الف) $x^2\equiv 19 \pmod{170}$؛

(ب) $x^2\equiv 73 \pmod{2^4\times 71^3\times 79^3}$؛

(ج) $x^2\equiv 76 \pmod{165}$؛

(د) $x^2\equiv 38 \pmod{79}$؛

(ه) $x^2\equiv 33 \pmod{2^6\times 37^3\times 83^4}$؛

(و) $x^2\equiv 4 \pmod{11025}$.

حل. (الف) $17\times 5\times 2 = 170$؛ روشن است که $x^2\equiv 19\equiv 1 \pmod 2$ یک جواب دارد. همچنین، $(19/5)=(4/5)=1$، لذا $x^2\equiv 19 \pmod 5$ دو جواب دارد. و بنابر (۱۲.۵)، $(19/17)=(2/17)=1$، لذا $x^2\equiv 19 \pmod{17}$ دو جواب دارد. از این‌رو، بنابر (۳.۴) (یا با استفاده از (۵.۵)، همنهشتی اصلی دارای $1\times 2\times 2 = 4$ جواب است.

(ب) بنابر (۱۲.۵)، $(73/71)=(2/71)=-1$. لذا جوابی به پیمانهٔ ۷۱ وجود ندارد، و از این‌رو همنهشتی مفروض حلپذیر نیست.

(ج) داریم $3\times 5\times 11 = 165$؛ پس بنابر (۱۱.۵) داریم $(76/3)=(1/3)=1$، $(76/5)=1$، و $(76/11)=(-1/11)=-1$. لذا به پیمانهٔ ۱۱ و از این‌رو به پیمانهٔ ۱۶۵ جواب وجود ندارد.

(د) با استفاده از لم گاوس،

$$(38/79)=(2/79)(19/79)=-(79/19)=-(3/19)=1$$

لذا دو جواب وجود دارد.

(ه) بنابر (۱۱.۵) داریم

$$(۳۳/۳۷) = (-۴/۳۷) = (-۱/۳۷)(۴/۳۷) = (-۱/۳۷) = ۱$$

ازاین‌رو، دو جواب به پیمانهٔ ۳۷ ولذا بنابر (۳.۵)، به‌ازای هر $k \geq ۱$، دو جواب به پیمانهٔ ۳۷^k وجود دارد. همچنین، بنابر (۱۲.۵)، $(۳۳/۸۳) = (-۵۰/۸۳) = (-۲/۸۳)(۲۵/۸۳) = (-۲/۸۳) = ۱$. لذا دو جواب به پیمانهٔ $۸۳^۴$ وجود دارد. از آنجا که بنابر (۱۴.۴)، $x^۲ \equiv ۳۳ (\mathrm{mod}\, ۶۴)$ حلپذیر است، (۵.۵) ایجاب می‌کند که همنهشتی اصلی $۱۶ = ۲^{۲+۲}$ جواب داشته باشد.

(و) توجه کنید که $۱۱۰۲۵ = ۳^۲ \, ۵^۲ \, ۷^۲$. چون ۴ یک مربع کامل است، یک جواب وجود دارد. لذا بنابر (۵.۵)، $۸ = ۲^۳$ جواب به پیمانهٔ ۱۱۰۲۵ وجود دارد.

۲۶.۵ تعداد جوابهای $x^۴ \equiv ۴ (\mathrm{mod}\, ۷۱^۳ \times ۹۷^۵)$ را به‌دست آورید.

حل. همنهشتی مفروض را به $x^۲ \equiv \pm ۲$ به پیمانهٔ $۷۱^۳$ و $۹۷^۵$ تبدیل می‌کنیم. توجه می‌کنید که بنابر (۱۲.۵)، $x^۲ \equiv ۲ (\mathrm{mod}\, ۷۱)$ دو جواب دارد؛ لذا از (۳.۵) نتیجه می‌شود که $x^۲ \equiv ۲ (\mathrm{mod}\, ۷۱^۳)$ دو جواب دارد. همچنین، $x^۲ \equiv -۲ (\mathrm{mod}\, ۷۱)$ جواب ندارد، زیرا بنابر (۱۱.۵) و (۱۲.۵)، $(-۲/۷۱) = (-۱/۷۱)(۲/۷۱) = (-۱)(+۱) = -۱$. لذا $x^۴ \equiv ۴ (\mathrm{mod}\, ۷۱^۳)$ دقیقاً دو جواب دارد.

به همین ترتیب، $(۲/۹۷) = ۱$ و $(-۲/۹۷) = ۱$؛ لذا $x^۴ \equiv ۴ (\mathrm{mod}\, ۹۷)$ چهار جواب دارد، و بنابراین چهار جواب به پیمانهٔ $۹۷^۵$ وجود دارد. ((۳.۵) را در مورد $x^۲ \equiv ۲ (\mathrm{mod}\, ۹۷^۵)$ و $x^۲ \equiv -۲ (\mathrm{mod}\, ۹۷^۵)$ به‌کار برید.) لذا $۸ = ۴ \times ۲$ جواب به پیمانهٔ $۹۷^۵ \times ۷۱^۳$ وجود دارد.

۲۷.۵ اگر p عدد اولی به‌صورت $۴k+۱$ باشد، نشان دهید $(۱/p)+(۲/p)+\cdots+(P/p) = ۰$، که در آن $P = (p-۱)/۲$. (راهنمایی: توجه کنید $(a/p) = ((p-a)/p)$ و مسألهٔ ۱۳.۵ را به‌کار برید.)

حل. بنابر (۱۱.۵)، $((p-a)/p) = (-a/p) = (-۱/p)(a/p)$. از مسألهٔ ۱۳.۵ نتیجه می‌شود که $(۱/p)+(۲/p)+\cdots+((p-۱)/p) = ۲[(۱/p)+(۲/p)+\cdots+(P/p)] = ۰$، که قضیه را ثابت می‌کند.

۲۸.۵ فرض می‌کنیم n عدد صحیح مثبتی به‌صورت $۴k+۳$ باشد. اگر $q = ۲n+۱$ اول باشد، ثابت کنید $q | ۲^n - ۱$.

حل. بنابر ملاک اویلر، $(2/q) \equiv 2^{(q-1)/2} = 2^n \pmod q$. چون $q = 2n+1$ و n به‌صورت $4k+3$ است، لذا q به‌صورت $8k+7$ است و بنابر (۱۲.۵)، $(2/q) = 1$. لذا $2^n \equiv 1 \pmod q$، یعنی $q \mid 2^n - 1$.

۲۹.۵ آیا ۸۳ عدد $2^{41} - 1$ را می‌شمارد؟ (راهنمایی: ملاک اویلر را به‌کار برید.)

حل. توجه کنید که $(83-1)/2 = 41$. بنابر ملاک اویلر، $(2/83) \equiv 2^{41} \pmod{83}$. اما بنابر (۱۲.۵)، $(2/83) = -1$، لذا $2^{41} \equiv -1 \pmod{83}$، یعنی $83 \mid 2^{41} + 1$، و لذا ۸۳ عدد $2^{41} - 1$ را نمی‌شمارد.

۳۰.۵ ملاک اویلر را برای بررسی شمارش‌پذیری $2^{999} - 1$ بر عدد اول ۱۹۹۹ به‌کار برید.

حل. توجه می‌کنید که $1999 \equiv 7 \pmod 8$، لذا بنابر (۱۲.۵)، $(2/1999) = 1$. از این‌رو بنابر ملاک اویلر، $2^{999} \equiv (2/1999) = 1 \pmod{1999}$، و لذا $1999 \mid 2^{999} - 1$.

۳۱.۵ فرض می‌کنیم q فرد باشد و $p = 4q+1$ اول،
(الف) ثابت کنید که ۲ یک نامانده‌ٔ درجهٔ دوم p است
(ب) ثابت کنید که $p \mid 4^q + 1$. (از ملاک اویلر استفاده کنید.)

حل. (الف) فرض می‌کنیم $q = 2k+1$. پس $p = 4q+1 = 8k+5$؛ حال از (۱۲.۵) استفاده کنید.

(ب) بنابر ملاک اویلر، $(2/p) \equiv 2^{(p-1)/2} = 2^{2q} = 4^q \pmod p$. بنابر (الف)، $(2/p) = -1$، لذا $4^q \equiv -1 \pmod p$، یعنی $p \mid 4^q + 1$.

۳۲.۵ فرض می‌کنیم p یک عدد اول به‌صورت $8k+5$ باشد، و همنهشتی $x^2 \equiv a \pmod p$ دارای جواب باشد. ثابت کنید که یکی از اعداد صحیح a^{k+1} یا $2^{2k+1}a^{k+1}$ جواب است. (از ملاک اویلر و (۱۲.۵) استفاده کنید.)

حل. بنابر ملاک اویلر، $a^{4k+2} \equiv 1 \pmod p$، ولذا $a^{2k+1} \equiv \pm 1 \pmod p$. اگر $a^{2k+1} \equiv 1$، آنگاه $a^{2k+2} \equiv a \pmod p$ و a با مربع a^{k+1} همنهشت به پیمانهٔ p است. حال فرض می‌کنیم $a^{2k+1} \equiv -1 \pmod p$. چون p به‌صورت $8k+5$ است، ۲ یک نامانده‌ٔ درجهٔ دوم p است، و لذا $2^{4k+2} \equiv -1 \pmod p$. نتیجه می‌شود که $2^{4k+2}a^{2k+1} \equiv 1 \pmod p$، و لذا

$(\mathrm{mod}\, p) \equiv a^{2k+2}2^{4k+2}$. بنابراین، در این حالت a با مربع $2^{2k+1}a^{k+1}$ همنهشت به پیمانهٔ p است.

۳۳.۵ فرض می‌کنیم p یک عدد اول فرد باشد. تعداد مانده‌های درجهٔ دوم p^n را پیدا کنید.

حل. مانده‌های درجهٔ دوم p^n متشکل از مربع اعداد بین ۱ و p^n است که نسبت به p اول‌اند. اما، اگر همنهشتی $x^2 \equiv a(\mathrm{mod}\, p^n)$ حلپذیر باشد، بنابر (۳.۵) دقیقاً دو جواب دارد، و لذا $\phi(p^n)/2 = p^{n-1}(p-1)/2$ ماندهٔ درجهٔ دوم از p^n وجود دارد.

۳۴.۵ فرض می‌کنیم $m = 2^k p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. تعداد مانده‌های درجهٔ دوم m را پیدا کنید. (راهنمایی: مسألهٔ قبل را ببینید.)

حل. اگر $\phi(m)$ عددِ از ۱ تا m را که با m متباین‌اند مربع کنیم، مانده‌های درجهٔ دوم m را به‌دست می‌آوریم. اما اگر $x^2 \equiv a(\mathrm{mod}\, m)$ حلپذیر باشد، تعداد جوابها به‌وسیلهٔ (۵.۵) ارائه شده است و بستگی به a ندارد. لذا تعداد مانده‌های درجهٔ دوم m به‌ترتیب مساوی $\phi(m)/2^r$، $\phi(m)/2^{r+1}$، و $\phi(m)/2^{r+2}$ است وقتی که $k = 0$ یا $k = 1$، $k = 2$، و $k \geq 3$.

۳۵.۵ ثابت کنید که ۳ یک نامانده‌ٔ درجهٔ دوم برای تمام اعداد اول به‌صورت $4^n + 1$ است.

حل. فرض کنیم $p = 4^n + 1$. چون $4 \equiv 1(\mathrm{mod}\, 3)$، داریم $p \equiv 2(\mathrm{mod}\, 3)$؛ همچنین، $p \equiv 1(\mathrm{mod}\, 4)$. لذا، بنابر قانون تقابل مربعی، $(3/p) = (p/3) = (2/3) = -1$.

۳۶.۵ آیا مربعی به‌صورت $55k - 1$ وجود دارد؟ توضیح دهید.

حل. اگر $55k - 1 = n^2$، آنگاه n^2 همنهشت با -1 به پیمانهٔ ۵۵ و لذا به پیمانهٔ ۱۱ است. این ممکن نیست، زیرا ۱۱ به‌صورت $4k + 1$ نیست ((۱۱.۵) را ببینید).

۳۷.۵ فرض می‌کنیم a مضرب ۷۱ نباشد. نشان دهید که همنهشتیهای $x^{26} \equiv a(\mathrm{mod}\, 71)$ و $x^{26} \equiv -a(\mathrm{mod}\, 71)$ هر دو حلپذیر نیستند.

حل. اگر این همنهشتیها حلپذیر باشند، آنگاه a و $-a$ هر دو مانده‌های درجهٔ دوم p هستند. اما، بنابر (۱۱.۵)، $(a/71) = -(a/71)$، $(-a/71) = (-1/71)(a/71)$، و لذا دقیقاً یکی از دو عدد صحیح a و $-a$ ماندهٔ درجهٔ دوم p است.

۳۸.۵ فرض می‌کنیم p اول باشد. ثابت کنید $(n^۲-۳)(n^۲-۵)(n^۲-۱۵)$ به‌ازای بی‌نهایت مقدار صحیح m، بر p بخشپذیر است.

حل. اگر $p=۲$، آنگاه n می‌تواند هر عدد صحیح فردی باشد؛ اگر $p=۳$ یا $p=۵$، آنگاه m می‌تواند هر مضرب ۱۵ باشد. لذا فرض می‌کنیم $p>۵$. اگر ۳ یا ۵ یک ماندهٔ درجهٔ دوم p باشد، آنگاه مقداری از n وجود دارد به‌طوری که $p|n^۲-۳$ یا $p|n^۲-۵$. اگر هیچ‌کدام از دو عدد ۳ و ۵ ماندهٔ درجهٔ دوم p نباشند، آنگاه $(۱۵/p)=(۳/p)(۵/p)=(-۱)(-۱)=۱$، لذا مقداری از n وجود دارد که $p|n^۲-۱۵$. بنابراین، در هر حالت، مقداری از n وجود دارد به‌طوری که p حاصلضرب مفروض را بشمارد. برای اینکه نشان دهیم بی‌نهایت n با این ویژگی وجود دارد، ملاحظه می‌کنید که، مثلاً اگر $n^۲\equiv ۳(\bmod p)$، آنگاه به‌ازای هر $k\geq ۱$، $(n+kp)^۲\equiv ۳(\bmod p)$.

◁ **۳۹.۵** فرض می‌کنیم $p\geq ۷$ عدد اولی به‌صورت $۴k+۳$ باشد. نشان دهید که مجموع مربعات مانده‌های درجهٔ دوم p (نامانده‌های درجهٔ دوم p) مضربی از p است. (راهنمایی: مسألهٔ ۲۲.۵ را به‌کار برید.)

حل. اگر a و b مانده‌ها (یا نامانده‌ها)ی درجهٔ دوم ناهمنهشتِ با p باشند، آنگاه $a^۲\not\equiv b^۲(\bmod p)$. زیرا اگر $a^۲\equiv b^۲(\bmod p)$ و $a\not\equiv b(\bmod p)$، آنگاه $a\equiv -b(\bmod p)$. اما در این‌صورت $(a/p)=(-b/p)=(-۱/p)(b/p)=-(b/p)$، و لذا a و b هر دو نمی‌توانند مانده (یا نامانده)های درجهٔ دومِ p باشند.

بنابر (۷.۵)، $(p-۱)/۲$ ماندهٔ درجهٔ دوم و $(p-۱)/۲$ نامانده وجود دارند. لذا مربعات مانده‌ها (یا نامانده‌ها) مجموعهٔ کاملی از $(p-۱)/۲$ مانده‌های درجهٔ دوم ناهمنهشت تشکیل می‌دهند، و قضیه اکنون از مسألهٔ ۲۲.۵ نتیجه می‌شود.

۴۰.۵ فرض می‌کنیم p عدد اولی است به‌صورت $۸k+۳$. آیا $p|۲^{(p-۱)/۲}-۱$؟

حل. نه. اگر $p|۲^{(p-۱)/۲}-۱$، آنگاه $۲^{(p-۱)/۲}\equiv ۱(\bmod p)$، و لذا بنابر ملاک اویلر داریم $(۲/p)=۱$. در صورتی‌که بنابر (۱۲.۵)، $(۲/p)=-۱$.

۴۱.۵ (الف) فرض کنیم p عدد اول فردی باشد که $r^۲+s^۲$ را می‌شمارد، و $(r,p)=(s,p)=۱$. ثابت کنید p به‌صورت $۴k+۱$ است.

(ب) اگر $n|r^۲+s^۲$، که $(r,n)=(s,n)=۱$، آنگاه n حاصلضرب، یا در برابر حاصلضرب توانهای اعداد اولی است که هر یک به‌صورت $۴k+۱$ است.

حل. (الف) اگر $p|r^۲+s^۲$، آنگاه $r^۲ \equiv -s^۲ (\mathrm{mod}\, p)$ و لذا

$$۱ = (r^۲/p) = (-s^۲/p) = (-۱/p)(s^۲/p) = (-۱/p)$$

از این‌رو بنابر (۱۱.۵)، p به‌صورت $۴k+۱$ است.

(ب) فرض می‌کنیم $n|r^۲+s^۲$ و p عدد اول فردی باشد که n را می‌شمارد. لذا بنابر (الف)، $p \equiv ۱ (\mathrm{mod}\, ۴)$. همچنین، اگر n زوج باشد، آنگاه n فقط یک عامل ۲ می‌تواند داشته باشد، زیرا اگر n زوج باشد، با توجه به فرض $(r,n) = (s,n) = ۱$، بایستی r و s هر دو فرد باشند، در این حالت $r^۲ + s^۲ \equiv ۲ (\mathrm{mod}\, ۴)$ و لذا $۴ \nmid r^۲ + s^۲$. بنابراین n به‌صورت $\prod p_i^{r_i}$ یا $۲\prod p_i^{r_i}$ است، که هر p_i عدد اولی است به‌صورت $۴k+۱$.

۴۲.۵ اگر $n > ۳$، ثابت کنید که $۱! + ۲! + \cdots + n!$ هرگز مربع نیست.

حل. فرض کنیم $N = ۱! + ۲! + \cdots + n!$. پس

$$N \equiv ۱! + ۲! + ۳! + ۴! = ۳۳ \equiv ۳ (\mathrm{mod}\, ۵)$$

لذا اگر $N = m^۲$، آنگاه $m^۲ \equiv ۳ (\mathrm{mod}\, ۵)$. اما به آسانی دیده می‌شود که ۳ یک نامانده درجهٔ دوم ۵ است.

قانون تقابل مربعی

۴۳.۵ فرض کنیم p و q اعداد اول فرد متمایز باشند. نشان دهید که می‌توان قانون تقابل مربعی را به‌صورت زیر بیان کرد: اگر p به‌صورت $۴k+۱$ باشد، آنگاه $(p/q) = (q/p)$. اگر p به‌صورت $۴k+۳$ باشد، آنگاه $(p/q) = (q/p)$. (این بیان اساساً همان بیان اصلی گاوس است.)

حل. وقتی k به‌صورت $۴k+۱$ باشد، روشن است که گفتهٔ گاوس و (۱۷.۵) یک قضیه را می‌دهند. حال فرض کنیم p به‌صورت $۴k+۳$ باشد. ملاحظه می‌کنید که $(-p/q) = (-۱/q)(p/q)$. اگر q به‌صورت $۴k+۱$ باشد، آنگاه $(-۱/q) = ۱$، و گفتهٔ گاوس با (۱۷.۵) مطابقت دارد، سرانجام، فرض کنیم q به‌صورت $۴k+۳$ باشد. پس $(-۱/q) = -۱$، لذا گفتهٔ گاوس ایجاب می‌کند که $(q/p) = -(p/q)$، که همان قضیهٔ (۱۷.۵) است.

۴۴.۵ با استفادهٔ مستقیم از لم گاوس نشان دهید که ۲ یک ماندهٔ درجهٔ دوم عدد اول p است اگر p به‌صورت $۸k+۱$ یا $۸k+۷$ باشد، و یک نامانده درجهٔ دوم p است هرگاه p به‌صورت $۸k+۳$ یا $۸k+۵$ باشد.

حل. اگر $1 \le j \le (p-1)/2$، آنگاه $2 \le 2j \le p-1$. فرض کنیم N تعداد اعداد صحیح در مجموعهٔ $A = \{2, 4, 6, \ldots, p-1\}$ باشد که از $p/2$ بزرگترند. در این‌صورت بنابر لم گاوس، $(2/p) = (-1)^N$. اما $2j > p/2$ اگر و تنها اگر $j > p/4$. اگر $p = 8k+1$، آنگاه $j > p/4$ که هم‌ارز است با $j > 2k + 1/4$. $2k$ عدد صحیح وجود دارند که در نابرابری آخر صدق می‌کنند؛ از آنجا که A دارای $(p-1)/2 = 4k$ عنصر است، نتیجه می‌شود که $N = 4k - 2k = 2k$. لذا اگر $p = 8k+1$، آنگاه $(2/p) = 1$.

با استدلالی مشابه، اگر p به‌صورت $8k+3$، $8k+5$، یا $8k+7$ باشد، آنگاه N به‌ترتیب، برابر است با $2k+1$، $(4k+1) - 2k = 2k+1$، یا $(4k+2) - (2k+1) = 2k+1$. لذا از لم گاوس نتیجه می‌شود که $(2/p) = 1$ یا $(2/p) = -1$ برحسب آنکه $p \equiv 1, 7 \pmod 8$ یا $p \equiv 3, 5 \pmod 8$.

۴۵.۵ اعداد اول $p \neq 7$ را تعیین کنید به‌طوری که $x^2 \equiv 7 \pmod p$ حلپذیر باشد.

حل. از (۲۰.۵) استفاده می‌کنیم. پس $p = 28k \pm a$، که a روی کوچکترین مانده‌های مثبت 1^2، 3^2، ...، $(2-7)^2$، یعنی ۱، ۹، و ۲۵ به پیمانهٔ ۲۸ تغییر می‌کند. لذا $(7/p) = 1$ اگر و تنها اگر $a = 28k \pm 1, 28k \pm 3, 28k \pm 9$. (توجه کنید که $\pm 25 \equiv \mp 3 \pmod{28}$.)

برهان دیگر: ابتدا اعداد اول به‌صورت $4k+1$ را بررسی می‌کنیم. در این‌صورت، بنابر قانون تقابل مربعی، $(7/p) = (p/7)$. اما این همان $(r/7)$ است، که r باقیماندهٔ تقسیم p بر ۷ است، و به‌راحتی دیده می‌شود که به‌ازای مقادیر ۱، ۲، و ۴ از r، $(r/7) = 1$. لذا p به‌صورت $28k+1$، $28k+9$، یا $28k+25$ است.

سپس به اعداد اول که به‌صورت $4k+3$ می‌پردازیم. بنابر قانون تقابل مربعی، $(7/p) = -(r/7)$، که r باقیماندهٔ تقسیم p بر ۷ است. لذا $(7/p) = 1$ اگر و تنها اگر $(r/7) = -1$، یعنی، اگر و تنها اگر r مساوی ۳، ۵، یا ۶ باشد. لذا بایستی p به‌صورت $28k+3$، $28k+19$، یا $28k+27$ باشد.

۴۶.۵ کمیّات زیر را حساب کنید: (الف) $(97/70)$؛ (ب) $(-14/83)$؛ (ج) $(331/263)$؛ (د) $(-383/219)$؛ (ه) $(773/461)$، (263، 331، 383، و 773 اعداد اول‌اند.)

حل. از (۱۰.۵)ـ(۱۲.۵)، و قانون تقابل مربعی استفاده می‌کنیم.

(الف) $(97/70) = (97/2)(97/5)(97/7)$. توجه کنید که $(97/2) = 1$ زیرا $97 \equiv 1 \pmod 8$. همچنین، $(97/5) = (2/5) = -1$، و

$$(۷/۹۷) = (۹۷/۷) = (-۱/۷) = -۱$$

لذا $(۷۰/۹۷) = ۱$.

(ب)

$$(-۱۴/۸۳) = (-۱/۸۳)(۲/۸۳)(۷/۸۳) = (-۱)(-۱)(۷/۸۳)$$
$$= (۷/۸۳) = -(۸۳/۷) = -(-۱/۷) = ۱$$

(ج)

$$(۲۶۳/۳۳۱) = -(۳۳۱/۲۶۳) = -(۶۸/۲۶۳)$$
$$= -(۴/۲۶۳)(۱۷/۲۶۳) = -(۱۷/۲۶۳) = -(۲۶۳/۱۷)$$
$$= -(۸/۱۷) = -(۲/۱۷) = -۱$$

(د)

$$(-۲۱۹/۳۸۳) = (۱۶۴/۳۸۳) = (۴/۳۸۳)(۴۱/۳۸۳)$$
$$= (۴۱/۳۸۳) = (۳۸۳/۴۱) = (۱۴/۴۱) = (۲/۴۱)(۷/۴۱) = (۷/۴۱)$$
$$= (۴۱/۷) = (۶/۷) = (-۱/۷) = -۱$$

(ه)

$$(۴۶۱/۷۷۳) = (۷۷۳/۴۶۱) = (۳۱۲/۴۶۱) = (۴/۴۶۱)(۲/۴۶۱)(۳/۴۶۱)(۱۳/۴۶۱)$$
$$= (+۱)(-۱)(۴۶۱/۳)(۴۶۱/۱۳) = (۶/۱۳) = (۲/۱۳)(۳/۱۳)$$
$$= -(۳/۱۳) = -(۱۳/۳) = -(۱/۳) = -۱$$

۴۷.۵ ثابت کنید که ۱۰ یک ماندهٔ درجهٔ دوم عدد اول فرد p است اگر و تنها اگر $p \equiv \pm ۱, \pm ۳, \pm q, \pm ۱۳ (\mathrm{mod}\ ۴۰)$.

حل. $(۱۰/p) = ۱$ اگر و تنها اگر $(۵/p) = (۲/p) = ۱$ یا $(۵/p) = (۲/p) = -۱$. بنابر (۱۲.۵) و (iv.۱۳.۵)، حالت اول برقرار است اگر و تنها اگر $p \equiv \pm ۱ (\mathrm{mod}\ ۸)$ و $p \equiv \pm ۱ (\mathrm{mod}\ ۵)$؛ لذا بنابر قضیهٔ باقیماندهٔ چینی $p \equiv \pm ۱, \pm ۹ (\mathrm{mod}\ ۴۰)$. حالت دوم برقرار است اگر و تنها اگر $p \equiv \pm ۳ (\mathrm{mod}\ ۸)$ و $p \equiv \pm ۲ (\mathrm{mod}\ ۵)$؛ لذا $p \equiv \pm ۳, \pm ۱۳ (\mathrm{mod}\ ۴۰)$.

۴۸.۵ ثابت کنید که بی‌نهایت عدد اول وجود دارد که به رقم ۹ ختم می‌شوند. (راهنمایی: ابتدا با ملاحظهٔ $N = ۵(n!)^۲ - ۱$ که $n > ۱$ و استفاده از (۱۳.۵)، نشان دهید که بی‌نهایت عدد اول به‌صورت $۱۰k - ۱$ وجود دارد.)

حل. فرض کنیم p یک مقسوم‌علیه اول N باشد؛ توجه کنید که p فرد است. پس $۵(n!)^۲ \equiv ۱$، و لذا، بنابر (۱۰.۵)، $(۵/p) = (۵(n!)^۲/p) = ۱$. لذا بنابر (۱۳.۵)، p به‌صورت $۵k - ۱$ یا $۵k - ۱$ است. ولی، اگر تمام مقسوم‌علیه‌های اول N به‌صورت $۵k + ۱$ باشند، N نیز به‌صورت $۵k + ۱$ خواهد بود. اما روشن است که N به‌صورت $۵k + ۱$ است، لذا بایستی N حداقل یک مقسوم‌علیه اول به‌صورت $۵k - ۱$ داشته باشد؛ در واقع، p به‌صورت $۱۰k - ۱$ است، زیرا $۱۰k + ۴$ نمی‌تواند اول باشد. توجه کنید که $p > n$ (زیرا اگر $p \le n$، آنگاه $p|n!$ و $p|N$، لذا $p|۱$، که یک تناقض است). بنابراین نشان داده‌ایم که به‌ازای هر عدد صحیح مثبت n، عدد اولی بزرگتر از n و به‌صورت $۱۰k - ۱$ وجود دارد. لذا بی‌نهایت عدد اول به‌صورت $۱۰k - ۱$ وجود دارد، که همهٔ آنها به رقم ۹ ختم می‌شوند.

۴۹.۵ قسمت (i) از قضیهٔ ۱۳.۵ را ثابت کنید: ۲ – یک ماندهٔ مربعی عدد اول فرد p است اگر و تنها اگر p به‌صورت $۸k + ۱$ یا $۸k + ۳$ باشد.

حل. $(-۲/p) = ۱$ اگر و تنها اگر $(۲/p) = (-۱/p)$ یا $(۲/p) = (-۱/p) = -۱$. بنابر (۱۱.۵) و (۱۲.۵)، حالت اول دقیقاً وقتی برقرار است که $p \equiv ۱ \pmod ۴$ و $p \equiv \pm ۱ \pmod ۸$؛ لذا برقرار است اگر و تنها اگر $p \equiv ۱ \pmod ۸$. حالت دوم برقرار است اگر و تنها اگر $p \equiv ۳ \pmod ۴$ و $p \equiv \pm ۳ \pmod ۸$، یعنی $p \equiv ۳ \pmod ۸$.

۵۰.۵ ثابت کنید که بی‌نهایت عدد اول به‌صورت (الف) $۸k + ۳$؛ (ب) $۸k + ۵$؛ (ج) $۸k + ۷$ وجود دارد. (راهنمایی: فرض کنید $p_۱$، $p_۲$، ...، p_n اعداد اول به‌صورت مفروض باشند. در (الف)، $N = (p_۱p_۲ \cdots p_n)^۲ + ۲$؛ در (ب)، $N = (p_۱p_۲ \cdots p_n)^۲ + ۴$؛ و در (ج) $N = (p_۱p_۲ \cdots p_n)^۲ - ۲$ را در نظر بگیرید.)

حل. در هر حالت، فرض می‌کنیم p یک مقسوم‌علیه اول N باشد.

(الف) چون $(p_۱p_۲ \cdots p_n)^۲ \equiv -۲ \pmod p$، داریم $(-۲/p) = ۱$. لذا بنابر (i.۱۳.۵)، p به‌صورت $۸k + ۱$ یا $۸k + ۳$ است. اگر هر مقسوم‌علیه اول N به‌صورت $۸k + ۱$ باشد، N نیز به همین صورت خواهد بود؛ اما روشن است که، $N \equiv ۳ \pmod ۸$ زیرا هر p_i در $p_i^۲ \equiv ۱ \pmod ۸$ صدق می‌کند. لذا N حداقل یک مقسوم‌علیه اول به‌صورت $۸k + ۳$

دارد، که نمی‌تواند یکی از p_iها باشد (در غیر این‌صورت $p \mid ۲$، که یک تناقض است زیرا N فرد است.)

(ب) توجه کنید که $N \equiv ۵ (\mathrm{mod}\, ۸)$، زیرا به‌ازای هر i، $p_i^۲ \equiv ۱ (\mathrm{mod}\, ۸)$. همچنین، $(p_۱p_۲\cdots p_n)^۲ \equiv -۴ (\mathrm{mod}\, p)$؛ از این‌رو $(-۴/p) = ۱$ و لذا $(-۱/p) = ۱$. پس بنابر (۱۱.۵)، p به‌صورت $۴k+۱$ و لذا $۸k+۱$ یا $۸k+۵$ است. بنابراین N حداقل دارای یک مقسوم‌علیه اول p به‌صورت $۸k+۵$ است که با تمام p_iها متفاوت است.

(ج) چون $(p_۱p_۲\cdots p_n)^۲ \equiv ۲ (\mathrm{mod}\, p)$، ۲ یک ماندهٔ درجهٔ دوم p است و لذا بنابر (۱۲.۵)، $p \equiv \pm ۱ (\mathrm{mod}\, ۸)$. اگر هر عامل اول N به‌صورت $۸k+۱$ باشد، N نیز به‌صورت $۲k+۱$ خواهد بود، که چنین نیست. (در واقع، N به‌صورت $۸k-۱$ است.) لذا حداقل یکی از عاملهای اول p به‌صورت $۸k-۱$ است، روشن است که، p یکی از p_iها نیست.

توضیح. حالت $۸k+۱$ تکنیک متفاوتی لازم دارد و در فصل بعد بررسی خواهد شد. (مسأله ۲۳.۶ را ببینید.)

۵۱.۵ با استفاده از (۲۰.۵) نشان دهید که ۳ یک ماندهٔ درجهٔ دوم عدد اول فرد p است اگر و تنها اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۱۲)$. (این مطلب، اثبات قسمت (ii) از (۱۳.۵) است.)

حل. بنابر (۲۰.۵)، p به‌صورت $۴ \times ۳k \pm a$ است، که در آن a روی کوچکترین مانده‌های مثبت $۱^۲$، $۳^۲$، ...، $(q-۲)^۲$ به پیمانهٔ ۱۲ تغییر می‌کند؛ در اینجا $q = ۳$، لذا $a = ۱$. بنابراین $(۳/p) = ۱$ اگر و تنها اگر $p = ۱۲k \pm ۱$.

۵۲.۵ اثبات قسمت (iii) از قضیهٔ ۱۳.۵؛ ۳− یک ماندهٔ درجهٔ دوم عدد اول فرد p است اگر و تنها اگر p به‌صورت $۶k+۱$ باشد.

حل. توجه کنید که $(-۳/p) = ۱$ اگر و تنها اگر (i) $(۳/p) = (-۱/p) = ۱$ یا (ii) $(۳/p) = (-۱/p) = ۱$. بنابر (ii.۱۳.۵)، شرط (i) برقرار است اگر و تنها اگر p به‌صورت $۴k+۱$ و نیز به‌صورت $۱۲k \pm ۱$ باشد، یعنی p به‌صورت $۱۲k+۱$ باشد. همچنین، (ii) برقرار است اگر و تنها اگر p به‌صورت $۴k+۳$ و $۱۲k \pm ۵$، یعنی، p به‌صورت $۱۲k+۷$ باشد. چون p به‌صورت $۶k+۱$ است اگر و تنها اگر به‌صورت $۱۲k+۱$ یا $۱۲k+۷$ باشد، قضیه نتیجه می‌شود.

۵۳.۵ قسمت (iv) از قضیهٔ ۱۳.۵ را ثابت کنید: ۵ یک ماندهٔ درجهٔ دوم عدد اول فرد p است اگر و تنها اگر $p \equiv \pm ۱ (\mathrm{mod}\, ۵)$.

حل. می‌توانیم با کاربرد (۲۰.۵) یا با استفاده از قانون تقابل مربعی نتیجه بگیریم که $(5/p) = (p/5)$. اگر $p = 5k + r$، آنگاه $(p/5) = (r/5)$. لذا $(5/p) = 1$ اگر و تنها اگر $(r/5) = 1$. چون تنها مانده‌های درجهٔ دوم ۵ عبارت‌اند از ۱ و ۴، بایستی p به‌صورت $5k + 1$ یا $5k + 4$، یعنی $5k \pm 1$ باشد.

۵۴.۵ ثابت کنید که بی‌نهایت عدد اول به‌صورت $6k + 1$ و بنابراین بی‌نهایت عدد اول به‌صورت $3k + 1$ وجود دارد. (راهنمایی: فرض کنید p_1، p_2، ...، p_n اعداد اول به‌صورت $6k + 1$ باشند، و $N = (p_1 p_2 \cdots p_n)^2 + 3$ را در نظر بگیرید.)

حل. فرض کنیم p یک مقسوم‌علیه اول N باشد؛ روشن است که، $p \neq 3$. در این‌صورت $(p_1 p_2 \cdots p_n)^2 \equiv -3$ و لذا -3 یک ماندهٔ درجهٔ دوم p است. لذا بنابر (iii.۱۳.۵)، p به‌صورت $6k + 1$ و از این‌رو همچنین به‌صورت $3k + 1$ است. آشکار است که p یکی از p_iها نیست. لذا، به‌ازای هر گردایهٔ متناهی از اعداد اول به‌صورت $6k + 1$، همواره می‌توان عدد اول دیگری به این صورت پیدا کرد.

۵۵.۵ تمام جوابهای (الف) $x^2 \equiv 41 \pmod{43}$؛ (ب) $x^2 \equiv -6 \pmod{103}$ را به‌دست آورید. (راهنمایی: از مسألهٔ ۳.۵ استفاده کنید.)

حل. ملاحظه می‌کنید که ۴۳ و ۱۰۳ هر دو به‌صورت $4k + 3$ هستند، لذا در صورت وجود جواب می‌توانیم از مسأله ۳.۵ برای یافتن جوابها استفاده کنیم.

(الف) برای ساده کردن محاسبات، -2 را به‌جای ۴۱ به‌کار می‌بریم. چون بنابر (i.۱۳.۵)، $(-2/43) = 1$، همنهشتی جواب دارد، و بر طبق مسألهٔ ۳.۵ جوابهای عبارت‌اند از $\pm(-2)^{11}$، یعنی ۱۶ و ۲۷ به پیمانهٔ ۴۳.

(ب) ببینید که $(-6/103) = (-1/103)(2/103)(3/103) = (-1)(+1)(-1) = 1$، لذا همنهشتی حلپذیر است. جوابهای عبارت‌اند از ± 32، یعنی $\pm 6^{26}$ به پیمانهٔ ۱۰۳.

◁ **۵۶.۵** فرض کنید $p = 4k + 1$ اول باشد. اگر d فرد و $d|k$، ثابت کنید $x^2 \equiv d \pmod{p}$ حلپذیر است.

حل. بنابر (ii.۱۰.۵)، یا مستقیماً، می‌توانیم ببینیم که اگر همنهشتیهای $x^2 \equiv a \pmod{p}$ و $x^2 \equiv b \pmod{p}$ حلپذیر باشند، $x^2 \equiv ab \pmod{p}$ نیز حلپذیر است. لذا برای اثبات حلپذیری $x^2 \equiv d \pmod{p}$، کافی است نشان دهیم که به‌ازای هر مقسوم‌علیه اول d مانند q،

$x^۲ \equiv q(\bmod p)$ حلپذیر است. بنابراین، فرض می‌کنیم q اول باشد و $q|k$. چون $p \equiv ۱(\bmod ۴)$، و $۴k \equiv ۰(\bmod q)$، قانون تقابل مربعی ایجاب می‌کند که

$$(q/p) = (p/q) = ((۴k+۱)/q) = (۱/q)$$

بنابراین، $x^۲ \equiv q(\bmod p)$ حلپذیر است.

۵۷.۵ مسألهٔ ۳.۵ را برای یافتن تمام جوابهای همنهشتی $۹x^۴ - ۱۹x^۲ + ۳۰ \equiv ۰(\bmod ۵۹)$ به‌کار برید.

حل. با کامل کردن مربع داریم $۱۸x^۲ - ۱۹)^۲ \equiv ۴۸ \equiv -۱۱(\bmod ۵۹)$. چون بنابر (iv.۱۰.۵) و (ii.۱۰.۵) داریم $(۴۸/۵۹) = (۳/۵۹) = ۱$، همنهشتی $y^۲ \equiv -۱۱(\bmod ۵۹)$ جواب دارد. بنابر مسألهٔ ۳.۵، این جوابها عبارت‌اند از $\pm ۱۱^{۱۵}$، یعنی، ± ۱۵. اکنون

$$۱۸x^۲ - ۱۹ \equiv \pm ۱۵(\bmod ۵۹)$$

را حل می‌کنیم؛ از آنجا $۱۸x^۲ \equiv ۳۴(\bmod ۵۹)$ و $۱۸x^۲ \equiv ۴(\bmod ۵۹)$. همنهشتی $۱۸x^۲ \equiv ۳۴(\bmod ۵۹)$ با $۹x^۲ \equiv ۱۷ \equiv ۱۳۵(\bmod ۵۹)$ هم‌ارز است، یعنی $x^۲ \equiv ۱۵(\bmod ۵۹)$. چون $(۱۵/۵۹) = (۳/۵۹)(۵/۵۹) = ۱$، جواب وجود دارد؛ بنابر مسألهٔ ۳.۵ این جوابها عبارت‌اند از $\pm ۱۵^۵$، یعنی، ± ۲۹. حال $۱۸x^۲ \equiv ۴ \equiv ۶۳(\bmod ۵۹)$، یعنی $۲x^۲ \equiv ۷ \equiv ۶۶(\bmod ۵۹)$ را بررسی می‌کنیم. داریم $x^۲ \equiv ۳۳(\bmod ۵۹)$، و چون $(۳۳/۵۹) = (۳/۵۹)(۱۱/۵۹) = (۵۹/۳)(۵۹/۱۱) = (۲/۳)(۴/۱۱) = -۱$، هیچ جوابی وجود ندارد.

بنابراین تنها جوابهای همنهشتی اصلی عبارت‌اند از ± ۲۹، یعنی ۲۹ و ۳۰.

۵۸.۵ از لمِ گاوس برای محاسبهٔ $(۱۴/۲۳)$ استفاده کنید.

حل. وقتی k مقادیر ۱ تا $۱۱ = ۲/(۱ - ۲۳)$ را اختیار می‌کند، کوچکترین مانده‌های مثبت $۱۴k$ عبارت‌اند از ۱۴، ۵، ۱۹، ۱۰، ۱، ۱۵، ۶، ۲۰، ۱۱، ۲، و ۱۶. از این اعداد ۵ تا بزرگتر از $۲۳/۲$ هستند، لذا بنابر لم گاوس، $(۱۴/۲۳) = (-۱)^۵ = -۱$.

۵۹.۵ فرض کنید $q > ۲$ اول باشد. اگر $p = ۲^q - ۱$ نیز اول باشد، ثابت کنید که $x^۲ \equiv ۳(\bmod p)$ حلپذیر نیست.

حل. چون q فرد است، داریم $p = ۲^q - ۱ \equiv (-۱)^q - ۱ = -۲ \equiv ۱ \pmod ۳$؛ لذا $(p/۳) = ۱$. توجه کنید که p به‌صورت $۴k + ۳$ است، لذا بنابر قانون تقابل مربعی، $(۳/p) = -(p/۳) = -۱$.

۶۰.۵ مقسوم‌علیه‌های اول فرد $n^۲ + ۱$، $n^۲ + ۲$، و $n^۲ + ۳$ را پیدا کنید.

حل. فرض کنیم p یک عدد اول فرد باشد. اگر $p | n^۲ + ۱$، آنگاه $n^۲ \equiv -۱ \pmod p$، لذا، بنابر (۱۱.۵)، p به‌صورت $۴k + ۱$ است. اگر $p | n^۲ + ۲$ و $p \neq ۲$، آنگاه $(-۲/p) = ۱$، و لذا بنابر (i.۱۳.۵)، p به‌صورت $۸k + ۱$ یا $۸k + ۳$ است. و اگر $p | n^۲ + ۳$ و $p > ۳$، آنگاه $(-۳/p) = ۱$؛ لذا بنابر (iii.۱۳.۵)، p به‌صورت $۶k + ۱$ است.

۶۱.۵ با استفاده از (الف) ملاک اویلر؛ (ب) لم گاوس؛ (ج) قانون تقابل مربعی، $(۶/۱۹)$ را محاسبه کنید.

حل. (الف) $(۶/۱۹) \equiv ۶^۹ \equiv ۶(۶^۲)^۴ \equiv ۶(-۲)^۴ \equiv ۶(-۳) \equiv ۱ \pmod{۱۹}$.

(ب) کوچکترین مانده‌های مثبتِ ۶، ۶×۲، ۶×۳، ...، ۶×۹ عبارت‌اند از ۶، ۱۲، ۱۸، ۵، ۱۱، ۱۷، ۴، ۱۰، و ۱۶. از این اعداد شش تا بزرگتر از $۱۹/۲$ هستند، و لذا لم گاوس ایجاب می‌کند که $(۶/۱۹) = (-۱)^۶ = ۱$.

(ج) با استفاده از قانون تقابل مربعی و (۱۲.۵) داریم

$$(۶/۱۹) = (۲/۱۹)(۳/۱۹) = -(۳/۱۹) = (۱۹/۳) = (۱/۳) = ۱$$

۶۲.۵ (الف) ثابت کنید که مقسوم‌علیه‌های اول فرد $۹n^۲ - ۶n + ۴$ به‌صورت $۶k + ۱$ هستند. (راهنمایی: مربع را کامل کنید و (iii.۱۳.۵) را به‌کار برید.)

(ب) ثابت کنید که مقسوم‌علیه‌های اول فرد $n^۲ + ۴n + ۶$ به‌صورت $۸k + ۱$ یا $۸k + ۳$ هستند.

(ج) ثابت کنید که مقسوم‌علیه‌های اول فرد $n^۲ - ۲n - ۴$ به‌صورت $۱۰k \pm ۱$ هستند.

حل. (الف) اگر $p | ۹n^۲ - ۶n + ۴$، آنگاه $۹n^۲ - ۶n + ۴ \equiv ۰ \pmod p$. با کامل کردن مربع داریم $y^۲ \equiv b^۲ - ۴ac \equiv -۱۰۸ \pmod p$. توجه کنید که $(-۱۰n/p) = (-۳/p)$، و (iii.۱۳.۵) را به‌کار برید.

(ب) مانند (الف) استدلال می‌کنیم. با کامل کردن مربع داریم $y^۲ \equiv -۸ \pmod p$. چون $(-۸/p) = (-۲/p)$، نتیجه از (i.۱۳.۵) حاصل می‌شود.

(ج) با کامل کردن مربع داریم $y^۲ \equiv ۲۰ (\mathrm{mod}\, p)$. توجه کنید که $(۵/p) = (۲۰/p)$ و (iv.۱۳.۵) را به‌کار برید تا نتیجه بگیرید که p به‌صورت $۵k \pm ۱$ است. چون p فرد است، k بایستی زوج باشد، و لذا p به‌صورت $۱۰k \pm ۱$ است.

۶۳.۵ اثبات یا رد کنید: اگر p و q اعداد اول فردی باشند به‌طوری که $p \equiv q (\mathrm{mod}\, ۲۶)$، آنگاه $(۱۳/p) = (۱۳/q)$.

حل. قضیه درست است. چون $p \equiv q (\mathrm{mod}\, ۲۶)$ و ۱۳ به‌صورت $۴k + ۱$ است، از قانون تقابل مربعی و (i.۱۰.۵) نتیجه می‌شود که

$$(۱۳/p) = (p/۱۳) = ((q + ۲۶k)/۱۳) = (q/۱۳) = (۱۳/q)$$

۶۴.۵ حلپذیری همنهشتیهای زیر را بررسی کنید: (الف) $x^۲ \equiv ۱۹۹۳ (\mathrm{mod}\, ۱۹۹۷)$؛ (ب) $x^۲ \equiv ۱۹۹۳ (\mathrm{mod}\, ۱۹۹۹)$. (۱۹۹۳، ۱۹۹۷ و ۱۹۹۹ اول هستند.)

حل. قانون تقابل مربعی را به‌کار می‌بریم. (الف)

$$(۱۹۹۳/۱۹۹۷) = (۱۹۹۷/۱۹۹۳) = (۴/۱۹۹۳) = ۱$$

لذا این همنهشتی حلپذیر است. (ب)

$$(۱۹۹۳/۱۹۹۹) = (۱۹۹۹/۱۹۹۳) = (۶/۱۹۹۳) = (۲/۱۹۹۳)(۳/۱۹۹۳)$$
$$= (۳/۱۹۹۳) = (۱۹۹۳/۳) = (۱/۳) = ۱$$

و لذا این همنهشتی جواب دارد.

۶۵.۵ به‌ازای چه اعداد اولی $۱۳x^۲ + ۷x + ۱ \equiv ۰ (\mathrm{mod}\, p)$ جواب دارد؟

حل. اگر $p = ۱۳$، آنگاه همنهشتی به $۷x \equiv ۱ (\mathrm{mod}\, ۱۳)$ بدل می‌شود که جواب دارد. اگر $p \neq ۱۳$، آنگاه از (۱۰.۵) برای تبدیل همنهشتی به $y^۲ \equiv b^۲ - ۴ac = -۳ (\mathrm{mod}\, p)$ استفاده می‌کنیم. لذا بنابر (iii.۱۳.۵)، همنهشتی مفروض حلپذیر است اگر و تنها اگر p به‌صورت $۶k + ۱$ باشد.

۶۶.۵ قانون تقابل مربع را برای بررسی حلپذیری $x^۴ - ۶x^۲ + ۳۵ \equiv ۰ \pmod{۳۷}$ به‌کار برید.

حل. با تکمیل مربع داریم $(۲x^۲ - ۶)^۲ \equiv ۴۴ \pmod{۳۷}$. (محاسبه را با تعویض ۳۵ با -۲ به پیمانهٔ ۳۷ ساده کردیم.) چون $۸۱ \equiv ۴۴ \pmod{۳۷}$، داریم $۲x^۲ - ۶ \equiv \pm ۹ \pmod{۳۷}$، ولذا $۲x^۲ \equiv ۱۵ \pmod{۳۷}$ یا $۲x^۲ \equiv -۳ \pmod{۳۷}$. این همنهشتیها با $x^۲ \equiv ۲۶ \pmod{۳۷}$ و $x^۲ \equiv ۱۷ \pmod{۳۷}$ هم‌ارزند. ملاحظه کنید که

$$(۱۷/۳۷) = (۳۷/۱۷) = (۳/۱۷) = (۱۷/۳) = (۲/۳) = -۱$$

همچنین، بنابر (۱۲.۵)،

$$\begin{aligned}(۲۶/۳۷) &= (۲/۳۷)(۱۳/۳۷) = -(۳۷/۱۳) = -(۱۱/۱۳) \\ &= -(۱۳/۱۱) = -(۲/۱۱) = ۱\end{aligned}$$

لذا همنهشتی اصلی دو جواب دارد.

نماد ژاکوبی

برای آسان کردن محاسبه، می‌توان نماد لژاندر را به حالتی توسعه داد که عدد مخرج اول نباشد. نماد ژاکوبی (a/m)، که در ۱۸۴۶ توسط کارل گوستاو ژاکوبی[1] (۱۸۰۴ـ۱۸۵۱) معرفی شد، فقط مقادیر ۱ و -۱ را می‌پذیرد و وقتی m اول است با نماد لژاندر مطابقت دارد. ولی، برخلافِ نماد لژاندر لازم نیست که قبل از وارد کردن، مخرج را به حاصلضربِ اعداد اول تجزیه کنیم. این مطلب نماد ژاکوبی را در محاسبهٔ نماد لژاندر به‌ویژه کارآمد می‌سازد.

بیشتر ویژگیهای نماد لژاندر برای نماد ژاکوبی صدق می‌کنند، از جمله قانون تقابل، اما یک استثنای مهم وجود دارد: $(a/m) = ۱$ ایجاب نمی‌کند که $x^۲ \equiv a \pmod{m}$ حلپذیر باشد. (این بهایی است که برای برقرار بودن قانون تقابل برای نماد ژاکوبی پرداخت می‌شود. اگر فقط تعریف کنیم (a/m) مساوی ۱ یا -۱ برحسب آنکه $x^۲ \equiv a \pmod{m}$ حلپذیر باشد یا نباشد، آنگاه نماد ژاکوبی قانون تقابل را برآورده نمی‌کند.)

در ادامه تعریف و ویژگیهای اصلی نماد ژاکوبی را فهرست می‌کنیم. (می‌توان برهان این نتایج را، مثلاً در کتاب نیون[2] و تسوکرمن[3] پیدا کرد؛ مراجع کلی در آخر کتاب را ببینید).

تعریف. فرض کنیم $m = \prod p_i^{k_i}$، که هر p_i یک عدد اول فرد است، و فرض می‌کنیم

1. Carl Gustav Jacobi 2. Niven 3. Zuckerman

$(a,m) = ۱$). نماد ژاکوبی (a/m) را با $(a/m) = \prod(a/p_i)^{k_i}$ تعریف می‌کنیم. که در آن عاملهای (a/p_i) نمادهای لژاندرند.

قضیه. فرض کنیم m و n اعداد صحیح مثبت فرد باشند.

(i) اگر $(a,m) = ۱$ و $a \equiv b(\mathrm{mod}\, m)$، آنگاه $(a/m) = (b/m)$.

(ii) اگر $(a,m) = (b,m) = ۱$، آنگاه $(ab/m) = (a/m)(b/m)$. به‌ویژه، $(a^۲/m) = ۱$.

(iii) اگر m و n نسبت به هم اول باشند و $(a,m) = (a,n) = ۱$، آنگاه $(a/mn) = (a/m)(a/n)$.

(iv) $(-۱/m) = ۱$ اگر و تنها اگر $m \equiv ۱(\mathrm{mod}\, ۴)$.

(v) $(۲/m) = ۱$ اگر و تنها اگر $m \equiv \pm ۱(\mathrm{mod}\, ۸)$.

(vi) (قانون تقابل) اگر $(m,n) = ۱$، آنگاه $(m/n)(n/m) = (-۱)^{\frac{m-۱}{۲}\frac{n-۱}{۲}}$.

۶۷.۵ اگر (a/m) معرف نماد ژاکوبی باشد، با مثالی نشان دهید که $(a/m) = ۱$ ایجاب نمی‌کند که $x^۲ \equiv a(\mathrm{mod}\, m)$ حلپذیر باشد.

حل. $x^۲ \equiv -۱(\mathrm{mod}\, ۲۱)$ را در نظر می‌گیریم. این معادله جواب ندارد، زیرا $x^۲ \equiv -۱(\mathrm{mod}\, ۳)$ جواب ندارد (۱۱.۵ را ببینید). اما

$$(-۱)/۲۱) = (-۱/۳)(-۱/۷) = (-۱)(-۱) = ۱$$

توضیح. به‌طورکلی، نماد ژاکوبی (a/m) برابر ۱ است به شرطی که تعداد زوجی از نمادهای لژاندر (a/p_i) که معرف (a/m) هستند برابر -۱ باشند.

۶۸.۵ فرض می‌کنیم نماد ژاکوبی (a/m) مساوی -۱ باشد. ثابت کنید که همنهشتی $x^۲ \equiv a(\mathrm{mod}\, m)$ حلپذیر نیست.

حل. اگر $(a/m) = -۱$، آنگاه بنابر تعریف نماد ژاکوبی، حداقل یکی از عاملهای (a/p_i) برابر -۱ است. بنابراین $x^۲ \equiv a(\mathrm{mod}\, p_i)$ جواب ندارد، و لذا $x^۲ \equiv a(\mathrm{mod}\, m)$ نمی‌تواند جواب داشته باشد.

۶۹.۵ مقدار $(۳۸۲۸/۲۵۳۹)$ را با استفاده از نماد ژاکوبی و نیز بدون استفاده از آن حساب کنید. (۲۵۳۹ اول است.)

حل. نماد ژاکوبی را به‌کار می‌بریم:

$$(۳۸۲۸/۲۵۳۹) = (-۱۲۵۰/۲۵۳۹) = (-۱/۲۵۳۹)(۲/۲۵۳۹)$$
$$= (۶۲۵/۲۵۳۹) = (-۱)(-۱)(۶۲۵/۲۵۳۹)$$

(زیرا $۲۵۳۹ \equiv ۳ \pmod ۸$). اما بدیهی است که $(۶۲۵/۲۵۳۹) = ۱$، زیرا ۶۲۵ مربع کامل است، ولی می‌خواهیم که از تجزیه خودداری کنیم (بجز تقسیم بر ۲)، زیرا برای اعداد بزرگ، تجزیه بسیار کُند صورت می‌گیرد. حال

$$(۶۲۵/۲۵۳۹) = (۲۵۳۹/۶۲۵) = (۳۹/۶۲۵) = (۶۲۵/۳۹) = (۱/۳۹) = ۱$$

نمادهای لژاندر را به‌کار می‌بریم:

$$(۳۸۲۸/۲۵۳۹) = (۴/۲۵۳۹)(۳/۲۵۳۹)(۱۱/۲۵۳۹)(۱۹/۲۵۳۹)$$
$$= [-(۲۵۳۹/۳)][-(۲۵۳۹/۱۱)][-(۲۵۳۹/۱۹)]$$
$$= -(۱/۳)(۹/۱۱)(۱۲/۱۹) = -(۳/۱۹) = (۱/۳) = ۱$$

۷۰.۵ به کمک نمادهای ژاکوبی تعیین کنید کدام‌یک از همنهشتیهای زیر حلپذیرند:
(الف) $x^۲ \equiv -۷۰ \pmod{۷۰۹}$؛ (ب) $x^۲ \equiv ۲۱۰ \pmod{۲۶۳}$؛ (ج) $x^۲ \equiv ۳۳۰ \pmod{۹۹۷}$. (۲۶۳ و ۹۹۷ اول‌اند.)

حل. (الف) $(-۷۰/۷۰۹) = (-۱/۷۰۹)(۲/۷۰۹)(۳۵/۷۰۹) = -(۳۵/۷۰۹)$ زیرا $۷۰۹ \equiv ۵ \pmod ۸$ و $۷۰۹ \equiv ۱ \pmod ۴$؛

$$-(۳۵/۷۰۹) = -(۷۰۹/۳۵) = -(۹/۳۵) = -(۳۵/۹) = -(-۱/۹) = -۱$$

زیرا $۹ \equiv ۱ \pmod ۴$. لذا همنهشتی حلپذیر نیست.

(ب)

$$(۲۱۰/۲۶۳) = (۲/۲۶۳)(۱۰۵/۲۶۳) = (۱۰۵/۲۶۳) = (۲۶۳/۱۰۵)$$
$$= (-۵۲/۱۰۵) = (۱۳/۱۰۵) = (۱۰۵/۱۳) = (۱/۱۳) = ۱$$

چون $(۲۱۰/۲۶۳)$ یک نماد لژاندر است (زیرا ۲۶۳ اول است)، در نتیجه همنهشتی مفروض حلپذیر است.

(ج)

$$(۳۳۰/۹۹۷) = (۲/۹۹۷)(۱۶۵/۹۹۷) = -(۱۶۵/۹۹۷)$$
$$= -(۹۹۷/۱۶۵) = -(۷/۱۶۵) = -(۱۶۵/۷) = -(۴/۷) = -۱$$

لذا همنهشتی حلپذیر نیست.

◁ **۷۱.۵** (الف) اعداد صحیح مثبتِ m متباین با ۳ را مشخص کنید به‌طوری که ۳ یک نامانده‌ٔ درجهٔ دوم m باشد.

(ب) اعداد صحیح مثبت m را که بر ۳ بخشپذیر نیستند معین کنید به‌طوری که نماد ژاکوبی $(۳/m)$ برابر ۱ باشد.

حل. (الف) فرض کنیم $m = ۲^k \prod p_i^{k_i}$، که در آن p_iها اعداد اول فردی غیر از ۳ هستند. چون همنهشتی $x^۲ \equiv ۳ (\mathrm{mod}\ ۴)$ جوابی ندارد، نتیجه می‌شود که اگر $k \geq ۲$، آنگاه ۳ یک نامانده‌ٔ درجهٔ دوم m است.

حال، فرض می‌کنیم $k = ۰$ یا $k = ۱$. بنابر (ii.۱۳.۵)، ۳ یک نامانده‌ٔ درجهٔ دوم عدد اولِ فرد p است اگر و تنها اگر p به‌صورت $۱۲k \pm ۵$ باشد. لذا برای m که بر ۳ یا ۴ بخشپذیر نیست، ۳ یک نامانده‌ٔ درجهٔ دوم m است اگر و تنها اگر حداقل یک i وجود داشته باشد که $p_i \equiv \pm ۵ (\mathrm{mod}\ ۱۲)$.

(ب) وقتی b زوج باشد نماد ژاکوبی (a/b) تعریف نمی‌شود. فرض می‌کنیم $(۳, m) = ۱$ و $m = \prod p_i^{k_i}$ فرد باشد. بر طبق تعریف نماد ژاکوبی، اگر k_i زوج باشد، $(۳/p_i)$ تأثیری در $(۳/m)$ ندارد. لذا $(۳/m) = ۱$ اگر و تنها اگر به‌ازای یک تعداد زوج (احتمالاً ۰) از p_iها که برای آنها k_i فرد است، $(۳/p_i) = -۱$؛ یعنی، اگر و تنها اگر تعداد زوجی از p_iها که برای آنها k_i فرد است به‌صورت $۱۲k \pm ۵$ باشند.

تمرینهایی برای فصل ۵

۱. نمادهای لژاندر $(۷۰/۹۷)$ و $(۲۶۳/۳۳۱)$ را محاسبه کنید.

۲. $(۱۴/۳۱۱)$، $(۱۶۵/۳۱۳)$، و $(۱۸۹۱/۱۹۹۹)$ را محاسبه کنید.

۳. $(۷۲/۷۳) + \cdots + (۲/۷۳) + (۱/۷۳)$ را محاسبه کنید.

۴. مقدار زیر را به‌دست آورید: $((۷۲/۷۳)(۷۱/۷۳)) + \cdots + ((۳/۷۳)(۲/۷۳)) + ((۲/۷۳)(۱/۷۳))$.

۵. لم گاوس را برای محاسبهٔ $(۳/۳۱)$ به‌کار برید.

۶. (الف) ملاک اویلر را برای محاسبهٔ (۳۷/۴۳) به‌کار برید.
(ب) لم گاوس را برای محاسبهٔ (۱۳/۱۹) به‌کار برید.
(ج) قانون تقابل مربعی را برای یافتن (۳۲۳/۳۵۳) به‌کار برید.

۷. با استفاده از ملاک اویلر یا به طریق دیگر، قضیهٔ ۱۰.۵ را ثابت کنید.

۸. فرض کنید p اول باشد. ثابت کنید که $(n^۲-۲)(n^۲-۵)(n^۲-۴۰)$ به‌ازای بی‌نهایت مقدار n بر p بخشپذیر است.

۹. (الف) آیا عدد صحیح مثبت n وجود دارد به‌طوری که $n^۲-۳$ مضرب ۳۱۳ باشد؟
(ب) آیا بی‌نهایت n وجود دارد به‌طوری که $n^۲+۳$ بر ۹۷ بخشپذیر باشد؟

۱۰. نشان دهید که مقسوم‌علیه‌های اول $۴n^۲+۲۸n+۵۱$ به‌صورت $۸k+۱$ یا $۸k+۳$ هستند.

۱۱. ثابت کنید که هر مقسوم‌علیه اول فرد $n^۴+۱۰۰$ به‌صورت $۱۲k+۱$ یا $۱۲k+۵$ است.

۱۲. مقسوم‌علیه‌های اول $n^۲+۶$ را معین کنید.

۱۳. اعداد اول p را تعیین کنید به‌طوری که $۱۱-$ یک ماندهٔ درجهٔ دوم p باشد.

۱۴. به‌ازای چه اعداد اول فرد p، $۵-$ یک ماندهٔ درجهٔ دوم p است؟

۱۵. اعداد اول فرد p را مشخص کنید که ۱۱ ماندهٔ درجهٔ دوم آنها باشد.

۱۶. اعداد اول فرد p را تعیین کنید به‌طوری که ۱۳ یک نامانده درجهٔ دوم آنها باشد.

۱۷. حلپذیری $x^۲ \equiv ۱۰۹ \pmod{۳۱۳}$ را بررسی کنید.

۱۸. حلپذیری همنهشتیهای زیر را بررسی کنید:
(الف) $x^۲+۳x+۳ \equiv ۰ \pmod{۴۱}$؛
(ب) $۳x^۲-۴x-۱ \equiv ۰ \pmod{۱۳۶۳}$. (راهنمایی: ابتدا ۱۳۶۳ را تجزیه کنید.)

۱۹. تعیین کنید $۶x^۲-۱۵x-۵ \equiv ۰ \pmod{۷۴۹}$ حلپذیر است یا نیست.

۲۰. با استفاده از ملاک اویلر حلپذیری $۵x^۲-۱۲x+۱ \equiv ۰ \pmod{۶۱}$ را بررسی کنید.

۲۱. قانون تقابل مربعی را برای بررسی حلپذیری $۲x^۲-۶x-۸۹ \equiv ۰ \pmod{۱۹۸۷}$ به‌کار برید. (۱۹۸۷ اول است.)

۲۲. تعیین کنید که $۷x^۲-۲۵x+۱ \equiv ۰ \pmod{۵۹۹}$ جواب دارد یا نه. (۵۹۹ اول است.)

۲۳. آیا همنهشتی $x^۴ \equiv -۱ \pmod{۲۹۹}$ حلپذیر است؟

۲۴. ثابت کنید $۱۷x^۲+۱۹x-۲ \equiv ۰ \pmod{۳۴۹۳}$ جواب دارد. چند جواب دارد؟

۲۵. تعداد جوابهای همنهشتیهای زیر را به‌دست آورید:
(الف) $x^۴ \equiv ۶ \pmod{۱۷۵}$؛

(ب) $x^۲ \equiv ۳۶۱ (\mathrm{mod}\, ۶۹۳)$؛

(ج) $x^۲ \equiv ۴۱ (\mathrm{mod}\, ۲^۶ \times ۵^۳ \times ۳۷^۲ \times ۷۳^۲)$.

۲۶. تعداد جوابهای $x^۲ \equiv ۵۷ (\mathrm{mod}\, ۲۵۶)$ و $x^۲ \equiv ۷۱ (\mathrm{mod}\, ۱۲۸)$ را تعیین کنید.

۲۷. $x^۲ \equiv -۳ (\mathrm{mod}\, ۳۷^۳)$ چند جواب دارد؟

۲۸. تعداد جوابهای $x^۲ \equiv ۶۹ (\mathrm{mod}\, ۴ \times ۵^۳ \times ۱۱^۲)$ و $x^۲ \equiv ۴۱ (\mathrm{mod}\, ۲^۳ \times ۵^۴ \times ۲۳^۲)$ را به‌دست آورید.

۲۹. تعداد جوابهای همنهشتیهای زیر را به‌دست آورید:

(الف) $x^۲ \equiv ۱۷ (\mathrm{mod}\, ۱۹ \times ۱۳^۲ \times ۲^۵)$؛

(ب) $x^۲ \equiv ۹ (\mathrm{mod}\, ۲^۴ \times ۵^۳ \times ۷^۲)$؛

(ج) $x^۲ \equiv ۵۷ (\mathrm{mod}\, ۲^۷ \times ۷^۵ \times ۵۹^۲)$.

۳۰. با استفاده از مسألهٔ ۳.۵ حلپذیری $x^۲ \equiv ۳ (\mathrm{mod}\, ۸۳)$ و $x^۲ \equiv ۱۳ (\mathrm{mod}\, ۸۳)$ را بررسی، و در صورت وجود جوابها را پیدا کنید.

۳۱. همهٔ جوابهای $x^۲ \equiv -۱ (\mathrm{mod}\, ۲۹)$ را به‌دست آورید.

۳۲. با استفاده از مسألهٔ ۳.۵ جوابهای $۹x^۲ - ۲۴x + ۱۳ \equiv ۰ (\mathrm{mod}\, ۷۳)$ را پیدا کنید.

۳۳. کوچکترین مانده‌های مثبت جوابهای همنهشتیهای زیر را به‌دست آورید.

(الف) $۹x^۲ - ۱۲x - ۵ \equiv ۰ (\mathrm{mod}\, ۵۳)$؛

(ب) $۴x^۲ + ۴۷x - ۴۹ \equiv ۰ (\mathrm{mod}\, ۵۹)$.

۳۴. همهٔ جوابهای $۵x^۲ - ۷x - ۱۱ \equiv ۰ (\mathrm{mod}\, ۶۱)$ را به‌دست آورید.

۳۵. با استفاده از قانون تقابل مربعی حلپذیری $x^۲ \equiv -۳ (\mathrm{mod}\, ۷۹)$ را ثابت کنید. هر دو جواب آن را به‌دست آورید.

۳۶. همهٔ جوابهای $۲x^۲ - ۳x - ۹ \equiv ۰ (\mathrm{mod}\, ۷۳)$ را پیدا کنید.

۳۷. ثابت کنید که $x^۲ - ۱۲x + ۱۷ \equiv ۰ (\mathrm{mod}\, ۷۹)$ حلپذیر است، و جوابها را به‌دست آورید.

۳۸. هر دو جواب همنهشتیهای زیر را پیدا کنید: (الف) $x^۲ \equiv ۲ (\mathrm{mod}\, ۲۶۳)$؛ (ب) $x^۲ \equiv -۵۳ (\mathrm{mod}\, ۸۳)$؛ (ج) $x^۲ \equiv ۲۰ (\mathrm{mod}\, ۷۹)$.

۳۹. با استفاده از قضیهٔ باقیماندهٔ چینی و مسألهٔ ۳.۵ همهٔ جوابهای $x^۲ \equiv ۳۷ (\mathrm{mod}\, ۷۷)$ را پیدا کنید.

۴۰. با استفاده از قضیهٔ باقیماندهٔ چینی کوچکترین ماندهٔ مثبت جوابهای همنهشتی زیر را پیدا کنید: $۲۵x^۲ - ۱۵۷x + ۱۱ \equiv ۰ (\mathrm{mod}\, ۱۸۷)$.

۴۱. همهٔ جوابهای $۳x^۲ - ۱۰x + ۷ \equiv ۰ (\mathrm{mod}\, ۱۵۴۷)$ را به‌دست آورید. (ابتدا ۱۵۴۷ را تجزیه کنید.)

۴۲. با استفاده از قضیهٔ باقیماندهٔ چینی همنهشتیهای زیر را حل کنید.

(الف) $۴x^۲ - ۱۲x + ۵ \equiv ۰ \pmod{۷۷}$؛

(ب) $۲x^۲ - x + ۷ \equiv ۰ \pmod{۹۱}$.

۴۳. جوابهای $۷x^۲ - x + ۲۴ \equiv ۰ \pmod{۳۶}$ را به‌دست آورید.

۴۴. همنهشتی $x^۲ + ۳x - ۷ \equiv ۰ \pmod{۷۷}$ را حل کنید.

۴۵. همهٔ جوابهای $۲۳x^۲ - x - ۲۱ \equiv ۰ \pmod{۹۱}$ را تعیین کنید.

۴۶. دو ماندهٔ درجهٔ دوم متوالی از ۸۹ را پیدا کنید.

۴۷. کوچکترین ماندهٔ نامنفی مجموع ماندههای درجهٔ دوم ۳۱ چقدر است؟

۴۸. فرض می‌کنیم N تعداد اعداد صحیح مثبتِ کوچکتر از ۱۶ باشد که ماندهٔ درجهٔ دوم ۳۱ هستند. نشان دهید که $۱۵! \equiv (-۱)^N \pmod{۳۱}$.

۴۹. کوچکترین ماندهٔ نامنفی حاصلضرب ماندههای درجهٔ دوم ۵۹ چقدر است؟

۵۰. اثبات یا رد کنید: اگر $x^۲ \equiv a \pmod{m}$ برای دو مقدار متفاوت a حلپذیر باشد، تعداد جوابهای هر همنهشتی یکی است.

۵۱. فرض می‌کنیم $p = ۲^{۲^n} + ۱$، که $n \geq ۱$. اگر p اول باشد، ثابت کنید که $۳^{(p-۱)/۲} + ۱$ بر p بخشپذیر است.

ملاحظاتی برای فصل ۵

۱. در بند ۱۵۲ از تحقیقات حسابی، گاوس به اختصار یافتن جوابهای $ax^۲+bx+c \equiv ۰ \pmod{m}$ را پاسخ داده است و روش تبدیل این مسأله را به مطالعهٔ همنهشتیهایی به‌صورت $y^۲ \equiv d \pmod{m}$ شرح داده است. در بندهای ۱۰۰ـ۱۰۵، گاوس از چگونگی تبدیل این همنهشتی آخر به $y^۲ \equiv d \pmod{p}$ به تفصیل بحث می‌کند.

۲. ظاهراً اویلر اولین ریاضیدانی است که ماندهها و نامانده‌ها را تعریف و به‌طور نظام‌مند با آنها کارکرده است. اما، یک قرن جلوتر، فرما به اعداد اولی پی برده بود که a یک ماندهٔ درجهٔ دوم آنها بود، a مساوی ۱−، ۲، ۳، و ۵.

۳. هیچ فرمول ساده‌ای نظیر قانون تقابل مربعی، برای ماندههای درجهٔ nام، که $n \geq ۳$، وجود ندارد. (ولی، قانونهای تقابلِ نسبتاً پیچیده‌ای برای یک چنین nها وجود دارد، ملموس‌ترین قضیه‌ها برای $n = ۳$ و $n = ۴$ موجود است.) در فصل ۶، ملاکی برای تعیین عدد صحیحی که ماندهٔ درجهٔ nام p^k یا $۲p^k$، باشد به‌دست می‌دهیم؛ در اینجا p یک عدد اول فرد است.

۴. مقدار اصلی نماد ژاکوبی (P/Q) وقتی Q اول باشد، در ساده کردن و سرعت بخشیدن

به محاسبهٔ نماد لژاندر نمایان می‌شود. محاسبات نماد ژاکوبی یک شباهت صوری قوی با الگوریتم اقلیدسی دارد، و به آسانی دیده می‌شود که زمان لازم برای محاسبهٔ (P/Q) و (P,Q) تقریباً یکی است. به‌ویژه، اگر p عدد اول بزرگ باشد، بررسی حلپذیری $x^2 \equiv a \pmod{p}$ به کمک نماد ژاکوبی و قانون تقابلِ مربوط، از محاسبهٔ نماد لژاندر (a/p) با استفاده از قانون تقابل مربعی خیلی سریع‌تر است.

وقتی که a و p تقریباً مرتبهٔ بزرگی واحد دارند، محاسبات نماد ژاکوبی و ملاک اویلر روشهای کارای تقریباً واحدی برای محاسبهٔ (a/p) هستند. اگر a خیلی کوچکتر از p باشد، محاسبهٔ نماد ژاکوبی سریعتر است، زیرا بعد از یک مرحلهٔ تقابل، ممکن است با مقدار کاملاً کوچکی سروکار پیدا کنیم. اگر به‌جای رایانه از یک حسابگر استفاده می‌کنیم و p مثلاً یک عدد اول هفت رقمی است، محاسبهٔ نماد ژاکوبی بسیار آسانتر است. مشکل استفاده از ملاک اویلر این است که در محاسبهٔ $a^{(p-1)/2}$ به پیمانهٔ p، ممکن است لازم باشد که با اعداد ۱۴ رقمی سروکار پیدا کنیم.

شرح مختصری از زندگینامه

فردینانت گوتهولت آیزنشتاین[1] در ۱۸۲۳ در برلین متولد شد. در جوانی غالباً بیمار بود و فقط در ۱۸۴۳ در دانشگاه برلین ثبت نام کرد. در این زمان، او بر تکنیکهای گاوس، ایریکله، و ژاکوبی دست یافته بود. در ۱۸۴۴ با چاپ ۲۵ مقالهٔ کوتاه در مجلهٔ کرله[2] سخت وارد صحنهٔ ریاضیات شد. از جملهٔ این مقاله‌ها دو برهان زیبا مربوط به قانون تقابل مربعی است، که یکی از آنها هنوز هم در اغلب کتابهای درسی تکرار می‌شود. دیگری متضمن اندیشه‌های کاملاً تازه‌ای است که او را قادر ساختند که در همان سال قوانین تقابل درجهٔ سوم و دو مجذوری را ثابت کند. قوانینی که گاوس سالها در صدد اثبات آنها بود.

در همان سال (ژوئن ۱۸۸۴. مترجم) به مدت دو هفته به دیدار با گاوس در گوتینگن گذرانید. گاوس بارها آیزنشتاین را ستوده است، دربارهٔ استعدادش می‌گوید «استعدادی که طبیعت در هر سده فقط به چند تنی عطا می‌کند». (شایع است که گاوس گفته است که فقط سه ریاضیدان تاریخ‌ساز وجود داشته‌اند: ارشمیدس، نیوتون، و آیزنشتاین؛ اما هیچ مدرکی برای این روایت که غالباً تکرار می‌شود وجود ندارد.) در ۱۸۴۷، گاوس یک مقدمهٔ تحسین‌آمیز بر مجموعه آثار آیزنشتاین نوشته است.

با وجود دفعات مکرر بیماری، آیزنشتاین به انجام کارهای درخشان در توابع بیضوی و قوانین تقابلهای درجات بالاتر ادامه می‌داد. مشکلات دیگری نیز وجود داشت. در ۱۸۴۸، در فعالیتهای

1. Ferdinand Gotthold Eisenstein 2. Crelle's Journal

انقلابی در برلین درگیر شد. و توسط سربازان پروسی به طرز بدی کتک خورد و برای مدت کوتاهی زندانی شد. در دو سالِ بعد، مقاله‌هایی سرشار از اندیشه‌هایی در مورد صورتهای درجهٔ دوم، مجموعهای گاوسی، و نظریهٔ ایدآلهای کومر[1] نوشت. در ۱۸۵۲ به‌عنوان جانشین ژاکوبی به عضویت آکادمی برلین انتخاب گردید.

آیزنشتاین در ۱۸۵۲ در سن ۲۹ سالگی به بیماری سل ریوی درگذشت.

مراجع

Harold Davenport, *The Higher Arithmetic* (Sixth Edition), Cambridge University Press, Cambridge, England, 1992.

این کتاب مختصر یکی از خواندنی‌ترین کتابهای موجود است و خلاصهٔ شگفت‌آوری از نظریهٔ مقدماتی اعداد به‌دست می‌دهد. به دلیل قطع کتاب، داونپورت به اندازهٔ کتابهای درسی استانده مطالب را اثبات نمی‌کند، اما قضیه‌های عرضه‌شده بیشتر سطوح مهم در نظریهٔ اعداد را می‌پوشانند وکاملاً مُوجّه هستند. برهانها مفصل وکامل‌اند، و چون به روش محاوره‌ای نوشته شده‌اند نمادگذاری مزاحمتی ایجاد نمی‌کنند. تعداد مثالها در این کتاب زیاد نیست، اما مثالهایی که آمده‌اند مفصلاً با بحث همراه‌اند. روی‌هم‌رفته، حساب عالی یک کتاب خیلی لذت‌بخش برای مطالعه است، و قویاً برای دانشجویان در هر سطحی توصیه می‌شود.

Carl Friedrich Gauss, *Disquisitions Arithmeticae*, translated by Arthur A. Clarke. (See Chapter 2.)

1. Kummer

۶

ریشه‌های اولیه و اندیسها

در فصل قبل، مانده‌های درجهٔ دوم از یک عدد صحیح مثبت m را مطالعه کردیم. در این فصل، به بررسی مانده‌های توانی kام m به‌ازای $k \geq ۲$ ـ یعنی، اعداد متباین با m مانند a که به‌ازای آنها $x^k \equiv a (\mathrm{mod}\, m)$ حلپذیر است ـ می‌پردازیم و روشی برای تعیین حلپذیری این چنین همنهشتیها ارائه خواهیم کرد.

به‌منظور یافتن جوابها، از وجود ریشه‌های اولیهٔ m و مفهوم اندیسها استفاده می‌کنیم و همنهشتی $x^k \equiv a (\mathrm{mod}\, m)$ را به $ky \equiv b (\mathrm{mod}\, \phi(m))$ بدل می‌کنیم، سپس می‌توانیم جوابهای همنهشتی آخر را با هر یک از روشهای مربوط به همنهشتیهای خطی که در فصل ۲ بیان شد پیدا کنیم. ویژگیهای اندیسها شباهت زیادی به ویژگیهای لگاریتمها دارند؛ کاربرد اندیسها به ما اجازه می‌دهد که یک مسأله شامل نماها را به مسأله شامل ضرب و همچنین یک مسألهٔ ضرب را به یک مسألهٔ جمع بدل کنیم.

با اینکه وجود یک ریشهٔ اولیه برای یک پیمانهٔ مفروض اهمیت نظری دارد و مطالعهٔ مانده‌های

توانی kام را ساده می‌سازد، اما چنین نیست که هر عدد صحیح مثبتی یک ریشهٔ اولیه داشته باشد. در واقع، قضیهٔ اصلی این فصل که در ۱۸۰۱ توسط گاوس اثبات شد، مشخص کردن اعداد صحیح مثبتی است که ریشهٔ اولیه دارند.

قضیه‌هایی برای فصل ۶

مرتبهٔ یک عدد صحیح

موضوع را با تعریف رسمی یک عدد صحیح شروع می‌کنیم، مفهومی که در فصل ۳ به اختصار به آن اشاره شد (۹.۳) را ببینید).

(۱.۶) تعریف. فرض کنیم m یک عدد صحیح مثبت باشد و $(a,m)=1$. مرتبهٔ a به پیمانهٔ m، که با $\operatorname{ord} a$ نشان داده می‌شود، کوچکترین عدد صحیح مثبتی مانند h است به‌طوری که $a^h \equiv 1 \pmod m$.

توضیح. ۱. نماد $\operatorname{ord} a$ ابهام‌آمیز است، زیرا مرتبهٔ یک عدد صحیح به پیمانه نیز بستگی دارد. نشان دادن مرتبه با $\operatorname{ord}_m a$ ممکن است واضحتر باشد. ولی، چون در خلال یک محاسبه معمولاً پیمانه ثابت است، نماد ساده‌تر مشکلی ایجاد نمی‌کند.

۲. اگر a با m متباین باشد، بنابر قضیهٔ اویلر، $a^{\phi(m)} \equiv 1 \pmod m$، و لذا مرتبهٔ یک عدد هرگز بزرگتر از $\phi(m)$ نیست. به آسانی دیده می‌شود که یک نمای کوچکتر ممکن است کفایت کند: به‌ازای هر عدد صحیح مثبت m، $\operatorname{ord} 1 = 1$، و اگر $m > 2$، $\operatorname{ord}(-1) = 2$.

۳. در کتابهای قدیمیتر، مرتبهٔ a به پیمانهٔ m، به نمایی که a به پیمانهٔ m به آن تعلق دارد گفته می‌شود. ولی، اکنون این اصطلاح تقریباً غیرمعمول است، و ما در این کتاب منحصراً مرتبهٔ a به پیمانهٔ m را به‌کار خواهیم برد، اصطلاحی که در نظریهٔ گروهها استانده است و ساختار جبری زیربنایی یک دستگاه مخفف مانده‌ها به پیمانهٔ m را منعکس می‌سازد.

(۲.۶) قضیه. فرض می‌کنیم m یک عدد مثبت باشد و $(a,m)=1$.

(i) $a^s \equiv 1 \pmod m$ اگر و تنها اگر $\operatorname{ord} a \mid s$. به‌ویژه، $\operatorname{ord} \mid \phi(m)$.

(ii) $a^s \equiv a^t \pmod m$ اگر و تنها اگر $s \equiv t \pmod{\operatorname{ord} a}$.

برهان. (i) اگر $s = k \operatorname{ord} a$، آنگاه $a^s = (a^{\operatorname{ord} a})^k \equiv 1^k = 1 \pmod m$. بعکس، فرض کنیم $a^s \equiv 1 \pmod m$. بنابر الگوریتم تقسیم، داریم $s = q \operatorname{ord} a + r$، که $0 \le r < \operatorname{ord} a$؛

لذا $a^s = (a^{\operatorname{ord} a})^q a^r \equiv a^r \pmod m$، زیرا بنابه تعریف، $a^{\operatorname{ord} a}$ کوچکترین توانِ مثبت a همنهشت با ۱ به پیمانهٔ m است. قسمت دوم از قضیهٔ اویلر نتیجه می‌شود.

(ii) می‌توانیم فرض کنیم که $s \geq t$. اگر $a^s \equiv a^t \pmod m$، آنگاه

$$a^s = a^t a^{s-t} \equiv a^s a^{s-t} \pmod m$$

چون $(a^s, m) = ۱$، از (vi.۲.۲) نتیجه می‌شود که $s^{s-t} \equiv ۱ \pmod m$. اکنون از قسمت (i) استفاده کنید. بعکس، اگر $s \equiv t \pmod{\operatorname{ord} a}$، آنگاه عدد صحیح k وجود دارد که $s = t + k \operatorname{ord} a$. لذا $a^s = a^t (a^{\operatorname{ord} a})^k \equiv a^t \pmod m$.

در حالتِ یک پیمانهٔ اولِ p (i.۲.۶) ایجاب می‌کند که مرتبهٔ a یک مقسوم‌علیه $p - ۱$ باشد. (اویلر اولین کسی بود که در ۱۷۳۶ برهان زیر را منتشر کرد: اگر p اول باشد و d کوچکترین عدد صحیح مثبتی باشد که $a^d \equiv ۱ \pmod p$، آنگاه $d | (p - ۱)$، ولی این قضیه توسط فرما در ۱۶۴۰ بیان شده بود. ((۹.۳) را ببینید.)

(۳.۶) قضیه. فرض کنیم m یک عدد صحیح مثبت باشد $(a, m) = ۱$.

(i) اگر $\operatorname{ord} a = d$، آنگاه به‌ازای هر $k \geq ۱$، $\operatorname{ord} a^k = d/(k, d)$.

(ii) اگر $\operatorname{ord} a = d$ و e یک مقسوم‌علیه مثبت d باشد، آنگاه e مرتبهٔ $a^{d/e}$ است.

برهان. از (i.۲.۶) نتیجه می‌شود که $(a^k)^j \equiv ۱ \pmod m$ اگر و تنها اگر kj مضربی از d باشد، یعنی، اگر و تنها اگر kj کوچکترین مضرب مشترک k و d باشد. اما این کوچکترین مضرب مشترک برابر $kd/(k, d)$ است، و لذا $j = d/(k, d)$. قسمت (ii) از (i) با توجه به این نکته حاصل می‌شود که اگر $e | d$، آنگاه $(d/e, d) = d/e$.

قضیه بعد چگونگی ساختن عدد صحیحی را نشان می‌دهد که مرتبه‌اش کوچکترین مضرب مشترک h و k باشد، هرگاه h و k مرتبه‌های مفروض دو عنصر باشند.

(۴.۶) قضیه. فرض کنیم $h = \operatorname{rod} a$ و $k = \operatorname{ord} b$. اگر $(h, k) = ۱$، آنگاه $\operatorname{rod} ab = hk$.

در حالت کلی، عدد صحیحی چون c وجود دارد به‌طوری که مرتبهٔ c برابر کوچکترین مضرب مشترک h و k است.

برهان. ابتدا نشان می‌دهیم که اگر $(h, k) = ۱$، آنگاه مرتبهٔ ab برابر hk است. فرض کنیم $r = \operatorname{ord} ab$. آشکار است که $(ab)^{hk} = (a^h)^k (b^k)^h \equiv ۱ \pmod m$، و لذا بنابر

(i.۲.۶)، $r|hk$. همچنین، $b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv ۱ (\mathrm{mod}\, m)$، و لذا $k|rh$. چون $(h,k) = ۱$، در نتیجه $k|r$. به روش مشابه، می‌توانیم نشان دهیم که $h|r$، و بنابراین $(h,k) = ۱$، پس $hk|r$. لذا $r = hk$.

حال فرض می‌کنیم که $(h,k) > ۱$، و فرض می‌کنیم M کوچکترین مضرب مشترکِ h و k باشد. اگر $h = p_۱^{h_۱} \cdots p_t^{h_t}$، و $k = p_۱^{k_۱} \cdots p_t^{k_t}$ آنگاه $M = p_۱^{\alpha_۱} \cdots p_t^{\alpha_t}$، که به‌ازای $i = ۱, ۲, \ldots, t$، $\alpha_i = \max(h_i, k_i)$ ((۱۷.۱) را ببینید). فرض کنیم h' حاصلضرب $p_i^{\alpha_i}$ها به‌ازای iهایی باشد که $h_i \geq k_i$ و فرض می‌کنیم k' حاصلضرب $p_i^{\alpha_i}$ها به‌ازای iهایی باشد که $k_i > h_i$. آشکار است که $h'|h$، $k'|k$، $(h',k') = ۱$ و $h'k' = M$.

بنابر (ii.۳.۶)، مرتبهٔ $a^{h/h'}$ برابر h' است. به همین طریق، مرتبهٔ $b^{k/h'}$ برابر k' است. فرض کنیم $c = a^{h/h'} b^{k/k'}$. چون $(h',k') = ۱$ از قسمت اول برهان نتیجه می‌شود که مرتبهٔ c برابر است با $h'k' = M$.

ریشه‌های اولیه

از (i.۲.۶) نتیجه می‌شود که به‌ازای هر a که با m متباین است $\mathrm{ord}\, a \leq \phi(m)$، و دیده‌ایم که مرتبهٔ a می‌تواند اکیداً کوچکتر از $\phi(m)$ باشد. یک سؤال بدیهی پیش می‌آید: به‌ازای یک پیمانهٔ مفروض m، آیا عدد صحیحی وجود دارد که مرتبه‌اش به‌قدر ممکن بزرگ، یعنی، برابر $\phi(m)$ باشد؟ یک عدد صحیح با این ویژگی یک ریشهٔ اولیهٔ m خوانده می‌شود، اصطلاحی که توسط اویلر معرفی شد، تعریف زیر را داریم.

(۵.۶) تعریف. فرض کنیم m عدد صحیح مثبتی باشد، و $(a,m) = ۱$، اگر مرتبهٔ a به پیمانهٔ m برابر $\phi(m)$ باشد، آنگاه a یک ریشهٔ اولیهٔ m نامیده می‌شود.

توجه به این نکته مهم است که بدانیم معلوم نیست که هر عدد صحیح یک ریشهٔ اولیه داشته باشد. مثلاً اگر $m = ۸$، آنگاه به‌ازای هر عدد صحیح فرد a، $a^۲ \equiv ۱ (\mathrm{mod}\, m)$. لذا به‌ازای هر a که با ۸ متباین باشد $\mathrm{ord}\, a \leq ۲$. اما $\phi(۸) = ۴$، و لذا ۸ هیچ ریشهٔ اولیه ندارد.

بعداً نشان می‌دهیم که هر عدد اول یک ریشهٔ اولیه دارد. این قضیه اولین بار در ۱۷۶۹ توسط ی. ه. لامبرت[1] در رابطه با بررسی بسط اعشاری کسر $۱/p$ بیان شد. در سال ۱۷۷۳، اویلر یک اثبات اساساً درست، ولی ناتمام، ارائه داد که هر عدد اول ریشهٔ اولیه دارد. در ۱۷۸۵، لژاندر نشان داد که اگر p یک عدد اول فرد و d یک مقسوم‌علیه $p - ۱$ باشد، دقیقاً $\phi(d)$ عدد ناهمنهشت وجود دارند که مرتبهٔ آنها به پیمانهٔ p برابر d است ((۱۴.۵) را ببینید)؛ لذا p دارای

1. J. H. Lambert

$\phi(p-1)$ ریشهٔ اولیه است. گاوس نیز اثبات کاملاً مفصل درکتاب تحقیقاتش (۱۸۰۱) به‌دست داده است. تمام اثباتها، از جمله اثباتی که در زیر می‌آید، از قضیهٔ لاگرانژ دربارهٔ تعداد ریشه‌های یک همنهشتی چندجمله‌یی استفاده کرده‌اند. شرح کاملی اعدادی که ریشهٔ اولیه دارند در آخرین بخشِ این فصل خواهد آمد.

(۶.۶) تعریف. فرض کنیم m یک عدد صحیح مثبتی باشد، و u کوچکترین عدد صحیح مثبتی باشد که به‌ازای هر a متباین با m، $a^u \equiv 1 \pmod m$. در این‌صورت u کوچکترین نمای عام m خوانده می‌شود.

توضیح. بنابر (i.۲.۶)، u کوچکترین مضرب مشترک اعداد $\operatorname{rod} a$ است، وقتی که a تمام اعداد صحیح متباین با m از ۱ تا m را طی کند. لذا، بااستفاده مکرر از (۴.۶)، می‌توانیم یک عدد صحیح چون c بیابیم که $\operatorname{ord} c = u$. مرتبهٔ این c ماکسیمم ممکن به پیمانهٔ m است. اگر $u = \phi(m)$، آنگاه c یک ریشهٔ اولیهٔ m است.

(۷.۶) قضیهٔ (لژاندر). هر عدد اول یک ریشهٔ اولیه‌دارد.

برهان. فرض کنیم p یک عدد اول و u کوچکترین نمای عام آن باشد، و فرض می‌کنیم g عدد صحیحی با مرتبهٔ u به پیمانه p باشد. در این‌صورت هر عدد صحیح که با p متباین باشد یک جواب همنهشتی $x^u \equiv 1 \pmod p$ است، لذا همنهشتی $p-1$ جواب دارد. اما بنابر قضیهٔ لاگرانژ، همنهشتی بیشتر از u جواب ندارد. در نتیجه $u = p-1$، و لذا g یک ریشهٔ اولیهٔ p است.

برای اینکه نشان دهیم g یک ریشهٔ اولیه m است قضیهٔ بعد کاملاً مفید است.

(۸.۶) قضیه. اگر $(g,m) = 1$، g یک ریشهٔ اولیهٔ m است اگر و تنها اگر به‌ازای هر مقسوم‌علیه اول q مانند $\phi(m)$، $g^{\phi(m)/q} \not\equiv 1 \pmod m$.

برهان. اگر g یک ریشهٔ اولیهٔ m باشد، به‌ازای هر عدد اول q، $g^{\phi(m)/q} \not\equiv 1 \pmod m$، زیرا اگر $g^{\phi(m)/q} \equiv 1 \pmod m$، مرتبهٔ g کمتر از $\phi(m)$ می‌شود.

بعکس، فرض کنیم $(g,m) = 1$ و g ریشهٔ اولیهٔ m نباشد. در این‌صورت، $d < \phi(m)$ وجود دارد به‌طوری که $d = \operatorname{ord} g$، و بنابر (i.۲.۶)، $d|\phi(m)$. فرض کنیم $\phi(m) = dk$، و q یک مقسوم‌علیه اول k است. بنابراین $\phi(m)/q$ مضربی از d است، و چون $g^d \equiv 1 \pmod m$، در نتیجه $g^{\phi(m)/q} \equiv 1 \pmod m$.

توضیح محاسبه‌یی. قضیهٔ قبل یک‌روش نسبتاً مؤثر برای این آزمون که g یک ریشهٔ اولیه p است به ما می‌دهد هرگاه p یک عدد اول فرد کوچکی باشد، ابتدا $q = ۲$ را اختیار می‌کنیم. اگر $g^{(p-۱)/۲} \equiv ۱ (\mathrm{mod}\, p)$، g ریشهٔ اولیه p نیست. بعد از بحث در مورد $q = ۲$، $g^{(p-۱)/q}$ به پیمانهٔ p را برای سایر مقسوم‌علیه‌های اول $p - ۱$ مانند q محاسبه می‌کنیم. اگر به‌ازای همهٔ این‌گونه qها $g^{(p-۱)/q} \not\equiv ۱ (\mathrm{mod}\, p)$، نتیجه می‌گیریم که g یک ریشهٔ اولیهٔ p است. (اگر p عدد اول بزرگی باشد، ممکن است یافتن عاملهای اول $p - ۱$ بسیار دشوار باشد، لذا قضیهٔ قبل زیاد مفید نیست.)

مثال. به آسانی می‌توان بررسی کرد که ۲ یک ریشهٔ اولیهٔ ۱۹ است. زیرا $\phi(۱۹) = ۱۸$، و تنها مقسوم‌علیه‌های اول ۱۸ عبارت‌اند از ۲ و ۳. لذا بنابر (۸.۶) کافی است نشان دهیم که $۲^{۹} \not\equiv ۱ (\mathrm{mod}\, ۱۸)$ و $۲^{۶} \not\equiv ۱ (\mathrm{mod}\, ۱۸)$. چون ۱۹ به‌صورت $۸k + ۳$ است، ۲ یک نامانده درجهٔ دوم ۱۹ است، و لذا $۲^{۹} \equiv -۱ \not\equiv ۱ (\mathrm{mod}\, ۱۹)$، همچنین، $۳^{۳} \equiv ۸ (\mathrm{mod}\, ۱۹)$، لذا $۳^{۶} \equiv ۷ \not\equiv ۱ (\mathrm{mod}\, ۱۹)$.

آزمون تعیین اول بودن که در زیر می‌آید یک وارون جزئی از قضیهٔ فرماست و بیشتر از همان مطلب قضیهٔ (۸.۶) استفاده می‌کند. این آزمون برای بررسی اول بودن اعداد بزرگی مانند m در حالت خاص که تجزیهٔ $m - ۱$ معلوم باشد به‌کار می‌رود.

(۹.۶) قضیهٔ (لوکا). فرض کنیم $m > ۱$، و فرض می‌کنیم عدد صحیح a وجود داشته باشد به‌طوری که $a^{m-۱} \equiv ۱ (\mathrm{mod}\, m)$ و به‌ازای هر مقسوم‌علیه اول $m - ۱$ مانند q، $a^{(m-۱)/q} \not\equiv ۱ (\mathrm{mod}\, m)$. در این‌صورت m اول است.

برهان. بنابر همان‌استدلالِ قضیهٔ (۸.۶)، می‌توانیم نشان دهیم که a دارای مرتبهٔ $m - ۱$ است. چون $\mathrm{ord}\, a \leq \phi(m) \leq m - ۱$، نتیجه می‌شود که $\phi(m) = m - ۱$، و لذا m اول است.

از آنجا که مرتبهٔ یک ریشهٔ اولیهٔ m برابر $\phi(m)$ است، می‌توان (۲.۶) را مجدداً چنین بیان کرد:

(۱۰.۶) قضیه. اگر g یک ریشهٔ اولیهٔ m باشد، آنگاه $g^s \equiv g^t (\mathrm{mod}\, m)$ اگر و تنها اگر $s \equiv t (\mathrm{mod}\, m)$. لذا $g^s \equiv ۱ (\mathrm{mod}\, m)$ اگر و تنها اگر $\phi(m) | s$.

یکی از مهمترین ویژگیهای یک ریشهٔ اولیهٔ m این است که توانهایش یک دستگاه مخفف مانده‌ها به پیمانهٔ m تشکیل می‌دهند. به‌طور دقیقتر داریم:

(۱۱.۶) قضیه. مجموعهٔ g، $g^۲$، ...، $g^{\phi(m)}$ یک دستگاه مخفف مانده‌ها به پیمانهٔ m است

اگر و تنها اگر g یک ریشهٔ اولیهٔ m باشد. به‌ویژه g، g^2، ...، g^{p-1}، به‌ترتیبی، با اعداد ۱، ۲، ...، $p-1$ همنهشت هستند اگر و تنها اگر g یک ریشهٔ اولیهٔ عدد اول p باشد.

برهان. فرض کنیم g یک ریشهٔ اولیهٔ m باشد، چون مجموعهٔ g، g^2، ...، $g^{\phi(m)}$ دارای $\phi(m)$ عنصر است، کافی است نشان دهیم که هر عنصر با m متباین است و هیچ دو عنصر به پیمانهٔ m همنهشت نیستند. چون $(g,m)=1$، در نتیجه به‌ازای هر $k \geq 1$، $(g^k,m)=1$. همچنین، اگر $g^s \equiv g^t \pmod m$، (۱۰.۶) ایجاب می‌کند که $\phi(m)|s-t$. چون هرکدام از s، t بین ۱ و $\phi(m)$ هستند، بایستی $s=t$. لذا مجموعهٔ مفروض یک دستگاه مخفف مانده‌ها به پیمانهٔ m است.

بعکس، فرض کنیم مجموعهٔ g، g^2، ...، $g^{\phi(m)}$ یک دستگاه مخفف مانده‌ها به پیمانهٔ m باشد. اگر $1 \leq d < \phi(m)$، داریم $g^d \not\equiv g^{\phi(m)} \pmod m$، و لذا مرتبهٔ g برابر $\phi(m)$ است.

هیچ روشِ کلی آسان برای یافتن ریشه‌های اولیهٔ m وجود ندارد حتی اگر وجود آنها معلوم باشد. ولی، اگر یک ریشهٔ اولیه مثلاً g، معلوم باشد، می‌توان به کمک قضیهٔ قبل سایر ریشه‌های اولیه را، که به‌صورت توان مناسبی از g هستند، به‌دست آورد، از این قرار:

(۱۲.۶) قضیه. فرض کنیم g یک ریشهٔ اولیهٔ m باشد. در این‌صورت g^k یک ریشهٔ اولیهٔ m است اگر و تنها اگر $(k,\phi(m))=1$.

برهان. چون $\operatorname{ord} g = \phi(m)$، از (۳.۶) نتیجه می‌شود که $\operatorname{ord} g^k = \phi(m)/(k,\phi(m))$. لذا g^k یک ریشهٔ اولیهٔ m خواهد بود. یعنی $\operatorname{ord} g^k = \phi(m)$، اگر و تنها اگر $(k,\phi(m))=1$.

همان‌گونه که قضیهٔ بعد نشان می‌دهد، اگر یک عدد صحیح مثبت دارای یک ریشهٔ اولیه باشد، معمولاً چندتایی ریشهٔ اولیه دارد. مثلاً، ۱۹ شش ریشهٔ اولیه دارد، و ۱۲۵ دارای ۴۰ ریشهٔ اولیه است. (این مطلب که ۱۲۵ ریشهٔ اولیه دارد از (۲۵.۶) نتیجه می‌شود.)

(۱۳.۶) قضیه. فرض می‌کنیم که m دارای یک ریشهٔ اولیه باشد، آنگاه m دقیقاً $\phi(\phi(m))$ ریشهٔ اولیهٔ ناهمنهشت دارد.

برهان. فرض می‌کنیم g ریشهٔ اولیهٔ m باشد. بنابر (۱۱.۶) و (۱۲.۶)، h یک ریشهٔ اولیهٔ m است اگر و تنها اگر عددی چون $k \leq \phi(m)$ با $(k,\phi(m))=1$ وجود داشته باشد به‌طوری که $h \equiv g^k \pmod m$. از آنجا که به روشنی تعداد $\phi(\phi(m))$ این گونه k وجود دارد، قضیه ثابت می‌شود.

مثال. قبلاً نشان دادیم که ۲ یک ریشهٔ اولیهٔ ۱۹ است. چون $\phi(19) = 18$، از (۱۲.۶) نتیجه می‌شود که تمام ریشه‌های اولیهٔ ۱۹ به‌صورت 2^k هستند، که در آن $1 \le k \le 18$ و $(k, 18) = 1$. دقیقاً تعداد $\phi(18) = 6$ این چنین k وجود دارد، یعنی ۱، ۵، ۷، ۱۱، ۱۳، و ۱۷؛ لذا ریشه‌های اولیهٔ ۱۹ عبارت‌اند از ۲، ۱۳، ۱۴، ۱۵، ۳، و ۱۰.

مطالب قضیه‌های (۱۲.۶) و (۱۳.۶) را می‌توان برای تعیین و یافتن تعداد عناصر با مرتبهٔ d به پیمانهٔ m تعمیم داد.

(۱۴.۶) قضیه. فرض کنیم g یک ریشهٔ اولیهٔ m و d یک مقسوم‌علیه مثبت $\phi(m)$ است. در این‌صورت، g^k دارای مرتبه d به پیمانهٔ m است اگر و تنها اگر k به‌صورت $j\phi(m)/d$ باشد، که در آن $(j, d) = 1$. لذا دقیقاً $\phi(d)$ عنصرِ ناهمنهشت از مرتبهٔ d به پیمانهٔ m وجود دارد.

برهان. بنابر (۳.۶)، مرتبهٔ g^k برابر $\phi(m)/(k, \phi(m))$ است. این مرتبه برابر d است اگر و تنها اگر $(k, \phi(m)) = \phi(m)/d$. فرض کنیم $k = j\phi(m)/d$؛ در این‌صورت $(k, \phi(m)) = (j, d)\phi(m)/d$. این برابر $\phi(m)/d$ است اگر و تنها اگر $(j, d) = 1$. اکنون محاسبهٔ تعداد عناصر با مرتبهٔ d آسان است: چون می‌توانیم فرض کنیم $1 \le k \le \phi(m)$، در نتیجه $1 \le j \le d$، و تعداد $\phi(d)$ این چنین j، متباین با d، وجود دارد.

مانده‌های توانی و اندیسها

فرض کنیم m دارای یک ریشهٔ اولیهٔ g باشد. اگر $(a, m) = 1$، آنگاه (۱۱.۶) ایجاب می‌کند که عدد صحیح یکتای i، با $1 \le i \le \phi(m)$ وجود داشته باشد به‌طوری که $g^i \equiv a \pmod m$. این مطلب اساس تکنیکی است که به ما اجازه می‌دهد تا محاسبات به پیمانهٔ m را که شامل فقط ضرب یا نما هستند ساده کنیم.

در بیشتر مطالب این بخش، m نشانگر عدد صحیح مثبت ثابتی است که ریشهٔ اولیه دارد، و g یک ریشهٔ اولیهٔ ثابتِ m را نشان می‌دهد.

(۱۵.۶) تعریف. فرض کنیم g یک ریشهٔ اولیهٔ m باشد، و $(a, m) = 1$. کوچکترین عدد صحیحِ مثبت i به‌طوری که $g^i \equiv a \pmod m$ اندیس a (به پایهٔ g) خوانده شده و با $\operatorname{ind} a$ نشان داده می‌شود.

دقیقتر بگوییم، اندیس a هم به پیمانهٔ m بستگی دارد و هم به ریشهٔ اولیهٔ m، یعنی g. اما، چون در هر کاربردی m و g ثابت‌اند، نماد $\operatorname{ind} a$ هیچ ابهامی ایجاد نخواهد کرد.

هر چند که مفهوم اندیسها به اویلر برمی‌گردد، ولی گاوس اولین ریاضیدانی بود که یک بحث نظام‌مند از آنها را ارائه داد. گاوس در تحقیقات حسابی اصطلاح اندیس و نماد $\operatorname{ind} a$ را وارد کرد. قضیهٔ زیر مهمترین ویژگیهای اندیسها را بیان می‌کند؛ برهانها نتیجهٔ سادهٔ تعریفِ اندیس و (۲.۶) هستند.

(۱۶.۶) قضیه. فرض کنیم g یک ریشهٔ اولیهٔ m باشد، و $\operatorname{ind} a$ که معرف اندیس a به پایهٔ g

(i) $\operatorname{ind} 1 \equiv 0 \pmod{\phi(m)}$؛ $\operatorname{ind} g \equiv 1 \pmod{\phi(m)}$.

(ii) $a \equiv b \pmod m$ اگر و تنها اگر $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{\phi(m)}$.

(iii) $\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\phi(m)}$.

(iv) به‌ازای هر $k \geq 0$، $\operatorname{ind} a^k \equiv k \operatorname{ind} a \pmod{\phi(m)}$.

شباهتِ زیادِ بین ویژگیهای اندیسها و ویژگیهای متناظرِ لگاریتم روشن است، ولی یک تفاوت مهم وجود دارد: لگاریتم یک عدد وقتی پایه مشخص باشد یکتاست، در حالی‌که اندیسِ یک عدد صحیح مفروض به پیمانهٔ m که به‌کار می‌رود نیز بستگی دارد. لذا اگر پیمانه تغییر کند، بایستی اندیسها مجدداً محاسبه شوند، و بنابراین یک جدول جداگانه از اندیسها برای هر پیمانهٔ مورد نظر لازم است.

با اینکه اصولاً اندیسها فایدهٔ نظری دارند، می‌توان آنها را برای حل معادلات چندجمله‌یی $bx^k \equiv c \pmod m$، که در آنها $(bc, m) = 1$، به‌کار برد. با ضرب این همنهشتی در وارون ضربی b به پیمانهٔ m، می‌توان آن را به یک همنهشتی هم‌ارز به‌صورت $x^k \equiv a \pmod m$ بدل کرد. این مطلب ما را به تعریف زیر، که تعمیم مفهوم ماندهٔ درجهٔ دوم است، راهنمایی می‌کند.

(۱۷.۶) تعریف. فرض کنیم m یک عدد صحیح مثبت باشد و $(a, m) = 1$. در این‌صورت a یک ماندهٔ توانی kام m خوانده می‌شود اگر همنهشتی $x^k \equiv a \pmod m$ حلپذیر باشد. اگر این همنهشتی هیچ جوابی نداشته باشد، a یک ناماندهٔ توانی kام m نامیده می‌شود.

قضیهٔ بعد روشی به‌دست می‌دهد تا بتوانیم بگوییم a یک ماندهٔ توانی kام m است یا نیست.

(۱۸.۶) قضیه. فرض می‌کنیم که m عدد صحیحی باشد که ریشهٔ اولیه دارد، و فرض می‌کنیم $(a, m) = 1$. در این‌صورت همنهشتی $x^k \equiv a \pmod m$ دارای جواب است اگر و تنها اگر

$$a^{\phi(m)/(k,\phi(m))} \equiv 1 \pmod m \qquad (1)$$

اگر همنهشتی $x^k \equiv a \pmod m$ حلپذیر باشد، دقیقاً $(k, \phi(m))$ جواب ناهمنهشت دارد.

برهان. فرض کنیم g یک ریشهٔ اولیهٔ m باشد، و $d = (k, \phi(m))$. با اندیس‌گیری، می‌بینیم که همنهشتی $x^k \equiv a \pmod m$ برقرار است اگر و تنها اگر $k \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\phi(m)}$. بنابر (۷.۲)، این همنهشتی خطی برای $\operatorname{ind} x$ حلپذیر است اگر و تنها اگر $d | \operatorname{ind} a$، و اگر دارای جواب باشد، آنگاه دقیقاً d جواب ناهمنهشت دارد.

برهان با نشان دادن اینکه (۱) برقرار است اگر و تنها اگر $d | \operatorname{ind} a$ کامل می‌شود. با اندیس‌گیری، می‌بینیم که (۱) با $(\phi(m)/d)\operatorname{ind} a \equiv ۰ \pmod{\phi(m)}$ هم‌ارز است، و این برقرار است اگر و تنها اگر $d | \operatorname{ind} a$.

از آنجا که هر پیمانهٔ اول ریشهٔ اولیه دارد، نتیجهٔ زیر را داریم.

(۱۹.۶) نتیجه. فرض کنیم p اول باشد و $(a, p) = ۱$. در این‌صورت a یک ماندهٔ توانی kام p است اگر و تنها اگر

$$a^{(p-۱)/(k,p-۱)} \equiv ۱ \pmod p$$

توضیح محاسبه‌یی. درحالی که نتیجهٔ قبل یک روند کارآمد برای تعیین اینکه آیا a یک ماندهٔ توانی kام p است به‌دست می‌دهد، یافتن یک عدد b به‌طوری که $b^k \equiv a \pmod p$، عملاً بسیار دشوارتر است. ولی اگر $(k, p-۱) = ۱$، محاسبه نسبتاً آسان است.

استفاده از الگوریتم اقلیدسی، اعداد صحیح s و t را می‌یابیم به‌طوری که $sk = t(p-۱)+۱$. بنابراین $a^{sk} = a^{t(p-۱)+۱} \equiv a \pmod p$. لذا a^s جوابی از همنهشتی $x^k \equiv a \pmod p$ است. به روش مشابه، اگر $d = (k, p-۱)$ و عدد b را یافته باشیم به‌طوری که $b^d \equiv a \pmod p$، یافتن جوابی از $x^k \equiv a \pmod p$ آسان‌است. متأسفانه، در حالت کلی به‌ازای یک مقسوم‌علیه d از $p-۱$، حل همنهشتی $x^d \equiv a \pmod p$ آسان نیست.

روشن است که همنهشتی $x^k \equiv ۱ \pmod m$ دارای جواب است، و لذا از (۱۸.۶) نتیجه می‌شود که اگر $k | \phi(m)$، آنگاه دقیقاً $(k, \phi(m)) = k$ جواب دارد. این مطلب تعمیم زیر از قضیهٔ (۸.۴) است.

(۲۰.۶) قضیه. فرض کنیم m دارای ریشهٔ اولیه باشد. اگر $k | \phi(m)$، آنگاه همنهشتی $x^k - ۱ \equiv ۰ \pmod m$ دقیقاً k جواب دارد.

(۲۱.۶) فرع. فرض کنیم m دارای ریشهٔ اولیه باشد. در این‌صورت تعداد مانده‌های توانی kامِ ناهمنهشتِ m عبارت‌اند از $\phi(m)/(k, \phi(m))$.

برهان. بنابر (۱۸.۶)، a یک ماندهٔ توانی kام m است اگر و تنها اگر a جوابی از همنهشتی $x^{\phi(m)/(k,\phi(m))} \equiv ۱ (\mathrm{mod}\, m)$ باشد. اما بنابر (۲۰.۶)، این همنهشتی $\phi(m)/(k,\phi(m))$ جوابِ ناهمنهشت دارد.

اگر همنهشتی $x^k \equiv a (\mathrm{mod}\, m)$ حلپذیر باشد، می‌توان از اندیسها برای یافتن جوابها استفاده کرد. ولی، برای انجام این کار بایستی جدولی از اندیسها را برای پیمانهٔ مفروض محاسبه کنیم (یا در دسترس داشته باشیم). (در یک پیوست تحقیقات حسابی، گاوس جدولی از اندیسها را برای تمام اعداد صحیحِ کمتر از ۱۰۰ که ریشهٔ اولیه دارند محاسبه کرده است. در ۱۸۳۹، ژاکوبی در *Canon Arithmeticus* جدولی از اندیسها برای تمام توانهای اولِ کمتر از ۱۰۰۰ را منتشر کرد.)

مثال زیر این تکنیک را نشان می‌دهد.

مثال. از اندیسها برای یافتن تمام جوابهای $۷x^{۱۰} \equiv ۵ (\mathrm{mod}\, ۱۳)$ استفاده می‌کنیم. ابتدا حل‌پذیری همنهشتی را با استفاده از (۱۸.۶) بررسی می‌کنیم: ابتدا با ضرب هر دو طرف در ۲، همنهشتی هم‌ارز $x^{۱۰} \equiv ۱۰ (\mathrm{mod}\, ۱۳)$ را به‌دست می‌آوریم، و ملاحظه می‌کنیم که $۱۰^{۱۲/(۱۰,۱۲)} = ۱۰^۶ \equiv ۳^۶ = ۲۷^۲ \equiv ۱ (\mathrm{mod}\, ۱۳)$ یا می‌توانستیم به آسانی اندیسها را مستقیماً به‌کار بریم؛ اگر جوابی وجود نداشته باشد، این مطلب بدیهی است، زیرا در این‌صورت یک همنهشتی خطی به‌دست می‌آوریم که حلپذیر نیست.

بررسی کنید که ۲ یک ریشهٔ اولیهٔ ۱۳ است (نشان دهید که $۲^۴$ و $۲^۶$ به پیمانهٔ ۱۳ همنهشت با ۱ نیستند). جدولی از اندیسها به قرار زیر ترتیب می‌دهیم:

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
$\mathrm{ind}\, a$	۱۲	۱	۴	۲	۹	۵	۱۱	۳	۸	۱۰	۷	۶

فرض کنیم y معرف $\mathrm{ind}\, x$ باشد؛ لذا $x \equiv ۲^y (\mathrm{mod}\, ۱۳)$. با اندیس‌گیری در همنهشتی اصلی و کاربرد ویژگیها (۱۶.۶)، همنهشتی هم‌ارز

$$\mathrm{ind}\,(۷x^{۱۰}) \equiv \mathrm{ind}\, ۷ + ۱۰\, \mathrm{ind}\, x \equiv \mathrm{ind}\, ۵ (\mathrm{mod}\, ۱۲)$$

را به‌دست می‌آوریم. مطمئن باشید که پیمانه در همنهشتی خطی $\phi(۱۳) = ۱۲$ است. همنهشتی $۱۰y \equiv ۱۰ (\mathrm{mod}\, ۱۲)$ با $۲y \equiv ۲ (\mathrm{mod}\, ۱۲)$ هم‌ارز است. اکنون می‌توانیم طرفین را بر ۲ تقسیم کنیم، اما پیمانه به $۱۲/(۲, ۱۲) = ۶$ تغییر می‌کند. همنهشتی هم‌ارز $y \equiv ۱ (\mathrm{mod}\, ۶)$ را به‌دست آوریم، و لذا $۱۰y \equiv ۱۰ (\mathrm{mod}\, ۱۲)$ دارای دو جواب $y = ۱, ۷ (\mathrm{mod}\, ۱۲)$ است.

سرانجام، $۲^{۷} \pmod{۱۳}$ یا $x \equiv ۲^{y} \equiv ۲^{۱}$. بنابراین، تنها جوابهای همنهشتی عبارت‌اند از ۲ و ۱۱.

توضیح. ۱. اشاره به این نکته سودمند است که می‌توانیم جدول اندیسها در این مثال را برای یافتن کوچکترین ماندهٔ مثبتِ $۲^{۷}$ (یا در واقع ۲^{j} به‌ازای هر j بین ۱ و ۱۲) به‌کار بریم. اندیس $۲^{۷}$ به‌وضوح ۷ است، و چون جدول نشان می‌دهد که اندیس ۱۱ نیز ۷ است، در نتیجه $۲^{۷} \equiv ۱۱ \pmod{۱۳}$. در واقع، می‌توان جدول اندیسها را برای یافتن کوچکترین ماندهٔ مثبتِ a^{k} به‌ازای هر a که با ۱۳ متباین باشد به‌کار برد. مثلاً، برای یافتن کوچکترین ماندهٔ مثبتِ $۵^{۷}$، از جدول داریم که ۵ دارای اندیس ۹ است، لذا اندیس $۵^{۷}$ همنهشت با ۹×۷ به پیمانهٔ ۱۲ است. لذا $۵^{۷}$ دارای اندیس ۳ است. با استفادهٔ مجدد از جدول، می‌بینیم که ۸ دارای اندیس ۳ است، لذا کوچکترین ماندهٔ مثبت $۵^{۷}$ به پیمانهٔ ۱۳ برابر ۸ است.

۲. اگر در مثال قبل ریشهٔ اولیهٔ متفاوتی به‌کار بریم، مقادیر اندیسها یکی نخواهند بود، ولی همان جوابها را به‌دست خواهیم آورد.

وجود ریشه‌های اولیه

قبلاً دیده‌ایم که هر عدد اول یک ریشهٔ اولیه دارد، و به آسانی دیده می‌شود که ۱ و ۴ نیز ریشهٔ اولیه دارند. برای تعیین اعداد صحیح مثبتی که ریشهٔ اولیه دارند، اکنون مسأله یافتن ریشه‌های اولیهٔ p^{k} و $۲p^{k}$ را با فرض اینکه یک ریشهٔ اولیهٔ عدد اول فرد p معلوم است بررسی می‌کنیم.

(۲۲.۶) قضیه. فرض کنیم p یک عدد اول فرد باشد.

(i) اگر g یک ریشهٔ اولیهٔ p باشد و $g^{p-۱} \not\equiv ۱ \pmod{p^{۲}}$، آنگاه g یک ریشهٔ اولیهٔ $p^{۲}$ است. اگر $g^{p-۱} \equiv ۱ \pmod{p^{۲}}$، آنگاه $g+p$ یک ریشهٔ اولیهٔ $p^{۲}$ است.

(ii) اگر $k \geq ۲$ و g یک ریشهٔ اولیه p^{k} باشد، g یک ریشهٔ اولیه $p^{k+۱}$ است.

برهان. (i) فرض کنیم h مرتبهٔ g به پیمانهٔ $p^{۲}$ باشد؛ در این‌صورت $h|\phi(p^{۲}) = p(p-۱)$. اما $g^{h} \equiv ۱ \pmod{p^{۲}}$ ایجاب می‌کند که $g^{h} \equiv ۱ \pmod{p}$، و چون مرتبهٔ g به پیمانهٔ p برابر $p-۱$ است، بنابر (i.۲.۶) بایستی $p-۱|h$. لذا $h = p-۱$ یا $h = p(p-۱)$. اگر $h = p(p-۱)$، آنگاه g یک ریشهٔ اولیهٔ $p^{۲}$ است. اگر $h = p-۱$، یعنی، اگر $g^{p-۱} \equiv ۱ \pmod{p^{۲}}$، در این‌صورت g یک ریشهٔ اولیهٔ $p^{۲}$ نیست. نشان می‌دهیم که در این حالت $g+p$ یک ریشهٔ اولیهٔ $p^{۲}$ است.

چون $g+p \equiv g \pmod{p}$، پس $g+p$ یک ریشهٔ اولیهٔ p است. استدلال بالا نشان می‌دهد که مرتبهٔ $g+p$ به پیمانهٔ $p^{۲}$ بایستی $p-۱$ یا $\phi(p^{۲})$ باشد. اگر مرتبه $p-۱$ باشد، آنگاه

$(g+p)^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$. با استفاده از قضیهٔ دوجمله‌یی داریم

$$1 \equiv (p+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$$

لذا $p^2 | pg^{p-2}$ و بنابراین $p | g^{p-2}$، یعنی $p|g$، که یک تناقض است زیرا $(p,g) = 1$. لذا مرتبهٔ $g+p$ به پیمانهٔ p^2 برابر $\phi(p^2)$ است، و بنابراین $g+p$ یک ریشهٔ اولیهٔ p^2 است.

(ii) فرض کنیم h مرتبهٔ g به پیمانهٔ p^{k+1} باشد؛ پس $h|\phi(p^{k+1}) = p^k(p-1)$. از آنجا که $g^h \equiv 1 (\mathrm{mod}\, p^{k+1})$ نتیجه می‌شود $g^h \equiv 1 (\mathrm{mod}\, p^k)$ و g یک ریشهٔ اولیهٔ p^k است، لذا بنابر (i.۲.۶)، $\phi(p^k) = p^{k-1}(p-1) | h$. بنابراین یا $h = p^{k-1}(p-1)$ یا $h = p^k(p-1)$. نشان می‌دهیم که $h \neq p^{k-1}(p-1)$.

فرض کنیم $t = \phi(p^{k-1})$؛ بنابر قضیهٔ اویلر $g^t \equiv 1 (\mathrm{mod}\, p^{k-1})$، و بنابراین عددی چون j وجود دارد که $g^t = 1 + jp^{k-1}$. اگر $p|j$، خواهیم داشت $g^t \equiv 1 (\mathrm{mod}\, p^k)$، و این با این مطلب که g یک ریشهٔ اولیهٔ p^k است و لذا به پیمانهٔ p^k دارای مرتبهٔ $\phi(p^k)$ است تناقض دارد. لذا $p \not| j$. چون $tp = \phi(p^k)$، با توجه به قضیهٔ دوجمله‌یی داریم

$$g^{tp} = (1 + jp^{k-1})^p \equiv 1 + jp^k \pmod{p^{k+1}}$$

(در اینجا از $p > 2$ و $k \geq 2$ استفاده می‌کنیم. لذا اولین جملهٔ حذف‌شده در بسط دوجمله‌یی $(p(p-1)/2) j^2 p^{2k-2}$ است و لذا بر p^{k+1} بخشپذیر است هرگاه $p \cdot p^{2k-2} \geq p^{k+1}$، یعنی، اگر $k \geq 2$.)

لذا، چون $p \not| j$، داریم $g^{\phi(p^k)} \not\equiv 1 (\mathrm{mod}\, p^{k+1})$. از این‌رو $h \neq p^{k-1}(p-1)$ و لذا $h = p^k(p-1) = \phi(p^{k+1})$، که ثابت می‌کند g یک ریشهٔ اولیهٔ p^{k+1} است.

مطالب قبلی در مورد ریشه‌های اولیه را در نتیجه زیر خلاصه می‌کنیم، که به‌طور صریح شامل روشی برای یافتن ریشه‌های اولیهٔ هر توان از یک عدد اول فرد p است هرگاه یک ریشهٔ اولیه از p در دست باشد.

(۲۳.۶) نتیجه. فرض کنیم p یک عدد اول فرد باشد.

(i) اگر g یک ریشهٔ اولیهٔ p باشد، آنگاه به‌ازای هر $k \geq 1$، g یک ریشهٔ اولیهٔ p^k است هرگاه $g^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$. اگر $g^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$، آنگاه به‌ازای هر $k \geq 1$، $g+p$ یک ریشهٔ اولیهٔ p^k است.

(ii) اگر g یک ریشهٔ اولیهٔ p^2 باشد، به‌ازای هر $k \geq 1$، g یک ریشهٔ اولیهٔ p^k است.

توضیح. یک ریشهٔ اولیهٔ p لزوماً ریشهٔ اولیهٔ p^2 نیست. مثلاً ۱۴ یک ریشهٔ اولیهٔ ۲۹ است ولی ریشهٔ اولیهٔ $(29)^2$ نیست؛ بررسی کنید که $14^{28} \equiv 1 \pmod{29^2}$ برقرار است. همچنین، ۱۸ یک ریشهٔ اولیهٔ ۳۷ است ولی ریشهٔ اولیهٔ $(37)^2$ نیست، و ۱۹ یک ریشهٔ اولیهٔ ۴۳ است ولی ریشهٔ اولیهٔ $(43)^2$ نیست. این اعداد تنها مثالها با شرط $p < 71$ هستند. (ما به ریشه‌های اولیهٔ p که بین ۱ و $p-1$ واقع‌اند توجه داریم. در غیر این‌صورت، برای هر عدد اول فرد p مثالهایی وجود دارد؛ مثلاً ۷ یک ریشهٔ اولیهٔ ۵ است ولی ریشهٔ اولیهٔ ۲۵ نیست یا ۸ یک ریشهٔ اولیه ۳ است ولی ریشهٔ اولیهٔ ۹ نیست.)

یک احتمال از $1/p - 1$ وجود دارد که یک ریشهٔ اولیهٔ g از p یک ریشهٔ اولیهٔ p^2 باشد (مسأله ۷۳.۶ را ببینید). بنابراین اگر p بزرگ باشد، بسیار غیرمحتمل است که $g^{p-1} \equiv 1 \pmod{p^2}$. از این‌رو، معمولاً درست است که ریشهٔ اولیهٔ مفروض p یک ریشهٔ اولیه p^2 و لذا به‌ازای هر k، یک ریشهٔ اولیهٔ p^k باشد.

(۲۴.۶) قضیه. فرض کنیم p یک عدد اول فرد باشد، و g یک ریشهٔ اولیهٔ p^k باشد. اگر g فرد باشد، آنگاه g یا ریشهٔ اولیهٔ $2p^k$ نیز هست. اگر g زوج باشد، آنگاه $g + p^k$ یک ریشهٔ اولیهٔ $2p^k$ است.

برهان. اگر g فرد باشد، آنگاه به‌ازای هر $j \geq 1$، $g^j \equiv 1 \pmod{2}$. از این‌رو $g^j \equiv 1 \pmod{2p^k}$ اگر و تنها اگر $g^j \equiv 1 \pmod{p^k}$، و لذا مرتبهٔ g به پیمانهٔ $2p^k$ برابر مرتبهٔ g به پیمانهٔ p^k، یعنی $\phi(p^k)$ است. چون $\phi(2p^k) = \phi(p^k)$، g یک ریشهٔ اولیهٔ $2p^k$ است.

اگر g زوج باشد نمی‌تواند یک ریشهٔ اولیهٔ $2p^k$ باشد، زیرا یک ریشهٔ اولیه همواره با پیمانه متباین است. اما $g + p^k$ فرد است و به‌وضوح یک ریشهٔ اولیهٔ p^k است، زیرا همنهشت با g به پیمانه p^k است. لذا بنابر استدلال قبل $g + p^k$ یک ریشهٔ اولیهٔ $2p^k$ است.

مهمترین قضیه‌ها دربارهٔ ریشه‌های اولیه را گاوس ثابت کرده است، که در ۱۸۰۱ با مشخص کردن اعداد صحیح مثبتی که ریشهٔ اولیه دارند، و در زیر می‌آیند، به اوج رسیده است.

(۲۵.۶) قضیه. تنها اعداد صحیح مثبتی که ریشهٔ اولیه دارند عبارت‌اند از ۱، ۲، ۴، p^k و $2p^k$، که p یک عدد اول فرد است.

برهان. ابتدا فرض می‌کنیم که $m > 2$ دارای ریشهٔ اولیه باشد. از (۱۸.۶)، با $d = 2$ نتیجه می‌شود که $x^2 \equiv 1 \pmod{m}$ فقط دو جواب دارد. بنابراین به موجب (۵.۵)، m بایستی ۴، p^k، یا $2p^k$ باشد، که p یک عدد اول فرد است.

برای اثبات عکس، ابتدا توجه می‌کنیم که آشکارا ۱، ۲، و ۴ ریشهٔ اولیه دارند (به‌ترتیب، ۱، ۱، ۳). اگر p یک عدد اول فرد باشد، (۷.۶) ایجاب می‌کند که p دارای ریشهٔ اولیه باشد. لذا بنابر (۲۳.۶) و (۲۴.۶)، p^k و $2p^k$ نیز ریشهٔ اولیه دارند.

مطلب زیر نتیجهٔ ساده‌ای از (۵.۵) و قضیهٔ قبل است.

(۲۶.۶) نتیجه. فرض کنیم $m > 2$. همنهشتی $x^2 \equiv 1 \pmod{m}$ دقیقاً دو جواب دارد (یعنی، ۱ و ۱−) اگر و تنها اگر m دارای ریشهٔ اولیه باشد.

مسأله‌ها و راه‌حلها

مرتبهٔ یک عدد صحیح

۱.۶ (الف) با استفاده از این واقعیت که ۶ یک ریشهٔ اولیهٔ ۴۱ است کوچکترین مانده‌های مثبتِ عامِ عناصرِ دارای مرتبهٔ ۸ به پیمانهٔ ۴۱ را به‌دست آورید.

(ب) تمام اعدادِ کمتر از ۶۱ را که دارای مرتبهٔ ۴ به پیمانهٔ ۶۱ هستند پیدا کنید. (۲ یک ریشهٔ اولیهٔ ۶۱ است.)

حل. (الف) چون ۶ یک ریشهٔ اولیهٔ ۴۱ است، پس مرتبهٔ آن ۴۰ به پیمانهٔ ۴۱ است. اگر $1 \le k \le 40$ آنگاه بنابر (۱۱.۶)، عددی مانند a وجود دارد به‌طوری که $a \equiv b^k \pmod{41}$. اما (۳.۶) ایجاب می‌کند که b^k دارای مرتبهٔ $40/(k, 40)$ باشد. لذا مرتبهٔ b^k برابر ۸ است اگر و تنها اگر $(k, 40) = 5$. اعداد مثبت $k \le 40$ که به‌ازای آنها $(k, 40) = 5$ عبارت‌اند از ۵، ۱۵، ۲۵، و ۳۵. کوچکترین مانده‌های مثبت به پیمانه ۴۱ از 6^5، 6^{15}، 6^{25}، و 6^{35} به‌ترتیب عبارت‌اند از ۲۷، ۳، ۱۴، و ۳۸.

(ب) همانند استدلال (الف)، 2^k دارای مرتبهٔ $60/(k, 60)$ به پیمانهٔ ۶۱ است. لذا 2^k دارای مرتبهٔ ۴ است اگر و تنها اگر $(k, 60) = 15$، یعنی $k = 15$ یا $k = 45$. کوچکترین مانده‌های مثبتِ 2^{15} و 2^{45} به پیمانهٔ ۶۱ عبارت‌اند از ۱۱ و ۵۰.

۲.۶ اگر p عدد اولی فرد باشد، ثابت کنید که مرتبهٔ a به پیمانهٔ p برابر ۲ است اگر و تنها اگر $a \equiv -1 \pmod{p}$.

حل. آشکار است که اگر $a \equiv -1 \pmod{p}$، آنگاه a دارای مرتبهٔ ۲ است. بعکس، اگر a دارای مرتبهٔ ۲ باشد، a جوابی است از معادلهٔ همنهشتی $x^2 \equiv 1 \pmod{p}$. اما این همنهشتی فقط دو جواب دارد، یعنی، ۱ (که دارای مرتبهٔ ۱ است) و ۱−.

۳.۶ اثبات یارد کنید: فرض کنید p عدد اول فردی باشد و $a \equiv \pm ۱ (\mathrm{mod}\, p)$. اگر $a^r \equiv ۱ (\mathrm{mod}\, p)$، با $r < p - ۱$، آنگاه $r | p - ۱$.

حل. یافتن مثالهای نقض برای این حکم آسان است. مثلاً، فرض کنیم $p = ۱۳$، و فرض می‌کنیم a عنصری از مرتبهٔ ۴، نظیر ۵ باشد. در این‌صورت $a^۴ \equiv ۱ (\mathrm{mod}\ ۱۳)$ و لذا $a^۸ \equiv ۱ (\mathrm{mod}\ ۱۳)$، اما ۱۲×۸.

توجه. قضیهٔ (۲.۶) گویای این حقیقت است که مرتبهٔ a عدد $p - ۱$ را عاد می‌کند.

۴.۶ فرض کنیم m یک عدد صحیح مثبت باشد، و فرض می‌کنیم $ab \equiv ۱ (\mathrm{mod}\, m)$. ثابت کنید $\mathrm{ord}\, a = \mathrm{ord}\, b$.

حل. از $ab \equiv ۱ (\mathrm{mod}\, m)$ نتیجه می‌شود که $(a, m) = ۱$، لذا مرتبهٔ a وجود دارد. برای اینکه نشان دهیم a و b دارای یک مرتبه‌اند، طرفین همنهشتی $ab \equiv ۱ (\mathrm{mod}\, m)$ را به‌توان k می‌رسانیم. پس $a^k b^k \equiv ۱ (\mathrm{mod}\, m)$. در نتیجه $a^k \equiv ۱ (\mathrm{mod}\, m)$ اگر و تنها اگر $b^k \equiv ۱ (\mathrm{mod}\, m)$. لذا کوچکترین عدد مثبت k به‌طوری که $a^k \equiv ۱ (\mathrm{mod}\, m)$ همان کوچکترین عدد مثبت k است که $b^k \equiv ۱ (\mathrm{mod}\, m)$. لذا $\mathrm{ord}\, a = \mathrm{ord}\, b$.

۵.۶ فرض کنید $n > ۲$. ثابت کنید $\phi(۲^n - ۱)$ بر n بخشپذیر است. (راهنمایی: ثابت کنید که مرتبهٔ ۲ به پیمانهٔ $۲^n - ۱$ برابر n است.)

حل. آشکار است که $۲^n \equiv ۱ (\mathrm{mod}\ ۲^n - ۱)$، و اگر $۱ \le k < n$، آنگاه $۲^k < ۲^n$ $۲ \le$، لذا $۲^k \not\equiv ۱ (\mathrm{mod}\ ۲^n - ۱)$. از تعریفِ مرتبه نتیجه می‌شود که ۲ دارای مرتبهٔ n به پیمانهٔ $۲^n - ۱$ است، و لذا (i.۲.۶) ایجاب می‌کند که $n | \phi(۲^n - ۱)$.

۶.۶ فرض کنید g یک ریشهٔ اولیه عدد اول p باشد. اگر $p \equiv ۳ (\mathrm{mod}\ ۴)$، ثابت کنید که مرتبهٔ $-g$ به پیمانهٔ p برابر است با $(p - ۱)/۲$. (راهنمایی: از ملاک اویلر، یعنی $g^{(p-۱)/۲} \equiv -۱ (\mathrm{mod}\, p)$ استفاده کنید.)

حل. داریم $g^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$. پس $p | g^{p-۱} - ۱ \equiv (g^{(p-۱)/۲} - ۱)(g^{(p-۱)/۲} + ۱)$ اما چون $\mathrm{ord}\, j = p - ۱$، پس $g^{(p-۱)/۲} \not\equiv ۱ (\mathrm{mod}\, p)$، یعنی $p \nmid (g^{p-۱/۲} - ۱)$ و چون p اول است، پس $p | g^{(p-۱)/۲} + ۱$، یعنی $g^{(p-۱)/۲} \equiv -۱ (\mathrm{mod}\, p)$ (۱). از (۱)، $-g \equiv g^{(p-۱)/۲} g (\mathrm{mod}\, p)$. اگر $p = ۴k + ۳$، داریم $-g \equiv g^{۲k+۲} (\mathrm{mod}\, p)$. اما

$(۲k+۲, ۴k+۲) = ۲$، لذا از (۳.۶) نتیجه می‌شود که $\operatorname{ord} g^{۲k+۲} = (p-۱)/۲$، و بنابراین مرتبهٔ $-g$ برابر $(p-۱)/۲$ است.

۷.۶ فرض کنید p عدد اولی به‌صورت $۴k+۳$ باشد. اگر مرتبهٔ $-a$ به پیمانهٔ p برابر $(p-۱)/۲$ باشد، با استفاده از (۴.۶) نشان دهید که a یک ریشهٔ اولیهٔ p است.

حل. چون مرتبهٔ -۱ برابر ۲ است و ۲ با $(p-۱)/۲$ متباین است، از (۴.۶) نتیجه می‌شود که $a = (-۱)(-a)$ دارای مرتبهٔ $p-۱$ است، و لذا a یک ریشهٔ اولیهٔ p است.

۸.۶ گیریم p یک عدد اول فرد باشد، و فرض می‌کنیم $\operatorname{rod}_p a = ۲k$. ثابت کنید $a^k \equiv -۱ (\operatorname{mod} p)$.

حل. چون $a^{۲k} \equiv ۱ (\operatorname{mod} p)$، پس a^k یک جواب همنهشتی $x^۲ \equiv ۱ (\operatorname{mod} p)$ است. این همنهشتی دو جواب ۱ و -۱ دارد. چون a دارای مرتبهٔ $۲k$ است، $a^k \not\equiv ۱ (\operatorname{mod} p)$، از اینجا نتیجه می‌شود که $a^k \equiv -۱ (\operatorname{mod} p)$.

۹.۶ اثبات یا رد کنید: اگر $(a, m) = ۱$ و $\operatorname{ord}_m a = m-۱$، آنگاه m اول است.

حل. قضیه درست است. مرتبهٔ a نمی‌تواند بزرگتر از $\phi(m)$ باشد. چون مرتبهٔ a برابر $m-۱$ است، در نتیجه $m-۱ \le \phi(m)$، و لذا $\phi(m) = m-۱$ و این تساوی اول بودن m را ایجاب می‌کند (مسأله ۵۹.۳ را ببینید).

۱۰.۶ فرض کنید $(a, m) = ۱$، اگر $a^h \equiv ۱ (\operatorname{mod} m)$ و $a^k \equiv ۱ (\operatorname{mod} m)$، ثابت کنید $a^{(h,k)} \equiv ۱ (\operatorname{mod} m)$.

حل. بنابر (i.۲.۶)، مرتبهٔ a اعداد h و k را می‌شمارد، و لذا (h, k) را می‌شمارد. از این‌رو مجدداً بنابر (i.۲.۶)، $a^{(h,k)} \equiv ۱ (\operatorname{mod} m)$.

۱۱.۶ اثبات یا رد کنید: اگر $d | \phi(m)$، آنگاه عنصری از مرتبهٔ d به پیمانهٔ m وجود دارد.

حل. این حکم در حالت کلی درست نیست. مثلاً، فرض کنیم $m = ۱۲$. به آسانی دیده می‌شود که اگر $(a, ۱۲) = ۱$، آنگاه $a^۲ \equiv ۱ (\operatorname{mod} ۲)$، لذا به‌ازای هر a، $\operatorname{ord} a \le ۲$. به‌ویژه، چون $\phi(۱۲) = ۴$ ، لذا هیچ عنصری از مرتبهٔ $\phi(۱۲)$ وجود ندارد.

۱۲.۶ اگر $\operatorname{ord}_m a = ۴r$، آنگاه $\operatorname{ord}_m(-a) = ۴r$.

حل. چون $(-a)^{۴r} = a^{۴r} \equiv ۱ (\mathrm{mod}\, m)$. (i.۲.۶) ایجاب می‌کند که $\mathrm{ord}\,(a-۱) | ۴r$. اگر $\mathrm{ord}\,(-a) = ۲s$، $a^{۲s} = ((-۱)(-a))^{۲s} = (-a)^{۲s} \equiv ۱ (\mathrm{mod}\, m)$ و $۲s < ۴r$. آنگاه $\mathrm{ord}\, a = ۴r$ تناقض دارد. اگر مرتبهٔ $-a$ عدد فرد t باشد، آنگاه $t | ۴r$ و لذا $t | r$، و بنابراین $(-a)^{r} \equiv ۱ (\mathrm{mod}\, m)$. در نتیجه $a^{۲r} \equiv (-a)^{۲r} \equiv ۱ (\mathrm{mod}\, m)$، که مجدداً با $\mathrm{ord}\, a = ۴r$ تناقض دارد.

◁ **۱۳.۶** گیریم $a_۱$، $a_۲$، ...، a_r یک دستگاه مخفف مانده‌ها به پیمانهٔ m باشد، و فرض می‌کنیم $n \geq ۱$. ثابت کنید $a_۱^n$، $a_۲^n$، ...، a_r^n یک دستگاه مخفف مانده‌ها به پیمانهٔ m است اگر و تنها اگر $(n, \phi(m)) = ۱$.

حل. آشکار است که هر a_i^n نسبت به m اول است؛ لذا کافی است ثابت کنیم که $a_۱^n$، $a_۲^n$، ...، a_r^n به پیمانهٔ m ناهمنهشت‌اند. ابتدا نشان می‌دهیم که اگر $(n, \phi(m)) = ۱$ و $a^n \equiv b^n (\mathrm{mod}\, m)$، آنگاه $a \equiv b (\mathrm{mod}\, m)$. فرض کنیم s و t اعداد صحیح نامنفی باشند به‌طوری که $ns = t\phi(m) + ۱$. در این‌صورت داریم $a^{ns} \equiv b^{ns} (\mathrm{mod}\, m)$. اما $a^{ns} \equiv a^{t\phi(m)+۱} \equiv a (\mathrm{mod}\, m)$، و به همین دلیل $b^{ns} \equiv b (\mathrm{mod}\, m)$، و لذا $a \equiv b (\mathrm{mod}\, m)$.

اکنون نشان می‌دهیم که اگر $(n, \phi(m)) \neq ۱$، آنگاه a و b وجود دارند که نسبت به m اول و به پیمانهٔ m ناهمنهشت‌اند، ولی $a^n \equiv b^n (\mathrm{mod}\, m)$. فرض کنیم p یک مقسوم‌علیه اول $(n, \phi(m))$ باشد. نشان می‌دهیم عدد صحیحی وجود دارد که مرتبه‌اش به پیمانهٔ m برابر p است. روشن است که -۱ دارای مرتبهٔ ۲ است، لذا می‌توانیم فرض کنیم p فرد است. فرض کنیم $m = \prod p_i^{a_i}$؛ در این‌صورت عددی چون i وجود دارد به‌طوری که $p | \phi(p_i^{a_i})$. اگر g یک ریشهٔ اولیهٔ $p_i^{a_i}$ باشد، آنگاه مرتبهٔ g به پیمانهٔ m مضربی از مرتبهٔ g به پیمانهٔ $p_i^{a_i}$ است، و لذا مرتبهٔ g به پیمانهٔ m مضربی از p است. بنابر (i.۳.۶)، می‌توانیم عدد صحیحی چون a بیابیم که $\mathrm{ord}_m a = p$. فرض کنیم $b = ۱$؛ در این‌صورت $a^n = ۱ = b^n (\mathrm{mod}\, m)$، ولی $a \not\equiv b (\mathrm{mod}\, m)$.

توضیح. اگر m دارای ریشهٔ اولیه باشد، می‌توان برهانی به مراتب کوتاهتر ارائه داد، تمرین ۶۵.۶ را ببینید.

مانده‌های توانی و اندیسها

۱۴.۶ (الف) بدون یافتن جوابها، نشان دهید که $x^۶ \equiv ۸ (\mathrm{mod}\, ۸۹)$ حلپذیر است. معادله چند جواب دارد؟

(ب) با استفاده از این حقیقت که ۳ یک ریشهٔ اولیهٔ ۸۹ است، کوچکترین ماندهٔ مثبت جوابهای $x^{۶} \equiv ۸ (\mathrm{mod}\ ۸۹)$ را پیدا کنید.

حل. (الف) بنابر (۱۸.۶)، این همنهشتی حلپذیراست اگر و تنها اگر $۸^{۴۴} \equiv ۱ (\mathrm{mod}\ ۸۹)$. محاسبهٔ مستقیم $۸^{۴۴}$ به پیمانهٔ ۸۹ قدری ناخوشایند است، و می‌توان از آن صرف‌نظرکرد. چون ۸۹ به‌صورت $۸k+۱$، ۲ یک ماندهٔ درجهٔ دوم ۸۹ است، و لذا بنابر ملاک اویلر، $۲^{۴۴} \equiv ۱ (\mathrm{mod}\ ۸۹)$. لذا $۸^{۴۴} = ۲^{۴۴ \times ۳} \equiv ۱ (\mathrm{mod}\ ۸۹)$ و در نتیجه $x^{۶} \equiv ۸ (\mathrm{mod}\ ۸۹)$ دارای جواب است. بنابر (۱۸.۶) دارای $۲ = (۶, \phi(۸۹))$ جواب است.

(ب) بنابر (۱۸.۶)، x جوابی از همنهشتی است اگر و تنها اگر $۶\mathrm{ind}\, x \equiv \mathrm{ind}\, ۸ (\mathrm{mod}\ ۸۸)$. اکنون می‌خواهیم $\mathrm{ind}\, ۸ = ۳\,\mathrm{ind}\, ۲$ را محاسبه کنیم. بررسی تساوی $\mathrm{ind}\, ۲ = ۱۶$ آسان است، لذا همنهشتی $۶k \equiv ۳ \times ۱۶ (\mathrm{mod}\ ۸۸)$ را حل می‌کنیم؛ این همنهشتی دارای جواب $k \equiv ۸ (\mathrm{mod}\ ۴۴)$ است. بنابراین جوابهای همنهشتی اصلی عبارت‌اند از $x \equiv ۳^{۸} (\mathrm{mod}\ ۸۹)$ و $x \equiv ۳^{۵۲} (\mathrm{mod}\ ۸۹)$. کوچکترین ماندهٔ مثبتِ جواب اولی ۶۴ است. اما اگر x یک جواب باشد، $-x$ نیز جواب است، لذا کوچکترین ماندهٔ مثبت جواب دوم ۲۵ است.

۱۵.۶ همنهشتی $x^{۵} \equiv ۲ (\mathrm{mod}\ ۷۳)$ را حل کنید. (راهنمایی: توضیح محاسبه‌ای بعد از (۱۹.۶) را ببینید.)

حل. چون ۵ نسبت به ۷۲ اول است، می‌توانیم اعداد صحیح مثبت s و t را بیابیم به‌طوری که $۵s = ۷۲t + ۱$، مثلاً، $s = ۲۹$ و $t = ۲$. لذا $۲^{۵s} = ۲^{۷۲t+۱} \equiv ۲ (\mathrm{mod}\ ۷۳)$، و بنابراین ۲^{s} جوابی از همنهشتی $x^{۵} \equiv ۲ (\mathrm{mod}\ ۷۳)$ است . لذا $۲^{۲۹}$ یک جواب همنهشتی داده شده است و چون $۱ = (۵, ۷۲)$، این جواب تنها جواب مسأله است. یک محاسبهٔ ساده نشان می‌دهد که کوچکترین ماندهٔ مثبت $۲^{۲۹}$ به پیمانهٔ ۷۳ برابر ۴ است.

۱۶.۶ با استفاده از جدولی از اندیسها کوچکترین ماندهٔ مثبت جوابهای $۹x^{۸} \equiv ۸ (\mathrm{mod}\ ۱۷)$ را پیدا کنید.

حل. ثابت می‌شود که ۳ یک ریشهٔ اولیهٔ ۱۷ است. این مطلب از جدول اندیسهای زیر روشن است:

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶
$\mathrm{ind}\, a$	۱۶	۱۴	۱	۱۲	۵	۱۵	۱۱	۱۰	۲	۳	۷	۱۳	۴	۹	۶	۸

اگر اندیس‌گیری کنیم، همنهشتی $۹x^{۸} \equiv ۸ (\mathrm{mod}\ ۱۷)$ به

$$\mathrm{ind}\, ۹ + ۸\, \mathrm{ind}\, x \equiv \mathrm{ind}\, ۸ (\mathrm{mod}\ ۱۶)$$

تبدیل می‌شود. با توجه به جدول بالا، داریم $۸\, \mathrm{ind}\, x \equiv ۱۰ (\mathrm{mod}\ ۱۶)$ یا، هم‌ارز با آن، $\mathrm{ind}\, x \equiv ۱ (\mathrm{mod}\ ۲)$. لذا جوابهای آن اعداد صحیح هستند که اندیس فرد دارند. با توجه به جدول فوق، کوچکترین مانده‌های مثبت جوابها عبارت‌اند از ۳، ۱۰، ۵، ۱۱، ۱۴، ۷، ۱۲، و ۶.

۱۷.۶ همنهشتی $۴x^{۱۲} \equiv -۲۳ (\mathrm{mod}\ ۲۹)$ دارای چهار جواب است. با استفاده از یک ریشهٔ اولیهٔ ۲۹ کوچکترین ماندهٔ مثبت سه‌تایی از آنها را پیدا کنید.

حل. برای اینکه ببینید ۲ یک ریشهٔ اولیهٔ ۲۹ است مسألهٔ ۳۴.۶ را ببینید. برای اجتناب از تهیهٔ یک جدول اندیس کامل برای ۲۹، چند کار مقدماتی روی همنهشتی مفروض انجام می‌دهیم. چون $۶ (\mathrm{mod}\ ۲۹) \equiv -۲۳$، همنهشتی هم‌ارز با آن، $۴x^{۱۲} \equiv ۶ (\mathrm{mod}\ ۲۹)$ را به‌دست می‌آوریم. طرفین را بر ۲ تقسیم می‌کنیم، به جای، ۳ ، -۲۶ را می‌گذاریم، مجدداً بر ۲ تقسیم می‌کنیم، و به جای -۱۳، ۱۶ را می‌گذاریم و همنهشتی هم‌ارز $x^{۱۲} \equiv ۱۶ (\mathrm{mod}\ ۲۹)$ را به‌دست می‌آوریم. با اندیس‌گیری، همنهشتی $۱۲\, \mathrm{ind}\, x \equiv ۴ (\mathrm{mod}\ ۲۸)$، یا هم‌ارز با آن، $۳\, \mathrm{ind}\, x \equiv ۱ (\mathrm{mod}\ ۷)$ را به‌دست می‌آوریم. بنابراین، $\mathrm{ind}\, x \equiv ۵ (\mathrm{mod}\ ۷)$، و لذا x دارای اندیس ۵، ۱۲، ۱۹، یا ۲۶ است. یک عنصر با اندیس ۵ عبارت است از $۲^{۵}$، که دارای کوچکترین ماندهٔ مثبت ۳ است. برای محاسبهٔ $۲^{۱۲}$، توجه می‌کنیم که $۲^{۷} \equiv ۳ \times ۱۲ \equiv ۷ (\mathrm{mod}\ ۲۹)$. برای دو جوابِ دیگر، ملاحظه می‌کنید که اگر x یک جواب باشد، $-x$ نیز یک جواب خواهد بود. لذا جوابها عبارت‌اند از ۳، ۷، ۲۶، و ۲۲. (توجه. هر جواب متوالی را می‌توان با ضرب یک جواب مفروض در $۲^{۷} \equiv ۱۲ (\mathrm{mod}\ ۲۹)$ به‌دست آورد، زیرا تفاوت هر دو نمای متوالی برابر ۷ است.)

۱۸.۶ تعیین کنید که آیا $x^{۵} \equiv ۶ (\mathrm{mod}\ ۱۰۱)$ جواب دارد یا نه. اگر جواب وجود دارد، آنها را پیدا کنید. (راهنمایی: ابتدا کوچکترین ماندهٔ مثبت $۲^{۷۰}$ به پیمانهٔ ۱۰۱ را به‌دست آورید.)

حل. کوچکترین ماندهٔ مثبت $۲^{۷۰}$ به پیمانهٔ ۱۰۱ را محاسبه می‌کنیم، ۶ به‌دست می‌آید. لذا $۲^{۱۴}$ جوابی از همنهشتی مفروض است، در نتیجه وجود جواب ثابت می‌شود. اگر ۲ یک ریشهٔ اولیه باشد، با اندیس‌گیری همنهشتی هم‌ارز $۵\, \mathrm{ind}\, x \equiv ۷۰ (\mathrm{mod}\ ۱۰۰)$ را به‌دست می‌آوریم، و لذا $\mathrm{ind}\, x$ عبارت است از ۱۴، ۳۴، ۵۴، ۷۴، یا ۹۴. پس x برابر است با ۲۲، ۷۰، ۸۵، ۹۶، یا ۳۰. (در واقع، لازم نیست که بدانیم ۲ یک ریشهٔ اولیه است. زیرا، بنابر (۱۸.۶)، می‌توانیم ببینیم که اگر همنهشتی دارای جواب باشد، ۵ جواب دارد، و ما ۵ جواب را یافته‌ایم.)

۱۹.۶ با استفاده از این واقعیت که ۲ یک ریشهٔ اولیهٔ ۵۹ است، کوچکترین مانده‌های مثبتِ همهٔ جوابهای $5x^5 \equiv -16 \pmod{59}$ را به‌دست آورید.

حل. چون $64 \equiv 5 \pmod{59}$، پس $\operatorname{ind} 5 = 6$. همچنین چون ۲ یک ناماندهٔ درجهٔ دوم ۵۹ است، داریم $-1 \equiv 2^{29} \pmod{59}$؛ پس ۱− دارای اندیس ۲۹ و لذا ۱۶− دارای اندیس $29 + 4 = 33$ است. با اندیس‌گیری، همنهشتی همارز $6 + 5 \operatorname{ind} x \equiv 33 \pmod{58}$، یا $5 \operatorname{ind} x \equiv 27 \pmod{58}$ را به‌دست می‌آوریم. از حل همنهشتی اخیر داریم $\operatorname{ind} x \equiv 17 \pmod{58}$. لذا $x \equiv 2^{17} \pmod{59}$ تنها جواب است؛ کوچکترین ماندهٔ مثبت جواب x، عبارت است از ۳۳.

۲۰.۶ نشان دهید که $x^5 \equiv 26 \pmod{71}$ جواب دارد، و کوچکترین ماندهٔ مثبت جوابها را به‌دست آورید. (راهنمایی: ۷ یک ریشهٔ اولیهٔ ۷۱ است و $\operatorname{ind} 26 = 45$.)

حل. به آسانی ثابت می‌شود که $7^{45} \equiv 26 \pmod{71}$. ابتدا ملاحظه می‌کنیم که ۷ یک ناماندهٔ ۷۱ است، و لذا $7^{35} \equiv -1 \pmod{71}$. اکنون فقط لازم است که به 7^{10} توجه کنیم. چون $7^3 \equiv -12 \pmod{71}$، داریم $7^6 \equiv 2 \pmod{71}$، $7^9 \equiv -24 \pmod{71}$، و لذا $7^{10} \equiv -168 \equiv -26 \pmod{71}$.

چون $7^{45} \equiv 26 \pmod{71}$، آشکاراست که 7^9 جوابی از همنهشتی $x^5 \equiv 26 \pmod{71}$ است. بنابر (۱۸.۶)، این همنهشتی ۵ جواب وجود دارد. با کاربرد اندیسها می‌توانیم همنهشتی همارز $5 \operatorname{ind} x \equiv 45 \pmod{70}$، یعنی $\operatorname{ind} x \equiv 9 \pmod{14}$ را به‌دست آوریم؛ بنابراین $\operatorname{ind} x$ برابر است با ۹، ۲۳، ۳۷، ۵۱، یا ۶۵. چون $7^{14} \equiv 54 \pmod{71}$، می‌توانیم نسبتاً سریع محاسبه کنیم که کوچکترین مانده‌های مثبت جوابها عبارت‌اند از ۴۷، ۵۳، ۲۲، ۵۲، و ۳۹.

۲۱.۶ با استفاده از جدولی از اندیسها برای یک ریشهٔ اولیهٔ ۱۹ کوچکترین مانده‌های مثبت جوابهای همنهشتیهای زیر را بیابید.

(الف) $8x^4 \equiv 3 \pmod{19}$؛ (ب) $5x^3 \equiv 2 \pmod{19}$؛ (ج) $x^7 \equiv 1 \pmod{19}$.

حل. با استفاده از ریشهٔ اولیهٔ ۲ جدول زیر را به‌دست می‌آوریم:

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸
$\operatorname{ind} a$	۱۸	۱	۱۳	۲	۱۶	۱۴	۶	۳	۸	۱۷	۱۲	۱۵	۵	۷	۱۱	۴	۱۰	۹

(الف) با اندیس‌گیری، همنهشتی همارز $4 \operatorname{ind} x + 3 \equiv 13 \pmod{18}$ را به‌دست می‌آوریم،

یعنی $\text{ind}\, x \equiv ۵ \pmod ۹$. ۲ لذا ازاین‌رو $\text{ind}\, x \equiv ۷ \pmod ۹$، و لذا $\text{ind}\, x$ برابر ۷ یا ۱۶ است. پس جوابها عبارت‌اند از $۲^۷$ و $۲^{۱۶}$، و لذا کوچکترین مانده‌های مثبت جوابها عبارت‌اند از ۱۴ و ۵.

(ب) همنهشتی هم‌ارز $۳\,\text{ind}\, x \equiv ۱ \pmod{۱۸}$ را به‌دست می‌آوریم. از این‌رو $\text{ind}\, x \equiv ۱ \pmod ۶$، و لذا $\text{ind}\, x$ برابر است با ۱، ۷، یا ۱۳. از اینجا جوابهای ۲، ۱۴، و ۳ به‌دست می‌آیند.

(ج) همنهشتی هم‌ارز $۷\,\text{ind}\, x \equiv ۱۸ \pmod{۱۸}$ را به‌دست می‌آوریم. لذا x دارای اندیس ۱۸ است، که مقدار ۱ را برای کوچکترین ماندهٔ مثبت تنها جواب به‌دست می‌دهد.

۲۲.۶ با استفاده از ریشه‌های اولیه و ویژگیهای اندیسها باقیماندهٔ تقسیم $۵^{۴۳}$ بر ۱۹ را به‌دست آورید. (راهنمایی: از جدول مسألهٔ قبل استفاده کنید.)

حل. برای استفاده از اندیسها، ملاحظه می‌کنیم که ۲ یک ریشهٔ اولیهٔ ۱۹ است، و از جدول مسأله ۲۱.۶ استفاده می‌کنیم. ملاحظه می‌کنید که $\text{ind}\, ۵ = ۱۶$؛ اگر $x = ۵^{۴۳}$، آنگاه $\text{ind}\, x = ۱۶ \times ۴۳ \pmod{۱۸}$، (ii.۱۶.۶)، و لذا بنابر $x \equiv ۲^{۱۶۴۳}$، چون $۱۶ \equiv -۲ \pmod{۱۸}$ و $-۲ \equiv ۴^۲ \pmod{۱۸}$، داریم $\text{ind}\, x = ۱۶$ و لذا باقیماندهٔ مورد نظر ۵ است.

۲۳.۶ فرض کنید p یک عدد اول فرد باشد.

(الف) ثابت کنید که $x^۴ \equiv -۱ \pmod p$ حلپذیر است اگر و تنها اگر $p \equiv ۱ \pmod ۸$.

(ب) ثابت کنید که بی‌نهایت عدد اول به‌صورت $۸k + ۱$ وجود دارد. (راهنمایی: فرض کنید $p_۱$، $p_۲$، ...، p_n اعداد اول به‌صورت $۸k + ۱$ باشند، و $(۲p_۱p_۲ \cdots p_n)^۴ + ۱$ را در نظر بگیرید.)

حل. (الف) بنابر (۱۹.۶)، این همنهشتی جواب دارد اگر و تنها اگر

$$(-۱)^{(p-۱)/(۴,p-۱)} \equiv ۱ \pmod p$$

یعنی، اگر و تنها اگر $(p-۱)/(۴, p-۱)$ زوج باشد. فرض کنیم $p = ۸k + r$، که در آن r مساوی ۱، ۳، ۵، یا ۷ است. در این‌صورت $(p-۱)/(۴, p-۱)$ به‌ترتیب، برابر است با $۲k$، $۴k + ۱$، و $۴k + ۳$، و لذا زوج است اگر و تنها اگر $r = ۱$.

(ب) فرض کنیم $p_۱$، $p_۲$، ...، p_n اعداد اولی به‌صورت $۸k + ۱$ باشند، و قرار می‌دهیم $N = (۲p_۱p_۲ \cdots p_n)^۴ + ۱$. فرض می‌کنیم p یک عامل اول N باشد؛ چون N فرد است، p نیز فرد است. لذا $۲p_۱p_۲ \cdots p_n$ جوابی از همنهشتی $x^۴ + ۱ \equiv ۰ \pmod p$ است، و از آنجا، بنابر (الف)، p به‌صورت $۸k + ۱$ است. اما آشکار است که p نمی‌تواند یکی از p_iها باشد. لذا به‌ازای هر n عدد اول به‌صورت $۸k + ۱$ وجود دارد، و بنابراین بی‌نهایت عدد اول این چنینی وجود دارد.

توضیح. اصولاً، با برهانی مشابه نشان داده می‌شود که اگر p عدد اولی فرد باشد، آنگاه همنهشتی $x^{۲^{n-۱}} \equiv -۱ (\mathrm{mod}\, p)$ حلپذیر است اگر و تنها اگر $p \equiv ۱ (\mathrm{mod}\, ۲^n)$. در نتیجه به‌ازای هر عدد صحیح مثبت n، تعداد نامتناهی عدد اول به‌صورت $۲^n k + ۱$ وجود دارد.

۲۴.۶ اثبات یا رد کنید: اگر p عدد اولی به‌صورت $۳k+۲$ باشد، آنگاه به‌ازای هر عدد صحیح مثبت کوچکتر از p مانند a، a یک ماندهٔ درجهٔ سوم p است (یعنی، $x^۳ \equiv a (\mathrm{mod}\, p)$ حلپذیر است).

حل. این حکم درست است. بنابر (۱۹.۶)، a یک ماندهٔ درجهٔ سوم $p = ۳k + ۲$ است اگر و تنها اگر $a^{(p-۱)/(۳,p-۱)} \equiv ۱ (\mathrm{mod}\, p)$. اما $(۳, p-۱) = (۳, ۳k+۱) = ۱$، و اگر $(a, p) = ۱$، آنگاه بنابر قضیهٔ فرما، $a^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$.

۲۵.۶ اگر $p = ۳k + ۱$ اول باشد، ثابت کنید که درست یک سوم اعداد صحیح ۱، ۲، ...، $p-۱$ مانده‌های درجهٔ سوم p هستند.

حل. بنابر (۲۱.۶)، تعداد مانده‌های درجهٔ سوم p (در یک دستگاه مخفف مانده‌ها) عبارت است از $\phi(p)/(۳, \phi(p)) = ۳k/(۳, ۳k) = k$، و k دقیقاً یک سوم $p-۱$ است.

۲۶.۶ اگر $p = ۴k + ۳$ اول باشد، نشان دهید که دقیقاً نصف اعداد صحیح ۱، ۲، ...، $p-۱$ مانده‌های درجهٔ چهارم p هستند.

حل. بنابر (۲۱.۶)، تعداد مانده‌های درجهٔ چهارم p (در یک دستگاه مخفف مانده‌ها) عبارت است از $\phi(p)/(۴, \phi(p)) = (۴k+۲)/۲$، که درست نصف $p-۱$ است.

برهان دیگر. نشان می‌دهیم که هر ماندهٔ درجهٔ دوم p یک ماندهٔ درجهٔ چهارم p است (عکس مطلب بدیهی است). فرض کنیم a یک ماندهٔ درجهٔ دوم p باشد، و فرض می‌کنیم $b^۲ \equiv a (\mathrm{mod}\, p)$؛ از اینجا نتیجه می‌شود که $(-b)^۲ \equiv a (\mathrm{mod}\, p)$. اما دقیقاً یکی از دو عدد b یا $-b$ یک ماندهٔ درجهٔ دوم p است، زیرا $(-b/p) = (-۱/p)(b/p) = -(b/p)$. اگر $c^۲ \equiv \pm b (\mathrm{mod}\, p)$، آنگاه $c^۴ \equiv a (\mathrm{mod}\, p)$.

۲۷.۶ فرض کنید p عدد اولی به‌صورت $۶k - ۱$ باشد. به‌ازای چه مقادیری از a همنهشتی $x^۳ \equiv a (\mathrm{mod}\, p)$ جواب یکتا دارد؟

حل. آشکار است که یک جواب یکتا وجود دارد اگر $a \equiv ۰ (\mathrm{mod}\, p)$. حال فرض کنیم $(a, p) = ۱$. گیریم g یک ریشهٔ اولیهٔ p باشد. در این‌صورت بنابر (۱۶.۶)، $u^۳ \equiv a (\mathrm{mod}\, p)$

اگر و تنها اگر $\text{ind}\, u \equiv \text{ind}\, a \pmod{p-1}$. اما چون $(3, p-1) = 1$، همنهشتی $3y \equiv \text{ind}\, a \pmod{p-1}$ جواب یکتا به پیمانهٔ $p-1$ دارد، و لذا $x^3 \equiv a \pmod{p}$ یک جواب یکتا دارد.

برهان دیگر. یک جواب وجود دارد اگر $a \equiv 0 \pmod{p}$. با استفاده از (۲۱.۶)، می‌توانیم نشان دهیم که $p-1$ ماندهٔ درجهٔ سوم از p وجود دارد. لذا همنهشتی $x^3 \equiv a \pmod{p}$ جوابی دارد وقتی که $(a, p) = 1$، و در نتیجه هیچ‌کدام از همنهشتیها نمی‌توانند بیش از یک جواب داشته باشند.

◁ **۲۸.۶** فرض کنید g یک ریشهٔ اولیهٔ عدد اول فرد p باشد و $p \nmid a$. ثابت کنید که $x^n \equiv a \pmod{p}$ جواب دارد اگر و تنها اگر $a \equiv g^{dk} \pmod{p}$، که در آن $d = (n, p-1)$ و k عدد صحیحی است که در $1 \le k \le (p-1)/d$ صدق می‌کند.

حل. بنابر (۱۸.۶)، a یک ماندهٔ توانی nام p است اگر و تنها اگر $a^{(p-1)/d} \equiv 1 \pmod{p}$، که $d = (n, p-1)$. اگر $a \equiv g^{dk} \pmod{p}$، آنگاه $a^{(p-1)/d} \equiv g^{(p-1)k} \equiv 1 \pmod{p}$، لذا a یک ماندهٔ توان nام p است.

بعکس، فرض کنیم که a یک ماندهٔ توان nام p باشد. لذا مقداری مانند b وجود دارد به‌طوری که $a \equiv b^n \pmod{p}$، از (۱۱.۶) برای نوشتن $b \equiv g^t \pmod{p}$ استفاده می‌کنیم؛ لذا $a \equiv g^{nt} \pmod{p}$. اگر r باقیماندهٔ تقسیم nt بر $p-1$ باشد، آنگاه بنابر قضیهٔ فرما، $a \equiv g^r \pmod{p}$. به آسانی دیده می‌شود که $d \mid r$. اگر قرار دهیم $r = dk$، آنگاه $1 \le k \le (p-1)/d$. لذا $a \equiv g^{dk} \pmod{p}$ و قضیه حاصل است.

۲۹.۶ همهٔ اعداد صحیح x را بیابید به‌طوری که (الف) $3^x \equiv 7 \pmod{17}$؛ (ب) $x^3 \equiv x \pmod{17}$. (راهنمایی: جدولِ مسألهٔ ۱۶.۶ را به‌کار برید.)

حل. (الف) کار را با ریشهٔ اولیهٔ ۳ شروع می‌کنیم. از جدول، پیدا می‌کنیم که ۷ دارای اندیس ۱۱ است. لذا همنهشتی هم‌ارز $x \equiv 11 \pmod{16}$ را به‌دست می‌آوریم، که تمام جوابهای x اعداد صحیح مثبتی به‌صورت $16k + 11$ هستند.

(ب) همنهشتی $x^x \equiv x \pmod{17}$ کمی پیچیده‌تر است. فرض کنیم $x = r + 16q$، که $0 \le r \le 15$. در این‌صورت چون $3^{16} \equiv 1 \pmod{17}$، داریم $3^x \equiv 3^r \pmod{17}$. لذا همنهشتی ما به $3^r - r \equiv 16q \pmod{17}$، یا هم‌ارز با آن، $q \equiv r - 3^r \pmod{17}$ بدل می‌شود. بنابراین، جوابها اعداد x به‌صورت $r + 16(r - 3^r + 17n) = 17r - 16 \times 3^r + 272n$

هستند، که n باید طوری انتخاب شود که $x \geq ۰$. متناظر با $r = ۰, ۱, ۲, \ldots, ۱۵$، ۱۶ خانواده جواب وجود دارد. فهرست کردن همهٔ آنها کِسل‌کننده است، لذا یکی را برای روشن شدن مطلب به‌کار می‌بریم. $r = ۵$ را اختیار می‌کنیم؛ در این‌صورت $x = ۲۷۲n - ۳۸۰۳$ را به‌دست می‌آوریم، که $n > ۱۳$، یا به‌طور هم‌ارز، $x = ۲۷۲n - ۲۶۷$، که n مثبت است.

۳۰.۶ آیا $x^{۱۳} \equiv ۱۰ \pmod{۱۳۲۳}$ جوابی دارد؟ (راهنمایی: از (۱۸.۶) استفاده کنید، ولی توجه کنید که ۱۳۲۳ ریشهٔ اولیه ندارد.)

حل. چون $۱۳۲۳ = ۳^۳ \times ۷^۲$، وجود جواب به پیمانه‌های $۳^۳$ و $۷^۲$ را بررسی می‌کنیم. چون ۲۷ ریشهٔ اولیه دارد، بنابر (۱۸.۶)، $x^{۱۳} \equiv ۱۰ \pmod{۲۷}$ جواب دارد اگر و تنها اگر $۱۰^{۱۸} \equiv ۱ \pmod{۲۷}$. (این مطلب از قضیهٔ اویلر نتیجه می‌شود.) با استدلال مشابه $x^{۱۳} \equiv ۱۰ \pmod{۴۹}$ جواب دارد، زیرا $۱۰^{۴۲} \equiv ۱ \pmod{۴۹}$. لذا، بنابر قضیهٔ باقیماندهٔ چینی $x^{۱۳} \equiv ۱۰ \pmod{۱۳۲۳}$ جواب دارد.

۳۱.۶ اظهارنظر زیر از گاوس را ثابت کنید: اگر p و q اول باشند و $p = ۲q + ۱$، آنگاه به‌ازای هر عدد صحیح مثبت k، همنهشتی $n^{۲k} \equiv ۱ \pmod{p}$ یا دو جواب دارد یا $p - ۱$ جواب.

حل. بنابر (۱۸.۶)، تعداد جوابها عبارت است از $(۲k, p - ۱) = ۲(k, q)$. چون q اول است، داریم $(k, q) = ۱$ یا $(k, q) = q$، و قضیه حاصل می‌شود.

◁ **۳۲.۶** گیریم p یک عدد اولِ فرد باشد. ثابت کنید که تعداد نامتناهی عدد اول به‌صورت $۲kp + ۱$ وجود دارد. (راهنمایی: قرار دهید $a = p_۱p_۲ \cdots p_n$، که در آن p_iها به‌صورت $۲kp + ۱$ هستند، و مقسوم‌علیه‌های اول $(a^p - ۱)/(a - ۱)$ را در نظر بگیرید. ابتدا نشان دهید که $a - ۱$ و $(a^p - ۱)/(a - ۱)$ نسبت به هم اول‌اند.)

حل. فرض کنیم $p_۱$، $p_۲$، ...، p_n اعداد اول به‌صورت $۲kp + ۱$ باشند؛ نشان می‌دهیم عدد اولی مانند p به‌صورت $۲kp + ۱$ و متمایز با p_iها وجود دارد. گیریم $a = pp_۱p_۲ \cdots p_n$، و فرض می‌کنیم $N = (a^p - ۱)/(a - ۱)$. ابتدا نشان می‌دهیم که $(a - ۱, N) = ۱$. اگر q عدد اولی باشد که $a - ۱$ را بشمارد، آنگاه $a \equiv ۱ \pmod{q}$ و لذا $N \equiv p \pmod{q}$، زیرا $N = a^{p-۱} + a^{p-۲} + \cdots + a + ۱$. چون $p|a$، داریم $q \neq p$ و بنابراین q نمی‌تواند N را بشمارد.

در ادامه نشان می‌دهیم که هر عدد اول q که N را بشمارد، باید به‌صورت $۲kp + ۱$ باشد. چون $q|a^p - ۱$، داریم $a^p \equiv ۱ \pmod{q}$. لذا مرتبهٔ a به پیمانهٔ q برابر ۱ یا p است. اما $\operatorname{ord} a \neq ۱$،

زیرا $q \nmid a - ۱$. بنابراین $\operatorname{ord} a = p$، و لذا بنابر (i.۲.۶)، $p|\phi(q) = q - ۱$. از این‌رو به‌ازای عدد صحیحی مانند m، $q - ۱ = mp$، و چون N فرد است، m بایستی زوج باشد. روشن است که q با هر p_i تفاوت دارد، زیرا در غیر این‌صورت $q|۱$.

ریشه‌های اولیه

۳۳.۶ ثابت کنید که ۳ یک ریشهٔ اولیهٔ ۱۷ است. تمام ریشه‌های اولیهٔ ناهمنهشتِ ۱۷ را که بین ۱ و ۱۶ هستند به‌دست آورید.

حل. نشان می‌دهیم که مرتبهٔ ۳ به پیمانهٔ ۱۷ برابر ۱۶ است. مرتبهٔ ۳ عدد $\phi(۱۷) = ۱۶$ را می‌شمارد، لذا کافی است که $۳^{۸} \not\equiv ۱ \pmod{۱۷}$ را بررسی کنیم. این کار را می‌توانیم مستقیماً یا در نظر گرفتن اینکه ۳ یک نامانده‌ٔ درجهٔ دوم ۱۷ است انجام دهیم، زیرا $(۲/۳) = (۱۷/۳) = (۳/۱۷) = -۱$. لذا بنابر ملاک اویلر، $۳^{۸} \equiv -۱ \pmod{۱۷}$.

بنابر (۱۲.۶)، ریشه‌های اولیهٔ ۱۷ با ۳^k به پیمانهٔ ۱۷ همنهشت‌اند، که در آنها $(k, ۱۶) = ۱$. لذا ۸ ریشهٔ اولیه وجود دارد، یعنی $۳^{۱}$، $۳^{۳}$، . . .، $۳^{۱۵}$. کوچکترین ماندهٔ مثبت این اعداد به ترتیب، عبارت‌اند از ۳، ۱۰، ۵، ۱۱، ۱۴، ۷، ۱۲، و ۶.

۳۴.۶ تمام ریشه‌های اولیهٔ ۲۹، واقع بین ۱ و ۲۸ را به‌دست آورید.

حل. ابتدا ملاحظه می‌کنیم که ۲ یک ریشهٔ اولیهٔ ۲۹ است. برای بررسی این مطلب، بنابر (۸.۶) کافی است نشان دهیم که $۲^{۱۴} \not\equiv ۱ \pmod{۲۹}$ و $۲^{۴} \not\equiv ۱ \pmod{۲۹}$. به پیمانهٔ ۲۹ داریم $۲^{۴} \equiv ۱۶ \equiv -۱۳$ و $۲^{۸} \equiv ۱۶۹ \equiv -۵$ و $۲^{۱۲} \equiv ۶۵ \equiv ۷$ و $۲^{۱۴} \equiv ۲۸ \equiv -۱۰$ لذا ۲ یک ریشهٔ اولیه ۲۹ است.

بنابر (۱۲.۶)، ریشه‌های اولیهٔ ۲۹ دقیقاً اعدادی هستند که با ۲^k به پیمانهٔ ۲۹ همنهشت‌اند و $(k, ۲۸) = ۱$. برای صرفه‌جویی در عملیات از $۲^{۱۴} \equiv -۱ \pmod{۲۹}$ استفاده می‌کنیم. در نتیجه ریشه‌های اولیهٔ ۲۹ عبارت‌اند از ۲، ۸، ۳، ۱۹، ۱۸، ۱۴، ۲۷، ۲۱، ۲۶، ۱۰، ۱۱، و ۱۵. (ملاحظه می‌کنید که $۲ \equiv -۲۷ \pmod{۲۹}$، $۸ \equiv -۲۱ \pmod{۲۹}$، و مانند آن.)

۳۵.۶ اعداد $m > ۱$ را تعیین کنید که درست یک ریشهٔ اولیه داشته باشند.

حل. اگر m دارای ریشهٔ اولیه باشد، بنابر (۱۳.۶) دارای $\phi(\phi(m))$ ریشهٔ اولیه است. تنها اعداد صحیح مثبت k به‌طوری که $\phi(k) = ۱$ عبارت‌اند از $k = ۱$ و $k = ۲$. لذا می‌خواهیم اعداد $m > ۱$ را تعیین کنیم به‌طوری که $\phi(m) = ۱$ یا $\phi(m) = ۲$ به آسانی دیده

می‌شود که m فقط مقادیر ۲، ۳، ۴، یا ۶ را اختیار می‌کند. برای هر کدام از اینها ۱− تنها ریشهٔ اولیه است.

۳۶.۶ کدام‌یک از اعداد زیر ریشهٔ اولیه دارند: ۱۹۸، ۱۹۹، ۲۰۰، ۲۰۱، ۲۰۲، ۲۰۳.

حل. بنابر (۲۵.۶)، لازم است تعیین کنیم کدام‌یک از اعداد مفروض به‌صورت p^n یا $2p^n$ هستند (p عدد اول فرد). اعداد ۱۹۹ و ۲۰۲ تنها جوابها هستند.

۳۷.۶ چه تعداد از نامانده‌های درجهٔ دوم ۴۷ ریشهٔ اولیه ۴۷ نیستند؟

حل. ۲۳ ناماندهٔ درجهٔ دوم و $\phi(46) = 22$ ریشهٔ اولیه از ۴۷ وجود دارند. چون هر ریشهٔ اولیه بایستی یک ماندهٔ درجهٔ دوم باشد، در نتیجه یک نامانده وجود دارد که ریشهٔ اولیه نیست. تعیین آن نامانده آسان است: چون ۴۷ به‌صورت $4k+4$ است، ۱− یک ناماندهٔ درجهٔ دوم ۴۷ است و به‌وضوح ریشهٔ اولیهٔ ۴۷ نیست.

◁ **۳۸.۶** فرض کنید g یک ریشهٔ اولیهٔ m باشد. ثابت کنید که مانده‌های درجهٔ دوم m با توانهای زوج g و نامانده‌های درجهٔ دوم m با توانهای فرد g همنهشت هستند.

حل. مسأله برای $m = 1$ و $m = 2$ بدیهی است، لذا فرض می‌کنیم $m \geq 3$. بنابر (۱۱.۶)، هر عنصر از یک دستگاه مخفف مانده‌ها با توانی از g همنهشت به پیمانهٔ m است. اگر $a \equiv g^{2d} \pmod m$، روشن است که a یک ماندهٔ درجهٔ دوم m است، زیرا $a \equiv (g^d)^2 \pmod m$. بعکس، اگر $a = g^{2d+1}$ توان فردی از g باشد، نشان می‌دهیم که a نمی‌تواند یک ماندهٔ درجهٔ دوم m باشد. زیرا اگر a یک ماندهٔ درجهٔ دوم m باشد، عددی چون b وجود دارد که $a \equiv b^2 \pmod m$. فرض کنیم $b \equiv g^e \pmod m$. پس $a \equiv g^{2e} \pmod m$، و لذا $g^{2d+1} \equiv g^{2e} \pmod m$. در این‌صورت، بنابر (i.۲.۶) $\phi(m)$ باید عدد $2e - 2d + 1$ را بشمارد. این عمل ممکن نیست، زیرا اگر $m > 2$، با بررسی فرمول $\phi(m)$ معلوم می‌شود که $\phi(m)$ زوج است.

۳۹.۶ اگر $m > 2$ ریشهٔ اولیه داشته باشد، نشان دهید که یک ناماندهٔ درجهٔ دوم از m مانند a در $a^{\phi(m)/2} \equiv -1 \pmod m$ صدق می‌کند. ((۱۸.۶) و (۲۶.۶) را به‌کار برید.)

حل. اگر در (۱۸.۶)، $k = 2$ را اختیار کنیم، در نتیجه $a^{\phi(m)/2} \not\equiv 1 \pmod m$. اما چون $a^{\phi(m)/2}$ جوابی از $x^2 \equiv 1 \pmod m$ است، (۲۰.۶) ایجاب می‌کند که $a^{\phi(m)/2} \equiv -1 \pmod m$.

۴۰.۶ فرض کنید m دارای ریشهٔ اولیه نباشد. با استفاده از (۲.۶) و (۲۵.۶) ثابت کنید که به‌ازای هر a که با m متباین است، $a^{\phi(m)/۲} \equiv ۱ (\mathrm{mod}\, m)$.

حل. فرض کنیم $(a, m) = ۱$ و فرض می‌کنیم m فرد باشد. بنابر (۲۵.۶)، m دارای حداقل دو عامل اول است. لذا می‌توانیم بنویسیم $m = rs$، که در آن $r > ۱$، $s > ۱$، و $(r, s) = ۱$؛ پس $\phi(m) = \phi(r)\phi(s)$. چون $\phi(r)$ و $\phi(s)$ هر دو زوج‌اند، $\phi(m)/۲$ مضربی از هر یک از آنهاست. لذا بنابر قضیهٔ اویلر، $a^{\phi(m)/۲} - ۱$ بر r و s بخشپذیر است، و چون $(r, s) = ۱$، در نتیجه $a^{\phi(m)/۲} - ۱$ بر m بخشپذیر است.

حال، فرض می‌کنیم m زوج باشد و قرار می‌دهیم $m = ۲^b c$، که c فرد است. اگر $c = ۱$، آنگاه (۲۵.۶) ایجاب می‌کند که $b \geq ۳$ و لذا $\phi(m) = ۲^{b-۱}$. چون m ریشهٔ اولیه ندارد، داریم $\mathrm{ord}\, a < \phi(m)$، و از (i.۲.۶) نتیجه می‌شود که $\mathrm{ord}\, a | ۲^{b-۲}$ و لذا $a^{\phi(m)/۲} \equiv ۱ (\mathrm{mod}\, m)$. سرانجام، اگر $c > ۱$، آنگاه $\phi(m)/۲$ مضربی از ۲^b و $\phi(c)$ است، و مجدداً از قضیهٔ اویلر نتیجه می‌گیریم که $a^{\phi(m)/۲} \equiv ۱ (\mathrm{mod}\, m)$.

۴۱.۶ اگر g^k یک ریشهٔ اولیهٔ m باشد، ثابت کنید که g نیز یک ریشهٔ اولیهٔ m است.

حل. بنابر (۳.۶)، $\mathrm{ord}\, g^k = \mathrm{ord}\, g/(k, \mathrm{ord}\, g)$؛ به‌ویژه $\mathrm{ord}\, g^k \leq \mathrm{ord}\, g$. اگر g^k ریشهٔ اولیهٔ m باشد، آنگاه $\mathrm{ord}\, g^k = \phi(m)$. در نتیجه $\mathrm{ord}\, g \geq \phi(m)$، و لذا $\mathrm{ord}\, g = \phi(m)$، یعنی g یک ریشهٔ اولیهٔ m است.

به طریق دیگر، اگر g^k یک ریشهٔ اولیه m باشد، بنابر (۱۱.۶)، هر b که با m اول باشد با توانی از g^k به پیمانهٔ m همنهشت است. اما این b با توانی از g به پیمانهٔ m همنهشت است، و لذا g یک ریشهٔ اولیهٔ m است.

۴۲.۶ گیریم q یک عدد اول فرد، و فرض می‌کنیم $p = ۲q + ۱$ نیز اول باشد. ثابت کنید p دارای q نامانده‌ٔ درجهٔ دوم و $q - ۱$ ریشهٔ اولیه است. لذا نشان دهید که ریشه‌های اولیهٔ p درست همان نامانده‌های درجهٔ دوم p هستند، بجز یکی. استثناء کدام است؟

حل. این مسأله تعمیم مسألهٔ ۳۷.۶ است. p دارای $q = (p - ۱)/۲$ نامانده‌ٔ درجهٔ دوم و $\phi(p - ۱) = \phi(۲q) = q - ۱$ ریشهٔ اولیه است. چون هر ریشهٔ اولیهٔ p یک نامانده‌ٔ درجهٔ دوم p است، دقیقاً یکی از نامانده‌های درجهٔ دوم ریشهٔ اولیهٔ p نیست. چون q فرد، یعنی به‌صورت $۲k + ۱$ است. لذا $p = ۲q + ۱$ به‌صورت $۴k + ۳$ است، و لذا -۱ یک نامانده‌ٔ درجهٔ دوم p است. اما روشن است که -۱ دارای مرتبهٔ ۲ است، و لذا -۱ ریشهٔ اولیهٔ p نیست.

توضیح. اگر q اول باشد، معلوم نیست که تعداد نامتناهی عدد اول به‌صورت $2q+1$ وجود داشته باشد. این اعداد را به احترام سوفی ژرمن[1]، ریاضیدان فرانسوی اوایل سدهٔ نوزدهم که آنها را در ارتباط با آخرین قضیهٔ فرما بررسی کرده است، معمولاً اعداد اولِ سوفی ژرمن می‌نامند.

۴۳.۶ (الف) فرض می‌کنیم q عدد اولی به‌صورت $4k+1$ باشد. اگر $p=2q+1$ اول باشد، ثابت کنید که ۲ یک ریشهٔ اولیهٔ p است. (مسألهٔ ۴۲.۶ را ببینید.)

(ب) فرض می‌کنیم q عدد اولی به‌صورت $4k+3$ باشد. اگر $p=2q+1$ اول باشد، ثابت کنید که -2 یک ریشهٔ اولیهٔ p است.

حل. (الف) چون p به‌صورت $8k+3$ است، بنابر (۱۲.۵)، ۲ یک ناماندهٔ درجهٔ دوم p است. بنابر مسألهٔ ۴۲.۶، هر ناماندهٔ درجهٔ دوم p بجز -1 یک ریشهٔ اولیهٔ p است. چون $p>3$ پس $-1\not\equiv 2 \pmod p$، لذا ۲ یک ریشهٔ اولیهٔ p است.

(ب) چون p به‌صورت $8k+7$ است، بنابر (۱۲.۵)، ۲ یک مانده و -1 یک ناماندهٔ درجه دوم p است. لذا -2 یک ناماندهٔ درجهٔ دوم p است. بقیهٔ برهان مانند قسمت (الف) ادامه پیدا می‌کند.

۴۴.۶ با استفاده از مسألهٔ قبل ریشه‌های اولیهٔ ۱۱ و ۲۳ را پیدا کنید.

حل. فرض کنیم $q=5$ و $p=2q+1=11$. چون q به‌صورت $4k+1$ است، ۲ یک ریشهٔ اولیهٔ ۱۱ است. برای همهٔ ریشه‌های اولیه، 2^k راکه $(k,10)=1$ در نظر می‌گیریم، و متوالیاً اعداد 2^2، 2^3، 2^7، و 2^9 را به‌دست می‌آوریم. کوچکترین مانده‌های مثبت عبارت‌اند از ۲، ۴، ۸، ۷، و ۶.

فرض می‌کنیم $q=11$ و $p=2q+1=23$. چون q به‌صورت $4k+3$ است، -2 یک ریشهٔ اولیهٔ ۲۳ است. اکنون اعداد $(-2)^k$ را، که $(k,22)=1$ در نظر می‌گیریم. با بدل به پیمانهٔ ۲۳، ریشه‌های اولیه عبارت‌اند از ۲، ۱۵، ۱۴، ۱۰، ۱۷، ۱۹، ۷، ۵، ۲۰، و ۱۱.

۴۵.۶ ثابت کنید که دو عدد صحیح متوالی مثبت کوچکتر از ۱۶۷ وجود دارند که ریشه‌های اولیهٔ ۱۶۷ هستند. (راهنمایی: از مسألهٔ ۴۲.۶ استفاده کنید.)

حل. چون ۸۳ اول است، مسألهٔ ۴۲.۶ نشان می‌دهد که ۱۶۷ دارای ۸۲ ریشهٔ اولیه است. اما ۱ و -1 ریشهٔ اولیه نیستند؛ لذا در فاصلهٔ ۲ تا ۱۶۵ تعداد ۸۲ عدد صحیح وجود دارند که ریشهٔ اولیه ۱۶۷ هستند. تنها راه برای تولید ۸۲ عدد صحیح در این فاصله که هیچ دو عدد صحیح متوالی وجود نداشته باشند این است که ۲، ۴، ...، ۱۶۴ یا ۳، ۵، ...، ۱۶۵ را انتخاب کنیم. اما هیچ‌کدام از اینها امکان ندارد جواب مطلوب باشند، زیرا روشن است که ۴ و ۹ ریشهٔ اولیه نیستند.

1. Sophie Germain

۴۶.۶ فرض کنید $p > ۲$ اول باشد. (الف) ثابت کنید که هر نامانده‌ٔ درجهٔ دوم p یک ریشهٔ اولیهٔ p است اگر و تنها اگر p به‌صورت $۲^k + ۱$ باشد. (ب) اگر $p > ۳$ عدد اولی به‌صورت $۲^k + ۱$ باشد، ثابت کنید که ۳ یک ریشهٔ اولیه p است.

حل. (الف) p دارای $(p-۱)/۲$ نامانده‌ٔ درجهٔ دوم و $\phi(p-۱)$ ریشهٔ اولیه است. از آنجا که هر ریشهٔ اولیه یک نامانده‌ٔ درجهٔ دوم است، در نتیجه هر نامانده‌ٔ درجهٔ دوم یک ریشهٔ اولیه است اگر و تنها اگر $\phi(p-۱) = (p-۱)/۲$، $\phi(n) = n/۲$ اگر و تنها اگر n به‌صورت ۲^k باشد (مسألهٔ ۶۵.۳ را ببینید).

(ب) با توجه به (الف)، کافی است ثابت کنیم که ۳ یک نامانده‌ٔ درجهٔ دوم p است. چون $۲^k + ۱ \equiv ۰ \pmod ۳$ یا $۲^k + ۱ \equiv ۲ \pmod ۳$، پس $p \equiv -۱ \pmod ۳$. اما اگر p، $۲^k + ۱$ نمی‌تواند اول باشد، زیرا $p > ۳$. لذا $p \equiv ۲ \pmod ۳$، چون p به‌صورت $۴u + ۱$ است، داریم $(p/۳) = (۲/۳) = -۱$؛ بنابراین ۳ یک نامانده‌ٔ درجهٔ دوم p و لذا یک ریشهٔ اولیهٔ p است.

۴۷.۶ آیا $x^{۲۰} \equiv -۱ \pmod{۴۱}$ جوابی دارد که ریشهٔ اولیهٔ ۴۱ نباشد؟

حل. بنابر ملاک اویلر، جوابهای همنهشتی مفروض ۲۰ نامانده‌ٔ درجهٔ دوم ۴۱ هستند. اما ۴۱ فقط $\phi(۴۰) = ۱۶$ ریشهٔ اولیه دارد، لذا همنهشتی چهار جواب دارد که ریشهٔ اولیهٔ ۴۱ نیستند. راه دیگر بررسی این مسأله این است که به اعدادی مثل a از مرتبهٔ کوچکتر از ۴۰ نظر کنیم که مرتبه آنها ۲۰ را نشمارد، یعنی اعداد a به مرتبهٔ ۸. بنابر (۱۴.۶)، $\phi(۸) = ۴$ عنصر از مرتبهٔ ۸ وجود دارد. به آسانی دیده می‌شود که ۳ و -۳ دارای مرتبهٔ ۸ به پیمانهٔ ۴۱ هستند، زیرا $۳^۴ \equiv -۱ \pmod ۴$، و لذا عناصر دیگر با مرتبهٔ ۸ عبارت‌اند از وارون ضربی ۳ و -۳ به پیمانهٔ ۴۱، یعنی ۱۴ و -۱۴.

۴۸.۶ فرض می‌کنیم p عدد اولی به‌صورت $۴k + ۱$ باشد. اگر g یک ریشهٔ اولیهٔ p باشد، ثابت کنید $-g$ نیز یک ریشهٔ اولیهٔ p است. (راهنمایی: $-g$ را به‌صورت توانی از g بیان کنید، یا اگر مرتبهٔ $-g$ کمتر از $p-۱$ است، نشان دهید که مرتبهٔ g نیز کمتر از $p-۱$ است.)

حل. چون g یک ریشهٔ اولیهٔ p است، پس یک نامانده‌ٔ درجهٔ دوم p است، و لذا بنابر ملاک اویلر، $g^{۲k} \equiv -۱ \pmod p$. بنابراین، $-g \equiv g^{۲k}g = g^{۲k+۱} \pmod p$. اما روشن است که $(۲k+۱, ۴k) = ۱$. لذا بنابر (۱۲.۶)، $g^{۲k+۱}$ یک ریشهٔ اولیهٔ p، یعنی، $-g$ یک ریشهٔ اولیهٔ p است.

راه دیگر، توجه کنید که $(-g)^{2k} \equiv -1 (\mathrm{mod}\, p)$، و لذا $g \equiv (-g)^{2k+1} (\mathrm{mod}\, p)$. لذا هر عددی که به پیمانهٔ p با توانی از g همنهشت باشد، با توانی از $-g$ نیز همنهشت است. اکنون قضیه از (۱۱.۶) حاصل می‌شود.

۴۹.۶ نشان دهید که -۳ یک ریشهٔ اولیهٔ عدد اولی به‌صورت $۳ + ۴^n$ نیست.

حل. اگر $p = ۳ + ۴^n$ اول باشد، نشان می‌دهیم که -۳ یک ماندهٔ درجهٔ دوم p است. چون p به‌صورت $۴k + ۳$ است، داریم $(-۱/p) = -۱$. بنابر قانون تقابل مربعی، $(۳/p) = -(p/۳) = -۱$، زیرا $p \equiv ۱ (\mathrm{mod}\, ۳)$. لذا $(-۳/p) = (-۱/p)(۳/p) = ۱$، بنابراین، -۳ یک ماندهٔ درجهٔ دوم p است و لذا نمی‌تواند ریشهٔ اولیهٔ p باشد.

۵۰.۶ فرض می‌کنیم که g یک ریشهٔ اولیهٔ m باشد و $gh \equiv ۱ (\mathrm{mod}\, m)$. ثابت کنید که h نیز یک ریشهٔ اولیهٔ m است.

حل. به‌ازای هر عدد صحیح مثبتِ n، $(gh)^n = g^n h^n \equiv ۱ (\mathrm{mod}\, m)$. لذا $g^n \equiv ۱ (\mathrm{mod}\, m)$ اگر و تنها اگر $h^n \equiv ۱ (\mathrm{mod}\, m)$. به‌ویژه، g و h دارای یک مرتبه هستند، و بنابراین اگر یکی ریشهٔ اولیهٔ m باشد، دیگری نیز هست.

۵۱.۶ فرض می‌کنیم $p > ۳$ اول باشد. ثابت کنید که حاصلضرب ریشه‌های اولیهٔ p بین ۱ و $p - ۱$ با ۱ به پیمانهٔ p همنهشت است. (راهنمایی: از مسأله قبل استفاده کنید.)

حل. اگر g یک ریشهٔ اولیهٔ p باشد، $(g, p) = ۱$، و لذا g یک وارون مانند h به پیمانهٔ p دارد. بنابر مسألهٔ قبل، h نیز یک ریشهٔ اولیهٔ p است. اگر g یک ریشهٔ اولیهٔ p باشد، وارونش h با g به پیمانهٔ p ناهمنهشت است. در غیر این‌صورت، خواهیم داشت $g^۲ \equiv ۱$، که $g \equiv \pm ۱ (\mathrm{mod}\, p)$ را به‌دست می‌دهد؛ اما نه ۱ و نه -۱ ریشهٔ اولیهٔ هیچ عددِ اول بزرگتر از ۳ نیستند. بنابراین، می‌توان ریشه‌های اولیهٔ p را به‌صورت جفتهایی که حاصلضرب عناصر هر جفت همنهشت با ۱ به پیمانهٔ p است مرتب کرد، و لذا حاصلضرب ریشه‌های اولیهٔ p با ۱ به پیمانهٔ p همنهشت است.

توضیح. اساساً به روشی مشابه می‌توان ثابت کرد که اگر m غیر از ۳، ۴، و ۶ باشد و دارای ریشهٔ اولیه باشد، حاصلضرب ریشه‌های اولیهٔ m با ۱ به پیمانهٔ m همنهشت است.

۵۲.۶ کوچکترین مانده‌های مثبت چهار ریشهٔ اولیهٔ ناهمنهشت از اعداد ۲۵، ۱۲۵، و ۲۵۰ را بیابید.

حل. ریشه‌های اولیهٔ ۵ عبارت‌اند از ۲ و ۳. بنابر (۲۲.۶)، اگر g یک ریشهٔ اولیهٔ ۵ باشد، $g+5k$ یک ریشهٔ اولیه ۲۵ است هرگاه $(g+5k)^4 \not\equiv 1 \pmod{25}$. لذا ۲، ۱۲، ۱۷، ۲۲ و نیز ۳، ۸، ۱۳، ۲۲ ریشه‌های اولیهٔ ۲۵ هستند. مجدداً بنابر همان (۲۲.۶)، این اعداد ریشه‌های اولیهٔ ۱۲۵ نیز هستند. بنابر (۲۴.۶)، هر ریشهٔ اولیهٔ فرد ۱۲۵ یک ریشهٔ اولیهٔ ۲۵۰ است. لذا ۱۷، ۳، ۱۳، و ۲۳ ریشه‌های اولیهٔ ۲۵۰ هستند (همین‌طور ۱۲۷ = ۱۲۵ + ۲ و مانند آن).

◁ **۵۳.۶** ثابت کنید که بی‌نهایت عدد اول p وجود دارند که به‌ازای آنها یک عدد صحیح a با $1 < a < p-1$ وجود دارد به‌طوری که نه a ریشهٔ اولیه p است، نه $-a$.

حل. ملاحظه می‌کنید که اگر p عدد اولی به‌صورت $4k+1$ باشد، به‌ازای هر a که مضرب p نباشد، داریم $(a/p) = (-1/p)(a/p) = (-a/p)$، لذا a و $-a$ هر دو مانده‌های درجهٔ دوم یا نامانده‌های درجهٔ دوم p هستند، اما بنابر مسألهٔ ۲۳.۵، تعداد نامتناهی عدد اول به‌صورت $4k+1$ وجود دارد، و هر عدد $p > 5$ به این‌صورت دارای یک ماندهٔ درجهٔ دوم a با $1 < a < p-1$ است (در واقع همواره می‌توان a را مساوی ۴ اختیار کرد). پس، $-a$ نیز یک ماندهٔ درجهٔ دوم p است، و لذا a و $-a$ هیچ‌کدام ریشهٔ اولیهٔ p نیستند.

۵۴.۶ فرض کنیم m دارای ریشهٔ اولیه باشد، و گیریم $a_1, a_2, \ldots, a_{\phi(m)}$ یک دستگاه مخفف مانده‌ها به پیمانهٔ m باشد. ثابت کنید $a_1 a_2 \cdots a_{\phi(m)} \equiv -1 \pmod{m}$. (ملاحظه کنید که اگر m اول باشد، این حکم آشکارا همان قضیهٔ ویلسن است.)

حل. قضیه به‌ازای $m = 1$ و $m = 2$ نمایان است، لذا $m \geq 3$ را اختیار و فرض کنیم g یک ریشهٔ اولیهٔ m باشد، و قرار می‌دهیم $k = \phi(m)$. بنابر (۱۱.۵)، عناصر یک دستگاه مخفف مانده‌ها به پیمانهٔ m، به‌ترتیبی، با اعداد $g^1, g^2, \ldots, g^k$، همنهشت به پیمانهٔ m هستند. لذا حاصلضرب آنها همنهشت با g^N به پیمانهٔ m است، که در آن $N = 1 + 2 + \cdots + k$. بنابر فرمول معمولی حاصل‌جمع تصاعد حسابی، $2N = k(k+1)$. ملاحظه کنید که چون $m \geq 3$، k زوج و لذا $k+1$ فرد است. اما $g^N = (g^{k/2})^{k+1}$. چون g یک ریشهٔ اولیهٔ m است، داریم $g^{k/2} \equiv -1 \pmod{m}$ و لذا $g^N \equiv -1 \pmod{m}$.

۵۵.۶ فرض کنید q و $p = 4q+1$ اول باشند. ثابت کنید که ۲ یک ریشهٔ اولیهٔ p است، و اگر $q > 3$، نشان دهید ۳ یک ریشهٔ اولیه p است. این مطلب نشان می‌دهد که، مثلاً، ۲ یک ریشهٔ اولیهٔ ۱۳ است و ۲ و ۳ ریشه‌های اولیهٔ ۲۹ و ۵۳ هستند. (راهنمایی: ابتدا نشان دهید که ۲ و ۳ نامانده‌های درجهٔ دوم p هستند.)

حل. روشن است که، $q \neq ۲$، بنابراین q به‌صورت $۲k+۱$، و لذا p به‌صورت $۸k+۵$ است. بنابر (۱۲.۵)، ۲ یک نامانده درجهٔ دوم p است. نشان می‌دهیم که مرتبهٔ ۲ به پیمانه p برابر $p-۱$ است. فرض کنیم $\operatorname{ord} ۲ = t$؛ پس $t|\phi(p)$ و لذا $t|۴۹$. بنابراین t برابر است با ۱، ۲، ۴، ۹، ۲۹، یا ۴۹. چون ۲ یک نامانده درجهٔ دوم p است، $۲^{۲۹} \equiv -۱ (\bmod p)$، و لذا t نمی‌تواند مقادیر ۱، ۲، ۹، یا ۲۹ را اختیار کند. سرانجام، چون $p \geq ۱۳$، $p \nmid ۲^۴ - ۱$، و لذا $t \neq ۴$.

اگر $q > ۳$، آنگاه $q \equiv ۱ (\bmod ۳)$، زیرا اگر $q \equiv ۲ (\bmod ۳)$، آنگاه p بر ۳ بخشپذیر است. بنابراین q به‌صورت $۳k+۱$ و لذا p به‌صورت $۱۲k+۵$ است. با یک محاسبهٔ سادهٔ نماد لژاندر داریم $(۲/۳) = (p/۳) = ((۱۲k+۵)/۳) = (۳/p) = -۱$. فرض کنیم t مرتبهٔ ۳ به پیمانهٔ p باشد. درست مانند حالت قبل، t نمی‌تواند ۱، ۲، q، یا $۲q$ باشد، اما t برابر ۴ نیز نمی‌تواند باشد، زیرا $p \nmid ۳^۴ - ۱$. لذا $t = ۴q = \phi(p)$، و بنابراین ۳ یک ریشهٔ اولیهٔ p است.

۵۶.۶ فرض کنید p عدد اولی غیر از ۲ و ۵ باشد. ثابت کنید که ۱۰ یک ریشهٔ اولیهٔ p است اگر و تنها اگر بسط اعشاری $۱/p$ دارای دورهٔ $p-۱$ باشد.

حل. روند «تقسیم طولانی» را که هنگام تقسیم ۱ بر p به‌کار می‌بریم در نظر می‌گیریم. بلافاصله بعد از آنکه رقم kام بعد از ممیز را به‌دست آوریم، یک «باقیماندهٔ» r_k داریم، که باقیماندهٔ معمولی تقسیم ۱۰^k بر p است. دورهٔ بسط اعشاری دقیقاً همان دورهٔ دنبالهٔ باقیمانده‌هاست.

فرض کنیم d مرتبهٔ ۱۰ به پیمانهٔ p باشد (این مرتبه وجود دارد، زیرا $(۱۰,p) = ۱$). در این‌صورت، دنبالهٔ $r_۱, r_۲, \ldots$ از باقیمانده‌ها دارای دورهٔ d است، و لذا بسط اعشاری $۱/p$ دارای دورهٔ d است. به‌ویژه، بسط اعشاری دارای دورهٔ $p-۱$ است اگر و تنها اگر $\operatorname{ord}_p ۱۰ = p-۱$، یعنی اگر و تنها اگر ۱۰ یک ریشهٔ اولیهٔ p باشد.

۵۷.۶ ثابت کنید که به‌ازای هر $k \geq ۱$، ۳ یک ریشهٔ اولیهٔ ۷^k است.

حل. بنابر (۲۲.۶)، اگر g یک ریشهٔ اولیهٔ عدد اول فرد p باشد، و $g^p \not\equiv ۱ (\bmod p^۲)$، آنگاه به‌ازای هر $k \geq ۱$، g یک ریشهٔ اولیهٔ p^k است. چون $۳^۲$ و $۳^۳$ همنهشت با ۱ به پیمانهٔ ۷ نیستند، لذا ۳ یک ریشهٔ اولیهٔ ۷ است. چون $۳^۶ \equiv ۴۳ \not\equiv ۱ (\bmod ۴۹)$، قضیه حاصل می‌شود.

۵۸.۶ اثبات یا رد کنید: اگر p عدد اولی به‌صورت $۴k+۱$ باشد، لااقل یکی از ریشه‌های اولیهٔ p واقع بین ۱ و $p-۱$ فرد است.

حل. اگر p به‌صورت $۴k+۱$ باشد و g یک ریشهٔ اولیه p، آنگاه $-g$ نیز یک ریشهٔ اولیهٔ

p است (مسأله ۴۸.۶ را ببینید). لذا اگر g یک ریشهٔ اولیهٔ زوج بین ۱ و $p-1$ باشد، $p-g$ یک ریشهٔ اولیهٔ فرد p بین ۱ و $p-1$ است. بنابراین، نیمی از ریشه‌های اولیهٔ p بین ۱ و $p-1$ زوج‌اند و نیم دیگر فرد.

۵۹.۶ اثبات یا رد کنید: اگر p اول باشد و $a^{(p-1)/2} \equiv -1 \pmod{p}$، آنگاه a یک ریشهٔ اولیهٔ p است.

حل. این حکم درست نیست. مثلاً اگر $p=7$، آنگاه $(-1)^{(p-1)/2} \equiv -1 \pmod{7}$، اما -1 یک ریشهٔ اولیهٔ p نیست.

توضیح. اگر $a^{(p-1)/2} \equiv -1 \pmod{p}$، بنابر ملاک اویلر، a یک نامانده‌ٔ درجهٔ دوم p است. لذا این حکم درست خواهد بود فقط در صورتی‌که هر نامانده‌ٔ درجهٔ دوم p یک ریشهٔ اولیهٔ p باشد و بنابراین درست نیست اگر $\phi(p-1) < (p-1)/2$. اگر $p = 4k+3$، این نامساوی همواره برقرار است. اگر $p = 4k+1$، آنگاه $\phi(p-1) < (p-1)/2$ برقرار است اگر و تنها اگر p به‌صورت $2^n + 1$ نباشد.

۶۰.۶ اگر p عدد اول فردی باشد، نشان دهید عدد صحیحی وجود دارد که به‌ازای هر $k \geq 1$، یک ریشهٔ اولیه p^k و $2p^k$ است. (راهنمایی: اگر g یک ریشهٔ اولیهٔ p باشد، آنگاه g، $g+p$، $g+p^2$، و $g+p+p^2$ را در نظر بگیرید.)

حل. فرض می‌کنیم g یک ریشهٔ اولیهٔ p باشد، بنابر (i.۲۲.۶) لااقل یکی از اعداد g و $g+p$ یک ریشهٔ اولیهٔ p^2 است. با افزودن p^2، در صورت لزوم، یک ریشهٔ اولیه فرد h از p^2 را به‌دست می‌آوریم؛ در این‌صورت h نیز یک ریشهٔ اولیهٔ p است، زیرا $h \equiv g \pmod{p}$. از (i.۲۲.۶) نتیجه می‌شود که به‌ازای هر $k \geq 1$، h یک ریشهٔ اولیهٔ p^k است. اما چون h فرد است، (۲۳.۶) ایجاب می‌کند که به‌ازای هر $k \geq 1$، h یک ریشهٔ اولیهٔ $2p^k$ نیز باشد.

۶۱.۶ اگر p اول باشد و k مثبت، نشان دهید که هر ریشهٔ اولیهٔ p^{k+1} یک ریشهٔ اولیهٔ p^k است.

حل. فرض کنیم g یک ریشهٔ اولیهٔ p^{k+1} باشد. به موجب (۱۱.۶)، اگر a با p^{k+1} متباین باشد، عدد صحیح مثبت j وجود دارد به‌طوری که $a \equiv g^j \pmod{p^{k+1}}$. لذا $a \equiv g^j \pmod{p^k}$. چون هر a که با p^k متباین باشد با توانی از g همنهشت به پیمانهٔ p^k است، از (۱۱.۶) نتیجه می‌شود که g یک ریشهٔ اولیهٔ p^k است.

◁ **۶۲.۶** گیریم g یک ریشهٔ اولیهٔ عدد اولِ فرد p باشد، و فرض می‌کنیم $k \geq ۲$. ثابت کنید g یک ریشهٔ اولیهٔ p^k است اگر و تنها اگر $g^{p-۱} \not\equiv ۱ (\mathrm{mod}\, p^۲)$. (راهنمایی: مسألهٔ قبل را ببینید.)

حل. اگر $g^{p-۱} \not\equiv ۱ (\mathrm{mod}\, p^۲)$، آنگاه بنابر (۲۳.۶)، g یک ریشهٔ اولیهٔ $p^۲$ است، و لذا g یک ریشهٔ اولیهٔ p^k است. بعکس، اگر g یک ریشهٔ اولیهٔ p^k باشد، آنگاه با استفادهٔ مکرر مسألهٔ قبل، می‌بینیم که به‌ازای هر عدد صحیح مثبت $j \leq k$، g یک ریشهٔ اولیهٔ p^j است، و به‌ویژه، g یک ریشهٔ اولیهٔ $p^۲$ است. لذا g دارای مرتبهٔ $\phi(p^۲) = p(p-۱)$ به پیمانهٔ $p^۲$ است، و بنابراین $g^{p-۱} \not\equiv ۱ (\mathrm{mod}\, p^۲)$.

◁ **۶۳.۶** فرض کنید p یک عدد اول فرد و $k \geq ۲$. ثابت کنید دقیقاً $(p-۱)\phi(p-۱)$ ریشهٔ اولیه از p^k وجود دارند که به پیمانهٔ $p^۲$ ناهمنهشت‌اند.

حل. تعداد $\phi(\phi(p^۲)) = (p-۱)\phi(p-۱)$ ریشهٔ اولیه از $p^۲$ وجود دارد، و به موجب (۲۳.۶) هرکدام از آنها یک ریشهٔ اولیهٔ p^k است. اما، بنابر استدلال مسألهٔ قبل، هر ریشهٔ اولیهٔ p^k یک ریشهٔ اولیهٔ $p^۲$ است و لذا به پیمانهٔ $p^۲$ با یکی از $(p-۱)\phi(p-۱)$ ریشه‌های اولیهٔ $p^۲$ همنهشت است.

۶۴.۶ اگر $m_۱$، $m_۲$، ...، m_r دوبه‌دو نسبت به‌هم اول باشند و هر m_i دارای ریشهٔ اولیه باشد، ثابت کنید که یک عدد صحیح g وجود دارد که همزمان یک ریشهٔ اولیهٔ هر m_i است.

حل. فرض کنیم g_i یک ریشهٔ اولیهٔ m_i باشد، و قضیهٔ باقیماندهٔ چینی را به‌کار می‌بریم تا عدد صحیح g را بیابیم به‌طوری که به‌ازای هر i، $g \equiv g_i (\mathrm{mod}\, m_i)$. در این‌صورت g به‌ازای هر i ریشهٔ اولیهٔ هر m_i است.

۶۵.۶ فرض می‌کنیم m دارای یک ریشهٔ اولیه باشد، و گیریم $a_۱$، $a_۲$، ...، a_r یک دستگاه مخفف مانده‌ها به پیمانهٔ m باشد. ثابت کنید $a_۱^n$، $a_۲^n$، ...، a_r^n یک دستگاه مخفف مانده‌ها به پیمانهٔ m است اگر و تنها اگر $(n, \phi(m)) = ۱$.

حل. فرض کنیم g یک ریشهٔ اولیهٔ m باشد. پس a_iها به‌ترتیبی با g، $g^۲$، ...، g^r که $r = \phi(m)$، همنهشت‌اند. با مرتب کردن a_iها، می‌توانیم فرض کنیم که $a_i \equiv g_i (\mathrm{mod}\, m)$. لذا $a_i^n \equiv g_i^n (\mathrm{mod}\, m)$. بنابر (۱۲.۶)، g^n یک ریشهٔ اولیهٔ m است اگر و تنها اگر $(n, \phi(m)) = ۱$. در نتیجه اعداد a_i^n یک دستگاه مخفف مانده‌ها تشکیل می‌دهند اگر و تنها اگر $(n, \phi(m)) = ۱$.

◁ **۶۶.۶** فرض می‌کنیم p یک عدد اول فرد باشد، و گیریم $S_n = ۱^n + ۲^n + \cdots + (p-۱)^n$. ثابت کنید $S_n \equiv -۱ (\mathrm{mod}\, p)$ اگر $(p-۱)|n$ در غیر این‌صورت $S_n \equiv ۰ (\mathrm{mod}\, p)$. (با مسألهٔ ۸.۳ مقایسه شود.)

حل. فرض کنیم g یک ریشهٔ اولیهٔ p باشد. پس ۱، g، $g^۲$، ...، $g^{p-۲}$ همنهشت به پیمانهٔ p هستند. لذا $S_n \equiv ۱ + g^n + g^{۲n} + \cdots + g^{(p-۱)n} (\mathrm{mod}\, p)$ اگر $(p-۱)|n$، قرار می‌دهیم $n = (p-۱)t$. بنابر قضیهٔ فرما $g^{kn} = (g^{p-۱})^{kt} \equiv ۱ (\mathrm{mod}\, p)$. لذا S_n مجموع $p-۱$ جمله است که هر کدام همنهشت با ۱ به پیمانهٔ p است، و بنابراین $S_n \equiv -۱ (\mathrm{mod}\, p)$.

حال، فرض کنیم $(p-۱) \nmid n$. از ضرب طرفین همنهشتی S_n در $g^n - ۱$ داریم $(g^n - ۱)S_n \equiv ۱ - g^{(p-۱)n} (\mathrm{mod}\, p)$. چون $g^{p-۱} \equiv ۱ (\mathrm{mod}\, p)$، در نتیجه $g^{(p-۱)n} - ۱ \equiv ۰ (\mathrm{mod}\, p)$. اما چون $(p-۱) \nmid n$ و g دارای مرتبهٔ $p-۱$ است. از (i.۲.۶) نتیجه می‌شود که $g^n \not\equiv ۱ (\mathrm{mod}\, p)$. لذا $S_n \equiv ۰ (\mathrm{mod}\, p)$.

برهان دیگر. اگر $(p-۱)|n$، قرار می‌دهیم $n = t(p-۱)$؛ در این‌صورت، بنابر قضیهٔ فرما به‌ازای هر a متباین با p داریم $a^n = (a^{p-۱})^t \equiv ۱ (\mathrm{mod}\, p)$. لذا S_n مجموع $p-۱$ جمله است که هر کدام همنهشت با ۱ به پیمانهٔ p است. بنابراین $S_n \equiv -۱ (\mathrm{mod}\, p)$.

اکنون فرض می‌کنیم که $(p-۱) \nmid n$، و a را عدد صحیحی می‌گیریم که بر p بخشپذیر نباشد. پس a، $۲a$، ...، $(p-۱)a$ به‌ترتیبی با ۱، ۲، ...، $p-۱$ همنهشت‌اند. لذا a^n، $(۲a)^n$، ...، $((p-۱)a)^n$ به‌ترتیبی با ۱^n، ۲^n، ...، $(p-۱)^n$ همنهشت‌اند. بنابراین $a^n S_n \equiv S_n (\mathrm{mod}\, p)$، و لذا $(a^n - ۱)S_n \equiv ۰ (\mathrm{mod}\, p)$ به‌ویژه اگر a یک ریشهٔ اولیهٔ p و $(p-۱) \nmid n$، آنگاه $a^n \not\equiv ۱ (\mathrm{mod}\, p)$ و لذا $S_n \equiv ۰ (\mathrm{mod}\, p)$.

◁ **۶۷.۶** نشان دهید که ۷ یک ریشهٔ اولیهٔ هر عدد اول به‌صورت $۴^{۲n} + ۱$ است. (راهنمایی: کافی است نشان دهید که $(۷/p) = -۱$، و سپس نشان دهید که یک عدد اول به‌صورت $۴^{۲n} + ۱$ همنهشت با ۳ یا ۵ به پیمانهٔ ۷ وجود دارد. مسألهٔ ۴۶.۶ را ببینید.)

حل. قرار می‌دهیم $p = ۴^{۲n} + ۱ = ۲^{۴n} + ۱$. به موجب مسأله ۴۶.۶، ریشه‌های اولیهٔ p دقیقاً نامانده‌های درجهٔ دوم p هستند، لذا فقط لازم داریم که نشان دهیم $(۷/p) = -۱$. به آسانی بررسی می‌شود که هر توانی از ۲ همنهشت با ۱، ۲، یا ۴ به پیمانهٔ ۷ است. لذا $۴^{۲n} + ۱$ با یکی از اعداد ۲، ۳، یا ۵ همنهشت به پیمانهٔ ۷ است. می‌خواهیم امکان برقراری $۴^{۲n} \equiv ۱ (\mathrm{mod}\, ۷)$ را

رد کنیم. چون مرتبهٔ ۴ به پیمانهٔ ۷ برابر ۳ است، پس $۴^{۲n} \equiv ۱ (\mathrm{mod}\, ۷)$ فقط اگر $۳ | ۲n$. اما اگر $۳ | ۲n$، آنگاه $۴^{۲n}$ مکعب کاملی، مثلاً $x^۳$ است، و چون $x^۳ + ۱ = (x+۱)(x^۲ - x + ۱)$، در نتیجه $۴^{۲n} + ۱$ اول نیست. بنابراین،اگر p اول باشد، p همنهشت با ۳ یا ۵ به پیمانهٔ ۷ است. بنابر قانون تقابل مربعی، $(۷/p) = (p/۷)$، و $(p/۷)$ یا مساوی $(۳/۷)$ یا مساوی $(۵/۷)$ است، که هر کدام -۱ است.

۶۸.۶ اگر m و n نسبت به‌هم اول و بزرگتر از ۲ باشند، به کمک تعریف ریشهٔ اولیه مستقیماً ثابت کنید که mn ریشهٔ اولیه ندارد.

حل. اگر $(a, mn) = ۱$، نشان می‌دهیم که مرتبهٔ a به پیمانهٔ mn کوچکتر از $\phi(mn)$ است، و این مطلب با تعریف ریشهٔ اولیه تناقض دارد. چون $\phi(n)$ و $\phi(m)$ زوج‌اند، قرار می‌دهیم $\phi(m) = ۲s$ و $\phi(n) = ۲t$. پس، بنابر قضیهٔ اویلر $a^{۲st} = (a^{۲s})^t \equiv ۱ (\mathrm{mod}\, m)$. به همین طریق، $a^{۲st} \equiv ۱ (\mathrm{mod}\, n)$. لذا چون $(m, n) = ۱$ داریم $a^{۲st} \equiv ۱ (\mathrm{mod}\, mn)$. اما $۲st = \phi(mn)/۲$، و لذا $\mathrm{ord}\, a \leq \phi(mn)/۲$. بنابراین a نمی‌تواند یک ریشهٔ اولیهٔ mn باشد.

۶۹.۶ فرض می‌کنیم که m ریشهٔ اولیه دارد. ثابت کنید که g یک ریشهٔ اولیهٔ m است اگر و تنها اگر به‌ازای هر عامل q از $\phi(m)$، g یک نامانده‌ٔ توانی qام باشد.

حل. بنابر (۱۸.۶)، با $k = q$، g یک نامانده‌ٔ توانی qام از m است اگر و تنها اگر $g^{(p-۱)/q} \not\equiv ۱ (\mathrm{mod}\, p)$. اما (۸.۶) ایجاب می‌کند که g یک ریشهٔ اولیهٔ m باشد اگر و تنها اگر به‌ازای هر مقسوم‌علیه اول $\phi(m)$ باشند q، $g^{(p-۱)/q} \not\equiv ۱ (\mathrm{mod}\, p)$.

◁ **۷۰.۶** فرض می‌کنیم $p \geq ۷$ اول باشد. با استفاده از ریشه‌های اولیه، ثابت کنید که مجموع مربعات مانده‌های درجه دوم p و مجموع مربعات نامانده‌های درجهٔ دوم p هر کدام بر p بخشپذیرند. (راهنمایی: مسأله ۳۸.۶ را ببینید.)

حل. فرض کنیم g یک ریشهٔ اولیهٔ p باشد و A معرف مجموع مربعات مانده‌های درجهٔ دوم p. به موجب مسألهٔ ۳۸.۶، $A \equiv g^۴ + g^۸ + \cdots + g^{۲(p-۱)} (\mathrm{mod}\, p)$. بنابراین، $(g^۴ - ۱)A \equiv g^۴(g^{۲(p-۱)} - ۱) (\mathrm{mod}\, p)$. چون سمت راست همنهشت با ۰ به پیمانهٔ p است، کافی است نشان دهیم که $g^۴ \not\equiv ۱ (\mathrm{mod}\, p)$. اگر $p > ۵$ این مطلب واضح است، زیرا g یک ریشهٔ اولیهٔ p است.

به همین طریق، فرض کنیم B معرف مجموع مربعات نامانده‌های درجهٔ دوم p باشد. داریم

$(g^۴-۱)B \equiv g^۲(g^{۲(p-۱)}-۱) \pmod p$. بنابراین، $B \equiv g^۲+g^۶+\cdots+g^{۲(p-۲)} \pmod p$.
اکنون مانند بند قبلی می‌توانیم نتیجه بگیریم که $B \equiv ۰ \pmod p$.

۷۱.۶ فرض می‌کنیم p اول باشد. با استفاده از وجود ریشهٔ اولیه برای p مستقیماً ثابت کنید که اگر $e|p-۱$، عنصری از مرتبهٔ e به پیمانهٔ p وجود دارد.

حل. یک ریشهٔ اولیهٔ p دارای مرتبهٔ $p-۱$ به پیمانهٔ p است، و لذا بنابر (ii.۳.۶)، به‌ازای هر $e|p-۱$ عنصری از مرتبهٔ e به پیمانهٔ p وجود دارد.

◁ **۷۲.۶** گیریم p یک عدد اول فرد باشد، و فرض می‌کنیم $k \geq ۲$. ثابت کنید ریشه‌های اولیهٔ $p^{k+۱}$ دقیقاً (تا همنهشتی به پیمانهٔ $p^{k+۱}$) اعدادی به‌صورت $g+jp^k$ هستند، که در آنها g یک ریشهٔ اولیهٔ p^k با $۱ \leq g < p^k$، و $۰ \leq j \leq p-۱$ است. (قضیه برای $k=۱$ برقرار نیست؛ مسأله بعد را ببینید.)

حل. فرض می‌کنیم $۱ < h < p^{k+۱}$ یک ریشهٔ اولیهٔ $p^{k+۱}$ باشد، می‌توانیم اعداد صحیح g و h را با $۱ \leq g < p^k$ و $۰ \leq j \leq p-۱$ بیابیم به‌طوری که $h = g+jp^k$ (فقط h را بر p^k تقسیم می‌کنیم، خارج‌قسمت j و باقیماندهٔ g به‌دست می‌آیند). چون h یک ریشهٔ اولیهٔ $p^{k+۱}$ است، h ریشهٔ اولیهٔ p^k نیز می‌شود، و لذا چون $g \equiv h \pmod{p^k}$، g یک ریشهٔ اولیهٔ p^k است. بنابراین هر ریشهٔ اولیهٔ $p^{k+۱}$ به پیمانهٔ $p^{k+۱}$ با یک عدد به‌صورت مورد نظر همنهشت است. بعکس، هر عدد به‌صورت $g+jp^k$، که در آن g یک ریشهٔ اولیهٔ p^k است، یک ریشهٔ اولیهٔ $p^{k+۱}$ است: زیرا $g+jp^k \equiv g \pmod{p^k}$، $g+jp^k$ یک ریشهٔ اولیهٔ p^k است و لذا بنابر (۲۳.۶)، یک ریشهٔ اولیهٔ $p^{k+۱}$ نیز هست.

◁ **۷۳.۶** فرض می‌کنیم p یک عدد اول فرد باشد، ثابت کنید که دقیقاً $\phi(p-۱)$ ریشهٔ اولیه از p وجود دارند که به پیمانهٔ $p^۲$ ناهمنهشت‌اند و ریشه‌های اولیهٔ $p^۲$ نیستند.

حل. اگر g یک ریشهٔ اولیهٔ p باشد، p ریشهٔ اولیه از p وجود دارند که با g به پیمانهٔ p همنهشت ولی به پیمانهٔ $p^۲$ ناهمنهشت‌اند، و اینها عبارت‌اند از g، $g+p$، $g+۲p$، ...، $g+(p-۱)p$.
چون p دارای $\phi(p-۱)$ ریشهٔ اولیه است، لذا $p\phi(p-۱)$ ریشهٔ اولیه از p وجود دارند که به پیمانهٔ $p^۲$ ناهمنهشت‌اند. اما $p^۲$ دارای $(p-۱)\phi(p-۱)$ ریشهٔ اولیه است، لذا تعداد ریشه‌های اولیهٔ p که به پیمانهٔ $p^۲$ ناهمنهشت‌اند و ریشه‌های اولیهٔ $p^۲$ نیستند عبارت است از
$p\phi(p-۱)-(p-۱)\phi(p-۱) = \phi(p-۱)$.

راه حل دیگر: به برهان (i.۲۲.۶) مراجعه می‌کنیم. $g+tp$ را که در آن $0 \le t \le p-1$ در نظر می‌گیریم. این اعداد ریشه‌های اولیهٔ p هستند که به پیمانهٔ p^2 ناهمنهشت‌اند. با استفاده از قضیهٔ دوجمله‌یی می‌توانیم نشان دهیم که $(g+tp)^{p-1} \equiv g^{p-1} - g^{p-2}tp \pmod{p^2}$. فرض می‌کنیم $g^{p-1} = 1+mp$، پس $g^{p-1} \equiv 1 \pmod{p^2}$ اگر و تنها اگر $mp - g^{p-2}tp \equiv 0 \pmod{p^2}$، یعنی، $g^{p-2}t \equiv m \pmod{p}$. این همنهشتی دارای یک جواب یکتاست. لذا به‌ازای تمام مقادیر t جز یکی $g+pt$ یک ریشهٔ اولیهٔ p است. چون p دارای $\phi(p-1)$ ریشهٔ اولیه است، قضیه حاصل می‌شود.

◁ **۷۴.۶** فرض می‌کنیم به‌ازای $k \ge 1$، $n = 3^k$. ثابت کنید $3n \mid 2^n + 1$. (راهنمایی: ابتدا ثابت کنید که ۲ یک ریشهٔ اولیهٔ $3n$ است.)

حل. به آسانی دیده می‌شود که ۲ یک ریشهٔ اولیهٔ 3^2 و لذا بنابر (۲۳.۶) یک ریشهٔ اولیهٔ 3^{k+1} است، از این‌رو ۲ دارای مرتبهٔ $\phi(3^{k+1}) = 2 \times 3^k$ به پیمانهٔ 3^{k+1} است، و به‌ویژه، نتیجه می‌شود که $2^{2n} \equiv 1 \pmod{3n}$. بنابراین، 2^n جوابی از همنهشتی $x^2 \equiv 1 \pmod{3n}$ است. رابطهٔ $2^n \equiv 1 \pmod{3n}$ برقرار نیست، زیرا در این‌صورت $\operatorname{ord} 2 \le n$. لذا $2^n \equiv -1 \pmod{3n}$، یعنی $3n \mid 2^n + 1$.

◁ **۷۵.۶** (الف) فرض می‌کنیم $m > 1$. عدد صحیح مثبت N را که بسط دهدهی آن با رقم مفروض $b \ge 1$ شروع می‌شود بیابید به‌طوری که اگر b به انتهای بسط دهدهی N برود، عدد جدید عدد صحیح N/m باشد. (مثلاً اگر $m = 2$ و $b = 1$، عدد صحیح مثبت N را که با رقم ۱ شروع می‌شود لازم داریم به‌طوری که اگر ۱ به انتهای عدد برود، عدد صحیح $N/2$ را به‌دست آوریم.)

(ب) کوچکترین جواب مثبت را به‌ازای (i) $b = 1$، $m = 2$؛ (ii) $b = 1$، $m = 5$ به‌دست آورید. نشان دهید که چرا جواب به‌دست آمده کوچکترین عدد صحیح مثبت با ویژگی مطلوب است.

حل. فرض می‌کنیم $N = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0$، که در آن $a_n = b$. اگر رقم پیشرو N را اختیار کرده و آن را به انتها ببریم، عدد $Q = a_{n-1}10^n + \cdots + 10a_0 + b$ را به‌دست می‌آوریم. لذا $10N - Q = b(10^{n+1} - 1)$، و $Q = N/m$ اگر و تنها اگر $b(10^{n+1} - 1) = (10m - 1)$. ابتدا نشان می‌دهیم که می‌توان n را چنان انتخاب کرد که $(10m - 1)$ عدد $b(10^{n+1} - 1)$ را بشمارد. برای انجام این کار کافی است اطمینان

حاصل کنیم که $(۱۰^{n+۱}-۱)|(۱۰m-۱)$. چون ۱۰ با $۱۰m-۱$ متباین است، به قضیهٔ اویلر متوسل می‌شویم و $n+۱=\phi(۱۰m-۱)$ را اختیار می‌کنیم. با این انتخاب n، داریم $N=mQ=mb(۱۰^{n+۱}-۱)/(۱۰m-۱)$.

(ب) (i) با توجه به اثبات (الف)، برقراری $(۱۰m-۱)|b(۱۰^{n+۱}-۱)$ را لازم داریم، یعنی، اینکه $۱۰^{n+۱}\equiv ۱ \pmod{۱۹}$. اثبات اینکه ۱۰ یک ریشهٔ اولیهٔ ۱۹ است آسان است، لذا کوچکترین مقدار ممکن برای h عدد ۱۷ است. بنابراین کوچکترین مقدار N با ویژگی مطلوب $۲(۱۰^{۱۸}-۱)/۱۹$ است. (ii) برای $m=۵$، تعیین مرتبهٔ ۱۰ به پیمانهٔ ۴۹ را لازم داریم. چون ۱۰ یک ریشهٔ اولیهٔ ۷ است و $۱۰^{۶}\not\equiv ۱ \pmod{۴۹}$، ۱۰ یک ریشهٔ اولیهٔ ۴۹ است و لذا دارای مرتبهٔ ۴۲ به پیمانهٔ ۴۹ است. لذا کوچکترین عدد N با ویژگی مطلوب عدد $۵(۱۰^{۴۲}-۱)/۴۹$ است.

کوچکترین نمای عام و تابع کار مایکل

در بقیهٔ مسائل این فصل دربارهٔ کوچکترین نمای عام m، یعنی، بزرگترین مرتبهٔ یک عدد صحیح به پیمانهٔ m بحث می‌شود (تعریف (۶.۶) را ببینید).

۷۶.۶ اگر a فرد و $n\geq ۳$، ثابت کنید $a^{۲^{n-۲}}\equiv ۱ \pmod{۲^n}$.

حل. بنابر (۲۵.۶)، ۲^n ریشهٔ اولیه ندارد، و لذا $\operatorname{ord} a<\phi(۲^n)$. اما $۲^{n-۱}|\phi(۲^n)$، و چون بنابر (i.۲.۶)، $\operatorname{ord} a|\phi(۲^n)$، نتیجه می‌گیریم که $\operatorname{ord} a|۲^{n-۲}$. اکنون قضیه از (i.۲.۶) نتیجه می‌شود.

۷۷.۶ ثابت کنید $۵^{۲^{n-۳}}\not\equiv ۱ \pmod{۲^n}$. (راهنمایی: به استقرا نشان دهید که $۵^{۲^{n-۳}}\equiv ۱+۲^{n-۱} \pmod{۲^n}$.)

حل. بررسی قضیه به‌ازای $n=۳$ آسان است. اکنون فرض کنیم $۵^{۲^{k-۳}}\equiv ۱+۲^{k-۱} \pmod{۲^k}$؛ نشان می‌دهیم که $۵^{۲^{k-۲}}\equiv ۱+۲^k \pmod{۲^{k+۱}}$. بنابه فرض، مقداری چون t وجود دارد که $۵^{۲^{k-۳}}=۱+۲^{k-۱}+t^{۲^k}$. طرفین را به توان ۲ می‌رسانیم، پس از ساده‌کردن به پیمانهٔ $۲^{k+۱}$ داریم $۵^{۲^{k-۲}}\equiv (۱-۲^{k-۱})^۲=۱+۲^k+۲^{۲k-۲} \pmod{۲^{k+۱}}$. اما $۲^{k+۱}|۲^{۲k-۲}$، زیرا برای $k\geq ۳$، $۲k-۲\geq k+۱$، و قضیه نتیجه می‌شود.

توضیح. با استفاده از این مسأله و مسألهٔ قبل نشان دهید که کوچکترین نمای عام برای ۲^n عبارت است $۲^{n-۲}$ هرگاه $n\geq ۳$.

تابع $\lambda(m)$ را به شرح زیر تعریف می‌کنیم. اگر m برابر ۱، ۲، یا ۴ باشد، قرار می‌دهیم $\lambda(m)=\phi(k)$؛ اگر $m>۴$ به‌صورت توانی از ۲ باشد، آنگاه $\lambda(m)=\phi(m)/۲$. هرگاه m

توانی از یک عدد اول فرد باشد، $\lambda(m) = \phi(m)$، و اگر $m = P_1P_2\cdots P_k$ که P_iها توانی از اعداد اول متمایزند، آنگاه $\lambda(m)$ کوچکترین مضرب مشترک $\lambda(P_i)$هاست. تابع $\lambda(m)$ توسط ریاضیدان امریکایی رابرت کارمایکل در ۱۹۰۸ معرفی شد. این موضوع حدود سی سال جلوتر توسط فرانسوا لوکا کشف شده بود.

۷۸.۶ اگر $(a,m) = 1$، ثابت کنید $a^{\lambda(m)} \equiv 1 \pmod m$. (راهنمایی: فرض کنید m حاصلضرب $P_1P_2\cdots P_k$ از توانهای اعداد اول متمایز باشد. به پیمانهٔ P_i محاسبه کنید و مسألهٔ ۷۶.۶ را به‌کار برید.)

حل. کافی است نشان دهیم که به‌ازای $1 \le i \le k$، $a^{\lambda(m)} \equiv 1 \pmod{P_i}$، زیرا از این همنهشتی نتیجه می‌شود $a^{\lambda(m)} \equiv 1 \pmod m$. اگر P_i برابر ۲، ۴، یا توانی از یک عددِ اولِ فرد باشد، بنابه تعریف $\lambda(P_i) = \phi(P_i)$، لذا $a^{\lambda(P_i)} \equiv 1 \pmod{P_i}$. چون $\lambda(P_i)|\lambda(m)$، $a^{\lambda(m)} \equiv 1 \pmod{P_i}$. اگر P_i توانی از ۲ بزرگتر از ۴ باشد، بنابر مسألهٔ ۷۶.۶، $a^{\lambda(P_i)} \equiv 1 \pmod{P_i}$، که مجدداً $a^{\lambda(m)} \equiv 1 \pmod{P_i}$ نتیجه می‌شود.

۷۹.۶ اگر a بر ۲، ۳، ۵، ۷، یا ۱۳ بخشپذیر نباشد، ثابت کنید $a^{۱۲} \equiv 1 \pmod{۶۵۵۲۰}$.

حل. $۶۵۵۲۰ = ۲^۴ \cdot ۳^۲ \cdot ۵ \cdot ۷ \cdot ۱۳$، لذا $\lambda(۶۵۵۲۰)$ کوچکترین مضرب مشترکِ ۴، ۶، و ۱۲ است؛ لذا $\lambda(۶۵۵۲۰) = ۱۲$. توجه کنید که $\phi(۶۵۵۲۰) = ۱۳۸۲۴$، لذا $\lambda(m)$ می‌تواند بسیار کوچکتر از $\phi(m)$ باشد.

۸۰.۶ فرض می‌کنیم N حاصلضرب اعداد اول متمایز P_1، ...، P_k باشد. ثابت کنید $\lambda(N)/\phi(N) \le ۱/۲^{k-۱}$. (بنابراین $\lambda(m)$ می‌تواند به‌طور قابل ملاحظه‌ای کوچکتر از $\phi(m)$ باشد.)

حل. به‌ازای $1 \le i \le k$ قرار می‌دهیم $p_i - ۱ = ۲b_i$. در این‌صورت $\phi(N) = ۲^k P$، که P حاصلضرب b_iهاست، در حالی‌که $\lambda(N) = ۲M$، که M کوچکترین مضرب مشترک h_iهاست. چون $M \le P$، قضیه نتیجه می‌شود.

◁ **۸۱.۶** نشان دهید که $\lambda(m)$ کوچکترین نمای عامِ m است. (مسأله‌های ۷۷.۶، ۷۸.۶ و قضیهٔ (۲۵.۶) را به‌کار برید.)

حل. اگر $(a,m) = ۱$، بنابر مسألهٔ ۷۸.۶، $a^{\lambda(m)} \equiv 1 \pmod m$، و لذا $\operatorname{ord} a \le \lambda(m)$،

باقی می‌ماند نشان دهیم که عنصری با مرتبهٔ دقیقاً $\lambda(m)$ وجود دارد. فرض کنیم $m = P_1 P_2 \cdots P_k$، که در آن P_iها توانهایی از اعداد اول متمایزند. نشان می‌دهیم که به‌ازای هر i، یک عدد صحیح a_i وجود دارد که مرتبه‌اش به پیمانهٔ P_i برابر $\lambda(P_i)$ است. اگر P_i برابر ۲ یا ۴ باشد، روشن است که یک چنین a_i وجود دارد؛ اگر P_i توانی از ۲ بزرگتر از ۴ باشد، بنابر مسألهٔ ۷۷.۶ می‌توانیم $a_i = 5$ را اختیار کنیم؛ و اگر P_i توانی از یک عددِ اولِ فرد باشد، a_i را یک ریشهٔ اولیهٔ P_i فرض می‌کنیم.

از قضیهٔ باقیماندهٔ چینی برای تولید یک عدد صحیح b به‌طوری که به‌ازای هر $i \leq k$، $b \equiv a_i \pmod{P_i}$ بهره می‌گیریم. فرض کنیم $e = \operatorname{ord}_m b$. آنگاه $b^e \equiv 1 \pmod{P_i}$ و لذا $a_i^e \equiv 1 \pmod{P_i}$. از این‌رو، بنابر (i.۲.۶)، به‌ازای هر i، $e \mid \lambda(P_i)$، و لذا کوچکترین مضرب‌مشترکِ $\lambda(p_i)$ها، یعنی $\lambda(m)$ عدد e را می‌شمارد. لذا $\operatorname{ord} b \geq \lambda(m)$ ، و چون $\operatorname{ord} b \leq \lambda(m)$، نتیجه می‌گیریم که $\operatorname{ord} b = \lambda(m)$.

۸۲.۶ فرض می‌کنیم m یک عدد صحیح مثبت باشد و p عدد اول فردی باشد که m را می‌شمارد. اگر p^k بزرگترین توانی از p باشد که m را می‌شمارد، با استفاده از مسألهٔ قبل نشان دهید که عدد صحیحی با مرتبهٔ $\phi(p^k)$ به پیمانهٔ m وجود دارد.

حل. از مسألهٔ ۸۱.۶ و توجه بعد از (۶.۶) نتیجه می‌شود که یک عدد صحیح c وجود دارد به‌طوری که $\operatorname{ord} c = \lambda(m)$. بنابر تعریف $\lambda(m)$ داریم $\phi(p^k) \mid \lambda(m)$. لذا بنابر (ii.۳.۶)، $c^{\lambda(m)/\phi(p^k)}$ دارای مرتبهٔ $\phi(p^k)$ به پیمانهٔ m است.

تمرینهایی برای فصل ۶

۱. (الف) مرتبهٔ ۳۴ به پیمانهٔ ۳۷ را به‌دست آورید.
(ب) مرتبهٔ 2^{12} به پیمانهٔ ۳۷ چقدر است؟

۲. تمام اعداد صحیح کوچکتر از ۳۷ را بیابید که مرتبهٔ ۶ به پیمانهٔ ۳۷ دارند.

۳. اثبات یا رد کنید: اگر $(a, m) = 1$ و $\operatorname{ord}_m a = m - 1$، آنگاه m اول است.

۴. فرض می‌کنیم $\operatorname{ord}_{41} 9 = 4$ و $\operatorname{ord}_{41} 10 = 5$. مرتبهٔ ۸ به پیمانهٔ ۴۱ چقدر است؟

۵. فرض می‌کنیم مرتبهٔ a به پیمانهٔ ۶۸۶ برابر ۴۲ باشد، مرتبهٔ a^{15} چقدر است؟

۶. با توجه به اینکه ۵ یک ریشهٔ اولیهٔ ۲۶۳ است، مرتبهٔ ۲۵۸ به پیمانهٔ ۲۶۳ را تعیین کنید.

۷. به‌ازای چه اعداد اولی همواره عناصری از مرتبهٔ ۴ به پیمانهٔ p وجود دارند؟

۸. تمام عناصرِ از مرتبهٔ ۸ به پیمانهٔ ۱۰۹ را تعیین کنید.

۹. با استفاده از اینکه ۲ یک ریشهٔ اولیهٔ ۱۰۱ است کوچکترین مانده‌های مثبت تمام عناصرِ از مرتبهٔ ۵ به پیمانهٔ ۱۰۱ را به‌دست آورید.

۱۰. نشان دهید که ۵ یک ریشهٔ اولیهٔ ۷۳ است، و تمام اعداد بین ۱ و ۷۲ را که دارای مرتبهٔ ۱۲ به پیمانهٔ ۷۳ هستند تعیین کنید.

۱۱. با استفاده از اینکه ۶ یک ریشهٔ اولیهٔ ۴۱ است کوچکترین مانده‌های مثبت تمام عناصرِ دارای مرتبهٔ ۸ به پیمانهٔ ۴۱ را پیدا کنید.

۱۲. فرض می‌کنیم که $n = ۲^{۴۵} - ۱$، ثابت کنید $\phi(n)$ مضربی از ۴۵ است.

۱۳. تعیین کنید کدام‌یک از اعداد زیر ریشهٔ اولیه دارند: ۱۴۳، ۱۴۷، ۶۲۶، ۱۳۳۱.

۱۴. تمام ریشه‌های اولیهٔ ۳۸ بین ۱ و ۳۷ را پیدا کنید.

۱۵. می‌دانیم که ۵ یک ریشهٔ اولیهٔ ۱۰۳ است. آیا ۲۵ نیز یک ریشهٔ اولیهٔ ۱۰۳ است؟

۱۶. تعداد ریشه‌های اولیهٔ (الف) ۶۲۵؛ (ب) ۶۲۶؛ (ج) ۶۸۶ را تعیین کنید.

۱۷. ثابت کنید که ۱۸ یک ریشهٔ اولیه ۳۷ است ولی ریشهٔ اولیه $۳۷^۲$ نیست.

۱۸. ثابت کنید که ۳ یک ریشهٔ اولیه ۱۹۹ است. آیا سه ریشهٔ اولیهٔ $(۱۹۹)^۲$ نیز هست؟

۱۹. دو ریشهٔ اولیه از (الف) ۱۷؛ (ب) ۲۸۹؛ (ج) ۵۷۸ را به‌دست آورید.

۲۰. کوچکترین مانده‌های مثبت چهار ریشهٔ اولیه ناهمنهشت از (الف) ۲۵؛ (ب) ۱۲۵؛ (ج) ۲۵۰ را به‌دست آورید.

۲۱. یک ریشهٔ اولیه از ۷۲۲ را پیدا کنید. ۷۲۲ چند ریشهٔ اولیهٔ ناهمنهشت دارد؟

۲۲. عدد صحیح ۶ یک ریشهٔ اولیهٔ ۱۰۹ است. وارون ضربی ۶ به پیمانهٔ ۱۰۹ را محاسبه کنید، و از آن برای یافتن ریشهٔ اولیهٔ دیگری از ۱۰۹ استفاده کنید.

۲۳. آیا هر نامانده درجهٔ دوم ۲۵۷ یک ریشهٔ اولیهٔ ۲۵۷ است؟

۲۴. عدد ۷ یک ریشهٔ اولیهٔ عدد اول ۲۴۱ است. آیا -۷ نیز یک ریشهٔ اولیهٔ ۲۴۱ است؟

۲۵. کوچکترین مانده‌های مثبت سه ریشهٔ اولیهٔ ناهمنهشت $۷^۲$، $۷^۳$، و ۲×۷^۳ را به‌دست آورید.

۲۶. عدد ۲ یک ریشهٔ اولیهٔ ۶۷ است. آیا ۳۴ نیز یک ریشهٔ اولیهٔ ۶۷ است.

◁ ۲۷. ثابت کنید که به‌ازای هر n که $۱ < n < ۸۲$، $-n^۲$ یک ریشهٔ اولیهٔ ۸۳ است.

۲۸. آیا $x^۲ \equiv ۱ \pmod{۵۹۹۱}$ جوابی جز ۱ و -۱ دارد؟ توضیح دهید.

۲۹. ثابت کنید تمام نامانده‌های درجهٔ دوم ۲۲۷ جز یکی، ریشهٔ اولیهٔ ۲۲۷ است؟

۳۰. چه تعداد از نامانده‌های درجهٔ دوم ۳۱۳ ریشه‌های اولیهٔ ۳۱۳ نیستند؟

۳۱. تمام ریشه‌های اولیهٔ ۳۷ را که بین ۱ و ۳۶ قرار دارند به‌دست آورید.

۳۲. فرض کنید g یک ریشهٔ اولیهٔ p^3 باشد، که در آن p یک عدد اول فرد است. آیا درست است که $g^{(p-1)/2} \equiv -1 \pmod{p}$؟ توضیح دهید.

۳۳. با استفاده از اینکه ۲ یک ریشهٔ اولیهٔ ۳۷ است نشان دهید که حاصلضرب مانده‌های درجهٔ دوم ۳۷ که بین ۱ و ۳۶ قرار دارند همنهشت با -1 به پیمانهٔ ۳۷ است. دربارهٔ نامانده‌های درجهٔ دوم ۳۷ که بین ۱ و ۳۶ قرار دارند چه می‌توان گفت؟

۳۴. کوچکترین ماندهٔ مثبت حاصلضرب تمام ریشه‌های اولیه ۲۹ بین ۱ و ۲۹ چیست؟

۳۵. فرض کنید h یک نامانده درجهٔ دوم ۱۴۹ باشد که مرتبه‌اش ۴ نیست. آیا h یک ریشهٔ اولیهٔ ۱۴۹ است؟

۳۶. اگر ۲ یک ریشهٔ اولیهٔ ۲۱۱ باشد، اندیس -1 در پایهٔ ۲ چقدر است؟

۳۷. جدول اندیسهای مسأله ۲۱.۶ را برای حل همنهشتیهای زیر به‌کار برید:

(الف) $9x \equiv 14 \pmod{19}$؛

(ب) $11x^7 \equiv 13 \pmod{19}$؛

(ج) $5x^6 \equiv 17 \pmod{19}$؛

(د) $9x \equiv 7 \pmod{19}$.

۳۸. ثابت کنید که ۲ یک ریشهٔ اولیهٔ ۵۳ است. با استفاده از این مطلب کوچکترین ماندهٔ مثبت تمام جوابهای $45x^{20} \equiv 31 \pmod{53}$ را پیدا کنید.

۳۹. (الف) بدون یافتن جواب، ثابت کنید که $x^5 \equiv 8 \pmod{89}$ حلپذیر است. چند جواب دارد؟

(ب) با استفاده از اینکه ۳ یک ریشهٔ اولیهٔ ۸۹ است جوابهای $x^6 \equiv 8 \pmod{89}$ را به‌دست آورید.

۴۰. نشان دهید که ۲ یک ریشهٔ اولیهٔ ۶۷ است، و با استفاده از این مطلب کوچکترین مانده‌های مثبت تمام ریشه‌های $x^3 \equiv -3 \pmod{67}$ را تعیین کنید.

۴۱. کوچکترین مانده‌های مثبت تمام جوابهای $16^x \equiv 9 \pmod{61}$ را به‌دست آورید. (راهنمایی: ۲ یک ریشهٔ اولیهٔ ۶۱ است و $\text{ind } 9 = 12$.)

۴۲. (الف) ثابت کنید که ۳ یک ریشهٔ اولیهٔ ۴۲ است.

(ب) با استفاده از اندیسها کوچکترین مانده‌های مثبت تمام جوابهای $x^9 \equiv 27 \pmod{43}$ را پیدا کنید.

۴۳. کوچکترین ماندهٔ مثبت $x^3 \equiv 1 \pmod{37}$ را به‌دست آورید. (راهنمایی: ابتدا نشان دهید که ۲ یک ریشهٔ اولیهٔ ۳۷ است و $\text{ind } 11 = 30$.)

۴۴. با استفاده از اندیسها تمام جوابهای $۱۱x^{۷} \equiv ۷(\mathrm{mod}\, ۳۷)$ را پیدا کنید.

۴۵. تعداد جوابهای همنهشتیهای زیر را به‌دست آورید: (الف) $x^{۹} \equiv ۲۷(\mathrm{mod}\, ۴۳)$؛ (ب) $x^{۹} \equiv ۲۷(\mathrm{mod}\, ۶۸۶)$.

۴۶. نشان دهید که $x^{۵} \equiv ۲۶(\mathrm{mod}\, ۷۱)$ جواب دارد، و تمام جوابها را به‌دست آورید. (راهنمایی: ۷ یک ریشهٔ اولیهٔ ۷۱ است و $\mathrm{ind}\, ۲۶ \equiv ۴۵$.)

۴۷. تعداد جوابهای همنهشتیهای زیر را به‌دست آورید:

(الف) $x^{۱۲} \equiv ۴۵(\mathrm{mod}\, ۵۸)$؛

(ب) $۱۳x^{۷} \equiv ۷(\mathrm{mod}\, ۵۸)$؛

(ج) $۴x^{۲۰} \equiv ۲۳(\mathrm{mod}\, ۴۳)$.

۴۸. به‌ازای چه مقادیری از c معادله $cx^{۶} \equiv ۱۷(\mathrm{mod}\, ۱۹)$ حلپذیر است؟

۴۹. اثبات یا رد کنید: اگر p عدد اولی به‌صورت $۶k - ۱$ باشد و $(a, p) = ۱$، آنگاه $x^{۳} \equiv a(\mathrm{mod}\, p)$ جواب یکتا دارد.

ملاحظاتی برای فصل ۶

۱. زمانی که گاوس کارش را در مورد ریشه‌های اولیه (در سن ۱۶ سالگی!) شروع کرد، از کارهای قبلی که توسط لامبرت، اویلر، لژاندر، و دیگران انجام شده بود اطلاعی نداشت. انگیزهٔ اولیهٔ او (همانند انگیزهٔ لامبرت) از بررسی بسط اعشاری کسرهای a/b، و به‌ویژه $۱/p$، که در آن p عدد اولی بجز ۲ و ۵ است پدید آمد. مثلاً، توجه می‌کنیم که $۱/۷ = ۰٫\overline{۱۴۲۸۵۷}$، $۱/۱۱ = ۰٫\overline{۰۹}$، و $۱/۱۳ = ۰٫\overline{۰۷۶۹۲۳}$. لذا بسط اعشاری $۱/۷$ دوره‌یی با دورهٔ ۶ است، $۱/۱۱$ دارای دورهٔ ۲ است، در حالی‌که $۱/۱۳$ دارای دورهٔ ۶ است.

اگر دربارهٔ روند «تقسیم طولانی» معمولی برای یافتن بسط اعشاری $۱/p$ فکر کنیم، تا حدی به آسانی می‌بینیم که این بسط دوره‌یی با دورهٔ k است اگر و تنها اگر k کوچکترین عدد صحیح مثبتی باشد که باقیماندهٔ تقسیم ۱۰^{k} بر p برابر ۱ باشد، یعنی، اگر و تنها اگر مرتبهٔ ۱۰ به پیمانهٔ p برابر k باشد. لذا بنابر (i.۲.۶)، دورهٔ بسط اعشاری $۱/p$ یک مقسوم‌علیه $p - ۱$ است. گاوس می‌خواست اعداد اول p (مثلاً، $p = ۷$) را که دورهٔ آنها $p - ۱$ است پیدا کند. این اعداد دقیقاً همان اعداد اول p هستند که برای آنها ۱۰ یک ریشهٔ اولیه است (مسألهٔ ۲۶.۶ را ببینید).

در مورد دوره‌های بسطهای اعشاری مطلب فراوانی است و زمینهٔ به‌کارگرفتن اساسی مفاهیم مطرح‌شده در این فصل است. (مقدمه‌ای در نظریهٔ اعداد تألیف گ. ه. هاردی و اِ. م. رایت[1]، و

1. G. H. Hardy and E. M. Wright

جلد اول از تاریخ نظریه اعداد نوشتهٔ ل. ی. دیکسن[1] را ببینید.)

۲. آیا عدد صحیحی مانند a وجود دارد به‌طوری که a ریشهٔ اولیهٔ بی‌نهایت عدد اول p باشد؟ گاوس حدس زد که عدد ۱۰ ریشهٔ اولیهٔ تعداد نامتناهی عدد اول است. در سال ۱۹۲۷، امیل آرتین[2] (۱۸۹۸ـ۱۹۶۲) حدس کلی زیر را ارائه داد: هر عدد صحیح a با $a \neq -1$ و مربع نبودن a، ریشهٔ اولیهٔ بی‌نهایت عدد اول است.

می‌توان نشان داد (مسألهٔ ۴۶.۶ را ببینید) که ۳ یک ریشهٔ اولیهٔ هر عدد فرما، یعنی، اعداد اولی به‌صورت $F_n = 2^{2^n} + 1$، است. این رابطه نشان می‌دهد که ۳ یک ریشهٔ اولیهٔ بی‌نهایت عدد اول است به شرطی که ثابت شود بی‌نهایت عدد اول فرما وجود دارد. حدود ۳۵۰ سال پیش فرما می‌دانست که F_4 اول است، ولی معلوم نیست که بعد از F_4 عدد اولی وجود داشته باشد.

بنابر مسألهٔ ۴۳.۶، اگر q عدد اولی به‌صورت $4k + 1$ و $p = 2q + 1$ نیز اول باشد، آنگاه ۲ یک ریشهٔ اولیهٔ p است. اما معلوم نیست که تعداد نامتناهی اعداد اول p و q به این‌صورت وجود داشته باشد.

دلیل محکم برای حدسیهٔ آرتین وجود دارد. فرض کنیم $P_q(x)$ بخشی از اعداد اولِ کوچکتر از x یا مساوی با x باشد که g یک ریشهٔ اول آنهاست. حدس زده شده است که $\lim_{x\to\infty} P_q(x)$ وجود دارد و مثبت است وقتی که g نه -1 باشد و نه یک مربع کامل؛ در واقع، یک فرمول صریحی برای مقدار این حد حدس وجود دارد که با شواهد عددی به‌خوبی همخوانی دارد. C. Hooley نشان داده است که این‌فرمول نتیجه‌ای از تعمیم فرضیه‌های ریمان است. بدون استفاده از هیچ‌یک از فرضهای ثابت نشده، محققان زیر: R. Gupta، P. M. Ram Murty، D. R. Heath-Brown، و H. Iwaniec کارهای قابل‌توجهی در جهت اثبات حدس آرتین انجام داده‌اند. برای مثال، اکنون معلوم شده است که همهٔ اعداد اول بجز دو تا، ریشهٔ اولیهٔ بی‌نهایت عدد اول هستند. ولی، عجیب اینکه می‌توان گفت، هیچ عدد اول مشخصی که ریشهٔ اولیهٔ بی‌نهایت عدد اول باشند شناخته نشده است. جهت اطلاعات بیشتر، به مرجع زیر مراجعه کنید:
Ribenboim's *The Book of Prime Number Records*.

۳. وجود ریشهٔ اولیهٔ m یک تعبیر نظریهٔ گروهی به‌ویژه ظریفی دارد. گروه ضربی به پیمانهٔ m، با عمل ضرب به پیمانهٔ m، متشکل از اعداد صحیح $0 \leq x < m$ است که نسبت به m اول‌اند. عدد g یک ریشهٔ اولیهٔ m است اگر و تنها اگر g این گروه را تولید کند، بدین معنی که اگر عناصر گروه همگی توانهای g باشند. گروهی که تنها با یک عنصر تولید شده باشد یک گروه دوری

1. L. E. Dickson 2. Emil Artin

خوانده می‌شود. در وضعیت، این گروه دارای $\phi(m)$ عنصر است. از آنجا که دوری است، به‌طور مجرد. گروهی که عناصرش ۰، ۱، . . .، $\phi(m) - ۱$ هستند، تحت عمل ضرب به پیمانهٔ $\phi(m)$، یکی است. این دلیلی است بر مشخصهٔ لگاریتم گونهٔ اندیسها.

درکارهای اخیر مربوط به روشهای مبتنی بر نظریه اعداد در رمزنویسی، اگر پیمانهٔ اول p و یک ریشهٔ اولیه از p مانند g مفروض باشند، اغلب اندیس a به‌عنوان لگاریتم گسسته a نامیده می‌شود. کوششهای قابل‌توجهی صرف یافتن الگوریتمهای کارآمد برای محاسبهٔ لگاریتم گسسته صورت گرفته است. اگر a باقیماندهٔ تقسیم g^k بر p باشد، محاسبهٔ a با روش مربع کردن مکرر نسبتاً آسان است. اما، عکس مسأله، یعنی، یافتن k وقتی a مفروض است (یعنی، مسألهٔ یافتن لگاریتم گسستهٔ a)، به نظر می‌رسد که برای اعداد بزرگ اول p از لحاظ محاسبه خیلی مشکلی باشد.

شرح مختصری از زندگینامه‌ها

آدرین ـ ماری لژاندر در ۱۷۵۲ در یک خانوادهٔ ثروتمند در پاریس متولد شد. بعد از تکمیل تحصیلاتش در دبیرستان دولتی مازارین[1] در ۱۸ سالگی، استقلال مالیش این امکان را فراهم ساخت که چند سالی به پژوهشهای محض بپردازد. در ۱۷۸۲، بر امر نوشتن مقاله‌ای در پرتابه‌ها برندهٔ جایز آکادمی برلین شد. لژاندر ریاضیدان بزرگی بود و کارهای ماندگار در نظریه اعداد انجام داد. ولی بدشانسی او این بود که در عصر لاگرانژ و گاوس زندگی می‌کرد و کمتر از آنچه که شایسته‌اش بود شناخته شد.

لژاندر اولین اثبات کامل این مطلب را که هر عدد اول یک ریشهٔ اولیه دارد ارائه داد. همچنین اولین کسی بود که تعداد نمایشهای یک عدد صحیح به‌صورت مجموع دو مربع را معین و ثابت کرد که هر عدد صحیح مثبت فرد که به‌صورت $۸k + ۷$ نباشد مجموع سه مربع است. (طولی نکشید که بعد از آن گاوس یک برهان کاملتر ارائه داد.) لژاندر قضیهٔ اعداد اول و قانون تقابل مربعی را حدس زد ولی نتوانست آنها را اثبات کند. همچنین حدس زد که هر تصاعد عددی مناسب بی‌نهایت، عدد اول دارد.

تقدیر چنین‌بود که کارهای لژاندر در نظریهٔ صورتهای درجه دوم، مانند کارهای لاگرانژ، به‌زودی تحت‌الشعاع کارهای گاوس قرارگیرند. شاید زیباترین اثر لژاندر بیان وجود جواب ناصفر برای معادلهٔ $ax^۲ + by^۲ + cz^۲ = ۰$ باشد. علاوه‌بر تحقیقاتش در نظریه اعداد، لژاندر در حوزه‌های کاربردی‌تر، نظیر معادلات دیفرانسیل و مکانیک سماوی کار کرد، و در افتخارگاوس برای ابداع روش کمترین مربعات سهیم است. همراه با لاگرانژ، لژاندر نقش عمده‌ای در طرح‌ریزی دستگاه متریک ایفا کرد.

1. Mazarin

در سالهای آخر عمرش، تحقیقات لژاندر بر انتگرالهای بیضوی متمرکز شد، و دریافت که موضوع مورد علاقه‌اش حوزهٔ وسیعی از تحقیقات آبل و ژاکوبی می‌شود.

در ۷۵ سالگی، لژاندر استدلالی از دیریکله را کامل کرد که نتیجهٔ آن برقراری آخرین قضیهٔ فرما در حالت $n = 5$ بود. لژاندر در ۱۸۸۳ در پاریس درگذشت.

مراجع

Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke, Yale University Press, New Haven, Connecticut, 1966.

گاوس یک معرفی بسیار مفصل از ریشه‌های اولیه و اندیسها به‌دست می‌دهد. در بیشتر موضوعات بعدی روند را به‌کار می‌گیرد که اساساً با روندی که در تحقیقات آمده است یکی است.

۷

اعداد اول

وجود بی‌نهایت عدد اول، و اصول تجزیهٔ یک عدد صحیح مثبت به حاصلضرب اعداد اول بر اقلیدس معلوم بوده است. در این فصل، بعضی ویژگیهای عمیقتر اعداد اول را بررسی خواهیم کرد، از جمله، قضیهٔ اعداد اول که در تخمین تعدادِ اعدادِ اولِ کوچکتر از یک عدد مفروض بحث می‌کند، و قضیهٔ دیریکله در نامتناهی بودن تعداد اعداد اول در تصاعدهای حسابی.

قضیهٔ اعداد اول نخستین بار در حدود سال ۱۸۰۰ فرمولبندی شد اما تا اواخر قرن نوزدهم اثبات نگردید؛ قضیهٔ دیریکله در ۱۸۳۷ اثبات شده بود. اثبات هر دو قضیه بسیار مشکل و خارج از محدودهٔ این کتاب است. ولی، قابل توجه است که برهان استانداردِ هر کدام شامل مفاهیم و تکنیکهایی از نظریهٔ توابع متغیرهای مختلط است. لذا، حتی اگر بتوان قضیه‌ها را برحسب مفاهیمِ مبتنی بر نظریهٔ اعداد به‌سادگی بیان کرد، در برهانها مفاهیمی به‌کار می‌روند که به‌کلی از مفاهیمِ عنوان‌شده در یک درسِ اولِ نظریهٔ اعداد خارج‌اند.

وجود اعداد اول به‌صورت $۲^n - ۱$ را نیز بررسی می‌کنیم. این اعداد، اعداد مرسن نامیده

می‌شوند و به‌طور مرسوم بزرگترین اعدادِ اولِ شناخته‌شده را تولید کرده‌اند. (در زمان نوشتن این کتاب، بزرگترین عدد مرسن معلوم عدد ۱ − ۲^۸۵۹۴۳۳ بود.)* هر چند اعدادِ اولِ مرسن تا قرن هفدهم به تفصیل مطالعه نشدند، ولی با اعداد تام، یعنی، اعداد صحیحی که با دو برابر مجموع مقسوم‌علیه‌های مثبت خود مساوی‌اند، و مفهومی خیلی قدیمی‌تر است، دارای ارتباط نزدیکی هستند. بررسی اعداد تام به یونانیان باستان برمی‌گردد، و یک روشی برای تولید اعداد تام زوج در اصول اقلیدس آمده است.

این فصل را با تعدادی مسألهٔ باز که با اعداد اول ارتباط دارند به پایان می‌بریم، معروفترین این اعداد حدسیهٔ گُلدباخ است: هر عدد صحیح زوجِ بزرگتر از ۲ مجموع دو عددِ اول است. این حدسیه در نامه‌ای به اویلر در ۱۷۴۲ مطرح شد؛ در بیش از ۲۵۰ سال بعد از آن، روی این مسأله کارهای فراوانی انجام گرفته است، اما لاینحل مانده است.

به دلیل ماهیت مطالب مورد بحث، بیشتر این فصل توضیحی است. در بسیاری از حالتها، ارائه آنها در یک درس مقدماتی نظریهٔ اعداد یا بسیار مشکل است، یا احکام هنوز مسائلی بازند.

قضیه‌هایی برای فصل ۷

غربال اراتستن

در فصل ۱، برهان اقلیدس مبنی بر وجود تعداد نامتناهی عدد اول را ارائه کردیم. بعد، روشی را برای یافتن تمام اعدادِ اولِ نابزرگتر از یک عدد صحیح مفروض مطرح می‌کنیم. این الگوریتم به‌عنوان غربال اراتستن معروف است و به نام مخترع آن، ریاضیدان یونانی اراتستن[1] (۱۹۴–۲۷۶ ق‌م)، نامگذاری شده است. اراتستن کتابدار کتابخانهٔ معروف اسکندریه بود و شاید به دلیل اولین محاسبهٔ دقیق محیط کرهٔ زمین، که از اوست، بهتر به‌خاطر آید.

فرض کنیم n عدد صحیح مثبتی باشد. ابتدا همهٔ اعدادِ صحیح از ۲ تا n را فهرست می‌کنیم. چون ۲ اول است، هر مضرب ۲ که از ۲ بزرگتر است مرکب است، لذا همهٔ مضارب ۲ را که از ۲ بزرگترند در فهرست خود خط می‌زنیم. واضح است، که اولین عددِ بعد از ۲ که خط نخورده است، یعنی ۳، اول است. حال همهٔ مضارب ۳ را که بزرگتر از ۳ هستند و قبلاً حذف نشده‌اند خط می‌زنیم. عددِ بعد از ۳ در فهرست ۵ است، که بایستی اول باشد، زیرا در غیر این‌صورت، بر یک عددِ اولِ کوچکتر از ۵ بخشپذیر خواهد بود، لذا قبلاً باید از فهرست حذف شده باشد. عمل را به همین ترتیب ادامه می‌دهیم: در هر مرحلهٔ معین، بعد از آنکه تمام مضارب یک عدد اولِ مفروض را خط زدیم، عدد صحیح بعدی در فهرست که خط نخورده است اول خواهد بود، و سپس همهٔ

* در ۲۶ اردیبهشت ۱۳۸۳ عدد ۱ − $2^{24036583}$ به‌عنوان بزرگترین عدد اول مرسن معرفی شد.ـم.

1. Eratosthenes

مضارب آن را حذف می‌کنیم (بجز خودش). وقتی که نتوان عمل را بیشتر از این ادامه داد، اعداد باقیمانده همگی اعدادِ اولِ نابزرگتر از n را به‌دست می‌دهند.

توضیحات. ۱. اراتستن دریافت که فقط لازم است عمل را تا یافتن عدد اولی بزرگتر از $\sqrt{n}$ ادامه داد؛ در این‌صورت همهٔ اعداد صحیحی که در فهرست می‌مانند بایستی اول باشند. زیرا اگر $k \leq n$ مرکب باشد، آنگاه k مقسوم‌علیه اولی مانند p دارد که $p \leq \sqrt{n}$ (مسألهٔ ۱.۷ را ببینید)، و لذا k قبلاً از فهرست ما حذف شده است.

۲. غربال اراتستن یک روش عملی برای تعیین اول بودن n نیست، برای مثال، یک روش سریعتر، مانند بالا، توجه به این نکته است که اگر یک عدد صحیح n اول نباشد، آنگاه عامل اولی مانند p دارد که $p \leq \sqrt{n}$. لذا برای بررسی اول بودن n، فقط لازم است که بخشپذیری n را بر عدد اولی نابزرگتر از $\sqrt{n}$ بررسی کنیم. ولی، غربال اراتستن یک کاربرد نسبتاً غیرمنتظره دارد: معمولاً به عنوان محکی برای آزمایش سرعتِ یک کامپیوتر به‌کار می‌رود.

اعداد تام

(۱.۷) تعریف. عدد صحیح مثبت n عدد تام خوانده می‌شود اگر n با مجموع مقسوم‌علیه‌های مثبتش، بجز خود n، برابر باشد.

بنابراین، n تام است اگر و تنها اگر $\sigma(n) = ۲n$، که در آن $\sigma(n)$ مجموع همهٔ مقسوم‌علیه‌های مثبت n (از جمله خود n) است.

موضوع اعداد تام به روزگار باستان برمی‌گردد، و در طول تاریخ، ویژگیهای مرموز بسیاری به آنها نسبت داده شده است، ریاضیدانان یونانی اولیه علاقهٔ ویژه‌ای به آنها داشتند، هر چند که در زمان اقلیدس تنها چهار عدد تام شناخته شده بود (۶، ۲۸، ۴۹۶، و ۸۱۲۸). این اطلاع کم به این حدسیه منجر شده بود که اعداد تام به تناوب به ۶ و ۸ ختم می‌شوند. گرچه این نادرست است (پنجمین و ششمین اعداد تام عبارت‌اند از ۳۳ ۵۵۰ ۳۳۶ و ۸ ۵۸۹ ۸۶۹ ۰۵۶)، ولی اینکه هر عدد تام زوج به ۶ و ۸ ختم می‌شود درست است. (مسألهٔ ۹.۷ را ببینید.)

اقلیدس درکتاب اصول روش زیر را برای یافتن اعداد تام زوج بیان کرده است.

(۲.۷) قضیهٔ (اقلیدس). اگر $۲^n - ۱$ اول باشد، آنگاه $۲^{n-۱}(۲^n - ۱)$ عدد تام است.

برهان. فرض کنیم $N = ۲^{n-۱}p$، که $p = ۲^n - ۱$. چون p اول است، روشن است که مقسوم‌علیه‌های N به‌صورت ۲^i یا $۲^i p$ هستند که $۰ \leq i \leq n - ۱$. لذا

$$\begin{aligned}\sigma(N) &= ۱ + ۲ + \cdots + ۲^{n-۱} + p + ۲p + \cdots + ۲^{n-۱}p \\ &= (۱ + p)(۱ + ۲ + \cdots + ۲^{n-۱}) \\ &= (۱ + p)(۲^n - ۱) = ۲^n(۲^n - ۱) = ۲N\end{aligned}$$

در نتیجه

$$N = ۲^{n-۱}(۲^n - ۱)$$

بنابراین N عدد تام است.

یک پرسش طبیعی این است که آیا عکس قضیهٔ اقلیدس برقرار است، یعنی، آیا هر عدد تام زوج به‌صورتی است که در (۲.۷) آمده است؟ تقریباً ۲۰۰۰ سال طول کشید تا بالاخره اویلر به این سؤال جواب داد:

(۳.۷) قضیهٔ (اویلر). هر عدد تام زوج به‌صورت $۲^{n-۱}(۲^n - ۱)$ است که در آن $۲^n - ۱$ اول است.

برهان. اگر N عدد تام زوجی باشد، آنگاه $\sigma(N) = ۲N$. فرض کنیم $N = ۲^{n-۱}m$، که در آن $n \geq ۲$ و m فرد است. چون $(۲^{n-۱}, m) = ۱$ و σ ضربی است (توضیح بعد از (۲۰.۱) را ببینید)، داریم

$$۲^n m = ۲N = \sigma(N) = \sigma(۲^{n-۱})\sigma(m) = (۲^n - ۱)\sigma(m)$$

از حل معادلهٔ $۲^n m = (۲^n - ۱)\sigma(m)$ برحسب $\sigma(m)$، داریم

$$\sigma(m) = m + m/(۲^n - ۱)$$

لذا $m/(۲^n - ۱)$ عددی صحیح است، و بنابراین m و $m/(۲^n - ۱)$ هر دو مقسوم‌علیه‌های m هستند. چون $\sigma(m) = m + m/(۲^n - ۱)$، در نتیجه m و $m/(۲^n - ۱)$ تنها مقسوم‌علیه‌های مثبت m می‌باشند. لذا $m/(۲^n - ۱) = ۱$، یعنی، $m = ۲^n - ۱$، و m اول است.

این بند را با دو سؤال مهم باز در مورد اعداد تام می‌بندیم. سؤال اول این است که آیا عدد تام فرد وجود دارد؟ اگر عدد تام فرد وجود داشته باشد معلوم شده است که بایستی بزرگتر از $۱۰^{۳۰۰}$ باشد و حداقل هشت عامل اول متمایز داشته باشد! بنابراین، مدارک محاسبه‌یی ظاهراً می‌گویند که اعداد تام فرد وجود ندارند.

سؤال دوم این است که آیا تعداد نامتناهی عدد تام زوج وجود دارد؟ در دوران باستان چهار عدد شناخته شده بود، ولی پنجمی تا سدهٔ پانزدهم کشف نشده بود. تاکنون (در زمان تألیف کتاب) ۳۳ عدد تام زوج شناخته شده است، که ۲۱ عدد آخر از سال ۱۹۰۰ به بعد کشف شدند.* تا این زمان بزرگترین عدد از این نوع $۲^{۲۸۵۹۴۳۲}(۲^{۲۸۵۹۴۳۳}-۱)$ است که تقریباً دارای ۵۱۷۴۳۰ رقم است.** به هر حال، وجود بی‌نهایت عدد تام زوج به‌عنوان یک سؤال باز باقیمانده است.

اعداد اول مِرسِن

با توجه به قضیه‌های اقلیدس و اویلر، وجود تعداد نامتناهی عدد تام زوج با موجود بودن تعداد نامتناهی عدد اول به‌صورت $۲^n-۱$ هم‌ارز است. *این اعداد اول، پس از آنکه راهب فرقهٔ فرانسیسیان در سدهٔ هفدهم به مطالعهٔ آنها پرداخت، به اعداد مِرسِن معروف شدند.*

(۴.۷) تعریف. فرض کنیم n عدد صحیح مثبتی باشد. mام عدد مِرسِن عدد صحیح $M_n=۲^n-۱$ است. اگر M_n اول باشد، آن را عدد اول مرسن می‌نامند.

کلی‌تر بگوییم می‌توانیم جویا شویم که چه وقت $a^n-۱$ برای $n\geq ۲$ اول است. نشان دادن اینکه باید $a=۲$ و n اول باشد مشکل نیست (مسألهٔ ۴.۷ را ببینید). لذا اگر M_n اول باشد، بایستی n اول باشد؛ بنابراین، برای جستجوی اعدادِ اولِ از این نوع، کافی است اعداد اول M_p مرسن را که p اول است در نظر بگیریم.

مِرسِن در اثرش اندیشه‌های فیزیک ریاضی[1] مربوط به سال ۱۶۴۴ حدس زد که M_p برای تمام اعداد اول $p<۲۵۷$ مرکب است، بجز به‌ازای ۱۱ مقدارِ ۲، ۳، ۵، ۷، ۱۳، ۱۷، ۱۹، ۳۱، ۶۷، ۱۲۷، و ۲۵۷. در ۱۷۷۲، اویلر نشان داد که $M_{۳۱}$ اول است. ولی در ۱۸۷۶، لوکا ثابت کرد که $M_{۶۷}$ مرکب است، هر چند که نتوانست عاملها را محاسبه کند. تقریباً سه سده طول کشید تا حدسیهٔ مِرسِن به‌طور کامل پاسخ داده شود. حدس مِرسِن ــ احتمالاً به دلیلی که حدس بود ــ به‌ازای پنج مقدارِ کمتر از ۲۵۷ رد شد.

درکوشش برای یافتن عاملهای اعداد مِرسِن، فرما دریافت که اگر p اول باشد، باقیماندهٔ هر عامل اول $۲^p-۱$ در تقسیم بر p برابر ۱ است. این دریافت در قضیهٔ زیر آمده است، که نخست در فصل ۳ اثبات شد. برای تکمیل مطلب آن را در اینجا بیان می‌کنیم. برهان در اساس شبیه

* اکنون ۴۲ عدد تام زوج شناخته شده است (تا ۱۸ فوریه ۲۰۰۵)، که ۳۱ عدد آخر از ۱۹۰۰ به بعد کشف شده‌اند. چهل و دومین (یا بزرگترین عدد) عبارت است از $۲^{۲۵۹۶۴۹۵۰}(۲^{۲۵۹۶۴۹۵۱}-۱)$ که تقریباً دارای ۷۸۱۶۲۳۰ رقم است!

** این اطلاعات از مترجم است.

1. Cogitata physico Mathematica

برهان (۸.۳) است، بجز آنکه از ویژگیهای مرتبهٔ یک عدد که در فصل قبل بسط داده شد استفاده شده است.

(۵.۷) قضیه. فرض کنیم p یک عدد اول فرد و q یک عامل اول $۲^p - ۱$ باشد. در این‌صورت، q به‌صورت $۲kp + ۱$ است.

برهان. چون $۲^p \equiv ۱ \pmod q$، (i۲.۶) ایجاب می‌کند که $\operatorname{ord}۲ | p$. لذا $\operatorname{ord}۲ = p$، زیرا p اول است و به‌وضوح $\operatorname{ord}۲ \neq ۱$. مجدداً بنابر (i۲.۶)، $p | q - ۱$، و لذا m وجود دارد که $q = mp + ۱$. چون q فرد است، m بایستی زوج باشد، که قضیه نتیجه می‌شود.

لذا برای یافتن عوامل اول M_p، بایستی فقط در جستجوی اعدادِ اولِ از نوع معینی باشیم. مثالهایی از این تکنیک در مسأله‌های ۱۵.۷ تا ۱۹.۷ ارائه شده است.

توضیحات. ۱. بزرگترین اعداد اول شناخته‌شده به‌طور مرسوم اعداد اولِ مِرسِن بوده‌اند، (برای یک استثنا توضیحات آخر فصل را ببینید.) هم‌اکنون ۳۳ عدد اول مرسن* (و لذا ۳۳ عدد تام زوج) شناخته شده است. بزرگترین آنها عدد $۲^{۸۵۹۴۳۳} - ۱$ است که در اوایل سال ۱۹۹۴ پس از تقریباً بیست ساعت زمان محاسبه بر روی یک اَبَر رایانه cray-2 کشف شد. دومین عدد مرسن بعد از آن $۲^{۷۵۶۸۳۹} - ۱$ است که در سال ۱۹۹۲ تقریباً با همان مقدار محاسبه به‌دست آمد. یافتن عدد رکورددار قبلی، $۲^{۲۱۶۰۹۱} - ۱$ «فقط» ۳ ساعت طول کشید.

۲. شاید مهمترین سؤال باز در رابطه با اعداد اول مِرسِن این باشد که آیا تعداد نامتناهی از این اعداد اول وجود دارند؟ یک استدلال مبتنی بر احتمال وجود دارد که نامتناهی بودن مجموعهٔ اعداد اول مِرسِن را موجه می‌سازد (Ribenboim در فصل ۶ را ببینید.)

اعداد فرما

برای یافتن اعدادِ اول به‌صورت $a^n - ۱$ دیدیم که کافی است اعداد به‌صورت $۲^p - ۱$ را که در آن p اول است در نظر بگیریم. به روش مشابه، می‌توانیم اعدادِ فردِ اول به‌صورت $a^n + ۱$ با $n > ۱$ را جستجو کنیم. برای آنکه چنین اعدادی اول باشند بایستی a زوج و n به‌صورت توانی از ۲ باشد. (مسألهٔ ۵.۷ را ببینید.) لذا به بررسی اعدادی به‌صورت $۲^{۲^n} + ۱$ هدایت می‌شویم.

(۶.۷) تعریف. یک عدد فرما عددی صحیح به‌صورت $F_n = ۲^{۲^n} + ۱$ است که در آن $n \geq ۰$. اگر F_n اول باشد، F_n یک عدد اول فرما خوانده می‌شود.

* هم‌اکنون ۴۲ عدد اول مِرسِن (و لذا ۴۲ عدد تام زوج) شناخته شده است. بزرگترین آنها $۲^{۲۵۹۶۴۹۵۱} - ۱$ است که در تاریخ ۲۹ بهمن ۱۳۸۳ توسط مارتین نواک (Martin Nowak) کشف شد. این عدد تقریباً ۷۸۱۶۲۳۰ رقم دارد. محاسبات نواک، بیش از ۵۰ ساعت روی رایانهٔ ۲٫۴ GHz Pentium4 انجام گرفته است.

به‌ازای $n = ۰, ۱, ۲, ۳, ۴$، مقادیر F_n ۳، ۵، ۱۷، ۲۵۷، و ۶۵۵۳۷ را اختیار می‌کند که همگی اول‌اند. شاید برمبنای این ملاکِ نسبتاً ناقص، فرما در نامه‌ای به فرنیکل در ۱۶۴۰ اظهار داشت که به‌ازای هر $n \geq ۰$، F_n اول است. مطابق معمول، فرما دلیلی ارائه نداد، ولی در ۱۶۵۸ ادعا کرد که با روش نزول نامتناهی برهانی داشته است. در حقیقت، این حدسیه نادرست است. حدود یک قرن بعد، در ۱۷۳۲، اویلر نشان داد که ۶۴۱ یک مقسوم‌علیه $F_۵$ است (مسألهٔ ۲۳.۲ را ببینید).

در پاسخ به سؤالی از فرنیکل در ۱۶۴۰، فرما با نشان دادن اینکه $۲^{۳۷} - ۱$ بر ۲۲۳ بخشپذیر است ثابت کرده بود که این عدد اول نیست. فرما اساساً همان استدلالِ برهان (۵.۷) را به کار برد تا نتیجه بگیرد که هر عامل اول $۲^{۳۷} - ۱$ به‌صورت $۷۴k + ۱$ است.

می‌توان استدلال مشابه را در مورد $F_۵ = ۲^{۳۲} + ۱$ به‌کار برد. اگر p عامل اولی از $F_۵$ باشد، آنگاه $۲^{۶۴} - ۱ = (۲^{۳۲} - ۱)(۲^{۳۲} + ۱) | p$؛ مانند استدلال بالا می‌توان نشان داد که به‌ازای مقداری از k، $p = ۶۴k + ۱$. چند عددِ اولِ از این نوع عبارت‌اند از: ۱۹۳، ۲۵۷، ۴۴۹، ۵۷۷، ۶۴۱، ...، و ۶۴۱ عدد $۲^{۳۲} + ۱$ را می‌شمارد. در واقع، بدین‌گونه اویلر نشان داد که $F_۵$ اول نیست، و کاملاً تعجب‌آور است که خود فرما روشی را که برای تجزیهٔ $۲^{۳۷} - ۱$ به‌کار برده بود، در مورد $۲^{۳۲} + ۱$ اجرا نکرده است.

با اندکی کار بیشتر، می‌توان نشان داد که عاملهای اول $۲^{۳۲} + ۱$ واقعاً به‌صورت $۱۲۸k + ۱$ هستند، نه فقط $۶۴k + ۱$. بعداً نشان خواهیم داد که قضیه مشابه برای عاملهای اول هر عدد فرما برقرار است. برای به‌دست آوردن عامل بیشترِ ۲ لازم است بدانیم که ۲ ماندهٔ درجهٔ دومِ کدام اعداد اولی است ((۱۲.۵ را ببینید).

(۷.۷) قضیه. فرض کنیم $n > ۱$. در این‌صورت هر عامل اولِ عدد فرمای $۲^{۲^n} + ۱$ به‌صورت $۲^{n+۲}k + ۱$ است.

برهان. فرض کنیم p یک عامل اول $۲^{۲^n} + ۱$ باشد. لذا $۲^{۲^n} \equiv -۱ \pmod{p}$، و چون $۴ | ۲^n$، همنهشتی $x^۴ \equiv -۱ \pmod{p}$ جواب دارد. لذا بنابر (۱۹.۶)، $(-۱)^{(p-۱)/(۴,p-۱)} \equiv ۱ \pmod{p}$، و بنابراین، $(p-۱)/(۴, p-۱)$ زوج است. لذا p به‌صورت $۸k + ۱$ است، و از (۱۲.۵) نتیجه می‌شود که ۲ یک ماندهٔ درجهٔ دوم p است. فرض کنیم $s^۲ \equiv ۲ \pmod{p}$؛ پس s جوابی از همنهشتی $x^{۲^{n+۱}} \equiv -۱ \pmod{p}$ است. با توسل مجدد به (۱۹.۶) مانند بالا نتیجه می‌گیریم که $(p-۱)/(۲^{n+۱}, p-۱)$ زوج است، و لذا $۲^{n+۲} | (p-۱)$، که قضیه را اثبات می‌کند.

توضیحات. ۱. فرما می‌دانست که از F_0 تا F_4 اول هستند، اما تاکنون عدد اول فرما بعد از F_4 یافت نشده است. ۸۴ عدد فرمای مرکب معلوم‌اند، که بزرگترین آنها F_{23471} است.

۲. اعداد فرما یک اثبات جالب توجه برای نامتناهی بودن مجموعهٔ اعداد اول ارائه می‌دهد. مسألهٔ ۲۴.۷ را ببینید.

اعداد اول فرما یک کاربرد غیرمنتظره در بررسی مسألهٔ کلاسیکِ ترسیم یک nـضلعی منتظم فقط به کمک خطکش و پرگار، دارد. در ۱۸۰۱، در بخشِ آخر تحقیقات حسابی، گاوس ثابت کرد که اگر $n = 2^k$ یا $n = 2^k p_1 p_2 \cdots p_m$، که $k \geq 0$ و p_iها اعداد اول فرمای متمایز هستند، آنگاه nـضلعی منتظم با کاربرد خطکش و پرگار قابل ترسیم است، و ادعا کرد که برهانی دارد برای اینکه هیچ چندضلعی منتظم دیگر با خطکش و پرگار قابل ترسیم نیست. (در ۱۸۳۷ یک اثبات توسط Wantzel به چاپ رسید.) به‌ویژه، می‌توان یک ۱۷ـضلعی منتظم را با ستاره و پرگار ترسیم کرد. این اولین ترسیم جدید از یک چندضلعی منتظم از زمان اقلیدس بوده است.

قضیهٔ اعداد اول

در فصل ۱ نشان دادیم که رخنه‌های بزرگ اتفاقی در دنبالهٔ اعداد اول وجود دارد (مسألهٔ ۲۸.۱ را ببینید). بنابراین، طبیعی است که سؤالات زیر مطرح شوند: به‌طور تقریب، چه تعداد عدد اول از عدد مفروضی کوچکترند؟ همچنین، بزرگی nامین عدد اول چه اندازه (به تقریب) است؟ (برهان اقلیدس در وجود تعداد نامتناهی عدد اول نشان می‌دهد که $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$، که در آن p_i معرف iامین عدد اول است.) هر دو سؤال توسط قضیهٔ عدد اول پاسخ داده می‌شوند.

(۸.۷) قضیهٔ اعداد اول. گیریم x یک عدد حقیقی مثبت است، و فرض می‌کنیم $\pi(x)$ معرف تعداد اعداد اولِ نابیشتر از x باشد. اگر x را به اندازهٔ کافی بزرگ اختیار کنیم، می‌توانیم نسبت $\pi(x)/(x/\log x)$ را به‌دلخواه به ۱ نزدیک کنیم.

به بیان غیررسمی‌تر، قضیهٔ اعداد اول اظهار می‌دارد که اگر x به اندازهٔ کافی بزرگ باشد، تعدادِ اعدادِ اولِ نابیشتر از x تقریباً برابر $x/\log x$ است. (در اینجا $\log x$ معرف لگاریتم طبیعی x، یعنی لگاریتم در پایهٔ e است.) این مطلب در ۱۷۹۳ توسط گاوس و در ۱۷۹۸ به‌وسیلهٔ لژاندر حدس زده شده بود؛ مبنای حدس مقادیر $\pi(x)$ به‌ازای $x < 10000$ بوده است که از جدولهای اعداد اول، که بعداً در دسترس قرار گرفتند، به‌دست آمده‌اند.

قضیهٔ اعداد اول یک قضیهٔ بسیار سنگینی است؛ در واقع، تا نزدیک به یک سده بعد اثبات

نشده بود. در ۱۸۹۶، برهانهایی مستقل از قضیهٔ اعداد اول توسط ژاک آدامار[1] (۱۹۶۳ـ۱۸۶۵) و شارل‌ـژان دولاواله‌ـپوسن[2] (۱۹۶۲ـ۱۸۶۶) ارائه گردید، که از تکنیکهایی از نظریهٔ توابع یک متغیر مختلط برگرفته از کار ریمان (۱۸۶۶ـ۱۸۲۶)، استفاده شده بود. در واقع، اکنون معلوم شده است که اگر $x \geq ۱۷$، آنگاه $\pi(x) \geq x/\log x$.

اگر p_n نشانگر nامین عدد اول باشد، روشن است که $\pi(p_n) = n$. لذا، با اختیار $x = p_n$ در (۸.۷) و استفاده از این مطلب که اگر x بزرگ باشد، $\log x\,/\log(x/\log x)$ تقریباً برابر با ۱ است، می‌توان نشان داد که $n\log n/p_n$ به ۱ میل می‌کند وقتی‌که n به بی‌نهایت میل کند. بنابراین بیان هم‌ارز زیر از قضیهٔ اعداد اول را داریم:

(۹.۷) قضیهٔ اعداد اول. اگر p_n معرف nامین عدد اول باشد، حد $p_n/(n\log n)$ برابر ۱ است وقتی که n به بی‌نهایت میل کند.

توضیح. در واقع، معلوم شده است که به‌ازای هر n، $p_n > n\log n$. «خطای» $p_n - n\log n$ ممکن است کاملاً بزرگ باشد، اما اگر n بزرگ باشد، خطا خیلی کوچکتر از $n\log n$ است.

از قضیهٔ اعداد اول نتیجه می‌شود که اگر $x > ۱$، یک عدد ثابت C وجود دارد به‌طوری که $\pi(x)/x < C/\log x$؛ لذا نسبت $(x - \pi(x))/x$ به ۱ میل می‌کند وقتی که x به بی‌نهایت میل کند. می‌توان این مطلب را به طریق زیر تعبیر کرد: از آنجا که $n - \pi(n)$ تعداد اعداد صحیح مثبت نابیشتر از n است که اول نیستند، نسبت $(n - \pi(n))/n$ معرف نسبت اعداد مرکب در میان نخستین n عدد صحیح است. لذا، بدین معنی که این نسبت به ۱ میل می‌کند، قضیهٔ اعداد اول ایجاب می‌کند که «تقریباً همهٔ» اعداد صحیح مثبت مرکب باشند.

ولی، به یک تعبیر، اعداد اول مخصوصاً کمیاب نیستند، زیرا تابع $\log x$ خیلی کند نمو می‌کند. مثلاً، $\log ۱۰^{۱۰۰}$ تقریباً برابر با ۲۳۰ است. لذا اگر عدد صحیح N را «به تصادف» در همسایگی $۱۰^{۱۰۰}$ انتخاب کنیم، احتمال اینکه N اول باشد تقریباً ۱/۲۳۰ است. اگر مطمئن باشیم که N بر ۲، ۳، یا ۵ بخشپذیر نیست، احتمال اینکه N عدد اول باشد به تقریباً ۱/۶۱ بالغ می‌شود، و با غربالِ سایر اعداد اول کوچک می‌توانیم آن‌را به‌طور قابل‌ملاحظه‌ای زیاد کنیم. این بدان معنی است که اگر یک آزمون تعیین اول بودن مؤثر به‌کار بریم، یافتن اعداد اول خیلی بزرگ کاملاً شدنی است.

توضیحات. ۱. یکی از نتایج قضیهٔ اعداد اول این است که اگر a و b اعداد صحیح مثبت باشند و $a < b$، آنگاه اگر x به اندازهٔ کافی بزرگ باشد حداقل یک عدد اول بین ax و bx قرار دارد.

1. Jacques Hadamard 2. Charles-Jean de la Vallée-Poussin

با انتخاب $a = ۱$ و $b = ۱ + \epsilon$، که در آن ϵ عدد مثبت دلخواهی است، نتیجهٔ جالب زیر را داریم: به‌ازای همهٔ مقادیر به اندازهٔ کافی بزرگ n، دست‌کم یک عدد اول بین n و $n(۱ + \epsilon)$ قرار دارد.

۲. ادموند لاندو[1] ثابت کرد که وقتی n به اندازهٔ کافی بزرگ باشد آنگاه $\pi(۲n) < ۲\pi(n)$. از این نابرابری نتیجه می‌شود که اگر n به‌قدر کافی بزرگ باشد، تعداد اعداد اول بین ۱ و n از تعداد اعداد اولِ بین n و $۲n$ بیشتر است.

۳. اینک یک نتیجهٔ جالب دیگر از قضیهٔ اعداد اول: مجموعهٔ همهٔ اعداد به‌صورت $\pm p/q$ که در آن p و q اعداد اول هستند، در R (مجموعهٔ اعداد حقیقی) چگال است. یا به‌طور هم‌ارز، به‌ازای هر عدد حقیقی x، عددی به‌صورت $\pm p/q$ وجود دارد که تا به‌خواهیم به x نزدیک است.

این بخش را با یک قضیه، معروف به اصل موضوع برتران، که وجود یک عدد اول بین n و $۲n$ را تضمین می‌کند، به پایان می‌بریم. ژوزف برتران در ۱۸۴۵ حدس خود را ارائه داد، او صحت ادعای خود را برای جمیع مقادیر n تا سه میلیون بررسی کرده بود، ولی قادر به اثبات نبود. هفت سال بعد اولین اثبات توسط ریاضیدان روسی پافنوتی چبیشف (۱۸۹۴ـ۱۸۲۱) ارائه گردید. با اینکه این اثبات بسیار ساده‌تر از اثبات قضیهٔ اعداد اول است، ولی از ظرفیت این کتاب خارج است.

(۱۰.۷) قضیهٔ اصل موضوع برتران. به‌ازای هر $n > ۱$، عدد اولی بین n و $۲n$ وجود دارد.

توضیحات. ۱. یک قضیهٔ قویتر برقرار است: اگر $n > ۵$، آنگاه دست‌کم دو عدد اول متمایز بین n و $۲n$ وجود دارد. یک نتیجهٔ سادهٔ این مطلب این است که $p_{n+۲} < ۲p_n$، و لذا $p_{n+۲} < p_n + p_{n+۱}$.

۲. در ۱۸۹۲، اصل موضوع برتران توسط جیمز جوزف سیلوستر[2] به‌ترتیب زیر تعمیم یافت: اگر m و n اعداد صحیح مثبتی باشند با $m > n$، آنگاه دست‌کم یکی از اعداد m، $m + ۱$، $m + ۲$، ...، $m + n - ۱$ عامل اولی بزرگتر از n دارد. (اصل موضوع برتران با انتخاب $m = n + ۱$ نتیجه می‌شود.)

۳. یک سؤالِ بازِ قدیمی مشابه در مورد اعداد اول بین دو مربعِ متوالی وجود دارد: آیا به‌ازای هر n، بین $n^۲$ و $(n + ۱)^۲$ عدد اولی وجود دارد؟

قضیهٔ دیریکله

قضیهٔ دیریکله بررسی مسألهٔ زیر است: اگر a و b نسبت به هم اول باشند ($a \neq ۰$)، آیا تعداد نامتناهی عدد اول به‌صورت $ak + b$ وجود دارد؟ (اگر a و b عامل مشترکی مانند $d > ۱$ داشته

1. Edmund Landau 2. James Joseph Sylvester

باشند، آشکار است که به‌ازای هر k، $d|ak+b$، و لذا به‌ازای حداکثر یک مقدار k عدد $ak+b$ اول است.) قبلاً تعدادی از حالتهای خاص این مسأله را دیده‌ایم؛ مثلاً، در فصل ۱ نشان داده شد (مسألهٔ ۳۱.۱ را ببینید) که تعداد نامتناهی عدد اول به‌صورت $4k+3$ وجود دارد؛ در فصل ۵، از قانون تقابل درجهٔ دوم برای نشان دادن، مثلاً وجود بی‌نهایت عدد اول به‌صورتهای $8k+3$، $8k+5$، و $8k+7$ استفاده شد. (مسأله‌های ۲۳.۵، ۴۸.۵، ۵۰.۵، و ۵۴.۵ را ببینید.) در برهانهای این قضیه‌ها روشن است که از تکنیکهایی استفاده شده‌اند که مختص مقادیر مفروض a و b هستند.

مسألهٔ کلی، در اوایل سدهٔ نوزدهم مورد توجه زیادی قرار گرفت. در واقع، در ۱۷۸۵، لژاندر ادعا کرد که وجود بی‌نهایت عدد اول به‌صورت $ak+b$ را که a و b اعداد اول هستند، ثابت کرده است. سرانجام مسأله در ۱۸۳۷ توسط ریاضیدان آلمانی، گوستاف پ. گ. لوژون دیریکله (۱۸۵۹ـ۱۸۰۵) اثبات گردید.

(۱۱.۷) قضیهٔ دیریکله. فرض می‌کنیم که a مثبت و $(a,b)=1$. در این‌صورت $ak+b$ به‌ازای بی‌نهایت مقدار k اول است.

در برهان اصلی دیریکله از ابزاری از نظریهٔ توابع یک متغیر مختلط، به‌ویژه از ویژگیهایی از تابع زتای ریمان، که به‌ازای اعداد مختلط مناسبِ s با $\zeta(s)=\sum_1^\infty 1/n^s$ تعریف می‌شود، استفاده می‌شود. قضیهٔ دیریکله اولین کاربرد مهم تکنیکهای آنالیز در نظریهٔ اعداد را نشان می‌دهد. در واقع، قضیهٔ دیریکله و قضیهٔ اعداد اول دو قضیهٔ مهم در نظریهٔ مقدماتی اعداد هستند که برهان آنها متضمن روشهای تحلیلی است.

براهین «مقدماتی» برای این دو قضیه، یعنی در براهینی که از ویژگیهای عمیق‌تر توابع یک متغیر مختلط استفاده می‌شود، وجود دارند، ولی حتی مشکلتر هستند.

سرانجام، قضیه‌ای را بیان می‌کنیم که ترکیبی از مفاهیم قضیهٔ دیریکله و قضیهٔ اعداد اول است.

(۱۲.۷) قضیهٔ (دو لا واله پوسن). گیریم a مثبت و $(a,b)=1$، و فرض می‌کنیم $\pi_{a,b}(x)$ معرف تعداد اعداد اول به‌صورت $ak+b$ باشد که نابیشتر از x هستند. در این‌صورت با انتخاب x به اندازهٔ کافی بزرگ می‌توان نسبت $\pi_{a,b}(x)/(x\log x)$ را به‌دلخواه به $1/\phi(a)$ نزدیک کرد.

توضیحات. ۱. حد $1/\phi(a)$ مستقل از انتخاب b است؛ تا وقتی که a و b نسبت به هم اول باشند، این نسبت به مقداری میل می‌کند که فقط به a بستگی دارد.

۲. قضیهٔ زیر نتیجه‌ای از (۱۲.۷) است: اگر d_1، d_2، ...، d_m و e_1، e_2، ...، e_n مجموعه‌ای

دلخواه از ارقام باشند، که در آن e_n فرد است و $e_n \neq ۵$، آنگاه تعداد نامتناهی عدد اول وجود دارد که با ارقام $d_۱$، $d_۲$، ...، d_m شروع و به $e_۱$، $e_۲$، ...، e_n ختم می‌شوند (مسألهٔ ۴۱.۷ را ببینید).

قضیهٔ ۱۲.۷ تعبیر خیلی ظریفی دارد، که ممکن است از بیان بالا آشکار بنا شده مثلاً، اگر $a = ۴$ را اختیار کنیم، (۱۲.۷) ایجاب می‌کند که (چون $\phi(۴) = ۲$) نیمی از همهٔ اعداد اول به‌صورت $۴k + ۱$ هستند و نیمی به‌صورت $۴k + ۳$. (به‌طور دقیقتر، اگر x به اندازهٔ کافی بزرگ اختیار شود، می‌توان نسبت $\pi_{۴,۱}(x)/\pi(x)$ را به دلخواه به ۱/۲ نزدیک کرد.) اگر $a = ۸$، آنگاه $\phi(۸) = ۴$، و نتیجه می‌گیریم که یک‌چهارم همهٔ اعداد اول به‌صورت $۸k + ۱$ هستند، یک‌چهارم به‌صورت $۸k + ۳$، یک‌چهارم به‌صورت $۸k + ۵$، و یک‌چهارم به‌صورت $۸k + ۷$.

به‌طور کلی، به‌ازای یک انتخاب مفروض $a \neq ۰$، اگر $b' \equiv b \pmod a$، آنگاه n به‌صورت $ak + b'$ است اگر و تنها اگر n به‌صورت $ak + b$ باشد. لذا $\phi(a)$ مقدار اساساً متفاوت از b وجود دارند به‌طوری که a و b نسبت به هم اول‌اند، قضیهٔ (۱۲.۷) ایجاب می‌کند که به‌ازای هر مقدار مجاز b، دنبالهٔ a، $a + b$، $a + ۲b$، ...، سهم خود از اعداد اول، یعنی، کسری از اعداد اول برابر با $۱/\phi(a)$ از تعداد کل اعداد اول، را دارد.

حدسیهٔ گولدباخ

کریستیان گولدباخ[1] (۱۷۶۴ـ۱۶۹۰) در نامه‌ای به اویلر، در ۱۷۴۲، حدس زده است که هر عدد صحیحِ زوج بزرگتر از ۲ مجموع دو عدد اول است. این ادعای مشهور به حدسیهٔ گولدباخ معروف است و موضوع تحقیقات وسیعی در دو و نیم سدهٔ گذشته بوده است. گ. ه. هاردی[2] (۱۹۴۷ـ۱۸۷۷) ریاضیدان مشهور انگلیسی حدسیهٔ گولدباخ را یکی از مشکل‌ترین مسأله‌های حل‌نشدهٔ ریاضی توصیف کرده است.

(۱۳.۷) حدسیهٔ گولدباخ. هر عدد صحیح زوج بزرگتر از ۲ مجموعِ دو عددِ اول است.

به نظر می‌رسد که شواهد عددی به‌وضوح برقراری حدسیهٔ گولدباخ را تأیید می‌کنند و اینکه راههای بسیاری برای نمایش یک عدد صحیحِ زوجِ بزرگ به‌صورت مجموع دو عدد اول وجود دارند. این حدسیه برای هر عدد زوج تا ۲×۱۰^{۱۰} بررسی شده است. در ۱۹۷۳، ج. ر. چن[3] نشان داد که هر عدد صحیح زوجِ به‌قدرکافی بزرگ را می‌توان به‌صورت $p + m$ نمایش داد، که در آن p اول و m یا اول یا حاصلضرب دو عدد اول است.

گولدباخ همچنین حدس زد که هر عدد صحیحِ فردِ بزرگتر از ۷ مجموع سه عدد اول فرد

1. Christian Goldbach 2. Godfrey Harald Hardy 3. J. R. Chen

است. گرچه خودِ این حدس به‌عنوان یک مسألهٔ باز باقی مانده است، ولی ای. م. وینوگرادوف[1] (۱۹۸۳ـ۱۸۹۱) در ۱۹۳۷ ثابت کرده است که هر عدد فردِ به‌قدر کافی بزرگ مجموع سه عدد اول فرد است. در واقع، نشان داده شده است که قضیهٔ وینوگرادوف به‌ازای هر عدد صحیح فردِ بزرگتر از $3^{3^{15}}$ برقرار است؛ لذا به‌طور نظری، می‌توان قضیه را برای همهٔ اعداد صحیح فردِ مثبت بررسی کرد. ولی، حتی اگر از سریعترین زَبَر رایانه‌ها استفاده شود، این کاملاً غیرعملی است: $3^{3^{15}}$ عددی با تقریباً هفت میلیون رقم است!

مسائل باز دیگر

یکی دیگر از مسائل باز بیان می‌کند که تعداد نامتناهی زوج اول دوقلو، یعنی، زوجهای اعداد صحیح فرد متوالی که هر دو اول هستند، وجود دارد. لئوپولد کرونکر[2] (۱۸۹۱ـ۱۸۲۳) متذکر شد، ولی اثبات نکرد، که در واقع می‌توان هر عدد صحیح زوج را به بی‌نهایت طریق به‌صورت تفاضل دو عدد اول بیان کرد، که این امر به‌ویژه، ایجاب می‌کند که تعداد نامتناهی عدد اول دوقلو وجود داشته باشد.

هر چند که هیچ برهانی ارائه نشده است، ولی داده‌های عددی به برقراری حدسیهٔ اعداد اول دوقلو دلالت می‌کند. در واقع، این احتمال وجود دارد که تعداد نامتناهی اعداد اول سه‌تایی، یعنی، اعدادی به‌صورت p، $p+2$، $p+6$ که همگی اول هستند، وجود داشته باشد. (تنها سه عدد صحیح متوالی فرد که اول هستند عبارت‌اند از ۳، ۵، و ۷؛ مسألهٔ ۳.۷ را ببینید.)

در سال ۱۷۳۷، اویلر ثابت کرد که مجموع سری $\sum 1/p$ متشکل از وارون اعداد اول بی‌نهایت است (مسألهٔ ۸.۷ را ببینید). یک طریق جالب برای رسیدن به مسألهٔ اعدادِ اولِ دوقلو ملاحظهٔ مجموع $\sum 1/p + 1/(p+2)$ است، که در آن مجموع روی همهٔ اعداد اول p که $p+2$ نیز اول باشد گرفته می‌شود. اگر این مجموع بی‌نهایت باشد، یعنی، اگر این سری واگرا باشد، این مطلب حدسیه را اثبات می‌کند (زیرا واضح است که مجموع تعداد متناهی جفتهای عدد اول متناهی است.) ولی، معلوم شده است که این سری همگراست.

سرانجام، سؤال زیر را مطرح می‌کنیم: آیا فرمول ساده‌ای وجود دارد که هر عدد اول، یا حداقل فقط اعداد اول را به‌دست دهد؟ هیچ فرمول عملی معلوم نشده است، هر چند که فرما (به غلط) تصور می‌کرد که $2^{2^n}+1$ همواره اول است. در این ارتباط، قضیهٔ عجیبی توسط میلز[3] در ۱۹۴۷ ثابت شد: عدد حقیقی مثبت a وجود دارد به‌طوری که به‌ازای هر عدد صحیح مثبت n، $[a^{3^n}]$ اول است ($[x]$ معرف بزرگترین تابع عدد صحیح است). ولی، این یک طریق عملی برای تولید

1. I. M. Vinogradov 2. Leopold Kronecker 3. W. H. Mills

اعداد اول نیست، زیرا برای استفاده از این قضیه، بایستی عدد a تا یک درجهٔ بالای دقت دلخواه معلوم باشد. (معلوم شده است که می‌توان a را تقریباً ۱٫۳۰۶۴ اختیار کرد.)

ولی، مثالهای معروفی از چندجمله‌ییها وجود دارند که مقادیرشان اعداد اول بسیاری را، حداقل در آغاز، اختیار می‌کنند. اویلر در نامه‌ای به یوهان برنولی[1] در ۱۷۷۲ متذکر شده بود که چندجمله‌یی درجهٔ دوم $x^2 - x + 41$ به‌ازای $x = 0, 1, \ldots, 40$ اول است (آشکار است که به‌ازای $x = 41$ مرکب است)، ولی حتی معلوم نیست که این چندجمله‌یی تعداد نامتناهی عدد اول اختیار می‌کند.

گولدباخ در مکاتبه با اویلر در ۱۷۴۲، دریافت که یک چندجمله‌یی با ضرایب صحیح نمی‌تواند فقط مقادیر اول اختیار کند. (اثبات این مطلب دشوار نیست؛ مسألهٔ ۴۷.۷ را ببینید.) به‌طور کلی‌تر، می‌توانیم این سؤال را مطرح کنیم: آیا یک چندجمله‌یی غیرخطی یک متغیره با ضرایب صحیح وجود دارد که تعداد نامتناهی مقدار اول اختیار کند؟ چنین چندجمله‌یی شناخته نشده است. (ما توجه خود را به چندجمله‌ییهای خطی معطوف می‌کنیم زیرا، مثلاً، چندجمله‌ییهای $4x + 1$، $4x - 1$، $8x + 1$، ... همگی بی‌نهایت عدد اول تولید می‌کنند.) در مورد چندجمله‌ییهای درجهٔ دوم، مسألهٔ باز قدیمی زیر وجود دارد: آیا بی‌نهایت عدد اول به‌صورت $n^2 + 1$ وجود دارد؟

برای مطالبِ وابسته به این مسائل، و سؤالهای بازِ دیگر راجع به اعداد اول، کتاب Ribenboim را که در مراجع انتهای فصل آمده است ببینید.

مسأله‌ها و راه‌حلها

۱.۷ اگر n مرکب باشد، ثابت کنید که n عامل اولی مانند p دارد که $p \leq \sqrt{n}$.

حل. اگر n مرکب باشد، می‌نویسیم $n = ab$ که $a > 1$ و $b > 1$؛ اعداد a و b هر دو نمی‌توانند بزرگتر از $\sqrt{n}$ باشند، زیرا در غیر این‌صورت، $ab > n$. لذا یکی از دو عدد صحیح a یا b و از این‌رو n، یک عامل اول نابزرگتر از $\sqrt{n}$ دارد.

۲.۷ فرض می‌کنیم p یک عدد اول فرد باشد. ثابت کنید که هر عامل اول $2^p - 1$ به‌صورت $8k - 1$ یا $8k + 1$.

حل. در واقع نشان می‌دهیم که اگر n فرد باشد، هر عامل اول $2^n - 1$ به‌صورت مورد نظر است. فرض کنیم عدد اول q (لزوماً فرد) عدد $2^n - 1$ را بشمارد. پس $2^n \equiv 1 \pmod{q}$، و لذا $2^{n+1} \equiv 2 \pmod{q}$. اگر $a = 2^{(n+1)/2}$، آنگاه $a^2 \equiv 2 \pmod{q}$، و بنابراین ۲ یک ماندهٔ درجهٔ دوم q است. از (۱۲.۵) نتیجه می‌شود که q به‌صورت $8k \pm 1$ است.

1. Johann Bernoulli

۳.۷ ثابت کنید که تنها سه عدد متوالی فرد وجود دارند که اول هستند و عبارت‌اند از ۳، ۵، و ۷.

حل. فرض کنیم n، $n+۲$، $n+۴$ سه عدد فرد متوالی باشند، این اعداد به پیمانهٔ ۳ ناهمنهشت هستند، لذا دقیقاً یکی از آنها بر ۳ بخشپذیر است. چون این اعداد همگی اول هستند، یکی از آنها، آشکارا n، بایستی ۳ باشد.

حل (مترجم). اگر $n = ۳k+۱$، آنگاه $n+۲$ مضرب ۳ است و اگر $n = ۳k-۱$، آنگاه $n+۴$ مضرب ۳ است، لذا $n = ۳k$، و چون n اول است پس $n = ۳$.

۴.۷ اگر $n > ۱$ و a عدد طبیعی باشد به‌طوری که $a^n - ۱$ اول باشد، ثابت کنید $a = ۲$ و n اول است. (راهنمایی: از اتحاد $x^j - ۱ = (x-۱)(x^{j-۱} + x^{j-۲} + \cdots + x + ۱)$ استفاده کنید).

حل. داریم $a^n - ۱ = (a-۱)(a^{n-۱} + \cdots + a + ۱)$. روشن است $a-۱ | a^n - ۱$، و چون $a - ۱ < a^n - ۱$ و $a^n - ۱$ اول است لذا $a - ۱ = ۱$ یا $a = ۲$.

حال نشان می‌دهیم که اگر $۲^n - ۱$ اول باشد، n اول است. فرض کنیم n اول نباشد، قرار می‌دهیم $n = st$ که $۱ < s < n$ و $۱ < t < n$. با فرض $x = ۲^s$ داریم

$$۲^n - ۱ = ۲^{st} - ۱ = (۲^s)^t - ۱ = x^t - ۱ = (x-۱)(x^{t-۱} + \cdots + x + ۱)$$

آشکار است که هر دو عامل بزرگتر از ۱ هستند و لذا $۲^n - ۱$ اول نیست که خلاف فرض است.

توضیح. عکس مسألهٔ بالا درست نیست. مثلاً $۲^{۱۱} - ۱ = ۲۰۴۷ = ۲۳ \times ۸۹$.

۵.۷ اگر $a \geq ۲$ و $a^n + ۱$ اول باشد، نشان دهید که a زوج است و n به‌صورت توانی از ۲ است. (راهنمایی: اگر j فرد باشد، آنگاه

$$x^j + ۱ = (x+۱)(x^{j-۱} - x^{j-۲} + \cdots - x + ۱)$$

حل. اگر a فرد باشد، $a^n + ۱ > ۳$ زوج است که خلاف فرض است. پس a زوج است. حال، نشان می‌دهیم که اگر $۲^n + ۱$ اول باشد، n به‌صورت توانی از ۲ است. فرض کنیم خیلی نباشد و مثلاً $n = st$ که $s > ۱$ فرد است. با فرض $x = ۲^t$ داریم

$$۲^n + ۱ = ۲^{st} + ۱ = (۲^t)^s + ۱ = x^s = (x+۱)(x^{s-۱} - x^{s-۲} + \cdots - x + ۱)$$

واضح است که $x+1>1$ و $x+1<2^n+1$. یعنی 2^n+1 مرکب است که خلاف فرض است. پس n به‌صورت توانی از ۲ است.

توضیح. عکس مسألهٔ بالا درست نیست. مثلاً $2^{2^5}+1=641|2^{2^5}+1$.

۶.۷ ثابت کنید که تعداد اعداد طبیعی مرکبی که نمی‌توان آنها را به‌صورت مجموع دو عدد اول نوشت نامتناهی است.

حل. ما دنبال اعداد صحیح مرکب فردی می‌گردیم که ویژگی فوق را داشته باشند. زیرا وجود بی‌نهایت مثال زوج کاملاً ناقض حدس گولدباخ است. اعداد به‌صورت $n=6k+5$ را در نظر می‌گیریم. آشکار است که به‌ازای هر k که مضرب ۵ باشد، n مرکب است. اما k هر عدد طبیعی باشد نمی‌توان n را به‌صورت مجموع دو عدد اول نوشت. زیرا اگر kیی وجود داشته باشد به‌طوری که $6k+5=p+q$. آشکار است که p و q هر دو نمی‌توانند عدد اول فرد باشند. پس $6k+5=2+q$. در این‌صورت $q=6k+3$ یعنی $3|q$ و این با اول بودن q تناقض دارد.

◁ **۷.۷** اگر k عددی طبیعی باشد، فرض می‌کنیم p_k، kامین عدد اول باشد، و فرض می‌کنیم $\alpha_k(x)$ تعداد اعداد طبیعی نابیشتر از x باشد که تمام مقسوم‌علیه‌های اولشان نابزرگتر از p_k هستند. ثابت کنید $\alpha_k(x)\le 2^k\sqrt{x}$. (راهنمایی: ابتدا نشان دهید که بیش از 2^k از این اعداد که خالی از مربع هستند وجود دارند.)

حل. فرض کنیم $a\le x$ عدد طبیعی خالی از مربعی باشد که بر هیچ عدد اولِ بزرگتر از p_k بخشپذیر نباشد، و فرض می‌کنیم $a=2^{a_1}3^{a_2}\cdots p_k^{a_k}$. چون هر a_i برابر ۰ یا ۱ است، حداکثر 2^k امکان برای نماها و لذا 2^k امکان برای a وجود دارد. به‌ازای هر a، حداکثر $\sqrt{x/a}$ عدد طبیعی n وجود دارد که $n^2a\le x$، لذا به‌ازای هر a، بیشتر از $\sqrt{x}$ امکان برای n وجود ندارد. در نتیجه $\alpha_k(x)\le 2^k\sqrt{x}$.

◁ **۸.۷** با استفاده از تمرین قبل ثابت کنید که سری $\sum 1/p$، مجموع وارونهای اعداد اول، واگراست.

حل. فرض کنیم p_i، iامین عدد اول باشد. اگر سری همگرا باشد، عدد طبیعی k وجود دارد به‌طوری که

$$\frac{1}{p_{k+1}}+\frac{1}{p_{k+2}}+\cdots<\frac{1}{2}$$

تعداد اعداد طبیعی کمتر از عدد مفروض x که بر عدد اول p بخشپذیرند از x/p تجاوز نمی‌کند. با

استفاده از نماد مسألهٔ قبل، $x - \alpha_k(x)$ نشانگر تعداد اعداد طبیعی است که از x تجاوز نمی‌کنند و حداقل بر یک عدد اول بزرگتر از p_k بخشپذیرند، و لذا

$$x - \alpha_k(x) < \frac{x}{p_{k+1}} + \frac{x}{p_{k+2}} + \cdots < \frac{x}{2}$$

سپس بنابر مسألهٔ ۷.۷ داریم $x/2 < \alpha_k(x) \leq 2^k\sqrt{x}$، و لذا $x < 2^{2k+2}$. این نابرابری درست نیست. هرگاه $x \geq 2^{2k+2}$، و بنابراین سری واگراست.

اعداد تام

۹.۷ ثابت کنید هر عدد تام زوج به رقم ۶ یا ۸ ختم می‌شود.

حل. بنابر (۳.۷)، هر عدد تام N به‌صورت $N = 2^{p-1}(2^p - 1)$ است که p اول است. اگر $p = 2$، آنگاه $N = 6$؛ لذا فرض می‌کنیم p فرد باشد. اگر $p = 4k + 1$، آنگاه $2^{p-1} = 2^{4k} = 16^k \equiv 6 \pmod{10}$ و $2^p - 1 = 2 \times 2^{p-1} - 1 \equiv 1 \pmod{10}$؛ لذا $N \equiv 6 \times 1 = 6 \pmod{10}$. اگر $p = 4k + 3$، آنگاه

$$2^{p-1} = 2^{4k+2} = 4 \times 16^k \equiv 4 \pmod{10}$$

و $2^p - 1 = 2 \times 2^{p-1} - 1 \equiv 7 \pmod{10}$؛ لذا $N \equiv 4 \times 7 \equiv 8 \pmod{10}$.

۱۰.۷ فرض کنید $N > 6$ یک عدد تام زوج باشد. ثابت کنید که N به‌صورت $9k + 1$ است.

حل. هر عدد تام زوج N به‌صورت $N = 2^{p-1}(2^p - 1)$ است که p اول است. به‌ویژه، اگر $N > 6$، p فرد است، ثابت می‌کنیم به‌ازای هر عدد فرد n، $2^{n-1}(2^n - 1) \equiv 1 \pmod{9}$.

اگر $n = 1, 3, 5, 7, \ldots$، آنگاه 2^{n-1} به‌ترتیب با ۱، ۴، ۷، ۱، ۴، ۷، ... همنهشت به پیمانهٔ ۹ است، در حالی‌که $2^n - 1$ به‌ترتیب با ۱، ۷، ۴، ۱، ۷، ۴، ... همنهشت به پیمانهٔ ۹ است. اگر ضرب کنیم می‌بینیم که $2^{n-1}(2^n - 1)$ به‌ترتیب با ۱، ۱، ۱، ۱، ... همنهشت به پیمانهٔ ۹ است، و لذا $N \equiv 1 \pmod{9}$.

۱۱.۷ اگر p اول باشد، ثابت کنید که p^k نمی‌تواند عدد تام باشد.

حل. مجموع مقسوم‌علیه‌های p^k عبارت است از $\sigma(p^k) = 1 + p + p^2 + \cdots + p^k$ و آشکار است که نمی‌تواند برابر $2p^k$ یا هر مضربی از p باشد. زیرا روشن است که نمی‌تواند $1 + p + \cdots + p^k$ را بشمارد.

راه‌حل دیگر

$$۱ + p + p^۲ + \cdots + p^{k-۱} = \frac{(p^k - ۱)}{(p-۱)} \leq p^k - ۱ < p^k$$

و لذا $\sigma(p^k) < ۲p^k$. بنابراین p^k عدد تام نیست.

۱۲.۷ ثابت کنید که n یک عدد تام است اگر و تنها اگر $\sum_{d/n} ۱/d = ۲$.

حل. n هر عدد طبیعی باشد داریم $\{d : d|n\} = \{n/d : d|n\}$. لذا

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{۱}{d}$$

لذا n تام است اگر و تنها اگر $\sum_{d|n} ۱/d = ۲$.

۱۳.۷ با استفاده از مسألهٔ قبل ثابت کنید که هیچ مقسوم‌علیه واقعی یک عدد تام، تام نیست.

حل. فرض کنیم n یک عدد تام، و k یک مقسوم‌علیه واقعی n باشد. بنابر مسألهٔ قبل، $\sum_{d|n} ۱/d = ۲$ داریم $\sum_{d|k} ۱/d + n \geq \sum_{d|n} ۱/d = ۲$، پس $\sum_{d|k} ۱/d < ۲$ و لذا k تام نیست.

۱۴.۷ اگر p و q اعداد اول متمایز باشند، ثابت کنید pq تام نیست.

حل. داریم $\sigma(pq) = \sigma(p)\sigma(q) = (p+۱)(q+۱)$. بدیهی است که $\sigma(pq)$ نمی‌تواند برابر $۲pq$ باشد. زیرا $۴|\sigma(pq)$ ولی $۴ \not| ۲pq$.

توضیح. استدلال مشابه نشان می‌دهد که حاصلضرب هر تعداد عدد اول فرد متمایز نمی‌تواند تام باشد. لذا یک عدد تام فرد (در صورت وجود) نمی‌تواند خالی از مربع باشد.

اعداد اول مِرسن و اعداد فرما

۱۵.۷ با استفاده از قضیهٔ (۵.۷) ثابت کنید که $۲^۷ - ۱$ اول است.

حل. بنابر (۵.۷) هر عامل اولِ $۱۲۷ = ۲^۷ - ۱$ به‌صورت $۱۴k + ۱$ است. لذا کافی است اعداد اولِ به این‌صورت را تا $\sqrt{۱۲۷}$ امتحان کنیم. چون چنین اعداد اولی وجود ندارند، پس ۱۲۷ اول است.

۱۶.۷ با استفاده از قضیهٔ ۵.۷ اول بودن $۲^{۱۱} - ۱$ را بررسی کنید.

حل. با توجه به (۵.۷) و مسألهٔ ۱.۷، اعداد اول q به‌صورت $۲۲k+۱$ راکه $q < \sqrt{۲^{۱۱}-۱} \approx ۴۵$ امتحان می‌کنیم. تنها عدد q به این‌صورت ۲۳ است و به آسانی معلوم می‌شود که $۲۳ | ۲^{۱۱} - ۱$، لذا $۲^{۱۱} - ۱$ مرکب است.

۱۷.۷ اول بودن یا اول نبودن $۲^{۲۹} - ۱$ را بررسی کنید.

حل. تنها مقسوم‌علیه‌های ممکن به‌صورت $۵۸k + ۱$ هستند، یعنی ۵۹، ۱۱۷، ۱۷۵، ۲۳۳، و مانند اینها. به آسانی دیده می‌شود که ۵۹ یک مقسوم‌علیه نیست؛ ۱۱۷ و ۱۷۵ اول نیستند و لازم نیست که امتحان شوند، زیرا کوچکترین مقسوم‌علیه بزرگتر از یک از $۲^{۲۹} - ۱$ بایستی اول باشد. به آسانی دیده می‌شود که ۲۳۳ اول است و $۲^{۲۹} - ۱$ را می‌شمارد، لذا $۲^{۲۹} - ۱$ مرکب است.

۱۸.۷ ثابت کنید که $۲^{۱۶}(۲^{۱۷} - ۱)$ یک عدد تام است.

حل. با توجه به (۲.۷) کافی است نشان دهیم که $۲^{۱۷} - ۱$ اول است. تنها لازم است که عاملهای اول تا $\sqrt{۲^{۱۷}-۱}$ را امتحان کنیم. بنابر (۵.۷)، عاملهای اول $M_{۱۷}$ به‌صورت $۳۴k + ۱$ هستند؛ لذا فقط بایستی ۱۰۳، ۱۳۷، ۲۳۹، و ۳۰۷ را امتحان کنیم. چون هیچ‌کدام از اینها $M_{۱۷}$ را نمی‌شمارند، نتیجه می‌گیریم که $۲^{۱۷} - ۱$ اول است.

۱۹.۷ (الف) با استفاده از (۵.۷) اول بودن یا اول نبودن $M_{۲۳} = ۲^{۲۳} - ۱$ را بررسی کنید.
(ب) با استفاده از این واقعیت که ۲ یک ماندهٔ درجهٔ دوم ۴۷ است اول بودن $M_{۲۳}$ را بررسی کنید.

حل. (الف) بنابر (۵.۷) هر عامل اول $M_{۲۳}$ بایستی به‌صورت $۴۶k + ۱$ باشد: ۴۷، ۱۳۹، ۲۷۷، . . . . به آسانی دیده می‌شود که $۴۷ | M_{۲۳}$.

(ب) چون ۲ یک ماندهٔ درجهٔ دوم ۴۷ است، بنابر ملاک اویلر $۲^{۲۳} \equiv ۱ \pmod{۴۷}$، و لذا $۴۷ | ۲^{۲۳} - ۱$.

۲۰.۷ فرض کنید q عدد اولی به‌صورت $۴k + ۳$ باشد، و $۲q + ۱$ اول باشد. ثابت کنید $۲q + ۱$ یک مقسوم‌علیه M_q است. با استفاده از اینکه q چنین عدد اولی است و اینکه $q > ۳$ نتیجه بگیرید که M_q مرکب است. (راهنمایی: ابتدا نشان دهید که ۲ یک ماندهٔ درجهٔ دوم $۲q + ۱$ است).

حل. چون $۲q + ۱$ عدد اولی به‌صورت $۸k + ۷$ است، از (۱۲.۵) نتیجه می‌شود که ۲ یک ماندهٔ درجهٔ دوم $۲q + ۱$ است. لذا بنابر ملاک اویلر $۲^{q} \equiv ۱ \pmod{۲q + ۱}$، و لذا

$۲q+۱ | ۲^q - ۱$. بنابراین، $۲q+۱$ یک مقسوم‌علیه سره M_q است مگر آنکه $M_q = ۲q+۱$. اگر $q = ۳$، آنگاه $M_q = ۷ = ۲q+۱$، و ما یک مقسوم‌علیه سره از M_q به‌دست نمی‌آوریم، اما اگر $n > ۳$ به آسانی بررسی می‌شود که $۲n+۱ < ۲^n - ۱$.

۲۱.۷ فرض کنید m عدد صحیح مثبت فردی باشد. ثابت کنید بی‌نهایت عدد مرسن M_n وجود دارد که بر m بخشپذیرند. (راهنمایی: از قضیهٔ اویلر استفاده کنید.)

حل. بنابر قضیهٔ اویلر، $۲^{\phi(m)} \equiv ۱ (\mathrm{mod}\, m)$، لذا به‌ازای هر عدد صحیح مثبت k، $۲^{k\phi(m)} \equiv ۱ (\mathrm{mod}\, m)$. لذا، اگر n مضرب مثبتی از $\phi(m)$ باشد، $m | M_n$.

۲۲.۷ ثابت کنید که $(۲^m - ۱, ۲^n - ۱) = ۲^{(m,n)} - ۱$. (راهنمایی: قرار دهید $d = (۲^m - ۱, ۲^n - ۱)$، و مرتبهٔ ۲ به پیمانهٔ d را در نظر بگیرید. همچنین، یادآور می‌شویم که اگر $r | s$ آنگاه $۲^r - ۱ | ۲^s - ۱$.)

حل. اگر $d = (۲^m - ۱, ۲^n - ۱)$ آنگاه $۲^m \equiv ۱ (\mathrm{mod}\, d)$، و لذا بنابر (i.۲.۶)، $\mathrm{ord}_d ۲ | m$؛ به همین ترتیب، $\mathrm{ord}_d ۲ | n$. لذا $\mathrm{ord}_d ۲ | (m,n)$ و از این‌رو $۲^{(m,n)} \equiv ۱ (\mathrm{mod}\, d)$، یعنی $d | ۲^{(m,n)} - ۱$. اما $۲^{(m,n)} - ۱$ یک مقسوم‌علیه مشترک $۲^m - ۱$ و $۲^n - ۱$ است و لذا d را می‌شمارد. بنابراین $d = ۲^{(m,n)} - ۱$.

برهان دیگر: می‌توانیم یک استدلال استقرایی نیز ارائه دهیم که فقط از ویژگیهای سادهٔ بزرگترین مقسوم‌علیه مشترک استفاده می‌شود. فرض کنیم d ثابت باشد. اگر قضیه برای تمام s و t؛ با فرض $۰ < s \le t < n$ و $(s,t) = d$ برقرار باشد. ثابت می‌کنیم که برای تمام s و t؛ با $۰ < s \le t \le n$ و $(s,t) = d$ برقرار است. اگر $s = t$ بدیهی است، لذا مثلاً فرض می‌کنیم $s < t$. با استفاده از این مطلب که $(a,b) = (a, b-a)$ داریم

$$(۲^s - ۱, ۲^t - ۱) = (۲^s - ۱, ۲^t - ۲^s) = (۲^s - ۱, ۲^s(۲^{t-s} - ۱)) = (۲^s - ۱, ۲^{t-s} - ۱)$$

چون $(s, t-s) = d$ و s و $t-s$ هر دو از n کمترند، بنابر فرض استقرا داریم

$$(۲^s - ۱, ۲^{t-s} - ۱) = ۲^q - ۱$$

و لذا $(۲^s - ۱, ۲^t - ۱) = ۲^d - ۱$.

توضیح. استدلال مشابه نشان می‌دهد که برای $a \ge ۲$، $(a^m - ۱, a^n - ۱) = a^{(m,n)} - ۱$.

۲۳.۷ اگر p و q اعداد اول فرد باشند و $p|۲^q+۱$، ثابت کنید یا $p=۳$ یا p به‌صورت $۲kq+۱$ است. با استفاده از این مطلب دو مقسوم‌علیه اول از $۲^{۱۳}+۱$ را پیدا کنید.

حل. ابتدا با برهانی نظیر برهان (۵.۷) گزارهٔ کلی را ثابت می‌کنیم. اگر $p|۲^q+۱$، آنگاه $۲^q \equiv -۱ (\bmod p)$ و از این‌رو $۲^{۲q} \equiv ۱ (\bmod p)$. بنابراین مرتبهٔ ۲ به پیمانهٔ p عدد $۲q$ را می‌شمارد. (q را نمی‌تواند بشمارد، زیرا $۲^q \equiv -۱ (\bmod p)$.) عدد صحیح ۲ دارای مرتبهٔ ۲ است فقط وقتی که $p=۳$. در سایر موارد، $۲q|p-۱$، یعنی p به‌صورت $۲kq+۱$ است.

چون $۲^۲ \equiv ۱ (\bmod ۳)$، نتیجه می‌شود که $۲^{۱۳} \equiv ۲ (\bmod ۳)$، لذا $۳|۲^{۱۳}+۱$. چون $۲۷۳۱ = ۳/(۲^{۱۳}+۱)$، عوامل اول دیگر $۲^{۱۳}+۱$ به‌صورت $۲۶k+۱$ خواهند بود و بایستی ۲۷۳۱ را بشمارند. تنها نامزدِ کمتر از $\sqrt{۲۷۳۱}$ عدد ۵۳ است که ۲۷۳۱ را نمی‌شمارد. لذا ۲۷۳۱ اول است، و بنابراین ۳ و ۲۷۳۱ تنها عاملهای اول $۲^{۱۳}+۱$ هستند.

◁ **۲۴.۷** (الف) فرض کنید F_k معرف kامین عدد فرما باشد. اگر $m \neq n$ ثابت کنید $(F_m, F_n)=۱$.
(راهنمایی: فرض کنید $p|F_m$؛ در آن‌صورت $۲^{۲^m} \equiv -۱ (\bmod p)$.)
(ب) با استفاده از قسمت (الف) اثبات دیگری برای وجود بی‌نهایت عدد اول بدهید.

حل. (الف) می‌توانیم فرض کنیم که $m<n$. فرض کنیم p عامل اولی از F_m باشد؛ در این‌صورت $۲^{۲^m} \equiv -۱ (\bmod p)$ چون $F_m - ۱ = ۲^{۲^m}$ برابر توان زوج $۲^{۲^n}$ است، لذا $F_n \equiv ۲ (\bmod p)$. به‌ویژه چون p فرد است نمی‌تواند F_n را بشمارد.

(ب) هر F_k عامل اولی مانند p_k (احتمالاً خود F_k) دارد. چون $(F_m, F_n)=۱$ وقتی که $m \neq n$، نتیجه می‌شود که $p_m \neq p_n$ وقتی که $m \neq n$. لذا مقادیر متمایز k اعداد اول متمایز p_k را تولید می‌کنند و در نتیجه بی‌نهایت عدد اول وجود دارد.

توضیح. لازم نیست که بدانیم بی‌نهایت عدد اول F_k وجود دارد؛ در واقع، این هنوز یک مسألهٔ باز است.

۲۵.۷ فرض کنید $c_۰=۲$ و برای $n \geq ۰$، $c_{n+۱} = c_n^۲ - c_n + ۱$. اگر $m \neq n$، ثابت کنید $(c_m, c_n)=۱$. (راهنمایی: می‌توانید فرض کنید $m<n$. اگر $p|c_m$، نشان دهید که p اعداد $c_{m+۱}$، $c_{m+۲}$، ... را نمی‌شمارد.)

حل. به استقرا بر i نشان می‌دهیم که اگر $p|c_m$، آنگاه به‌ازای هر $i \geq ۱$، $c_{m+i} \equiv ۱ (\bmod p)$.

فرض کنیم $P(x) = x^۲ - x + ۱$. اگر $i = ۱$، آنگاه

$$c_{m+i} = P(c_m) \equiv ۰^۲ - ۰ + ۱ = ۱ (\mathrm{mod}\, p)$$

حال، فرض می‌کنیم $c_{m+i} \equiv ۱ (\mathrm{mod}\, p)$؛ لذا

$$c_{m+i+۱} = P(c_{m+i}) \equiv ۱^۲ - ۱ + ۱ = ۱ (\mathrm{mod}\, p)$$

توضیح. این مطلب باز هم برهان دیگری برای وجود بی‌نهایت عدد اول است. رابطهٔ نزدیکی بین این مسأله و مسألهٔ قبل وجود دارد. اگر F_n، nامین عدد فرما باشد، به آسانی بررسی می‌شود که $F_{n+۱} = F_n^۲ - ۲F_n + ۲ = Q(F_n)$، که $Q(x) = x^۲ - ۲x + ۲$. می‌توانیم استدلالی را که به‌کار برده‌ایم طوری سازگار کنیم که اگر عدد اول p عدد F_m را بشمارد، به‌ازای هر عدد صحیح مثبت i، $F_{m+i} \equiv ۲ (\mathrm{mod}\, p)$. چون هر عدد فرما فرد است، این همنهشتی نشان می‌دهد که هر دو عدد فرمای متمایز نسبت به هم اول‌اند. قضیه‌های مشابه در مورد اعداد فرما-نما را می‌توان با کاربرد چندجمله‌ییهای مربوط اثبات کرد.

۲۶.۷ ثابت کنید که $F_۴ = ۲^{۱۶} + ۱$ اول است. (از (۷.۷) استفاده کنید.)

حل. بنابر (۷.۷)، هر عامل اول $F_۴$ به‌صورت $۲^۶k + ۱$ است. همهٔ اعدادِ اولِ نابیشتر از $\sqrt{F_۴}$ را که به این‌صورت هستند امتحان می‌کنیم. تنها ۱۹۳ واجد شرط است، و عدد $F_۴$ را نمی‌شمارد؛ لذا $F_۴$ اول است.

۲۷.۷ اگر F_n معرف nامین عدد فرما باشد، ثابت کنید به‌ازای بی‌نهایت مقدار n، عدد $F_n + ۲$ مرکب است. (راهنمایی: به پیمانهٔ ۷ عمل کنید.)

حل. ملاحظه کنید که $۲^{۲^{n+۱}}$ مربع $۲^{۲^n}$ است؛ لذا با شروع از $n = ۰$، $۲^{۲^n}$ به‌ترتیب با ۲، ۴، ۲، ۴، ... همنهشت به پیمانهٔ ۷ است. لذا اگر n فرد باشد، نتیجه می‌شود که $F_n + ۲ \equiv ۴ + ۱ + ۲ \equiv ۰ (\mathrm{mod}\, ۷)$. بنابراین، به‌ازای هر n فردِ بزرگتر از ۱، $F_n + ۲$ مرکب است.

۲۸.۷ در نامه‌ای به فِرنیکل، فرما حدس زد که اگر a زوج باشد، $N = a^{۲^n} + ۱$ اول است مگر آنکه N بر یک عدد فرمای F_k بخشپذیر باشد. این حدس را رد کنید. (راهنمایی: $a = ۱۲$ را اختیار کنید.)

حل. اگر $a = ۱۲$ و $n = ۲$، آنگاه $N = ۸۹ \times ۲۳۳$. اعداد ۸۹ و ۲۳۳ اول هستند، و هیچ‌کدام یک عدد فرما نیستند.

۲۹.۷ اگر $n > ۱$، ثابت کنید عدد فرمای F_n به رقم ۷ ختم می‌شود.

حل. اگر $n > ۱$، نشان دهیم که $F_n \equiv ۲ (\mathrm{mod}\, ۵)$. چون F_n فرد است، نتیجه خواهد شد که F_n به رقم ۷ ختم می‌شود. اگر $n > ۱$، آنگاه $۴ | ۲^n$؛ فرض کنیم $۲^n = ۴k$. لذا $F_n = (۲^۴)^k + ۱ \equiv ۱^k + ۱ = ۲ (\mathrm{mod}\, ۵)$.

۳۰.۷ (آزمون پِپن[1]) فرض کنید $n \geq ۱$. ثابت کنید عدد فرمای F_n اول است اگر و تنها اگر $۳^{(F_n - ۱)/۲} \equiv -۱ (\mathrm{mod}\, F_n)$. (راهنمایی: از (۹.۶) استفاده کنید.)

حل. ابتدا فرض می‌کنیم F_n اول باشد، که در آن $n \geq ۱$. به آسانی دیده می‌شود که ۳ یک ناماندهٔ درجهٔ دوم F_n است: $F_n \equiv ۱ (\mathrm{mod}\, ۴)$ و $F_n \equiv ۲ (\mathrm{mod}\, ۳)$، لذا $(۳/F_n) = (F_n/۳) = (۲/۳) = -۱$. لذا بنابر ملاک اویلر، $۳^{(F_n - ۱)/۲} \equiv -۱ (\mathrm{mod}\, F_n)$.

عکس مطلب نتیجهٔ بلافصل (۹.۶) از آزمون تعیین اول بودن لوکاست. زیرا اگر $۳^{(F_n - ۱)/۲} \equiv -۱ (\mathrm{mod}\, F_n)$، آنگاه $۳^{F_n - ۱} \equiv ۱ (\mathrm{mod}\, F_n)$. چون تنها عامل اول $F_n - ۱$ عدد $q = ۲$ است و $۳^{(F_n - ۱)/۲} \not\equiv ۱ (\mathrm{mod}\, F_n)$، از (۹.۶) نتیجه می‌شود که F_n اول است.

قضیهٔ اعداد اول و اصل موضوع برتران

۳۱.۷ فرض می‌کنیم p_n معرف nامین عدد اول باشد. با استفاده از اصل برتران نشان دهید که اگر $n \geq ۲$ آنگاه $p_n < ۲^n$.

حل. اثبات به استقرا بر n. اگر $n = ۲$ آنگاه $p_۲ = ۳$ و روشن است که $۳ < ۲^۲$. فرض کنیم $n \geq ۲$ و $p_n < ۲^n$ (۱). گوییم $p_{n+۱} < ۲^{n+۱}$. بنابر اصل برتران عدد اولی بین p_n و $۲p_n$ وجود دارد، لذا $p_{n+۱} < ۲p_n$. در نتیجه بنابر (۱) داریم $p_{n+۱} < ۲p_n < ۲ \times ۲^n = ۲^{n+۱}$.

۳۲.۷ فرض می‌کنیم p_n معرف nامین عدد اول باشد. با توجه به این واقعیت که به‌ازای هر $n \geq ۶$، حداقل دو عدد اول بین n و $۲n$ وجود دارد ثابت کنید $p_{n+۲} < p_n + p_{n+۱}$.

حل. فرض می‌کنیم $p_n > ۵$. چون بین p_n و $۲p_n$ لااقل دو عدد اول وجود دارد، پس روشن است که $p_{n+۲}$ و $p_{n+۱}$ بین p_n و $۲p_n$ قرار دارند. به‌ویژه $p_{n+۲} < ۲p_n$ (۱) از طرفی همواره داریم $۲p_n < p_n + p_{n+۱}$. لذا، بنابر (۱)، $p_{n+۲} < p_n + p_{n+۱}$.

1. Pepin

۳۳.۷ اگر $m \geq ۲$ و $m! = p_۱^{a_۱} \cdots p_k^{a_k}$، با استفاده از اصل برتران ثابت کنید که به‌ازای حداقل یک i، $a_i = ۱$.

حل. برای $m = ۲$ مسأله واضح است. پس فرض می‌کنیم $m > ۲$. اگر m زوج باشد، مثلاً $m = ۲n$، آنگاه بنابر اصل برتران عدد اول p وجود دارد که $n < p < ۲n$. لذا $۲p > ۲n = m$. بنابراین توان p در تجزیهٔ $m!$ برابر ۱ است. اگر m فرد باشد، مثلاً $m = ۲n + ۱$، آنگاه عدد اول p وجود دارد که $n + ۱ < p < ۲n + ۲$ و لذا $۲p > ۲n + ۲ > ۲n + ۱ = m$. بنابراین توان p در تجزیهٔ $m!$ برابر ۱ خواهد بود.

۳۴.۷ فرض می‌کنیم $m > ۱$. با استفاده از مسألهٔ قبل ثابت کنید که اگر $k \geq ۲$، آنگاه $m!$ هرگز توان kام عددی نخواهد شد.

حل. بنابر مسألهٔ قبل، عدد اول p وجود دارد به‌طوری که نمای p در تجزیهٔ $m!$ برابر ۱ است. اما نمای هر عامل اول در تجزیهٔ یک توان kام مضربی از k است، لذا اگر $k > ۱$، آنگاه $m!$ نمی‌تواند توان kام عددی باشد.

◁ **۳۵.۷** فرض می‌کنیم $s(x)$ معرف تعداد مربعهای کاملِ مثبتِ نابیشتر از x باشد. با استفاده از قضیهٔ اعداد اول نشان دهید که می‌توان $s(x)/\pi(x)$ را هر قدر که بخواهیم کوچک سازیم، هرگاه x به اندازهٔ کافی بزرگ باشد. (این نشان می‌دهد که تعداد اعداد اول بیشتر از تعداد مربعهاست، بدین معنی که به‌ازای x بزرگ، تعداد اعداد اول در بازهٔ $۱ \leq u \leq x$ بیشتر از تعداد مربعهاست.

حل. فرض می‌کنیم $x > ۱$. اگر $g(x) = x/\log x$، آنگاه

$$s(x)/\pi(x) = (s(x)/g(x))(g(x)/\pi(x))$$

اما $s(x) \leq \sqrt{x}$. لذا $s(x)/g(x) \leq (\log x/\sqrt{x})(g(x)/\pi(x))$. اکنون، بنابر قضیهٔ اعداد اول، $g(x)/\pi(x)$ به ۱ میل می‌کند وقتی x بزرگ شود. همچنین، بنابر تکنیکهای استانداردِ حسابان $\log x/\sqrt{x}$ به ۰ میل می‌کند هرگاه x بزرگ شود. در نتیجه $s(x)/\pi(x)$ به ۰ میل می‌کند هرگاه x بزرگ شود.

◁ **۳۶.۷** به موجب یکی از قضیه‌های چبیشف اعداد ثابت مثبت c و C وجود دارند به‌طوری که به‌ازای هر $x \geq ۲$، $c(x/\log x) < \pi(x) < C(x/\log x)$. با استفاده از این قضیه برهان دیگری برای این مطلب که: شکافهای وسیع دلخواه در دنبالهٔ اعداد اول وجود دارند ارائه دهید.

حل. فرض کنیم چنین نباشد. لذا عدد صحیح d وجود دارد به‌طوری که تفاضل بین اعداد اولِ متوالی هرگز از d تجاوز نمی‌کند، و لذا به‌ازای هر عدد $x \geq ۲$، عدد اول p وجود دارد که $x < p \leq x + d$. در نتیجه حداقل $(x-۲)/d$ عددِ اولِ نابیشتر از x وجود دارند، و لذا $\pi(x) \geq (x-۲)/d$. اما بنابر قضیهٔ چبیشف، عدد مثبت C وجود دارد که $\pi(x) < Cx/\log x$. لذا به‌ازای هر $x > ۲$، داریم $(x-۲)/d \leq \pi(x) < Cx/\log x$. این ایجاب می‌کند که به‌ازای هر $x > ۲$، $\log x < Cdx/(x-۲)$، که آشکارا نادرست است، زیرا اگر x به‌قدر کافی بزرگ اختیار شود می‌توان $\log x$ را به دلخواه بزرگ ساخت.

قضیهٔ دیریکله

۳۷.۷ اگر c و d مثبت و نسبت به هم اول باشند، فرض می‌کنیم حداقل یک عدد اول به‌صورت $ck + d$ وجود دارد. حال، اگر a را مثبت و $(a, b) = ۱$، ثابت کنید بی‌نهایت عدد اول به‌صورت $ak + b$ وجود دارد. (راهنمایی: ثابت کنید که به‌ازای هر $n \geq ۱$ عدد اولی به‌صورت $a^n k + b$ وجود دارد.)

حل. می‌توانیم فرض کنیم $a > ۱$، زیرا به‌ازای $a = ۱$ دنبالهٔ $ak + b$ درست $b + ۱$، $b + ۲$، $b + ۳$، ...، است که آشکارا شامل تعداد نامتناهی عدد اول است. چون $(a, b) = ۱$، به‌ازای هر $n \geq ۱$ نیز داریم $(a^n, b) = ۱$؛ لذا بنابه فرض، عدد اول p به‌صورت $a^n k + b$، و بنابراین به‌صورت $am + b$ وجود دارد. چون $p > a^n$، درنتیجه به‌ازای هر $n \geq ۱$، می‌توانیم عدد اولی به‌صورت $am + b$ بیابیم که بزرگتر از a^n باشد، و لذا تعداد نامتناهی عدد اول این چنینی وجود دارد.

۳۸.۷ فرض می‌کنیم N یک عدد صحیح مثبت باشد و $(a, b) = ۱$. بدون استفاده از قضیهٔ دیریکله، ثابت کنید که تعداد نامتناهی عدد به‌صورت $ak + b$ وجود دارند که با N متباین هستند. (راهنمایی: فرض کنید P حاصلضرب اعداد اولی باشد که N را می‌شمارند اما a را نمی‌شمارند، و به‌ازای یک s مناسب قرار دهید $k = s + tP$.)

حل. فرض می‌کنیم P مطابق تعریف در راهنمایی باشد. چون $(a, P) = ۱$، همنهشتی $ax + b \equiv ۱ (\mathrm{mod}\, P)$ دارای جوابی است مانند s؛ در این‌صورت به‌ازای هر عدد صحیح t، $s + tP$ نیز یک جواب است. قرار می‌دهیم $k = s + tP$. اول نشان می‌دهیم که اگر عدد اول p عدد N را بشمارد، p عدد $ak + b$ را نمی‌شمارد، سپس نشان می‌دهیم که $ak + b$ با N متباین است.

اگر $p|a$، آنگاه p نمی‌تواند $ak + b$ را بشمارد، زیرا a و b نسبت به‌هم اول‌اند. اگر $p \nmid a$،

آنگاه $p|P$، و لذا $as+b \equiv ۱ (\mathrm{mod}\, p)$. لذا $ak+b \equiv as+b \equiv ۱ (\mathrm{mod}\, p)$، لذا مجدداً $p \nmid (ak+b)$. در نتیجه $ak+b$ و N نسبت به هم اول‌اند. از آنجا که هیچ محدودیتی برای t وجود ندارد، تعداد نامتناهی عدد به‌صورت $ak+b$ وجود دارند که با N متباین هستند.

◁ **۳۹.۷** یک عدد اول p به‌صورت $۸k+۱$ به‌دست آورید به‌طوری که ۳، ۵، ۷، و ۱۱ مانده‌های درجهٔ دوم آن باشند. (راهنمایی: از قانون تقابل مربعی و قضیهٔ دیریکله استفاده کنید.)

حل. چون بایستی p به‌صورت $۸k+۱$ باشد، سپس بنابر قانون تقابل مربعی لازم است که $(p/۳) = (p/۵) = (p/۷) = (p/۱۱) = ۱$. این برابریها شرایطی را بر باقیمانده‌های تقسیم p بر ۳، ۵، ۷، و ۱۱ وضع می‌کنند، لازم داریم که $p \equiv ۱ (\mathrm{mod}\, ۳)$، $p \equiv ۱$ یا $۴ (\mathrm{mod}\, ۵)$، $p \equiv ۱$ یا $۶ (\mathrm{mod}\, ۷)$، و $p \equiv ۱$ یا $۹ (\mathrm{mod}\, ۱۱)$. (علاوه بر $p \equiv ۱ (\mathrm{mod}\, ۸)$ $p \equiv ۱, ۳, ۴, ۵$). با ترکیب این امکانات برای باقیمانده‌ها در هر یک از $۲ \times ۳ \times ۵ = ۳۰$ طریق ممکن، تعداد ۳۰ دستگاهِ متفاوت از پنج همنهشتی به‌دست می‌آوریم. برای هر یک از این دستگاهها می‌توانیم قضیهٔ باقیماندهٔ چینی را برای به‌دست آوردن یک همنهشتی هم‌ارز به‌صورت $p \equiv b (\mathrm{mod}\, N)$ به‌کار بریم، که در آن $N = ۸ \times ۳ \times ۵ \times ۷ \times ۱۱$ و b هر یک از ۳۰ مقدار را اختیار می‌کند، که به آسانی دیده می‌شود که همگی با N متباین هستند. بنابراین ۳۰ تصاعد حسابی وجود دارند که می‌توانیم در آنها به دنبال اعداد اول باشیم، و بنابر قضیهٔ دیریکله هر یک تعداد نامتناهی عدد اول دارند. ساده‌ترین حالت با انتخاب p همنهشت با ۱ به پیمانه‌های ۸، ۳، ۵، ۷، و ۱۱ به‌دست می‌آید: در این حالت، اعداد اول به‌صورت $Nk+۱$ را جستجو می‌کنیم. خوشبختانه $N = ۹۲۴۰$ فوراً به‌دست می‌آید، و اثبات اول بودن ۹۲۴۱ مشکل نیست.

در حالت دیگر، می‌توانیم تنها همنهشتیهای به پیمانه‌های ۸، ۳، و ۵ را دسته‌بندی کنیم و لذا اعداد اول به‌صورت $۱۲۰k+۱$ یا $۱۲۰k+۴۹$ را جستجو کنیم که در همنهشتیهای دیگری به پیمانه‌های ۷ و ۱۱ صدق کنند. اگر به همین طریق ادامه دهیم، $p = ۲۶۸۹$ را نسبتاً سریع به‌دست می‌آوریم که ویژگیهای مورد نظر را دارد، یعنی، همنهشت با ۱ به پیمانه‌های ۳، ۷، و ۸، همنهشت با ۴ به پیمانهٔ ۵، و همنهشت با ۵ به پیمانهٔ ۱۱ است. این کوچکترین مثال است.

توضیح. به‌طور کلی، اگر بخواهیم عدد اول p به‌صورت $۸k+۱$ به‌گونه‌ای باشد که $n-۱$ عدد اول فرد $p_۲$، $p_۳$، ...، p_n مانده‌های درجهٔ دوم p باشند، می‌توانیم p را هر عدد اولی در دنبالهٔ $N+۱$، $۲N+۱$، $۳N+۱$، ...، که در آنها $N = ۸p_۲p_۳\cdots p_n$ است در نظر بگیریم.

◁ **۴۰.۷** با استفاده از قضیهٔ دیریکله ثابت کنید که به‌ازای هر عدد x، بی‌نهایت عدد اول p وجود دارد به‌طوری که کوچکترین ریشهٔ اولیهٔ مثبت p بزرگتر از x باشد. (راهنمایی: از توضیح قبل استفاده کنید.)

حل. فرض می‌کنیم $p_n > \cdots > p_2 > p_1$ اعداد اولِ نابیشتر از x باشند، و فرض می‌کنیم p عدد اولی به‌صورت $8k+1$ باشد که p_2، p_3، ...، p_n مانده‌های درجهٔ دوم آن باشند؛ بنابر قضیهٔ دیریکله، تعداد نامتناهی این چنین p وجود دارد (توضیح قبل را ببینید). چون p به‌صورت $8k+1$ است، ۲ نیز یک ماندهٔ درجهٔ دوم p است. اگر m عدد صحیحی باشد که در تجزیه‌اش حداکثر اعداد اول p_1، p_2، ...، p_n به‌کار آید، آنگاه m یک ماندهٔ درجهٔ دوم p است، زیرا حاصلضرب مانده‌های درجهٔ دوم یک ماندهٔ درجهٔ دوم است. لذا هر عددِ صحیح مثبتِ نابیشتر از x یک ماندهٔ درجهٔ دوم p است. حال، فرض کنیم g یک ریشهٔ اولیهٔ مثبت p باشد. چون g یک نامانده‌ٔ درجهٔ دوم p است، در نتیجه بایستی بزرگتر از x باشد.

۴۱.۷ با استفاده از قضیهٔ ۱۲.۷ نشان دهید که تعداد نامتناهی عدد اول وجود دارند که نمایش اعشاری آنها با ۱ شروع و به ۷ ختم می‌شود.

حل. مجموعهٔ همهٔ اعدادی به‌صورت $10k+7$ را که بین 10^n و 2×10^n قرار دارند با S_n نشان می‌دهیم. نمایش اعشاری هر عدد در S_n با ۱ شروع و به ۷ ختم می‌شود.

فرض کنیم $f(x)$ تعداد اعداد اول به‌صورت $10k+7$ باشد که بزرگتر از x نیستند. اگر $y = 10^n$، آنگاه تعداد اعداد اول در S_n برابر است با $f(2y) - f(y)$. چون $\phi(10) = 4$، (۱۲.۷) ایجاب می‌کند که بتوان نسبت $f(x)/(x/\log x)$ را با اختیار x به‌قدرکافی بزرگ، به دلخواه به ۱/۴ نزدیک کرد. عدد n را آن‌قدر بزرگ اختیار می‌کنیم که به‌ازای هر $x > 10^n$، این نسبت بین ۱/۵ و ۱/۳ واقع شود. لذا حداقل $g(y) = (1/5)2y/\log(2y) - (1/3)y/\log y$ عدد اول در S_n وجود دارند. محاسبه نشان می‌دهد که $g(y) = y(\log y - 5\log 2)/15\log y(\log 2 + \log y)$. به آسانی نشان داده می‌شود که اگر y به اندازهٔ کافی بزرگ اختیار شود، می‌توان $g(y)$ را به‌دلخواه بزرگ ساخت؛ به‌ویژه، می‌توان $g(y)$ را بزرگتر از ۱ ساخت. لذا به‌ازای هر عدد صحیح n که به اندازهٔ کافی بزرگ باشد، حداقل یک عدد اول در S_n وجود دارد.

حدسیهٔ گولدباخ و سایر مسائل باز

۴۲.۷ ثابت کنید که حدسیهٔ گولدباخ ایجاب می‌کند که هر عدد صحیحِ فردِ بزرگتر از ۷ مجموع سه عدد اول فرد باشد.

حل. اگر n عدد صحیح فردی بزرگتر از ۷ باشد، آنگاه $n-3$ زوج و بزرگتر از ۴ است. لذا، بنابر حدسیهٔ گولدباخ، $n-3$ مجموع دو عدد اولِ p و q است. علاوه بر این، p و q فرد هستند، زیرا فقط ۴ مجموع دو عدد اول زوج است. در نتیجه $n=3+p+q$، مجموع سه عدد اول فرد.

۴۳.۷ معلوم شده است که هر عدد صحیح مثبتِ فرد که به اندازهٔ کافی بزرگ باشد، مجموعِ سه عدد اول فرد است (وینوگرادوف). با استفاده از این حکم نشان دهید که هر عدد صحیح مثبت که به اندازهٔ کافی بزرگ باشد، مجموع حداکثر چهار عدد اول است.

حل. با استفاده از قضیهٔ وینوگرادوف، نشان می‌دهیم که هر عدد صحیح زوج که به اندازهٔ کافی بزرگ باشد مجموع چهار عدد اول است. فرض می‌کنیم عدد زوج n به آن اندازه بزرگ باشد که $n-3$ مجموع سه عدد اول فرد p، q، و r باشد. لذا $n=3+p+q+r$.

۴۴.۷ ثابت کنید که حدسیهٔ گولدباخ با حکم زیر هم‌ارز است: هر عدد $n>5$ مجموع سه عدد اول است.

حل. ابتدا فرض می‌کنیم که حدسیهٔ گولدباخ درست باشد. نشان می‌دهیم که هر $n>5$ مجموع سه عدد اول است. اگر $n>5$، آنگاه $n-2$ زوج و حداقل ۴ است، لذا $n-2$ مجموع دو عدد اول p و q است. بنابراین $n=2+p+q$، که مجموع سه عدد اول است، اگر $n>5$ فرد باشد، آنگاه $n-3$ زوج و حداقل ۴ است، بنابراین $n-3$ مجموع دو عدد اول، و لذا n مجموع سه عدد اول است.

حال، فرض می‌کنیم که هر $n>5$ مجموع سه عدد اول باشد. نشان می‌دهیم که حدسیهٔ گولدباخ برقرار است. فرض کنیم $n\geq 4$ زوج باشد؛ آنگاه $n+2$ مجموع سه عدد اول است. اما چون $n+2$ زوج است، حداقل یکی از این اعداد اول بایستی ۲ باشد (اگر هر سه فرد باشند، آنگاه $n+2$ فرد خواهد شد). لذا اعداد اول p و q وجود دارند که $n+2=2+p+q$، و لذا $n=p+q$، که مجموع دو عدد اول است.

۴۵.۷ (الف) اگر $x-1$ و $x+1$ اول باشند، نشان دهید که x^2-1 دقیقاً چهار مقسوم‌علیه مثبت دارد. (ب) اگر x مثبت و x^2-1 دقیقاً چهار مقسوم‌علیه مثبت داشته باشد، ثابت کنید یا $x=3$ یا $x-1$ و $x+1$ هر دو اول هستند.

حل. (الف) قرار می‌دهیم $p=x-1$ و $q=x+1$. پس $x^2-1=pq$، و آشکار است که ۱، p، q، و pq تنها عاملهای مثبت pq هستند.

(ب) اعداد ۱، $x-1$، $x+1$، و x^2-1 عاملهای x^2-1 هستند و همگی متمایزند، زیرا روشن است که $x>2$. لذا آنها تنها مقسوم‌علیه‌های x^2-1 هستند. به‌ویژه، $x-1$ نمی‌تواند عاملهای مثبتی جز ۱ و $x-1$ داشته باشد، و لذا $x-1$ اول است. همچنین، $x+1$ نمی‌تواند مقسوم‌علیه‌های مثبتی غیر از $x+1$، و (احتمالاً) $x-1$ داشته باشد. لذا اگر $x-1$ عدد $x+1$ را نشمارد، آنگاه $x+1$ اول است، و اگر $x>2$ و $x-1$ عدد $x+1$ را بشمارد، آنگاه $x=3$.

۴۶.۷ (شینتسل[1]، ۱۹۵۸) (الف) فرض کنید m و n اعداد صحیح مثبتی باشند. ثابت کنید عدد صحیح c وجود دارد به‌طوری که $(c,m)=(2n-c,m)=1$. (راهنمایی: ابتدا حالتی را که m اول است در نظر بگیرید، و سپس از تجزیهٔ m استفاده کنید.)

(ب) با استفاده از (الف) و قضیهٔ دیریکله ثابت کنید که به‌ازای هر پیمانهٔ مفروض m و هر عدد زوج $2n$؛ تعداد نامتناهی اعداد اول p و q وجود دارند به‌طوری که $2n\equiv p+q(\bmod m)$.

حل. (الف) فرض کنیم $m=\prod_{i=1}^{t}p_i^{a_i}$. نشان می‌دهیم که به‌ازای هر عدد اول p_i، عدد صحیح c_i وجود دارد به‌طوری که $(c_i,p_i)=(2n-c_i,p_i)=1$. اگر $p_i=2$، قرار می‌دهیم $c_i=1$. اگر p_i یک عدد اول فرد باشد، آنگاه p_i نمی‌تواند هر دو عدد $2n-1$ و $2n+1$ را بشمارد. بنابراین قرار می‌دهیم $c_i=1$ اگر p_i $(2n-1)$ و در غیر این‌صورت قرار می‌دهیم $c_i=-1$. حال از قضیهٔ باقیماندهٔ چینی را برای یافتن عدد صحیح c به‌طوری که برای $1\le i\le t$، $c\equiv c_i(\bmod p_i)$ استفاده می‌کنیم. آشکار است که $(c,m)=(2n-c,m)=1$.

(ب) قسمت (الف) را برای یافتن یک عدد صحیح c به‌طوری‌که $(c,m)=(2n-c,m)=1$ به‌کار می‌بریم. فرض کنیم p و q دو عدد اول به‌ترتیب، به‌صورت $mk+c$ و $mk+2n-c$ باشند. (بنابر قضیهٔ دیریکله، بی‌نهایت عدد اول به‌صورت هر یک وجود دارند.) بدیهی است که $p+q\equiv 2n(\bmod m)$.

توضیح. قسمت (ب) یک صورت خیلی ضعیفی از حدسیهٔ گولدباخ است، زیرا اعداد اول p و q به m بستگی دارند.

۴۷.۷ ثابت کنید که هیچ چندجمله‌یی غیرثابت $f(x)$ با ضرایب صحیح وجود ندارد که به‌ازای هر عدد صحیح مثبت n، $f(n)$ اول باشد.

حل. فرض کنیم $f(1)=p$، که در آن p اول است. چون $1+kp\equiv 1(\bmod p)$، از (ii.۳.۲) نتیجه می‌شود که به‌ازای هر عدد صحیح k، $f(1+kp)\equiv f(1)\equiv 0(\bmod p)$.

1. Schinzel

لذا اگر بخواهد $f(n)$ به‌ازای هر عدد صحیح مثبت n اول باشد، بایستی داشته باشیم به‌ازای هر k، $f(۱+kp)=p$. فرض می‌کنیم $g(x)=f(x)-p$. اگر به‌ازای هر k، $f(۱+kp)=p$، آنگاه معادلهٔ $g(x)=۰$ بی‌نهایت ریشه دارد. این ممکن نیست مگر آنکه $g(x)$ چندجمله‌یی صفر باشد، یعنی $f(x)$ چندجمله‌یی ثابت p باشد.

۴۸.۷ فرض کنید $f(x)$ یک چندجمله‌یی غیرثابت با ضرایب صحیح باشد. ثابت کنید تعداد نامتناهی عدد اول p وجود دارد به‌طوری که همنهشتی $f(x)\equiv ۰ \pmod p$ یک جواب دارد. (راهنمایی: اگر $a_۰$ جملهٔ ثابت $f(x)$ باشد، فرض کنید $a_۰\neq ۰$ و $f(a_۰x)=a_۰(۱+xg(x))$ را در نظر بگیرید.)

حل. اگر $a_۰=۰$، آنگاه $f(۰)=۰$، و لذا $f(۰)$ بر هر عدد اول بخشپذیر است. اگر $a_۰\neq ۰$، چندجمله‌یی $g(x)$ با ضرایب صحیح وجود دارد به‌طوری که $f(a_۰x)=a_۰(۱+xg(x))$. ثابت می‌کنیم به‌ازای هر عدد n، عدد اول $p>n$ وجود دارد به‌طوری که همنهشتی $f(x)\equiv ۰ \pmod p$ دارای جواب است.

هر یک از معادله‌های $xg(x)+۱=۱$ و $xg(x)+۱=-۱$ تعداد متناهی جواب دارند. قرار می‌دهیم $b=N!$، که در آن $N\geq n$ طوری انتخاب شده است که b بزرگتر از هر یک از این جوابها باشد. در این‌صورت $bg(b)+۱$ نمی‌تواند برابر ۱ یا -۱ باشد و لذا بر عدد اولی مانند p بخشپذیر است. اگر $p\leq N$، آنگاه $p\mid b$ و لذا $p\nmid bg(b)+۱$. بنابراین $p>N\geq n$. چون $p\mid bg(b)+۱$، در نتیجه $f(a_۰b)\equiv ۰ \pmod p$.

۴۹.۷ فرض می‌کنیم $f(x)$ یک چندجمله‌یی غیرثابت با ضرایب صحیح باشد. با استفاده از مسألهٔ قبل نشان دهید که به‌ازای هر k، عدد a وجود دارد به‌طوری که $f(a)$ بر لااقل k عدد اول بخشپذیر است.

حل. عدد صحیح مثبت k را اختیار می‌کنیم. بنابر مسألهٔ قبل k عدد اول $p_۱$، $p_۲$، ...، p_k وجود دارند به‌طوری که همنهشتی $f(x)\equiv ۰ \pmod{p_i}$ جوابی دارد، مثل a_i. بنابر قضیهٔ باقیماندهٔ چینی a وجود دارد به‌طوری که به‌ازای هر $۱\leq i\leq k$، $a\equiv a_i \pmod{p_i}$. لذا به‌ازای هر $i\leq k$، $f(a)\equiv ۰ \pmod{p_i}$، و بنابراین $f(a)$ بر حداقل k عدد اول بخشپذیر است.

تمرینهایی برای فصل ۷

۱. اثبات یا رد کنید: مقادیری از $n>۱$ وجود دارند به‌طوری که $n!$ یک مربع کامل است.

۲. اولین عدد تام زوج بزرگتر از 10^6 چیست؟

۳. دو رقم آخر عدد تام $2^{112^{12}}(2^{112^{13}}-1)$ چه هستند؟

۴. اثبات یا رد کنید: اگر 2^p-1 اول باشد، آنگاه $n=2^{p-1}+2^p+2^{p+1}+\cdots+2^{2(p-1)}$ یک عدد تام است.

۵. ثابت کنید که هر عدد تام که به ۸ ختم شود، به ۲۸ ختم می‌شود.

۶. اثبات یا رد کنید: اگر r، s، و t اعداد تام زوج متمایز باشند، آنگاه $\phi(rst)=8\phi(r)\phi(s)\phi(t)$.

۷. نشان دهید که هر عدد تام فرد به‌صورت pm^2 است، که در آن p اول است و $p\equiv 1 \pmod 4$. (مسألهٔ ۱۴.۷ را ببینید.)

۸. عدد صحیح مثبت n زائد خوانده می‌شود اگر $\sigma(n)>2n$. (الف) کوچکترین عدد زائد فرد را پیدا کنید. (سابقاً باور این بود که وجود ندارد.) (ب) اگر n زائد باشد، نشان دهید که هر مضرب مثبت n، نیز زائد است.

۹. بزرگترین مقسوم‌علیه مشترک $2^{30}-1$ و $2^{54}-1$ را به‌دست آورید.

۱۰. فرض کنید N عدد صحیحی باشد که بسط اعشاری آن تماماً از ۱ها تشکیل شده باشد. اگر N اول باشد، نشان دهید که تعداد ۱ها عددی اول است.

۱۱. اعداد $2^{26}+1$ و $2^{34}+1$ را تجزیه کنید. (راهنمایی: $4n^4+1=(2n^2+2n+1)(2n^2-2n+1)$.)

۱۲. فرض کنید F_n معرف عدد nام فرما باشد، اگر $n\geq 1$، ثابت کنید F_n+4 هرگز اول نیست.

۱۳. نشان دهید که $2^{2^n}+7$ به‌ازای بی‌نهایت مقدار n مرکب است. (راهنمایی: با پیمانهٔ ۱۱ کار کنید.)

۱۴. اگر $n\geq 1$، ثابت کنید عدد فرمای $2^{2^n}+1$ به‌صورت $9k-1$ یا $9k-4$ است.

۱۵. نشان دهید که $\phi(n)$ توانی از ۲ است اگر و تنها اگر n به‌صورت $2^s p_1 p_2 \cdots p_t$ باشد که در آن $s,t\geq 0$ و p_iها اعداد اول متمایز فرما هستند. (توجه کنید که هر حاصلضرب تهی بنابه تعریف برابر ۱ است.)

۱۶. ثابت کنید به‌ازای هر $n\geq 1$ اعداد n و $2^{2^n}+1$ نسبت به هم اول‌اند. (راهنمایی: از این مطلب استفاده کنید که هر عامل اول $2^{2^n}+1$ به‌صورت $2^{n+2}k+1$ است.)

۱۷. با استفاده از اصل برتران ثابت کنید به‌ازای هر $k>2$، عدد اول p وجود دارد به‌طوری که $p<k<2p$.

۱۸. با استفاده از قضیهٔ دیریکله نشان دهید که بی‌نهایت عدد اول وجود دارد که نمایش اعشاری آنها به ۱۱۱۱ ختم می‌شود.

۱۹. با استفاده از قضیهٔ دیریکله نشان دهید که به‌ازای هر عدد صحیح مثبت m، بی‌نهایت

عدد اول p و عدد اول q وجود دارند که $q \equiv p + ۲ (\mathrm{mod}\, m)$. (راهنمایی: مسألهٔ ۴۶.۷ را ببینید.)

۲۰. فرض کنید حدسیهٔ گولدباخ راست است. نشان دهید که می‌توان هر عدد فرد n را به بی‌نهایت طریق متفاوت به‌صورت $n = p + q - r$ بیان کرد، که در آن p، q، و r اول هستند.

ملاحظاتی برای فصل ۷

۱. تابع $x/\log x$ ابداً بهترین تقریب سادهٔ مناسب برای $\pi(x)$ نیست. گاوس در ۱۵ سالگی، یک جوری حدس زد که یک تقریب بسیار خوب $\mathrm{li}(x)$، انتگرال لگاریتمی، است که با $\mathrm{li}(x) = \int_۲^x (۱/\log t)dt$ تعریف می‌شود.

کوشش فراوانی برای تخمین اندازهٔ جملهٔ خطا، یعنی، بررسی رفتار تابع $\mathrm{li}(x) - \pi(x)$ به‌کار رفته است. معلوم شده است که اغلب این تابع بی‌نهایت بار تغییر علامت می‌دهد، و زمینه‌هایی برای این حدس وجود دارد که به‌ازای مقادیر به‌قدر کافی بزرگِ x، داریم $|\mathrm{li}(x) - \pi(x)| < x^{۱/۲} \log x$، ولی مسأله خیلی مشکل است. مسأله اندازهٔ جملهٔ خطا ارتباط نزدیکی با یکی از مشهورترین مسأله‌های بازِ تمام ریاضیات، یعنی، فرضیهٔ ریمان دارد. این فرضیه اظهار می‌دارد که تمام صفرهای تابع $\sum_{n=۱}^{\infty} ۱/n^s$، که s عدد مختلطی است، به‌صورت $s = ۱/۲ + t\sqrt{-۱}$ هستند که t حقیقی است. شواهد بسیار فراوانی وجود دارند که فرضیهٔ ریمان برقرار است، اما بیش از یکصد سال است که به یک راه‌حل قطعی تن در نداده است.

معلوم شده است که به‌ازای تعداد نامتناهی x، $|\mathrm{li}(x) - \pi(x)| > \sqrt{x}$. این چیزی است که بایستی به خاطر داشته باشیم هرگاه قضیهٔ اعداد اول را به این معنی تعبیر کنیم که $\pi(x)$ «تقریباً» $\mathrm{li}(x)$ (یا، «تقریباً» $x/\log x$) است. این تنها به این معنی است که برای x بزرگ، جملهٔ خطا خیلی از $\pi(x)$ کوچکتر است، اما به این معنی نیست که خطا در جمله‌های قدرمطلق کوچکتر است. مثلاً، معلوم است که اگر $x = ۴ \times ۱۰^{۱۶}$، آنگاه $\pi(x)$ دقیقاً برابر ۱۰۷۵۲۹۲۷۷۸۷۵۳۱۵۰ است. عدد $x/\log x$ با خطای ۲٫۷٪ تقریباً به اندازهٔ ۲۸۹۲۹۹۰۰۵۷۹۹۵۰ کوچکتر از $\pi(x)$ است، در حالی‌که $\mathrm{li}(x)$ با خطای $۰٫۵ \times ۱۰^{-۸}$ تقریباً به اندازهٔ ۵۵۳۸۸۶۱ بزرگتر از $\pi(x)$.

۲. فرض کنیم $\omega(n)$ تعداد عاملهای اول متمایز باشد. رفتار تابع $\omega(x)$ کاملاً نامنظم است، ولی می‌توان اندازهٔ متوسط آن را تعیین کرد. اگر $f(x) = \sum_{n \le x} \omega(n)$، آنگاه با انتخاب x به‌قدر کافی بزرگ می‌توان نسبت $f(x)/x \log(\log x)$ را به دلخواه به ۱ نزدیک کرد. بنابراین، مثلاً، اعداد صحیح مثبت تا تقریب یک بیلیون، به‌طور متوسط، تنها سه عامل اولِ متمایز دارند. یک

نتیجهٔ مربوط حتی شگفت‌آورتر است. فرض کنیم $\Omega(n)$ تعداد کل عاملهای اول n باشد؛ مثلاً، اگر $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$، آنگاه $\Omega(n) = a_1 + a_2 + \cdots + a_k$. اگر $g(x) = \sum_{n \le x} \Omega(n)$، آنگاه مجدداً اگر x به اندازهٔ کافی بزرگ اختیار شود. می‌توان نسبت $g(x)/\log(\log x)$ را به دلخواه به ۱ نزدیک کرد. برای تفصیل بیشتر، آشنایی با نظریهٔ اعداد نوشتهٔ هاردی و رایت را ببینید.

۳. بزرگترین اعداد اول شناخته شده تقریباً همیشه اعداد اول مرسن بوده‌اند. بیشترین استثنای اخیر دورهٔ کوتاهی از اوت ۱۹۸۹ تا مارس ۱۹۹۲ بود وقتی که $۳۹۱۵۸۱ \times ۲^{۲۱۶۱۹۳} - ۱$ بزرگترین عدد اول شناخته شده بود؛ که در مارس ۱۹۹۲ توسط عدد اول مرسنِ $۲۷۵۶۸۳۹ - ۱$ از میدان به در شد.

شرح مختصری از زندگینامه‌ها

پافنوتی چبیشف[1] در ۱۸۲۱ به دنیا آمد و مهمترین ریاضیدان روسی نسل خودش شد. تحت هدایت او سن‌پترزبورگ برای اولین بار از زمان اویلر مرکز فعالیتهای ریاضی شد. او سهم قابل توجهی در بسیاری از شاخه‌های ریاضی، از جمله احتمال و آنالیز عددی دارد. چبیشف در کارهایش در آنالیز عددی به‌طور وسیعی بسط کسر مسلسل یک تابع را به‌کار برد. برخلافِ بسیاری از ریاضیدانان سدهٔ نوزدهم، توجه دقیقی به کرانهای خطا داشت.

علاوه بر به‌دست آوردن کرانهای بالا و پایین خوب در نسبت $\pi(x)$ به $x/\log x$، در ۱۸۵۲ چبیشف نشان داد که اگر نسبت دارای حد باشد، آن حد بایستی ۱ باشد. او همچنین خاطرنشان ساخت که اصل برتران به آسانی از تخمینش برای $\pi(x)$ نتیجه می‌شود. سایر تحقیقات اصلی چبیشف در نظریهٔ اعداد در حوزهٔ تقریب دیوفانتی قرار دارد (که به اجمال، عبارت است از مطالعهٔ مقادیر مینیمم توابع وقتی که متغیرها اعداد صحیح را اختیار می‌کنند).

چبیشف در ۱۸۹۴ در سن‌پترزبورگ درگذشت.

پیتر گوستاو لوژون دیریکله[2] در ۱۸۰۵، در نزدیکی شهر کولن[3] در آلمان متولد شد معلم ریاضیات او در دبیرستان گئورگ اُهم[4] بود، که اکنون به خاطر قانون اُهم معروف است. دیریکله در ۱۸۲۲ به پاریس رفت که در آن زمان مرکز جهانی علوم ریاضی بود. دیریکله قویاً تحت تأثیر فوریه و حتی بیشتر از آن مطالعهٔ تحقیقات حسابی گاوس بود. پس از اقامت کوتاهی در برسلائو[5]، سمتی را در دانشگاه برلین پذیرفت، او تقریباً تا آخر عمرش در برلین اقامت کرد، او در

1. Pavnuty Chebyshev 2. Peter Gustav Lejeune Dirichlet 3. Cologne
4. Georg Ohm 5. Breslau

میان همکاران و دانشجویان ریاضیدانانی نظیر ژاکوبی، کومر، آیزنشتاین، کرونکر، دوکینت، و ریمان را برشمرده است. به‌ویژه، ژاکوبی یک دوست شخصی نزدیک دیریکله بود.

دیریکله در آنالیز مختلط و سریهای فوریه پیشرفتهای چشمگیری داشت. نخستین کار عالی او در نظریهٔ اعداد در ۱۸۲۸ انتشار یافت، زمانی که با لژاندر آخرین قضیهٔ فرما را در حالت $n = 5$ اثبات کرد. شاید دست‌آورد اصلی دیریکله در نظریهٔ اعداد اثبات این مطلب باشد که تمام تصاعدهای حسابی مناسب دارای بی‌نهایت عدد اول هستند؛ او در این اثبات یک روش تحلیلی ابداع کرد، که توسط دیگران به تناسب تظریف شد در بسیاری از تحقیقات بنیادی، از جمله قضیهٔ اعداد اول به‌کار رفت. دیریکله همچنین سهم مهمی در نظریهٔ اعداد صحیح جبری دارد، او نشان داد که می‌توان یکه‌ها را در یک روش نسبتاً ساده تولید کرد. کتاب دروس نظریهٔ اعداد[1] او بیش از پنجاه سال یک کتاب درسی پیشرفتهٔ استانده در نظریهٔ اعداد بود.

بعد از چهار سال که به‌عنوان استاد ریاضیات در گوتینگن جانشین گاوس گردید، در ۱۸۵۹ درگذشت.

گئورگ برنهارت ریمان در ۱۸۲۶ متولد شد و در گوتینگن در خدمت گاوس تحصیل کرد و دکترایش را در ۱۸۵۱ دریافت نمود. در دوران کوتاه زندگیش، ریاضیات را دگرگون ساخت، آثاری در حساب دیفرانسیل و انتگرال و آنالیز مختلط ابداع کرد. او در نظریهٔ اعداد تنها یک مقاله نوشت، در آن مقاله با استفاده از ویژگیهای تابعی که اکنون به‌عنوان تابع زتای ریمان شناخته می‌شود، روشی را به اختصار برای اثبات قضیهٔ اعداد اول تبیین کرد. این شرح مختصر، که سرشار از اندیشه‌های فراوان است، راهنمای برهانی از کار درآمد که توسط آدامار و دو لا واله پوسن کشف شد، هر چند که مشکلات فنی زیادی باید برطرف شود.

ریمان به علت بیماری سل ریوی در ۱۸۶۶ در ۳۹ سالگی درگذشت.

مراجع

Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

این کتابِ درسی یک مقدمهٔ عالی در نظریهٔ اعداد برای دانشجویانی است که زمینه‌ای قوی در آنالیز دارند. به‌ویژه، این کتاب اثباتهای مفصل از قضیهٔ اعداد اول و قضیهٔ دیریکله در اعداد اول را به‌صورت تصاعدهای حسابی ارائه می‌دهد. برآوردهای بسیار دیگری، معمولاً با کرانهای خطا، از اندازهٔ متوسطِ توابع مهم نظریه اعداد وجود دارند.

1. Vorlesungen über Zahlentheorie

David M. Bressoud, *Factorization and Primality Testing.* (See Chapter 3.)

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Fourth Edition), The Clarendon Press, Oxford, England, 1971.

این کتاب یکی از بزرگترین کتابهای کلاسیک در میان کتابهای نظریهٔ اعداد به زبان انگلیسی است. بسیاری از بخشها مقدماتی هستند، اما کتاب برهان کاملی از قضیهٔ اعداد اول، همچنین بحثی از مطالبی نظیر افرازها و هندسهٔ اعداد را که به‌ندرت درکتابهای مقدماتی یافت می‌شوند دربر دارد.

Paulo Ribenboim, *The Book of Prime Number Records* (Second Edition), Springer-Verlag, New York, 1989.

این یک بازنگری دایرةالمعارفی است از آنچه که دربارهٔ اعداد اول در ۱۹۸۹ معلوم بود، با مقدار وسیعی اطلاعات تاریخی و یک کتابشناسی عالی، مسائل باز مطرح‌شده در این فصل، و بسیاری دیگر، تماماً با گزارشهای پیشرفت و مدارک عددی تفصیلی، بررسی شده‌اند. مطالعهٔ این کتاب به دلیل بینشی که دربارهٔ حوزهٔ وسیع پژوهش در مورد اعداد اول به خواننده می‌دهد شدیداً توصیه می‌شود.

۸

چند معادلهٔ دیوفانتی و آخرین قضیهٔ فرما

اصطلاح معادلهٔ دیوفانتی در اصل به یک معادلهٔ جبری برمی‌گردد که برای آن تنها جوابهای گویای مثبت مد نظر بوده است، هر چند که اکنون عموماً در مورد معادلاتی که جوابهای آنها به اعداد صحیح مقید می‌شوند به‌کار می‌رود. تعدادی مسأله از این نوع را می‌توان در ریاضیات بابلیها (حدود ۲۰۰۰ تا ۱۶۰۰ ق‌م) پیدا کرد، ولی اولین بررسی نظام‌مند درکتاب حساب دیوفانتوس (حوالی ۲۵۰ م) ظاهر می‌شود. این اثر، که قسمتی از آن به‌جا مانده است، گردایه‌ای بالغ بر ۲۵۰ مسأله است که بیشتر شامل معادلات درجهٔ دوم است. دیوفانتوس معمولاً به تعیین یک جواب گویا برای هر معادله اکتفا می‌کرد.

یکی از قدیمی‌ترین معادله‌های دیوفانتی در مورد مثلثهای قائم‌الزاویه‌ای است که طول اضلاعشان عدد صحیح است، و اغلب مثلثهای فیثاغورسی نامیده می‌شوند، معادلهٔ مورد نظر $x^2 + y^2 = z^2$ است. در یکی از جدولهای سفالی بابلیها پانزده جواب که بعضی از آنها نظیر (۴۹۶۱، ۶۴۸۰، ۸۱۶۱) خیلی بزرگ هستند، یافت شده است. این دلیلی است بر این باور که آنها یک روش نظام‌مندی برای تولید جوابها داشته‌اند. این معادله از زمان ریاضیدانان باستانی یونان

مورد توجه بیشتری واقع شد، به‌ویژه فیثاغورس (حوالی ۵۷۰ ق م)، کسی که عموماً افتخار فرمولی را که بی‌نهایت جواب تولید می‌کند به او داده شده است.

بعدها، کرجی، ریاضیدان عربی‌نویس در قرن یازدهم روشهای دیوفانتوس را توسعه داد. در قرون وسطی، لئوناردو پیسایی، (ح ۱۱۷۵ـ۱۲۵۰)، که بیشتر به‌عنوان فیبوناتچی شناخته می‌شود، جبر و بنابراین به‌طور غیرمستقیم کارهای دیوفانتوس را، از دنیای عرب انتقال داد و مورد توجهٔ ریاضیدانان اروپایی قرار داد.

در سدهٔ هفدهم، فرما معادلات دیوفانتی را به‌طور وسیعی مورد بررسی قرار داد. در ۱۶۳۷ در نسخه‌ای از کتاب حساب دیوفانتوس که توسط باشه به لاتین ترجمه شده بود، فرما یکی از مشهورترین حدسیه‌های ریاضی را بیان کرد: اگر $n \geq 3$، معادلهٔ $x^n + y^n = z^n$ هیچ جواب صحیح غیرصفر برای x، y، و z ندارد. این حدسیه، که معروف به آخرین قضیهٔ فرماست، نیروی خلاقه نسلهایی از ریاضیدانان را مجذوب خود کرد و متجاوز از سه و نیم قرن تن به اثبات نداد تا سرانجام، یک اثبات کامل در بیش از ۲۰۰ صفحه در اکتبر ۱۹۹۴ برای آن پیدا شد.

مسألهٔ معروف دیگری که به زبان دیوفانتوس برمی‌گردد، یافتن اعداد صحیح مثبتی است که می‌توان آنها را به‌صورت مجموع دو مربع نوشت. در مکاتبه با مرسین و روبروال در ۱۶۴۰، فرما به این مسأله جواب درست داد، و تعداد چنین نمایشها را مطرح کرد، هر چند که برهانی ارائه نداد.

یک مسألهٔ دیگر در این ارتباط بررسی این مسأله است که کدام عدد صحیح را می‌توان به‌صورت مجموع چهار مربع نوشت. باشه حدس زده بود که هر عدد صحیح مثبت چنین نمایشی دارد. فرما، در نسخهٔ شخصی خود از کتاب دیوفانتوس نوشت که برهانی متکی بر روش نزول نامتناهی، تکنیکی که در مسألهٔ دو مربع نیز به‌کار برده بود، داشته است. اویلر سهم عمده‌ای در حل این مسأله دارد، اما اولین اثبات کامل توسط لاگرانژ در ۱۷۷۰ ارائه گردید.

در همان سال، ادوارد ورینگ انگلیسی (۱۷۳۴ـ۱۷۹۸) در کوشش برای تعمیم مسألهٔ چهار مربع، حدس زد که هر عدد را می‌توان به‌صورت مجموع ۴ مربع، ۹ مکعب، ۱۹ توان چهار، و به‌طور کلی، به‌ازای هر عدد صحیح مثبت k به‌صورت مجموع ثابتی از توانهای k نوشت. از آن زمان، مسألهٔ ورینگ توجه زیادی را به خود جلب کرد. سرانجام در ۱۹۰۹ توسط داوید هیلبرت (۱۸۶۲ـ۱۹۴۳) ریاضیدان آلمانی حل شد، اما مسأله‌های وابسته به آن موضوع تحقیقات جدی باقی ماند.

قضیه‌هایی برای فصل ۸

بحث خود را از معادلات دیوفانتی با یک دسته‌بندی از تمام مثلثهای قائم‌الزاویه که طول اضلاعشان عدد صحیح هستند، آغاز می‌کنیم.

معادلهٔ $x^2 + y^2 = z^2$

قضیهٔ مشهور فیثاغورس بیان می‌دارد که در یک مثلث قائم‌الزاویه، مربع وتر برابر است با مجموع مربعات دو ضلع دیگر. بنابراین به معادلهٔ $x^2 + y^2 = z^2$ هدایت می‌شویم. مسألهٔ یافتن جوابهای صحیح این معادله به تقریباً ۴۰۰۰ سال قبل برمی‌گردد.

(۱.۸) تعریف. فرض کنیم x، y، و z اعداد صحیح مثبت هستند. اگر $x^2 + y^2 = z^2$، آنگاه (x, y, z) یک سه‌تایی فیثاغورسی خوانده می‌شود. (سه‌تاییهای (x, y, z) و (y, x, z) متفاوت به حساب نمی‌آیند.) علاوه بر این، اگر x، y، و z عامل مثبت مشترکی بجز ۱ نداشته باشند، آنگاه (x, y, z) یک سه‌تایی اولیه نامیده می‌شود.

مثلث قائم‌الزاویه با اضلاع صحیح را یک مثلث فیثاغورسی نیز می‌نامیم.

توضیح. اگر عدد صحیح k دو تا از اعداد x، y، و z را بشمارد، سری را، هم می‌شمارد. مثلاً، اگر k اعداد x و y را بشمارد، آنگاه $k^2 | x^2 + y^2$؛ لذا $k | z$. با استدلالی مشابه، اگر $k | y$ و $k | z$، آنگاه $k^2 | z^2 - y^2$، لذا $k | x$. بنابراین، اگر یکی از (x, y)، (x, z)، یا (y, z) برابر ۱ باشد، همگی برابر ۱ هستند.

اگر (x, y, z) یک سه‌تایی فیثاغورسی باشد و d بزرگترین مقسوم‌علیه مشترک x، y، و z، آنگاه روشن است که $(x/d, y/d, z/d)$ یک سه‌تایی فیثاغورسی اولیه است. لذا هر سه‌تایی فیثاغورسی مضربی از یک سه‌تایی اولیه است، و بنابراین کافی است که جوابهای اولیه را جستجو کنیم.

هم‌ارز هندسی فرمولهای زیر برای تولید سه‌تاییهای فیثاغورسی به فیثاغورث نسبت داده شده است: $x = k$، $y = (k^2 - 1)/2$، و $z = (k^2 + 1)/2$، که در آن $k > 1$ فرد است. مشهور است که پلاتو (حدود ۳۸۰ ق م) قاعدهٔ مشابه، یعنی $x = 2k$، $y = k^2 - 1$، و $z = k^2 + 1$ را به‌دست آورده است. ولی، هیچ‌یک از فرمولها همهٔ سه‌تاییهای اولیهٔ فیثاغورسی را تولید نمی‌کنند. (مثلاً سه‌تایی $(20, 21, 29)$ به‌صورت هیچ‌کدام نیست.) صورت کلی جواب، که بعداً ارائه می‌دهیم، درکتاب حساب دیوفانتوس و اصول اقلیدس آمده است. برهانی که در واقع جواب کلی است، خیلی بعد به‌دست آمد.

توضیح. اگر (x, y, z) یک سه‌تایی فیثاغورسی باشد، x و y هر دو نمی‌توانند فرد باشند، زیرا در غیر این‌صورت $x^2 \equiv y^2 \equiv 1 \pmod 4$ و بنابراین $z^2 \equiv 2 \pmod 4$ که غیرممکن است.

قضیهٔ زیر روشی را برای تولید همهٔ سه‌تاییهای فیثاغورسی با نشان دادن چگونگی تولید تمام سه‌تاییهای اولیه ارائه می‌دهد.

(۲.۸) قضیه. یک سه‌تایی فیثاغورسی (x, y, z)، با فرض زوج بودن y، اولیه است اگر و تنها اگر به‌صورت

$$x = a^۲ - b^۲ \qquad y = ۲ab \qquad z = a^۲ + b^۲$$

باشد که در آنها a و b دو عدد صحیح مثبت هستند که یکی زوج و دیگری فرد است، $a > b$ و $(a, b) = ۱$. هر سه‌تایی فیثاغورسی مضربی از یک سه‌تایی فیثاغورسی اولیه است.

برهان. آشکار است که x، y، و z با تعریف بالا در $x^۲ + y^۲ = z^۲$ صدق می‌کنند. ملاحظه می‌کنید که $z + x = ۲a^۲$ و $z - x = ۲b^۲$. لذا اگر p یک عامل اول مشترک از x و z باشد، آنگاه $p|۲a^۲$ و $p|۲b^۲$؛ چون p فرد است پس $p|a$ و $p|b$. چون $(a, b) = ۱$، در نتیجه $(x, z) = ۱$، و لذا (x, y, z) یک سه‌تایی اولیه است.

بعکس، اگر (x, y, z) یک سه‌تایی اولیه باشد، آنگاه روشن است که x و y هر دو نمی‌توانند زوج باشند. از آنجا که به دنبال جوابها با y زوج هستیم، بایستی x فرد باشد و لذا z فرد است. بنابراین، $z + x$ و $z - x$ زوج‌اند. قرار می‌دهیم $r = (z + x)/۲$ و $s = (z - x)/۲$. چون $z = r + s$ و $x = r - s$، هر مقسوم‌علیه مشترک r و s عدد (z, x) را نیز می‌شمارد، و لذا $(r, s) = ۱$. چون $y^۲ = z^۲ - x^۲ = (z + x)(z - x)$، داریم $(y/۲)^۲ = rs$؛ اما r و s نسبت به‌هم اول هستند، لذا هر کدام از r و s بایستی مربع کامل باشند. (این مطلب به آسانی از تجزیهٔ r و s به عوامل اول حاصل می‌شود؛ مسألهٔ ۳۳.۱ را ببینید.) اگر $r = a^۲$ و $s = b^۲$، آنگاه $a > b$ و $x = r - s = a^۲ - b^۲$، $z = r + s = a^۲ + b^۲$، و $y^۲ = ۴rs = ۴a^۲b^۲$، یعنی $y = ۲ab$. آشکار است که یکی از a و b فرد و دیگری زوج است، زیرا در غیر این‌صورت x زوج خواهد شد. سرانجام، ملاحظه می‌کنیم که $(a, b) = ۱$، زیرا هر مقسوم‌علیه مشترک a و b به‌وضوح x، y، و z را می‌شمارد.

توضیح. ۱. شایان توجه است که حتی اگر هیچ محدودیتی روی a و b (جز آنکه $a > b$) قرار ندهیم، فرمولهای (۲.۸) همهٔ سه‌تاییهای فیثاغورسی را تولید نمی‌کند. (مسألهٔ ۵.۸ را ببینید.) سه‌تاییهایی را که بدین‌طریق می‌توان به‌دست آورد در مسألهٔ ۶.۸ مشخص شده‌اند.

۲. در فصل ۱۱، با استفاده از اعداد صحیح گاوسی، برهان دیگری از (۲.۸) را ارائه خواهیم کرد.

آخرین قضیهٔ فرما

کمی بعد از ۱۶۳۰، فرما در حاشیهٔ نسخهٔ شخصی کتاب دیوفانتوس خود که توسط باشه در ۱۶۲۱ به لاتین ترجمه شده بود، مطلب زیر را نوشت:

> غیرممکن است مکعبی را به‌صورت مجموع دو مکعب، یک توان چهارم را به‌صورت مجموع دو توان چهارم و به‌طور کلی، هر توانی بزرگتر از ۲ را به‌صورت مجموعی از دو توان مشابه نوشت. من اثباتی به‌راستی شگفت‌انگیز برای این دارم، اما این حاشیه تنگتر از آن است که گنجایش درج آن را داشته باشد.

این حدسیه، که یکی از معروفترین مسائل در ریاضیات است، به‌عنوان آخرین قضیهٔ فرما شناخته شده است. می‌توان آن را با اصطلاحات جدید به‌صورت زیر بیان کرد.

(۳.۸) آخرین قضیهٔ فرما. اگر $n \geq ۳$، معادلهٔ $x^n + y^n = z^n$ جواب صحیح غیرصفر ندارد.

از قضیه‌هایی که فرما در حاشیه‌های حساب دیوفانتوس نوشت، همگی جز آخرین قضیه‌اش، بعداً ثابت شدند. تعداد زیادی از ریاضیدانان برجسته، برای اثبات این حدسیه تلاشهای ناموفقی کردند. در ژوئن ۱۹۹۳، اعلام شد که بعد از سه سده و نیم، اثباتی از آخرین قضیهٔ فرما یافت شده است. این اثبات که توسط اندرو وایلز[1] ارائه گردید، بسیار طولانی (متجاوز از ۲۰۰ صفحه) بود و در آن از نتایج بسیار عمیقی از هندسه جبری استفاده شده بود. ولی رخنه‌هایی در برهان اولیه وجود داشت که توسط وایلز و ریچارد تیلر[2] در اکتبر ۱۹۹۴ اصلاح گردیدند.

برهانی که فرما در خاطر داشت، احتمالاً برهانی بود که در آن از روش نزول نامتناهی استفاده می‌کرد، این روش تکنیک اصلی او در اثباتهایش بود و اغلب در مکاتباتش (تقریباً همیشه بدون شرح جزئیات) به آن اشاره می‌کرد. می‌توان این روش را چنین توصیف کرد: فرض کنیم حکمی به‌ازای یک عدد صحیح مثبت مفروض برقرار باشد، سپس نشان می‌دهیم که این حکم به‌ازای یک عدد صحیح مثبت کوچکتر برقرار است. اگر این روند را ادامه دهیم، سرانجام به یک تناقض می‌رسیم، زیرا نمی‌توانیم به‌طور نامحدود اعداد صحیح مثبت متوالی را کوچکتر تولید کنیم. لذا نتیجه می‌گیریم که حکم به‌ازای هیچ عدد صحیح مثبتی برقرار نیست.

ما روش نزول نامتناهی را برای آخرین قضیهٔ فرما در حالت $n = ۴$ به‌کار خواهیم برد. در واقع قضیهٔ کمی قویتر زیر را اثبات می‌کنیم. خود فرما در ۱۶۵۹ با کاربرد نزول متناهی برهانی برای یک قضیهٔ نزدیک به آن ادامه داد. این تنها برهانی است که فرما از کارهایش در نظریهٔ اعداد

1. Andrew Wiles 2. Richard Taylor

به‌جا گذاشته است. اولین اثبات به ثبت رسیده از قضیهٔ بعد منتسب به فرنیکل است، اما دلیل قوی وجود دارد که اصل استدلال از فرما بوده است.

(۴.۸) قضیه. معادلهٔ $x^۴ + y^۴ = z^۲$ جواب صحیح غیرصفر ندارد.

برهان. می‌توانیم فرض کنیم که جوابها (در صورت وجود) اعداد صحیح مثبت هستند، زیرا تغییر در علامتهای x، y، یا z باز هم جوابی به‌دست می‌دهد. برهان با روش نزول نامتناهی فرما خواهد بود. دقیقتر بگوییم، اگر فرض کنیم معادله جوابی در اعداد صحیح مثبت دارد، آنگاه جواب مثبتی وجود دارد که z کوچکترین مقدار را دارد؛ سپس جواب مثبت دیگری با مقدار کوچکتری برای z به‌دست می‌آوریم، و این تناقض قضیه را اثبات می‌کند.

لذا فرض می‌کنیم x، y، z یک جواب مثبت باشد، که در آن z مینیمال است. اگر x و y عامل مشترکی بزرگتر از ۱ داشته باشند، یک عدد اول p وجود دارد که x و y را می‌شمارد. چون $p^۴|x^۴ + y^۴$، داریم $p^۴|z^۲$ و لذا $p^۲|z$. از این رو $(x/p)^۴ + (y/p)^۴ = (z/p^۲)^۲$، و ما یک جواب مثبت با مقدار z کوچکتر تولید کرده‌ایم. بنابراین، x و y نمی‌توانند عامل مشترکِ بزرگتر از ۱ داشته باشند؛ به‌ویژه، $(x^۲, y^۲, z)$ یک سه‌تایی فیثاغورسی اولیه است. لذا $x^۲$ و $y^۲$ مخالف همپایگی هستند؛ فرض می‌کنیم $x^۲$ فرد و $y^۲$ زوج باشد. لذا بنابر (۲.۸)، u و v که نسبت به‌هم اول‌اند وجود دارند به‌طوری که

$$x^۲ = u^۲ - v^۲, \qquad y^۲ = ۲uv, \qquad z = u^۲ + v^۲$$

به‌ویژه، با فرض x فرد، (x, v, u) یک سه‌تایی فیثاغورسی اولیه است. بنابراین، اعداد متباین s و t وجود دارند به‌طوری که

$$x = s^۲ - t^۲, \qquad v = ۲st, \qquad u = s^۲ + t^۲$$

چون $y^۲ = ۲uv = ۴ust$ و t, s، و u دوبه‌دو نسبت به‌هم اول‌اند، پس همگی مربع کامل هستند (مسألهٔ ۳۳.۱ را ببینید). لذا اعداد صحیح a، b، c وجود دارند به‌طوری که $s = a^۲$، $t = b^۲$، و $u = c^۲$. چون $u = s^۲ + t^۲$، در نتیجه $a^۴ + b^۴ = c^۲$. ملاحظه می‌کنید که $c^۲ = u$ و $z = u^۲ + v^۲$؛ لذا $c < z$. بنابراین a، b، c یک جواب معادله اصلی است با $c < z$، که با مینیمال بودن z تناقض دارد. این برهان را کامل می‌کند.

قضیهٔ بعد را می‌توان با کاربرد استدلال مشابه اثبات کرد. برای شرح جزئیات مسألهٔ ۱۸.۸ را ببینید.

(۵.۸) قضیه. معادلهٔ $x^۴ - y^۴ = z^۲$ جواب صحیح غیرصفر ندارد.

توضیح. ۱. با توجه به (۴.۸)، به‌ازای هر $n \geq ۳$ آخرین قضیهٔ فرما ثابت می‌شود، هرگاه بتوانیم نشان دهیم که برای نماهای اول برقرار است. (مسألهٔ ۱۴.۸ را ببینید.)

۲. این برهان را برهانی با نزول نامتناهی خواندیم، زیرا این اصطلاحی است که فرما به‌کار برده است. این برهان در واقع برهانی است به‌وسیلهٔ استقرا، زیرا، آنچه که نشان داده شده این است که اگر معادله جوابی با z مثبت و کمتر از یک عدد صحیح w نداشته باشد، با $z = w$ نیز جواب ندارد. (این برهان نشان می‌دهد که اگر جوابی با $z = w$ می‌داشتیم جوابی با $z < w$ وجود خواهد داشت.)

در ۱۷۷۰، اویلر یک برهان ناقص از آخرین قضیهٔ فرما در حالت $n = ۳$ با استفاده از نزول نامتناهی ارائه داد. (برهان اویلر متکی به تجزیهٔ یکتای اعداد صحیح در هیئت اعداد جبری $Q(\sqrt{-۳})$ است، در باب این مبحث در فصل ۱۱ بحث خواهد شد.) حالت $n = ۵$ در ۱۸۲۵ توسط دیریکله و لژاندر بررسی شد. (هر دو اثبات نزول نامتناهی را به‌کار برده‌اند.) لامه[1] در ۱۸۳۹ حالت $n = ۷$ را ثابت کرد.

مهمترین پیشرفت سدهٔ نوزدهم در اثبات آخرین قضیهٔ فرما توسط ریاضیدان آلمانی ارنست ادوارت کومر[2] انجام شد. یک راه طبیعی ورود به آخرین قضیهٔ فرما بیان چندجمله‌یی $z^n - x^n$ به‌صورت حاصلضرب عاملهای خطی با ضرایب در یک توسیع مناسب از اعداد صحیح است. در ۱۸۴۷، لامه ادعا کرد که برهان کاملی بر پایهٔ این مفهوم دارد. ولی، در برهانش (به اشتباه) فرض کرده بود که تجزیهٔ یکتا به حاصلضرب اعداد اول در هیئتهای اعداد جبری عمومی‌تر برقرار است. (توضیحات انتهای فصل را ببینید.) تقریباً در همان زمان، کومر به‌منظور اصلاح تجزیهٔ یکتا، نظریه‌اش دربارهٔ ایده‌آلها را توسعه می‌داد، و توانست آخرین قضیهٔ فرما را برای تمام اعدادِ اول کوچکتر از ۱۰۰ جز برای ۳۷، ۵۹، و ۶۷ اثبات کند، و یک استدلال اساساً درست برای حالتهای باقیماندهٔ زیر ۱۰۰ را به اختصار به‌دست داد. ولی به دادن یک اثبات کامل توفیق نیافت.

برای یک بررسی تاریخی از آخرین قضیهٔ فرما و یک بحث مفصل از مفاهیم مربوط، کتابهای نوشته شده توسط H. Edwards و P. Ribenboim را که در مراجع آخر این فصل داده شده‌اند ببینید.

1. Lamé 2. Ernst Eduard Kummer

مجموعهای دو مربع

در تعدادی مسأله درکتاب حساب دیوفانتوس موضوع نمایش یک عدد صحیح مثبت به‌صورت مجموع دو مربع مطرح شده است. این مسائل توسط فرما در سدهٔ هفدهم بیرون کشیده شده بود. در نامه‌ای به مرسن در روز کریسمس ۱۶۴۰، فرما بدون اثبات اظهار داشت که هر عدد اول به‌صورت $4k+1$ نمایشی یکتا به‌صورت مجموع دو مربع دارد. او بعداً مشخص کرد که برای اثبات این حکم از روش نزول نامتناهی استفاده کرده است؛ در واقع، همین بود که موجب شد اویلر قضیه را بعد از گذشت بیش از یکصد سال در ۱۷۴۵ ثابت کند.

خصوصیات کامل از اینکه دقیقاً کدام اعداد صحیح مجموع دو مربع هستند در قضیهٔ ۹.۸ آمده است و عموماً به فرما نسبت داده شده است؛ اولین اثبات توسط اویلر در ۱۷۴۹ به چاپ رسید. به آسانی دیده می‌شود که هیچ عدد اول ــ در واقع، هیچ عدد صحیح، به‌صورت $4k+3$ چنین نمایشی ندارد. زیرا فرض کنیم $n=a^2+b^2$. چون مربع هر عدد صحیح با ۰ یا ۱ به پیمانهٔ ۴ همنهشت است، آشکار است که n همنهشت با ۰، ۱، یا ۲ به پیمانهٔ ۴ می‌شود. ولی یک قضیهٔ قویتر برقرار است.

(۶.۸) قضیه. فرض کنیم n بر یک عدد اول q به‌صورت $4k+3$ بخشپذیر است. (i) اگر $n=a^2+b^2$، آنگاه $q|a$ و $q|b$. (ii) اگر n مجموع دو مربع باشد، q با توان زوج در تجزیهٔ n ظاهر می‌شود. به‌ویژه، هیچ عدد اول به‌صورت $4k+3$ مجموع دو مربع نیست.

برهان. (i) اگر $q \nmid a$، آنگاه عددی چون s وجود دارد به‌طوری که $sa \equiv 1 \pmod{q}$. اما اگر $n=a^2+b^2$ و $q|n$، آنگاه $a^2+b^2 \equiv 0 \pmod{q}$. اگر در s^2 ضرب کنیم، داریم $(sb)^2 \equiv -1 \pmod{q}$، که غیرممکن است، زیرا -1 یک ماندهٔ درجهٔ دوم اعداد اول به‌صورت $4k+3$ نیست. لذا $q|a$، و به قرینه q عدد b را نیز می‌شمارد.

(ii) از قسمت (i) نتیجه می‌شود که اگر $a^2+b^2=n$، آنگاه $q^2|n$. با تقسیم $a^2+b^2=n$ بر q^2 داریم $n/q^2=(a/q)^2+(b/q)^2$. فرض کنیم $n=q^2n_1$؛ اگر $q|n_1$، آنگاه مانند بالا $q^2|n_1$. اگر به همین طریق ادامه دهیم، می‌بینیم که n دقیقاً بر تعداد زوجی از عاملهای q بخشپذیر است.

عکس قضیهٔ بالا نیز برقرار است: اگر هر عدد اول $4k+3$ که n را می‌شمارد با توان زوج در تجزیهٔ n به اعداد اول ظاهر شود، آنگاه می‌توان n را به‌صورت مجموع دو مربع نمایش داد. در برهان معمولی این مطلب یک اتحادی به‌کار می‌رود که به‌طور ضمنی توسط دیوفانتوس استفاده

شده بوده و در لیبر کوادراتورم فیبوناتچی آمده است (۱۲۲۵). از یک اتحاد کلی‌تر توسط برهمگوپتهٔ هندی در سدهٔ هفتم استفاده شده است.

(۷.۸) لم. اگر m و n هر کدام مجموع دو مربع باشند، حاصلضربشان نیز مجموع دو مربع است. به‌ویژه، اگر $m = a^۲ + b^۲$ و $n = c^۲ + d^۲$ آنگاه

$$mn = (ac + bd)^۲ + (ad - bc)^۲ = (ac - bd)^۲ + (ad + bc)^۲$$

توضیح. می‌توان حکم (۷.۸) را به آسانی (به استقرا) به حاصلضرب هر تعداد متناهی جمله، که هر جملهٔ آن مجموع دو مربع است، بسط داد.

حال فرض می‌کنیم هر عدد اول $۴k + ۳$ که n را می‌شمارد با توان زوج در تجزیهٔ n ظاهر شود. می‌نویسیم $n = c^۲m$، که در آن m بدون مربع است؛ لذا آشکار است که m بر هر عدد اولی به‌صورت $۴k + ۳$ بخشپذیر نیست. بنابراین، m به‌صورت $۲^t \prod p_i$ است که در آن t مساوی ۰ یا ۱ است و p_iها اعداد اولی به‌صورت $۴k + ۱$ هستند. ملاحظه می‌کنید که $۲ = ۱^۲ + ۱^۲$؛ لذا اگر بتوانیم ثابت کنیم که هر عدد اول $۴k + ۱$ مجموع دو مربع است، آنگاه کاربرد مکرر (۷.۸) ایجاب می‌کند که حاصلضرب $m = ۲^t \prod p_i$ نیز به‌صورت چنین مجموعی باشد. سرانجام، اگر $m = a^۲ + b^۲$، آنگاه $n = (ca)^۲ + (cb)^۲$، و لذا n قابل بیان‌به‌صورت مجموع دو مربع است.

لذا برهان قضیهٔ (۸.۸) فرما تکمیل می‌شود هرگاه نشان‌دهیم که هر عدد اول به‌صورت $۴k + ۱$ مجموع دو مربع است. در مسألهٔ ۴۸.۸، برهانی برای این قضیه ارائه می‌دهیم که اساساً همان برهان اویلر با استفاده از روش نزول نامتناهی است. ولی، استدلال زیر بسیار کوتاهتر است

(۸.۸) قضیه. هر عدد اول به‌صورت $۴k + ۱$ را می‌توان به‌صورت مجموع دو مربع متباین نوشت.

برهان. اگر p عدد اولی به‌صورت $۴k + ۱$ باشد، (۱۱.۵) ایجاب می‌کند که -۱ یک ماندهٔ درجهٔ دوم p باشد، لذا عدد صحیح s وجود دارد به‌طوری که $s^۲ \equiv -۱ \pmod p$. اعداد صحیح $sx - y$ را که در آن $۰ \le x, y < \sqrt{p}$ در نظر می‌گیریم. تعداد $[\sqrt{p}] + ۱$ انتخاب برای هر یک از x و y وجود دارد، و چون $([\sqrt{p}] + ۱)^۲ > (\sqrt{p})^۲ = p$، حداقل دو مقدار از $sx - y$ به پیمانه p همنهشت هستند، مثلاً $sx_۱ - y_۱ \equiv sx_۲ - y_۲ \pmod p$. فرض کنیم $x = x_۱ - x_۲$ و $y = y_۱ - y_۲$؛ در این‌صورت x و y هر دو صفر نیستند، زیرا جفتهای $x_۱$، $y_۱$ و $x_۲$، $y_۲$ متمایزند. آشکار است که $sx \equiv y \pmod p$ و لذا $s^۲x^۲ \equiv y^۲ \pmod p$، یعنی $-x^۲ \equiv y^۲ \pmod p$.

لذا $x^۲+y^۲$ مضربی از p است، و چون $۰<x^۲+y^۲<۲(\sqrt{p})^۲=۲p$، نتیجه می‌شود که $x^۲+y^۲=p$.

برای نشان دادن اینکه $(x,y)=۱$، توجه می‌کنیم که اگر $d|x$ و $d|y$، آنگاه $d^۲|x^۲+y^۲$ و چون $x^۲+y^۲$ اول است، در نتیجه $d^۲=۱$.

توضیح. اثباتی از این قضیه، بااستفاده ازکسرهای مسلسل در مسألهٔ ۱۰.۹، و برهان دیگری، بر مبنای وجود جواب برای معادلهٔ پل، را می‌توان در قضیهٔ ۲۰.۱۰ پیدا کرد. هر دو اثبات روشی برای یافتن مربعهای لازم برای نمایش عدد اول $۴k+۱$ به‌دست می‌دهند. باز هم اثبات دیگری، با استفاده از ویژگیهای اعداد اول گاوسی، در بحثِ قبل از (۱۲.۱۱) ارائه شده است.

مطالب قبل را در قضیهٔ زیر خلاصه می‌کنیم.

(۹.۸) قضیهٔ (فرما؛ اویلر، ۱۷۴۹). فرض کنیم n یک عدد صحیح مثبت باشد. در این‌صورت n مجموع دو مربع است اگر و تنها اگر هر عامل اول n به‌صورت $۴k+۳$ با توانهای زوج در تجزیهٔ n به اعداد اول ظاهر شود.

سرانجام، به مسألهٔ تعیین تعداد نمایشهای یک عدد صحیح به‌صورت مجموع دو مربع می‌پردازیم. در نامهٔ فرما به مرسن در روزکریسمس ۱۶۴۰، فرما تعداد نمایشهای p^m، که p عدد اولی به‌صورت $۴k+۱$ است، و به‌طورکلی‌تر، هر عدد صحیح n را که بتوان به‌صورت مجموع دو مربع نوشت، محاسبه کرده است.

(۱۰.۸) تعریف. فرض کنیم $N(n)$ معرف تعداد کل نمایشهای n به‌صورت مجموع دو مربع باشد. نمایشها متمایز به‌حساب می‌آیند حتی اگر تنها در علامت جمله‌ها یا در ترتیب جمله‌ها اختلاف داشته باشند.

مثلاً $N(۱۳)=۸$، زیرا $۱۳=(\pm۲)^۲+(\pm۳)^۲=(\pm۳)^۲+(\pm۲)^۲$. لذا با تغییر علامت و ترتیبِ اعدادِ به‌کار رفته هشت نمایش به‌دست می‌آوریم.

می‌توان اثبات قضیهٔ بعد را در مسأله‌های ۶۹.۸ و ۷۲.۸ جستجو کرد. این قضیه یک نتیجهٔ ساده از ویژگیهای اعداد صحیح گاوسی نیز هست و مجدداً در فصل ۱۱ اثبات خواهد شد.

(۱۱.۸) قضیه. فرض کنیم بتوان n را به‌صورت مجموع دو مربع نمایش داد، و می‌نویسیم $n=۲^a\prod p_i^{a_i}\prod q_i^{b_i}$، که در آن p_iها اعداد اول به‌صورت $۴k+۱$ و q_i ها اعداد اولِ $۴k+۳$

هستند (b_iها لزوماً زوج هستند). در این‌صورت

$$N(n) = ۴\prod(a_i + ۱)$$

(حاصلضربی که هیچ جمله‌ای نداشته باشد ۱ گرفته می‌شود.) به‌ویژه، اگر p عدد اولی به‌صورت $۴k + ۱$ باشد، آنگاه $N(p^m) = ۴(m + ۱)$.

یک بیان دیگر از $N(n)$ که منتسب به کارل گوستاو ژاکوبی (۱۸۰۴ـ۱۸۵۱) است، در قضیهٔ بعد می‌آید. برای یک برهان، مسأله‌های ۷۳.۸ تا ۷۵.۸ را ببینید.

(۱۲.۸) قضیه. فرض کنیم n یک عدد صحیح مثبت باشد، و فرض می‌کنیم $D_۱$ و $D_۳$، به‌ترتیب، نشانگر تعداد عوامل n به‌صورت $۴k + ۱$ و $۴k + ۳$ باشند، در این‌صورت

$$N(n) = ۴(D_۱ - D_۳)$$

توضیح. ۱. یک نمایش از n به‌صورت مجموع دو مربع که غیرصفرند و قدرمطلق متفاوت دارند، هشت نمایش متفاوت تولید می‌کند (با خودش)، که از تغییر ترتیب و علامت جمله‌ها به‌دست می‌آیند. اگر خود n مربع باشد، مثلاً، $n = m^۲$، می‌توانیم بنویسیم $n = m^۲ + ۰^۲$؛ این چهار نمایش زیر را تولید می‌کند؛ $m^۲ + ۰^۲$، $(-m)^۲ + ۰^۲$، $m^۲ + ۰^۲$، و $(-m)^۲ + ۰^۲$. اینها همگی مانند فرمول $N(n)$ متمایز به حساب می‌آیند. اگر $n = ۲m^۲$، چهار نمایش تولید می‌شود، یعنی $n = (\pm m)^۲ + (\pm m)^۲$.

۲. اگر p عدد اولی به‌صورت $۴k + ۱$ باشد، آنگاه $N(p) = ۸$. لذا، صرف‌نظر از ترتیب و علامت جمله‌ها، هر عدد اول به‌صورت $۴k + ۱$ را می‌توان به یک و تنها به یک طریق به‌صورت مجموع دو مربع نمایش داد.

تعداد نمایشهای اساساً متمایز (یعنی، نمایشهایی که از تغییر ترتیب و علامت جمله‌ها به‌دست نمی‌آیند) در مسألهٔ ۴۵.۸ مورد بحث قرار می‌گیرند.

مجموعهای دو مربعِ متباین

در این بخش، مسألهٔ نمایش یک عدد صحیح به‌صورت مجموع دو مربع متباین را بررسی می‌کنیم. با یک تعریف شروع می‌کنیم.

(۱۳.۸) تعریف. نمایش $n = a^۲ + b^۲$ یک نمایش مثبت خوانده می‌شود اگر a و b مثبت باشند. این نمایش اولیه است اگر a و b نسبت به هم اول باشند. (توجه کنید که لازم نیست یک نمایش اولیه یک نمایش مثبت باشد.)

اکثر قضیه‌های مربوط به نمایشهای اولیه از قضیهٔ بعد نتیجه می‌شوند. استدلال به‌کار رفته در برهان آن خیلی شبیه به برهان (۸.۸) است.

(۱۴.۸) قضیه. فرض می‌کنیم $n > ۱$. به‌ازای هر نمایش اولیه مثبتِ $n = a^۲ + b^۲$، یک جواب یکتای s از $x^۲ \equiv -۱ (\mathrm{mod}\, n)$ وجود دارد به‌طوری که $sa \equiv b (\mathrm{mod}\, n)$، و نمایشهای اولیهٔ مثبت متعارف با مقادیر متفاوت s متناظرند.

بعکس، یک جواب s از $x^۲ \equiv -۱ (\mathrm{mod}\, n)$ یک نمایش اولیهٔ مثبت یکتا مانند $n = a^۲ + b^۲$ تعیین می‌کند به‌طوری که $sa \equiv b (\mathrm{mod}\, n)$.

برهان. فرض کنیم $n = a^۲ + b^۲$، با a و b مثبت و $(a, b) = ۱$. در این‌صورت $(a, n) = ۱$، و لذا بنابر (۸.۲)، عدد یکای s به پیمانهٔ n وجود دارد به‌طوری که $sa \equiv b (\mathrm{mod}\, n)$. چون $a^۲ + b^۲ \equiv ۰ (\mathrm{mod}\, n)$، داریم $a^۲ \equiv -b^۲ \equiv -(sa)^۲ = -s^۲ a^۲ (\mathrm{mod}\, n)$، و با تقسیم بر $a^۲$ داریم $s^۲ \equiv -۱ (\mathrm{mod}\, n)$. حال، فرض می‌کنیم که نمایش $c^۲ + d^۲$ نیز متناظر با s باشد، یعنی $sc \equiv d (\mathrm{mod}\, n)$. چون $a^۲ + b^۲$ و $c^۲ + d^۲$ نمایشهای مثبت هستند، داریم $۱ \le a < \sqrt{n}$ و $۱ \le d < \sqrt{n}$؛ لذا $۱ \le ad < n$. با استدلالی مشابه $۱ \le bc < n$. چون $bc \equiv (sa)c \equiv ad (\mathrm{mod}\, n)$، در نتیجه $bc = ad$. لذا $b | ad$، و چون $(a, b) = ۱$، داریم $b | d$. به قرینه، همچنین داریم $d | b$. بنابراین $b = d$ و لذا $a = c$.

اکنون فرض می‌کنیم $s^۲ \equiv -۱ (\mathrm{mod}\, n)$، و مجموعهٔ جفتهای مرتب (j, k) را در نظر می‌گیریم به‌گونه‌ای که n مربع نباشد $۰ \le j, k < \sqrt{n}$ و اگر n مربع باشد $۰ \le j \le \sqrt{n}$ و $۰ \le k < \sqrt{n}$. در این‌صورت، به ترتیب تعداد $([\sqrt{n}] + ۱)^۲$ یا $(\sqrt{n} + ۱)\sqrt{n}$ این چنین جفتهای مرتب وجود دارند، و بنابراین بیش از n تا در هر مورد، حال $sj - k$ را وقتی که (j, k) این جفتهای مرتب را اختیار می‌کند در نظر می‌گیریم. چون هر عدد صحیح به پیمانهٔ n با یکی از اعداد $۰, ۱, ۲, \ldots, n - ۱$ همنهشت است، اعداد $sj - k$ همگی نمی‌توانند به پیمانهٔ n متمایز باشند. لذا دو جفت $(j_۱, k_۱)$ و $(j_۲, k_۲)$ وجود دارند به‌طوری که $sj_۱ - k_۱ \equiv sj_۲ - k_۲ (\mathrm{mod}\, n)$. قرار می‌دهیم $A = j_۱ - j_۲$ و $B = k_۱ - k_۲$؛ در این‌صورت $|A| \le \sqrt{n}$، $|B| < \sqrt{n}$، و $sA \equiv B (\mathrm{mod}\, n)$. چون جفتهای مرتب $(j_۱, k_۱)$ و $(j_۲, k_۲)$ متمایزند، نتیجه می‌شود که لااقل یکی از A یا B غیرصفر است؛ لذا $A^۲ + B^۲ \ge ۱$. همچنین، از $sA \equiv B (\mathrm{mod}\, n)$

نتیجه می‌شود که $s^۲A^۲ \equiv B^۲ (\mathrm{mod}\, n)$، یعنی، $-A^۲ \equiv B^۲ (\mathrm{mod}\, n)$. بنابراین $A^۲ + B^۲$ مضربی از n است. چون $A^۲ + B^۲$ مثبت و کوچکتر از $۲n$ است، داریم $A^۲ + B^۲ = n$.

حال، نشان می‌دهیم $(A, B) = ۱$. فرض کنیم $d = (A, B)$؛ چون $B \equiv sA (\mathrm{mod}\, n)$، درنتیجه $B/d \equiv sA/d (\mathrm{mod}\, n/d)$، ولذا $(B/d)^۲ \equiv s^۲(A/d)^۲ \equiv -(A/d)^۲ (\mathrm{mod}\, n/d)$. بنابراین، $n/d^۲ = (A/d)^۲ + (B/d)^۲ \equiv (A/d)^۲ - (A/d)^۲ = ۰ (\mathrm{mod}\, n/d)$. لذا n/d عدد $n/d^۲$ را می‌شمارد، و روشن است که، این حالت فقط وقتی اتفاق می‌افتد که $d = ۱$.

سرانجام، اگر A و B هردو مثبت یا هر دو منفی باشند، قرار می‌دهیم $a = |A|$ و $b = |B|$؛ در این‌صورت، مثلاً، اگر $A < ۰$ و $B > ۰$، داریم $sa = s(-A) = -sA \equiv -B = b (\mathrm{mod}\, n)$. در غیر این‌صورت، اگر یکی از A و B مثبت و دیگری منفی باشد، قرار می‌دهیم $a = |B|$ و $b = |A|$؛ لذا، مثلاً، اگر $A > ۰$ و $B < ۰$، $sa = -sB \equiv -s^۲A \equiv A = b (\mathrm{mod}\, n)$. در هر حالت، $a^۲ + b^۲$ یک نمایش اولیهٔ مثبت از n است به‌طوری که $sa \equiv b (\mathrm{mod}\, n)$.

فرما در ۱۶۴۰ بیان کرد، و اویلر در ۱۷۴۲ اثبات کرد، که اگر $n = a^۲ + b^۲$ با $(a, b) = ۱$، آنگاه تمام عاملهای اول فرد n به‌صورت $۴k + ۱$ هستند. این در قضیهٔ بعد، که شرح کاملی است از اعداد صحیح مثبت که نمایشهای اولیه دارند، می‌آید.

(۱۵.۸) قضیه. یک عدد صحیح مثبت n نمایشهای اولیهٔ مثبت به‌صورت مجموع دو مربع دارد اگر و تنها اگر n بر ۴ یا بر هر عدد اول به‌صورت $۴k + ۳$ بخشپذیر نباشد. لذا می‌توان n را به‌صورت مجموع دو مربع متباین نمایش داد اگر و تنها اگر $n = p_۱^{a_۱} \cdots p_r^{a_r}$ یا $n = ۲p_۱^{a_۱} \cdots p_r^{a_r}$، که در آنها هر p_i عدد اولی به‌صورت $۴k + ۱$ است.

برهان. اگر n نمایشهای اولیه داشته باشد، آنگاه بنابر (۱۴.۸)، همنهشتی $x^۲ \equiv -۱ (\mathrm{mod}\, n)$ حلپذیر است. اما اگر $۴|n$ و $x^۲ \equiv -۱ (\mathrm{mod}\, n)$، آنگاه بایستی $x^۲ \equiv -۱ (\mathrm{mod}\, ۴)$ حلپذیر باشد، که معلوم است که نیست؛ و اگر $q|n$، که q اول و $q \equiv ۳ (\mathrm{mod}\, ۴)$، آنگاه باید $x^۲ \equiv -۱ (\mathrm{mod}\, q)$ حلپذیر باشد، که با (۱۱.۵) تناقض دارد.

بعکس، اگر n بر ۴ یا بر عدد اولی به‌صورت $۴k + ۳$ بخشپذیر نباشد، آنگاه یا $n = p_۱^{a_۱} \cdots p_r^{p_r}$ یا $n = ۲p_۱^{a_۱} \cdots p_r^{a_r}$، که در آنها هر p_i عدد اولی به‌صورت $۴k + ۱$ است. بنابر (۱۱.۵)، به‌ازای هر i، $x^۲ \equiv -۱ (\mathrm{mod}\, p_i)$ حلپذیر است، و لذا (i.۴.۵) ایجاب می‌کند که $x^۲ \equiv -۱ (\mathrm{mod}\, p_i^{a_i})$ نیز دارای جواب باشد. بنابراین، $x^۲ \equiv -۱ (\mathrm{mod}\, n)$ نیز بنابر (۵.۵) حلپذیر است، و از (۱۴.۸) نتیجه می‌شود که می‌توان n را به‌صورت مجموع مربعهای متباین نمایش داد.

حال به بررسی تعداد نمایشهای اولیه‌ای که یک عدد صحیح مثبت می‌تواند داشته باشد می‌پردازیم. از قضیهٔ ۱۴.۸ نتیجه می‌شود که یک تناظر ۱ − ۱ بین جوابهای $x^2 \equiv -1 (\mathrm{mod}\, n)$ و نمایشهای اولیهٔ مثبت n وجود دارد، در شمارش نمایشهای اولیهٔ مثبت در (۱۴.۸)، نمایش $a^2 + b^2$ برای n متمایز از $b^2 + a^2$ در نظر گرفته شد، یعنی، این دو صورت از جوابهای متفاوت $x^2 \equiv -1 (\mathrm{mod}\, n)$ تولید می‌شوند. زیرا فرض کنیم جواب s نمایش $a^2 + b^2$ باشد؛ پس $sa \equiv b (\mathrm{mod}\, n)$. چون $-s$ نیز یک جواب است، $-s$ یک نمایش اولیهٔ مثبت یکتا مانند $c^2 + d^2$ را تعیین می‌کند به‌طوری که $(-s)c \equiv d (\mathrm{mod}\, n)$. چون

$$(-s)b \equiv (-s)sa = -s^2 a \equiv -(-1)a = a (\mathrm{mod}\, n)$$

از (۱۴.۸) نتیجه می‌شود که $-s$ متناظر با نمایش $a^2 + b^2$ است. لذا، یک جفت جوابهای s و $-s$ نمایشهای اولیهٔ مثبتی را تولید می‌کنند که تنها در ترتیب جمعوندها تفاوت دارند.

آشکار است که یک نمایش اولیهٔ مثبت مفروض با تعویض علامت (و نه ترتیب) جمله‌ها مجموعی از چهار نمایش اولیه تولید می‌کند:

$$n = a^2 + b^2 = a^2 + (-b)^2 = (-a)^2 + b^2 = (-a)^2 + (-b)^2$$

بنابراین، قضیهٔ زیر را داریم.

(۱۶.۸) قضیه. فرض کنیم $n > 1$، و فرض می‌کنیم S معرف تعداد جوابهای $x^2 \equiv -1 (\mathrm{mod}\, n)$ باشد. پس n دارای دقیقاً S نمایش اولیهٔ مثبت است، و تعداد کل نمایشهای اولیه $4S$ است.

مثال. (به قضیهٔ ۱۴.۸ مراجعه شود.) فرض کنیم $p = 13$؛ پس $x^2 \equiv -1 (\mathrm{mod}\, 13)$ دارای دو جواب ± 5، یعنی، ۵ و ۸ است. ریشهٔ ۵ با نمایش $2^2 + 3^2$ متناظر است، زیرا $2 \times 3 \equiv 5 (\mathrm{mod}\, 13)$، و با تغییر علامت جمله‌ها، نمایشهای $(2, -3)$، $(-2, 3)$، و $(-2, -3)$ را به‌دست می‌آوریم. چون $2 \times 2 \equiv 8 (\mathrm{mod}\, 13)$، ریشهٔ ۸ نمایش $3^2 + 2^2$ را معین می‌کند، و تغییرات این، نمایشهای $(3, -2)$، $(-3, 2)$، و $(3, -2)$ را ارائه می‌دهد. لذا همهٔ هشت تغییر به‌دست آمده از تغییر ترتیب و علامت جمله‌ها به حساب آمده‌اند.

قضیهٔ بعد پاسخی است به این سؤال که کدام اعداد صحیح را می‌توان با یک روش اساساً یکتا به‌صورت مجموع دو مربع متباین نمایش داد.

(۱۷.۸) قضیه. یک عدد صحیح $n > 2$ یک نمایش اولیه یکتا (صرف‌نظر از ترتیب و علامت

جمله‌ها) دارد اگر و تنها اگر $n = p^m$ یا $n = 2p^m$، که در آن p عدد اولی است به‌صورت $4k+1$ و $m \geq 1$.

برهان. چون به‌ازای یک نمایش مفروض، تغییر ترتیب و علامت جمله‌ها هشت تغییر پدید می‌آورد، لذا n دارای یک نمایش اساساً یکتا به‌صورت مجموع دو مربع متباین است اگر و تنها اگر n دارای مجموعی از هشت نمایش اولیه باشد. بنابر (۱۶.۸)، این مطلب زمانی رخ می‌دهد که $x^2 \equiv -1 \pmod{n}$ دقیقاً دو جواب داشته باشد. حالا حکم از (۵.۵) نتیجه می‌شود.

به‌طور کلی، می‌توانیم (۱۶.۸) را برای تعیین تعداد نمایشهای اولیه وقتی که چنین نمایشهایی وجود داشته باشند، به‌کار بریم.

(۱۸.۸) قضیه. فرض کنیم $n > 2$ دارای نمایشهای اولیه باشد؛ لذا بنابر (۱۵.۸)، $n = p_1^{a_1} \cdots p_r^{a_r}$ یا $n = 2p_1^{a_1} \cdots p_r^{a_r}$، که در آنها p_iها به‌صورت $4k+1$ هستند. در این‌صورت روی‌هم‌رفته n دارای دقیقاً 2^{r+2} نمایش اولیه و 2^{r-1} نمایش اساساً اولیهٔ متمایز (یعنی، نمایشهایی که تغییرات در ترتیب و علامت جمله‌ها نادیده گرفته می‌شوند.) است.

برهان. بنابر (۱۶.۸)، تعداد نمایشهای اولیهٔ n چهار برابر تعداد جوابهای $x^2 \equiv -1 \pmod{n}$ است. اگر n به یکی از دو صورت ارائه‌شده در قضیه باشد، از (۵.۵) نتیجه می‌شود که این همنهشتی 2^r جواب دارد؛ لذا n دارای دقیقاً $4 \times 2^r = 2^{r+2}$ نمایش اولیه است. چون هر نمایش اولیه شامل دو مربع غیرصفر متمایز است، لذا با تغییر ترتیب و علامت جمله‌ها هشت تغییر به‌دست می‌آید. بنابراین تعداد $2^{r+2}/8 = 2^{r-1}$ نمایش اساساً اولیهٔ متمایز از n وجود دارند.

سرانجام، توجه می‌کنیم که حتی اگر n دارای نمایشهای اولیه باشد، لزومی ندارد که تمام نمایشهای n اولیه باشند. در واقع، اگر $n > 2$ قابل نمایش به‌صورت مجموع دو مربع باشد، هر نمایش n اولیه است اگر و تنها اگر $n = p_1 p_2 \cdots p_r$ یا $n = 2p_1 p_2 \cdots p_r$، که در آنها هر p_i عدد اولی به‌صورت $4k+1$ است. (مسألهٔ ۶۰.۸ را ببینید.)

مجموعهای چهار مربع

با توجه به (۶.۸)، آشکار است که هر عدد صحیحی مجموع دو مربع نیست؛ به همین ترتیب نمی‌توان هر عدد صحیحی را به‌صورت مجموع سه مربع نوشت (بخش زیر را ببینید).

در ۱۶۲۱ باشه اظهار داشت (بدون اثبات) که هر عدد صحیح مثبت مجموع حداکثر چهار مربع است. در ۱۶۳۶، فرما در یادداشتی در نسخهٔ شخصی‌اش از کتاب دیوفانتوس ادعا کرد که

این مطلب را با استفاده از روش مورد علاقه‌اش، نزول نامتناهی، اثبات کرده است.

اویلر، برجسته‌ترین ریاضیدان سدهٔ هجدهم، اولین بار در ۱۷۳۰ به این مسأله علاقه‌مند شد و آثار مهمی در یک سری مقاله از ۱۷۴۷ تا ۱۷۵۱ به‌وجود آورد، اما قادر نشد که برهان کاملی ارائه دهد. ولی، او نقش اصلی را در حل نهایی این مسأله داشت، که توسط لژاندر و بر اساس کار اویلر در ۱۷۷۰ ارائه گردید، دو سال بعد اویلر یک اثبات زیبا از قضیهٔ چهار مربع ارائه داد، اثباتی که به اثبات قضیهٔ دو مربع برای اعدادِ اول به‌صورت $4k+1$ بسیار شبیه است. (مسأله ۹۵.۸ را ببینید.) اساس استدلالهای لاگرانژ و اویلر در یک اتحاد قابل توجه از اویلر نهاده شده است (اثبات قضیهٔ زیر را ببینید). در نامه‌ای به گولدباخ در ۱۷۴۸ این اتحاد برای یک اثبات به‌وسیلهٔ نزول نامتناهی مجاز شمرده شد.

(۱۹.۸) لم (اویلر). اگر هر کدام از m و n مجموع چهار مربع باشند، حاصلضربشان mn نیز مجموع چهار مربع است.

برهان. فرض کنیم $m=a^2+b^2+c^2+d^2$ و $n=A^2+B^2+C^2+D^2$. پس $mn=r^2+s^2+t^2+u^2$ که در آن $r=aA+bB+cC+dD$، $s=aB-bA+cD-dC$، $t=aC-bD-cA+dB$، و $u=aD+bC-cB-dA$. با ضرب هر طرف می‌توان صحت این مطلب را تحقیق کرد.

هر عدد صحیح $n>1$ حاصلضرب اعداد اول است. لذا با کاربرد مکرر (۱۹.۸)، نتیجه خواهد شد که هر عدد صحیح مثبت مجموع چهار مربع است (ممکن است بعضی از مربعها ۰ باشند) اگر بتوانیم نشان دهیم که هر عدد اول مجموع چهار مربع است. آشکار است که ۲ مساوی چنین مجموعی است، همان‌گونه که بنابر (۸.۸) هر عدد اول به‌صورت $4k+1$ نیز چنین است، لذا کافی است ثابت کنیم که هر عدد اول به‌صورت $4k+3$ مجموع چهار مربع است.

این همان روش رایجی است که در اثبات قضیهٔ چهار مربع به‌کار می‌رود (مسألهٔ ۹۵.۸ را ببینید). ولی، در اثباتی که ما ارائه می‌دهیم از فرمول اویلر استفاده نمی‌شود و با استدلال به‌کار رفته در اثبات قضیهٔ دو مربع (۸.۸) بسیار شبیه است. لِمهای زیر را لازم داریم:

(۲۰.۸) لم (**سیلوستر**[1]، **۱۸۴۷**). اگر $3m$ مجموع چهار مربع باشد، m نیز مجموع چهار مربع است.

برهان. فرض کنیم $3m=s^2+t^2+u^2+v^2$. چون هر مربع به پیمانهٔ ۳ با ۰ یا ۱

1. Sylvester

همنهشت است، حداقل یکی از s، t، u، و v مضرب ۳ است. لذا می‌توانیم فرض کنیم که مثلاً s مضرب ۳ است. چون $t^۲ + u^۲ + v^۲ \equiv ۰ \pmod ۳$، لذا با یک انتخاب مناسب از علامتهای t، u، و v همچنین می‌توانیم فرض کنیم که $t \equiv u \equiv v \pmod ۳$. با بسط دادن و ساده کردن، می‌بینیم که m مجموع مربعات اعداد صحیح زیر است: $(t+u+v)/۳$، $(s+u-v)/۳$، $(s-t+v)/۳$، و $(s+t-u)/۳$.

(۲۱.۸) لم. فرض کنیم n یک عدد صحیح عاری از مربع باشد. در این‌صورت اعداد صحیح a و b وجود دارند به‌طوری که $a^۲ + b^۲ \equiv -۱ \pmod n$.

برهان. ابتدا نشان می‌دهیم که قضیه برای وقتی که n عدد اولی مانند p باشد برقرار است. برای $p = ۲$ بدیهی است. برای pهایی به‌صورت $۴k + ۱$ از (۱۱.۵) نتیجه می‌شود که عدد a وجود دارد به‌طوری که $a^۲ \equiv -۱ \pmod p$؛ لذا می‌توانیم b را مساوی ۰ اختیارکنیم. ولی، برهان جداگانه‌ای ارائه می‌دهیم که برای همهٔ اعداد اول فرد کارساز است.

فرض‌کنیم $q = (p-۱)/۲$، و مجموعهٔ A را با $\{۰^۲, ۱^۲, \dots, q^۲\}$ تعریف می‌کنیم و مجموعهٔ B را با $\{-۱-q^۲, \dots, -۱-۱^۲, -۱-۰^۲\}$. هر دو عنصر A به پیمانهٔ p ناهمنهشت‌اند. زیرا فرض کنیم $۰ \le i < j \le q$. اگر $i^۲ \equiv j^۲ \pmod p$، آنگاه $p|j^۲ - i^۲$، و لذا $p|j+i$ یا $p|j-i$. اما این ممکن نیست، زیرا j و i نامنفی و از p کوچکترند. به همین‌دلیل، هر دو عنصر B نیز به پیمانهٔ p ناهمنهشت‌اند. لذا A و B هرکدام $(p+۱)/۲$ اعداد صحیح ناهمنهشت دارند. در نتیجه عنصر $a^۲$ از A و عنصر $-۱-b^۲$ از B وجود دارند به‌طوری‌که $a^۲ \equiv -۱-b^۲ \pmod p$، زیرا در غیر این‌صورت، خواهیم داشت $۲(p+۱)/۲ = p+۱$ به پیمانهٔ p ناهمنهشت‌اند، که غیرممکن است. با این انتخاب از a و b، داریم $a^۲ + b^۲ \equiv -۱ \pmod p$.

به آسانی می‌توان این قضیه را برای اعداد n به‌صورت $n = \prod p_i$، که p_iها اعداد اول متمایزند، بسط داد. به‌ازای هر p_i، اعداد a_i و b_i را انتخاب می‌کنیم به‌طوری که $a_i^۲ + b_i^۲ \equiv -۱ \pmod{p_i}$. قضیهٔ باقیماندهٔ چینی را برای یافتن اعداد a و b به‌طوری که به‌ازای هر i، $a \equiv a_i \pmod{p_i}$ و $b \equiv b_i \pmod{p_i}$ به‌کار می‌بریم. لذا به‌ازای هر i، $a^۲ + b^۲ \equiv -۱ \pmod{p_i}$، و بنابراین $a^۲ + b^۲ \equiv -۱ \pmod n$.

اکنون آماده‌ایم تا قضیهٔ چهار مربع را ثابت کنیم. فرض می‌کنیم n یک عدد صحیح مثبت باشد. می‌توان n را به‌صورت $n = k^۲m$ بیان کرد، که در آن m عاری از مربع است. اگر بتوانیم ثابت کنیم که m مجموع چهار مربع است، مثلاً $m = s^۲ + t^۲ + u^۲ + v^۲$، آنگاه نتیجه می‌شود که $n = (ks)^۲ + (kt)^۲ + (ku)^۲ + (kv)^۲$، که مجموع چهار مربع است.

(۲۲.۸) قضیهٔ (لاگرانژ، ۱۷۷۰؛ اویلر، ۱۷۷۲). هر عدد صحیح مثبت مجموع چهار مربع است.

برهان. با توجه به نکات بالا، کافی است نشان دهیم که اگر عدد صحیح مثبت n عاری از مربع باشد، n مجموع چهار مربع است؛ روشن است که می‌توانیم $n > ۱$ را اختیار کنیم. فرض کنیم a و b اعداد صحیحی باشند که $a^۲ + b^۲ \equiv -۱ (\mathrm{mod}\, n)$. همهٔ زوجهای مرتب $(as + bt - u, bs - at - v)$ را در نظر می‌گیریم، که در آن s، t، u، و v همهٔ اعداد صحیح از ۰ تا $[\sqrt{n}]$ را اختیار می‌کنند. تعداد $(۱ + [\sqrt{n}])^۴ > n^۲$ انتخاب برای s، t، u، v وجود دارند. اما چون تنها $n^۲$ جفت مرتبِ متمایز به پیمانهٔ n وجود دارند، لذا چهارتاییهای مرتب متمایز $(s_۱, t_۱, u_۱, v_۱)$ و $(s_۲, t_۲, u_۲, v_۲)$ که همهٔ درایه‌های آنها در بازهٔ از ۰ تا $\sqrt{n}$ واقع‌اند، وجود دارند به‌طوری که $as_۱ + bt_۱ - u_۱ \equiv as_۲ + bt_۲ - u_۲ (\mathrm{mod}\, n)$ و $bs_۱ - at_۱ - v_۱ \equiv bs_۲ - at_۲ - u_۲ (\mathrm{mod}\, n)$.

فرض کنیم $s = s_۱ - s_۲$، $t = t_۱ - t_۲$، $u = u_۱ - u_۲$، و $v = v_۱ - v_۲$. پس $as + bt \equiv u (\mathrm{mod}\, n)$ و $bs - at \equiv v (\mathrm{mod}\, n)$. بنابراین

$$(as + bt)^۲ + (bt - as)^۲ \equiv u^۲ + v^۲ (\mathrm{mod}\, n)$$

اما $(as+bt)^۲ + (bt-as)^۲ = (s^۲ + t^۲)(a^۲ + b^۲)$، و چون $a^۲ + b^۲ \equiv -۱ (\mathrm{mod}\, n)$، و از اینجا نتیجه می‌شود که $-(s^۲ - t^۲) \equiv u^۲ + v^۲ (\mathrm{mod}\, n)$، لذا عددی مانند k وجود دارد به‌طوری که $s^۲ + t^۲ + u^۲ + v^۲ = kn$. آشکار است که s، t، u، و v همگی نابیشتر از $[\sqrt{n}]$ هستند. همگی ۰ نیستند، زیرا چهارتاییهای مرتب $(s_۱, t_۱, u_۱, v_۱)$ و $(s_۲, t_۲, u_۲, v_۲)$ متمایزند. همچنین، $s^۲ + t^۲ + u^۲ + v^۲ < ۴[\sqrt{n}]^۲$ و لذا k مساوی ۱، ۲، یا ۳ است.

اگر $k = ۱$ کار تمام است. اگر $k = ۳$، آنگاه بنابر (۲۰.۸)، خود n مجموع چهار مربع است. حال فرض کنیم $k = ۲$؛ چون $۲n$ زوج است، یا هیچ‌کدام، یا دو تا، یا چهار تا از اعداد s، t، u و v باید زوج باشند. اگر دقیقاً دو تا زوج باشند، می‌توانیم فرض کنیم که آنها s و t هستند. لذا در هر حالت، $s \pm t$ و $u \pm v$ زوج هستند، و لذا n مجموع مربعات اعداد زیر است $(s+t)/۲$، $(s-t)/۲$، $(u+v)/۲$، و $(u-v)/۲$، که برهان را کامل می‌کند.

چنین نیست که هر عدد صحیح مثبت ــ یا حتی هر عدد صحیحِ مثبتِ به اندازهٔ کافی بزرگ ــ مجموع چهار مربع غیرصفر است. در واقع، عدد صحیح مثبت n مجموع چهار مربع غیرصفر است اگر و تنها اگر n مساوی اعداد زیر نباشد، ۱، ۳، ۵، ۹، ۱۱، ۱۷، ۲۹، ۴۱، $۴^k \times ۲$، $۴^k \times ۶$، $۴^k \times ۱۴$. به‌ویژه، بی‌نهایت عدد زوج، و تنها تعداد متناهی عدد فرد وجود دارند که

نمی‌توان آنها را به‌صورت مجموع چهار مربع غیرصفر نمایش داد. ولی، قضیهٔ زیر برقرار است. (برای یک برهان، مسألهٔ ۸.۸۰ را ببینید.)

(۲۳.۸) قضیه. هر عدد صحیح مثبت به اندازهٔ کافی بزرگ مجموع پنج مربع غیرصفر است.

توضیح. تنها اعداد صحیح مثبتی که مجموع پنج مربع غیرصفر نیستند عبارت‌اند از ۱، ۲، ۳، ۴، ۶، ۷، ۹، ۱۰، ۱۲، ۱۵، ۱۸، و ۳۳.

سرانجام، قضیه زیر از ژاکوبی را داریم.

(۲۴.۸) قضیه. فرض کنیم $M(n)$ معرف تعداد کل نمایشهای n به‌صورت مجموع چهار مربع باشد (ازجمله تغییر در ترتیب یا علامتهای جمله‌ها). در این‌صورت $M(n)$ برابر است‌با ۸ برابر مجموع مقسوم‌علیه‌های مثبت n که بر ۴ بخشپذیر نیستند.

مجموعهای سه مربع

حاصلضرب دو عدد که هرکدام مجموع سه مربع هستند لزوماً مجموع سه مربع نیست (مسألهٔ ۸۲.۸ را ببینید). لذا برای تعیین اینکه چه اعدادی قابل نمایش به‌صورت مجموع سه مربع هستند، نمی‌توانیم از یک اتحاد شبیه اتحادهای (۷.۸) یا (۱۹.۸) استفاده کنیم. بنابراین مسألهٔ مربوط به اینکه چه اعداد صحیحی مجموع سه مربع هستند بسیار دشوارتر از مسائل مشابه برای دو مربع و چهار مربع است.

یک بررسی آسان از طریق همنهشتی نشان می‌دهد که هر عدد به‌صورت $8k+7$، و به‌طورکلی، هر عدد به‌صورت $4^m(8k+7)$ را نمی‌توان به‌صورت مجموع سه مربع نمایش داد (مسألهٔ ۸۳.۸ را ببینید). در واقع، این اعداد تنها اعدادی هستند که نمی‌توانند به‌صورت مجموع سه مربع نوشته شوند. این مطلب اولین بار توسط فرما، شاید حدود ۱۶۳۰، مورد توجه قرار گرفت. در ۱۷۹۸، لژاندر یک برهان پیچیده و قدری ناکامل ارائه داد. گاوس نخستین کسی بود که یک برهان کامل، همراه با فرمولی برای تعداد نمایشها، در تحقیقات حسابی ارائه داد، اما استدلال مشکل است و نظریه صورتهای درجهٔ دوم گاوس در آن به‌کار می‌رود. شرح آن از این قرار است.

(۲۵.۸) قضیهٔ (لژاندر، گاوس). یک عدد صحیح مثبت مجموع سه مربع است اگر و تنها اگر به‌صورت $4^m(8k+7)$ نباشد.

توضیح. با کاربرد برهانی شبیه به برهان (۸.۸)، اثبات اینکه هر عدد اول به‌صورت $8k+1$ یا $8k+3$ به‌صورت $2a^2+b^2$ است مشکل نیست (مسألهٔ ۹۰.۸ را ببینید). به‌ویژه، هر چنین عدد اولی مجموع سه مربع است.

مسألهٔ ورینگ

کارهای لاگرانژ در ۱۷۷۰ نشان می‌دهد که هر عدد صحیح مثبت مجموع چهار مربع است. در همان سال، ورینگ یک حدسیهٔ جامعتر ارائه داد: هر عدد مجموع ۴ مربع، ۹ مکعب، ۱۹ توان چهارم، و به‌طور کلی، به‌ازای هر عدد صحیح مثبت k، مجموع تعداد ثابتی از توان kام است. مطلب زیر بیان دقیق حدسیهٔ ورینگ است.

(۲۶.۸) مسألهٔ ورینگ. به‌ازای هر $k \geq ۲$، عدد صحیح مثبت s (که تنها به k بستگی دارد) وجود دارد به‌طوری که می‌توان هر عدد صحیح مثبت را به‌صورت مجموع s توان kام نامنفی بیان کرد.

در واقع، دو سؤال در مورد مسألهٔ ورینگ وجود دارد. اولی آن است که آیا به‌ازای هر $k \geq ۲$ یک عدد s وجود دارد؟ در اواخر سدهٔ نوزدهم، معلوم شد که برای $k \leq ۸$ جواب این سؤال مثبت است. در ۱۹۰۹ این سؤال توسط داوید هیلبرت کاملاً جواب داده شد؛ ولی، برهان هیلبرت یک استدلال وجودی است و هیچ روشی را برای تعیین s به‌ازای یک مقدار خاص k ارائه نمی‌دهد.

دومین سؤال مربوط به یافتن کوچکترین مقدار s به‌ازای یک kی مفروض است. به‌ازای $k \geq ۲$، $g(k)$ را کوچکترین عدد s تعریف می‌کنیم به‌طوری که هر عدد صحیح مثبت مجموع s توان kام نامنفی باشد. برای $k = ۲$، به آسانی دیده می‌شود که $g(۲) = ۴$: قضیهٔ لاگرانژ ایجاب می‌کند که به‌ازای هر عدد صحیح بیشتر از چهار مربع مورد نیاز نیست، و از (۲۵.۸) نتیجه می‌شود که هر عدد به‌صورت $۸k + ۷$ دقیقاً چهار مربع لازم دارد.

برای $k > ۲$، مسأله خیلی دشوارتر است. برای تقریباً یکصد سال، پیشرفت چندانی حاصل نشد. در ۱۸۵۹، لیوویل[1] ثابت کرد که $g(۴) \leq ۵۳$، و در ۱۹۰۹ ویفریش[2] نشان داد که $g(۳) = ۹$. این مسأله توجه بسیاری از ریاضیدانان مشهور، از جمله هاردی، لیتلوود[3]، و وینوگرادوف را به خود جلب کرد. اکنون مشخص شده است که $g(۴) = ۱۹$ (این مطلب سرانجام در ۱۹۸۶ ثابت شد) و $g(۵) = ۳۷$ (در ۱۹۶۴ به اثبات رسید). جز در موارد $k = ۲$ و $k = ۳$، در اثباتها روشهای تحلیلی به‌کار می‌روند و به نظریهٔ توابع یک متغیر مختلط استناد می‌شوند.

در ۱۷۷۲، یوهان اویلر[4] (فرزند لئونهارت اویلر مشهور) ملاحظه کرد که به‌ازای هر $k \geq ۲$، $g(k) \geq ۲^k + [(۳/۲)^k] - ۲$ (مسألهٔ ۹۶.۸ را ببینید). برای اثبات این نامساوی کافی است که عدد صحیح مثبتی مانند n بیابیم به‌طوری که n به‌صورت مجموع s توان kام باشد (در اینجا $s = ۲^k + [(۳/۲)^k] - ۲$). به تعبیری، این بدترین حالت ممکن است، و حدس زده شده است ــ و

1. Liouville 2. Wieferich 3. Littlewood 4. Johannes Euler

با احتمال زیاد درست است ــ که در واقع به‌ازای هر مقدار k، $g(k) = 2^k + [(3/2)^k] - 2$. اکنون معلوم شده است که این تساوی برای هر $k \leq 471600000$ و نیز برای kهای به اندازه کافی بزرگ، برقرار است.

مسأله‌ها و راه‌حلها

توضیح. مسألهٔ زیر بسیار قدیمی است. روایت شده است که دربارهٔ دیوفانتوس است. اما این معادلهٔ خطی ساده ابداً نمونه‌ای از کار دیوفانتوس نیست.

۱.۸ دورهٔ طفولیت او ۱/۶ عمرش طول کشید، ریشش پس از ۱/۱۲ دیگر از عمرش روئید. پس از ۱/۷ دیگر از عمرش ازدواج کرد، و پسرش ۵ سال بعد متولد شد؛ پسر به اندازهٔ نصف عمر پدر زندگی کرد، و پدر چهار سال بعد از پسرش در گذشت. وقتی فوت کرد چند ساله بود؟

حل. اگر تا x سالگی زندگی کرده باشد، داریم

$$(1/6)x + (1/12)x + (1/7)x + 5 + (1/2)x + 4 = x$$

لذا $x = 84$.

معادلهٔ $x^2 + y^2 = z^2$

۲.۸ همهٔ سه‌تاییهای فیثاغورسی (x, y, z) با $40 \leq z \leq 50$ را پیدا کنید.

حل. ابتدا همهٔ سه‌تاییهای اولیه را با بیان z به‌صورت $a^2 + b^2$، که در آن $(a, b) = 1$ و یکی از a و b زوج و دیگری فرد است، فهرست می‌کنیم. تساوی $41 = 16 + 25$ سه‌تایی $(9, 40, 41)$ را تولید می‌کند؛ هیچ عدد فرد دیگری در حوزهٔ مقادیر با مجموع دو مربع متباین نیست.

به‌طور کلی، سعی می‌کنیم z را به‌صورت $z = tz_1$ بیان کنیم، که در آن z_1 وتر یک مثلث اولیه است. به‌ازای $z = 40$، $z_1 = 5$ را اختیار می‌کنیم، که سه‌تایی $(24, 32, 40)$ را به‌دست می‌دهد. به‌ازای $z = 45$، مجدداً $z_1 = 5$ را انتخاب می‌کنیم، که سه‌تایی $(27, 36, 45)$ را ارائه می‌دهد. برای $z = 50$، می‌توانیم $z_1 = 5$ یا $z_1 = 25$ را اختیار کنیم که سه‌تاییهای $(30, 40, 50)$ و $(14, 48, 50)$ را تولید می‌کنند.

۳.۸ همهٔ مثلثهای فیثاغورسی را که یک ضلع آنها ۱۸ است پیدا کنید.

حل. با استفاده از (۲.۸)، ابتدا مثلثهای فیثاغورسی اولیه‌ای را پیدا می‌کنیم که دارای ضلعی باشند که ۱۸ را بشمارد. روشن است که نه ۱ و نه ۲ ضلع یک مثلث فیثاغورسی نیستند، و ۳ ضلع

تنها مثلث $(۳,۴,۵)$ است؛ لذا ۱۸ ضلع یک مثلث $(۱۸,۲۴,۳۰)$ است. چون ۶ زوج است، برای آنکه ضلع یک مثلث فیثاغورسی اولیه برابر ۶ باشد، بایستی ۶ به‌صورت $۲ab$ باشد، که یکی از a، b زوج و دیگری فرد است؛ روشن است که این ویژگی نمی‌تواند برقرار شود. با استدلالی مشابه، ضلع یک مثلث اولیه برابر ۱۸ نیست. سرانجام، ۹ را به‌صورت $a^۲-b^۲$ می‌نویسیم (۹ نمی‌تواند به‌صورت $a^۲+b^۲$ یا $۲ab$ باشد)؛ لذا $a=۵$ و $b=۴$. از آنجا مثلث $(۹,۴۰,۴۱)$ به‌دست می‌آید؛ اگر در ۲ ضرب کنیم مثلث $(۱۸,۸۰,۸۲)$ حاصل می‌شود.

۴.۸ همهٔ سه‌تاییهای فیثاغورسی (x,y,z) با $x<y$ و $z=۴۸۱$ را به‌دست آورید. کدام‌یک از این سه‌تاییها اولیه هستند؟ (راهنمایی: ۴۸۱ را تجزیه کنید، و از (۷.۸) برای نوشتن ۴۸۱ به‌صورت مجموع دو مربع استفاده کنید.)

حل. چون $۴۸۱=۱۳\times ۳۷=(۳^۲+۲^۲)(۶^۲+۱^۲)=۲۰^۲+۹^۲=۱۶^۲+۱۵^۲$، می‌توانیم در (۲.۸)(الف) قرار دهیم $a=۲۰$، $b=۹$ و سه‌تایی اولیهٔ $(۳۱۹,۳۶۰,۴۸۱)$ را به‌دست آوریم، و (ب) قرار دهیم $a=۱۶$، $b=۱۵$ و سه‌تایی اولیهٔ $(۳۱,۴۸۰,۴۸۱)$ را به‌دست آوریم. اکنون سه‌تاییهای (kx,ky,kz) را در نظر می‌گیریم که در آن $kz=۴۸۱$، $k>۱$، و (x,y,z) اولیه است. لذا k مساوی ۱۳ یا ۳۷ است. اگر $k=۱۳$، آنگاه $a^۲+b^۲=۳۷$ ایجاب می‌کند $a=۶$ و $b=۱$، که سه‌تایی اولیه $(۳۵,۱۲,۳۷)$ و لذا با ضرب آن در ۱۳، سه‌تایی غیر اولیهٔ $(۱۵۶,۴۵۵,۴۸۱)$ به‌دست می‌آید (برای برقراری $x<y$، x و y را عوض می‌کنیم). با روشی مشابه، برای $k=۳۷$، داریم $a^۲+b^۲=۱۳$، و لذا $a=۳$، $b=۲$. از آنجا $(۵,۱۲,۱۳)$، و با ضرب آن در ۳۷، سه‌تایی غیر اولیهٔ $(۱۸۵,۴۴۴,۴۸۱)$ حاصل می‌شود.

۵.۸ قضیهٔ ۲.۸ تضمین می‌کند که هر سه‌تایی فیثاغورسی اولیه به‌صورت $x=a^۲-b^۲$، $y=۲ab$، $z=a^۲+b^۲$ است، که در آن $(a,b)=۱$، اگر a و b لزوماً نسبت به هم اول نباشند، آیا هر سه‌تایی فیثاغورسی بدین‌صورت است؟

حل. خیر، مثلاً، سه‌تایی $(۹,۱۲,۱۵)$ به این‌صورت نیست، زیرا نمی‌توان ۱۵ را به‌صورت مجموع دو مربع نوشت.

مسألهٔ زیر آن سه‌تاییهای فیثاغورسی را معرفی می‌کند که می‌توان از فرمولهای (۲.۸) به‌دست آورد که a و b لزوماً نسبت به هم اول نیستند یا یکی زوج و دیگری فرد نیست.

◁ **۶.۸** فرض کنید $r=a^۲-b^۲$، $s=۲ab$، و $t=a^۲+b^۲$، که در آن a و b اعداد صحیح مثبت هستند با $a>b$. فرض کنید $d=(a,b)$ و قرار دهید $A=a/d$، $B=b/d$.

(الف) اگر دقیقاً یکی از A و B فرد باشد، ثابت کنید که سه‌تایی فیثاغورسی (r,s,t) به‌صورت $(d^۲x, d^۲y, d^۲z)$ است، که در آن (x,y,z) یک سه‌تایی اولیه با y زوج است.

(ب) اگر A و B هر دو فرد باشند، ثابت کنید که (r,s,t) به‌صورت $(۲d^۲x, ۲d^۲y, ۲d^۲z)$ است که در آن (x,y,z) یک سه‌تایی اولیه با x زوج است.

حل. (الف) به آسانی تحقیق می‌شود که (r,s,t) یک سه‌تایی فیثاغورسی است. چون یکی از A و B زوج و دیگری فرد است و $(A,B)=۱$، (۲.۸) ایجاب می‌کند که $(A^۲-B^۲, ۲AB, A^۲+B^۲)$ یک سه‌تایی اولیه باشد، و روشن است که $r = d^۲(A^۲ - B^۲)$، $s = d^۲(۲AB)$، $t = d^۲(A^۲ + B^۲)$.

(ب) چون A و B هر دو فردند، $x = (A+B)/۲$ و $y = (A-B)/۲$ اعداد صحیح‌اند. در این‌صورت $(x,y) = ۱$، زیرا اگر عدد اول p اعداد x, y را بشمارد، آنگاه $p|x+y$ و $p|x-y$، یعنی $p|A$ $p|B$، که با $(A,B) = ۱$ تناقض دارد. همچنین، یکی از x و y زوج دیگری فرد است، زیرا $x+y = A$ و A فرد است.

چون $(x,y) = ۱$ و یکی از x و y زوج و دیگری فرد است، (۲.۸) ایجاب می‌کند که $(۲xy, x^۲ - y^۲, x^۲ + y^۲)$ یک سه‌تایی اولیه باشد (عنصر زوج را در ابتدا ثبت کردیم). ملاحظه می‌کنید که $۴xy = A^۲ - B^۲$؛ از آنجا که $A = x + y$ و $B = x - y$، نیز داریم $۲AB = ۲(x^۲-y^۲)$ و $A^۲+B^۲ = ۲(x^۲+y^۲)$. لذا $r = d^۲(A^۲-B^۲) = ۲d^۲(۲xy)$، $s = d^۲(۲AB) = ۲d^۲(x^۲ - y^۲)$، و $t = d^۲(A^۲ + B^۲) = ۲d^۲(x^۲ + y^۲)$.

۷.۸ فرض کنید (x,y,z) یک سه‌تایی فیثاغورسی اولیه باشد. (الف)، ثابت کنید یکی از x یا y بر سه بخشپذیر است (ب) یکی از x، y، یا z مضرب ۵ است.

حل. (الف) به آسانی دیده می‌شود که هر مربع به پیمانه ۳ همنهشت با ۰ یا ۱ است. لذا اگر هیچ‌یک از x و y مضرب ۳ نباشد، آنگاه $x^۲ + y^۲ = ۲ \pmod ۳$؛ به‌ویژه، $x^۲ + y^۲$ نمی‌تواند یک مربع کامل باشد.

(ب) هر مربع به پیمانه ۵ با ۰، ۱، یا ۱− همنهشت است. لذا اگر نه x و نه y بر ۵ بخشپذیر نباشند، آنگاه $x^۲ + y^۲$ به پیمانهٔ ۵ با ۰، ۲، یا ۲− همنهشت است. اما اگر $x^۲ + y^۲ \equiv \pm ۲ \pmod ۵$، آنگاه $x^۲ + y^۲$ نمی‌تواند یک مربع کامل باشد. لذا $x^۲ + y^۲ \equiv ۰ \pmod ۵$، و از آنجا یکی از x و y (یا هر دو) مضرب ۵ است یا z بر ۵ بخشپذیر است.

۸.۸ اگر (x,y,z) یک سه‌تایی فیثاغورسی باشد، ثابت کنید $۶۰|xyz$.

حل. بنابر مسألهٔ ۷.۸، xyz بر ۳ و ۵ بخشپذیر است. کافی است نشان دهیم که xyz مضرب ۴ است. روشن است که فقط لازم است سه‌تاییهای اولیه را در نظر بگیریم. بنابر (۲.۸)، یکی از x و y، مثلاً، y زوج است، و لذا y به‌صورت $y = ۲ab$ است، که در آن یکی از a و b زوج و دیگری فرد است. لذا $۴|y$.

۹.۸ فرض کنید $n \geq ۳$ ثابت کنید که سه‌تایی فیثاغورسیی وجود دارد که یکی از عناصر آن n است.

حل. ابتدا فرض می‌کنیم $n \geq ۳$ فرد باشد، مثلاً $n = ۲k + ۱$. در این‌صورت $n = (k+۱)^۲ - k^۲$، با فرض $a = k+۱$ و $b = k$ در (۲.۸)، می‌بینیم که n یک عنصر از سه‌تایی اولیهٔ $(a^۲ - b^۲, ۲ab, a^۲ + b^۲)$ است.

حال، فرض می‌کنیم n زوج و به‌صورت $n = ۲^t m$ باشد، که m فرد است. اگر $t \geq ۲$، آنگاه در (۲.۸) قرار می‌دهیم $a = ۲^{t-۱}m$ و $b = ۱$. لذا n عنصری از سه‌تایی اولیهٔ $(a^۲ - b^۲, ۲ab, a^۲ + b^۲)$ است. اگر $t = ۱$، آنگاه $n = ۲m$. چون m فرد است، یک سه‌تایی اولیهٔ (x, y, z) با $x = m$ وجود دارد. بنابراین n عنصر اول $(۲x, ۲y, ۲z)$ است.

۱۰.۸ (الف) ثابت کنید $(۳, ۴, ۵)$ تنها سه‌تایی فیثاغورسی اولیه است که عناصرش تصاعد عددی هستند.

(ب) ثابت کنید که $(۳k, ۴k, ۵k)$ با $k \geq ۱$ تنها سه‌تاییهای فیثاغورسی هستند که عناصرشان تصاعد عددی تشکیل می‌دهند.

حل. (الف) (ب). فرض کنیم x و y و z یک سه‌تایی باشد که عناصرشان به‌صورت تصاعد عددی هستند. در این‌صورت اعداد صحیح a و k وجود دارند به‌طوری که $x = a - k$، $y = a$، و $z = a + k$. از معادلهٔ $x^۲ + y^۲ = z^۲$ داریم $a^۲ = ۴ak$، و لذا $a = ۴k$، بنابراین، سه‌تایی به‌صورت $(۳k, ۴k, ۵k)$ است. اگر سه‌تایی اولیه باشد، بایستی $k = ۱$.

۱۱.۸ اثبات یا رد کنید: بی‌نهایت سه‌تایی فیثاغورسی اولیهٔ (x, y, z) وجود دارد که y یک عدد زوج و مربع کامل است.

حل. درست است. استدلال مسألهٔ ۹.۸ نشان می‌دهد که به‌ازای هر چنین y، سه‌تایی فیثاغورسی اولیه (x, y, z) وجود دارد، زیرا y بر ۴ بخشپذیر است.

۱۲.۸ همهٔ مثلثهای قائم‌الزاویه‌ای را تعیین کنید که اضلاع آنها صحیح و عدد مساحتشان با عدد

محیطشان برابر باشند.

حل. هر سه‌تایی فیثاغورسی، با فرض اینکه k، a، b اعداد صحیح مثبت باشند به‌صورت $(k(a^۲-b^۲), k(۲ab), k(a^۲+b^۲))$ است. با توجه به شرط مسأله داریم $xy/۲ = x+y+z$، یعنی، $k^۲ab(a^۲-b^۲) = k(۲a^۲+۲ab)$، یا هم‌ارز با آن $kb(a-b) = ۲$. اگر $k=۱$، آنگاه با فرض $b=۱$، داریم $a=۳$، و لذا سه‌تایی $(۸,۶,۱۰)$ به‌دست می‌آید؛ با فرض $b=۲$، داریم $a=۳$، که $(۵,۱۲,۱۳)$ حاصل می‌شود. اگر $k=۲$، آنگاه $b(a-b)=۱$، و لذا $b=۱$، $a=۲$، که $(۶,۸,۱۰)$ حاصل می‌شود. لذا صرف‌نظر از جابه‌جایی x و y، تنها جوابها عبارت‌اند از $(۶,۸,۱۰)$ و $(۵,۱۲,۱۳)$.

◁ **۱۳.۸** فرض کنید (x,y,z) یک سه‌تایی فیثاغورسی اولیه باشد. آیا $x-y$ می‌تواند مربعی بزرگتر از ۱ باشد؟

حل. فرض کنیم y زوج باشد؛ در این‌صورت $x=a^۲-b^۲$ و $y=۲ab$، که در آن یکی از a و b زوج و دیگری فرد و $(a,b)=۱$. داریم $x-y=(a-b)^۲-۲b^۲$. لذا می‌خواهیم که a و b و c چنان باشند که $(a-b)^۲-۲b^۲=c^۲$؛ یعنی، $(a-b)^۲-c^۲=۲b^۲$، یا $(a-b-c)(a-b+c)=۲b^۲$). برای یافتن جوابها، قرار می‌دهیم $a-b-c=۲$ و $a-b+c=b^۲$؛ از تفریق این دو رابطه داریم $۲c=b^۲-۲$. لذا اگر b را زوج اختیار کنیم a به‌دست می‌آید. مثلاً $b=۴$ ایجاب می‌کند $c=۷$، لذا $a=c+b+۲=۱۳$؛ بنابراین، $x=۱۵۳$، $y=۱۰۴$، و $x-y=۷^۲$. به تشابه، $b=۶$ نتیجه می‌دهد $c=۱۷$، لذا $a=۲۵$؛ پس $x=۵۸۹$، $y=۳۰۰$، و $x-y=۱۷^۲$.

توضیح. ۱. مسألهٔ مشخص کردن همهٔ سه‌تاییهایی که به‌ازای آنها $x-y=k^۲$ $(k\geq ۱)$ دشوارتر است، و جوابها تنها برای مقادیر معینی از k وجود دارند. جواب کلی با

$$a=e^۲+(e+d)^۲, \qquad b=۲de, \qquad k=۲e^۲-d^۲$$

داده می‌شود که در آن d فرد است و $(d,e)=۱$. مثلاً اگر $d=۳$ و $e=۴$، آنگاه $k=۲۳$، $b=۲۴$، $a=۶۵$؛ لذا $x=۳۶۴۹$، $y=۳۱۲۰$ و $x-y=(۲۳)^۲$.

توضیح. ۲. اگر تعیین سه‌تایی (x,y,z) با $y>x$، y زوج، و $y-x$ مربع کامل مورد نظر باشد، مسأله پیچیده‌تر است و بهترین کار آن است که با تکنیک حل معادلهٔ پل بررسی شود (مسألهٔ ۴۰.۱۰ را ببینید). برای $y-x=۱$، این روند سه جواب زیر (از میان تعداد نامتناهی) را به‌دست می‌دهد: $(۳,۴,۵)$، $(۱۶۹,۱۲۰,۱۱۹)$، و $(۴۰۵۹,۴۰۶۰,۵۷۴۱)$.

آخرین قضیهٔ فرما

۱۴.۸ نشان دهید که برای اثبات آخرین قضیهٔ فرما، کافی است که آن را برای حالتی اثبات کنیم که نما یک عدد اول فرد باشد. (راهنمایی: از (۴.۸) استفاده کنید.)

حل. اگر نمای n مضربی از ۴ باشد، آخرین قضیهٔ فرما از (۴.۸) نتیجه می‌شود. زیرا اگر $n = 4k$ و $a^n + b^n = c^n$، آنگاه $(a^k)^4 + (b^k)^4 = (c^{2k})^2$، که این با اینکه $x^4 + y^4 = z^2$ جواب صحیح نامنفی ندارد متناقض است. حال فرض می‌کنیم p یک عامل اول فرد n باشد، و فرض می‌کنیم $n = kp$. اگر آخرین قضیهٔ فرما برای نمای n برقرار نباشد، آنگاه برای نمای p نیز برقرار نیست، زیرا اگر $x^n + y^n = z^n$، پس $(x^k)^p + (y^k)^p = (z^k)^p$.

۱۵.۸ اگر $n \geq 3$، ثابت کنید که یک سه‌تایی فیثاغورسی نمی‌تواند جواب $x^n + y^n = z^n$ باشد.

حل. فرض کنیم $x^2 + y^2 = z^2$ با $y > x$. آنگاه

$$x^n + y^n = x^2 x^{n-2} + y^2 y^{n-2} < (x^2 + y^2) y^{n-2} = z^2 y^{n-2} < z^2 z^{n-2} = z^n$$

۱۶.۸ اگر $x^5 + y^5 = z^5$، نشان دهید که لااقل یکی از x، y، و z مضرب ۵ است. (راهنمایی: با پیمانهٔ ۲۵ عمل کنید.)

حل. تمام مقادیر ممکن برای a^5 به پیمانهٔ ۲۵ را ثبت می‌کنیم. چون $(a+5k)^5 \equiv a^5 \pmod{25}$، کافی است $a = 0, \pm 1, \pm 2$ را در نظر بگیریم. لذا a^5 به پیمانهٔ ۲۵ همنهشت با 0، ± 1، یا ± 7 است. امتحان سادهٔ حالتها نشان می‌دهد که اگر $x^5 + y^5 = z^5$ و هیچ‌کدام از x و y بر ۵ بخشپذیر نباشند، آنگاه z بر ۵ بخشپذیر است.

۱۷.۸ با استفاده از (۴.۸) ثابت کنید که $x^4 - 4y^4 = z^2$ هیچ جواب صحیح مثبت ندارد. (راهنمایی: اگر جوابی وجود داشته باشد، هر دو طرف را به توان ۲ برسانید و جمله‌ها را طوری مرتب کنید که $x^4 + y^4 = z^2$ جواب داشته باشد.)

حل. فرض کنیم اعداد صحیح مثبت r، s، و t وجود داشته باشند به‌طوری که $r^4 - 4s^4 = t^2$. دو طرف را به توان ۲ می‌رسانیم و معادلهٔ حاصل را به‌صورت $(2rs)^4 + t^4 = (r^4 + 4s^4)^2$ می‌نویسیم. لذا $z^2 = x^4 + y^4$ جواب صحیح مثبت دارد، که با (۴.۸) متناقض است.

توضیح. نشان دادیم که از یک جواب مفروض $x^۴ - ۴y^۴ = z^۲$ در اعداد صحیح مثبت، می‌توانیم یک جواب صحیح مثبت برای $x^۴ + y^۴ = z^۲$ تولید کنیم. می‌توان به آسانی استدلال را معکوس کرد و جوابی برای $x^۴ - ۴y^۴ = z^۲$ از جواب $x^۴ + y^۴ = z^۲$ تولید کرد. معادله‌های $x^۴ + ۴y^۴ = z^۲$ و $x^۴ - y^۴ = z^۲$ نیز به این معنی هم‌ارزند.

◁ **۱۸.۸** نشان دهید که معادلهٔ $x^۴ - y^۴ = z^۲$ جواب صحیح مثبت ندارد.

حل. اگر جواب مثبتی وجود داشته باشد، فرض می‌کنیم x کوچکترین عدد صحیح مثبتی باشد که به‌ازای آن اعداد مثبت y و z وجود دارند به‌طوری که $x^۴ - y^۴ = z^۲$. همانند اثبات (۴.۸)، اگر x، y، و z دوبه‌دو نسبت به هم اول نباشند، جواب مثبت کوچکتری به‌دست می‌آوریم، که با مینیمال بودن x تناقض دارد. لذا $(y^۲, z, x^۲)$ یک سه‌تایی فیثاغورسی اولیه است.

اگر y فرد باشد، آنگاه بنابر (۲.۸)، اعداد مثبت a و b وجود دارند به‌طوری که $x^۲ = a^۲ + b^۲$ و $y^۲ = a^۲ - b^۲$؛ پس $a^۴ - b^۴ = (xy)^۲$، چون $a^۲ < x^۲$، این مینیمال بودن x را نقض می‌کند.

اگر y زوج باشد، آنگاه اعداد صحیح متباین a و b که یکی زوج و دیگری فرد است وجود دارند به‌طوری که $x^۲ = a^۲ + b^۲$ و $۲ab = y^۲$. می‌توانیم فرض کنیم که a فرد و b زوج است. لذا (a, b, x) یک سه‌تایی فیثاغورسی اولیه است با bی زوج، و بنابراین اعداد متباین s و t وجود دارند به‌طوری که $a = s^۲ - t^۲$ و $b = ۲st$. اما چون $۲ab = y^۲$، در نتیجه a یک مربع کامل و b دو برابر یک مربع کامل است. فرض کنیم $a = c^۲$ و $b = ۲d^۲$. چون $b = ۲st = ۲d^۲$ و $(s, t) = ۱$)، پس s و t هرکدام مربع کامل هستند. اگر $s = u^۲$ و $t = v^۲$، آنگاه $c^۲ = a = s^۲ - t^۲ = u^۴ - v^۴$. چون روشن است که $u < x$، این مجدداً مینیمال بودن x را نقض می‌کند.

۱۹.۸ ثابت کنید که حداکثر یک عنصر از سه‌تایی فیثاغورسی می‌تواند مربع کامل باشد. (راهنمایی: از (۴.۸) و (۵.۸) استفاده کنید.)

حل. فرض کنیم (x, y, z) یک سه‌تایی فیثاغورسی باشد. اگر x و y مربع کامل باشند، آنگاه می‌توان $z^۲$ را به‌صورت مجموع دو توان چهارم نوشت، که با (۴.۸) متناقض است. اگر y و z مربع کامل باشند، آنگاه می‌توان $x^۲$ را به‌صورت تفاضل دو توان چهارم بیان کرد، که با (۵.۸) متناقض است.

۲۰.۸ ثابت کنید اعداد مثبت a و b وجود ندارند به‌طوری که $a^۲ + b^۲$ و $a^۲ - b^۲$ هر دو مربع کامل باشند.

حل. اگر a^2+b^2 و a^2-b^2 مربع کامل باشند، حاصلضربشان a^4-b^4 نیز مربع کامل است که با (۵.۸) متناقض است.

۲۱.۸ آیا مساحت یک مثلث فیثاغورسی می‌تواند مربع کامل باشد؟ دو برابر یک مربع کامل چطور؟ (راهنمایی: مسأله‌های ۲۰.۸ و ۱۸.۸ را به‌کار برید.)

حل. فرض کنیم (x,y,z) یک سه‌تایی فیثاغورسی باشد، و فرض کنیم مساحت مثلث مربوط $xy/2$، مثلاً a^2 باشد. لذا $(x+y)^2=z^2+(2a)^2$ و $(x-y)^2=z^2-(2a)^2$، که با توجه به مسألهٔ ۲۰.۸ یک تناقض است.

با استدلالی مشابه، اگر $xy/2=2a^2$، داریم $(x+y)^2=z^2+8a^2$ و $(x-y)^2=z^2-8a^2$. لذا $(x^2-y^2)^2=(2a)^4-4z^4$، که مسأله ۱۸.۸ را نقض می‌کند.

۲۲.۸ (الف) ثابت کنید که $x^4-2y^2=1$ جواب صحیح مثبت ندارد. به‌ویژه، $x^4-2y^4=1$ حلپذیر نیست.

(ب) ثابت کنید که معادلهٔ $x^4-2y^2=-1$ جواب صحیح مثبت دیگری بجز $x=y=1$ ندارد. (لذا $x^4-2y^4=-1$ تنها یک جواب مثبت دارد.)

حل. (الف) اگر $x^4-2y^2=1$، آنگاه $2y^2=x^4-1$ و لذا $4y^4=x^8-2x^4+1$. با افزودن $4x^4$ به دو طرف داریم $4(y^4+x^4)=(x^4+1)^2$؛ پس x^4+1 زوج است. اگر $z=(x^4+1)/2$، نتیجه می‌شود که $x^4+y^4=z^2$، که (۴.۸) را نقض می‌کند.

(ب) اکنون کاربرد همان استدلالِ (الف) $y^4-x^4=z^2$ را حاصل می‌سازد، که تنها جوابهای نمایان $x=\pm1$، $y=\pm1$ و $z=0$ را دارد. لذا تنها جواب صحیح مثبتِ معادله اصلی $x=y=1$ است.

◁ **۲۳.۸** ثابت کنید که $x^2-2y^4=1$ جواب صحیح مثبت ندارد. (راهنمایی: x^2-1 را به حاصلضرب تبدیل کنید و قسمت (الف) از مسألهٔ قبل را به‌کار برید.)

حل. اگر $x^2-2y^4=1$، آنگاه $2y^4=(x-1)(x+1)$. با تغییر علامت x اگر لازم باشد، می‌توانیم فرض کنیم $x\equiv1 \pmod 4$، یعنی، $x=4k+1$. از این‌رو، می‌توان معادلهٔ آخر را به‌صورت $4k(2k+1)=y^4$ نوشت، و لذا y زوج است، مثلاً $y=2z$. پس $k(2k+1)=4z^4$، و چون $2k+1$ فرد است، داریم $k|4$. لذا، با فرض $k=4s$، داریم $s(8s+1)=z^4$. در نتیجه $s=u^4$ و $8s+1=v^4$، زیرا s و $8s+1$ نسبت به هم اول‌اند.

لذا $v^۴ - ۸u^۴ = ۱$، یعنی $v^۴ - ۲(۲u^۲)^۲ = ۱$. بنابر قسمت (الف) از مسألهٔ قبل، این معادله تنها دارای جواب نمایان $v = \pm ۱$، $u = ۰$ است. بنابراین $s = ۰$، که $k = ۰$ را ایجاب می‌کند و لذا $x = ۱$. لذا معادلهٔ اصلی جواب صحیح مثبت ندارد.

مجموعهای دو مربع

۲۴.۸ تعیین کنید کدام‌یک از اعداد زیر مجموع دو مربع است: ۹۸، ۳۴۳، ۷۳۵، ۱۴۲۸، و ۴۶۸۰.

حل. بنابر (۸.۸)، n مجموع دو مربع است اگر و تنها اگر در تجزیهٔ n به اعداد اول هر عدد اول به‌صورت $۴k + ۳$ با توان زوج ظاهر شود. این مطلب روشن است که برای $۹۸ = ۲ \times ۴۹$ برقرار است و برای $۳۴۳ = ۷^۳$ برقرار نیست. با جمع ارقام ۷۳۵، می‌بینیم که ۷۳۵ مضرب ۳ است ولی مضرب ۹ نیست، لذا ۷۳۵ مجموع دو مربع نیست. به دلیل مشابه، ۱۴۲۸ مجموع دو مربع نیست. چون $۴۶۸۰ = ۲^۳ \times ۳^۲ \times ۵ \times ۱۳$، پس مجموع دو مربع است.

۲۵.۸ همهٔ نمایشهای اساساً متفاوت ۵۵۲۵ به‌صورت مجموع دو مربع را بیابید.

حل. چون $۵۵۲۵ = ۵^۲ \times ۱۳ \times ۱۷$، (۱۱.۸) ایجاب می‌کند که $N(۵۵۲۵) = ۴۸$. چون ۵۵۲۵ نه یک مربع کامل است و نه دو برابر یک مربع کامل، در نتیجه ۵۵۲۵ دارای شش نمایش اساساً متفاوت به‌صورت مجموع دو مربع است. ابتدا نمایشهای $۱۳ \times ۱۷ = ۲۲۱$ به‌صورت مجموع دو مربع را پیدا می‌کنیم. تعداد دو نمایش اساساً متفاوت این چنینی وجود دارند، که می‌توان آنها را با جستجو یا با کاربرد (۷.۸) پیدا کرد. برای استفاده از (۷.۸)، توجه داریم که $۱۳ = ۲^۲ + ۳^۲$ و $۱۷ = ۱^۲ + ۴^۲$. فرمول $(a^۲ + b^۲)(c^۲ + d^۲) = (ac - bd)^۲ + (ad + bc)^۲$، با $a = ۲$، $b = ۳$، $c = ۱$، و $d = ۴$، رابطهٔ $۲۲۱ = ۱۰^۲ + ۱۱^۲$ را به‌دست می‌دهد (بعد از تعویض علامت). با جابه‌جایی نقشهای a و b، $۲۲۱ = ۵^۲ + ۱۴^۲$ را به‌دست می‌آوریم. اگر طرفین تساوی را در ۲۵ ضرب کنیم، خواهیم داشت $۵۵۲۵ = ۵۰^۲ + ۵۵^۲$ و $۵۵۲۵ = ۲۵^۲ + ۷۰^۲$.

با استفاده از همین تکنیک و اینکه $۲۵ = ۳^۲ + ۴^۲$، داریم $۲۵ \times ۱۳ = ۶^۲ + ۱۷^۲$ و $۲۵ \times ۱۳ = ۱^۲ + ۱۸^۲$. ترکیب این و نمایش $۱۷ = ۱^۲ + ۴^۲$ چنین می‌دهد $۵۵۲۵ = ۶۲^۲ + ۴۱^۲ = ۷^۲ + ۷۴^۲ = ۷۱^۲ + ۲۲^۲ = ۱۴^۲ + ۷۳^۲$.

۲۶.۸ همهٔ نمایشهای اساساً متفاوت ۱۴۳۶۵ به‌صورت مجموع دو مربع را بیابید.

حل. با توجه اینکه $۱۴۳۶۵ = ۵ \times ۱۳^۲ \times ۱۷$، دقیقاً مانند مسألهٔ قبل نتیجه می‌گیریم که

۱۴۳۶۵ دارای شش نمایش اساساً متفاوت به‌صورت مجموع دو مربع است. آنها عبارت‌اند از $۱۱۷^۲ + ۲۶^۲$، $۹۱^۲ + ۷۸^۲$، $۶۹^۲ + ۹۸^۲$، $۱۱۸^۲ + ۲۱^۲$، $۱۰۷^۲ + ۵۴^۲$، و $۱۱۴^۲ + ۳۷^۲$.

۲۷.۸ دو نمایشِ اساساً متفاوت ۲۲۹۳۲۰ به‌صورت مجموع دو مربع را به‌دست آورید.

حل. چون $۲۲۹۳۲۰ = ۲^۳ \times ۳^۲ \times ۷^۲ \times ۵ \times ۱۳ = ۱۳۰ \times ۵ \times ۲$، ابتدا ۱۳۰ را نمایش می‌دهیم. می‌توانیم از روش ماشینی (۷.۸) برای این کار استفاده کنیم، ولی می‌توان جوابها را به آسانی از راه تجسس به‌دست آورد: $۱۳۰ = ۳^۲ + ۱۱^۲ = ۷^۲ + ۹^۲$. اگر در $۲^۲ \times ۳^۲ \times ۷^۲$ ضرب کنیم، نمایشهای $۲۹۴^۲ + ۳۷۸^۲$ و $۱۲۶^۲ + ۴۶۲^۲$ حاصل می‌شوند.

۲۸.۸ فرض کنید عدد اول q به‌صورت $۴k + ۳$ باشد. ثابت کنید که $q^۲$ مجموع دو مربع غیرصفر نیست.

حل. فرض کنیم $q^۲ = a^۲ + b^۲$. بنابر (i.۶.۸)، $q|a$. لذا اگر $a \neq ۰$، آنگاه $a^۲ \geq q^۲$ و بنابراین $b = ۰$.

برهان دیگر: چهار نمایش بدیهی داریم، یعنی، $(\pm q)^۲ + ۰^۲$ و $۰^۲ + (\pm q)^۲$. ولی، بنابر (۱۱.۸)، $N(q^۲) = ۴$، و لذا اینها تنها نمایشها هستند.

۲۹.۸ ثابت کنید عدد اول p به‌صورت $۴k + ۱$ است اگر و تنها اگر $n \geq ۱$ وجود داشته باشد به‌طوری که $p|n^۲ + (n+۱)^۲$. (راهنمایی: ملاحظه کنید که $(n, n+۱) = ۱$.)

حل. ابتدا فرض می‌کنیم که $p|n^۲ + (n+۱)^۲$. اگر p به‌صورت $۴k + ۳$ باشد، آنگاه بنابر (i.۶.۸)، داریم $p|n$ و $p|n+۱$، که ممکن نیست. چون p فرد است، در نتیجه p به‌صورت $۴k + ۱$ است.

حال، فرض کنیم $p \equiv ۱ \pmod ۴$. می‌خواهیم یک مقدار از n بیابیم به‌طوری که $n^۲ + (n+۱)^۲ \equiv ۰ \pmod p$، یا $۲n^۲ + ۲n + ۱ \equiv ۰ \pmod p$. با ضرب این همنهشتی در ۲ و کامل کردن مربع داریم $(۲n+۱)^۲ \equiv -۱ \pmod p$. چون -۱ یک ماندهٔ درجهٔ دوم p است، عددی چون x وجود دارد به‌طوری که $x^۲ \equiv -۱ \pmod p$. لذا اگر x فرد باشد، قرار می‌دهیم $n = (x-۱)/۲$، و اگر x زوج باشد، $n = (p-x-۱)/۲$.

۳۰.۸ (الف) فرض کنید $n = ۱۷۶۹۶۲۵$، تعداد نمایشهای اولیهٔ n به‌صورت مجموع دو مربع را پیدا کنید. (ب) تمام نمایشهای اساساً متمایز n به‌صورت مجموع دو مربع را بیابید. (ج) یک

نمایش $8n$ به‌صورت مجموع دو مربع را به‌دست آورید.

حل. (الف) داریم $n = 3^2 \times 5^3 \times 11^2 \times 13$. چون n بر عدد اولی به‌صورت $4k+3$ بخشپذیر است، از (۱۵.۸) نتیجه می‌شود که n نمایش اولیه ندارد.

(ب) بنابر (۱۱.۸)، $n = 3^2 \times 5^3 \times 13$ دارای $2 \times 4 \times 4 = 32$ نمایش است، و لذا n دارای $32/8 = 4$ نمایش اساساً متمایز است. برای یافتن آنها، ابتدا $5^3 \times 13$ را به‌صورت مجموع دو مربع می‌نویسیم. آشکار است که $2^2 + 3^2$ تنها نمایش ۱۳ است. چون $1^2 + 2^2 = 5$، (۷.۸) ایجاب می‌کند که $5^2 = (1^2 + 2^2)(1^2 + 2^2) = 5^2 + 0^2 = 3^2 + 4^2$، و لذا $5^3 = (1^2 + 2^2)(3^2 + 4^2) = 11^2 + 2^2$ و $5^3 = (1^2 + 2^2)(5^2 + 0^2) = 5^2 + 10^2$. با استفاده از (۷.۸) در ترکیبات مختلف $5^3 \times 13$، داریم

$$(5^2+10^2)(3^2+2^2) = (15 \pm 20)^2 + (10 \mp 30)^2 = 35^2 + 20^2 = 5^2 + 40^2$$
$$(11^2+2^2)(3^2+2^2) = (33 \pm 4)^2 + (22 \mp 6)^2 = 37^2 + 16^2 = 29^2 + 28^2.$$

بنابراین، نمایشهای خود n با ضریب هر نمایش از $5^3 \times 13$ در 33^2 به‌دست می‌آیند؛ یعنی، $6602^2 + 1155^2$، $13202^2 + 1652^2$، $5282^2 + 1221^2$، و $9243^2 + 957^2$.

(ج) چون $2^2 + 2^2 = 8$، لذا برای به‌دست آوردن تمام نمایشهای (اساساً متمایز) $8n$ می‌توانیم (۷.۸) را با هر نمایش به‌دست آمده در (ب) به‌کار بریم: $9902^2 + 3632^2$، $23102^2 + 2972^2$، $13862^2 + 3498^2$، و $6622^2 + 3762^2$.

۳۱.۸ عدد صحیح n را پیدا کنید به‌طوری که n دقیقاً سه نمایش اساساً متمایز به‌صورت مجموع دو مربع داشته باشد.

حل. (۱۱.۸) را به‌کار می‌بریم. اگر $n = p^2q$، که در آن p و q اعداد اول متمایز به‌صورت $4k+1$ هستند، آنگاه $N(n) = 4 \times 3 \times 2 = 24$. یک نمایش n به‌صورت مجموع دو مربع متمایز غیرصفر هشت‌گونه حاصل می‌سازد که از تغییر علامت یا ترتیب جمله‌ها تولید می‌شوند. لذا p^2q دارای $24/8 = 3$ نمایش اساساً متمایز به‌صورت مجموع دو مربع دارد. مثلاً، $n = 5^2 \times 13$ ویژگی مورد نظر را دارد.

به روش دیگر، اگر p عدد اولی به‌صورت $4k+1$ باشد، آنگاه $N(p^m) = 4(m+1)$. با همان استدلال بالا، اگر $m+1 = 6$، آنگاه p^m دقیقاً سه نمایش اساساً متمایز به‌صورت مجموع دو مربع دارد.

مثال دیگر $n = p^۴$، که p به‌صورت $۴k + ۱$ است. بنابر (۱۱.۸)، داریم $N(n) = ۲۰$. روشن است که، n دارای نمایش $n = (p^۲)^۲ + ۰^۲$ است، که مجموعی از چهار نمایش به‌دست می‌دهد اگر ترتیب و علامت را به حساب بیاوریم. ۱۶ نمایش باقیمانده به دو خانواده، هر یک با ۸ نمایش تجزیه می‌شوند. لذا $p^۴$ دقیقاً سه نمایش اساساً متمایز دارد.

توضیح. نشان دادن اینکه می‌توان همهٔ جوابها را با ضرب جوابهای بالا در عددی به‌صورت $m^۲$ یا $۲m^۲$ به‌دست آورد، که m هیچ عامل اولی به‌صورت $۴k + ۱$ نداشته باشد، دشوار نیست.

۳۲.۸ اثبات یا رد کنید: حداقل یکی از هر چهار عدد صحیح مثبت متوالی مجموع دو مربع نیست.

حل. درست است. زیرا یکی از اعداد همنهشت با ۳ به پیمانهٔ ۴ است و لذا نمی‌تواند مجموع دو مربع باشد.

۳۳.۸ فرض کنید $n = ۲ \times ۳^۲ \times ۵^۳ \times ۱۳^۵$. آیا یک مثلث فیثاغورسی با وتر n وجود دارد؟ یک مثلث فیثاغورسی اولیه با وتر n چطور؟

حل. جویا می‌شویم که آیا می‌توان $n^۲$ را به‌صورت مجموع دو مربع غیرصفر نمایش داد. مسلماً، $n^۲$ مجموع دو مربع است، لذا بنابر (۱۱.۸)، داریم $N(n^۲) = ۴ \times (۶ + ۱)(۱۰ + ۱)$. چهار نمایش نمایان $n^۲$ به‌صورت مجموع دو مربع را، که یکی از آنها ۰ است، کنار می‌گذاریم. لذا $۴ \times (۷۷ - ۱)$ نمایش به‌صورت مجموع مربعهای غیرصفر به‌دست می‌آوریم. در نتیجه $۳۸ = ۸/(۷۶ \times ۴)$ مثلث فیثاغورسی متفاوت با وتر n وجود دارند.

هیچ مثلث فیثاغورسی اولیه با وتر n وجود ندارد. این مطلب از (۱۵.۸) نتیجه می‌شود، زیرا $n^۲$ بر عدد اولی به‌صورت $۴k + ۳$ بخشپذیر است.

۳۴.۸ ثابت کنید که n مجموع دو مربع است اگر و تنها اگر $n = m^۲N$، که در آن N عاری از مربع است و هر عامل اول N به‌صورت $۴k + ۱$ است.

حل. این مسأله تنها یک بیان دیگر از (۹.۸) است. اگر n به‌صورت مفروض باشد، آنگاه بنا بر (۹.۸)، N مجموع دو مربع است. اگر $N = a^۲ + b^۲$، آنگاه $n = (ma)^۲ + (mb)^۲$. بعکس، اگر n مجموع دو مربع باشد، آنگاه بنابر (۹.۸)، هر عامل اول به‌صورت $۴k + ۳$ در تجزیه n به اعداد اول با توان زوج ظاهر می‌شود. لذا، اگر n را به‌صورت $m^۲N$ بنویسیم، که در آن N عاری

از مربع است، آنگاه هیچ عامل اول به‌صورت $4k+3$ عدد N را نمی‌شمارد، و لذا هر عامل اول فرد N به‌صورت $4k+1$ است.

۳۵.۸ (فرما، ۱۶۳۶) نشان دهید که نمی‌توان ۲۱ را به‌صورت مجموع مربعهای دو اعداد گویا بیان کرد.

حل. فرض می‌کنیم (فرض خُلف) که $r^2+s^2=21$، که در آن r و s گویا هستند. می‌نویسیم $r=a/c$، $s=b/c$، که a، b، و $c>0$ اعداد صحیح هستند. در این‌صورت، $21c^2=a^2+b^2$. اما چون عدد اول ۳ در تجزیهٔ $21c^2$ به اعداد اول با توان فرد ظاهر می‌شود، (۶.۸) ایجاب می‌کند که $21c^2$ نتواند مجموع مربعهای دو عدد صحیح باشد.

۳۶.۸ نشان دهید که عدد صحیح مثبت n مجموع دو مربع غیرصفر است اگر و تنها اگر در تجزیهٔ n به اعداد اول هر عامل به‌صورت $4k+3$ با توان زوج ظاهر شود و یا توان ۲ فرد باشد و یا n حداقل یک عامل اول به‌صورت $4k+1$ داشته باشد.

حل. اگر n به‌صورت مطلوب باشد، بنابر (۹.۸)، n مجموع دو مربع است، و این اعداد بایستی غیرصفر باشند مگر آنکه n یک مربع کامل باشد. فرض کنیم n مربع کامل باشد و قرار می‌دهیم $n=m^2p^2$، که در آن p عدد اولی به‌صورت $4k+1$ است. نشان می‌دهیم که p^2 مجموع دو مربع غیرصفر است. می‌نویسیم $p=a^2+b^2$؛ لذا، بنابر (۷.۸)،

$$p^2=(a^2+b^2)(a^2+b^2)=(2ab)^2+(a^2-b^2)^2$$

روشن است که a و b صفر نیستند و $a\neq b$، لذا p^2 را به‌صورت مجموع دو مربع غیرصفر بیان کرده‌ایم.

بعکس، اگر n مجموع دو مربع غیرصفر باشد، آنگاه تمام عاملهای اول به‌صورت $4k+3$ در تجزیهٔ n به عوامل اول با توان زوج ظاهر می‌شوند. لذا فرض می‌کنیم $n=s^2m$، که در آن m بر عدد اولی به‌صورت $4k+3$ بخشپذیر نیست. اگر m بر عدد اولی به‌صورت $4k+1$ بخشپذیر باشد، کار تمام است. در غیر این‌صورت، m توانی از ۲ است، و به آسانی دیده می‌شود که m نمی‌تواند توان زوجی از ۲ باشد. لذا n به‌صورت 2^ts^2 است، که در آن t فرد و تمام عاملهای اول s به‌صورت $4k+3$ هستند.

توضیح. استدلال مشابه مطلب زیر را نشان می‌دهد: n مجموع دو مربع غیرصفر متفاوت است اگر و تنها اگر هر عامل اول n که به‌صورت $4k+3$ است با توان زوج ظاهر شود و n لااقل یک عامل اول به‌صورت $4k+1$ داشته باشد.

۳۷.۸ ثابت کنید عدد صحیح مثبت n وتر یک مثلث فیثاغورسی است اگر و تنها اگر n بر لااقل یک عدد اول به‌صورت $۴k+۱$ بخشپذیر باشد.

حل. عدد صحیح مثبت n وتر یک مثلث فیثاغورسی است اگر و تنها اگر $n^۲$ دارای نمایشی به‌صورت مجموع دو مربع غیرصفر باشد. ابتدا فرض می‌کنیم که $p|n$، که p عدد اولی به‌صورت $۴k+۱$ است، و فرض می‌کنیم $n^۲=k^۲p^۲$. سپس، بنابر (۱۵.۸)، $p^۲$ دارای نمایش $p^۲=a^۲+b^۲$ به‌صورت مجموع دو مربع متباین است؛ روشن است که، هیچ‌کدام از a و b صفر نیستند. لذا $n^۲=(ka)^۲+(kb)^۲$، و بنابراین n وتر یک مثلث فیثاغورسی است.

بعکس، فرض کنیم n وتر یک مثلث فیثاغورسی باشد؛ لذا اعداد صحیح مثبت a و b وجود دارند به‌طوری که $n^۲=a^۲+b^۲$. فرض کنیم $d=(a,b)$، چون $(n/d)^۲=(a/d)^۲+(b/d)^۲$، پس n/d وتر یک مثلث فیثاغورسی اولیه است. لذا بنابر (۱۵.۸)، n/d بر هیچ عدد اولی به‌صورت $۴k+۳$ بخشپذیر نیست. چون n/d فرد است و مساوی با ۱ نیست، نتیجه می‌شود که n/d، و لذا n، بر عدد اولی به‌صورت $۴k+۱$ بخشپذیر است.

برهان دیگر: ابتدا فرض می‌کنیم که n و در نتیجه $n^۲$ هیچ عامل اولی به‌صورت $۴k+۱$ نداشته باشد، لذا بنابر (۱۱.۸)، $N(n^۲)=۴$. چون $n^۲$ دارای چهار نمایش بدیهی به‌صورت مجموع دو مربع است، یکی از آنها ۰ است، $n^۲$ هیچ نمایش به‌صورت مجموع دو مربع غیرصفر ندارد.

بعکس، فرض کنیم n یک مقسوم‌علیه اول به‌صورت $۴k+۱$ دارد. لذا (۱۱.۸) ایجاب می‌کند که $N(n^۲)\geq ۱۲$. در نتیجه $n^۲$ لااقل یک نمایش به‌صورت دو مربع غیرصفر دارد.

۳۸.۸ به‌ازای یک عدد صحیح مثبت مفروض z، ثابت کنید که تعداد سه‌تاییهای فیثاغورسی (x,y,z) با $۰<x<y$، برابر است با $(N(z^۲)-۴)/۸$، که در آن $N(z^۲)$ تعداد (کل) نمایشهای $z^۲$ به‌صورت مجموع دو مربع است.

حل. هر سه‌تایی فیثاغورسی (x,y,z) با یک نمایش $z^۲$ به‌صورت مجموع دو مربع مثبت متناظر است، و این نمایش به‌طور یکتا تعیین می‌شود اگر فرض کنیم که $۰<x<y$. (نمی‌توانیم داشته باشیم $x=y$، زیرا در این‌صورت $z^۲=۲x^۲$، که غیرممکن است، زیرا $z^۲$ دارای تعدادی زوج‌عامل و $۲x^۲$ دارای تعدادی فردعامل ۲ است.) هر نمایش $z^۲$ به‌صورت مجموع دو مربع غیرصفر دارای هشت تغییر است اگر تغییرات در علامت و ترتیب جمله‌ها را منظور کنیم؛ همچنین، $z^۲$ دارای نمایش $z^۲+۰^۲$ است، که چهار تغییر را می‌پذیرد و به‌وضوح متناظر با یک سه‌تایی

فیثاغورسی نیست. اگر این چهار نمایش را کنار بگذاریم، $N(z^۲) - ۴$ نمایشهای باقیمانده با $(N/z^۲) - ۴)/۸$ نمایشهای به‌صورت $x^۲ + y^۲$، که $۰ < x < y$، متناظرند.

۳۹.۸ در نامه‌ای به مرسن در تاریخ ۲۵ دسامبر ۱۶۴۰، فرما عدد nی را خواسته است که وتر دقیقاً ۳۶۷ مثلث قائم‌الزاویه با اضلاع صحیح باشد. مسألهٔ قبل را برای پاسخ به سؤال فرما به‌کار برید.

حل. فرض کنیم $n = m\prod p_i^{a_i}$، که در آن p_iها اعداد اول به‌صورت $۴k+۱$ هستند، m بر هیچ عدد اولی به‌صورت $۴k+۱$ بخشپذیر نیست، و هر عامل اول m که به‌صورت $۴k+۳$ است با توان زوج ظاهر می‌شود. در این‌صورت (۱۱.۸) ایجاب می‌کند که $N(n^۲) = ۴\prod(۲a_i+۱)$، و لذا، بنابر مسألهٔ قبل، $۴\prod(۲a_i+۱) - ۴)/۸$ مثلث فیثاغورسی متفاوت با وتر n وجود دارند. اکنون، یافتن n برای هر تعداد مثلث فیثاغورسی با وتر n که بخواهیم، آسان است. مثلاً، فرض کنیم $n = ۵^k$. در این‌صورت $۴(۲k+۱) - ۴)/۸ = k$ مثلث فیثاغورسی با وتر n وجود دارند. لذا اگر $n = ۵^{۳۶۷}$، آنگاه n وتر دقیقاً ۳۶۷ مثلث قائم‌الزاویه با اضلاع صحیح است. (جوابهای بسیاری وجود دارند؛ کوچکترین آنها $n = ۵^{۱۴} \times ۱۳^۲ \times ۱۷$ است.)

۴۰.۸ اثبات یا رد کنید: هر عدد صحیح مثبت n حداقل همان تعداد عامل به‌صورت $۴k+۱$ دارد که به‌صورت $۴k+۳$ دارد.

حل. این حکم برقرار است و فوراً از (۱۲.۸) نتیجه می‌شود، زیرا به‌ازای هر n، $N(n) \geq ۰$.

۴۱.۸ فرض کنید $n = ۲^۳ \times ۵^۴ \times ۱۷ \times ۳^۶ \times ۱۱^۴$. ثابت کنید که n دقیقاً ۱۰ عامل به‌صورت $۴k+۱$ بیشتر از عاملهای به‌صورت $۴k+۳$ دارد. (راهنمایی: ابتدا نشان دهید که n نمایشهایی به‌صورت مجموع دو مربع دارد.)

حل. بنابر (۹.۸)، n دارای نمایشی به‌صورت مجموع دو مربع است، زیرا هر عامل اول به‌صورت $۴k+۳$ با توان زوج در تجزیهٔ n به عوامل اول ظاهر می‌شود. لذا، بنابر (۱۱.۸)، $N(n) = ۴(۴+۱)(۱+۱) = ۴۰$. اما بنابر (۱۲.۸)، $N(n) = ۴(D_۱ - D_۳)$، لذا $D_۱ - D_۳ = ۱۰$.

۴۲.۸ فرض کنید $n = q_۱^{b_۱} \cdots q_r^{b_r}$، که در آن هر q_i عدد اولی به‌صورت $۴k+۳$ است. اگر $b_۱ + b_۲ + \cdots + b_r$ فرد باشد، ثابت کنید که n همان تعداد عامل به‌صورت $۴k+۱$ دارد که به‌صورت $۴k+۳$.

حل. چون مجموع b_iها فرد است، لذا حداقل یکی از b_iها فرد است. از (۹.۸) نتیجه می‌شود که n هیچ نمایشی به‌صورت مجموع دو مربع ندارد، و لذا بنابر (۱۲.۸)، $D_1 - D_3 = 0$، یعنی، $D_1 = D_3$.

۴۳.۸ فرض می‌کنیم $n = 670761000$. عدد n چه تعداد عامل به‌صورت $4k + 1$ بیشتر از عاملهای به‌صورت $4k + 3$ دارد؟

حل. داریم $n = 2^3 \times 3^4 \times 7^2 \times 5^3 \times 13^2$، و لذا بنابر (۱۱.۸) و (۱۲.۸)، $N(n) = 4(3 + 1)(2 + 1) = 48 = 4(D_1 - D_3)$؛ از این رو $D_1 - D_3 = 12$.

۴۴.۸ نشان دهید که تعداد عاملهای به‌صورت $4k + 1$ و تعداد عاملهای به‌صورت $4k + 3$ مربوط به عدد 980496003 برابرند. (احتیاجی به تجزیهٔ این عدد نیست.)

حل. توجه داریم که 3 عدد 980496003 را می‌شمارد ولی 9 این عدد را نمی‌شمارد؛ لذا، بنابر (۹.۸)، $N(n) = 0$. از (۱۲.۸) نتیجه می‌شود که $D_1 - D_3 = 0$.

◁ **۴۵.۸** (الف) اگر $8 | N(n)$، ثابت کنید که n دقیقاً $N(n)/8$ نمایش اساساً متمایز به‌صورت مجموع دو مربع دارد.

(ب) اگر $8 \nmid N(n)$، ثابت کنید که عدد صحیح k وجود دارد به‌طوری که $N(n) = 8k + 4$ و n دقیقاً $k + 1$ نمایش اساساً متمایز به‌صورت مجموع دو مربع دارد.

حل. (الف) هر نمایش n به‌صورت مجموع دو مربع متفاوت غیرصفر دارای هشت صورت مختلف نمایان است (مثالِ قبل از (۱۷.۸) را ببینید.)؛ اگر یکی از مربعها 0 باشد یا اگر مربعها برابر باشند، آنگاه تنها چهار صورت مختلف وجود دارد. اما n حداکثر یک نمایش به‌صورت $m^2 + 0^2$ و حداکثر یک نمایش به‌صورت $m^2 + m^2$ می‌تواند داشته باشد؛ هر دو نمایش را نیز نمی‌تواند داشته باشد، زیرا به‌طور همزمان n نمی‌تواند هم یک مربع کامل و هم دو برابر یک مربع کامل باشد. بنابراین $N(n)$ به‌صورت $8k$ است اگر n نه یک مربع کامل باشد و نه دو برابر یک مربع کامل، و در غیر این‌صورت n به‌صورت $8k + 4$ است. اگر $8 | N(n)$، آنگاه هر نمایش شامل دو مربع نامساوی غیرصفر است، و لذا دقیقاً $N(n)/8$ نمایش اساساً متمایز وجود دارند.

(ب) اگر $8 \nmid N(n)$، آنگاه n یک مربع یا دو برابر یک مربع است، مثلاً $n = m^2$ یا $n = 2m^2$. اگر $n = m^2$، آنگاه فرض می‌کنیم k تعداد نمایشهای اساساً متمایز به‌صورت مجموع دو مربع غیرصفر از n باشد. اینها مجموعی از $8k$ صورت مختلف تولید می‌کنند. علاوه بر این،

n دارای نمایش $m^2 + 0^2$، با ۴ صورت مختلف است. لذا $N(n) = 8k + 4$، و مجموعی از $k + 1$ نمایش اساساً متمایز وجود دارند. استدلال برای $n = 2m^2$ اساساً عین همین است.

توضیح. استدلال بالا نشان می‌دهد که $N(n)$ مضربی از ۸ است اگر و تنها اگر n نه مربع باشد و نه دو برابر یک مربع.

۴۶.۸ فرض می‌کنیم $n = 5^4 \times 13^2$؛ پس $N(n) = 4 \times 5 \times 3 = 60$. با استفاده از مسألهٔ قبل، دربارهٔ تعداد نمایشهای اساساً متمایز n به‌صورت مجموع دو مربع چه نتیجه‌ای می‌گیرید؟

حل. با توجه به مسألهٔ قبل، چون $60 = 7 \times 8 + 4$، n دارای ۷ نمایش اساساً متمایز به‌صورت مجموع دو مربع متمایز غیرصفر است، و همچنین یک نمایش که یکی از مربعها 0^2 است، یعنی $n = (5^2 \times 13)^2 + 0^2$.

۴۷.۸ عدد صحیح مثبتی بیابید که بر ۱۴ بخشپذیر باشد و دقیقاً پنج نمایش اساساً متمایز به‌صورت مجموع دو مربع غیرصفر داشته باشد.

حل. عدد $n = 2 \times 7^2 m$ را جستجو می‌کنیم به‌طوری که هر عامل اول m به‌صورت $4k + 1$ باشد. فرض کنیم $m = \prod p_i^{a_i}$؛ پس $N(n) = 4 \prod (a_i + 1)$. اگر مطمئن باشیم که m مربع کامل نیست، آنگاه n نمایشهایی دارد که به‌صورت مجموع مربعهای نامساوی غیرصفر هستند، و لذا تعداد نمایشهای اساساً مجزا $4 \prod (a_i + 1)/8$ است. با فرض $a_1 = 4$ و $a_2 = 1$ می‌توانیم این مقدار را برابر ۵ اختیارکنیم؛ مثلاً $n = 2 \times 7^2 \times 5^4 \times 13$ را اختیارکنیم. همچنین می‌توانیم به دنبال جوابهایی باشیم که مربع کامل یا دو برابر مربع کامل هستند. بررسی مشابه نشان می‌دهد که اگر، مثلاً $n = 2 \times 7^2 \times 5^2 \times 13^2$، آنگاه n دارای پنج نمایش اساساً متمایز به‌صورت مجموع دو مربع غیرصفر دارد. این کوچکترین جواب است.

◁ **۴۸.۸** مطالب زیر اساساً برهان اویلر است که هر عدد اول به‌صورت $4k + 1$ مجموع دو مربع است.

(الف) فرض کنید p عدد اولی به‌صورت $4k + 1$ باشد. ثابت کنید $1 \leq k < p$ وجود دارد به‌طوری که kp مجموع دو مربع است.

(ب) فرض کنید m کوچکترین عدد صحیح مثبتی باشد به‌طوری که mp مجموع دو مربع است. ثابت کنید $m = 1$. لذا خود p مجموع دو مربع است.

حل. (الف) بنابر (۱۱.۵)، -1 یک ماندهٔ درجهٔ دوم p است، لذا عدد صحیحی چون s بین

$-(p-1)/2$ و $(p-1)/2$ وجود دارد به‌طوری که $s^2 \equiv -1 \pmod{p}$. لذا $k \geq 1$ وجود دارد به‌طوری که $kp = s^2 + 1$، و $kp < (p/2)^2 + 1 < p^2$، از آنجا $1 \leq k < p$.

(ب) فرض می‌کنیم $m > 1$ و می‌نویسیم $mp = a^2 + b^2$. فرض می‌کنیم A و B اعدادی با قدرمطلق مینیمال باشند که به پیمانهٔ m با a و b همنهشت هستند؛ لذا $|A| \leq m/2$ و $|B| \leq m/2$. در این‌صورت

$$A^2 + B^2 \equiv a^2 + b^2 \equiv 0 \pmod{m}$$

و لذا

$$A^2 + B^2 = km, \quad \text{با} \quad 0 \leq km \leq 2(m/2)^2 < m^2.$$

بنابراین $0 \leq k < m$. اگر $k = 0$، آنگاه $A = B = 0$ و m اعداد a و b را می‌شمارد؛ لذا $m^2 | mp$، یعنی، $m|p$، که یک تناقض است زیرا $m < p$. بنابراین $k > 0$. بنابر (۷.۸)،

$$m^2 kp = (mp)(km) = (a^2 + b^2)(A^2 + B^2) = r^2 + s^2 \qquad (1)$$

که در آن $r = aB - Ab$ و $s = aA + bB$. چون $A \equiv a \pmod{m}$ و $B \equiv b \pmod{m}$، داریم $r \equiv ab - ab = 0 \pmod{m}$ و $s \equiv a^2 + b^2 \equiv 0 \pmod{m}$؛ لذا r و s هرکدام بر m بخشپذیرند. از تقسیم (۱) بر m^2، داریم $kp = (r/m)^2 + (s/m)^2$، با $0 < k < m$. این با این مطلب که mp کوچکترین مضرب مثبت p است که مجموع دو مربع است، تناقض دارد. لذا $m = 1$، و بنابراین خود p مجموع دو مربع است.

۴۹.۸ اگر p اول و $2p - 1$ مربع کامل باشد، ثابت کنید $k \geq 1$ وجود دارد به‌طوری که $p = k^2 + (k+1)^2$.

حل. فرض کنیم $2p - 1 = n^2$؛ روشن است که n فرد است. اگر $k = (n-1)/2$، آنگاه $k + 1 = (n+1)/2$ و $p = k^2 + (k+1)^2$.

۵۰.۸ می‌توان عدد فرمای $F_5 = 2^{32} + 1$ را به‌صورت $(62264)^2 + (20449)^2$ نوشت. با استفاده از این مطلب و کاربرد مسألهٔ قبل بیان کنید که چرا F_5 اول نیست.

حل. همچنین داریم $F_5 = (2^{16})^2 + 1^2$، لذا F_5 دارای حداقل دو نمایش اساساً متمایز به‌صورت مجموع دو مربع است. لذا، بنابر مسألهٔ قبل، F_5 مرکب است.

۵۱.۸ فرض می‌کنیم n دارای (حداقل) دو نمایش اساساً متمایز به‌صورت مجموع دو مربع باشد. به‌خصوص، فرض می‌کنیم $n = s^۲ + t^۲ = u^۲ + v^۲$، که در آن $s \geq t \geq ۰$، $u \geq v \geq ۰$، و $s > u$. اگر $d = (su - tv, n)$، نشان دهید که d یک مقسوم‌علیه سره n است. (راهنمایی: ابتدا نشان دهید که $s^۲u^۲ \equiv t^۲v^۲ (\mathrm{mod}\, n)$.)

حل. داریم $s^۲ \equiv -t^۲ (\mathrm{mod}\, n)$ و $u^۲ \equiv -v^۲ (\mathrm{mod}\, n)$. از ضرب اینها، داریم $s^۲u^۲ \equiv t^۲v^۲ (\mathrm{mod}\, n)$، و لذا $(su + tv)(su - tv)$ بر n بخشپذیر است. چون $n^۲ = (s^۲ + t^۲)(u^۲ + v^۲) = (su + tv)^۲ + (sv - tu)^۲$ و $sv > tu$، نتیجه می‌شود که $su + tv < n$. چون $۰ < su - tv < n$ و $(su + tv)(su - tv)$ بر n بخشپذیر است، نتیجه می‌گیریم که $su - tv$ و n یک مقسوم‌علیه مشترک غیرنمایان دارند، و بنابراین $(su - tv, n)$ یک مقسوم‌علیه سرهٔ n است.

توضیح. اگر این مطلب را در مورد $F_۵$ به‌صورت مجموع دو مربع ارائه‌شده در مسألهٔ قبل، با $s = ۲^{۱۶}$، $t = ۱$، $u = ۶۲۲۶۴$، و $v = ۲۰۴۴۹$، به‌کار بریم، می‌بینیم که $(su - tv, F_۵) = ۶۴۱$، و لذا $۶۴۱ | F_۵$.

مجموعهای دو مربع متباین

۵۲.۸ آیا ۱۹۴۹۲۲ را می‌توان به‌صورت مجموع دو مربع بیان کرد؟ آیا ۱۹۴۹۲۲ نمایشی به‌صورت مجموع دو مربع متباین دارد؟

حل. فرض کنیم $n = ۱۹۴۹۲۲$. پس $n = ۲ \times ۳^۲ \times ۷^۲ \times ۱۳ \times ۱۷$. به‌ویژه، تمام اعداد اول به‌صورت $۴k + ۳$ با توان زوج در تجزیهٔ n ظاهر می‌شوند، و لذا بنابر (۹.۸)، می‌توان n را به‌صورت مجموع دو مربع بیان کرد. چون n بر عدد اولی به‌صورت $۴k + ۳$ بخشپذیر است، (۱۵.۸) ایجاب می‌کند که n مجموع دو مربع متباین نباشد.

۵۳.۸ ۳۳۲۵۱۴ را به‌صورت مجموع دو مربع بیان کنید. آیا می‌توان ۳۳۲۵۱۴ را به‌صورت مجموع دو مربع متباین بیان کرد؟

حل. چون $۳۳۲۵۱۴ = ۲ \times ۳^۲ \times ۷^۲ \times ۱۳ \times ۲۹$، پس ۳۳۲۵۱۴ مقسوم‌علیه اولی به‌صورت $۴k + ۳$ دارد و لذا، بنابر (۱۵.۸)، نمی‌تواند به‌صورت مجموع مربعهای متباین بیان شود. برای نمایش آن به‌صورت مجموع دو مربع، مشاهده می‌کنیم که $۲۹ = ۲^۲ + ۵^۲$ و $۲۶ = ۱^۲ + ۵^۲$. لذا بنابر (۷.۸)، داریم $۱۵^۲ + ۲۳^۲ = ۲۷^۲ + ۵^۲ = ۲۹ \times ۱۳ \times ۲$. با ضرب این تساویها

در $۷^۲ \times ۳^۲$، داریم $(۳۱۵)^۲ + (۴۸۳)^۲ = (۱۰۵)^۲ + (۵۶۷)^۲ = ۳۳۲۵۱۴$. (اینها تنها جواب هستند.)

۵۴.۸ تمام نمایشهای ۱۱۰۵۰ را به‌صورت مجموع دو مربع متباین پیدا کنید.

حل. داریم $۱۱۰۵۰ = ۲ \times ۵^۲ \times ۱۳ \times ۱۷$. لذا بنابر (۱۸.۸)، عدد ۱۱۰۵۰ دارای $۴ = ۲^{۳-۱}$ نمایش اساساً متمایز به‌صورت مجموع دو مربع متباین دارد. یافتن تمام آنها مشکل نیست. با استفاده از اینکه $۱۷ = ۱^۲ + ۴^۲$، و $۱۳ = ۲^۲ + ۳^۲$، $۵۰ = ۱^۲ + ۷^۲$، و کاربرد (۷.۸)، داریم $۱۷^۲ + ۱۹^۲ = ۱۱^۲ + ۲۳^۲$، و لذا $۱۳ \times ۵۰ = ۲۳^۲ + ۱۱^۲$

$$۱۱۰۵۰ = ۶۷^۲ + ۸۱^۲ = ۲۱^۲ + ۱۰۳^۲ = ۸۷^۲ + ۵۹^۲ = ۴۹^۲ + ۹۳^۲$$

۵۵.۸ شش کوچکترین عدد صحیح را بیابید که دقیقاً دارای چهار نمایش الزاماً متمایز به‌صورت مجموع دو مربع باشند و حداقل یکی از نمایشها اولیه باشد.

حل. با توجه به (۱۵.۸)، هر جواب مانند n حداکثر یک عامل ۲ دارد و هیچ مقسوم‌علیه اول به‌صورت $۴k + ۳$ ندارد. همچنین، لازم داریم که $N(n) = ۳ \times ۸ + ۴ = ۲۸$ یا $N(n) = ۴ \times ۸ = ۳۲$ (مسألهٔ ۴۵.۸ را ببینید)؛ لذا اگر $n = ۲^a p_۱^{a_۱} \cdots p_r^{a_r}$ که هر p_i عدد اولی به‌صورت $۴k+۱$ است، آنگاه (۱۱.۸) ایجاب می‌کند که ۸ یا ۷ $= (a_۱ + ۱) \cdots (a_r + ۱)$. لذا n به یکی از صورتهای زیر است: $p^۶$، $p_۱ p_۲ p_۳$، $p_۱ p^۳_۲$، یا $p^۷$، یا در برابر هر یک از این اعداد. شش کوچکترین عدد از این صورتها عبارت‌اند از $۱۱۰۵ = ۱۷ \times ۱۳ \times ۵$، $۱۶۲۵ = ۱۳ \times ۵^۳$، $۱۸۸۵ = ۲۹ \times ۱۳ \times ۵$، $۲۱۲۵ = ۱۷ \times ۵^۳$، $۲۲۱۰ = ۱۷ \times ۱۳ \times ۵ \times ۲$، و $۳۲۵۰ = ۲ \times ۵^۳ \times ۱۳$.

۵۶.۸ یک عدد صحیح مثبت به‌دست آورید که پنج نمایش الزاماً متمایز به صورت مجموع دو مربع داشته باشد، با این شرط که هیچ‌کدام از این نمایشها اولیه نباشند.

حل. دنبال جوابهای به‌صورت $N^۲$ می‌گردیم. برای اطمینان از اینکه هیچ نمایشی اولیه نباشد، فرض می‌کنیم $N = mn$ که در آن $n > ۱$ و n عامل اولی به‌صورت $۴k + ۱$ نداشته باشد، و m تنها بر اعداد اول به‌صورت $۴k + ۱$ بخشپذیر باشد. لذا می‌خواهیم که $m^۲$ پنج نمایش الزاماً متمایز داشته باشد. نمایش نمایان $m^۲ = ۰^۲ + m^۲$ دارای چهار صورت است، بنابراین لازم است که $N(m^۲) = ۳۶$، زیرا در این‌صورت ، جدای از نمایش نمایان، $۴ = ۸/(۴ - ۳۶)$ نمایش الزاماً مجزای دیگر وجود خواهد داشت. از (۱۱.۸) نتیجه می‌شود که $m = p^۴$، که p عدد اولی

به‌صورت $4k+1$ است، یا $m=pq$، که p و q اعداد اول متمایز به‌صورت $4k+1$ هستند. لذا، مثلاً می‌توانیم $N=2\times 5^4$ را اختیار کنیم. استدلال مشابه نشان می‌دهد که برای به‌دست آوردن جوابی به‌صورت $2N^2$، بایستی m و n را مانند بالا انتخاب کنیم.

برای جوابهایی که به‌صورت N^2 یا $2N^2$ نیستند، فرض می‌کنیم $x=n^2m$ یا $x=2n^2m$، که در آن $n>1$ و n مقسوم‌علیه اولی به‌صورت $4k+1$ ندارد، و تمام مقسوم‌علیه‌های اول m به‌صورت $4k+1$ هستند. سپس لازم داریم که $N(m)=40$. از (۱۱.۸) نتیجه می‌شود که $m=p^9$ یا $m=p^4q$، که p و q اعداد اولی متمایز به‌صورت $4k+1$ هستند.

۵۷.۸ اثبات یا رد کنید: اگر هر یک از m و n نمایش اولیه‌ای به‌صورت مجموع دو مربع داشته باشد، mn نیز یک نمایش اولیه دارد.

حل. یافتن یک مثال نقض آسان است. فرض کنیم $m=n=2$؛ در این‌صورت m و n یک نمایش اولیه دارند، ولی mn نمایش اولیه‌ای ندارد. در واقع می‌توانیم تمام مثالهای نقض را مشخص کنیم. بنابر (۱۵.۸)، یک عدد صحیح دارای یک نمایش اولیه است اگر و تنها اگر بر ۴ یا بر هر عدد اول به‌صورت $4k+3$ بخشپذیر نباشد. لذا اگر m و n یک نمایش اولیه داشته باشند، ولی mn نداشته باشد، بایستی به این دلیل باشد که mn بر ۴ بخشپذیر است. بنابراین هر یک از m و n در برابر حاصلضربی اعداد اول به‌صورت $4k+1$ هستند.

۵۸.۸ فرض می‌کنیم هر یک از اعداد صحیح $m>2$ و $n>2$ دارای نمایش اولیه‌ای به‌صورت مجموع دو مربع باشند. اگر $(m,n)=1$، ثابت کنید که mn دارای حداقل دو نمایش اولیه الزاماً متمایز است.

حل. فرض کنیم m دارای r مقسوم‌علیه اول متمایز به‌صورت $4k+1$ و n دارای s چنین مقسوم‌علیهی باشد. چون m و n نمایشهای اولیه دارند، در نتیجه $r\geq 1$ و $s\geq 1$. چون $(m,n)=1$، پس mn دارای $r+s$ مقسوم‌علیه اول متمایز به‌صورت $4k+1$ است، و از (۱۸.۸) نتیجه می‌شود که mn دارای 2^{r+s-1} نمایش اولیهٔ الزاماً متمایز است. آشکار است که این عدد حداقل ۲ است.

۵۹.۸ فرض می‌کنیم n عدد صحیحی به‌صورت $4k+1$، با $k>1$ باشد. ثابت کنید که n اول است اگر و تنها اگر n دقیقاً یک نمایش (صرف‌نظر از ترتیب و علامت جمله‌ها) به‌صورت مجموع دو مربع داشته باشد و آن نمایش اولیه است.

حل. فرض می‌کنیم n عدد اولی به‌صورت $4k+1$ باشد. لذا بنابر (۹.۸)، n دارای یک نمایش به‌صورت مجموع دو مربع است، و روشن است که هر نمایش n اولیه است. بنابر (۱۱.۸)، $N(n)=8$، لذا n الزاماً تنها یک نمایش دارد.

بعکس، فرض می‌کنیم n فقط دارای نمایشهای اولیه‌ای به‌صورت مجموع دو مربع باشد. در این‌صورت n خالی از مربع است، زیرا اگر $n=c^2m$ که $c>1$، آنگاه می‌توانیم یک نمایش غیراولیه برای n از یک نمایش m تولید کنیم. (بنابر (۹.۸)، m دارای یک نمایش است.) لذا اگر n به‌صورت $4k+1$ باشد، بایستی حاصلضربی از اعداد اول به‌صورت $4k+1$ باشد. اما اگر این چنین n اول نباشد، حداقل دارای دو عامل اول متمایز است، و لذا (۱۱.۸) ایجاب می‌کند که $N(n)\geq 16$. در نتیجه اگر n فقط نمایشهای اولیه داشته باشد و الزاماً فقط یکی، آنگاه n اول است.

۶۰.۸ فرض می‌کنیم $n>2$ قابل نمایش به‌صورت مجموع دو مربع باشد. ثابت کنید که هر نمایش n اولیه است اگر و تنها اگر $n=p_1p_2\cdots p_r$ یا $n=2p_1p_2\cdots p_r$، که در آن هر p_i عدد اولی به‌صورت $4k+1$ است.

حل. ابتدا نشان می‌دهیم که اگر n به یکی از دو صورت فوق مشخص شده باشد، هر نمایش n اولیه است. زیرا فرض می‌کنیم $n=a^2+b^2$، و $d=(a,b)$؛ لذا $d^2|n$. چون روشن است که هیچ مربعی بزرگتر از ۱ مقسوم‌علیه $p_1p_2\cdots p_r$ یا $2p_1p_2\cdots p_r$ نیست، در نتیجه $d=1$.

حال فرض کنیم هر نمایش n اولیه باشد. بنابر (۱۵.۸)، n بر ۴ یا بر هر عدد اولی به‌صورت $4k+3$ بخشپذیر نیست. همچنین، n خالی از مربع است. زیرا اگر $n=c^2m$، که $c>1$، آنگاه m نمایش $m=a^2+b^2$ به‌صورت مجموع دو مربع دارد، زیرا m هیچ عامل اولی به‌صورت $4k+3$ ندارد. اما در این‌صورت $n=(ca)^2+(cb)^2$ یک نمایش غیراولیهٔ n است. لذا n حاصلضرب اعداد اول متمایز است، و قضیه ثابت می‌شود.

۶۱.۸ فرض می‌کنیم n دارای نمایشهای اولیه‌ای به‌صورت مجموع دو مربع باشد. مستقیماً ثابت کنید که n نمی‌تواند بر ۴ یا بر هر عدد به‌صورت $4k+3$ بخشپذیر باشد.

حل. فرض می‌کنیم $n=a^2+b^2$. اگر n بر ۴ بخشپذیر باشد، آنگاه a و b زوج هستند، زیرا مجموع دو مربع فرد همنهشت با ۲ به پیمانهٔ ۴ است. لذا a و b نسبت به هم اول نیستند، و از این‌رو نمایش $n=a^2+b^2$ اولیه نیست.

اگر n بر عددی به‌صورت $4k+3$ بخشپذیر باشد، آنگاه n بر عدد اولی به همین‌صورت بخشپذیر است. اما در این‌صورت بنابر (i.۶.۸)، $p|a$ و $p|b$، و مجدداً این نمایش، نمایش اولیه نیست.

۶۲.۸ اثبات یا رد کنید: اگر n فرد یا ۲ برابر یک عدد صحیح فرد باشد و تنها دارای عاملهای اول فردی به‌صورت $4k+1$ باشد، تمام نمایشهای n اولیه هستند.

حل. صحیح نیست. مثلاً $25 = 0^2 + 5^2$. در حالت کلی، اگر چنین عددی بر یک مربع بزرگتر از ۱ بخشپذیر باشد، آنگاه n یک نمایش دارد که اولیه نیست. زیرا فرض کنیم $n = c^2 m$ که $c > 1$، و فرض می‌کنیم $m = a^2 + b^2$ (چون m بر عدد اولی به‌صورت $4k+3$ بخشپذیر نیست دارای یک نمایش است). لذا $n = (ca)^2 + (cb)^2$ نمایشی از n است که اولیه نیست.

۶۳.۸ اگر n نمایش اولیه‌ای به‌صورت مجموع دو مربع داشته باشد، آیا هر مضرب n نیز یک نمایش اولیه خواهد داشت؟

حل. نَه. در واقع، اگر عدد اولی به‌صورت $4k+3$ با توان فرد در تجزیهٔ m ظاهر شود، mn هیچ نمایشی به‌صورت مجموع دو مربع نخواهد داشت. تولید یک مثال که در آن mn دارای یک نمایش باشد ولی هیچ نمایش اولیه نداشته باشد آسان است. مثلاً، بنابر (۱۵.۸)، می‌توانیم $m = 4$ (یا اگر n زوج باشد، $m = 2$) را اختیار کنیم.

۶۴.۸ اثبات یا رد کنید: اگر n دارای یک نمایش اولیه باشد و $d|n$، آنگاه d نیز یک نمایش اولیه دارد.

حل. اگر n دارای یک نمایش اولیه باشد، از (۱۵.۸) نتیجه می‌شود که n بر ۴ و بر هر عدد اولی به‌صورت $4k+3$ بخشپذیر نیست. اگر $d|n$، d نمی‌تواند بر ۴ یا بر عدد اولی به‌صورت $4k+3$ بخشپذیر باشد، و لذا بنابر (۱۵.۸)، d یک نمایش اولیه دارد.

۶۵.۸ آیا برای یک عدد صحیح n که هیچ نمایش اولیه ندارد، تساوی $N(n) = 44$ برقرار است؟ اگر هست، این n را بیابید. اگر نیست، چرا نیست.

حل. ابتدا عدد صحیح m را پیدا می‌کنیم که $N(m) = 44$؛ با توجه به (۱۱.۸)، می‌توانیم $m = 5^{10}$ را اختیار کنیم. فرض کنیم $n = 9 \times 5^{10}$؛ در این‌صورت (۱۱.۸) ایجاب می‌کند که $N(n) = 44$، اما بنابر (۱۵.۸)، n هیچ نمایش اولیه ندارد.

۶۶.۸ فرض می‌کنیم p عدد اولی به‌صورت $4k+1$ باشد، و $p = a^2 + b^2$. با استفاده از (۷.۸) مستقیماً ثابت کنید که p^2 یک نمایش اولیه به‌صورت مجموع دو مربع دارد.

حل. بنابر (۷.۸)، $p^۲ = (a^۲ + b^۲)^۲ = (۲ab)^۲ + (a^۲ - b^۲)^۲$، و اثبات تساوی $(۲ab, a^۲ - b^۲) = ۱$ دشوار نیست. زیرا اگر $d = (۲ab, a^۲ - b^۲)$، آنگاه $d^۲|p^۲$ و لذا d مساوی ۱ یا p است. اگر $d = p$، آنگاه $p|۲ab$ و لذا $p|a$ یا $p|b$. می‌توانیم فرض کنیم که $p|a$؛ چون $p|a^۲ - b^۲$، داریم $p|b^۲$ و لذا $p|b$. این با $(a, b) = ۱$ تناقض دارد، بنابراین $d = ۱$.

◁ **۶۷.۸** فرض می‌کنیم p عدد اولی به‌صورت $۴k + ۱$ باشد. با استفاده از (۱۱.۸) ثابت کنید که، صرف‌نظر از ترتیب و علامت جمله‌ها، p^n دقیقاً یک نمایش اولیه دارد.

حل. به‌ازای $n = ۱$، (۱۱.۸) ایجاب می‌کند که p^n الزاماً یک نمایش به‌صورت مجموع دو مربع داشته باشد؛ روشن است، که این نمایش اولیه است. حال فرض می‌کنیم $n \geq ۲$. بنابر (۱۱.۸)، p^n کلاً دارای $۴(n + ۱)$ نمایش، و $p^{n-۲}$ دارای $۴(n - ۱)$ نمایش است. هر نمایش از $p^{n-۲}$ یک نمایش از p^n را تولید می‌کند؛ اگر $p^{n-۲} = a^۲ + b^۲$، آنگاه $p^n = (pa)^۲ + (pb)^۲$. آشکار است که هیچ‌کدام از این نمایشها اولیه نیستند. همچنین، اگر $p^n = u^۲ + v^۲$ یک نمایش غیراولیه از p^n باشد، آنگاه بزرگترین مقسوم‌علیه مشترک u و v عدد p^n را می‌شمارد، و لذا u و v مضاربی از p هستند. بنابراین، هر نمایش غیراولیه از p^n به‌صورت $(pa)^۲ + (pb)^۲$ است، که در آن $a^۲ + b^۲ = p^{n-۲}$. در نتیجه p^n دارای دقیقاً $۴(n - ۱)$ نمایش غیراولیه است. لذا p^n دارای دقیقاً $۴(n + ۱) - ۴(n - ۱) = ۸$ نمایش اولیه است، یعنی، صرف‌نظر از علامت و ترتیب جمله‌ها، دقیقاً یک نمایش اولیه دارد.

۶۸.۸ اثبات یا رد کنید: هیچ عدد صحیحی به‌صورت $n^۲ - ۱$ نمایش اولیه ندارد.

حل. درست است. ملاحظه کنید که $n^۲ - ۱ \equiv ۰$ یا $۳ \pmod ۴$ برحسب آنکه n فرد یا زوج باشد. لذا اگر n فرد باشد $n^۲ - ۱$ بر ۴ بخشپذیر است، و اگر n زوج باشد، $n^۲ - ۱$ لااقل یک عامل اول به‌صورت $۴k + ۳$ دارد. در هر دو حالت، بنابر (۱۵.۸)، $n^۲ - ۱$ نمایش اولیه ندارد.

چهار مسأله بعد برهانی برای اثبات قضیهٔ ۱۱.۸ هستند. یادآور می‌شویم که $N(n)$ مقدار کل نمایشهای n به‌صورت مجموع دو مربع است.

۶۹.۸ فرض می‌کنیم $n = q^۲m$، که در آن $q = ۲$ یا q عدد اولی به‌صورت $۴k + ۳$ است. مستقیماً (بدون استفاده از (۱۱.۸)) نشان دهید که $N(n) = N(m)$.

حل. ابتدا فرض می‌کنیم که $q = ۲$. اگر $X^۲ + Y^۲ = m$ و $x = ۲X$، $y = ۲Y$، آنگاه $x^۲ + y^۲ = ۴m = n$. به‌علاوه، هر نمایش n به‌صورت مجموع دو مربع به این طریق تولید

می‌شود، زیرا اگر $x^۲ + y^۲ = n$، آنگاه چون $n \equiv ۰ \pmod ۴$، x و y باید زوج باشند. لذا اگر قرار دهیم $x = ۲X$ و $Y = ۲y$، آنگاه $X^۲ + Y^۲ = n/۴ = m$. لذا یک تناظر ۱ـ۱ بین نمایشهای n و نمایشهای m وجود دارد، و بنابراین $N(n) = N(m)$. اگر q عدد اولی به‌صورت $۴k + ۳$ باشد، استدلال مشابه الزاماً کارساز است، زیرا اگر $x^۲ + y^۲ = n$ ، آنگاه بنابر (i.۶.۸)، q باید اعداد x و y را بشمارد.

۷۰.۸ فرض می‌کنیم m فرد باشد و $n = ۲m$. مستقیماً نشان دهید که $N(n) = N(m)$. (راهنمایی: توجه کنید که $X^۲ + Y^۲ = m$ اگر و تنها اگر $(X + Y)^۲ + (X - Y)^۲ = n$.)

حل. چون $(X+Y)^۲+(X-Y)^۲ = ۲X^۲+۲Y^۲$، هر جفت X و Y به‌طوری‌که $X^۲+Y^۲ = m$ یک جفت $X + Y$، $X - Y$ را مشخص می‌کنند به‌طوری که $(X + Y)^۲ + (X - Y)^۲ = n$. به‌علاوه، هر جفتِ x و y به‌طوری که $x^۲ + y^۲ = n$ به این طریق تولید می‌شود. زیرا، چون n دو برابر یک عدد فرد است، داریم $x^۲ + y^۲ \equiv ۲ \pmod ۴$، و لذا x و y فرد هستند. لذا اعداد صحیح X و Y که به‌طور یکتا تعیین می‌شوند وجود دارند به‌طوری که $X + Y = x$ و $X - Y = y$، یعنی، $X = (x + y)/۲$، $Y = (x - y)/۲$، و به‌آسانی بررسی می‌شود که $X^۲ + Y^۲ = m$. لذا یک تناظر ۱ـ۱ بین نمایشهای n و نمایشهای m وجود دارد و بنابراین $N(n) = N(m)$.

◁ **۷۱.۸** اگر x عدد صحیح مثبتی باشد، فرض می‌کنیم $\omega(x)$ معرف تعداد اعداد اول متمایزی باشد که x را می‌شمارند. فرض می‌کنیم n و d اعداد صحیح مثبتی باشند به‌طوری که $d^۲|n$. نشان دهید تعداد جفتهای مرتب x و y از اعداد صحیح مثبت به‌طوری که $(x, y) = d$ و $xy = n$ عبارت است از $۲^{\omega(n/d^۲)}$. با استفاده از این، ثابت کنید $\tau(n) = \sum ۲^{\omega(n/d^۲)}$، که در آن $\tau(n)$ تعداد مقسوم‌علیه‌های مثبت n، و مجموعیابی روی تمام اعداد صحیح d که $d^۲|n$ گرفته می‌شود. (راهنمایی: مسألهٔ ۲۶.۱ را ببینید.)

حل. اگر $(x, y) = d$ و $xy = n$، قرار می‌دهیم $X = x/d$ و $Y = y/d$. در این‌صورت X و Y نسبت به هم اول‌اند و $XY = n/d^۲$. بعکس، اگر اعداد صحیح مثبت متباین X و Y مفروض باشند به‌طوری که $XY = n/d^۲$، آنگاه با فرض $x = dX$ و $y = dY$، داریم $(x, y) = d$ و $xy = n$. لذا می‌خواهیم تعداد جفتهای متباین X و Y را به‌طوری که $XY = n/d^۲$ بشماریم. بنابر مسألهٔ ۲۶.۱، تعداد چنین جفتها برابر $۲^{\omega(n/d^۲)}$ است.

سرانجام، چون $۲^{\omega(n/d^۲)}$ جفتهای x و y را که $(x, y) = d$ و $xy = n$ می‌شمرد، لذا با

مجموعیابی این اعداد روی تمام dها که $d^۲|n$، تعداد کل جفتهای مرتب x و y که $xy=n$، یعنی، تعداد مقسوم‌علیه‌های n را می‌شمرد.

◁ **۷۲.۸** فرض می‌کنیم $\omega(x)$ مانند مسألهٔ قبل تعریف شده است. فرض می‌کنیم m حاصلضرب اعداد اولی به‌صورت $۴k+۱$ باشد. نشان دهید که تعداد جفتهای مرتب x و y از اعداد صحیح به‌طوری که $x^۲+y^۲=m$ برابر است با $۴\sum ۲^{\omega(m/d^۲)}$، که در آن مجموع روی تمام اعداد صحیح d به‌طوری که $d^۲|m$ گرفته می‌شود. این نتیجه و مسألهٔ قبل را برای اثبات قضیهٔ ۱۱.۸ به‌کار برید.

حل. فرض کنیم $d^۲|m$. جوابهای $x^۲+y^۲=m$ را به‌دست می‌آوریم به‌طوری که $(x,y)=d$ بدین‌ترتیب که اعداد متباین X و Y را که در $x^۲+Y^۲=m/d^۲$ صدق کنند انتخاب می‌کنیم و قرار می‌دهیم $x=dX$ و $y=dY$. اما، بنابر (۱۸.۸)، تعداد این قبیل جفتهای مرتب برابر است با $۴\times ۲^{\omega(m/d^۲)}$. مجموع این اعداد روی تمام dها تعداد کل نمایشهای m به‌صورت مجموع دو مربع را به‌دست می‌دهد. لذا $N(n)=۴\sum ۲^{\omega(m/d^۲)}$، که در آن مجموع روی تمام اعداد صحیح مثبت d که $d^۲|m$ گرفته می‌شود.

بنابر مسألهٔ قبل، $۴\sum ۲^{\omega(m/d^۲)}=۴\tau(m)$. فرض کنیم بتوان n را به‌صورت مجموع دو مربع نمایش داد، و می‌نویسیم $n=۲^a\prod p_i^{a_i}\prod q_i^{b_i}$، که در آن p_iها اعداد اول به‌صورت $۴k+۱$ و q_iها اعداد اول به‌صورت $۴k+۳$ هستند (لذا هر b_i زوج است). با استفادهٔ مکرر از مسألهٔ ۶۹.۸ و مسألهٔ ۷۰.۸ در صورت لزوم $N(n)=N(m)$ را به‌دست می‌آوریم، که $m=\prod p_i^{a_i}$. لذا $N(n)=۴\tau(m)=۴\prod(a_i+۱)$.

سه مسألهٔ بعد برهانی برای قضیهٔ ۱۲.۸ به‌دست می‌دهند.

◁ **۷۳.۸** فرض می‌کنیم $f(n)=D_۱(n)-D_۳(n)$، که $D_۱(n)$ و $D_۳(n)$ به‌ترتیب تعداد مقسوم‌علیه‌های n به‌صورت $۴k+۱$ و $۴k+۳$ هستند. با استفاده از تعریف $D_۱(n)$ و $D_۳(n)$ مستقیماً نشان دهید که $f(n)$ یک تابع ضربی است.

حل. بایستی ثابت کنیم اگر $(m,n)=۱$، آنگاه $f(mn)=f(m)f(n)$. هر مقسوم‌علیه mn مانند r به‌طور یکتا به‌صورت $r=de$ بیان می‌شود که $d|m$ و $e|n$. همچنین، r به‌صورت $۴k+۱$ است اگر و تنها اگر d و e هر دو به‌صورت $۴k+۱$ یا هر دو به‌صورت $۴k+۳$ باشند. بنابراین $D_۱(mn)=D_۱(m)D_۱(n)+D_۳(m)D_۳(n)$. همچنین،

$D_3(mn) = D_1(m)D_3(n) + D_3(m)D_1(n)$. لذا

$$\begin{aligned} f(mn) &= D_1(mn) - D_3(mn) \\ &= D_1(m)D_1(n) + D_3(m)D_3(n) - D_1(m)D_3(n) - D_3(m)D_1(n) \\ &= (D_1(m) - D_3(m))(D_1(n) - D_3(n)) = f(m)f(n) \end{aligned}$$

◁ **۷۴.۸** به‌ازای $n \geq 1$، قرار می‌دهیم $g(n) = N(n)/4$. با استفاده از (۱۱.۸) ثابت کنید $g(n)$ یک تابع ضربی است.

حل. بایستی ثابت کنیم اگر $(m,n) = 1$، آنگاه $g(mn) = g(m)g(n)$. ابتدا فرض می‌کنیم که عدد اولی به‌صورت $4k+3$ با توان فرد در تجزیه یکی از دو عدد صحیح m و n، مثلاً m، ظاهر شود؛ پس $g(m) = 0$. چون $(m,n) = 1$، همان عدد اول با توان فرد در تجزیهٔ mn می‌آید. بنابراین $g(mn) = 0$ و لذا $g(mn) = g(m)g(n)$.

اگر هیچ عدد اولی به‌صورت $4k+3$ با یک توان فرد در تجزیهٔ m یا n ظاهر نشود، آنگاه m، n و mn قابل نمایش به‌صورت مجموع دو مربع هستند. فرض کنیم m_1 و n_1، به‌ترتیب، حاصلضرب اعداد اول به‌صورت $4k+1$ باشند که m و n را می‌شمارند. بنابر (۱۱.۸)، $g(m) = g(m_1)$، $g(n) = g(n_1)$، و $g(mn) = g(m_1n_1)$. فرض می‌کنیم $m_1 = \prod p_i^{a_i}$ و $n_1 = \prod q_j^{b_j}$ تجزیه‌های m_1 و n_1 باشند. چون m_1 و n_1 نسبت به هم اول‌اند، اعداد اول p_i و q_j متمایزند. سپس از (۱۱.۸) نتیجه می‌شود که $g(m_1) = \prod(a_i+1)$، $g(n_1) = \prod(b_j+1)$، و $g(m_1n_1) = \prod(a_i+1)\prod(b_j+1)$. لذا $g(m_1n_1) = g(m_1)g(n_1)$، و بنابراین $g(mn) = g(m)g(n)$.

۷۵.۸ قضیهٔ ۱۲.۸ را ثابت کنید. (راهنمایی: از دو مسألهٔ قبل استفاده کنید.)

حل. فرض می‌کنیم $f(n) = D_1(n) - D_3(n)$ و $g(n) = N(n)/4$. نشان می‌دهیم که به‌ازای هر $n \geq 1$، $f(n) = g(n)$. فرض کنیم $n = \prod p_i^{a_i}$ تجزیهٔ n باشد. بنابر دو مسألهٔ قبل، f و g توابع ضربی هستند، و لذا

$$f(n) = \prod f(p_i^{a_i}), \qquad g(n) = \prod g(p_i^{a_i})$$

با این نشان دادن که به‌ازای هر p^a، $f(p^a) = g(p^a)$ برهان را کامل می‌کنیم.

اگر $p = ۲$، آنگاه $f(p^a) = ۱$ و $g(p^a) = ۱$. اگر p به‌صورت $۴k + ۱$ باشد، آنگاه $f(p^a) = a+۱$، و بنابر (۱۱.۸)، $g(p^a) = a+۱$. سرانجام، فرض می‌کنیم p به‌صورت $۴k+۳$ باشد. اگر a فرد باشد، آنگاه p^a، $(a+۱)/۲$ مقسوم‌علیه به‌صورت $۴k+۱$ و $(a+۱)/۲$ مقسوم‌علیه به‌صورت $۴k+۳$ دارد، و لذا $f(p^a) = ۰$. با استدلالی مشابه، اگر a زوج باشد، آنگاه $f(p^a) = ۱$. اما اگر a فرد باشد، آنگاه $N(p^a) = ۰$، حال آنکه اگر a زوج باشد، آنگاه $N(p^a) = ۴$، لذا مجدداً $f(p^a) = g(p^a)$.

مجموعهای سه و چهار مربع

۷۶.۸ تعداد کل نمایشهای ۳۶۰ به‌صورت مجموع چهار مربع را به‌دست آورید.

حل. می‌توانیم با فهرست کردن نمایشها مستقیماً به حل مسأله بپردازیم، اما آسانتر آن است که قضیهٔ ژاکوبی (۲۴.۸) را به‌کار بریم. چون $۳۶۰ = ۲^۳ \times ۳^۲ \times ۵$، $\sigma(n) = (۱+۲+۴+۸)(۱+۳+۹)(۱+۵) = ۱۱۷۰$. مجموع مقسوم‌علیه‌های ۳۶۰ که بر ۴ بخشپذیرند $۴\sigma(۹۰) = ۹۳۶$ است. لذا مجموع مقسوم‌علیه‌های ۳۶۰ که بر ۴ بخشپذیر نیستند ۲۳۴ است، و لذا ۳۶۰ دارای $۸ \times ۲۳۴ = ۱۸۷۲$ نمایش به‌صورت مجموع چهار مربع است.

۷۷.۸ عدد صحیح مثبتی پیدا کنید که دقیقاً پنج نمایش الزاماً مجزا به‌صورت مجموع چهار مربع غیرصفر داشته باشد.

حل. فرمول ژاکوبی یعنی (۲۴.۸) برای یافتن برد مناسب سودمند است، ولی شمارش پیچیده است، به دلیل اینکه تعداد صورتهای غیرالزامی نمایشها به اینکه چه تعداد مربع مساوی به‌کار رفته است بستگی دارد. اندکی تجسس نشان می‌دهد که، مثلاً، ۱۰۰ دارای پنج نمایش الزاماً متمایز به‌صورت مجموع مربعهای غیرصفر دارد: $۱+۹+۹+۸۱$، $۴+۱۶+۱۶+۶۴$، $۱+۱+۴۹+۴۹$، $۱+۲۵+۲۵+۴۹$، و $۲۵+۲۵+۲۵+۲۵$.

۷۸.۸ (الف) فرض می‌کنیم $n = a^۲ + b^۲ + c^۲ + d^۲$، که در آن a، b، c، و d اعداد صحیح غیرصفر متمایزند. با تغییر علامت و ترتیب جمله‌ها چه تعداد صورت می‌توان به‌دست آورد؟ (ب) چه اتفاق می‌افتد اگر a، b، c، و d غیرصفر باشند ولی همگی متمایز نباشند؟ (ج) چه می‌شود اگر a، b، c، و d متمایز باشند و دقیقاً یکی ۰ باشد؟

حل. (الف) بدون تغییر در ترتیب، می‌توان $۲^۴$ صورت تنها با تغییر علامت به‌دست آورد. با

هر صورت تغییر علامت، !۴ صورت از تغییر در ترتیب حاصل می‌شود، در نتیجه کل صورتها برابر است با ۳۸۴ = ۲۴ × ۱۶.

(ب) حال فرض می‌کنیم a، b، c، و d همگی متمایز نباشند. اگر دقیقاً دو تا برابر باشند، مثلاً $a = b$، آنگاه $\binom{۴}{۲}۲^۴ = ۱۹۲$ صورت وجود دارد، حال آنکه اگر $a = b$، و $c = d$ ولی $a \neq c$، آنگاه $\binom{۴}{۲}۲^۴ = ۹۶$ صورت وجود دارد. اگر دقیقاً سه تا برابر باشند، آنگاه $\binom{۴}{۱}۲^۴ = ۶۴$ صورت وجود دارد. و اگر $a = b = c = d$، آنگاه درست $۲^۴ = ۱۶$ صورت وجود دارد.

(ج) اگر a، b، c، و d متمایز باشند و دقیقاً یکی ۰ باشد، آنگاه $۲^۳ \times ۴! = ۱۹۲$ صورت وجود دارد.

◁ **۷۹.۸** عدد صحیح مثبتی پیدا کنید که تنها با دو روش بتوان آن را به‌صورت مجموع چهار مربع غیرصفر نمایش داد. (تغییر علامت و ترتیب جمعوندها را در نظر نمی‌گیریم.) (راهنمایی: (۲۴.۸) و مسألهٔ قبل را به‌کار برید.)

حل. چون وقتی می‌نویسیم $n = a^۲ + b^۲ + c^۲ + d^۲$، تغییر در علامت و ترتیب را در نظر نخواهیم گرفت، می‌توانیم فرض کنیم که $a \geq b \geq c \geq d \geq ۰$. برای ساده کردن مسأله، عدد n را جستجو می‌کنیم که بر ۴ بخشپذیر نباشد؛ لذا، بنابر (۲۴.۸)، تعداد کل نمایشها ۸ برابر مجموع مقسوم‌علیه‌های مثبت n است، یعنی، $M(n) = ۸\sigma(n)$. در جستجو برای نمایشهای n، باید حساب کنیم که بعضی مربعها ممکن است ۰ باشند یا بعضی مربعها تکراری باشند. ما تمام حالتهای ممکن را رسیدگی نمی‌کنیم، اما حالتهای زیر را در نظر می‌گیریم.

اگر $M(n) = ۷۶۸$، آنگاه امکان دارد که (i) تمام نمایشهای n شامل مربعهای مثبت متمایز باشند (بنابر مسألهٔ قبل، هر نمایش ۳۸۴ صورت دارد)؛ (ii) دقیقاً دو مربع از چهار مربع غیرصفر تکرار شوند؛ (iii) دقیقاً یک مربع ۰ است و سه‌تای دیگر متمایزند (هر نمایش در (ii) و (iii)، ۱۹۲ صورت تولید می‌کند). چون $M(n) = ۸\sigma(n)$، بایستی داشته باشیم $\sigma(n) = ۹۶$. فرض می‌کنیم $n = rs$، که $(r, s) = ۱$. چون σ ضربی است (توضیحِ بعد از (۲۰.۱) را ببینید)، داریم $\sigma(r)\sigma(s) = ۹۶$. چند احتمال وجود دارد.

نخست، اگر بنویسیم $۱۲ \times ۸ = ۹۶$، آنگاه داریم $\sigma(r) = ۸$، $\sigma(s) = ۱۲$ یعنی، $r = ۷$، $s = ۱۱$، و لذا $n = ۷۷$. نوشتن نمایشهای ۷۷ به‌صورت مجموع چهار مربع آسان است:

$$۷۷ = ۸^۲ + ۳^۲ + ۲^۲ + ۰^۲ = ۶^۲ + ۶^۲ + ۲^۲ + ۱^۲$$
$$= ۶^۲ + ۵^۲ + ۴^۲ + ۰^۲ = ۶^۲ + ۴^۲ + ۴^۲ + ۳^۲,$$

بنابر مسألهٔ قبل هر نمایش ۱۹۲ صورت دارد. لذا ۷۷ دارای دقیقاً دو نمایش الزاماً متمایز به‌صورت مجموع چهار مربع غیرصفر است. اگر $۳۲ \times ۳ = ۹۶$، داریم $r = ۲$، $s = ۳۱$، و لذا $n = ۶۲$. بررسی کنید که

$$۶۲ = ۶^۲ + ۵^۲ + ۱^۲ + ۰^۲ = ۷^۲ + ۳^۲ + ۲^۲ + ۰^۲ = ۶^۲ + ۴^۲ + ۳^۲ + ۱^۲.$$

در نمایش اول ۱۹۲ صورت دارند، و آخری ۳۸۴ (به جای مجموع ۷۶۸)، اما ۶۲ تنها یک نمایش به‌صورت مجموع چهار مربع غیرصفر دارد. و از $۲۴ \times ۴ = ۹۶$ داریم $r = ۳$، $s = ۲۳$، و لذا

$$n = ۶۹ = ۸^۲ + ۲^۲ + ۱^۲ + ۰^۲ = ۷^۲ + ۴^۲ + ۲^۲ + ۰^۲ = ۶^۲ + ۵^۲ + ۲^۲ + ۲^۲$$
$$= ۶^۲ + ۴^۲ + ۴^۲ + ۱^۲.$$

که هر نمایش دارای ۱۹۲ صورت است. لذا ۶۹ دقیقاً دو نمایش الزاماً متمایز به‌صورت مجموع چهار مربع غیر صفر دارد.

اکنون حالتی را در نظر می‌گیریم که $M(n) = ۸\sigma(n) = ۳۸۴ + ۱۹۲ = ۵۷۶$؛ لذا $\sigma(n) = ۷۲$. اگر بنویسیم $۲۴ \times ۳ = ۷۲$، داریم $r = ۲$، $s = ۲۳$، یعنی $n = ۴۶$. چون $۵^۲ + ۴^۲ + ۲^۲ + ۱^۲ = ۶^۲ + ۳^۲ + ۱^۲ + ۰^۲ = ۴۶$ (اولی با ۳۸۴ صورت و دومی با ۱۹۲)، نتیجه می‌شود که ۴۶ تنها یک نمایش به‌صورت مجموع مربعهای غیرصفر دارد. حال می‌نویسیم $۱۸ \times ۴ = ۷۲$؛ پس $r = ۳$، $s = ۱۷$، و لذا $n = ۵۱$. بررسی کنید که $۵۱ = ۵^۲ + ۴^۲ + ۳^۲ + ۱^۲ = ۷^۲ + ۱^۲ + ۱^۲ + ۰^۲ = ۵^۲ + ۵^۲ + ۱^۲ + ۰^۲$، که اولی ۳۸۴ صورت و دوتای دیگر ۹۶ صورت ($۲(۲^۴) = ۱۲$ تغییر ترتیب و $۲^۳$ تغییر علامت) دارند. لذا ۵۱ جواب نیست. سرانجام، می‌نویسیم $۱۲ \times ۶ = ۷۲$؛ پس $r = ۵$، $s = ۱۱$ و لذا $n = ۵۵$. توجه کنید که $۵۵ = ۷^۲ + ۲^۲ + ۱^۲ + ۱^۲ = ۵^۲ + ۵^۲ + ۲^۲ + ۱^۲$ (هرکدام با ۱۹۲ صورت) و $۵۵ = ۶^۲ + ۵^۲ + ۲^۲ + ۰^۲$ (با ۱۹۲ صورت: $۲^۳$ تغییر در علامت و $۴!$ تغییر در ترتیب). لذا ۵۵ دارای دقیقاً دو نمایش الزاماً متمایز به‌صورت مجموع چهار مربع غیرصفر دارد.

◁ **۸۰.۸** (الف) قضیهٔ ۲۳.۸ را ثابت کنید: هر $n > ۱۶۹$ مجموع پنج مربع غیرصفر است. (راهنمایی: از مربع بودن ۱۶۹ و نیز مجموع دو، سه، یا چهار مربع غیرصفر بودن استفاده کنید.)

(ب) نشان دهید که تعداد نامتناهی عدد صحیح مثبت وجود دارند که مجموع چهار مربع غیرصفر نیستند. (راهنمایی: نشان دهید که اگر $۸|n$ مجموع چهار مربع غیرصفر باشد، $۴|n$ نیز چنین است.)

حل. (الف) فرض می‌کنیم $k = n - ۱۶۹$. پس بنابر قضیهٔ لاگرانژ، اعداد صحیح a، b، c، d وجود دارند به‌طوری که $k = a^۲ + b^۲ + c^۲ + d^۲$. اگر اینها همگی غیرصفر باشند، آنگاه

$n = a^۲ + b^۲ + c^۲ + d^۲ + ۱۶۹$ به‌صورت مجموع پنج مربع غیرصفر نوشته شده است. اگر دقیقاً یکی از اعداد a، b، c، d (مثلاً d) صفر باشد آنگاه چون $۱۶۹ = ۲۵ + ۱۴۴$، داریم $n = a^۲ + b^۲ + c^۲ + ۲۵ + ۱۴۴$، مجموعی از پنج مربع غیرصفر. با استدلالی مشابه، می‌توانیم از $۱۶۹ = ۹ + ۱۶ + ۱۴۴$ و $۱۶۹ = ۱۶ + ۱۶ + ۱۶ + ۱۲۱$ برای مواردی که دو یا سه تا از a، b، c، d صفر هستند استفاده کنیم.

(ب) فرض می‌کنیم که $n \equiv ۰ \pmod ۸$ و $n = a_۱^۲ + a_۲^۲ + a_۳^۲ + a_۴^۲$ مجموعی از چهار مربع غیرصفر است. از آنجا که مربع هر عدد فرد همنهشت با ۱ به پیمانهٔ ۸ است، لذا اگر a_iها فرد باشند، داریم $\sum a_i^۲ \equiv ۴ \pmod ۸$. اگر دقیقاً دو a_i فرد باشند، آنگاه $\sum a_i^۲ \equiv ۲ \pmod ۴$. لذا، اگر $n \equiv ۰ \pmod ۸$ و $n = a_۱^۲ + a_۲^۲ + a_۳^۲ + a_۴^۲$، آنگاه همهٔ a_iها باید زوج باشند. قرار می‌دهیم $a_i = ۲A_i$. پس $n/۴ = A_۱^۲ + A_۲^۲ + A_۳^۲ + A_۴^۲$، و لذا $n/۴$ مجموع چهار مربع غیرصفر است. چون آشکار است که ۲ مجموع چهار مربع غیرصفر نیست، و در نتیجه ۸، ۳۲، ۱۲۸، ... نمی‌توانند به‌صورت مجموع چهار مربع غیرصفر بیان شوند. با استدلالی مشابه، چون ۶ نیز مجموع چهار مربع غیرصفر نیست، پس ۲۴، ۹۶، ۳۸۴، ... نیز چنین هستند.

۸۱.۸ اتحاد اویلر یعنی (۱۹.۸) را برای بیان ۸۰۵۰ به‌صورت مجموع چهار مربع به‌کار برید.

حل. داریم $۸۰۵۰ = ۲ \times ۵^۲ \times ۷ \times ۲۳$. روشن است که، کافی است $۲ \times ۷ \times ۲۳$ را به‌صورت مجموع چهار مربع بیان کنیم. داریم $۲۳ = ۱^۲ + ۲^۲ + ۳^۲ + ۳^۲$ و $۱۴ = ۰^۲ + ۱^۲ + ۲^۲ + ۳^۲$. از اتحاد اویلر با (در نمادگذاری (۱۹.۸)) $a = ۰$، $b = ۱$، $c = ۲$، $d = ۳$، و $A = ۱$، $B = ۲$، $C = ۳$، $D = ۳$ استفاده می‌کنیم. پس $r = ۱۷$، $s = -۴$، $t = ۱$، و $u = -۴$. از آنجا $۸۰۵۰ = ۸۵^۲ + ۲۰^۲ + ۵^۲ + ۲۰^۲$. چندین جواب دیگر نیز وجود دارند.

۸۲.۸ ثابت کنید که حاصلضرب دو عدد صحیح، که هر کدام مجموع سه مربع هستند، لزوماً مجموع سه مربع نیست. نشان دهید که این مطلب اغلب بی‌نهایت بار اتفاق می‌افتد. ((۲۵.۸) را به‌کار برید.)

حل. ۳ و ۵ هرکدام مجموع سه مربع هستند ولی ۱۵ نیست. در حالت کلی، اگر $m \equiv ۳ \pmod ۸$ و $n \equiv ۵ \pmod ۸$، آنگاه (۲۵.۸) ایجاب می‌کند که m و n هر دو مجموع سه مربع باشند، اما، حاصلضربشان، که به‌صورت $۸k + ۷$ است، نیست. (مثالهای دیگر: $m = ۲^a(۸s + ۳)$، $n = ۲^b(۸t + ۵)$، که در آن $a + b$ زوج است؛ و $m = ۲^a(۸s + ۱)$، $n = ۲^b(۸t + ۷)$، که a و b هر دو فردند.)

◁ **۸۳.۸** بدون استفاده از (۲۵.۸)، نشان دهید که هر عدد صحیح به‌صورت $۸k+۷$ نمی‌تواند به‌صورت مجموع سه مربع نوشته شود، با استفاده از این مطلب ثابت کنید اگر n به‌صورت $۴^m(۸k+۷)$ باشد، آنگاه n مجموع سه مربع نیست.

حل. هر عدد صحیح به پیمانه ۸ همنهشت با ۰، ۱، یا ۴ است. هیچ ترکیب سه‌تایی از اینها مجموعی همنهشت با ۷ به پیمانهٔ ۸ پدید نمی‌آورد. در نتیجه یک عدد صحیح به‌صورت $۸k+۷$ نمی‌تواند مجموع سه مربع باشد.

به استقرا بر m نشان می‌دهیم که $۴^m(۸k+۷)$ نمی‌تواند مجموع سه مربع باشد. محاسبهٔ بالا حالت $m=۰$ را دربر می‌گیرد. حال اگر $۴^s(۸k+۷)$ مجموع سه مربع نباشد، نشان می‌دهیم که $۴^{s+۱}(۸k+۷)$ مجموع سه مربع نیست. برعکس، فرض می‌کنیم که $۴^{s+۱}(۸k+۷)=a^۲+b^۲+c^۲$. در این‌صورت به‌ویژه $a^۲+b^۲+c^۲\equiv ۰ \pmod ۴$. به آسانی دیده می‌شود که a، b، و c باید زوج باشند. فرض کنیم $a=۲A$، $b=۲B$، و $c=۲C$. در این‌صورت $۴^{s+۱}(۸k+۷)=۴A^۲+۴B^۲+۴C^۲$، و بنابراین $۴^s(۸k+۷)=A^۲+B^۲+C^۲$، و این تساوی با این فرض که $۴^s(۸k+۷)$ مجموع سه مربع نیست، تناقض دارد.

۸۴.۸ (فرما، ۱۶۳۶) نشان دهید که هیچ عدد صحیح به‌صورت $۸k+۷$ را نمی‌توان به‌صورت مجموع سه مربع از اعداد گویا بیان کرد.

حل. فرض می‌کنیم n به‌صورت $۸k+۷$ باشد و $n=r^۲+s^۲+t^۲$، که در آن r، s، و t اعداد گویا هستند. فرض می‌کنیم $r=a/d$، $s=b/d$، و $t=c/d$، که a، b، c، و $d>۰$ اعداد صحیح هستند. پس $nd^۲=a^۲+b^۲+c^۲$. فرض کنیم $d=۲^e q$، که q فرد است؛ پس $nd^۲=۲^{۲e}q^۲$. چون $q^۲\equiv ۱ \pmod ۸$، داریم $nq^۲\equiv ۷ \pmod ۸$؛ همچنین، $۲^{۲e}$ توانی از ۴ است. لذا $nd^۲$ نمی‌تواند به‌صورت مجموع مربعات سه عدد صحیح بیان شود ((۲۵.۸) و مسألهٔ ۸۳.۸ را ببینید)، و این با $nd^۲=a^۲+b^۲+c^۲$ تناقض دارد.

۸۵.۸ اثبات یا رد کنید: اگر $n\geq ۱$، آنگاه یا n مجموع سه مربع است یا $۲n$.

حل. روشن است که، حداقل یکی از دو عدد n یا $۲n$ به‌صورت $۴^m(۸k+۷)$ نیست. اما بنابر (۲۵.۸)، هر عدد که به این‌صورت نباشد مجموع سه مربع است، و قضیهٔ حاصل.

۸۶.۸ با استفاده از قضیهٔ گاوس در مجموعهای سه مربع (قضیهٔ ۲۵.۸)، ثابت کنید که هر عدد صحیح فرد را می‌توان به‌صورت مجموع سه مربع، که یکی از آنها ۰ یا ۱ است، نوشت.

حل. فرض می‌کنیم که n یک عدد صحیح فرد مثبت باشد. اگر n به‌صورت $4K = 1$ باشد، آنگاه (۲۵.۸) ایجاب می‌کند که n مجموع سه مربع باشد و لذا مجموع چهار مربع است، که یکی از آنها ۰ است. اگر n به‌صورت $4k + 3$ باشد، (۲۵.۸) ایجاب می‌کند که $n - 1$ مجموع سه مربع باشد، و لذا n چهار مربع است، که یکی از آنها ۱ است.

۸۷.۸ با استفاده از قضیهٔ (۲۵.۸) ثابت کنید که هر عدد صحیح مثبت فرد به‌صورت $r^2 + s^2 + 2t^2$ است. (راهنمایی: ابتدا نشان دهید که به‌ازای هر n عدد $4n + 2$ مجموع سه مربع است که دقیقاً دو تای آنها فردند.)

حل. فرض می‌کنیم n یک عدد صحیح مثبت باشد؛ لذا روشن است که $4n + 2$ به‌صورت $4^m(8k + 7)$ نیست. لذا بنابر (۲۵.۸)، می‌توانیم بنویسیم $4n + 2 = a^2 + b^2 + c^2$. اعداد صحیح a، b، و c همگی نمی‌توانند زوج باشند، زیرا $4n + 2$ بر ۴ بخشپذیر نیست؛ لذا دقیقاً دو تا از a، b، و c فردند. بنابراین فرض می‌کنیم a و b فرد باشند و c زوج باشد، مثلاً، $c = 2t$؛ لذا $a + b$ و $a - b$ زوج‌اند. اگر $a + b = 2r$ و $a - b = 2s$، آنگاه $a = r + s$ و $b = r - s$. در نتیجه، $4n + 2 = (r + s)^2 + (r - s)^2 + 4t^2 = 2r^2 + 2s^2 + 4t^2$، و لذا $2n + 1 = r^2 + s^2 + 2t^2$.

۸۸.۸ با استفاده از قضیهٔ گاوس در مجموع سه مربع ثابت کنید که هر عدد صحیح فرد را می‌توان به‌صورت $r^2 + s^2 + t^2 + (t + 1)^2$ نوشت. (راهنمایی: به‌ازای $n \geq 1$، نشان دهید که $4n + 1 = a^2 + b^2 + c^2$ که c فرد است، مثلاً $c = 2t + 1$. اکنون $2n + 1$ را برحسب a، b، و t بیان کنید.)

حل. به‌ازای هر $n \geq 0$، بنابر (۲۵.۸)، $4n + 1$ مجموع سه مربع است. فرض می‌کنیم $4n + 1 = a^2 + b^2 + c^2$؛ در این‌صورت دقیقاً یکی از a، b، و c فرد است، زیرا هر مربع به پیمانه ۴ همنهشت با ۰ یا ۱ است. فرض کنیم $a = 2u$، $b = 2v$، $c = 2t + 1$؛ در این‌صورت به آسانی بررسی می‌شود که عدد فرد $2n + 1$ مجموع مربعات $u + v$، $u - v$، t، و $t + 1$ است.

۸۹.۸ ثابت کنید بی‌نهایت عدد اول p وجود دارد که می‌توان p را به‌صورت $a^2 + b^2 + c^2 + 1$ نمایش داد.

حل. بی‌نهایت عدد اول به‌صورت $4k + 3$ وجود دارد. اگر p یکی از آنها باشد، آنگاه $p - 1$ به‌صورت $4K + 2$ است و لذا به‌صورت $4^m(8k + 7)$ نیست. از این‌رو، بنابر (۲۵.۸)، $p - 1$ مجموع سه مربع است، که قضیه را ثابت می‌کند.

◁ **۹۰.۸** (اویلر، ۱۷۶۳) فرض می‌کنیم p عدد اولی به‌صورت $8k+1$ یا $8k+3$ باشد. با استدلالی مشابه با برهان (۸.۸) ثابت کنید که اعداد صحیح a و b وجود دارند به‌طوری که $p = 2a^2 + b^2$. به‌ویژه، p مجموع سه مربع است. (راهنمایی: توجه کنید که $(-2/p) = 1$ اگر و تنها اگر $p \equiv 1, 3 \pmod 8$.)

حل. بنابر (i.۱۳.۵)، -2 یک ماندهٔ درجهٔ دوم p است، و لذا عدد صحیح s وجود دارد به‌طوری که $s^2 \equiv -2 \pmod p$. اعداد صحیح $sx - y$ را که در آن $0 \le x, y < \sqrt{p}$ در نظر می‌گیریم. تعداد $[\sqrt{p}] + 1$ انتخاب برای هرکدام از x و y وجود دارد، و چون $([\sqrt{p}]+1)^2 > (\sqrt{p})^2 = p$، لااقل دو مقدار از $sx - y$ همنهشت به پیمانهٔ p هستند، مثلاً $sx_1 - y_1 \equiv sx_2 - y_2 \pmod p$. فرض می‌کنیم $a = x_1 - x_2$ و $b = y_1 - y_2$: در این‌صورت a و b هر دو نمی‌توانند 0 باشند زیرا جفتهای مرتب (x_1, y_1) و (x_2, y_2) مجزا هستند. چون $sa \equiv b \pmod p$، نتیجه می‌شود که $s^2a^2 \equiv b^2 \pmod p$، یعنی، $-2a^2 \equiv b^2 \pmod p$. لذا $2a^2 + b^2$ مضرب مثبتی از p است، و چون $3p = 3(\sqrt{2})^2$، $2a^2 + b^2 < 3(\sqrt{2})^2$، بایستی داشته باشیم $2a^2 + b^2 = p$ (در این حالت مسأله ثابت شده است) یا $2a^2 + b^2 = 2p$. در حالت دوم، b زوج است؛ اگر $b = 2c$، آنگاه $2p = 2a^2 + (2c)^2$، یعنی، $p = a^2 + 2c^2$.

۹۱.۸ اثبات یا رد کنید: اگر عدد اول فرد p به‌صورت $2a^2 + b^2$ باشد، آنگاه $p \equiv 1 \pmod 8$ یا $p \equiv 3 \pmod 8$.

حل. درست است. اگر $2a^2 + b^2$ فرد باشد، آنگاه b فرد است، لذا $b^2 \equiv 1 \pmod 8$. همچنین، چون هر مربع به پیمانهٔ ۸ همنهشت با 0، 1، یا 4 است، در نتیجه $2a^2 \equiv 0, 2 \pmod 8$. لذا $2a^2 + b^2$ یا $3 \pmod 8$.

۹۲.۸ با استفاده از قضیهٔ گاوس در مورد مجموعهای سه مربع ثابت کنید که هر عدد صحیح مثبت مجموع چهار مربع است.

حل. با توجه به (۲۵.۸)، کافی است نشان دهیم که اگر $n = 4^m(8k+7)$، آنگاه n مجموع چهار مربع است. اما، $n - 4^m = 4^m(8k+6)$، لذا بنابر (۲۵.۸)، $n - 4^m$ مجموع سه مربع است. فرض کنیم $n - 4^m = a^2 + b^2 + c^2$؛ لذا $n = a^2 + b^2 + c^2 + (2^m)^2$.

۹۳.۸ تعمیم زیر از (۲۱.۸) را ثابت کنید: همنهشتی $x^2 + y^2 + 1 \equiv 0 \pmod m$ حلپذیر است اگر و تنها اگر $4 \nmid m$.

حل. اگر $4|m$ و $a^2+b^2+1\equiv 0 \pmod m$، آنگاه $a^2+b^2+1\equiv 0 \pmod 4$، که ممکن نیست، زیرا هر مربع به پیمانهٔ ۴ همنهشت با ۰ یا ۱ است.

حال فرض می‌کنیم که $4 \nmid m$. می‌نویسیم $m=2^{k_0}p_1^{k_1}\cdots p_r^{k_r}$، که $k_0=0$ یا $k_0=1$ و p_i اعداد اول فرد متمایزند؛ اگر $k_0=1$، فرض می‌کنیم $p_0=2$. نشان می‌دهیم که به‌ازای هر i، اعداد a_i و b_i وجود دارند به‌طوری که $a_i^2+b_i^2+1\equiv 0 \pmod{p_i^{k_i}}$. قضیه برای p_0 بدیهی است، لذا کافی است نشان دهیم که به‌ازای هر عدد اول p_i، همنهشتی $x^2+y^2+1\equiv 0 \pmod{p_i^{k_i}}$ جواب دارد. بنابر (۲۱.۸)، اعداد صحیح a_i و y_i وجود دارند به‌طوری که $a_i^2+y_i^2+1\equiv 0 \pmod{p_i}$. چون همنهشتی $y^2\equiv -(a_i^2+1) \pmod{p_i}$ جواب دارد، از (۴.۵) نتیجه می‌شود که به‌ازای هر i، همنهشتی $y^2\equiv -(a_i^2+1) \pmod{p_i^{k_i}}$ جواب دارد، و به‌ویژه، عدد صحیح b_i وجود دارد به‌طوری که $a_i^2+b_i^2+1\equiv 0 \pmod{p_i^{k_i}}$.

حال، مانند برهان (۲۱.۸)، با استفاده از قضیهٔ باقیماندهٔ چینی اعداد صحیح a و b را به‌دست می‌آوریم به‌طوری که به‌ازای هر i، $a\equiv a_i \pmod{p_i^{k_i}}$ و $b\equiv b_i \pmod{p_i^{k_i}}$. لذا $a^2+b^2+1\equiv 0 \pmod m$.

در مسألهٔ بعد برهان دیگری است برای اینکه هر عدد صحیح مثبت مجموع چهار مربع است. همان‌گونه که در بند بعد از (۱۹.۸) مشخص شد، کافی است نشان دهیم که هر عدد اول q به‌صورت $4k+3$ مجموع چهار مربع است. راه اثبات آن است که نشان دهیم یک مضرب مثبت q مجموع چهار مربع است و سپس استدلال کنیم که کوچکترین مضرب مثبت q که مجموع چهار مربع باشد خود q است. با برهانی شبیه به برهان قضیهٔ دو مربع که در مسألهٔ ۴۸.۸ ارائه گردید، توجه شود.

◁ **۹۴.۸** فرض می‌کنیم q عدد اولی است به‌صورت $4k+3$. ثابت کنید اعداد صحیح a و b وجود دارند به‌طوری که $a^2+b^2+1\equiv 0 \pmod q$، با این فرض که $a^2\equiv h-1 \pmod q$، که در آن h کوچکترین ناماندهٔ درجهٔ دوم مثبت q است. به‌ویژه نشان دهید که عدد صحیح r با $0<r<q$ وجود دارد به‌طوری که rq مجموع چهار مربع است.

حل. فرض می‌کنیم h کوچکترین ناماندهٔ درجهٔ دوم مثبت q باشد. پس $h\geq 2$، و چون $h-1$ یک ماندهٔ درجهٔ دوم q است، عدد صحیح a با $0<a<q/2$ وجود دارد به‌طوری که $a^2\equiv h-1 \pmod q$. بنابر (۱۱.۵)، -1 یک ناماندهٔ درجهٔ دوم q است؛ لذا $(-h/q)=(-1/q)(h/q)=1$. بنابراین، عدد صحیح b با $0<b<q/2$ وجود دارد به‌طوری که $b^2\equiv -h \pmod q$. در نتیجه $a^2+b^2+1\equiv (h-1)+(-h)+1\equiv 0 \pmod q$. لذا عدد صحیح r وجود دارد به‌طوری که $a^2+b^2+1=rq$، و بنابراین rq مجموع چهار (در

واقع، سه) مربع است. چون $0 < a^2 + b^2 + 1 < 2(q/2)^2 + 1 < q^2$، نتیجه می‌گیریم که $0 < r < q$.

◁ **۹۵.۸** نشان دهید که هر عدد اول به‌صورت $4k + 3$ مجموع چهار مربع است.

حل. فرض می‌کنیم q عدد اولی به‌صورت $4k + 3$ باشد. فرض می‌کنیم m کوچکترین عدد صحیح مثبتی باشد که mq مجموع چهار مربع است، مثلاً $mq = a^2 + b^2 + c^2 + d^2$. لذا بنابر مسألهٔ ۹۴.۸، $0 < m < q$؛ نشان می‌دهیم که $m = 1$.

اگر m زوج باشد، آنگاه یا ۰، ۲، یا ۴ تا از اعداد a، b، c، d زوج هستند؛ اگر دقیقاً دو تا زوج باشند، می‌توانیم فرض کنیم که آنها a و b هستند. لذا در هر سه حالت، $a \pm b$ و $c \pm d$ زوج هستند؛ بنابراین

$$(m/2)q = ((a+b)/2)^2 + ((a-b)/2)^2 + ((c+d)/2)^2 + ((c-d)/2)^2$$

که با مینیمال بودن m تناقض دارد. لذا m زوج نیست.

حال فرض می‌کنیم m فرد باشد؛ اگر $m \neq 1$، آنگاه $3 \leq m < q$. اعداد صحیح a، b، c، d به پیمانهٔ m با اعداد صحیح A، B، C، D همنهشت هستند، اعداد اخیر از دستگاه کامل مانده‌ها متشکل از اعداد صحیح x انتخاب شده‌اند به‌طوری که $-(m-1)/2 \leq x \leq (m-1)/2$؛ لذا اعداد A، B، C، و D از لحاظ قدرمطلق از $m/2$ کوچکترند. در این‌صورت،

$$A^2 + B^2 + C^2 + D^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$$

و بنابراین،

$$A^2 + B^2 + C^2 + D^2 = km \quad \text{با} \quad 0 \leq km < 4(m/2)^2 = m^2$$

لذا $0 \leq k < m$. اگر $k = 0$، آنگاه $A = B = C = D = 0$، و m اعداد a، b، c، و d را می‌شمارد؛ از این‌رو $m^2 | mq$، یعنی، $m | q$، که یک تناقض است، زیرا $m < q$. بنابراین، $k > 0$. لذا

$$\begin{aligned} m^2 kq = (mq)(km) &= (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ &= r^2 + s^2 + t^2 + u^2 \end{aligned} \tag{۱}$$

که در آن r، s، t، و u مانند برهان (۱۹.۸) تعریف شده‌اند. چون

$$A \equiv a, B \equiv b, C \equiv c, D \equiv d \pmod{m}$$

در نتیجه r، s، t، و u بر m بخشپذیرند. مثلاً،

$$t = aC - bD - cA + dB \equiv ac - bd - ca + db \equiv ۰ \pmod m$$

با تقسیم (۱) بر $m^۲$ داریم

$$kq = (r/m)^۲ + (s/m)^۲ + (t/m)^۲ + (u/m)^۲$$

که $۰ < k < m$. این روابط با این واقعیت که mq کوچکترین مضرب q است که مجموع چهار مربع است تناقض دارد. لذا $m = ۱$، و برهان کامل است.

مسألهٔ وِرینگ

◁ **۹۶.۸** (یوهانس اویلر، ۱۷۷۲) فرض می‌کنیم که $g(k)$ کوچکترین تعداد توانهای k باشد که برای نمایش هر عدد صحیح مثبت لازم است. ثابت کنید به‌ازای هر $k \geq ۲$، $g(k) \geq ۲^k + [(۳/۲)^k] - ۲$. (راهنمایی: فرض کنید $n = ۲^k[(۳/۲)^k] - ۱$، و تعداد توانهای kام را که برای نمایش n لازم است پیدا کنید.)

حل. فرض می‌کنیم $q = [(۳/۲)^k]$. چون $q < (۳/۲)^k$، نتیجه می‌شود که $n = ۲^k q - ۱ < ۳^k$. لذا برای نمایش n به‌صورت مجموع توانهای kام، تنها می‌توانیم ۱^k و ۲^k را به‌کار بریم. آشکار است که، مینیمم تعداد توانهای kام مورد نیاز، کاربرد همان تعدادِ ممکن ۲^k، یعنی، $q - ۱$ را ایجاب می‌کند. از آنجا $n - ۲^k(q - ۱) = ۲^k - ۱$ تعداد برای نمایش می‌ماند، که آشکارا $۲^k - ۱$ تعداد ۱^k را ایجاب می‌کند. بنابراین حداقل $(q - ۱) + (۲^k - ۱) = ۲^k + [(۳/۲)^k] - ۲$ توان kام برای نمایش n لازم داریم.

۹۷.۸ با این اثبات که اگر $n \equiv ۴ \pmod ۹$ یا $n \equiv ۵ \pmod ۹$، آنگاه n هیچ نمایشی به‌صورت مجموع کمتر از چهار مکعب ندارد، ثابت کنید $g(۳) \geq ۴$.

حل. با در نظر گرفتن $۰^۳$، $۱^۳$، ...، $۸^۳$، می‌توانیم ثابت کنیم که هر مکعب به پیمانهٔ ۹ با ۰، ۱، یا -۱ همنهشت است. مجموع مکعبهایی که a مکعب همنهشت با ۱ به پیمانه ۹، b مکعب همنهشت با -۱، و احتمالاً تعدادی مکعب همنهشت با ۰ دارند، همنهشت با $a - b$ به پیمانهٔ ۹ است. به آسانی دیده می‌شود که ۴ کوچکترین مقدار $a + b$ است که به‌ازای آن $a - b \equiv ۴ \pmod ۹$ و همچنین، کوچکترین مقدار برای آنکه $a - b \equiv ۵ \pmod ۹$.

۹۸.۸ ثابت کنید تعداد نامتناهی عدد صحیح مثبت وجود دارند که نمی‌توانند به‌صورت مجموع کمتر از ۱۵ توان چهارم نمایش داده شوند. (راهنمایی: مانده‌های توانهای چهارم به پیمانهٔ ۱۶ را در نظر بگیرید.)

حل. آشکار است که اگر x زوج باشد، آنگاه $x^۴ \equiv ۰ \pmod{۱۶}$؛ اگر x فرد باشد، آنگاه $x^۴ \equiv ۱ \pmod{۱۶}$. می‌توان این مطلب را به چند طریق بررسی کرد، مثلاً، بسط $(۲y+۱)^{۱۶}$ با استفاده از قضیهٔ دو جمله‌یی، یا به‌طور ساده‌تر، توجه به اینکه $۱^۴$، $۳^۴$، $۵^۴$، و $۷^۴$ هرکدام همنهشت با ۱ به پیمانهٔ ۱۶ هستند.

فرض می‌کنیم n را به‌صورت مجموع توانهای چهارم، با استفاده از دقیقاً k توان چهارم از اعداد صحیح فرد (و احتمالاً توانهای چهارم از تعدادی عدد صحیح زوج) بیان کرده‌ایم. در این‌صورت $n \equiv k \pmod{۱۶}$. به‌ویژه، اگر $n \equiv ۱۵ \pmod{۱۶}$، آنگاه نمی‌توان n را با کمتر از ۱۵ توان چهارم نمایش داد.

توضیح. ۱. می‌توان قضیهٔ بالا را قدری بهتر کرد. به استقرا بر m می‌توانیم نشان دهیم که اگر $n = ۳۱ \times ۱۶^m$، آنگاه n تعداد ۱۶ توان چهارم لازم دارد. روشن است که به‌ازای $m = ۰$ صادق است. نشان می‌دهیم که اگر به‌ازای $m = k$ برقرار باشد برای $m = k+۱$ نیز برقرار است. فرض کنیم $m = ۳۱ \times ۱۶^{k+۱}$. اگر در نمایش n فقط اعداد فردی را به‌کار بریم، بایستی حداقل ۱۶ تا به‌کار بریم. اگر تنها اعداد زوج را به‌کار بریم، تمام توانهای چهارم آنها بر ۱۶ بخشپذیرند. لذا نمایشی از ۳۱×۱۶^k به‌صورت مجموع توانهای چهارم به‌دست می‌آوریم، و بنابر فرض استقرا چنین نمایشی حداقل ۱۶ توان چهارم لازم دارد.

۲. مقدار $g(k)$ بیش از حد تحت تأثیر ویژگیهای اتفاقی اعداد صحیح کوچک قرار می‌گیرد. $G(k)$ را به‌عنوان کوچکترین عدد صحیح s تعریف می‌کنیم به‌طوری که بتوان هر عدد صحیح به‌قدر کافی بزرگ را به‌صورت مجموع s یا کمتر از s توان kام مثبت نمایش داد. واضح است که $G(k) \le g(k)$. به‌طور کلی، ثابت می‌شود که $G(k)$ اساساً کوچکتر از $g(k)$ است. استدلال بالا نشان می‌دهد که $G(۴) \ge ۱۶$. داونپورت[1] در ۱۹۳۹ ثابت کرد که، در واقع، $G(۴) = ۱۶$.

◁ **۹۹.۸** (الف) اگر $p > ۳$ اول باشد، نشان دهید که به‌ازای هر $n \ge ۱$، p^n نمی‌تواند مجموع دو مکعب مثبت باشد. (ب) اگر $p = ۲$ یا $p = ۳$ چه اتفاقی می‌افتد؟

حل. (الف) برهان با روش نزول (استقرا) صورت می‌گیرد. اگر توانی از p وجود داشته باشد که مجموع دو مکعب مثبت باشد، آنگاه توان کوچکتری از p با این ویژگی وجود دارد. فرض کنیم

1. Davenport

$p^n = a^۳ + b^۳$. چون $a^۳ + b^۳ = (a+b)(a^۲ - ab + b^۲)$، در نتیجه k وجود دارد به‌طور کلی که $a + b = p^k$ و $a^۲ - ab + b^۲ = p^{n-k}$. در این‌صورت $k > ۰$، زیرا a و b مثبت هستند، و $k < n$، زیرا $a^۳ + b^۳ > a + b$ مگر آنکه $a = b = ۱$.

چون $۰ < k < n$ و $۳ab = (a+b)^۲ - (a^۲ - ab + b^۲) = p^{۲k} - p^{n-k}$، در نتیجه $p|۳ab$. چون $p > ۳$، پس p یا a را می‌شمارد یا b را، مثلاً $p|a$؛ در این‌صورت $a + b = p^k$ ایجاب می‌کند که $p|b$. فرض کنیم $a = pA$ و $b = pB$؛ در این‌صورت، به آسانی دیده می‌شود که $A^۳ + B^۳ = p^{n-۳}$. این تساوی با انتخاب n به‌عنوان کوچکترین عدد صحیحی که p^n مجموع دو مکعب مثبت است تناقض دارد.

(ب) فرض می‌کنیم $p = ۲$. با همان روش می‌توانیم نشان دهیم که $a^۳ + b^۳ = ۲^n$ ایجاب می‌کند که a و b بر ۲ بخشپذیر باشند مگر آنکه $a = b = ۱$، و اگر A و B مانند بالا تعریف شوند، آنگاه $A^۳ + B^۳ = ۲^{n-۳}$. لذا اگر a و b مثبت باشند و $a^۳ + b^۳ = ۲^n$، آنگاه n باید به‌صورت $۳k + ۱$ باشد و $a = b = ۲^k$.

برای $p = ۳$ یک پیچیدگی وجود دارد، زیرا از $p|۳ab$ نمی‌توان نتیجه گرفت که $p|a$ یا $p|b$. اما به آسانی دیده می‌شود که $a^۳ + b^۳ > ۳(a+b)$ مگر آنکه عدد بزرگتر از دو عدد a و b، مثلاً a، ۲ یا کمتر باشد، و لذا ۳^{n-k} بر ۹ بخشپذیر است. در نتیجه a و b بر ۳ بخشپذیرند جز در حالت $a = ۲$، $b = ۱$. بنابراین اگر a و b با $a \geq b$ مثبت باشند و $a^۳ + b^۳ = ۳^n$، آنگاه n به‌صورت $۳k + ۲$ است و $a = ۲ \times ۳^k$، $b = ۳^k$.

تمرینهایی برای فصل ۸

۱. همهٔ سه‌تاییهای فیثاغورسی را که یکی از عناصرش ۱۵ است به‌دست آورید.

۲. همهٔ سه‌تاییهای فیثاغورسی (x, y, z) را تعیین کنید به‌طوری که $۰ < x < y$ و $z = ۳۷۷$.

۳. فرض کنید $N = ۲ \times ۳^۲ \times ۵^۳ \times ۱۳^۵$. آیا یک مثلث فیثاغورسی با وتر N وجود دارد؟ آیا یک مثلث فیثاغورسی اولیه با وتر N وجود دارد؟

۴. چه تعداد سه‌تایی فیثاغورسی (x, y, z) با $z = ۱۸۸۵$ وجود دارد؟

۵. اثبات یا رد کنید: یک مثلث فیثاغورسی با وتر ۷۷ وجود دارد.

۶. فرض کنید n یک عدد صحیح مثبت باشد. اگر حداقل یک مثلث فیثاغورسی اولیه وجود داشته باشد که یک ضلع آن n واحد کمتر از وتر باشد، ثابت کنید تعداد نامتناهی مثلث فیثاغورسی وجود دارد.

۷. همهٔ نمایشهای الزاماً مجزای ۱۵۰۲۸۰ و ۷۰۷۸۵۰ به‌صورت مجموع دو مربع را پیدا کنید.

۸. یک آزمون بخشپذیری برای تعیین اینکه ۷۶۵۴۹۳۱۷ نمایشی به‌صورت مجموع دو مربع دارد یا نه، به‌کار برید.

۹. آیا $(۶۴۶)^{۴۱}$ مجموع دو مربع است؟

۱۰. مثالی از یک عدد صحیح مثبت که مضرب ۲۱ است بیاورید به‌طوری که دقیقاً شش عامل به‌صورت $۴k+۱$ بیشتر از عاملهای به‌صورت $۴k+۳$ داشته باشد.

۱۱. همهٔ نمایشهای ۳۳۳۲۳۴۰۰ به‌صورت مجموع $a^۲+b^۲$ را بیابید به‌طوری a و b اعداد صحیح مثبت باشند و $a>b$.

۱۲. ثابت کنید که تعداد عاملهای به‌صورت $۴k+۱$ و $۴k+۳$ در عدد $۲^۳\times۳^۵\times۵^۳\times۷^۲\times۱۱^۴\times۱۳$ برابرند.

۱۳. بدون تجزیه، در مورد نمایش‌پذیری ۷۶۸۳۱۲۷۴۱ یا ۳۵۱۶۹۴۸۴۳ به‌صورت مجموع دو مربع تحقیق کنید.

۱۴. عدد صحیح مثبتی پیدا کنید که مضرب ۳۳ باشد و دقیقاً شش نمایش الزاماً متفاوت به‌صورت مجموع دو مربع داشته باشد.

۱۵. اگر $n\equiv ۳(\bmod ۹)$، ثابت کنید که n همان تعداد مقسوم‌علیه به‌صورت $۴k+۳$ دارد که به‌صورت $۴k+۱$ دارد.

۱۶. همهٔ نمایشهای الزاماً متفاوت ۴۳۴۸۲۶ و ۲۵۳۳۹۸۶ به‌صورت مجموع دو مربع را تعیین کنید.

۱۷. می‌توان عدد ۹۹۲۲۱ را به‌صورتهای $(۳۱۱)^۲+۵۰^۲$ و $(۳۱۴)^۲+۲۵^۲$ نمایش داد. با استفاده از این مطلب نشان دهید که ۹۹۲۲۱ اول نیست.

۱۸. همهٔ نمایشهای اولیهٔ ۶۴۰۹ به‌صورت مجموع دو مربع را به‌دست آورید.

۱۹. اثبات یا رد کنید: اگر q عدد اولی به‌صورت $۴k+۳$ باشد و q عدد $c^۲+d^۲$ را بشمارد، آنگاه $q^۲$ عدد $c^۲+d^۲$ را می‌شمارد.

۲۰. همهٔ نمایشهای الزاماً متفاوت ۱۶۹۰۰۰ به‌صورت مجموع دو مربع را تعیین کنید. آیا هیچ نمایش اولیه‌ای وجود دارد؟

۲۱. یک عدد صحیح مثبت پیدا کنید که دقیقاً شش نمایش الزاماً متمایز به‌صورت مجموع دو مربع غیرصفر داشته باشد، و هیچ‌کدام از نمایشها اولیه نباشد.

۲۲. همهٔ نمایشهای اولیهٔ ۱۱۰۵۰ به‌صورت مجموع دو مربع را به‌دست آورید.

۲۳. مطلوب است تعیین کوچکترین پنج عدد صحیح مثبت که دقیقاً سه نمایش الزاماً مختلف به‌صورت مجموع دو مربع داشته باشند، با حداقل یک نمایش اولیه.

۲۴. اثبات یا رد کنید: اگر p_1، p_2، ...، p_n اعداد اولی به‌صورت $4k+1$ باشند، آنگاه $p_1p_2\cdots p_n$ فقط نمایشهای اولیه به‌صورت مجموع دو مربع دارد.

۲۵. اگر n خالی از مربع باشد (یعنی، بر هیچ مربعی بزرگتر از ۱ بخشپذیر نباشد)، آیا هر نمایش n اولیه است؟

۲۶. فرض می‌کنیم $n=a^2+b^2$، که $(a,b)=1$. اگر p یک عامل اول فرد n باشد، با اثبات $(-1/p)=1$، نشان دهید $p\equiv 1 \pmod 4$. (راهنمایی: از $a^2\equiv -b^2 \pmod p$ برای حلپذیری $x^2\equiv -1 \pmod p$ استفاده کنید.)

۲۷. ثابت کنید که یک عدد صحیح را می‌توان به‌صورت مجموع مربعات دو عدد گویا بیان کرد اگر و تنها اگر بتوان آن را به‌صورت مجموع مربعات دو عدد صحیح بیان کرد.

۲۸. مثالی از یک عدد صحیح بزرگتر از ۲۰۰۰۰۰۰۰ بیاورید که مجموع چهار مربع غیرصفر نباشد.

۲۹. آیا ۹۹۵۲ مجموع سه مربع است؟ آیا ۱۲! مجموع سه مربع است؟

۳۰. ثابت کنید که توانی از ۲ نمی‌تواند مجموع سه مربع غیرصفر باشد.

۳۱. تعیین کنید کدام‌یک از اعداد زیر مجموع چهار مربع غیرصفر است: ۱۲۳۴۵؛ ۷۳۷۲۸؛ ۹۸۳۰۴.

۳۲. اولین چهار عدد بزرگتر از ۱۰۰۰۰۰۰ را پیدا کنید که مجموع چهار مربع غیرصفر نباشند.

۳۳. اولین دو عدد بزرگتر از ۹۸۳۰۳ را پیدا کنید که مجموع چهار مربع غیرصفر باشند.

۳۴. ثابت کنید ۲ تنها عدد اولی است که مجموع دو مکعب مثبت است. (راهنمایی: $x^3+y^3=(x+y)((x-y)^2+xy)$.)

۳۵. فرض می‌کنیم که p عدد اول فردی باشد. ثابت کنید p یک نمایش یکتا به‌صورت a^2-b^2 دارد، که در آن a و b اعداد صحیح مثبت هستند.

۳۶. فرض می‌کنیم n یک عدد صحیح مثبت فرد باشد. اگر n دقیقاً یک نمایش به‌صورت a^2-b^2 داشته باشد که در آن a و b اعداد صحیح مثبت هستند، ثابت کنید یا n اول است یا مربع یک عدد اول.

۳۷. ثابت کنید که هر عدد صحیح مثبت به‌صورت $r^2+s^2+t^2$ یا $r^2+s^2+2t^2$ است.

ملاحظاتی برای فصل ۸

۱. اویلر در ۱۷۷۸ حدس زد که اگر $n\geq 3$، هیچ توان مثبت mام مجموع کمتر از n توان مثبت mام نیست. البته آخرین قضیهٔ فرما فوراً از این نتیجه می‌شود. حدسیهٔ اویلر برای $n=3$ برقرار

است، زیرا همان‌گونه که خود اویلر ثابت کرد، $x^3 + y^3 = z^3$ جواب صحیح مثبت ندارد. ولی، در ۱۹۶۶، اِل. جِی. لاندر[1] و تی. آر. پارکین[2] با مثال زیر نشان دادند که حدسیه نادرست است:

$$۱۴۴^۵ = ۲۷^۵ + ۸۴^۵ + ۱۱۰^۵ + ۱۳۳^۵$$

در ۱۹۸۸، اِن. الکیز[3] نشان داد که حدسیه برای $n = ۴$ نیز نادرست است؛ کوچکترین مثال نقض عبارت است از

$$(۹۵۸۰۰)^۴ + (۲۱۷۵۱۹)^۴ + (۴۱۴۵۶۰)^۴ = (۴۲۲۴۸۱)^۴$$

حدس اویلر برای $n \geq ۶$ هنوز باز است.

۲. شکاف موجود در برهان مختصرِ لامه از آخرین قضیهٔ فرما اساساً مشابه مسألهٔ اثبات اویلر از همین قضیه در حالت $n = ۳$ است. هر یک بدون دلیل توجیهی فرض کرده‌اند که همواره می‌توان «اعداد صحیح» را در میدانهای اعداد عمومی‌تر به‌طور یکتا به حاصلضرب اعداد اول تجزیه کرد. (این مسأله در فصل ۱۱ بحث شده است.) در واقع، تجزیهٔ یکتا برای اعداد صحیح در $Q(\omega)$، که $\omega = (-۱ + \sqrt{-۳})/۲$، وجود دارد، حالتی که به $n = ۳$ مربوط می‌شود، ولی کوشی نشان داد که قضیهٔ اصلی حساب، مثلاً، برای «اعداد صحیحی» که در حالت $n = ۲۳$ تولید می‌شوند صدق نمی‌کند.

۳. برای آخرین قضیهٔ فرما دو حالت وجود دارد: حالت I (حالت ساده‌تر): p هیچ‌کدام از اعداد صحیح x، y، یا z را نمی‌شمارد؛ و حالت II (حالت دشوارتر): p یکی از x، y، یا z را می‌شمارد. پیش از کارهای وایلز، آخرین قضیهٔ فرما در حالت I برای همهٔ توانهایی که عامل اول فردی کوچکتر از $۱۰^{۱۷}$ دارند، و در حالت II برای همهٔ اعداد اول کمتر از $۱۰^۶$ ثابت شده بود.

برای به‌دست آوردن یک تخمین در حالت I: در ۱۹۰۹، ویفریش ثابت کرد که اگر حالت I برای یک توان اول p برقرار نباشد، آنگاه $۲^{p-۱} \equiv ۱ (\mathrm{mod}\, p^۲)$. این چنین اعداد اول به‌عنوان اعداد اول ویفریش معروف‌اند، و تنها اعداد اول ویفریش که کمتر از ۶×۱۰^۹ هستند عبارت‌اند از ۱۰۹۳، ۳۵۱۱. در ۱۹۱۳، میری مانوف[4]، نیز نشان داد که اگر حالت I برای عدد اول p برقرار نباشد، $۳^{p-۱} \equiv ۱ (\mathrm{mod}\, p^۲)$. اعداد اول ۱۰۹۳ و ۳۵۱۱ در این همنهشتی صدق نمی‌کنند، و لذا حالت I برای اعداد اول $p < ۶ \times ۱۰^۹$ برقرار است.

این راه به طریق زیر بسط داده شد: اگر حالت I برای یک توان اول p برقرار نباشد، آنگاه به‌ازای هر عدد اول $q \leq ۸۹$، $q^{p-۱} \equiv ۱ (\mathrm{mod}\, p^۲)$. تا پیش از آنکه وایلز آخرین قضیهٔ فرما را

1. L. J. Lander 2. T. R. Parkin 3. N. Elkies 4. Mirimanoff

ثابت کند، این مطلب، بدون هیچ محدودیتی نشان داد که حالت I برای همهٔ اعداد اولِ کوچکتر از ۷۱۴ ۵۹۱ ۴۱۶ ۰۹۱ ۳۸۹ برقرار است؛ بررسیهای بعدی این کران را تا 10^{17} رساند. علاوه بر این، نشان داده شده است که حالت I برای هر عدد مِرسن برقرار است.

۴. تعدادی مسألهٔ «آسان‌ـبیان» مربوط به مثلثهای فیثاغورسی وجود دارند که علی‌رغم کوششهای قابل توجه حل نشده باقی مانده‌اند. در اینجا چند نمونه ارائه می‌شوند

(الف) آیا یک جعبهٔ فیثاغورسی وجود دارد؟ یعنی، آیا جعبه‌ای وجود دارد که یالهایش، قطرهای وجوهش، و قطر اصلیش طول صحیح داشته باشند؟

(ب) آیا یک مربع $ABCD$ و یک نقطهٔ P وجود دارند به‌طوری که فاصله‌های AB، PA، PB، PC، و PD همگی اعداد صحیح باشند؟

(ج) آیا تعداد نامتناهی مثلث فیثاغورسی وجود دارند که وتر و یکی از اضلاع مثلثها اعداد اول باشند؟

۵. در اینجا، به نقل اثبات کامل فرما (ترجمهٔ هیث[1]) از این مطلب که مساحت یک مثلث فیثاغورسی نمی‌تواند یک مربع باشد، یا هم‌ارز با آن، معادلهٔ $x^4 - y^4 = z^2$ جواب مثبت ندارد، می‌پردازیم:

اگر مساحت یک مثلث قائم‌الزاویه یک مربع باشد، دو توان چهارم وجود خواهند داشت که تفاضلشان یک مربع است، و لذا دو مربع وجود دارند که مجموع و تفاضل آنها مربع هستند. لذا یک مربع وجود دارد که مساوی مجموع یک مربع و دو برابر یک مربع است، به‌طوری که مجموع دو مربع مؤلفه‌ای یک مربع است. اما اگر یک مربع مساوی مجموع یک مربع و دو برابر یک مربع باشد، ریشه‌اش نیز مجموع یک مربع و دو برابر یک مربع است، که به آسانی می‌توانم اثبات کنم. در نتیجه این ریشه مجموع دو ضلع یک مثلث قائم‌الزاویه است، یکی از مربعها قاعده و در برابر دیگری ارتفاع را می‌سازند. لذا، این مثلث قائم‌الزاویه از دو مربع تشکیل می‌شود که مجموع و تفاضلشان مربع هستند. اما می‌توان نشان داد که این دو مربع کوچکتر از مربعهایی هستند که بنابه فرض مجموع و تفاضلشان مربع هستند. با استدلالی مشابه، اعداد صحیح کوچکتر و کوچکتر خواهیم داشت که در همان شرایط صدق می‌کنند. اما این غیرممکن است، زیرا بی‌نهایت عدد صحیح مثبت کوچکتر از یک عدد صحیح مفروض وجود ندارد. اینجا برای اثبات کامل و همهٔ بسطهایش بسیار تنگ است.

1. Heath

شرح مختصری از زندگینامه‌ها

دیوفانتوس (حوالی ۲۵۰ م) روشهای جبری را در ریاضیات یونانی وارد کرد. به‌ویژه، نمادهایی برای مجهول، مربع و مکعبِ آن معرفی کرد. به هر حال، روش مستقیمی برای دیوفانتوس وجود نداشت که به‌طور همزمان با چند مجهول کار کند. کتاب آریتمتیکای (علم حساب) او گردایه‌ای متجاوز از ۲۵۰ مسأله است، که بسیاری از آنها به‌طور استادانه‌یی حل شده‌اند، و در معادلات جبری که جوابهای گویا برای آنها مورد نظر است بحث می‌کند. معمولاً، دیوفانتوس به تولید یک پاسخ عددی قناعت می‌کند، ولی اغلب آشکار است که او یک روش کلی در اختیار دارد.

اساساً هیچ چیز در مورد زندگانی دیوفانتوس معلوم نیست. اگر بپذیریم که روایت مسألهٔ ۱.۸ دربارهٔ او درست است، او در سن ۸۴ سالگی درگذشته است.

کارل گوستاف یاکوبی* در ۱۸۰۴ در پوتسدام[1] به دنیا آمد. یک کودک نابغه که بیشتر خودآموز بود و ریاضیاتش را از کارهای اویلر و لاگرانژ فرا گرفت. در ۱۸۲۱، به دانشگاه برلین وارد شد؛ در همان سال لیسانس و در ۱۸۲۵ دکترایش را دریافت کرد. موضوع رسالهٔ دکترایش کسرهای مسلسل بود. به مدت هجده سال در کونیکسبرگ[2] تدریس کرد، اما شهرت زیاد سریع او موجب انتخاب او به عضویت در آکادمی علوم پروس گردید، و با اقامت دائم در برلین در ۱۸۴۴ بیشتر زمان را در آنجا گذراند. یاکوبی در اصل به دلیل کارهایش در نظریهٔ توابع بیضوی معروف است و اصولاً متخصص در نظریهٔ اعداد نبود. اما او نشان داد که چگونه می‌توان اتحادهای شامل توابع بیضوی را برای حل مسائل نظریهٔ اعداد، به‌ویژه، مسائلی دربارهٔ تعداد نمایشهای یک عدد صحیح به‌صورت مجموع یک تعداد مشخص از مربعها، به‌کار برد. مفاهیم مربوط به اعداد یکی از زمینه‌های اصلی نظریهٔ اعداد از اواسط سدهٔ نوزدهم تا امروز شده‌اند. یاکوبی، برخلاف اکثر همکارانش، سرزنده، منطقی، و اجتماعی بود. او اطلاعات جامعی از ریاضیات داشت و به یک معلم بزرگ مشهور و به‌غایت سخت‌کوش بود.

یاکوبی در ۱۸۵۱ به مرض آبله در برلین درگذشت.

مراجع

Leonard Eugene Dickson, *History of the Theory of Numbers*, Volume II. (See Chapter 3.)

Harold M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to*

* تلفظِ فرانسویِ آن، ژاکوبی، در ایران متداول شده است.

1. Potsdam 2. Königsberg

Algebraic Number Theory, Springer-Verlag, New York, 1977.

ادواردز بیان می‌کند که چگونه نظریهٔ جبری اعداد به‌طور طبیعی از کوششهای مربوط به اثبات آخرین قضیهٔ فرما و سایر مسائل دیوفانتوس، عمدتاً مسائل شامل صورتهای درجهٔ دوم، به‌وجود آمد. این کتاب برای درک مطالب ریاضی مولد این مفاهیم ضروری است. سه فصل اول کتاب کاملاً قابل فهم هستند و اطلاعات ارزشمندی در مورد مجموعهای مربعات و معادلهٔ پل دارند. ادواردز جزئیات تاریخی مفصلی را ارائه می‌دهد؛ هم او بود که نشان داد که در واقع هیچ مبنایی دال بر این تأیید غالباً تکراری که کومر آخرین قضیهٔ فرما را اثبات کرده است وجود ندارد بلکه به اشتباه یک ویژگی تجزیهٔ یکتا را فرض کرده است.

Sir Thomas L. Heath, *Diophantus of Alexandria*, Dover, New York, 1964.

در این کتاب، که نخستین بار در ۱۸۸۵ به چاپ رسید، هیث ترجمهٔ جدیدی از چاپ محدود تانری[1] از قسمتی از حساب دیوفانتوس را که در آن زمان در دسترس بود، ارائه می‌دهد، او این قسمت را با شرح قضیه‌هایی از فرما و اویلر که ملهم از دیوفانتوس بودند، از جمله یادداشت حاشیه‌یی معروف فرما، ادامه می‌دهد. کتاب هیث به سبک بسیار خوب دانش‌پژوی سدهٔ نوزدهم نوشته شده است. این کتاب کامل است و برای کسی که معلوماتی از جبر دبیرستان دارد قابل فهم است. از جملهٔ کتابهای دیگر هیث ترجمه‌هایی از اقلیدس، آپولونیوس، و ارشمیدس هستند.

Paulo Ribenboim, *The Book of Prime Number Records* (Second Edition). (See Chapter 7.)

Paulo Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

Jacques Sesiano, *Books IV to VII of Diophantus' Arithmetica*, Springer-Verlag, New York, 1982.

در اوایل ۱۹۷۰ معلوم شد که یک قسمت تا به حال ناشناخته از کتاب حساب (دیوفانتوس) در یک ترجمهٔ عربی، در میان گردایه‌ای از نسخه‌های خطی ریاضی در کتابخانهٔ آستان قدس رضوی قرار دارد. این کتاب یک چاپ انتقادی از موضوع، همراه با یک ترجمهٔ انگلیسی و شرح ریاضی عالمانه است.

André Weil, *Number Theory: An approach through history from Hammurapi to Legendre*. (See Chapter 3.)

1. Tannery

۹

کسرهای مسلسل

در این فصل تکنیکی را برای نوشتن هر عدد حقیقی به‌صورت یک دنبالهٔ بارستی از خارج‌قسمتها بیان می‌کنیم. (مثلاً، می‌توان ۱۵۸/۴۹ را به‌صورت زیر نوشت

$$۳ + \cfrac{۱}{۴ + \cfrac{۱}{۲ + \cfrac{۱}{۵}}}$$

وقتی عدد مفروض گویا باشد، یک چنین عبارت را که کسر مسلسل نامیده می‌شود، می‌توان از الگوریتم اقلیدس به‌دست آورد، اما بسطهای کسر مسلسل برای اعداد گنگ را نیز می‌توان پیدا کرد.

به دلیل ارتباط نزدیکشان با الگوریتم اقلیدسی، تاریخ‌گذاری منشأ کسرهای مسلسل به‌طور دقیق مشکل است. به صورت کمابیش جدید، کسرهای مسلسل اول بار در کارهای ریاضیدانان ایتالیایی

رافائل بومبلی[1] (۱۵۷۳ـ۱۵۲۶) و پیترو کاتلدی[2] (۱۶۲۶ـ۱۵۴۸) برای تقریب ریشه‌های دوم آشکار شد. فیزیکدان هلندی کریستیان هویگِنس[3] (یا با تلفظ هلندی هویخنس) (۱۶۹۵ـ۱۶۲۹) در کتابش «شرح افلاک‌نمای خودکار»[4] (۱۷۳۰)، کسرهای مسلسل را در ارتباط با ساخت یک مدل مکانیکی سیارات مطالعه کرده است. مثلاً، نسبت دورهٔ گردش زحل و زمین (به دور خورشید) به‌طور تقریب $\alpha = ۷۷۷۰۸۴۳۱/۲۶۴۰۸۵۸$ بود. هویگنس لازم داشت که دو چرخ دندانه‌دار با تعداد دندانه‌های p و q که نسبتاً کوچک باشند بسازند به‌طوری که p/q تقریباً برابر α باشد. او دریافت که $p = ۲۰۶$ و $q = ۷$ خطایی کمتر از ۴۰ دقیقهٔ کمان در هر قرن به‌دست می‌دهد. بیش از ۱۱۰۰ سال پیش، آریبهطه تکنیکی مشابه برای تقریب دورهٔ گردش مشتری به‌کار برده بود. در نامه‌ای که حدود ۱۷۳۰ اویلر به گلدباخ[5] نوشته است، کسرهای مسلسل و ارتباطشان با اعداد گنگ درجهٔ دوم آمده است. اویلر به ارتباط کسرهای مسلسل و تقریبات به‌وسیلهٔ اعداد گویا آگاهی داشت و مشاهده کرد که یک عدد گویا دارای بسط کسر مسلسل متناهی است که می‌تواند از الگوریتم اقلیدسی به‌دست آید. در ۱۷۵۹، اویلر کسرهای مسلسل را برای حل معادلاتی به‌صورت $x^۲ - dy^۲ = ۱$ به‌کار برد. این معادله، معروف به معادلهٔ پِل، تاریخی طولانی دارد و به تفصیل در فصل بعد مورد مطالعه قرار خواهد گرفت. در اوایل سال ۱۷۶۶، قضیه‌های اساسی در مورد کسرهای مسلسل دوره‌یی برای اولین بار توسط لاگرانژ اثبات گردید.

تعمیمهای کسرهای مسلسل کاربردهای فراوانی در آنالیز دارند، که اولین بار توسط اویلر و لاگرانژ بررسی شده است. مثلاً، الگوریتمهایی که توسط حسابگرها علمی برای تقریب توابعی نظیر e^x و $\sin x$ به‌کار می‌روند ریشه‌هایی در کسرهای مسلسل دارند.

قضیه‌هایی برای فصل ۹

کسرهای مسلسل متناهی

موضوع را با بررسی ارتباط بین الگوریتم اقلیدسی و بسط کسر مسلسل یک عدد گویا آغاز می‌کنیم. اگر الگوریتم اقلیدسی را در مورد اعداد ۱۵۸ و ۴۹ به‌کار بریم داریم

$$۱۵۸ = ۳ \times ۴۹ + ۱۱، \quad \text{و لذا} \quad ۱۵۸/۴۹ = ۳ + ۱۱/۴۹؛$$
$$۴۹ = ۴ \times ۱۱ + ۵، \quad \text{و لذا} \quad ۴۹/۱۱ = ۴ + ۵/۱۱؛$$
$$۱۱ = ۲ \times ۵ + ۱، \quad \text{و لذا} \quad ۱۱/۵ = ۲ + ۱/۵؛$$

1. Rafael Bombelli 2. Pietro Cataldi 3. Christiaan Huygens
4. Descriptio Automati Planetarii 5. Goldbach

بنابراین می‌توانیم عدد گویای ۱۵۸/۴۹ را به‌صورت زیر بنویسیم:

$$۱۵۸/۴۹ = ۳ + \frac{۱۱}{۴۹} = ۳ + \frac{۱}{۴ + \frac{۵}{۱۱}} = ۳ + \frac{۱}{۴ + \frac{۱}{۲ + \frac{۱}{۵}}}$$

یک عبارت از این نوع را یک کسر مسلسل خوانیم، که با $\langle ۳, ۴, ۲, ۵ \rangle$ نشان می‌دهیم. اعداد ۳، ۴، ۲، و ۵ جمله‌ها، یا خارج‌قسمتهای جزئی کسر مسلسل خوانده می‌شوند، زیرا خارج‌قسمتهایی هستند که در الگوریتم اقلیدسی ظاهر می‌شوند.

(۱.۹) تعریف. فرض کنیم $a_۰$، $a_۱$، $a_۲$، ...، a_n همگی بجز احتمالاً $a_۰$ اعداد حقیقی مثبت باشند. کسر مسلسل $\langle a_۰, a_۱, a_۲, \ldots, a_n \rangle$ را چنین تعریف می‌کنیم:

$$a_۰ + \cfrac{۱}{a_۱ + \cfrac{۱}{a_۲ + \cfrac{۱}{\ddots + \cfrac{۱}{a_{n-۱} + \cfrac{۱}{a_n}}}}}$$

اگر هر a_i عدد صحیحی باشد، کسر مسلسل ساده نامیده می‌شود.

در مثال بالا، چون $۱/(۴ + ۱/۱) = ۱/۵$، همچنین داریم $۱۵۸/۴۹ = \langle ۳, ۴, ۲, ۴, ۱ \rangle$. در واقع، $\langle ۳, ۴, ۲, ۵ \rangle$ و $\langle ۳, ۴, ۲, ۴, ۱ \rangle$ تنها نمایشهای ۱۵۸/۴۹ به‌صورت یک کسر مسلسل سادهٔ متناهی هستند. همان‌گونه که قضیهٔ زیر نشان می‌دهد، هر عدد گویا دقیقاً دو بسط کسر مسلسل ساده دارد.

(۲.۹) قضیه. هر عدد گویای r دقیقاً دو بسط کسر مسلسل متناهی دارد. وقتی r عدد صحیحی باشد، نمایشها عبارت‌اند از $\langle r \rangle$ و $\langle r - ۱, ۱ \rangle$. اگر r عدد صحیح نباشد و $\langle a_۰, a_۱, \ldots, a_n \rangle$ کسر مسلسلی باشد که از الگوریتم اقلیدسی به‌دست آمده باشد، آنگاه $a_n > ۱$ و لذا نمایش دیگر r عبارت است از $\langle a_۰, a_۱, \ldots, a_n - ۱, ۱ \rangle$.

برهان. آشکار است که $\langle ۱ \rangle = \langle ۰, ۱ \rangle = ۱$. در مسألهٔ ۵.۹ ثابت می‌کنیم که یک عدد گویا فقط دارای یک نمایش کسر مسلسل متناهی است که در آن آخرین خارج‌قسمت جزئی بزرگتر از ۱ است.

در نتیجه اگر $r \neq ۱$، آنگاه عدد r بسط کسر مسلسل یکتا دارد که در آن آخرین خارج‌قسمت جزئی برابر ۱ است. (در غیر این‌صورت، می‌توانیم دو بسط متفاوت تولید کنیم که به عدد صحیحی بزرگتر از ۱ ختم شوند، زیرا اگر $a_n > ۱$ داریم $\langle a_۰, a_۱, \ldots, a_n \rangle = \langle a_۰, a_۱, \ldots, a_n - ۱, ۱ \rangle$) بنابراین اگر r عدد صحیحی باشد، آنگاه $\langle r - ۱, ۱ \rangle$ و $\langle r \rangle$ تنها بسطهای r هستند.

اکنون فرض می‌کنیم $r = a/b$ عدد صحیح نباشد. با کاربرد الگوریتم اقلیدسی داریم

$$a = a, b + r_۱, b = q_۲ r_۱ + r_۲, r_۱ = q_۳ r_۲ + r_۳, \ldots, r_{n-۲}$$
$$= q_n r_{n-۱} + r_n, r_{n-۱} = q_{n+۱} r_n$$

به‌طوری که $r_۱ > r_۲ > \cdots > r_{n-۱} > r_n > ۰$. (چون r عدد صحیح نیست، $r_۱ > ۰$ و لذا $n \geq ۱$.) در این‌صورت، همانند مثال قبل، $a/b = \langle q_۱, q_۲, \ldots, q_{n+۱} \rangle$. روشن است که، $q_{n+۱}$ عدد صحیح مثبتی است. اگر $q_{n+۱} = ۱$، آنگاه $r_{n-۱} = q_{n+۱} n_n = r_n$، که با $r_{n-۱} > r_n$ تناقض دارد. لذا بایستی داشته باشیم $q_{n+۱} \geq ۲$. چون $q_{n+۱} = (q_{n+۱} - ۱) + ۱/۱$ و $q_{n+۱} - ۱$ عدد صحیح مثبتی است، a/b دارای بسط $\langle q_۱, q_۲, \ldots, q_{n+۱} - ۱, ۱ \rangle$ نیز می‌باشد. بنابر مسألهٔ ۵.۹، نتیجه می‌شود که این بسطها تنها بسطهای کسر مسلسل a/b هستند.

اکنون به مسألهٔ یافتن یک روش کارآمد برای محاسبهٔ یک کسر مسلسل سادهٔ مفروض $\langle a_۰, a_۱, \ldots, a_n \rangle$ برمی‌گردیم.

(۳.۹) تعریف. فرض کنیم $a_۰$، $a_۱$، $a_۲$، ... دنباله‌ای از اعداد صحیح باشد، که همگی بجز احتمالاً $a_۰$ مثبت هستند. دنباله‌های $\{p_k\}$ و $\{q_k\}$ را چنین تعریف می‌کنیم:

$$p_{-۱} = ۱, \quad p_۰ = a_۰ \quad \text{و} \quad p_k = a_k p_{k-۱} + p_{k-۲} \quad k \geq ۱$$
$$q_{-۱} = ۰, \quad q_۰ = ۱ \quad \text{و} \quad q_k = a_k q_{k-۱} + q_{k-۲} \quad k \geq ۱$$

توضیح. بنابه تعریف $q_۰ = ۱$؛ از آنجاکه اگر $k \geq ۱$، آنگاه a_kها اعداد صحیح مثبت هستند، داریم $a_۱ \leq a_۲ \leq \cdots$. به‌ویژه به‌ازای هر $k \geq ۰$ داریم $q_k \geq k$. در واقع، q_kها به نسبت نمایی بزرگ می‌شوند؛ اگر $k \geq ۲$، اثبات $q_k \geq ۲^{k/۲}$ مشکل نیست (مسألهٔ ۷.۹ را ببینید).

قضیهٔ بعدی در سرتاسر فصل به‌کار می‌رود. مسألهٔ ۶.۹ را برای یک برهان ببینید.

(۴.۹) قضیه. فرض کنیم a_0، a_1، a_2، ... دنباله‌ای از اعداد صحیح باشد که همهٔ جمله‌ها بجز احتمالاً a_0 مثبت هستند. در این‌صورت به‌ازای هر عدد حقیقی مثبت x، هر $k \geq 1$،

$$\langle a_0 a_1, \ldots, a_{k-1}, x\rangle = (xp_{k-1} + p_{k-2}/(xq_{k-1} + q_{k-2})$$

به‌ویژه

$$\langle a_0, a_1, \ldots, a_k\rangle = p_k/q_k$$

(۵.۹) تعریف. عدد $c_k = \langle a_0, a_1, \ldots, a_k\rangle$، که در آن $k \leq n$، همگرای kام کسر مسلسل $\langle a_0, a_1, \ldots, a_n\rangle$ خوانده می‌شود. بنابر قضیهٔ (۴.۹)، $c_k = p_k/q_k$.

(۶.۹) مثال. می‌توانیم (۳.۹) و (۴.۹) را برای محاسبهٔ $\langle -4, 2, 3, 1, 2\rangle$ به‌کار بریم. با کاربرد جدول زیر محاسبات به‌نحو ساده‌تری انجام می‌شود:

k	-1	0	1	2	3	4
a_k		-4	2	3	1	2
p_k	1	-4	-7	-25	-32	-89
q_k	0	1	2	7	9	25

(سه عددی که پررنگ نوشته شده‌اند برای هر چنین محاسبه‌ای یکی هستند.) درایه‌ها بر طبق فرمولهای ارائه‌شده در (۳.۹) محاسبه شده‌اند. مثلاً، برای یافتن $p_3 = a_3p_2 + p_1$، $a_3 = 1$ را در آخرین مقدار محاسبه‌شدهٔ p یعنی p_2 (یعنی، -25) ضرب و با جملهٔ قبلی p_1 جمع می‌کنیم. لذا $p_3 = 1(-25) + (-7) = -32$. سرانجام، ملاحظه می‌کنیم که $\langle -4, 2, 3, 1, 2\rangle = p_4/q_4 = -89/25$.

قضیهٔ زیر در بسیاری از قضیه‌های بعدی نقش دارد؛ مثلاً، می‌توان آن را برای یافتن جوابهای معادلهٔ $ax + by = c$ به‌کار برد. (بخش بعدی را ببینید.)

(۷.۹) قضیه. به‌ازای هر $k \geq 0$

$$p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1} \qquad (1)$$

به‌ویژه، $(p_k, q_k) = 1$.

برهان. اثبات به استقرا. به‌ازای $k = ۰$ رابطهٔ (۱) با توجه به تعریف (۳.۹) به آسانی ثابت می‌شود. فرض کنیم $k \geq ۰$ و (۱) برقرار باشد. بنابر (۳.۹) داریم

$$\begin{aligned} p_{k+۱}q_k - p_kq_{k+۱} &= (q_{k+۱}p_k + p_{k-۱})q_k - p_k(a_{k+۱}q_k + q_{k-۱}) \\ &= -(p_kq_{k-۱} - p_{k-۱}q_k) \overset{(۱)}{=} -(-۱)^{k-۱} = (-۱)^k, \end{aligned}$$

و این همان (۱) است که در آن به جای k عدد $k+۱$ گذاشته شده است.

در حالت خاص، اگر $d = (p_k, q_k)$، آنگاه بنابر (۱)، $d|(-۱)^{k-۱}$ و چون d مثبت است پس $d = ۱$.

(۸.۹) فرع. به‌ازای هر $k \geq ۰$ معادلهٔ $p_kq_{k-۲} - p_{k-۲}q_k = (-۱)^k a_k$ برقرار است.

برهان. داریم

$$\begin{aligned} p_kq_{k-۲} - p_{k-۲}q_k &= (a_kp_{k-۱} + p_{k-۲})q_{k-۲} - p_{k-۲}(a_kq_{k-۱} + q_{k-۲}) \\ &= a_k(p_{k-۱}q_{k-۲} - p_{k-۲}q_{k-۱}) = (-۱)^{k-۲}a_k = (-۱)^k a_k \end{aligned}$$

قضیهٔ بعد نشان می‌دهد که در یک کسر مسلسل $r = \langle a_۰, a_۱, \ldots, a_n \rangle$ همگراهای با اندیس فرد متوالیاً به r نزدیک می‌شوند و از این‌رو تقریبهای بهتر و بهتری برای r می‌دهند. قضیهٔ مشابه برای همگراهای با اندیس زوج نیز برقرار است.

(۹.۹) قضیه. فرض کنیم c_k همگرای kام از $r = \langle a_۰, a_۱, \ldots, a_n \rangle$ باشد. در این‌صورت

$$c_۰ < c_۲ < c_۴ < \cdots \qquad \cdots < c_۵ < c_۳ < c_۱$$

به‌ویژه هر همگرا با اندیس زوج کوچکتر از هر همگرا با اندیس فرد است.

برهان. چون $c_k = p_k/q_k$، با تقسیم معادلهٔ (۸.۹) بر $q_kq_{k-۲}$ داریم

$$c_k - c_{k-۲} = (-۱)^k a_k/q_kq_{k-۲}$$

چون به‌ازای هر $i \geq ۰$، $q_i > ۰$ و اگر $i > ۰$، آنگاه $a_i \geq ۱$، لذا به‌ازای هر عدد زوج $k \geq ۲$ داریم $c_k - c_{k-۲} > ۰$. با استدلالی مشابه اگر $k \geq ۳$ فرد باشد، آنگاه $c_k - c_{k-۲} < ۰$. برای اثبات اینکه به‌ازای هر دو عدد صحیح نامنفی m و n، $c_{۲m} < c_{۲n+۱}$، ابتدا ملاحظه می‌کنیم که اگر دو طرف معادلهٔ (۷.۹) بر $q_kq_{k-۱}$ تقسیم شود، داریم $c_k - c_{k-۱} = (-۱)^{k-۱}/q_kq_{k-۱}$. از این‌رو اگر k فرد باشد $c_k > c_{k-۱}$. لذا $c_{۲m} < c_{۲m+۲n} < c_{۲m+۲n+۱} < c_{۲n+۱}$.

یک کاربرد: جوابهای $ax + by = c$

فرض کنیم a/b عددگویایی باشدکه $(a, b) = ۱$ و $b > ۰$. با استفاده ازالگوریتم اقلیدسی می‌نویسیم $a/b = \langle a_۰, a_۱, \ldots, a_n \rangle$. بنابر (۵.۹)، $a/b = p_n/q_n$؛ چون $(a, b) = (p_n, q_n) = ۱$ و $q_n > ۰$، داریم $a = p_n$ و $b = q_n$. لذا بنابر (۷.۹)، $aq_{n-۱} - bp_{n-۱} = (-۱)^{n-۱}$. بنابراین قضیهٔ زیر را داریم:

(۱۰.۹) قضیه. فرض کنیم $a/b = \langle a_۰, a_۱, \ldots, a_n \rangle$، با $(a, b) = ۱$ و $b > ۰$. اگر n فرد باشد، معادله دارای جواب $x = cq_{n-۱}$، $y = -cp_{n-۱}$ است. اگر n زوج باشد، $x = -cq_{n-۱}$، $y = cp_{n-۱}$ یک جواب است.

(۱۱.۹) مثال. برای یافتن جوابی از $۸۹x - ۲۵y = ۳$ قضیهٔ (۱۰.۹) را به‌کار می‌بریم. معادله را به‌صورت $-۸۹x + ۲۵y = -۳$ می‌نویسیم؛ در اینجا $a = -۸۹$، $b = ۲۵$، و $c = -۳$. بنابر (۶.۹)، $-۸۹/۲۵ = \langle -۴, ۲, ۳, ۱, ۲ \rangle$ و لذا مقدار n، یعنی اندیس آخرین خارج‌قسمت جزئی، برابر ۴ است. از این‌رو (۱۰.۹) یک جواب زیر را به‌دست می‌دهد.

$$x = -cq_{n-۱} = ۳q_۳ = ۳(۹) = ۲۷, \quad y = cp_{n-۱} = -۳p_۳ = -۳(-۳۲) = ۹۶$$

توضیح. می‌توان روش مذکور در (۱۰.۹) را برای حل همنهشتیهای خطی نیز به‌کار برد. این مطلب ارتباط نزدیکی با الگوریتم اقلیدسی توسعه یافته دارد که در دنبال توضیح (۲۳.۱) آمده است.

کسرهای مسلسل نامتناهی

در این بخش، کسر مسلسل سادهٔ نامتناهی را تعریف می‌کنیم و نشان می‌دهیم که مقدارکسر همواره یک عدد گنگ است.

(۱۲.۹) قضیه. فرض کنیم $a_۰$، $a_۱$، ... دنباله‌ای نامتناهی از اعداد صحیح باشد، به‌طوری که همهٔ عناصر آن احتمالاً بجز $a_۰$ مثبت هستند، و فرض می‌کنیم $c_k = \langle a_۰, a_۱, \ldots, a_k \rangle$. در این صورت $\lim_{k\to\infty} c_k$ وجود دارد. همچنین، به‌ازای هر $i \geq ۰$ و $j \geq ۰$، $c_{۲i} < \lim_{k\to\infty} c_k < c_{۲j+۱}$.

برهان. بنابر (۹.۹)، دنبالهٔ $\{c_{۲k}\}$ صعودی و از بالا کراندار است (مثلاً $c_۱$ یک کران بالای آن است)، و لذا $\lim_{k\to\infty} c_{۲k}$ وجود دارد. با استدلالی مشابه $\{c_{۲k+۱}\}$ دنباله‌ای نزولی و از پایین کراندار است (به $c_۰$)، و لذا همگراست. نشان خواهیم داد که این دو حد برابرند.

همانند برهان (۹.۹)، داریم $c_{2k+1} - c_{2k} = 1/q_{2k+1}q_{2k}$، که حد آن وقتی $k \to \infty$ برابر ۰ است زیرا $q_{2k} \geq 2k$ (توضیح بعد از (۳.۹) را ببینید). لذا $\lim c_{2k} = \lim c_{2k+1}$. فرض کنیم $\alpha = \lim c_{2k}$؛ به آسانی می‌توان دید که دنبالهٔ $\{c_k\}$ همگراست و حد آن α است. سرانجام، چون $\{c_{2k}\}$ اکیداً صعودی و $\{c_{2k+1}\}$ اکیداً نزولی است، لذا به‌ازای هر i و j، $c_{2i} < \alpha < c_{2j+1}$.

توضیح. بجاست تأکید کنیم که اگر $\alpha = \lim_{k\to\infty} c_k$، هر همگرای با اندیس فرد بزرگتر از α و هر همگرای با اندیس زوج کوچکتر از α است. این مطلب در بسیاری از مسائل به‌کار خواهد رفت. همچنین، توجه کنید که همگراهای با اندیس فرد متوالیاً به α نزدیکتر می‌شوند، و همچنین، همگراهای با اندیس زوج متوالیاً به α نزدیکتر می‌شوند.

(۱۳.۹) تعریف. فرض کنیم a_0، a_1، a_2، ... دنباله‌ای نامتناهی از اعداد صحیح باشد، به‌طوری که تمام جمله‌های آن بجز احتمالاً a_0 مثبت هستند. اگر $c_k = \langle a_0, a_1, \ldots, a_k\rangle$، آنگاه مقدار کسر مسلسل سادهٔ متناهی $\langle a_0, a_1, a_2, \ldots\rangle$ را به‌صورت $\lim_{k\to\infty} c_k$ تعریف می‌کنیم.

اندکی بعد ثابت خواهیم کرد که دو کسر مسلسل نامتناهی متمایز به مقادیر متفاوت همگرایند. لم زیر را لازم داریم.

(۱۴.۹) لم. فرض کنیم $\alpha = \langle a_0, a_1, a_2, \ldots\rangle$. در این‌صورت $a_0 = [\alpha]$ و $\alpha = a_0 + 1/\langle a_1, a_2, \ldots\rangle$.

برهان. با توجه به (۹.۹) و (۱۳.۹) روشن است که $a_0 = c_0 < \alpha < c_1 = a_0 + 1/a_1$. لذا چون $a_1 \geq 1$ داریم $a_0 < \alpha < a_0 + 1$، و بنابراین $a_0 = [\alpha]$. اگر $k \geq 1$، آنگاه $c_k = \langle a_0, a_1, \ldots, a_k\rangle = a_0 + 1/\langle a_1, \ldots, a_k\rangle$. با تعیین حد آن وقتی $k \to \infty$، داریم $\alpha = a_0 + 1/\langle a_1, a_2, \ldots\rangle$.

(۱۵.۹) قضیه. فرض کنیم دو کسر مسلسل نامتناهی $\langle a_0, a_1, a_2, \ldots\rangle$ و $\langle b_0, b_1, b_2, \ldots\rangle$ به یک مقدار همگرا باشند. در این‌صورت، به‌ازای هر $i \geq 0$، $a_i = b_i$.

برهان. فرض کنیم هر یک از کسرهای مسلسل همگرا به α باشد. از (۱۴.۹) نتیجه می‌شود که $a_0 = [\alpha] = b_0$. چون $a_0 + 1/\langle a_1, a_2, \ldots\rangle = b_0 + 1/\langle b_1, b_2, \ldots\rangle$، داریم $\langle a_1, a_2, \ldots\rangle = \langle b_1, b_2, \ldots\rangle$. استدلال مشابه نشان می‌دهد که $a_1 = b_1$. با ادامهٔ کار به استقرا نتیجه می‌گیریم که به‌ازای هر $i \geq 0$، $a_i = b_i$.

قضیهٔ بعد نشان می‌دهد که هر کسر مسلسل نامتناهی به یک عدد گنگ همگراست.

(۱۶.۹) قضیه. مقدار هر کسر مسلسل نامتناهی عددی است کنگ.

برهان. فرض کنیم $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$. اگر α گویا باشد، آنگاه $\alpha = m/n$، که در آن m و n اعداد صحیح هستند و $n > 0$. اگر k زوج باشد، بنابر (۱۲.۹)، $c_k < \alpha < c_{k+1}$. لذا

$$0 < \frac{m}{n} - \frac{p_k}{q_k} < \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{1}{q_k q_{k+1}}$$

با ضرب طرفین در nq_k داریم $0 < mq_k - np_k < n/q_{k+1}$، و لذا اگر عدد زوج k به‌قدر کافی بزرگ باشد $mq_k - nq_k < 1 < 0$. این ممکن نیست، زیرا $mq_k - np_k$ عدد صحیح است، لذا نتیجه می‌گیریم که α کنگ است.

کسر مسلسلِ نامتناهیِ یک عدد کنگ

در (۱۶.۹) نشان دادیم که یک کسر مسلسل نامتناهی معرف یک عدد کنگ است. آیا هر عدد کنگ یک بسط کسر مسلسل نامتناهی دارد؟ پاسخ مثبت است، و در این بخش روشی برای تعیین کسر مسلسل نامتناهی یک عدد کنگ مفروض به‌دست می‌دهیم.

(۱۷.۹) بحث. فرض کنیم α کنگ است، و فرض می‌کنیم $\alpha_0 = \alpha$. تعریف می‌کنیم $a_0 = [\alpha_0]$؛ چون α_0 کنگ است، پس $0 < \alpha_0 - a_0 < 1$. قرار می‌دهیم $\alpha_1 = 1/(\alpha_0 - a_0)$؛ در این‌صورت α_1 کنگ است، $\alpha_1 > 1$، و $\alpha_0 = a_0 + 1/\alpha_1$، یعنی $\alpha_0 = \langle a_0, \alpha_1 \rangle$. به روشی مشابه قرار می‌دهیم $a_1 = [\alpha_1]$ و فرض می‌کنیم $\alpha_1 = 1/(\alpha_1 - a_1)$؛ لذا $\alpha_0 = \langle a_0, a_1, \alpha_2 \rangle$. با ادامهٔ این روش، اگر α_1، α_2، ...، α_k و a_0، a_1، ...، a_k تعریف شده باشند، فرض می‌کنیم

$$a_{k+1} = \frac{1}{\alpha_k - a_k} \quad \text{و} \quad a_{k+1} = [\alpha_{k+1}]$$

در این‌صورت به‌ازای هر $k \geq 0$، $\alpha_0 = \langle a_0, a_1, \ldots, a_k, \alpha_{k+1} \rangle$.

قضیهٔ بعد فرمول روشنی برای تفاضل بین α و همگرای kام p_k/q_k به‌دست می‌دهد.

(۱۸.۹) قضیه. فرض کنیم α کنگ باشد، و فرض می‌کنیم α_i و a_i مانند (۱۷.۹) تعریف شده باشند. در این‌صورت

$$\alpha - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\alpha_{k+1} q_k + q_{k-1})}$$

برهان. چون به‌ازای $k \geq 0$، $\alpha = \langle a_0, a_1, \ldots, a_k, \alpha_{k+1} \rangle$، (۴.۹) ایجاب می‌کند که $\alpha = (\alpha_{k+1} p_k + p_{k-1})/(\alpha_{k+1} q_k + q_{k-1})$. با کم کردن p_k/q_k از دو طرف و ساده کردن حاصل، داریم

$$\alpha - \frac{p_k}{q_k} = \frac{p_{k-1} q_k - p_k q_{k-1}}{q_k(\alpha_{k+1} q_k + q_{k-1})},$$

و نتیجه از (۷.۹) به‌دست می‌آید.

اکنون ثابت می‌کنیم که هر عدد گنگ یک بسط کسر مسلسل نامتناهی دارد.

(۱۹.۹) قضیه. گیریم α گنگ باشد، و فرض می‌کنیم α_k و a_k مانند (۱۷.۹) تعریف شده باشند، در این‌صورت $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$. به‌طور کلی، به‌ازای هر $k \geq 0$، $\alpha_k = \langle a_k, a_{k+1}, a_{k+2}, \ldots \rangle$.

برهان. آشکار است که به‌ازای هر k، α_k گنگ است. لذا $0 < \alpha_k - a_k < 1$، و بنابراین به‌ازای هر $k \geq 0$، $\alpha_{k+1} > 1$ و $a_{k+1} > 1$. از (۱۸.۹) نتیجه می‌شود که $\lim_{k\to\infty}(p_k/q_k) = \alpha$، و لذا بنابه تعریف $\alpha = \langle a_k, a_{k+1}, a_{k+2}, \ldots \rangle$.

برای اثبات اینکه به‌ازای هر $k \geq 1$، $\alpha_k = \langle a_k, a_{k+1}, \ldots \rangle$، به آسانی روند کار را با a_k به جای $\alpha = \alpha_0$ شروع نموده و قسمت اول را به‌کار می‌بریم.

(۲۰.۹) مثال. روش بالا را برای محاسبهٔ بسط کسر مسلسل $\alpha = \sqrt{15}$ به‌کار می‌بریم. با انجام کار مانند (۱۷.۹) داریم

$$a_0 = [\sqrt{15}] = 3, \quad \alpha_1 = 1/(\alpha_0 - a_0) = 1/(\sqrt{15} - 3) = (\sqrt{15} + 3)/6;$$

$$a_1 = [\alpha_1] = 1, \quad \alpha_2 = 1/(\alpha_1 - a_1) = 1/((\sqrt{15} - 3)/6) = \sqrt{15} + 3;$$

$$a_2 = [\alpha_2] = 6, \quad \alpha_3 = 1/(\alpha_2 - a_2) = 1/(\sqrt{15} - 3).$$

چون $\alpha_1 = \alpha_3$، آشکار است که بسط کسر مسلسل $\sqrt{15}$ دوره‌یی است؛ یعنی، خارج‌قسمتهای جزئی تکرار می‌شوند، و داریم

$$\sqrt{15} = \langle 3, 1, 6, 1, 6, 1, 6 \ldots \rangle$$

توضیح. اگر α_1، α_2، α_3، ... را به‌طور جبری بیان کنیم، مثلاً اگر عبارت دقیق $\alpha_1 = (\sqrt{15} + 3)/6$ را به جای یک تقریب عددی به‌کار بریم، آنگاه آشکار می‌شود که چه

موقع αها شروع به تکرار شدن می‌کنند. ولی، اگر عبارتهای شامل $\sqrt{۱۵}$ را با یک حسابگر محاسبه کنیم، که یک تقریب از مقدار واقعی به‌دست دهد، آنگاه، مثلاً، ثابت نکرده‌ایم که $\alpha_۳ = \alpha_۱$؛ تنها نشان داده‌ایم که دو عدد تقریباً برابرند. در بخش بعد، تنها با استفاده از حساب عدد صحیح کامل، روش خیلی بهتری برای یافتن بسط کسر مسلسل بعضی از اعداد گنگ ارائه خواهیم داد.

کسرهای مسلسل دوره‌یی

اکنون به مطالعهٔ بسط کسر مسلسل اعدادی به‌صورت $(a + \sqrt{d})/b$ می‌پردازیم، که در آن a و b اعداد صحیح و d یک عدد صحیح مثبت است که مربع کامل نیست. (توجه کنید که بنابر مسألهٔ ۳۵.۱، $\sqrt{d}$ گنگ است.) نشان خواهیم داد که بسطهای کسر مسلسل چنین اعدادی دوره‌یی هستند و اینها تنها اعدادی هستند که بسط دوره‌یی دارند.

(۲۱.۹) تعریف. کسر مسلسل سادهٔ نامتناهی

$$\langle c_۰, c_۱, \ldots, c_n, \overline{a_۰\, a_۱, \ldots, a_{m-۱}} \rangle$$

دوره‌یی خوانده می‌شود. خط افقی در بالای ارقام مشخص می‌کند که دنبالهٔ $a_۰$، $a_۱$، ...، $a_{m_۱}$ به‌طور نامحدود تکرار می‌شود، کوچکترین مقدار m با این ویژگی طول دوره یا، به‌طور ساده‌تر، دورهٔ تناوب نامیده می‌شود. اگر کسر مسلسل به‌صورت $\langle \overline{a_۰, a_۱, \ldots, a_{m-۱}} \rangle$ باشد، دوره‌یی محض خوانده می‌شود.

مثلاً $\sqrt{۱۵} = \langle ۳, \overline{۱, ۶} \rangle = \langle ۳, ۱, ۶, ۱, ۶, ۱, ۶, \ldots \rangle$. ((۲۰.۹) را ببینید.)

(۲۲.۹) تعریف. عدد حقیقی α گنگ درجه دوم است اگر α گنگ و ریشهٔ یک چندجمله‌یی درجهٔ دوم با ضرایب صحیح باشد، یعنی هرگاه α جوابی از معادلهٔ $ax^۲ + bx + c = ۰$ باشد، که در آن a، b، c صحیح هستند و $a \neq ۰$.

(۲۳.۹) قضیه. اگر α یک عدد گنگ درجه دوم باشد، می‌توان α را به‌صورت $\alpha = (r+\sqrt{d})/s$ نوشت، که در آن d عدد صحیح مثبتی است که مربع کامل نیست و r و s اعداد صحیحی هستند به‌طوری که $s|d - r^۲$. علاوه بر این، اگر d، r، و s مفروض باشند به‌طوری که $\alpha = (r + \sqrt{d})/s$ ولی $s \nmid d - r^۲$، آنگاه می‌توانیم اعداد D، R، و S را بیابیم به‌طوری که $\alpha = (R + \sqrt{d})/S$ و $S|D - R^۲$.

برهان. اگر α یک عدد گنگ درجه دوم باشد، بنابه تعریف، α در معادله‌ای به‌صورت $ax^۲ + bx + c = ۰$ با $a \neq ۰$ صدق می‌کند؛ از این‌رو، $\alpha = (-b \pm \sqrt{b^۲ - ۴ac})/۲a$.

چون α عددی است گنگ، پس $b^2 - 4ac$ مربع کامل نیست. قرار می‌دهیم $d = b^2 - 4ac$. اگر $\alpha = (-b + \sqrt{d})/2a$، فرض می‌کنیم $r = -b$ و $s = 2a$؛ اگر $\alpha = (-b - \sqrt{d})/2a$، قرار می‌دهیم $r = b$ و $s = -2a$. در هر دو حالت، $s | d - r^2$.

اگر $\alpha = (r + \sqrt{d})/s$ و $s \nmid d - r^2$، می‌نویسیم $\alpha = (R + \sqrt{D})/S$، که در آن $D = ds^2$، $R = r|s|$، و $S = s|s|$. در این‌صورت $S | D - R^2$.

در قضیهٔ بعد الگوریتمی می‌دهیم که می‌توان آن را برای یافتن بسط کسر مسلسل یک عدد گنگ درجهٔ دوم به‌کار برد. این روش منتسب به اویلر است، اما اساساً همان تکنیک لرد ویلیام برونکر[1] (۱۶۸۴ـ۱۶۲۰) است که در یک قرن جلوتر، داده شده است، هر چند که برونکر به‌طور صریح کسرهای مسلسل را به‌کار نبرده است. این روش با «روش دوری» بهاسکره، بیش از پنج قرن قبل از برونکر، ارتباط نزدیکی دارد.

(۲۴.۹) قضیه. فرض کنیم α یک عدد گنگ درجهٔ دوم باشد، و قرار می‌دهیم $\alpha_0 = \alpha$، $a_0 = [\alpha]$. بنابر (۲۳.۹) می‌نویسیم $\alpha_0 = (r_0 + \sqrt{d})/s_0$ که در آن d مربع کامل نیست و $s_0 | d - r_0^2$. یادآور می‌شویم که $\alpha_{k+1} = 1/(\alpha_k - a_k)$ و $a_{k+1} = [\alpha_{k+1}]$ ((۱۷.۹)) را ببینید). به‌ازای $k \geq 0$ تعریف می‌کنیم

$$s_{k+1} = (d - r_{k+1}^2)/s_k, \qquad r_{k+1} = a_k s_k - r_k .$$

در این‌صورت، به‌ازای هر $k \geq 0$ احکام زیر برقرارند:

(الف) r_k و s_k اعداد صحیح هستند، با $s_k \neq 0$؛

(ب) $s_k | d - r_k^2$؛

(ج) $\alpha_k = (r_k + \sqrt{d})/s_k$، و لذا $a_k = [(r_k + \sqrt{d})/s_k]$.

برهان. اثبات به استقرا. به‌ازای $k = 0$ روشن است که این احکام برقرارند. فرض کنیم $k \geq 0$ و احکام برقرار باشند. از تعریف آشکار است که r_{k+1} عددی صحیح است و $r_{k+1} \equiv -r_k \pmod{s_k}$. لذا

$$d - r_{k+1}^2 \equiv d - r_k^2 \equiv 0 \pmod{s_k} .$$

از تعریف s_{k+1} نتیجه می‌شود که s_{k+1} عددی صحیح است، و چون d مربع کامل نیست $s_{k+1} \neq 0$. همچنین، $d - r_{k+1}^2 = s_k s_{k+1}$، و لذا $s_{k+1} | d - r_{k+1}^2$. سرانجام، چون $\alpha_k = (r_k + \sqrt{d})/s_k$، داریم

1. Lord William Brouncker

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} = \frac{s_k}{r_k + \sqrt{d} - a_k s_k} = \frac{s_k}{-r_{k+1} + \sqrt{d}}$$
$$= \frac{s_k(r_{k+1} + \sqrt{d})}{d - r_{k+1}^2} = \frac{r_{k+1} + \sqrt{d}}{s_{k+1}}$$

توضیح محاسبه‌یی. به‌ازای عدد گنگ درجهٔ دوم مفروض $\alpha = (r_0 + \sqrt{d})/s_0$، خارج‌قسمت جزئی آغازی a_0 تنها برابر است با $[\alpha]$. در این‌صورت اعداد r_1 و s_1 از فرمولهای بالا محاسبه می‌شوند، و خارج‌قسمت جزئی بعدی a_1 از تساوی $a_1 = [\alpha_1] = [(r_1+\sqrt{d})/s_1]$ به‌دست می‌آید. به‌طورکلی، اگر r_k و s_k به‌دست آمده باشند، آنگاه $a_k = [\alpha_k] = [(r_k + \sqrt{d})/s_k]$. در واقع، می‌توان محاسبه را ساده کرد:

$$a_k = [(r_k + a_0)/s_k],$$

که در آن $a_0 = [\sqrt{d}]$ (مسألهٔ ۵۹.۱ را ببینید). بنابراین، تمام آنچه لازم داریم بدانیم جزء صحیح $\sqrt{d}$ است.

می‌توان به الگوریتم بیان‌شده در (۲۴.۹) با توجه به رابطهٔ $s_{k+1} = s_{k-1} + a_k(r_k - r_{k+1})$ سرعت بخشید (مسألهٔ ۲۸.۹ را ببینید).

(۲۵.۹) مثال. روش بالا را برای محاسبهٔ بسط کسر مسلسل $\alpha = (۴ - \sqrt{۳})/۳$ به‌کار می‌بریم. $\alpha = \alpha_0$ را به‌صورت $(r+\sqrt{d})/s = (\sqrt{۳} - ۴)/-۳$ می‌نویسیم، در این‌صورت، $s \mid d - r^2$. لذا بایستی صورت و مخرج را در $|s| = |-۳| = ۳$ ضرب کنیم تا

$$\alpha_0 = (r_0 + \sqrt{d})/s_0 = (-۱۲ + \sqrt{۲۷})/(-۹)$$

را که $s_0 \mid d - r_0^2$ به‌دست آوریم. اکنون جدول زیر را با استفاده از فرمولهای ارائه‌شده در (۲۴.۹) می‌سازیم

k	۰	۱	۲	۳	۴	۵
r_k	-۱۲	۱۲	۱	۵	۵	۵
s_k	-۹	۱۳	۲	۱	۲	۱
a_k	۰	۱	۳	۱۰	۵	

چون $a_k = [\alpha_k] = [(r_k + ۵)/s_k]$، ملاحظه می‌کنیم که به‌ازای هر k، $a_5 = [\sqrt{۲۷}] = ۵$. چون $r_3 = r_5$ و $s_3 = s_5$، روشن است که از $k = ۵$ به بعد جدول تکرار می‌شود. لذا $(۴ - \sqrt{۳})/۳ = \langle ۰, ۱, ۳, \overline{۱۰, ۵} \rangle$.

همچنین داریم $\alpha_k = (r_k + \sqrt{d})/s_k = \langle a_k, a_{k+1}, \ldots \rangle$. لذا، مثلاً $\alpha_2 = (1 + \sqrt{27})/2 = \langle 3, \overline{10, 5} \rangle$ و $\alpha_3 = 5 = \sqrt{27} = \langle \overline{10, 5} \rangle$.

(۲۶.۹) تعریف. فرض کنیم $\alpha = (a + b\sqrt{d})/c$، که در آن a، b، و c اعداد صحیح هستند، با $c \neq 0$، و d عدد صحیحی است که مربع کامل نیست. در این‌صورت α'، مزدوج α با $\alpha' = (a - b\sqrt{d})/c$ تعریف می‌شود.

عمل مزدوج‌گیری تعدادی ویژگی ساده دارد که بارها به‌کار خواهند رفت. مسألهٔ ۲۹.۹ را برای براهین ببینید.

(۲۷.۹) لم. فرض کنیم α و β هر کدام به‌صورت $(a + b\sqrt{d})/c$ باشند که d ثابت است. در این‌صورت $(\alpha + \beta)' = \alpha' + \beta'$، $(\alpha\beta)' = \alpha'\beta'$، و $(\alpha/\beta)' = \alpha'/\beta'$.

(۲۸.۹) قضیهٔ (لاگرانژ). بسط کسر مسلسل هر عدد گنگ درجه دوم دوره‌یی است.

برهان. فرض کنیم α یک عدد گنگ درجه دوم باشد، و الگوریتم بیان‌شده در (۲۴.۹) را به‌کار می‌بندیم. ابتدا نشان می‌دهیم عدد صحیح m وجود دارد به‌طوری که $\alpha'_m < 0$ (α'_m مزدوج α_m است). با توجه به (۱۸.۹) یادآور می‌شویم که $\alpha - p_k/q_k = (-1)^k/q_k(\alpha_{k+1}q_k + q_{k-1})$. در ضرب این رابطه در مزدوجش داریم

$$\left(\alpha - \frac{p_k}{q_k}\right)\left(\alpha' - \frac{p_k}{q_k}\right) = \frac{1}{q_k^2(\alpha_{k+1}q_k + q_{k-1})(\alpha'_{k+1}q_k + q_{k-1})}.$$

چون $\alpha' \neq \alpha$ و p_k/q_k همگرا به α است، لذا مقداری از k وجود دارد به‌طوری که p_k/q_k بین α و α' واقع می‌شود (توضیح بعد از (۱۲.۹) را ببینید). به‌ازای این k، سمت چپ رابطهٔ بالا منفی است، لذا $\alpha'_{k+1}q_k + q_{k-1} < 0$؛ از این‌رو اگر $m = k + 1$، آنگاه $\alpha'_m < 0$.

درواقع، اگر به‌ازای $m > 0$، $\alpha'_m < 0$، آنگاه به‌ازای هر $n > m$، $-1 < \alpha'_n < 0$. برای اثبات این مطلب کافی است نشان دهیم که $-1 < \alpha'_{m+1} < 0$. چون $\alpha_{m+1} = 1/(\alpha_m - a_m)$، داریم $-1 < \alpha'_{m+1} < 0$ $\alpha'_{m+1} = 1/(\alpha'_m - a_m)$، و لذا چون $a_m \geq 1$، $-1 < \alpha'_{m+1}$. اکنون فرض کنیم $k \geq 1$ به اندازهٔ کافی بزرگ باشد به‌طوری که $-1 < \alpha'_k < 0$. در این‌صورت $0 < s_k < 2\sqrt{d}$ و لذا $1 < \alpha_k - \alpha'_k = 2\sqrt{d}/s_k$. چون $\alpha_k = (r_k + \sqrt{d})/s_k$، داریم $\alpha_k\alpha'_k = (r_k^2 - d)/s_k^2$. در نتیجه $r_k^2 < d$، یعنی $-\sqrt{d} < r_k < \sqrt{d}$. در واقع، چون $0 < \alpha_k + \alpha'_k = 2r_k/s_k$، $0 < \alpha_k$، $r_k > 0$.

لذا به‌ازای kهای بزرگ، جفت r_k، s_k حداکثر $2d$ مقدار متفاوت اختیار می‌کنند، و بنابراین اعداد صحیح m و n یا $m < n$ وجود دارند به‌طوری که $r_n = r_m$ و $s_n = s_m$. در این‌صورت رابطه‌های بازگشتی ارائه شده در (۲۴.۹) ایجاب می‌کند که به‌ازای هر عدد صحیح مثبت t، $a_{m+t} = a_{n+t}$، و لذا بسط کسر مسلسل α دوره‌یی است.

توضیح. عکس قضیهٔ لاگرانژ نیز برقرار است، مقدار هر کسر مسلسل دوره‌یی عدد گنگ درجه دوم است (مسألهٔ ۳۰.۹ را ببینید).

یک مثال ملموس برای نشان دادن چگونگی انجام محاسبات می‌آوریم:

(۲۹.۹) مثال. برای یافتن مقدارکسر مسلسل دوره‌یی $\alpha = \langle 4, \overline{3, 2} \rangle$، قرار می‌دهیم $\beta = \langle \overline{3, 2} \rangle$. در این‌صورت

$$\beta = 3 + 1/(2 + 1/\beta) = 3 + \beta/(2\beta + 1) = (7\beta + 3)/(2\beta + 1)$$

و لذا $2\beta^2 - 6\beta - 3 = 0$. از آنجا، چون روشن است که $\beta > 0$، داریم $\beta = (3 + \sqrt{5})/2$. لذا $\alpha = 4 + 1/\beta = (9 + \sqrt{15})/3$.

کسرهای مسلسل دوره‌یی محض

در بخش قبل نشان دادیم که هر عدد گنگ درجه دوم یک بسط کسر مسلسل دوره‌یی دارد. اکنون به بررسی مسألهٔ تعیین اعداد گنگ درجه دومی می‌پردازیم که بسط دوره‌یی محض، یعنی، بسطی به‌صورت $\langle \overline{a_0, a_1, \ldots, a_m} \rangle$ دارند.

(۳۰.۹) تعریف. عدد گنگ درجه دوم $\alpha = (r + \sqrt{d})/s$ را ساده‌شده خوانیم هرگاه $\alpha > 1$ و مزدوجش $\alpha' = (r - \sqrt{d})/s$ در $-1 < \alpha' < 0$ صدق کند.

قضیهٔ بعد اعداد گنگی را که بسط دوره‌یی محض دارند مشخص می‌کند. این تشخیص قبلاً درکار لاگرانژ اشاره شده است، ولی اولین برهان در ۱۸۲۸ توسط اِ وارِست گالوا[1] (۱۸۳۲ـ۱۸۱۱) داده شده است.

(۳۱.۹) قضیه. عدد گنگ درجه دوم α دارای یک کسر مسلسل دوره‌یی محض است اگر و تنها اگر α ساده شده باشد، همچنین، اگر $\alpha = \langle \overline{a_0, a_1, \ldots, a_{m-1}} \rangle$، آنگاه $-1/\alpha' = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_1, a_0} \rangle$.

1. Évariste Galois

برهان. ابتدا فرض می‌کنیم که $\alpha = \langle a_0, a_1, \ldots \rangle$ ساده شده باشد، و فرض می‌کنیم α_k مانند (۱۷.۹) تعریف شده باشد. از $\alpha_{k+1} = 1/(\alpha_k - a_k)$ با مزدوج‌گیری داریم $\alpha'_{k+1} = 1/(\alpha'_k - a_k)$. چون $a_k \geq 1$، نتیجه می‌شود که اگر $\alpha'_k < 0$، آنگاه $-1 < \alpha'_{k+1} < 0$. لذا اگر α_k ساده شده باشد، α_{k+1} نیز هست. اما $\alpha = \alpha_0$ ساده شده است، و لذا به‌ازای هر n، α_n ساده شده است. از $\alpha'_{k+1} = 1/(\alpha'_k - a_k)$ داریم $\alpha'_k = a_k + 1/\alpha'_{k+1}$. با فرض $\beta_i = -1/\alpha'_i$، داریم $\beta_{k+1} = a_k + 1/\beta_k$. توجه داریم که $0 < \beta_k < 1$، و لذا $a_k = [\beta_{k+1}]$.

بسط کسر مسلسل α دوره‌یی است، مثلاً با دورهٔ m. لذا j وجود دارد به‌طوری که $\alpha_{m+j} = \alpha_j$، و با مزدوج‌گیری داریم $\beta_{m+j} = \beta_j$. اگر $j > 0$، آنگاه

$$\beta_j = a_{j-1} + \frac{1}{\beta_{j-1}} \quad \text{و} \quad \beta_{m+j} = a_{m+j-1} + \frac{1}{\beta_{m+j-1}}$$

چون $a_{j-1} = [\beta_j]$ و $a_{m+j-1} = [\beta_{m+j}]$، در نتیجه $a_{j-1} = a_{m+j-1}$، و بنابراین $1/\beta_{m+j-1} = 1/\beta_{j-1}$. اکنون با وارون کردن این رابطه و سپس با مزدوج‌گیری $\alpha_{j-1} = \alpha_{m+j-1}$ حاصل می‌شود؛ اگر $j - 1 > 0$، عمل را تکرار می‌کنیم. سرانجام، $\alpha_0 = \alpha_m$ را به‌دست می‌آوریم، یعنی، α یک بسط کسر مسلسل دوره‌یی محض دارد.

برای اثبات عکس فرض می‌کنیم $\alpha = \langle \overline{a_0, a_1, \ldots, a_{m-1}} \rangle$. حالت $m = 1$ بدیهی است، لذا فرض می‌کنیم $m > 1$. چون $\alpha_0 = \alpha_m > 1$، داریم $a_0 \geq 1$، و لذا تمام a_iها مثبت هستند. با فرض $k = m - 1$ در معادلهٔ $\beta_{k+1} = a_k + 1/\beta_k$، رابطهٔ

$$\beta_0 = \beta_m = a_{m-1} + 1/\beta_{m-1} = \langle a_{m-1}, \beta_{m-1} \rangle$$

را به‌دست می‌آوریم. اما $\beta_{m-1} = a_{m-2} + 1/\beta_{m-2}$، و لذا $\beta_0 = \langle a_{m-1}, a_{m-2}, \beta_{m-2} \rangle$. اگر به این طریق ادامه دهیم داریم

$$\beta_0 = \langle a_{m-1}, a_{m-2}, \ldots, a_0, \beta_0 \rangle$$

و بنابراین

$$-1/\alpha' = \beta_0 = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_0} \rangle .$$

به‌ویژه، $-1/\alpha' > 1$، و لذا α ساده شده است.

(۳۲.۹) مثال. اگر $\alpha = 5 + \sqrt{27}$، آنگاه $\alpha' = 5 - \sqrt{27}$ و $-1 < \alpha' < 0$، لذا α ساده شده است. بنابر (۲۵.۹)، α دارای بسط دوره‌یی محض $\langle \overline{10, 5} \rangle$ است.

تقریبهای گویا برای اعداد گنگ

اگر α عدد گنگی باشد و p_k/q_k همگرای kام بسط کسر مسلسل α باشد، آنگاه دنبالهٔ $\{p_k/q_k\}$ همگرا به α است، بنابراین با انتخاب k به اندازهٔ کافی بزرگ هر قدر بخواهیم می‌توان p_k/q_k را به α نزدیک کرد. لذا همگراهای α تقریبهای به دلخواه نزدیک به α را عرضه می‌کنند. قضیهٔ بعد تخمینی است برای اینکه ببینیم تا چه اندازه این تقریبها خوب هستند.

(۳۳.۹) قضیه. فرض کنیم p_k/q_k همگرای kام عدد گنگ α باشد. در این‌صورت به‌ازای هر $k \geq ۰$،

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{۱}{q_k q_{k+۱}}$$

به‌ویژه به‌ازای هر $k \geq ۰$، $|\alpha - p_k/q_k| < ۱/q_k^۲$.

برهان. بنابر (۱۸.۹)، $|\alpha - p_k/q_k| = ۱/q_k(\alpha_{k+۱}q_k + q_{k-۱})$. چون $\alpha_{k+۱} < q_{k+۱}$ و $a_{k+۱}q_k + q_{k-۱} = q_{k+۱}$، قضیه نتیجه می‌شود.

(۳۴.۹) قضیه. فرض کنیم α عددی گنگ و $\alpha = \langle a_۰, a_۱, a_۲, \ldots\rangle$، و همگرای kام آن $p_k/q_k = \langle a_۰, a_۱, \ldots, a_k\rangle$. در این‌صورت همگراهای α متوالیاً به α نزدیکترند، یعنی،

$$|\alpha - p_{k+۱}/q_{k+۱}| < |\alpha - p_k/q_k| \qquad (۱)$$

در واقع نابرابری قوی‌تر زیر را داریم

$$|q_{k+۱}\alpha - p_{k+۱}| < |q_k\alpha - p_k|\,. \qquad (۲)$$

برهان. اگر (۳۳.۹) را با $k+۱$ به جای k به‌کار بریم داریم $|q_{k+۱}\alpha - p_{k+۱}| < ۱/q_{k+۲}$. بنابر (۱۸.۹)، $|q_k\alpha - p_k| = ۱/(\alpha_{k+۱}q_k + q_{k-۱})$. چون $a_{k+۱} = [\alpha_{k+۱}]$، داریم

$$q_k\alpha_{k+۱} + q_{k-۱} < q_kq_{k+۱} + q_k + q_{k-۱} = q_{k+۱} + q_k$$

اما $q_{k+۱} + q_k \geq q_{k+۱} + q_k = a_{k+۲}q_{k+۱} + q_k$، و نابرابری (۲) نتیجه می‌شود. نابرابری (۱) نتیجهٔ سادهٔ (۲) است.

قضیهٔ بعد نشان می‌دهد که همگراهای α نقش بسیار استثنائی در یافتن اعداد صحیح s و t به‌طوری که $|t\alpha - s|$ کوچک باشد بازی می‌کنند.

(۳۵.۹) قضیه. گیریم α عدد گنگی باشد، و فرض می‌کنیم s/t $(t > 0)$ دارای این ویژگی باشد که اگر $1 \le v < t$ آنگاه $|t\alpha - s| < |v\alpha - u|$. در این‌صورت، s/t یک همگرای α است.

برهان. فرض کنیم $c_k = p_k/q_k$ همگرای kام α باشد. ابتدا فرض می‌کنیم که $s/t < c_0$. در این‌صورت $|t\alpha - s| \ge |\alpha - s/t| > |\alpha - c_0| = |q_0\alpha - p_0|$ (زیرا $q_0 = 1$)، که با فرضِ مربوط به s/t تناقض دارد.

اکنون فرض کنیم $s/t > c_1$؛ در این‌صورت $|\alpha - s/t| > |c_1 - s/t|$. از آنجا $|t\alpha - s| > |tp_1 - sq_1|/q_1 \ge 1/q_1$. اما بنابر (۳۳.۹) داریم $|a_0\alpha - p_0| < 1/q_1$، لذا مجدداً به تناقض می‌رسیم.

بنابراین nی وجود دارد به‌طوری که s/t بین c_{n-1} و c_{n+1} قرار می‌گیرد. اگر s/t با یکی از c_{n-1} یا c_{n+1} برابر باشد اثبات تمام است. در غیر این‌صورت، توجه می‌کنیم که این دو همگرا در یک طرف α، و c_n در طرف دیگر آن واقع می‌شوند. در نتیجه $|s/t - c_{n-1}| < |c_n - c_{n-1}|$. از ضرب طرفین در tq_nq_{n-1}، داریم $q_n|sq_{n-1} - tp_{n-1}| < t|p_nq_{n-1} - p_{n-1}q_n| = t$. چون $sq_{n-1} - tp_{n-1}$ نامنفی است، لذا $q_n < t$.

همچنین، داریم $|\alpha - s/t| > |c_{n+1} - s/t|$. از ضرب طرفین در t، داریم

$$|t\alpha - s| > |tp_{n+1} - sq_{n+1}|/q_{n+1} \ge 1/q_{n+1}$$

اما بنابر (۳۳.۷)، $|q_n\alpha - p_n| < 1/q_{n+1}$. چون $a_n < t$، باز هم به تناقض می‌رسیم و برهان کامل می‌شود.

(۳۶.۹) فرع. گیریم α عددی گنگ باشد، و فرض می‌کنیم c و $d > 0$ اعداد صحیحی باشند. اگر $|d\alpha - c| < |q_k\alpha - p_k|$، آنگاه $d \ge q_{k+1}$.

برهان. فرض می‌کنیم t کوچکترین عدد صحیح مثبت است که به‌ازای آن عددی مانند s وجود دارد به‌طوری که $|t\alpha - s| < |q_k\alpha - p_k|$. بنابر (۳۵.۹)، s/t یک همگرای α است؛ فرض کنیم $s/t = p_m/q_m$. چون همگراهای α متوالیاً به α نزدیکتر می‌شوند، لذا $m \ge k+1$، و بنابراین $t \ge q_{k+1}$. چون روشن است که $d \ge t$، نتیجه حاصل می‌شود.

قضیهٔ بعد نشان می‌دهد که p_k/q_k یعنی همگرای kام عدد گنگ α در واقع بهترین تقریب گویا به α در بین همهٔ اعداد گویایی است که مخرجشان نابزرگتر q_k هستند.

(۳۷.۹) قضیه. اگر $k \ge 1$ وجود داشته باشد به‌طوری که $|\alpha - c/d| < |\alpha - p_k/q_k|$، آنگاه $d > q_k$.

برهان خلف. فرض کنیم $d \leq q_k$. از ضرب این نابرابری در نابرابری فرض داریم $|\alpha d - c| < |\alpha q_k - p_k|$. لذا بنابر (۳۶.۹) داریم $d \geq q_{k+1}$. این با فرض $d \leq q_k$ تناقض دارد مگر اینکه $a_{k+1} = 1$، و این نیز به‌ازای $k \geq 1$ ممکن نیست.

توضیح. در واقع، اگر $q_{k+1} > 2q_k$ نتیجه‌ای قوی‌تر برقرار است؛ اگر $|\alpha - c/d| < |\alpha - p_k/q_k|$، آنگاه $d > q_{k+1}/2$. مسألهٔ ۴۶.۹ را برای یک برهان ببینید.

پاسخ به سؤال کلیتر زیر دشوارتر است: اگر s عدد صحیح مثبتی باشد، بهترین تقریب به عدد گنگ α در میان همهٔ اعداد گویایی که مخرجشان نابزرگتر از s است چیست؟ (قضیه قبل فقط پاسخ به حالتی است که در آن به‌ازای kای $s = q_k$.) پاسخ به این سؤال متضمن مفهوم همگراهای میانی α است، که در بخش آخر این مسائل مطرح شده‌اند. جواب کامل در مسألهٔ ۶۶.۹ آمده است: به‌ازای هر عدد صحیح مثبت s، بهترین تقریب گویا برای α با مخرج نابیشتر از s یا یک همگرا یا یک همگرای میانی α است.

(۳۸.۹) مثال. قضیه‌های پیشین را برای یافتن «بهترین» تقریبهای گویای π می‌توان به‌کار برد. با استفاده از تکنیک (۱۷.۹) می‌توانیم نُه نخستین خارج‌قسمت جزئی π را محاسبه کنیم: $\pi = \langle 3, 7, 15, 1, 292, 1, 1, 1, 2, \ldots \rangle$. (مسألهٔ ۵۷.۹ را ببینید. دقت این مقادیر به دقت حسابگری که به‌کار می‌رود بستگی دارد.) جدول زیر را تشکیل می‌دهیم:

k	-1	0	1	2	3	4
a_k		۳	۷	۱۵	۱	۲۹۲
p_k	۱	۳	۲۲	۳۳۳	۳۵۵	۱۰۳۹۹۳
q_k	۰	۱	۷	۱۰۶	۱۱۳	۳۳۱۰۲

همگرای p_1/q_1 همان تقریب آشنای ۲۲/۷ است که اولین بار توسط ارشمیدس در حدود ۲۵۰ ق. م داده شده است. این عدد بهترین تقریب در میان همهٔ اعداد گویایی است که مخرجشان از ۷ تجاوز نمی‌کند، تقریب $p_2/q_2 = 333/106$ اولین بار در قرن شانزدهم در اروپا ظاهر شد، و تقریب قابل ملاحظهٔ ۳۵۵/۱۱۳ در قرن پنجم برای چینیها معلوم بوده است. بنابر (۳۳.۹)،

$$|\pi - 355/113| < 1/113 \times 33102 < 0.0000003$$

و لذا ۳۵۵/۱۱۳ تا ۶ رقم دقیق است. در واقع ۳۵۵/۱۱۳ در میان همهٔ اعداد گویایی که

مخرجشان از ۱۶۶۰۳ تجاوز نمی‌کنند بهترین تقریب به π است (مسألهٔ ۷۰.۹). برای نتایج بیشتر در مورد π، مسائل ۵۴.۹ تا ۵۹.۹ و مسأله ۶۹.۹ را ببینید.

قضیهٔ زیر نشان می‌دهد که اگر یک عدد گویا عدد گنگ α را به اندازهٔ «کافی» نزدیک تقریب بزند، آنگاه عدد گویا بایستی یکی از همگراهای بسط کسر مسلسل نامتناهی α باشد. (برای یک برهان، مسأله ۵۳.۹ را ببینید.)

(۳۹.۹) قضیه. فرض کنیم α عدد گنگ باشد. اگر عدد گویای c/d با $d \geq 1$ به‌گونه‌ای باشد که $|\alpha - c/d| < 1/2d^2$، آنگاه c/d یکی از همگراهای بسط کسر مسلسل نامتناهی α است.

قضیهٔ قبل درفصل ۱۰ برای نشان دادن ارتباط بین کسرهای مسلسل و معادلهٔ پِل به‌کار می‌رود.

توضیح. اینکه هر همگرای α در نابرابری (۳۹.۹) (که آشکارا قوی‌تر از نابرابری دوم (۳۳.۹) است) صدق می‌کند درست نیست. ولی، از دو همگرای متوالی، حداقل یکی، مثلاً p/q، در نابرابری $|\alpha - p/q| < 1/2q^2$ صدق می‌کند. (برای یک برهان مسأله ۵۲.۹ را ببینید.) سرانجام متذکر می‌شویم که قضیه‌های قبلی تقریبها، با اندکی استثنا، وقتی α گویا باشد نیز برقرارند.

یک کاربرد: تقویمها

کرهٔ زمین تقریباً در هر ۳۶۵ روز، ۵ ساعت، ۴۸ دقیقه، و ۴۶ ثانیه خورشید را یک دور می‌زند. لذا طول واقعی یک سال ۳۶۵ روز و ۲۰۹۲۶/۸۶۴۰۰ از یک روز است. چگونه می‌توان یک تقویم را که اساس آن بر مبنای یک سال ۳۶۵ روز نهاده شده اصلاح کرد تا تقریب دقیقتری به مقدار واقعی به‌دست دهد؟ جواب به یافتن یک تقریب خوب برای ۲۰۹۲۶/۸۶۴۰۰ بستگی دارد، کاری که انجام آن آسان است.

با کاربرد الگوریتم اقلیدسی بسط کسر مسلسل ۲۰۹۲۶/۸۶۴۰۰، یعنی $\langle 0, 4, 7, 1, 3, 5, 64 \rangle$ کار را آغاز می‌کنیم. اکنون جدول زیر را ترتیب می‌دهیم

k	-1	0	1	2	3	4	5
a_k		0	4	7	1	3	5
p_k	1	0	1	7	8	31	163
q_k	0	1	4	29	33	128	673

در سال ۴۵ ق. م. یولیوس سزار[1] تصحیح ۱/۴ (که همگرای p_1/q_1 است) را با افزودن

1. Julius Caesar

یک روز ــ ۲۹ فوریه ــ در هر ۴ سال، یعنی ۱/۴ روز برای هر سال، به‌کار برد. کاربرد یک سال کبیسه تقویم یولیایی را در حدود ۱۱ دقیقه در یک سال تصحیح کرد، که به خطای تقریباً ۱۰ روز در ۱۵۰۰ سال بالغ می‌شود. همان‌گونه که در پاراگراف بعد بیان شده است، این مطلب تصحیح بیشتری را از سوی پاپ گرگوری[1] XIII ضروری ساخت.

در سدهٔ یازدهم، منجم، ریاضیدان، و شاعر ایرانی اَل خیامی (۱۱۲۳ـ۱۰۵۰) که در غرب به عمرخیام معروف است، تصحیح ۸/۳۳ (همگرای p_3/q_3) را پیشنهاد کرد، که خطای فقط ۱۹ ثانیه در سال را می‌داد. تقویم گرگوری در هر سال که مضرب ۴ باشد، بجز سالهایی که مضرب ۱۰۰ هستند ولی به ۴۰۰ بخشپذیر نیستند، یک روز اضافه دارد، دقت تقویم گرگوری در حدود ۲۶ ثانیه در سال است. این تصحیح با تقریب ۲۰۹۲۶/۸۶۴۰۰ به ۹۷/۴۰۰ متناظر است، زیرا در هر ۴۰۰ سال ۹۷ سال کبیسه وجود دارد. گرچه ۹۷/۴۰۰ یکی از همگراهای ۲۰۹۲۶/۸۶۴۰۰ نیست، ولی انجام تصحیحی که هم‌اکنون بیان شد آسانتر از کاربرد تصحیح دقیقتر ۸/۳۳ است.

سرانجام، خاطرنشان می‌کنیم که همگرای چهارم ۳۱/۱۲۸ (که می‌توان آن را به‌کار گرفت، مثلاً، با حذف یک کبیسه در هر ۱۲۸ سال) تصحیح به‌غایت دقیقی به‌دست می‌دهد: ۳۱/۱۲۸ + ۳۶۵ با طول واقعی سال تا ۴ رقم اعشار مطابقت دارد. در واقع، خطای حاصل تقریباً یک ثانیه در سال، یا حدود یک و نیم دقیقه در هر قرن است.

مسأله‌ها و راه‌حلها

کسرهای مسلسل متناهی

۱.۹ بسطهای کسر مسلسل هر یک از اعداد گویای زیر را به‌دست آورید: (الف) ۳۵۵/۱۱۳، (ب) ۵/۳۲، (ج) ۴۷۵۶/۱۱۲۱.

حل. (الف) با کاربرد الگوریتم اقلیدسی داریم ۱۶+۳×۱۱۳=۳۵۵، ۱+۷×۱۶=۱۱۳، ۱×۱۶=۱۶. بنابراین $\langle 3,7,15,1\rangle = \langle 3,7,16\rangle = 355/113$. (ب) همچنین $\langle 0,6,2,1,1\rangle = \langle 0,6,2,2\rangle = 5/32$. (ج) $4756 = 1121 \times 4 + 272$، $1121 = 272 \times 4 + 33$، $272 = 33 \times 8 + 8$، $33 = 8 \times 4 + 1$، $8 = 8 \times 1$. لذا $\langle 4,4,8,4,7,1\rangle = \langle 4,4,8,4,8\rangle = 4756/1121$.

توضیح. می‌توانستیم بسط کسر مسلسل ۴۷۵۶/۱۱۲۱ را با استفاده از تکنیک بیان‌شده در (۱۷.۹) نیز پیدا کنیم، هر چند که α در اینجا گویاست. (بهتر است خاطرجمع باشید که

1. Pope Gregory

این روش هنوز هم کسر مسلسل α را حتی وقتی α گویاست تولید می‌کند.) در این حالت، با $\alpha_۰ = ۴۷۵۶/۱۱۲۱$ داریم $a_۰ = [\alpha_۰] = ۴$، $\alpha_۱ = ۱/(\alpha_۰ - a_۰) = ۴٫۱۲۱۳۰۰۰$، و مانند آن. بسیار آسانتر خواهد بود اگر حسابگر به‌کار گرفته شود: اگر $\alpha_{k-۱}$ معلوم باشد، جزء صحیح آن را (که $a_{k-۱}$ است) کم کنید و حاصل را وارون سازید، و این روند را تا به‌ازای مقداری از k که عدد صحیح شود تکرار کنید. در این‌صورت $a_k = [a_k]$ آخرین خارج‌قسمت جزئی است.

ولی مواظب باشید: نبود دقت کافی حسابگر معمولاً در آنچه که باید مرحلهٔ نهایی باشد عددی را ادامه می‌دهد که عدد صحیح نیست. در این مثال، آخرین خارج‌قسمت جزئی در حسابگر ۷٫۹۹۹۹۹۴۹۵۴ بود، که تقریب مقدار درست ۸ است. اگر فرض نمی‌کردیم که این باید ۸ باشد و روند را با کم کردن ۷ و سپس وارون کردن ادامه می‌دادیم، کسر جزئی ۱ را به‌دست می‌آوردیم، و یک مرحلهٔ بیشتر مقدار کاملاً نادرست ۱۹۸۱۵۹ را به ما می‌داد!

۲.۹ اعداد گویای معرف بسط کسرهای مسلسل زیر را تعیین کنید. (الف) $\langle ۱, ۲, ۳\rangle$، (ب) $\langle -۳, ۴, ۲, ۵\rangle$، (ج) $\langle ۱, ۱, ۱, ۱, ۱, ۱\rangle$.

حل. در هر حالت، بهترین روش تشکیل یک جدول همانند (۶.۹) است:

k	-۱	۰	۱	۲
a_k		۱	۲	۳
p_k	۱	۱	۳	۱۰
q_k	۰	۱	۲	۷

k	-۱	۰	۱	۲	۳
a_k		-۳	۴	۲	۵
p_k	۱	-۳	-۱۱	-۲۵	-۱۳۶
q_k	۰	۱	۴	۹	۴۹

لذا، بنابر (۴.۹) $\langle ۱, ۲, ۳\rangle = p_۲/q_۲ = ۱۰/۷$ و $\langle -۳, ۴, ۲, ۵\rangle = p_۳/q_۳ = -۱۳۶/۴۹$.
به روش مشابه می‌توان نشان داد که $\langle ۱, ۱, ۱, ۱, ۱, ۱\rangle = ۱۳/۸$.

۳.۹ جدولی تشکیل دهید و همگراهای ۷۷۶/۲۴۷ را حساب کنید.

حل. با استفاده از الگوریتم اقلیدسی داریم $\langle ۳, ۷, ۱۷, ۲\rangle = ۷۷۶/۲۴۷$. (اگر از روش بیان‌شده در «توضیح» بعد از مسأله ۱.۹ استفاده شود، محققاً ۱٫۹۹۹۹۹۹۸۹۸ به‌صورت ۲ منظور می‌شود.) اکنون جدول زیر را تشکیل می‌دهیم:

k	-۱	۰	۱	۲	۳
a_k		۳	۷	۱۷	۲
a_k	۱	۳	۲۲	۳۷۷	۷۷۶
q_k	۰	۱	۷	۱۲۰	۲۴۷

لذا همگراهای ۷۷۶/۲۴۷ عبارت‌اند از ۳، ۲۲/۷، ۳۷۷/۱۲۰، و ۷۷۶/۲۴۷.

۴.۹ به استقرا ثابت کنید که یک کسر مسلسل سادهٔ متناهی نمایش یک عدد گویاست.

حل. به استقرا روی n نشان می‌دهیم که هرکسر مسلسل سادهٔ متناهی با n خارج‌قسمت جزئی نمایش یک عدد گویاست. به‌ازای $n = ۰$ نتیجه آشکار است. فرض کنیم $n \geq ۰$ و هرکسر مسلسل با n خارج‌قسمت جزئی نمایش یک عدد گویا باشد. اگر $\langle a_۰, a_۱, \ldots, a_n\rangle$ کسر مسلسلی با $n+۱$ خارج‌قسمت جزئی باشد، داریم $\langle a_۰, a_۱, \ldots, a_n\rangle = a_۰ + ۱/\langle a_۱, a_۲, \ldots, a_n\rangle$، که بنابر فرض استقرا یک عدد گویاست.

۵.۹ فرض کنیم $r = \langle a_۰, a_۱, \ldots, a_n\rangle = \langle b_۰, b_۱, \ldots, b_m\rangle$، به‌طوری که اعداد صحیح a_i و b_i همگی بجز احتمالاً $a_۰$ و $b_۰$ مثبت هستند، اگر $a_n > ۱$ و $b_m > ۱$، ثابت کنید $m = n$ و به‌ازای $i = ۰, ۱, ۲, \ldots, n$، $a_i = b_i$.

حل. اگر r عدد صحیحی باشد، آنگاه $n = ۰$؛ در غیر این‌صورت، $a_۰ < r = \langle a_۰, a_۱, \ldots, a_n\rangle = a_۰ + ۱/\langle a_۱, \ldots, a_n\rangle < a_۰ + ۱$، که غیرممکن است. به تشابه داریم $m = ۰$، و لذا $a_۰ = b_۰ = r$. حال فرض می‌کنیم که r عدد صحیحی نباشد، در این‌صورت، $n \geq ۱$ و $m \geq ۱$، و داریم

$$r = a_۰ + ۱/\langle a_۱, a_۲, \ldots, a_n\rangle = b_۰ + ۱/\langle b_۱, b_۲, \ldots, b_m\rangle$$

روشن است که، $۰ < ۱/\langle a_۱, a_۲, \ldots, a_n\rangle < ۱$ و $۰ < ۱/\langle b_۱, b_۲, \ldots, b_m\rangle < ۱$. چون $a_n > ۱$ داریم $a_۱ > ۱$ یا $n \geq ۲$. در هر دو حالت، $۱/\langle a_۱, \ldots, a_n\rangle < ۱$؛ با استدلالی مشابه، $۱/\langle b_۱, \ldots, b_m\rangle < ۱$. لذا $a_۰ < r < a_۰ + ۱$ و $b_۰ < r < b_۰ + ۱$، و بنابراین،

$a_0 = b_0 = [۷]$. لذا $\langle a_1, a_2, \ldots, a_n\rangle = \langle b_1, b_2, \ldots, b_m\rangle$. بدون آنکه به کلیت استدلال خللی وارد آید، فرض می‌کنیم که $n \geq m$. با تکرار استدلال بالا، سرانجام به‌دست می‌آوریم که $a_1 = b_1$، $a_2 = b_2$، ...، $a_{m-1} = b_{m-1}$ و $a_m = b_m$، $\langle a_m, a_{m+1}, \ldots, a_n\rangle = \langle b_m\rangle = b_m$. چون b_m عددی صحیح است، از قسمت اول برهان نتیجه می‌شود که $n = m$ و $a_m = b_m$.

۶.۹ (۴.۹) را ثابت کنید: فرض کنیم a_0، a_1، a_2، ... دنباله‌ای از اعداد صحیح باشد، به‌طوری که همگی بجز احتمالاً a_0 مثبت باشند. ثابت کنید که به‌ازای هر عدد حقیقی مثبت x و هر $k \geq 1$،

$$\langle a_0, a_1, \ldots, a_{k-1}, x\rangle = (xp_{k-1} + p_{k-2})/(xq_{k-1} + q_{k-2})$$

به‌ویژه، $\langle a_0, a_1, a_2, \ldots, a_k\rangle = p_k/q_k$. (راهنمایی: از استقرا استفاده کنید).

حل. به‌ازای $k = 1$ داریم

$$(xp_0 + p_{-1})/(xq_0 + q_{-1}) = (x \times a_0 + 1)/(x \times 1 + 0) = a_0 + 1/x = \langle a_0, x\rangle$$

حال، فرض کنیم که قضیه برای $\langle a_0, a_1, \ldots, a_{k-1}, x\rangle$ درست باشد. در این‌صورت بنابر تعریف ۳.۹

$$\begin{aligned}\langle a_0, a_1, \ldots, a_k, x\rangle &= \langle a_0, a_1, \ldots, a_{k-1}, a_k + 1/x\rangle \\ &= ((a_k + 1/x)p_{k-1} + p_{k-2})/((a_k + 1/x)q_{k-1} + q_{k-2}) \\ &= (x(a_k p_{k-1} + p_{k-2}) + p_{k-1})/(x(a_k q_{k-1} + q_{k-2}) + q_{k-1}) \\ &= (xp_k + p_{k-1})/(xq_k + q_{k-1})\,.\end{aligned}$$

۷.۹ فرض کنیم q_k مانند (۳.۹) تعریف شود. به استقرا نشان دهید که اگر $k \geq 2$، آنگاه $q_k \geq 2^{k/2}$.

حل. به آسانی می‌توان دید که قضیه به‌ازای $k = 2$ و $k = 3$ برقرار است. حال فرض کنیم $q_n \geq 2^{n/2}$، نشان می‌دهیم $q_{n+2} \geq 2^{(n+2)/2}$. روشن است که $q_{n+1} = q_n$ و لذا $q_{n+2} = a_n + 2q_{n+1} + q_n > 2q_n$. در نتیجه $a_{n+2} > 2 \times 2^{n/2} = 2^{(n+2)/2}$.

۸.۹ فرض کنیم p_k/q_k همگرای kام $\langle a_0, a_1, \ldots, a_n\rangle$ باشد. اگر $a_0 \geq 1$، ثابت کنید $p_k/p_{k-1} = \langle a_k, a_{k-1}, \ldots, a_1, a_0\rangle$ و $q_k/q_{k-1} = \langle a_k, a_{k-1}, \ldots, a_2, a_1\rangle$. (راهنمایی: با استفاده از (۳.۹) نشان دهید که $(p_k/p_{k-1} = a_k + 1/(p_{k-1}/p_{k-2}))$.

حل. به آسانی ثابت می‌شود که $p_k/p_{k-1} = a_k + 1/(p_{k-1}/p_{k-2})$. چون $p_{k-2} < p_{k-1}$ ((۳.۹) را ببینید)، در نتیجه اولین خارج‌قسمت جزئی p_k/p_{k-1} برابر است با $a_k = [p_k/p_{k-1}]$. بنابراین $p_k/p_{k-1} = \langle a_k, p_{k-1}/p_{k-2}\rangle$. تکرار این استدلال نشان می‌دهد که دومین خارج‌قسمت جزئی برابر است با a_{k-1}، سومی عبارت است از a_{k-2}، الی آخر. در مرحلهٔ kام داریم

$$p_k/p_{k-1} = \langle a_k, a_{k-1}, \ldots, a_1, p_0/p_{-1}\rangle = \langle a_k, a_{k-1}, \ldots, a_1, a_0\rangle$$

زیرا $a_0 = p_0$ و $p_{-1} = 1$. برای q_k/q_{k-1}، رابطهٔ $q_k = a_k q_{k-1} + q_{k-2}$ را به‌کار می‌بریم و مانند بالا استدلال می‌کنیم. در این‌صورت، در مرحلهٔ $(k-1)$ام داریم

$$q_k/q_{k-1} = \langle a_k, a_{k-1}, \ldots, a_2, q_1, q_0\rangle = \langle a_k, a_{k-1}, \ldots, a_2, a_1\rangle$$

زیرا $q_1 = a_1$ و $q_0 = 1$ ((۳.۹) را ببینید).

◁ **۹.۹** گیریم a/b عدد گویایی تحویل‌ناپذیر باشد، و فرض می‌کنیم $a/b = \langle a_0, a_1, \ldots, a_n\rangle$، که در آن هر a_i عدد صحیح مثبتی است. ثابت کنید اگر n فرد باشد، کسر مسلسل متقارن است (یعنی، $a_0 = a_n$، $a_1 = a_{n-1}$، ...) اگر و تنها اگر $a|b^2 + 1$، و حال آنکه اگر n زوج باشد، کسر مسلسل متقارن است اگر و تنها اگر $a|b^2 - 1$. (راهنمایی: از مسألهٔ قبل استفاده کنید.)

حل. اگر $n = 0$ قضیه بدیهی است، زیرا در این‌صورت a/b عددی صحیح است. لذا می‌توانیم فرض کنیم که $n \geq 1$. اگر کسر مسلسل متقارن باشد، از مسألهٔ ۸.۹ و (۴.۹) نتیجه می‌شود که $p_n/p_{n-1} = \langle a_0, a_1, \ldots, a_n\rangle = p_n/q_n = a/b$. چون $(p_n, q_n) = 1$، داریم $p_{n-1} = q_n = b$ و $p_n = a$؛ لذا بنابر (۷.۹) داریم

$$p_n q_{n-1} - p_{n-1} q_n = a q_{n-1} - b^2 = (-1)^{n-1}$$

و لذا $a|b^2 + (-1)^{n-1}$. حال فرض می‌کنیم که $a|b^2 + (-1)^{n-1}$. در این‌صورت، بنابر (۷.۹) $p_n q_{n-1} - p_{n-1} q_n = a q_{n-1} - b p_{n-1} = (-1)^{n-1}$، و لذا a مقسوم‌علیه $b(b - p_{n-1}) = b p_{n-1} + (-1)^{n-1} - b^2 + (-1)^{n-1}$ است. چون $(a, b) = 1$، بایستی داشته باشیم $a|b - p_{n-1}$. ملاحظه می‌کنید که $n \geq 1$ ایجاب می‌کند که $a/b > 1$؛ لذا $a > b > b - p_{n-1}$ (زیرا اگر $i \geq 0$ آنگاه $p_i > 0$)، همچنین، چون $p_n > p_{n-1}$ و $p_n = a$، داریم $p_{n-1} < a < a + b$، و لذا $b - p_{n-1} > -a$. بنابراین $a > b - p_{n-1} > -a$، و

چون $a|b-p_{n-1}$، باید داشته باشیم $b-p_{n-1}=0$، یعنی، $b=p_{n-1}$. لذا، بنابر مسألهٔ ۸.۹ داریم $\langle a_0,a_1,\ldots,a_n\rangle=a/b=p_n/p_{n-1}=\langle a_n,a_{n-1},\ldots,a_1,a_0\rangle$.

◁ **۱۰.۹** گیریم $n>1$، و فرض می‌کنیم $s^2\equiv -1 \pmod n$. فرض کنیم p_k/q_k همگرای بسط کسر مسلسل s/n باشد به‌طوری که $q_k<\sqrt{n}\le q_{k+1}$. نشان دهید که $(sq_k-np_k)^2+q_k^2=n$.

حل. چون $s^2\equiv -1 \pmod n$، به آسانی ثابت می‌شود که $(sq_k-np_k)^2+q_k^2\equiv 0 \pmod n$. اما بنابر (۳۳.۹)، $|s/n-p_k/q_k|\le 1/q_kq_{k+1}$، و لذا $|sq_k-np_k|\le n/q_{k+1}$. چون $q_{k+1}\ge\sqrt{n}$، نتیجه می‌شود که $|sq_k-np_k|\le\sqrt{n}$. با توجه به انتخاب q_k، داریم $q_k<\sqrt{n}$. لذا $(sq_k-np_k)^2+q_k^2<2n$. چون $q_k\ge 1$، نتیجه می‌شود که $(sq_k-np_k)^2+q_k^2$ مضرب مثبتی از n است که از $2n$ کمتر است و بنابراین برابر n است.

توضیح. تحقیق اینکه نمایش n در بالا به‌صورت مجموع دو مربع اولیه است، دشوار نیست، و لذا برهان دیگری برای قسمت اصلی (۱۴.۸) داریم. بنابراین همین که یک جواب s از همنهشتی $x^2\equiv -1 \pmod n$ داشته باشیم، روند کسر مسلسل یک روش خیلی کارآمد برای ساختن یک نمایش اولیهٔ n به‌صورت مجموع دو مربع به‌دست می‌دهد.

معادلهٔ $ax+by=c$

۱۱.۹ روش کسرهای مسلسل را برای یافتن جواب $377x-120y=-3$ به‌کار برید. (مسألهٔ ۳.۹ را ببینید.)

حل. برای کاربرد (۱۰.۹)، لازم است که $b>0$؛ بنابراین معادله را به‌صورت $-377x+120y=3$ می‌نویسیم و مانند (۱۱.۹) ادامه می‌دهیم. یا اینکه اصلاً جوابهای معادله $377x+120y=-3$ را به‌دست می‌آوریم و $-y$ را به جای y می‌گذاریم. بنابر الگوریتم اقلیدسی، $377/120=\langle 3,7,17\rangle$. جدول زیر را تشکیل می‌دهیم

k	-1	0	1	2
a_k		3	7	17
p_k	1	3	22	377
q_k	0	1	7	120

حال (۱۰.۹) را به‌کار می‌بریم. چون $n=2$ زوج است، $377x+120y=-3$ دارای جواب

$x = -cq_{n-1} = ۳ \times ۷ = ۲۱$، $y = cp_{n-1} = -۳ \times ۲۲ = -۶۶$ است. لذا $x = ۲۱$، $y = ۶۶$ جوابی از $۳۷۷x - ۱۲۰y = -۳$ است.

۱۲.۹ کسرهای مسلسل را برای بیان بزرگترین مقسوم‌علیه مشترک ۳۷۷ و ۱۲۰ به‌صورت ترکیب خطی از این اعداد به‌کار برید. (راهنمایی: (۱۰.۹) و مسألهٔ قبل را به‌کار برید.)

حل. کنترل کنید که $(۳۷۷, ۱۲۰) = ۱$. بنابر مسأله ۱۱.۹، $۳۷۷/۱۲۰ = \langle ۳, ۷, ۱۷ \rangle$. لذا (۱۰.۹) ایجاب می‌کند که $۳۷۷x + ۱۲۰y = ۱$ دارای جواب $x = -q_۱$، $y = p_۱$، باشد، و بنابراین از جدول بالا داریم $x = -۷$ و $y = ۲۲$.

۱۳.۹ کسرهای مسلسل را برای یافتن جوابهای معادلات زیر به‌کار برید: (الف) $۹۸x + ۲۶۳y = ۱$؛ $۱۲۵۵x + ۱۷۷y = -۱$.

حل. (الف) $۲۶۳/۹۸ = \langle ۲, ۱, ۲, ۶, ۵ \rangle$. جدول زیر را تشکیل می‌دهیم:

k	-۱	۰	۱	۲	۳	۴
a_k		۲	۱	۲	۶	۵
p_k	۱	۲	۳	۸	۵۱	۲۶۳
q_k	۰	۱	۱	۳	۱۹	۹۸

کاربرد (۱۰.۹) جواب $x = ۵۱$، $y = -۱۹$ را به‌دست می‌دهد.

(ب) $۱۲۵۵/۱۷۷ = \langle ۷, ۱۱, ۱۶ \rangle$. جدول زیر را تشکیل می‌دهیم:

k	-۱	۰	۱	۲
a_k		۷	۱۱	۱۶
p_k	۱	۷	۷۸	۱۲۵۵
q_k	۰	۱	۱۱	۱۷۷

سپس از (۱۰.۹) جواب $x = ۱۱$ $y = -۷۸$ حاصل می‌شود.

کسرهای مسلسل نامتناهی

۱۴.۹ عدد α دارای بسط کسر مسلسلی است که اولین سه خارج‌قسمت جزئی آن عبارت‌اند از ۱، ۲، و ۳، و α دارای حداقل یک خارج‌قسمت جزئی دیگر است (کسر مسلسل ممکن است متناهی یا نامتناهی باشد). دربارهٔ اندازهٔ α چه می‌توان گفت؟

حل. داریم $\alpha = \langle ۱, ۲, ۳, \beta \rangle$ که $\beta \geq ۱$. با محاسبهٔ کسر مسلسل متناهی، داریم $\alpha = (۱۰\beta + ۳)/(۷\beta + ۲) = ۱۰/۷ + ۱/(۴۹\beta + ۱۴)$. لذا $\alpha > ۱۰/۷$ و $\alpha \leq ۱۰/۷ + ۱/۵۶ = ۸۱/۵۶$.

۱۵.۹ فرض کنیم $\alpha = \langle a_۰, a_۱, \ldots, a_{n-۱}, a_n, \ldots \rangle$ و $\beta = \langle b_۰, b_۱, \ldots, b_{n-۱}, b_n, \ldots \rangle$ کسرهای مسلسل متناهی یا نامتناهی باشند به‌طوری که به‌ازای $۰ \leq i \leq n-۱$، $a_i = b_i$ و به‌ازای $i \geq n$، $a_i \neq b_i$. ثابت کنید که

(الف) اگر n زوج باشد، آنگاه $\alpha > \beta$ اگر و تنها اگر $a_n > b_n$،

(ب) اگر n فرد باشد، آنگاه $\alpha > \beta$ اگر و تنها اگر $b_n > a_n$.

حل. مطابق معمول، فرض می‌کنیم $\alpha_k = \langle a_k, a_{k+۱}, \ldots \rangle$ و $\beta_k = \langle b_k, b_{k+۱}, \ldots \rangle$. در این‌صورت $\alpha > \beta$ اگر و تنها اگر $a_۰ + ۱/\alpha_۱ > b_۰ + ۱/\beta_۱$ اگر و تنها اگر $\alpha_۱ > \beta_۱$. همچنین، $\beta_۱ > \alpha_۱$ اگر و تنها اگر $a_۱ + ۱/\alpha_۲ > b_۱ + ۱/\beta_۲$ اگر و تنها اگر $\alpha_۲ > \beta_۲$. اگر همین روند را ادامه دهیم، ثابت می‌شود که اگر n زوج باشد، $\alpha > \beta$ اگر و تنها اگر $\alpha_n > \beta_n$ اگر و تنها اگر $a_n + ۱/\alpha_{n+۱} > b_n + ۱/\beta_{n+۱}$. چون $۱/\alpha_{n+۱} < ۱$ و $۱/\beta_{n+۱} < ۱$، نابرابری آخر برقرار است اگر و تنها اگر $a_n > b_n$. اگر n فرد باشد، داریم $\alpha > \beta$ اگر و تنها اگر $\beta_n > \alpha_n$. اگر و تنها اگر $b_n > a_n$.

۱۶.۹ فرض کنیم $\alpha = \langle a_۰, a_۱, \ldots, a_{n-۱} \rangle$ و $\beta = \langle a_۰, a_۱, \ldots, a_{n-۱}, b_n, \ldots \rangle$. با استفاده از مسألهٔ قبل ثابت کنید $\alpha > \beta$ اگر و تنها اگر n زوج باشد.

حل. اگر $a_{n-۱} = ۱$، می‌نویسیم

$$\alpha = \langle a_۰, a_۱, \ldots, a_{n-۲}, ۱ \rangle = \langle a_۰, a_۱, \ldots, a_{n-۳}, a_{n-۲} + ۱ \rangle$$

و مسألهٔ قبل را در مورد بسط دوم و β به‌کار می‌بریم. چون نخستین $n-۲$ خارج‌قسمت جزئی این بسطها برابرند و $a_{n-۲} < a_{n-۲} + ۱$، نتیجه می‌شود که $\alpha > \beta$ اگر و تنها اگر $n-۲$ زوج باشد و لذا اگر و تنها اگر n زوج باشد. اگر $a_{n-۱} > ۱$، آنگاه α دارای بسط $\langle a_۰, a_۱, \ldots, a_{n-۱} - ۱, ۱ \rangle$ نیز هست. در این‌صورت نخستین $n-۱$ خارج‌قسمت جزئی α و β برابرند. بنابر مسألهٔ ۱۵.۹، چون $a_{n-۱} > ۱ = a_{n-۱} - ۱$، لذا $\alpha > \beta$ اگر و تنها اگر $n-۱$ فرد باشد، یعنی، اگر و تنها اگر n زوج باشد.

۱۷.۹ در هر مورد، تعیین کنید که مقدار کسر مسلسل اول بزرگتر از مقدار دومی هست یا نیست.

(الف) $\langle ۱, ۲, ۳, ۴, ۵\rangle$، $\langle ۱, ۲, ۳, ۴, ۳\rangle$؛
(ب) $\langle ۱, ۲, ۳, ۴, ۵\rangle$، $\langle ۱, ۲, ۳, ۵, ۴, \ldots\rangle$؛
(ج) $\langle ۱, ۲, ۳, ۴, ۵, ۶\ldots\rangle$، $\langle ۱, ۲, ۳, ۴\rangle$؛
(د) $\langle ۲۹۲, ۱, ۱۵, ۷\rangle$، $\langle ۲۹۲, ۱, ۱, \ldots\rangle$؛
(ه) $\langle ۲۹۲, ۱, ۱۵, ۷, \ldots\rangle$، $\langle ۲۹۲, ۱, ۱۵\rangle$؛

حل. فرض کنیم α و β به‌ترتیب معرف کسرهای مسلسل اول و دوم باشند. بنابر مسأله‌های ۱۵.۹ و ۱۶.۹، در موارد (ب)، (د)، و (ه، $\alpha > \beta$ و در قسمتهای (الف) و (ج)، $\beta > \alpha$.

۱۸.۹ فرض کنیم x یک عدد حقیقی بزرگتر از ۱ و $x = \langle a_۰, a_۱, a_۲, \ldots\rangle$. (ممکن است که بسط متناهی باشد.) ثابت کنید $۱/x = \langle ۰, a_۰, a_۱, a_۲, \ldots\rangle$.

حل. با استفاده از (۱۴.۹) نتیجه می‌گیریم که

$$\langle ۰, a_۰, a_۱, a_۲, \ldots\rangle = ۰ + ۱/\langle a_۰, a_۱, \ldots\rangle = ۱/x$$

۱۹.۹ با استفاده از (۱۷.۹)، نخستین نُه خارج‌قسمت جزئی بسط کسر مسلسل π را به‌دست آورید.

حل. با کاربرد الگوریتم بیان شده در (۱۷.۹)، داریم $a_۰ = [\pi] = ۳$. سپس $\alpha_۱ = ۱/(\alpha_۰ - a_۰) = ۱/(\pi - ۳)$، و لذا $a_۱ = [\alpha_۱] = ۷$. با ادامهٔ این روند خواهیم داشت $\pi = \langle ۳, ۷, ۱۵, ۱, ۲۹۲, ۱, ۱, ۱, ۲, \ldots\rangle$.

توضیح. انجام الگوریتم توسط حسابگر آسان است. جزء صحیح π (یعنی، ۳) را کم کنید، سپس وارون سازید؛ جزء صحیح حاصل را کم کنید، سپس وارون سازید. ادامهٔ این روند خارج‌قسمتهای جزئی متوالی π را ارائه می‌دهد. مواظب باشید که بعد از تعدادی مرحله (که بستگی به دقت حسابگر دارد)، خارج‌قسمتهای جزئی محاسبه‌شده درست نخواهند بود. البته، بسیاری از حسابگرها بایستی نخستین نُه خارج‌قسمت جزئی π را به‌طور صحیح به‌دست دهند.

۲۰.۹ (الف) گیریم α گنگ باشد، و فرض می‌کنیم $a/b < \alpha < c/d$، که در آن a، b، c، و d اعداد صحیح مثبتی هستند به‌طوری که $bc - ad = ۱$. ثابت کنید که لااقل یکی از کسرهای a/b و c/d یک همگرای α است.

(ب) مثالی ارائه دهید که در آن دقیقاً یکی از کسرهای a/b و c/d یک همگرا باشد، و نشان دهید که ممکن است a/b و c/d هر دو همگرا باشند. (راهنمایی: فرض کنید نابرابری واقع در (۳۹.۹) برای a/b و c/d برقرار نیست.)

حل. (الف) توجه کنید که چون α گنگ است، رابطهٔ $|\alpha - a/b| = 1/2b^2$ برقرار نیست. لذا، اگر $|\alpha - a/b| < 1/2b^2$ و $|\alpha - c/d| < 1/2d^2$ هر دو برقرار نباشند، آنگاه $1/bd = (bc-ad)/bd = c/d - a/b = |\alpha - a/b| + |\alpha - c/d| > 1/2b^2 + 1/2d^2$ از ضرب کسرهای اول و آخر در $2b^2d^2$ به‌دست می‌آوریم $2bd > b^2 + d^2$، یعنی $(b-d)^2 < 0$، که ممکن نیست. پس یا $|\alpha - a/b| < 1/2b^2$ یا $|\alpha - c/d| < 1/2d^2$، و لذا، بنابر (۳۹.۹)، حداقل یکی از کسرهای a/b و c/d یک همگرای α است.

(ب) برای اینکه نشان دهیم a/b و c/d می‌توانند همگرا باشند، فرض می‌کنیم α عددی گنگ و k فرد باشد. پس بنابر (۱۲.۹)، $p_{k-1}/q_{k-1} < \alpha < p_k/q_k$، و بنابر (۷.۹)، $p_kq_{k-1} - p_{k-1}q_k = 1$. اگر $\alpha = \sqrt{6}$، آنگاه $2/5 < \sqrt{6} < 3/7$ و $3 \times 5 - 2 \times 7 = 1$؛ ولی، فقط $2/5$ یک همگرای $\sqrt{6}$ است. (عدد $3/7$ یک همگرای میانی $\sqrt{6}$ است؛ بخش آخر مسائل را برای خاصیتهای همگراهای میانی ببینید.)

۲۱.۹ گیریم $\alpha > 1$ گنگ باشد، فرض کنیم p_k/q_k و P_k/Q_k به‌ترتیب معرف همگرای kام α و $1/\alpha$ باشند. ثابت کنید $P_k/Q_k = q_{k-1}/p_{k-1}$. (راهنمایی: مسألهٔ ۱۸.۹ را ببینید.)

حل. بنابر مسألهٔ ۱۸.۹، $1/\alpha = \langle 0, a_0, a_1, \ldots \rangle$. لذا بنابر (۴.۹) همگرای kام $1/\alpha$ عبارت است از $q_{k-1}/p_{k-1} = 1/\langle a_0, a_1, \ldots, a_{k-1} \rangle = \langle 0, a_0, a_1, \ldots, a_{k-1} \rangle$.

کسرهای مسلسل دوره‌یی

۲۲.۹ جدولی تشکیل دهید و (۲۴.۹) را برای یافتن بسط کسر مسلسل (الف) $\sqrt{47}$؛ (ب) $(\sqrt{2} + 4)/3$؛ (ج) $(\sqrt{11} - 7)/3$ به‌کار برید.

حل. (الف) ملاحظه کنید که $\sqrt{47} = (0 + \sqrt{47})/1$ و $47 - 0^2 | 1$. بنابر (۲۴.۹)،

k	0	1	2	3	4	5
r_k	0	6	5	5	6	6
s_k	1	11	2	11	1	11
a_k	6	1	5	1	12	

از آنجا که $r_1 = r_5$ و $s_1 = s_5$، درایه‌های جدول از $k = 5$ به بعد تکرار می‌شوند. لذا $\sqrt{47} = \langle 6, \overline{1, 5, 1, 12} \rangle$.

(ب) چون ۳ عدد $۴^۲ - ۲$ را نمی‌شمارد، صورت و مخرج را در $|۳ -$ | ضرب می‌کنیم تا $(۱۲ + \sqrt{۱۸})/q$ به‌دست آید (برهانِ (۲۳.۹) را ببینید)؛ در اینجا $d = ۱۸$، $r_۰ = ۱۲$، $s_۰ = q$. جدول زیر را تشکیل می‌دهیم:

k	۰	۱	۲	۳	۴
r_k	۱۲	-۳	۴	۴	۴
s_k	۹	۱	۲	۱	۲
a_k	۱	۱	۴	۸	

چون درایه‌های ستون $k = ۴$ با درایه‌های ستون $k = ۲$ یکسان هستند، داریم

$$(۴ + \sqrt{۲})/۳ = \langle ۱, ۱, \overline{۴, ۸} \rangle$$

(ج) $(۳/\sqrt{۱۱} - ۷)$ را به‌صورت $(-۳)/(\sqrt{۱۱} + ۷-)$ می‌نویسیم؛ چون ۳− عدد $۷^۲ - ۱۱$ را نمی‌شمارد، صورت و مخرج را در ۳ ضرب می‌کنیم تا $(-۹)/(\sqrt{۹۹} + ۲۱-)$ به‌دست آید؛ پس $d = ۹۹$، $r_۰ = -۲۱$، و $s_۰ = -۹$. جدول زیر را محاسبه می‌کنیم:

k	۰	۱	۲	۳	۴	۵	۶
r_k	-۲۱	۱۲	۸	۶	۳	۷	۸
s_k	-۹	۵	۷	۹	۱۰	۵	۷
a_k	۱	۴	۲	۱	۱	۳	

چون $r_۲ = r_۶$ و $s_۲ = s_۶$، داریم $(۳/(\sqrt{۱۱} - ۷) = \langle ۱, ۴, \overline{۲, ۱, ۱, ۳} \rangle$.

۲۳.۹ (الف) جدولی مانند جدول (۲۵.۹) برای یافتن بسط کسر مسلسل $\sqrt{۱۳۰}$ تشکیل دهید.

(ب) این جدول را برای تعیین بسط کسر مسلسل $(۹/(\sqrt{۱۳۰} + ۷)$ به‌کار برید. (راهنمایی: (۲۴.۹) و (۱۹.۹) را به‌کار برید.)

حل. (الف) جدول زیر را تشکیل می‌دهیم:

k	۰	۱	۲	۳	۴
r_k	۰	۱۱	۱۷	۱۱	۱۱
s_k	۱	۹	۹	۱	۹
a_k	۱۱	۲	۲	۲۲	

لذا $\sqrt{۱۳۰} = \langle ۱۱, \overline{۲, ۲, ۲۲} \rangle$.

(ب) بنابر (iii.۲۴.۹)، $\alpha_۲ = (r_۲ + \sqrt{۱۳۰})/s_۲ = (۷ + \sqrt{۱۳۰})/۹$، و بنابر (۱۹.۹)
$\alpha_۲ = \langle a_۲, a_۳, \ldots \rangle$. لذا $(۷ + \sqrt{۱۳۰})/۹ = \langle ۲, ۲۲, ۲, ۲, ۲۲, ۲, \ldots \rangle = \langle \overline{۲, ۲۲, ۲} \rangle$.

۲۴.۹ ثابت کنید به‌ازای $n \geq ۱$، $\sqrt{n^۲ + ۱} = \langle n, \overline{۲n} \rangle$ و $\sqrt{n^۲ + ۲} = \langle n, \overline{n, ۲n} \rangle$.

حل. (۲۴.۹) را به‌ترتیب برای ساختن جدولهای $\sqrt{n^۲ + ۱}$ و $\sqrt{n^۲ + ۲}$ به‌کار می‌بریم:

k	۰	۱	۲
r_k	۰	n	n
s_k	۱	۱	۱
a_k	n	$۲n$	

k	۰	۱	۲	۳
r_k	۰	n	n	n
s_k	۱	۲	۱	۲
a_k	n	n	$۲n$	

در جدول اول $r_۱ = r_۲$ و $s_۲ = s_۱$، لذا خارج‌قسمتهای جزئی با شروع از $a_۱ = ۲n$، تکرار می‌شوند؛ لذا $\sqrt{n^۲ + ۱} = \langle n, \overline{۲n} \rangle$. در جدول دوم، $r_۱ = r_۳$ و $s_۳ = s_۱$، و لذا خارج‌قسمتهای جزئی با شروع از $a_۱ = n$ تکرار می‌شوند؛ بنابراین، $\sqrt{n^۲ + ۲} = \langle n, \overline{n, ۲n} \rangle$.

۲۵.۹ ثابت کنید (الف) به‌ازای $n \geq ۲$، $\sqrt{n^۲ - ۱} = \langle n - ۱, \overline{۱, ۲n - ۲} \rangle$؛
(ب) به‌ازای $n \geq ۲$، $\sqrt{n^۲ - n} = \langle n - ۱, \overline{۲, ۲n, -۲} \rangle$؛
(ج) به‌ازای $n \geq ۳$، $\sqrt{n^۲ - ۲} = \langle n - ۱, \overline{۱, n - ۲, ۱, ۲n - ۲} \rangle$.

حل. با استفاده از جدولهای زیر به‌ترتیب برای $\sqrt{n^۲ - ۱}$، $\sqrt{n^۲ - n}$، و $\sqrt{n^۲ - ۲}$، مانند مسألهٔ ۲۴.۹ ادامه می‌دهیم:

k	۰	۱	۲	۳
r_k	۰	$n - ۱$	$n - ۱$	$n - ۱$
s_k	۱	$۲n - ۲$	۱	$۲n - ۲$
a_k	$n - ۱$	۱	$۲n - ۲$	

k	۰	۱	۲	۳
r_k	۰	$n - ۱$	$n - ۱$	$n - ۱$
s_k	۱	$n - ۱$	۱	$n - ۱$
a_k	$n - ۱$	۲	$۲n - ۲$	

k	۰	۱	۲	۳	۴	۵
r_k	۰	$n-۱$	$n-۲$	$n-۲$	$n-۱$	$n-۱$
r_k	۱	$۲n-۳$	۲	$۲n-۳$	۱	$۲n-۳$
a_k	$n-۱$	۱	$n-۲$	۱	$۲n-۲$	

۲۶.۹ اگر $n \geq ۱$، بسط کسر مسلسل $\sqrt{n^۲+۱}+n^۲$ را بیابید. (راهنمایی: مسألهٔ ۲۴.۹ را به‌کار برید.)

حل. بنابر مسألهٔ ۲۴.۹ داریم

$$\sqrt{n^۲+n}+n^۲ = n^۲+\langle n, \overline{۲n}\rangle = n^۲+n+۱/\langle \overline{۲n}\rangle = \langle n^۲+n, \overline{۲n}\rangle$$

برهان دیگر. (۱۸.۹) را به‌کار می‌بریم. فرض کنیم $\alpha_۰ = \sqrt{n^۲+۱}+n^۲$؛ سپس $a_۰ = [\alpha_۰] = n+n^۲$. قرار می‌دهیم

$$\alpha_۱ = ۱/(\alpha_۰ - a_۰) = ۱/(\sqrt{n^۲+۱}-n) = \sqrt{n^۲+۱}+n$$

پس $a_۱ = [\alpha_۱] = ۲n$. اکنون ملاحظه می‌کنیم که

$$\alpha_۲ = ۱/(\alpha_۱ - a_۱) = ۱/(\sqrt{n^۲+۱}-n) = \alpha_۱$$

و لذا $a_۲ = a_۱$. سپس آشکار است که به‌ازای هر $k \geq ۲$، $a_k = a_۱$، و لذا $\sqrt{n^۲+۱}+n^۲ = \langle n^۲+n, \overline{۲n}\rangle$.

۲۷.۹ فرض کنیم d عدد صحیح مثبتی است که مربع کامل نیست، و فرض می‌کنیم a، b، r، و s اعداد صحیحی هستند با b و s غیرصفر. اگر $(a+\sqrt{d})/b = (r+\sqrt{d})/s$، ثابت کنید $a=r$ و $b=s$.

حل. معادلهٔ بالا ایجاب می‌کند که $(s-b)\sqrt{d} = br-as$. اگر $b \neq s$، آنگاه $\sqrt{d} = (br-as)/(s-b)$، که با گنگ بودن $\sqrt{d}$ تناقض دارد. از این‌رو $b=s$، و لذا $a=r$.

۲۸.۹ در قضیهٔ (۲۴.۹)، s_{k+1} با فرمول $s_{k+1} = (d - r_{k+1}^2)/s_k$ تعریف شد. نشان دهید که $s_{k+1} = s_{k-1} + q_k(r_k + r_{k+1})$.

حل. داریم $s_k s_{k+1} = d - r_{k+1}^2$ و $s_{k-1}s_k = d - r_k^2$. از آنجا

$$s_k(s_{k+1} - s_{k-1}) = r_k^2 - r_{k+1}^2 = (r_k - r_{k+1})(r_{k+1}). \qquad (1)$$

اما بنابر تعریف r_{k+1} داریم $r_k + r_{k+1} = a_k s_k$. از این رابطه (۱)

$$s_{k+1} - s_{k-1} = a_k(r_k - r_{k+1})$$

که فرمول مورد نظر را به ما می‌دهد.

توضیح. وقتی d خیلی بزرگ باشد، معمولاً می‌توان عبارت مربوط به s_{k+1} را که در این مسأله ارائه شده است سریعتر از عبارت $(d - r_{k+1}^2)/s_k$ محاسبه کرد، زیرا معمولاً عمل تقسیم به‌طور قابل ملاحظه‌ای کندتر از ضرب، که آن نیز خیلی کندتر از عمل جمع است صورت می‌گیرد. عبارت $(d - r_{k+1}^2)/s_k$ وقتی با حسابگر کار می‌کنیم مناسبتر است.

۲۹.۹ فرض کنیم $\alpha = u_a + v_a\sqrt{d}$ و $\beta = u_b + v_b\sqrt{d}$، که u_a، v_a، u_b، و v_b اعداد گویا هستند. ثابت کنید $(\alpha + \beta)' = \alpha' + \beta'$، $(\alpha\beta)' = \alpha'\beta'$، و، اگر $\beta \neq 0$، $(\alpha/\beta)' = \alpha'\beta'$. (برای تعریف α'، مزدوج α، تعریف (۲۶.۹) را ببینید.)

حل. داریم

$$(\alpha + \beta)' = (u_a + u_b + (v_a + v_b)\sqrt{d})' = (u_a - v_a\sqrt{d}) + (u_b - v_b\sqrt{d}) = \alpha'\beta'$$

همچنین، $(\alpha\beta)' = u_a u_b + dv_a v_b - (u_a v_b + u_b v_a)\sqrt{d} = \alpha'\beta'$.

برای تقسیم، کافی است ثابت کنیم $(1/\beta)' = 1/\beta'$. اما

$$1/\beta = \beta'/(\beta\beta') = (u_b - v_b\sqrt{d})/(u_b^2 - dv_b^2)$$

با مزدوج‌گیری داریم $(u_b + v_b\sqrt{d})/(u_b^2 - dv_b^2)$. به آسانی دیده می‌شود که این همان $1/\beta'$ است.

۳۰.۹ عکس قضیهٔ لاگرانژ (۲۸.۹) را ثابت کنید: مقدار هر کسر مسلسل دوره‌یی یک عدد گنگ درجهٔ دوم است.

حل. گیریم $\alpha = \langle c_0, \ldots, c_n, \overline{a_0, \ldots, a_{m-1}} \rangle$ و فرض می‌کنیم

$$\beta = \langle \overline{a_0, \ldots, a_{m-1}} \rangle$$

توجه داریم که $\alpha = \langle c_0, \ldots, c_n, \beta \rangle$؛ لذا بنابر (۴.۹)، $\alpha = (\beta p_n + p_{n-1})/(\beta q_n + q_{n-1})$، که در آن p_k/q_k معرف همگرای kام $\langle c_0, \ldots, c_n \rangle$ است. اگر β را برحسب α حساب کنیم داریم

$$\beta = -(\alpha q_{n-1} - p_{n-1})/(\alpha q_n - p_n)\,. \qquad (1)$$

اما بنابر (۴.۹) داریم

$$\beta = \langle a_0, \ldots, a_{m-1}, \beta \rangle = (\beta p'_{m-1} + p'_{m-2})/(\beta q'_{m-1} + q'_{m-2}), \qquad (2)$$

که در آن p'_k/q'_k همگراهای $\langle a_0, a_1, \ldots, a_{m-1} \rangle$ هستند. اکنون در (۲) به جای β مقدارش را از (۱) می‌گذاریم. بعد از ساده کردن، می‌بینیم که α در یک معادلهٔ درجهٔ دوم با ضرایب صحیح صدق می‌کند. چون بنابر (۱۶.۹) α گنگ است، نتیجه می‌شود که α یک گنگ درجهٔ دوم است.

کسرهای مسلسل دوره‌یی محض

۳۱.۹ فرض کنید $\alpha = \langle \overline{1, 2, 3} \rangle$. ثابت کنید $\alpha = (4 + \sqrt{37})/7$. با استفاده از (۲۴.۹)، جدولی جهت امتحان پاسخ خود تشکیل دهید.

حل. بنابر (۱۴.۹) داریم $\alpha = 1 + 1/(2 + 1/(3 + 1/\alpha)) = (10\alpha + 3)/(7\alpha + 2)$. از آنجا معادلهٔ $7\alpha^2 - 8\alpha - 3 = 0$ به‌دست می‌آید، و چون مثبت بودن α واضح است، $\alpha = (4 + \sqrt{37})/7$. (ملاحظه کنید که $\alpha > 1$ و مزدوجش $\alpha' = (4 - \sqrt{37})/7$ در $-1 < \alpha' < 0$ صدق می‌کند؛ از این‌رو α ساده شده است، و لذا بنابر(۳۱.۹) بسط کسر مسلسل آن بایستی دوره‌یی محض باشد.)

می‌توانیم پاسخ خود را با محاسبهٔ جدول زیر برای $(4 + \sqrt{37})/7$ امتحان کنیم (به بازنویسی این عبارت نیازی نیست، زیرا $|37 - 4^2| = 7$):

k	۰	۱	۲	۳
r_k	۴	۳	۵	۴
s_k	۷	۴	۳	۷
a_k	۱	۲	۳	

چون درایه‌ها برای $k = ۳$ با درایه‌ها به‌ازای $k = ۰$ مانند هم هستند، نتیجه می‌گیریم که $\langle \overline{۱, ۲, ۳} \rangle = (۴ + \sqrt{۳۷})/۷$.

۳۲.۹ مقدار کسرهای مسلسل زیر را محاسبه کنید: (الف) $\langle ۱, ۱, ۱, \ldots \rangle$؛ (ب) $\langle ۲, ۳, ۱, ۱, ۱, \ldots \rangle$؛ (ج) $\langle \overline{۱, ۲} \rangle$؛ (د) $\langle ۱, ۳, \overline{۱, ۲} \rangle$.

حل. این چهارکسر مسلسل را به‌ترتیب با α، β، γ، و δ نشان می‌دهیم. (الف) بنابر (۱۴.۹)، داریم $\alpha = ۱ + ۱/\alpha$، و لذا $\alpha^۲ - \alpha - ۱ = ۰$، از آنجا که α مثبت است، از این معادله داریم $\alpha = (۱ + \sqrt{۵})/۲$.

(ب) بنابر (۱۴.۹) داریم $\beta = ۲ + ۱/(۳ + ۱/\alpha) = (۷\alpha + ۲)/(۳\alpha + ۱)$، که در آن $\alpha = (۱ + \sqrt{۵})/۲$. لذا $\beta = (۲۵ - \sqrt{۵})/۱۰$.

(ج) چون $\gamma = ۱ + ۱/(۲ + ۱/\gamma) = (۳\gamma + ۱)/(۲\gamma + ۱)$، از آنجا $۲\gamma^۲ - ۲\gamma - ۱ = ۰$، و لذا $\gamma = (۱ + \sqrt{۳})/۲$.

(د) داریم $\delta = ۱ + ۱/(۳ + ۱/\gamma) = (۴\gamma + ۱)/(۳\gamma + ۱) = ۳ - \sqrt{۳}$.

۳۳.۹ فرض کنیم a و b دو عدد صحیح مثبت باشند به‌طوری که $a|b$. اگر $b = ac$، ثابت کنید $\langle \overline{b, a} \rangle = (b + \sqrt{b^۲ + ۴c})/۲$.

حل. فرض کنیم $\alpha = \langle \overline{b, a} \rangle$؛ پس (۱۴.۹) ایجاب می‌کند که

$$\alpha = b + ۱/(a + ۱/\alpha) = ((ab + ۱)\alpha + b)/(a\alpha + ۱)$$

از اینجا معادلهٔ درجه دوم $a\alpha^۲ - ab\alpha - b = ۰$ به‌دست می‌آید. روشن است که α مثبت است، و لذا ریشهٔ مثبت این معادله را به‌کار می‌بریم. بنابراین

$$\alpha = (ab + \sqrt{a^۲b^۲ + ۴ab})/۲a = (ab + \sqrt{a^۲b^۲ + ۴a^۲c})/۲a$$

$$= (b + \sqrt{b^۲ + ۴c})/۲ .$$

۳۴.۹ مقدار کسر مسلسل دوره‌یی محض $\langle n, n, n, \ldots \rangle$ را بیابید.

حل. فرض کنیم $\alpha = \langle n, n, \ldots \rangle$. پس (۱۴.۹) ایجاب می‌کند که

$$\alpha = n + ۱/\langle n, n, \ldots \rangle = n + ۱/\alpha$$

از اینجا معادلهٔ $\alpha^۲ - n\alpha - ۱ = ۰$ پیدا می‌شود که دارای ریشه‌های $(n \pm \sqrt{n^۲ + ۴})/۲$ است. چون α مثبت است، داریم $\alpha = (n + \sqrt{n^۲ + ۴})/۲$.

برهان دیگر. مسألهٔ قبل را با $a = b = n$ و $c = ۱$ به‌کار برید.

۳۵.۹ تعیین کنید کدام‌یک از اعداد زیر دارای بسط کسر مسلسل دوره‌یی محض می‌باشد: (الف) $(۱ + \sqrt{۳})/۲$؛ (ب) $(۳ + \sqrt{۱۳})/۲$؛ (ج) $\sqrt{۳۲} + ۵$؛ (د) $(۷ + \sqrt{۱۱})/۵$.

حل. با توجه به (۳۱.۹) بایستی در هر حالت تعیین کنیم کدام‌یک از اعداد گنگ درجه دوم مفروض ساده شده است، یعنی، $\alpha = (r + \sqrt{d})/s$ و مزدوجش $\alpha' = (r - \sqrt{d})s$ در $\alpha > ۱$ و $۰ > \alpha' > -۱$ صدق می‌کنند. به آسانی معلوم می‌شود که این دو شرط برای سه عدد اول برقرارند، لذا هر یک از آنها ساده شده هستند، و بنابراین هر کدام دارای یک بسط دوره‌یی محض هستند. چون $(۷ - \sqrt{۱۱})/۵ < ۱$، عدد آخری ساده شده نیست و بنابراین بسط دوره‌یی محض ندارد.

۳۶.۹ (الف) فرض کنیم $\alpha = (۲ + \sqrt{۱۰})/۲$. با استفاده از (۲۴.۹) جدولی برای محاسبهٔ r_k، s_k، و q_k به‌ازای $۰ \le k \le ۴$ تشکیل دهید. بسط کسر مسلسل α را بیابید.

(ب) فقط با استفاده از قسمت (الف)، $\langle \overline{۱, ۱, ۲} \rangle$ و $\langle \overline{۱, ۲, ۱} \rangle$ را به‌صورت $(r + \sqrt{d})/s$ که در آن $s | d - r^۲$، بیان کنید.

حل. (الف) اگر $\alpha = (r + \sqrt{d})/s$، آنگاه $d = ۱۰$ و $r = s = ۲$؛ لذا $s | d - r^۲$. (بنابراین به تعدیل α با ضرب صورت و مخرج آن در $|s|$ نیازی نیست.) با کاربرد فرمولهای (۲۴.۹)، داریم

k	۰	۱	۲	۳	۴
r_k	۲	۲	۱	۲	۲
s_k	۲	۳	۳	۲	۳
a_k	۲	۱	۱	۲	

(ملاحظه کنید که با شروع از $k = ۳$ مقادیر جدول تکرار می‌شوند.) لذا $\alpha = \langle \overline{۲, ۱, ۱} \rangle$.

(ب) بنابر (۱۹.۹) و (iii.۲۴.۹)، $\alpha_k = \langle a_k, a_{k+1}, \ldots \rangle = (r_k + \sqrt{d})/s_k$. بنابراین، $\overline{\langle 1, 1, 2 \rangle} = \langle a_1, a_2, \ldots \rangle = \alpha_1 = (r_1 + \sqrt{d})/s_1 = (2 + \sqrt{10})/3$. با استدلالی مشابه، $\overline{\langle 1, 2, 1 \rangle} = \langle a_2, a_3, \ldots \rangle = \alpha_2 = (r_2 + \sqrt{d})/s_2 = (1 + \sqrt{10})/3$.

۳۷.۹ بنا به تعریف، یک عدد گنگ درجه دوم مانند α ساده شده است اگر $\alpha > 1$ و $-1 < \alpha' < 0$، که در آن α' مزدوج α است (۳۰.۹) را ببینید). آیا امکان دارد که $\alpha < 1$ ولی $-1 < \alpha' < 0$؟

حل. آری. مثلاً، $\alpha = (1 + \sqrt{5})/4$ یا $\alpha = (3 + \sqrt{11})/7$. در هر مورد، به آسانی معلوم می‌شود که $\alpha < 1$ و $-1 < \alpha' < 0$.

۳۸.۹ فرض کنیم $\alpha = (r + \sqrt{d})/s$ یک عدد گنگ درجه دوم باشد. ثابت کنید α ساده شده است اگر و تنها اگر $0 < r < \sqrt{d}$ و $\sqrt{d} - r < s < \sqrt{d} + r$. (به‌ویژه، از این دو رابطه داریم $0 < s < 2\sqrt{d}$.)

حل. ابتدا فرض می‌کنیم α ساده شده باشد؛ لذا $\alpha > 1$ و $-1 < \alpha' < 0$، به‌طوری که $\alpha' = (r - \sqrt{d})/s$. چون $1 < \alpha - \alpha' = 2\sqrt{d}/s$، داریم $s > 0$ و $s < 2\sqrt{d}$. همچنین، $0 < \alpha + \alpha' = 2r/s$ ایجاب می‌کند که $r > 0$، و $\alpha' < 0$ نتیجه می‌دهد $r < \sqrt{d}$. از $\alpha > 1$ فوراً نتیجه می‌شود که $s < r + \sqrt{d}$، و چون $\alpha' > -1$، داریم $-s < (r - \sqrt{d})$، یعنی، $\sqrt{d} - r < s$.

اکنون فرض می‌کنیم $0 < r < \sqrt{d}$ و $\sqrt{d} - r < s < \sqrt{d} + r$. پس $s > 0$ و لذا $\alpha = (r + \sqrt{d})/s > 1$. همچنین، $r < \sqrt{d}$ ایجاب می‌کند که $\alpha' < 0$. چون $\sqrt{d} - r < s$، نتیجه می‌شود که $-s < r - \sqrt{d}$ و لذا $\alpha' = (r - \sqrt{d})/s > -1$. بنابراین α ساده شده است.

تقریبهای گویا برای اعداد گنگ

۳۹.۹ بهترین تقریب گویا به‌صورت a/b برای $\sqrt{2}$ با $b \leq 70$ را بیابید. بدون محاسبهٔ $\sqrt{2} - a/b$، بیان کنید که چرا $|\sqrt{2} - a/b| < 0.000085$.

حل. (۳۷.۹) را به‌کار می‌بریم. ابتدا بررسی می‌کنیم که $\sqrt{2} = \langle 1, \overline{2} \rangle$. اکنون جدول زیر را برای تعیین نخستین پنج همگرای $\sqrt{2}$ تشکیل می‌دهیم:

k	-۱	۰	۱	۲	۳	۴	۵	۶
a_k		۱	۲	۲	۲	۲	۲	۲
p_k	۱	۱	۳	۷	۱۷	۴۱	۹۹	۲۳۹
q_k	۰	۱	۲	۵	۱۲	۲۹	۷۰	۱۶۹

در این‌صورت از (۳۷.۹) نتیجه می‌شود که ۹۹/۷۰ بهترین تقریب گویا برای $\sqrt{۲}$ در میان تمام کسرهایی است که مخرجهای آنها از ۷۰ تجاوز نمی‌کنند. همچنین، بنابر (۳۳.۹) داریم

$$|\sqrt{۲} - ۹۹/۷۰| < ۱/(۷۰ \times ۱۶۹) = ۰٫۰۰۰۰۸۴۵۳\ldots < ۰٫۰۰۰۰۸۵.$$

۴۰.۹ فرض می‌کنیم $\sqrt{۳} - ۳ = \langle ۱, ۳, \overline{۱, ۲} \rangle$.

(الف) به‌ازای $۰ \le k \le ۴$ مقادیر r_k و s_k را محاسبه کنید.

(ب) فقط با استفاده از (الف) $\langle \overline{۱, ۲} \rangle$ را به‌صورت یک عدد گنگ درجه دوم بیان کنید.

(ج) درستی $\sqrt{۳} - ۳ < ۵۲/۴۱$ را به کمک قضیه‌ای از همگراها بررسی کنید.

(د) درستی $|۱۹ - ۱۵(۳ = \sqrt{۳})| < |۴۰(۳ = \sqrt{۳}) - ۵۱|$ را با استفاده از قضیه‌ای از تقریبها تعیین کنید.

حل. (الف) برای کاربرد (۲۴.۹) جهت محاسبهٔ r_k و s_k، ابتدا بایستی $\sqrt{۳} - ۳$ را به‌صورت $(r_۰ + \sqrt{d})/s_۰$ بنویسیم، به‌طوری که $s|d - r^۲$. در این حالت، داریم $\sqrt{۳} - ۳ = (-۳ + \sqrt{۳})/(-۱)$، لذا $r_۰ = -۳$ و $s_۰ = -۱$. بنابراین

k	۰	۱	۲	۳	۴
r_k	-۳	۲	۱	۱	۱
s_k	-۱	۱	۲	۱	۲
a_k	۱	۳	۱	۲	

لذا $\sqrt{۳} - ۳ = \langle ۱, ۳, \overline{۱, ۲} \rangle$.

(ب) بنابر (۱۹.۹) و (۲۴.۹)،

$$\langle \overline{۱, ۲} \rangle = \langle a_۲, a_۳, \ldots \rangle = \alpha_۲ = (r_۲ + \sqrt{d})/s_۲ = (۱ + \sqrt{۳})/۲$$

(ج) جدول زیر را تشکیل می‌دهیم

k	-۱	۰	۱	۲	۳	۴	۵
a_k		۱	۳	۱	۲	۱	۲
p_k	۱	۱	۴	۵	۱۴	۱۹	۵۲
q_k	۰	۱	۳	۴	۱۱	۱۵	۴۱

بنابر (۱۲.۹) داریم $\sqrt{۳} - ۳ < ۵۲/۴۱ = c_۵$.

(د) نامساوی برقرار نیست، زیرا (۳۶.۹) ایجاب می‌کند که $q_۵ \geq ۴۰$، یعنی $۴۱ \geq ۴۰$.

۴۱.۹ فرض می‌کنیم $\sqrt{۱۸} = \langle ۴, \overline{۴, ۸} \rangle$. با کاربرد قضیه‌ای از تقریبها، تمام اعداد گویای a/b در ساده‌ترین صورت با $۱۰ < b < ۱۰۰۰$ را بیابید به‌طوری که $|\sqrt{۱۸} - a/b| < ۱/۵b^۲$.

حل. جدول زیر را برای $\sqrt{۱۸}$ تشکیل می‌دهیم

k	-۱	۰	۱	۲	۳	۴
a_k		۴	۴	۸	۴	۸
p_k	۱	۴	۱۷	۱۴۰	۵۷۷	۴۷۵۶
q_k	۰	۱	۴	۳۳	۱۳۶	۱۱۲۱

اگر $|\sqrt{۱۸} - a/b| < ۱/۵b^۲ < ۱/۲b^۲$، آنگاه (۳۹.۹) ایجاب می‌کند که a/b همگرایی از $\sqrt{۱۸}$ باشد. لذا تنها مقادیر ممکن برای a/b، با $۱۰ < b < ۱۰۰۰$، عبارت‌اند از ۱۴۰/۳۳ و ۵۷۷/۱۳۶. (با یک حسابگر) بررسی کنید که $a/b = ۱۴۰/۳۳$ در نامساوی مفروض صدق نمی‌کند، ولی $a/b = ۵۷۷/۱۳۶$ صدق می‌کند.

◁ **۴۲.۹** فرض می‌کنیم $|\sqrt{۱۸} - ۱۴۰/۳۳| < |\sqrt{۱۸} - r/s|$. ثابت کنید $s \geq ۴۸$. (راهنمایی: ابتدا فرض می‌کنیم که $|\sqrt{۱۸} - r/s| < ۱/۲۵^۲$).

حل. اگر $|\sqrt{۱۸} - r/s| < ۱/۲۵^۲$، آنگاه بنابر (۳۹.۹)، r/s یک همگراست. چون $s < ۱۳۶$، بایستی داشته باشیم $r/s = ۱۴۰/۳۳, ۱۷/۴$، یا ۴/۱. (جدول مسألهٔ قبل را ببینید.) واضح است که، ۱۴۰/۳۳ امکان ندارد، و بنابر (۳۴.۹) مقادیر دیگر نیز غیرممکن هستند. لذا، بنابر (۳۳.۹)، $۱/۲s^۲ \leq |\sqrt{۱۸} - r/s| < |\sqrt{۱۸} - ۱۴۰/۳۳| < ۱/(۳۳ \times ۱۳۶)$. در نتیجه $s > \sqrt{۳۳ \times ۱۳۶/۲} = ۴۷٫۳۷۰۰۰$، و لذا $s \geq ۴۸$.

۴۳.۹ آیا ۲۲/۹ یکی از همگراهای $\sqrt{b}$ است؟ بدون محاسبهٔ همگراها بیان کنید.

حل. آری؛ $|\sqrt{۶} - ۲۲/۹| = ۰٫۰۰۵۰۴۵۰۰۰ < ۱/(۲ \times ۹^۲) = ۰٫۰۰۶۱۷۲۰۰۰$.
اکنون (۳۹.۹) را برای اثبات اینکه $۲۲/q$ بایستی یک همگرای $\sqrt{۶}$ باشد به‌کار برید.

۴۴.۹ بهترین تقریب گویا را برای $(\sqrt{b} - ۴)/۲$ با مخرجی که از ۳۹۶ تجاوز نکند پیدا کنید.

حل. $(\sqrt{b} - ۴)/۲$ را به‌صورت $(r_۰ + \sqrt{d})/s_۰$ می‌نویسیم؛ لذا $d = ۶$، $r_۰ = -۴$، $s_۰ = ۲$. چون $s|d - r^۲|$، می‌توانیم (۲۴.۹) را برای تشکیل جدولهای زیر به‌کار بریم:

k	۰	۱	۲	۳
r_k	−۴	۲	۲	۲
s_k	۲	۱	۲	۱
a_k	−۱	۴	۲	

k	−۱	۰	۱	۲	۳	۴	۵
a_k		−۱	۴	۲	۴	۲	۴
p_k	۱	−۱	−۳	−۷	−۳۱	−۶۹	−۳۰۷
q_k	۰	۱	۴	۹	۴۰	۸۹	۳۹۶

اکنون (۳۷.۹) را به‌کار برید تا نتیجه بگیرید که در میان تمام اعداد گویا با مخرج نابیشتر از ۳۹۶ کسر $-۳۰۷/۳۹۶$ بهترین تقریب گویا برای $(\sqrt{۶} - ۴)/۲$ است.

۴۵.۹ فرض می‌کنیم a و b و عدد صحیح مثبت و $\sqrt{۲} < a/b < ۹۹/۷۰$. نشان دهید $b > ۱۶۹$.

حل. با استفاده از (۳۳.۹) و جدول مربوط به مسألهٔ ۳۹.۹ داریم

$$۰ < |۹۹/۷۰ - a/b| < |\sqrt{۲} - ۹۹/۷۰| < ۱/(۷۰ \times ۱۶۹)$$

با ضرب نامساوی در $۷۰b$ داریم $۰ < |۹۹b - ۷۰a| < b/۱۶۹$. چون روشن است که $|۹۹b - ۷۰a|$ عدد صحیح مثبتی است، داریم $b/۱۶۹ > ۱$، یعنی، $b > ۱۶۹$.

۴۶.۹ فرض می‌کنیم α گنگ، و فرض می‌کنیم a و b دو عدد صحیح باشند با b مثبت به‌طوری که $|\alpha - a/b| < |\alpha - p_k/q_k|$. ثابت کنید $b > q_{k+۱}/۲$.

حل. بنابر نابرابری مثلثی

$$۰ < |a/b - p_k/q_k| \le |a/b - \alpha| + |\alpha - p_k/q_k| < ۲|\alpha - p_k/q_k| < ۲/q_k q_{k+۱}$$

با ضرب نامساوی در bq_k داریم $0 < aq_k - bp_k| < 2b/q_{k+1}$. چون $|aq_k - p_k/q_k|$ عدد صحیح مثبتی است، داریم $2b/q_{k+1} > 1$، و لذا $b > q_{k+1}/2$.

توضیح. قضیهٔ معمولی (۳۷.۹) ایجاب می‌کند که اگر $|\alpha - a/b| < |\alpha - p_k/q_k|$، آنگاه $b > q_k$. از این‌رو، اگر $q_k > q_{k+1}/2$، نتیجهٔ این مسأله ضعیفتر است. مثلاً، اگر $\alpha = \pi$، آنگاه $p_2/q_2 = 333/106$، $p_3/q_3 = 355/113$، و $p_4/q_4 = 103993/33102$؛ لذا به‌ازای $k = 2$، نابرابری $b > q_k$ ایجاب می‌کند که $b > 106$، در حالی‌که $b > q_{k+1}/2$ فقط نتیجه می‌دهد که $b > 56$. اما این مسأله می‌تواند نتیجهٔ بسیار قوی‌تری را ارائه دهد: اگر $k = 3$، آنگاه $b > q_k$ ایجاب می‌کند که $b > 113$، اما $b > q_{k+1}/2$ ایجاب می‌کند که $b > 16551$!

۴۷.۹ فرض می‌کنیم $|\sqrt{2} - 41/29| < |\sqrt{2} - r/s|$، که $s > 0$. نشان دهید که $s \geq 36$. (راهنمایی: از مسألهٔ قبل استفاده کنید.)

حل. به جدول مسألهٔ ۳۹.۹ مراجعه می‌کنیم. چون $|\sqrt{2} - p_4/q_4| < |\sqrt{2} - r/s|$، از مسألهٔ قبل نتیجه می‌شود که $s > q_5/2$، یعنی $s \geq 36$.

۴۸.۹ فرض می‌کنیم p_k/q_k همگرای kام عدد گنگ α باشد. اگر a و b اعداد صحیح باشند و $b \geq 1$ و $\alpha < a/b < p_k/q_k$ (یا $(p_k/q_k) < a/b < \alpha$)، ثابت کنید $b > q_{k+1}$.

حل. استدلال اساساً مشابه راه‌حل مسألهٔ ۴۵.۹ است. با استفاده از (۳۳.۹) داریم $0 < |a/b - p_k/q_k| < \alpha - p_k/q_k| < 1/q_k q_{k+1}$، و از ضرب نابرابری در bq_k نتیجه می‌شود $0 < |aq_k - bp_k| < b/q_{k+1}$. چون $|aq_k - bq_k|$ عدد صحیح مثبتی است، نتیجه می‌شود که $b/q_{k+1} > 1$، یعنی $b > q_{k+1}$.

۴۹.۹ فرض می‌کنیم p_k/q_k همگرای kام عدد گنگ α باشد. ثابت کنید به‌ازای هر $k \geq 0$، $1/2q_k q_{k+1} < |\alpha - p_k/q_k| < 1/q_k q_{k+1}$.

حل. نابرابری دوم در (۳۳.۹) ثابت شده است. برای اثبات نابرابر اول، ملاحظه کنید که α بین $c_k = p_k/q_k$ و $c_{k+1} = p_{k+1}/q_{k+1}$ قرار دارد (توضیح بعد از (۱۲.۹) را ببینید). همچنین، بنابر (۳۴.۹)، α به c_{k+1} نزدیکتر است تا به c_k. بنابراین، فاصلهٔ بین α و c_k بزرگتر از نصف فاصلهٔ بین c_k و c_{k+1} است. با استفاده از (۷.۹) به آسانی دیده می‌شود که فاصلهٔ بین c_k و c_{k+1} عبارت است از $1/q_k\, q_{k+1}$، که نابرابری اول را به‌دست می‌دهد.

۵۰.۹ فرض کنیم α گنگ و $|s\alpha - r| \geq 1/s$، که $(r,s) = 1$ و $s \geq 1$. ثابت کنید r/s نمی‌تواند یکی از همگراهای α باشد.

حل. از نابرابری فرض داریم $|\alpha - r/s| \geq 1/s^2$، که با (۳۳.۹) اگر r/s همگرا باشد تناقض دارد.

۵۱.۹ اگر p_k/q_k همگرای kـام عدد گنگ α باشد، ثابت کنید

$$|\alpha - p_k/q_k| > 1/q_k(q_k + q_{k+1})$$

حل. در (۱۸.۹) نشان داده شد که $\alpha - p_k/q_k = (-1)^k/q_k(\alpha_{k+1}q_k + q_{k-1})$. اما $\alpha_{k+1} < a_{k+1} + 1$ (زیرا $a_{k+1} = [\alpha_{k+1}]$). لذا

$$\alpha_{k+1}q_k + q_{k-1} < a_{k+1}q_k + q_{k-1} + q_k = q_{k+1} + q_k$$

و نتیجه حاصل است.

◁ **۵۲.۹** فرض کنیم α گنگ باشد. ثابت کنید دست‌کم یکی از هر دو همگرای متوالی بسط کسر مسلسل α در $|\alpha - p/q| < 1/2q^2$ صدق می‌کند. (راهنمایی: اتحاد

$$|\alpha - p_k/q_k| + |p_{k+1}/q_{k+1} - \alpha| = 1/q_kq_{k+1}$$

را به‌کار برید.)

حل. اتحاد ارائه‌شده در راهنمایی نتیجهٔ بلافصل این حقیقت است که α بین p_k/q_k و p_{k+1}/q_{k+1} قرار دارد و اینکه $p_{k+1}q_k - p_kq_{k+1} = \pm 1$. اکنون فرض می‌کنیم که $|\alpha - p_k/q_k| \geq 1/2q_k^2$ و $|\alpha - p_{k+1}/q_{k+1}| \geq 1/2q_{k+1}^2$. چون α گنگ است، برابری امکان ندارد. لذا، با کاربرد اتحاد داریم $1/q_kq_{k+1} > 1/2q_k^2 + 1/2q_{k+1}^2$. از ضرب این نامساوی در $2q_k^2q_{k+1}^2$ و ساده کردن، به‌دست می‌آوریم $(q_k - q_{k+1})^2 < 0$، که ممکن نیست.

◁ **۵۳.۹** قضیهٔ (۳۹.۹) را ثابت کنید: اگر α گنگ باشد و c/d عدد گویایی با $d \geq 1$ باشد به‌طوری که $|\alpha - c/d| < 1/2d^2$، آنگاه c/d یکی از همگراهای بسط کسر مسلسل α است. (راهنمایی: (۳۵.۹) را به‌کار برید.)

حل. فرض کنیم u و $v > 0$ دوعدد صحیح باشند به‌طوری که $u/v \neq c/d$ و $|u/v - c/d| \leq |\alpha - u/v| + |\alpha - c/d|$. بنابر نابرابری مثلثی داریم $|v\alpha - u| \leq |d\alpha - c|$.

چون $|d\alpha - c| < 1/2d$، در نتیجه $|u/v - c/d| < 1/d^2$. از ضرب این نابرابری در dv داریم $|du - cv| < v/d$. اما $du - cv$ عدد صحیح غیرصفری است، و لذا $v > d$. اکنون نتیجه از (۳۵.۹) حاصل می‌شود.

تقریب گویای π

۵۴.۹ فرض کنیم r/s عدد گویایی باشد به‌طوری که $\pi < r/s < 22/7$. ثابت کنید $s > 106$. (راهنمایی: حل مسألهٔ ۴۵.۹ را ببینید.)

حل. بنابر (۳۳.۹) داریم $0 < |22/7 - r/s| < |\pi - 22/7| < 1/(7 \times 106)$، زیرا $22/7$ همگرایی از π است. اگر در s ضرب کنیم، به‌دست می‌آوریم $0 < |22s - 7r| < s/106$. چون $|22s - 7r|$ عدد صحیح مثبتی است، داریم $s/106 > 1$، یعنی $s > 106$.

◁ **۵۵.۹** اگر r و s دو عدد صحیح مثبت باشند و $\pi < r/s < 22/7$، ثابت کنید $s \geq 113$. (راهنمایی: حالتهای $r/s < 355/113$ و $r/s \geq 355/113$ را جداگانه بررسی کنید. (۳۸.۹) را ببینید.)

حل. ابتدا فرض می‌کنیم $r/s < 355/113$ ($355/113$ سومین همگرای π است)؛ در این‌صورت $|\pi - 355/113| < |\pi - r/s|$، و لذا بنابر (۳۷.۷)، $s > 113$. اکنون فرض می‌کنیم $\pi < 355/113 \geq r/s < 22/7$. اگر $r/s = 355/113$، آنگاه $s \geq 113$ (در واقع، اگر $(r, s) = 1$، $s = 113$). اگر $r/s > 355/113$، آنگاه (بنابر (۸.۹) یا با محاسبهٔ مستقیم) $0 < |r/s - 22/7| < |22/7 - 355/113| = 1/(7 \times 113)$. از ضرب نابرابری در $7s$ داریم $0 < |7r - 22s| < s/113$. چون $7r - 22s$ عدد صحیح نامنفی است، داریم $|7r - 22s| \geq 1$، و لذا $s/113 > 1$، یعنی $s > 113$. بنابراین در هر حالت، $s \geq 113$.

۵۶.۹ (الف) فرض کنیم r و s اعداد صحیح مثبتی باشند به‌طوری که

$$|\pi - r/s| < |\pi - 355/113|$$

نشان دهید $s \geq 16552$. (راهنمایی: مسأله‌ای از بخش قبل را به‌کار برید.)

(ب) در میان تمام اعداد گویایی که مخرجشان از ۱۶۵۵۱ تجاوز نمی‌کند بهترین تقریب گویا برای π را بیابید.

حل. از جدول مربوط به (۳۸.۹) داریم $p_3/q_3 = 355/113$ و $q_4 = 33102$. لذا از مسألهٔ ۴۶.۹ نتیجه می‌شود که $s > q_4/2 = 16551$.

(ب) با توجه به قسمت (الف)، ۳۵۵/۱۱۳ بهترین تقریب گویا برای π با مخرجی که از ۱۶۵۵۱ تجاوز نمی‌کند است.

۵۷.۹ بهترین تقریب گویا را برای π با مخرج کمتر از ۱۳۰۰۰۰ به‌دست آورید. (راهنمایی: جدول مربوط به (۳۸.۹) را تا $k = 8$ توسعه دهید، و مسألهٔ ۴۶.۹ را به‌کار برید.)

حل. جدول زیر را محاسبه می‌کنیم ((۳۸.۹) را ببینید):

k	-1	۰	۱	۲	۳	۴	۵	۶	۷	۸
a_k		۳	۷	۱۵	۱	۲۹۲	۱	۱	۱	۲
p_k	۱	۳	۲۲	۳۳۳	۳۵۵	۱۰۳۹۹۳	۱۰۴۳۴۸	۲۰۸۳۴۱	۳۱۲۶۸۹	۸۳۳۷۱۹
q_k	۰	۱	۷	۱۰۶	۱۱۳	۳۳۱۰۲	۳۳۲۱۵	۶۶۳۱۷	۹۹۵۳۲	۲۶۵۳۸۱

بنابر (۳۷.۹)، p_7/q_7 بهترین تقریب گویا برای π در میان تمام اعداد گویا با مخرج نابیشتر از $q_7 = 99532$ است. اکنون فرض می‌کنیم $|\pi - r/s| < |\pi - p_7/q_7|$. با استفاده از مسألهٔ ۴۶.۹ داریم $s > q_8/2 > 130000$. لذا نتیجه می‌گیریم که هیچ عدد گویای r/s؛ $s < 130000$ وجود ندارد که π را بهتر از $p_7/q_7 = 312689/99532$ تقریب زند.

۵۸.۹ فرض می‌کنیم r/s عدد گویایی باشد که $r/s \neq 22/7$. اگر $0 < s \leq 53$، ثابت کنید که $|\pi - r/s| < |\pi - 22/7|$. به عبارت دیگر، نشان دهید که ۲۲/۷ عدد π را بهتر از هر عدد گویای دیگر با مخرج نابیشتر از ۵۳ تقریب می‌زند.

حل. مسألهٔ ۴۶.۹ را به‌کار می‌بریم. ملاحظه کنید که $22/7 = p_1/q_1$ و $333/106 = p_2/q_2$ همگراهای π هستند ((۳۸.۹) را ببینید). اگر $|\pi - 22/7| < |\pi - r/s|$، مسألهٔ ۴۶.۹ ایجاب می‌کند که $s > q_2/2 = 106/2 = 53$. چون $s \leq 53$، نتیجه می‌شود که $|\pi - r/s| < |\pi - 22/7|$. (ملاحظه کنید که $|\pi - r/s|$ نمی‌تواند برابر $|\pi - 22/7|$ باشد؛ در غیر این‌صورت، چون $r/s \neq 27/7$، داریم $r/s = 2\pi - 22/7$، که گویا نیست.)

توضیح. اگر $s \leq 56$ نتیجه درست است ولی برای $s = 57$ درست نیست؛ در واقع، عدد گویای ۱۷۹/۵۷ عدد π بهتر از ۲۲/۷ تقریب می‌کند. عدد ۱۷۹/۵۷ یک همگرای میانی π است؛ برای مشاهده ویژگیهای همگراهای میانی بخش بعدی مسائل را ببینید. مثلاً، واقعیت دارد که بهترین تقریب گویای π با مخرج نابیشتر از ۵۶ بایستی یا یک همگرا یا یک همگرای میانی از π باشد (مسألهٔ ۶۶.۹ را ببینید). به آسانی بررسی می‌شود که هیچ همگرای میانی از π وجود

ندارد که مخرجش بین ۵۳ و ۵۶ باشد، و لذا نتیجهٔ مسألهٔ ۵۸.۹ برای $s \le 56$ برقرار است. این نشان می‌دهد که وقتی $|\alpha - r/s| < |\alpha - p_k/q_k|$ ایجاب می‌کند $s \ge q_k$ (بنابر (۳۷.۹)) ولی نتیجه نمی‌دهد که $s \ge q_{k+1}$. (برای π، $q_1 = 7$ و $q_2 = 106$، اما (دقیقاً هفت) عدد گویا با مخرجِ بین ۷ و ۱۰۶ وجود دارند که π را بهتر از ۲۲/۷ تقریب می‌زنند. مسألهٔ ۶۹.۹ را ببینید.)

◁ **۵۹.۹** عدد گویای r/s را پیدا کنید به‌طوری که $|\pi - 22/7| < |\pi - r/s|$ و $s < 106$. (راهنمایی: π را با $\langle 3, 7, 15\rangle = 333/106$ تقریب بزنید، و ملاحظه کنید که $\langle 3, 7, 15, 1\rangle = \langle 3, 7, 14, 1\rangle$. سپس (۳۳.۹) و مسألهٔ ۴۹.۹ را به‌کار برید.)

حل. همگراهای $\langle 3, 7, 14, 1\rangle$ را از جدول زیر پیدا می‌کنیم:

k	-1	0	1	2	3
a_k		3	7	14	1
p_k	1	3	22	311	333
q_k	0	1	7	99	106

توجه کنید که ۲۲/۷ و ۳۳۳/۱۰۶ همگراهای متوالی π هستند (۳۱۱/۹۹ همگرایی از π نیست، بلکه یک همگرای میانی است؛ بخش زیر را ببینید). اکنون (۷.۹)، (۳۳.۹)، و نابرابری مثلثی را به‌کار می‌بریم تابه‌دست آوریم:

$$\begin{aligned} |\pi - 311/99| &\le |\pi - 333/106| + |333/106 - 311/99| \\ &< 1/106^2 + |333 \times 99 - 311 \times 106|/(99 \times 106) \\ &= 1/(106)^2 + 1/(99 \times 106) < 1/(2 \times 7 \times 106)\,. \end{aligned}$$

بالاخره، مسألهٔ ۴۹.۹ ایجاب می‌کند که $|\pi - 22/7| > 1/(2 \times 7 \times 106)$. و لذا نتیجه می‌گیریم که $|\pi - 22/7| < |\pi - 311/99|$.

همگراهای میانی

فرض کنیم α گنگ است، و فرض می‌کنیم p_k/q_k همگرای kام α را نشان دهد. به‌ازای $k \ge 2$، دنبالهٔ زیر را در نظر می‌گیریم

$$\frac{p_{k-2}}{q_{k-2}},\ \frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}},\ \frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}},\ \dots,\ \frac{p_{k-2}+a_kp_{k-1}}{q_{k-2}+a_kq_{k-1}} = \frac{p_k}{q_k}\,.$$

بجز جمله‌های اول و آخر، یعنی $p_{k-۲}/q_{k-۲}$ و p_k/q_k، سایر اعدادِ دنباله همگراهای میانی α خوانده می‌شوند. برای ساده کردن نمادگذاری، فرض می‌کنیم

$$c_{k,t} = p_{k,t}/q_{k,t} = (p_{k-۲} + tp_{k-۱})/(q_{k-۲} + tq_{k-۱})$$

که $۱ \le t \le a_k - ۱$. آشکار است که اگر $a_k = ۱$، آنگاه هیچ همگرای میانی بین $p_{k-۲}/q_{k-۲}$ و p_k/q_k قرار ندارد.

ملاحظه کنید که همگرای میانی $c_{k,t}$ همگی بین جفتی از همگراها واقع می‌شوند که اختلاف اندیس آنها ۲ است و لذا (بنابر (۱۲.۹)) یا هر دو بزرگتر از α هستند (اگر k فرد باشد) یا هر دو کوچکتر از α (اگر k زوج باشد). در زیر نشان خواهیم داد که همگراهای میانی α در ساده‌ترین صورت هستند و همگراهای میانی بین $p_{k-۲}/q_{k-۲}$ و p_k/q_k وقتی k زوج باشد صعودی اکید و اگر k فرد باشد نزولی اکید هستند؛ در نتیجه همگی در یک سمت α قرار دارند. و مانند همگراها، در همان نوع معادلهٔ ارائه‌شده در (۷.۹) صدق می‌کنند: اگر r/s و r'/s' همگراهای میانی متوالی باشند، آنگاه $rs' - r's = \pm ۱$.

این ویژگیها به ما اجازه می‌دهند که به سؤال طرح‌شده در توضیحِ بعد از (۳۷.۹) به‌طور کامل پاسخ دهیم: اگر s عدد صحیح مثبتی باشد، بهترین تقریب برای عدد گنگ α در میان تمام اعداد گویا با مخرج نابیشتر از s چیست؟ همان‌گونه که در مسألهٔ ۶۶.۹ نشان خواهیم داد، به‌ازای هر s مفروض، بهترین تقریب گویای دارای این ویژگی همواره یا یک همگراست یا یک همگرای میانی.

برای روشن شدن مطلب، همگراهای $\pi = \langle ۳, ۷, ۱۵, ۱, \ldots \rangle$ را در نظر می‌گیریم؛ لذا $p_۰/q_۰ = ۳/۱$، $p_۱/q_۱ = \langle ۳, ۷ \rangle = ۲۲/۷$، و $p_۲/q_۲ = \langle ۳, ۷, ۱۵ \rangle = ۳۳۳/۱۰۶$. بنا به تعریف، همگراهای میانی بین ۳/۱ و ۳۳۳/۱۰۶ عبارت‌اند از اعداد $(۳ + ۲۲t)/(۱ + ۷t)$، با $۱ \le t \le a_۲ - ۱ = ۱۴$؛ لذا اولین همگرای میانی ۲۵/۸ و آخری ۳۱۱/۹۹ است. می‌توان این همگراهای میانی را به روش مفید زیر مشخص کرد. این همگراها دقیقاً مقادیر $\langle ۳, ۷, t \rangle$ به‌ازای $۱ \le t \le ۱۴$ هستند. اینکه این مطلب در حالت کلی درست است در قضیهٔ بعد ثابت شده است.

۶۰.۹ فرض می‌کنیم $\alpha = \langle a_۰, a_۱, a_۲, \ldots \rangle$ گنگ است، و $p_{k,t}q_{k,t}$ یک همگرای میانی بین $p_{k-۲}/q_{k-۲}$ و p_k/q_k. ثابت کنید

$$p_{k,t}/q_{k,t} = \langle a_۰, a_۱, \ldots, a_{k-۱}, t \rangle$$

حل. بنابر (۴.۹) داریم

$$\langle a_0, a_1, \ldots, a_{k-1}, t\rangle = (tp_{k-1} + p_{k-2})/(tq_{k-1} + q_{k-2}) = p_{k,t}/q_{k,t}$$

در چند مسألهٔ بعدی اثبات بعضی از ویژگیهای اساسی همگراهای میانی داده شده است.

۶۱.۹ اگر r/s و r'/s' دو همگرای میان متوالی بین p_{k-2}/q_{k-2} و p_k/q_k باشند، ثابت کنید $rs' - r's = (-1)^k$.

حل. فرض می‌کنیم $r/s = c_{k,t}$ و $r'/s' = c_{k,t+1}$. سپس با کاربرد (۷.۹)، از تعریف به آسانی می‌توان رسیدگی کرد که به‌ازای هر مقدار t، $rs' - r's = p_{k-1}q_k - p_kq_{k-1} = (-1)^k$. (جمله‌های شامل t حذف شده‌اند.)

۶۲.۹ اگر $p_{k,t}/q_{k,t}$ یک همگرای میانی α باشد، ثابت کنید $(p_{k,t}, q_{k,t}) = 1$.

حل. این مطلب مستقیماً از مسألهٔ قبل نتیجه می‌شود. زیرا اگر d یک مقسوم‌علیه مشترکِ $p_{k,t}$ و $q_{k,t}$ باشد، آنگاه $d|(-1)^k$ و لذا $d = 1$. این نتیجه همچنین یک نتیجهٔ آسان مسألهٔ ۶۰.۹ است؛ چون $p_{k,t}/q_{k,t} = \langle a_0, a_1, \ldots, a_{k-1}, t\rangle$، (۴.۹) ایجاب می‌کند که $p_{k,t}/q_{k,t}$ همان آخرین همگرای این کسر مسلسل باشد. اکنون (۷.۹) را به‌کار برید.

۶۳.۹ ثابت کنید همگراهای میانی بین p_{k-2}/q_{k-2} و p_k/q_k اگر k زوج باشد دنباله‌ای اکیداً صعودی و اگر k فرد باشد دنباله‌ای اکیداً نزولی تشکیل می‌دهند. (راهنمایی: این مطلب به آسانی از مسأله‌های ۱۵.۹ و ۶۰.۹ نتیجه می‌شوند.)

حل. این مطلب را می‌توان مستقیماً از تعریف همگراهای میانی با نشان دادن اینکه $c_{k,t} - c_{k,t+1} = (-1)^k/q_{k,t}q_{k,t+1}$ به‌دست آورد، از آنجا قضیه حاصل می‌شود. یک روش آسانتر برای اثبات این قضیه این است که مسألهٔ ۶۰.۹ را به‌کار بریم و بنویسیم $c_{k,t} = \langle a_0, a_1, \ldots, a_{k-1}, t\rangle$ و $c_{k,t+1} = \langle a_0, a_1, \ldots, a_{k-1}, t+1\rangle$. سپس نتیجه از مسألهٔ ۱۵.۹ به آسانی به‌دست می‌آید.

قضیه‌های زیر اثبات ویژگیهای تقریبِ همگراهای میانی را به‌دست می‌دهند.

◁ **۶۴.۹** فرض می‌کنیم α گنگ، و $|\alpha - p_{k,t}/q_{k,t}| < |\alpha - c/d|$. ثابت کنید یا $c/d = p_{k-1}/q_{k-1}$، یا $d > q_{k,t}$.

حل. مطابق معمول، فرض می‌کنیم $c_{k-1} = p_{k-1}/q_{k-1}$. بنابر نابرابری مثلثی می‌نویسیم

$$|c/d - c_{k-1}| \le c/d - \alpha| + |\alpha - c_{k-1}| \le |\alpha - c_{k,t}| + |\alpha - c_{k-1}| = |c_{k-1} - c_{k,t}|$$

(تساوی آخر برقرار است زیرا $\alpha - c_{k-1}$ و $\alpha - c_{k,t}$ مختلف‌العلامه هستند: بنابر (۱۲.۹)، $c_{k,t}$ همانند c_k و c_{k-2} در یک طرف α، و c_{k-1} در طرف دیگر α قرار دارند.) اگر به واقع نابرابری اول یک برابری باشد، آنگاه c/d و c_{k-1} بایستی در دو طرف α واقع شوند، و لذا α بین c/d و c_{k-1} واقع است. اگر در نابرابری دوم برابری برقرار باشد، آنگاه c/d و $c_{k,t}$ به فاصلهٔ مساوی از α قرار دارند، و لذا اگر $c/d \neq c_{k,t}$، آنگاه c/d و c_{k-1} در یک طرف α واقع می‌شوند، که یک تناقض است. بنابراین لااقل یکی از این دو نابرابری اکید است.

ملاحظه کنید که بنابر (۷.۹)، $p_{k-1}q_{k,t} - q_{k-1}p_{k,t} = p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k$. لذا اگر $c/d \neq c_{k-1}$، داریم $0 < |c/d - c_{k-1}| < |c_{k-1} - c_{k,t}| = 1/q_{k-1}q_{k,t}$. سپس از ضرب در dq_{k-1} داریم $0 < |cq_{k-1} - dp_{k-1}| < d/q_{k,t} \le 1$، و لذا $d > q_{k,t}$.

۶۵.۹ فرض می‌کنیم p/q یک همگرا یا یک همگرای میانی عدد گنگ α باشد. اگر c/d عدد گویایی بین α و p/q باشد، ثابت کنید $d > q$. (راهنمایی، مسألهٔ قبل را به‌کار برید.)

حل. اگر p/q یک همگرا باشد، نتیجه از (۳۷.۹) حاصل می‌شود. حال، فرض می‌کنیم p/q یک همگرای میانی، مثلاً $c_{k,t}$ باشد. ملاحظه کنید که c_{k-1} نمی‌تواند بین α و $c_{k,t}$ واقع شود، زیرا c_{k-1} و $c_{k,t}$ در دو طرف α قرار دارند؛ لذا c/d نمی‌تواند با c_{k-1} برابر شود. از مسألهٔ قبل نتیجه می‌شود که $d > q$.

اکنون به قضیهٔ اصلی مربوط به ویژگیهای تقریبِ همگراها و همگراهای میانی می‌پردازیم.

◁ **۶۶.۹** فرض می‌کنیم α گنگ و s عدد صحیح مثبتی باشد. ثابت کنید که بهترین تقریبِ α در میان تمام اعداد گویا با مخرجِ نابیشتر از s یا یک همگرا یا یک همگرای میانی α است. به عبارت هم‌ارز، ثابت کنید اگر r/s به‌گونه‌ای باشد که هر عدد گویای بین r/s و α دارای مخرجی بزرگتر از s باشد، آنگاه r/s یا یک همگرا یا یک همگرای میانی α است.

حل. صورتِ دوم مسأله را ثابت می‌کنیم. فرض کنیم S معرف دنبالهٔ صعودی همگراهای با اندیس زوجِ α، به ضمیمهٔ تمام همگراهای میانی بین آنها باشد. همچنین، فرض می‌کنیم T معرف دنبالهٔ صعودی همگراهای با اندیسِ فردِ α، به ضمیمه تمام همگراهای میانی بین آنها باشد. فرض می‌کنیم r/s نه یک همگرا و نه یک همگرای میانی α باشد. دو حالت در نظر می‌گیریم. اگر

$r/s < \alpha$، آنگاه r/s در همان طرفی از α است که همگراهای با اندیس زوج قرار دارند، و لذا یا r/s بین دو جملهٔ متوالی S قرار می‌گیرد یا $r/s < p_0/q_0 = a_0$. همچنین، اگر $r/s > \alpha$، آنگاه r/s در همان طرفی از α است که همگراهای با اندیس فرد قرار دارند، و بنابراین یا r/s بین دو جملهٔ متوالی T قرار می‌گیرد یا $r/s > (p_{-1}+p_0)/(q_{-1}+q_0) = a_0 + 1$ (تنها همگرای میانی α که بزرگتر از p_1/q_1 است). اگر یا $r/s < a_0 = [\alpha] < \alpha$ یا $r/s > a_0 + 1 > \alpha$ (زیرا $a_0 \le \alpha < a_0 + 1$)، آنگاه r/s در مفروضات مسأله صدق نمی‌کند، زیرا عدد گویایی بین α و r/s با مخرج ۱ قرار دارد، یعنی، به‌ترتیب، a_0 یا $a_0 + 1$. (توجه کنید که فرض بر این است که مخرج بزرگتر از s، و $s \ge 1$.)

بنابراین، می‌توانیم فرض کنیم که r/s بین دو جملهٔ متوالی S یا T قرار دارد. این جمله‌ها را با $c = p/q$ و $c' = p'/q'$ نشان می‌دهیم؛ لذا یا $c' < r/s < c < \alpha$ یا $a < c < r/s < c'$. در هر دو حالت، c بین r/s و α واقع می‌شود؛ همچنین، $0 < |r/s - c'| < |c - c'| = 1/qq'$ (با کاربرد مسألهٔ ۶۱.۹). از ضرب نابرابری در sq'، داریم $0 < |rq' - sp'| < s/q$، و چون $|rq' - sp'|$ عدد صحیح مثبتی است، نتیجه می‌شود که $s > q$. لذا، بین r/s و α عدد گویای p/q با مخرج کمتر از s قرار دارد، که با فرض متناقض است. در نتیجه r/s یا یک همگرا یا یک همگرای میانی α است.

از همگراهای میانیِ بین p_{k-2}/q_{k-2} و p_k/q_k، بعضی α را بهتر از همگرای p_{k-1}/q_{k-1} تقریب می‌زنند، و بعضی چنین نیستند. مسألهٔ بعد دقیقاً بیان می‌کند که کدام یک از همگرای میانی تقریب بهتری است.

◁ **۶۷.۹** فرض می‌کنیم α گنگ باشد. ثابت کنید $|\alpha - p_{k,t}/q_{k,t}| < |\alpha - p_{k-1}/q_{k-1}|$ اگر و تنها اگر (i) $t > a_k/2$ یا (ii) $t = a_k/2$ و $\langle a_k, a_{k+1}, \ldots\rangle > \langle a_k, a_{k-1}, \ldots, a_1\rangle$. به‌ویژه، اگر $t < a_k/2$، آنگاه $p_{k,t}/q_{k,t}$ هرگز تقریبی بهتر از p_{k-1}/q_{k-1} برای α نیست.

حل. از تعریف $p_{k,t}$ و $q_{k,t}$ داریم

$$|\alpha - p_{k,t}/q_{k,t}| < |\alpha - p_{k-1}/q_{k-1}|$$

اگر و تنها اگر

$$|t(\alpha q_{k-1} - p_{k-1}) + \alpha q_{k-2} - p_{k-2}|/q_{k,t} < |\alpha q_{k-1} - p_{k-1}|/q_{k-1}.$$

بنابر (۴.۹) و (۱۹.۹)،

$$\alpha = \langle a_0, a_1, \ldots, a_{k-1}, \alpha_k\rangle = (\alpha_k p_{k-1} + p_{k-2})/(\alpha_k q_{k-1} + q_{k-2})$$

و لذا $\alpha_k = -(\alpha q_{k-2} - p_{k-2})/(\alpha q_{k-1} - p_{k-1})$. بنابراین، نابرابری آخر برقرار است اگر و تنها اگر $|(t-\alpha_k)(\alpha q_{k-1} - p_{k-1})|/q_{k,t} < |\alpha q_{k-1} - p_{k-1}|/q_{k-1}$، یعنی، اگر و تنها اگر $|\alpha_k - t| q_{k-1} < q_{k,t} = q_{k-2} + t p_{k-1}$. چون $t < a_k < \alpha_k$، لذا $\alpha_k - t$ مثبت است، و بنابراین نابرابر آخر با $2t q_{k-1} + q_{k-2} > \alpha_k q_{k-1}$ هم‌ارز است. اگر $2t \geq a_k + 1$ این شرط برقرار است، زیرا در این‌صورت $2t q_{k-1} + q_{k-2} \geq (a_k+1) q_{k-1} > \alpha_k q_{k-1}$، و اگر $2t \leq a_k - 1$، و اگر $2t \leq a_k - 1$ این شرط برقرار نیست، زیرا در این‌صورت

$$2t q_{k-1} + q_{k-2} \leq (a_k - 1) q_{k-1} + q_{k-1} = a_k q_{k-1} < \alpha_k q_{k-1}.$$

سرانجام، اگر $2t = a_k$، شرط برقرار است اگر و تنها اگر $a_k q_{k-1} + q_{k-2} > \alpha_k q_{k-1}$، یعنی، $q_k/q_{k-1} > \alpha_k$، و بنابر مسألهٔ ۸.۹، نابرابری $q_k/q_{k-1} > \alpha$ با

$$\langle a_k, a_{k-1}, \ldots, a_1 \rangle > \langle a_k, a_{k+1}, \ldots \rangle$$

هم‌ارز است.

توضیح. این مسأله نشان می‌دهد که از همگراهای میانی بین p_{k-2}/q_{k-2} و p_k/q_k، تنها آنهایی که در نیمهٔ دوم دنباله قرار دارند نزدیکتر از p_{k-1}/q_{k-1} (که در طرف دیگر α قرار دارد) به α هستند. اگر a_k زوج باشد، یک همگرای میانی «وسط» وجود خواهد داشت، و این بر طبق شرط ارائه‌شده در بالا بایستی به‌طور جداگانه بررسی شود.

۶۸.۹ فرض می‌کنیم $\alpha = \langle a_0, a_1, \ldots \rangle$ گنگ باشد. از مسألهٔ قبل نتیجه می‌شود که اگر $a_k \geq 3$، آنگاه $|\alpha - (p_k - p_{k-1})/(q_k - q_{k-1})| < |(\alpha - p_{k-1}/q_{k-1}|$. (ملاحظه کنید که $(p_k - p_{k-1})/(q_k - q_{k-1})$ آخرین همگرای بین p_{k-1}/q_{k-1} و p_K/q_K است.) با مثالی نشان دهید که نابرابری بالا به‌ازای $a_k = 2$ لزوماً برقرار نیست. (راهنمایی: $\alpha = (1+\sqrt{3})/2$ را در نظر بگیرید.)

حل. بازبینی می‌کنیم که $\alpha = (1+\sqrt{3})/2 = \langle \overline{1, 2} \rangle$؛ در این‌صورت $a_3 = 2$، $p_1/q_1 = 3/2$، $p_2/q_2 = 4/3$، و $p_3/q_3 = 11/8$. تنها همگرای میانیِ بین $3/2$ و $11/8$ عبارت است از $(3+4)/(2+3) = 7/5$، اما $|\alpha - 7/4| < |\alpha - 4/3|$.

سرانجام، قضیه‌های قبلی را در مورد همگراهای میانی π به‌کار می‌بریم.

۶۹.۹ با کاربرد مسألهٔ ۶۸.۹ تعیین کنید کدام‌یک از همگراهای میانی π که بین 3 و $333/106$

قرار دارند، عدد π را بهتر از ۲۲/۷ تقریب می‌زنند. بهترین تقریب π در میان تمام اعداد گویا با مخرجِ نابیشتر از ۱۰۰ چیست؟

حل. به مثال (۳۸.۸) مراجعه می‌کنیم: $p_0/q_0 = ۳/۱$، $p_1/q_1 = ۲۲/۷$، و $p_2/q_2 = ۳۳۳/۱۰۶$. لذا همگراهای میانی با $(۳ + ۲۲t)/(۱ + ۷t)$ که $۱ \geq t \geq ۱۴$، داده می‌شوند:

$$۲۵/۸,\ ۴۷/۱۵,\ ۶۹/۲۲,\ \ldots,\ ۱۵۷/۵۰,\ ۱۷۹/۵۷,\ \ldots,\ ۲۸۹/۹۲,\ ۳۱۱/۹۹$$

بنابر مسألهٔ قبل، همگراهای میانیِ به‌ازای $۷ \leq t \leq ۱$ (یعنی، همگراهای تا با ۱۵۷/۵۰) بدتر از ۲۲/۷ عدد π را تقریب می‌زنند در حالی‌که همگراهای میانیِ به‌ازای $۱۴ \leq t \leq ۸$ (از ۱۷۴/۵۷ تا با ۳۱۱/۹۹) به‌ترتیب تقریبهای بهتری از ۲۲/۷ ارائه می‌دهند. از آنجا که همگرا یا همگرای میانیِ بعد از ۳۱۱/۹۹ عبارت است از ۳۳۳/۱۰۶، از مسألهٔ ۶۶.۹ نتیجه می‌شود که ۳۱۱/۹۹ بهترین تقریب π در میان تمام اعداد گویا با مخرجِ نابیشتر از ۱۰۰ است.

توضیح. چون $a_2 = ۱۵$، مقدار بحرانیِ وسط $t = a_k/۲$ برای بررسی جداگانه وجود ندارد. (مسألهٔ بعد را ببینید.)

۷۰.۹ اگر r/s بهتر از ۳۵۵/۱۱۳ عدد π را تقریب بزند، ثابت کنید $s \geq ۱۶۶۰۴$. (با مسأله ۵۶.۹ مقایسه کنید.) لذا، ۳۵۵/۱۱۳ بهترین تقریب π در میان تمام اعداد گویا با مخرجِ نابیشتر از ۱۶۶۰۳ است. (راهنمایی: مسائل ۶۶.۹، ۶۷.۹ و ۱۵.۹ را به‌کار برید.)

حل. بنابر مسألهٔ ۶۶.۹، یک تقریب بهتر از $p_3/q_3 = ۳۵۵/۱۱۳$ برای π بایستی یا یک همگرا یا یک همگرای میانی باشد. از آنجا که همگرای بعد از ۳۵۵/۱۱۳ برای π عبارت است از $p_4/q_4 = ۱۰۳۹۹۳/۳۲۱۰۲$ ((۳۸.۹) را ببینید)، بایستی به همگراهای میانیِ بین ۳۳۳/۱۰۶ و ۱۰۳۹۹۳/۳۳۱۰۲، یعنی، اعداد گویای به‌صورت $(۳۵۵t + ۱۱۳)/(۱۰۶t + ۳۳۳)$، که $۲۹۱ \geq t \geq ۱$ مراجعه کنیم. بر طبق مسألهٔ ۶۷.۹، همگراهای میانی به‌ازای $۲۹۱ \geq t \geq ۱۴۷$ (به‌ترتیب) تقریبهای بهتری از ۳۵۵/۱۱۳ هستند. اما چون ۲۹۲ زوج است، همگرای میانیِ مربوط به $t = ۱۴۶$ بایستی با تعیین برقراری یا عدم برقراری $\langle ۲۹۲, ۱, ۱, ۱, \ldots \rangle < \langle ۲۹۲, ۱, ۱۵, ۷ \rangle$، جداگانه بررسی شود. (جدول مربوط به مسألهٔ ۵۷.۹ را ببینید.) بنابر مسألهٔ ۱۵.۹، این نابرابری برقرار است (در اینجا، n زوج و $۱ < ۱۵$)، و لذا نتیجه می‌گیریم که بهترین تقریب π بعد از ۳۵۵/۱۱۳ همگرای میانی $p_{۴۱۴۶}/q_{۴۱۴۶} = ۵۲۱۶۳/۱۶۶۰۴$ است.

تمرینهایی برای فصل ۹

۱. با استفاده از کسرهای مسلسل جوابی از معادله‌های زیر پیدا کنید:

(الف) $۱۳۶x + ۴۹y = ۱$؛

(ب) $۲۴۷x - ۷۷۶y = -۲$؛

۲. با استفاده از کسرهای مسلسل جوابی از معادلات زیر را به‌دست آورید.

(الف) $۷۹x + ۲۱۲y = -۳$،

(ب) $-۸۵x + ۱۹y = ۷$.

۳. بسطهای کسر مسلسل سادهٔ ۳۹۷/۱۲۱ و $-۷/۲۲$ را تعیین کنید.

۴. بسطهای کسر مسلسل اعداد گویای ۳,۰۹ و ۱۱۵٫۹ را پیدا کنید.

۵. کسر مسلسل $\langle ۱, ۲, ۳, ۴, ۵, ۶ \rangle$ نمایشگر چه عدد گویایی است؟

۶. اعداد گویایی را که توسط کسرهای مسلسل سادهٔ زیر نمایش داده شده‌اند تعیین کنید:

(الف) $\langle ۴, ۱, ۲, ۱, ۳ \rangle$، (ب) $\langle ۱, ۲, ۳, ۴, -۵ \rangle$.

۷. همگراهای کسر مسلسل متناهی $\langle ۱, ۲, ۱, ۷, ۱, ۶, ۳ \rangle$ را بیابید.

۸. همگراهای $\langle ۹, ۴, ۱, ۵, -۲ \rangle$ را محاسبه کنید.

۹. نخستین چهار همگرای بسط کسر مسلسل ۲٫۰۸۶۷ را به‌دست آورید.

۱۰. اعداد ۷۳۹/۳۴ و $-۷۳۹/۳۴$ را به‌صورت کسرهای مسلسل سادهٔ متناهی بیان کنید.

۱۱. بسط کسر مسلسل سادهٔ اعداد زیر را به‌دست آورید: (الف) $\sqrt{۹۸}$؛ (ب) $۲/(\sqrt{۵}+۱)$؛ (ج) $۵/(\sqrt{۱۱}+۱۲)$.

۱۲. نخستین شش خارج‌قسمت جزئی بسط کسر مسلسل نامتناهی اعداد زیر را پیدا کنید: (الف) $\sqrt[۳]{۲}$، (ب) e، (ج) $\pi^۲$.

۱۳. نخستین شش همگرای بسط کسر مسلسل نامتناهی اعداد (الف) e، (ب) $\pi^۲$ را به‌دست آورید.

۱۴. در هر یک از موارد زیر تعیین کنید که مقدار کسر مسلسل اول بزرگتر از مقدار کسر مسلسل دوم هست یا نه:

(الف) $\langle ۶, ۷, ۵, ۱, ۳ \rangle$، $\langle ۶, ۷, ۳, ۱, ۵ \rangle$؛

(ب) $\langle ۸, ۳, ۱, ۷, ۴ \rangle$، $\langle ۸, ۳, ۱, ۴, ۷, \ldots \rangle$؛

(ج) $\langle ۴, ۳, ۷, ۹, ۶, \ldots \rangle$، $\langle ۴, ۳, ۷, ۹ \rangle$؛

(د) $\langle ۱۱, ۷, ۵, ۶۳ \rangle$، $\langle ۱۱, ۷, ۴, \ldots \rangle$.

(ه) $\langle ۵, ۱۹, ۴۵, ۳۸, \ldots \rangle$، $\langle ۵, ۱۹, ۴۵ \rangle$.

۱۵. محاسبه کنید (الف) $\langle \overline{۱, ۲, ۱} \rangle$؛ (ب) $\langle ۱, \overline{۲, ۱, ۵} \rangle$؛ (ج) $\langle \overline{۵, ۴} \rangle$.

۱۶. بسط کسر مسلسل $\sqrt{۳۱۱}$ را پیدا کنید.

۱۷. ثابت کنید $\sqrt{۹n^۲+۶} = \langle ۳n, \overline{n, ۶n}\rangle$.

۱۸. تعیین کنید کدام‌یک از اعداد زیر بسط کسر مسلسل دوره‌ای محض دارند: (الف) $\sqrt{۱۱}/۳+۱)$، (ب) $۲/(\sqrt{۶}+۲)$، (ج) $۳/(۷+\sqrt{۱۰۱})$.

۱۹. (الف) با تشکیل جدولی برای r_k و s_k بسط کسر مسلسل $\sqrt{۳}-۳$ را بیابید.

(ب) قسمت (الف) را برای بیان $\langle \overline{۱, ۲}\rangle$ به‌صورت گنگ درجه دوم به‌کار برید.

۲۰. عدد گنگی را که بسط کسر مسلسل آن $\langle ۱, \overline{۲, ۳}\rangle$ است بیابید.

۲۱. مقدار کسر مسلسل دوره‌ای $\langle ۱, ۱, \overline{۳, ۵, ۷}\rangle$ را تعیین کنید.

۲۲. (الف) با تشکیل جدولی برای r_k، s_k، و a_k بسط کسر مسلسل $۲/(\sqrt{۱۰}-۳)$ را محاسبه کنید.

(ب) از قسمت (الف) برای بیان $\langle \overline{۱۲, ۳}\rangle$ به‌صورت یک عدد گنگ درجه دوم استفاده کنید.

۲۳. (الف) با تشکیل جدولی برای r_k و s_k بسط کسر مسلسل نامتناهی $\sqrt{۲۱}+۲)/۳$ را پیدا کنید.

(ب) از جدول قسمت (الف) برای تعیین کسر مسلسل $۴/(\sqrt{۱۸۹}+۱۳)$ استفاده کنید.

۲۴. بهترین تقریب گویای $\sqrt{۲}$ را در میان تمام اعداد گویایی که مخرجشان از ۹۸۵ تجاوز نمی‌کنند پیدا کنید.

۲۵. بهترین تقریب گویا برای $\sqrt[۳]{۲}$ با مخرج نابیشتر از ۵۰ به‌دست آورید.

۲۶. بهترین تقریب گویا برای e با مخرج کمتر از ۸ چیست؟

۲۷. بهترین تقریب برای $\sqrt[۳]{۹}$ را در میان تمام اعداد گویایی که مخرجشان از (الف) ۴۸۷؛ (ب) از ۳۰۰ تجاوز نمی‌کنند پیدا کنید. (راهنمایی: برای (ب) به همگراهای میانی مراجعه کنید.)

۲۸. بهترین تقریب گویا با مخرج نابیشتر از ۱۰۰ برای $\sqrt{۲}$ چیست؟

۲۹. عدد گویای ۹۶۱/۴۶۲ یک همگرای $\sqrt[۳]{۹}$ است. آیا نتیجه می‌شود که

$$|\sqrt[۳]{۹} - ۹۶۱/۴۶۲| < ۱/(۲ \times ۴۶۲^۲)?$$

۳۰. بدون محاسبهٔ بسط کسر مسلسل $\sqrt[۳]{۵۰}$، ثابت کنید که ۷۰/۱۹ یک همگراست.

۳۱. (الف) نخستین پنج خارج‌قسمت جزئی بسط کسر مسلسل π ۲ را محاسبه کنید.

(ب) بهترین تقریب گویای π ۲ با مخرج نابیشتر از ۷ چیست؟ با مخرج نابیشتر از ۵۳ چیست؟

۳۲. بدون محاسبهٔ بسط کسر مسلسل $\alpha = (۱+\sqrt{۳})/۲$، معین کنید که ۱۵۳/۱۱۲ و ۵۷۱/۴۱۸ دو همگرای متوالی α هستند یا نه.

۳۳. بهترین تقریب گویای π با مخرج نابیشتر از ۲۵۰۰۰ را پیدا کنید.

۳۴. با استفاده از قضیه‌ای از تقریبها ثابت کنید ۵۲/۲۵ همگرایی از $\sqrt[3]{9}$ است.

۳۵. فرض می‌کنیم $52/25 < a/b < \sqrt[3]{9}$، که در آن a و b اعداد صحیح مثبت هستند. ثابت کنید $b > 462$.

۳۶. فرض می‌کنیم $\sqrt{41} = \langle b, \overline{2, 2, 12} \rangle$. با استفاده از قضیه‌ای از تقریبها تمام اعداد گویای a/b با ساده‌ترین صورت را بیابید (در صورت وجود) به‌طوری که $50 < b < 250$ و $|\sqrt{41} - a/b| < 1/3b^2$.

ملاحظاتی برای فصل ۹

۱. بسیاری از فرمولهای اساسی این فصل بر اویلر معلوم بوده‌اند، اما اساساً تمام نظریه را لاگرانژ بسط داده است. به‌ویژه، لاگرانژ ثابت کرده است که تمام اعداد گنگ درجهٔ دوم بسط کسر مسلسل دوره‌یی دارند. او همچنین تقریب اعداد حقیقی به‌وسیلهٔ کسرهای مسلسل، از جمله ویژگیهای همگراهای میانی را بررسی کرده است.

۲. بین کسرهای مسلسل و الگوریتم اقلیدسی ارتباط نزدیکی وجود دارد. به‌ویژه، الگوریتم اقلیدسی منبسط، که به اختصار در توضیح بعد از (۲۳.۱) ذکر شده، اساساً عین روند بازگشتی برای محاسبهٔ همگراهای اعداد گویای a/b است (۱۰.۹ را ببینید). تنها تفاوتهای جزئی قراردادی وجود دارند؛ تغییر علامتها، که در (۱۰.۹) روشن است، در بیان معمولی الگوریتم اقلیدسی منبسط نهفته است. الگوریتم اقلیدسی منبسط، یا، هم‌ارز با آن، الگوریتم محاسبهٔ p_k و q_k، شیوهٔ بسیار مؤثری برای بیان بزرگترین مقسوم‌علیه مشترک a و b به‌صورت یک ترکیب خطی از a و b به‌دست می‌دهد. کاربرد این شیوه در رایانه یا حسابگرهای قابل برنامه‌ریزی آسان است و در محاسبات با دست نیز به‌خوبی کارایی دارد. برای محاسبهٔ با دست، بهتر آن است که جدولی مانند جدولِ مثالِ ۶.۹ ترتیب داد. برای اعداد کوچکِ a و b، شیوهٔ جایگزینی پَسرو که بعد از (۲۳.۱) بیان شده است شاید طبیعی‌تر باشد.

اگر α عدد گنگی باشد، می‌توان شیوهٔ محاسبهٔ خارج‌قسمتهای جزئی a_0، a_1، ... را به‌عنوان نوعی الگوریتم اقلیدسی در نظر گرفت. فرض می‌کنیم $x, y > 0$ دو عدد حقیقی باشند، و فرض می‌کنیم z کوچکترین عدد حقیقی مثبت به‌صورت $x - ny$ باشد، که n اعداد صحیح را اختیار می‌کند. در این‌صورت، به‌ازای عدد صحیحی مانند q، $x = qy + z$، و به آسانی دیده می‌شود که $q = [x/y]$. در قیاس با اعداد صحیح، وقتی x به y تقسیم شود q را خارج‌قسمت و z را باقیمانده خوانیم. با این مفهوم خارج‌قسمت و باقیمانده، الگوریتم اقلیدسی معمولی را در مورد اعداد α و ۱ به‌کار می‌بریم. به آسانی دیده می‌شود که «خارج‌قسمتهای» متوالی که به‌دست می‌آوریم

دقیقاً همان خارج‌قسمتهای جزئی a_0، a_1، ... در بسط کسر مسلسل α هستند.

یک روش هندسی تقریباً مربوط در مقالهٔ x از اصول اقلیدس برای اثبات برابری نسبتها به‌کار رفته است. ریاضیدانان یونانی حتی اصطلاحات فنی استاندارد، *anthypharesis* و *antanairesis*، را برای تعمیم الگوریتم اقلیدسی داشتند. اگر الگوریتم را برای قطر و ضلع یک مربع به‌کار بریم (یعنی، بسط کسر مسلسل $\sqrt{2}$ را پیدا کنیم)، آنگاه دوره‌یی بودن را کاملاً سریع مشاهده می‌کنیم. می‌توان این مطلب را به‌یک اثبات هندسی زیبا از گنگ بودن $\sqrt{2}$ تبدیل کرد. همواره این گمان وجود داشته است که این موضوع بر ریاضیدانان یونانی قرن چهارم قبل از میلاد معلوم بوده است.

اگر الگوریتم اقلیدسی منبسط برای اعداد حقیقی a و b، که b/a گنگ است (مثلاً، $a = 1$ و $b = \alpha$)، به‌کار گرفته شود، می‌توانیم باقیمانده‌های متوالی را به‌صورت $r_n = ax_n + by_n$ بیان کنیم. حد دنبالهٔ $\{r_n\}$ صفر است، و لذا دنبالهٔ $\{-x_n/y_n\}$ همگرا به b/a است. این یک روش ابتدایی برای به‌دست آوردن تقریبهای گویای b/a است، تکنیکی که اساساً باروشی که کسرهای مسلسل را به‌کار می‌برد هم‌ارز است.

۳. قضیهٔ (۲۸.۹) توصیف کاملی از بسط کسر مسلسل گنگهای درجه دوم، یعنی، اعداد گنگی که ریشه‌های چندجمله‌یی با ضرایب صحیح هستند، به ما می‌دهد. ولی، هیچ چنین توصیفی برای اعداد حقیقی (بجز اعداد گویا و گنگهای درجه دوم) که ریشه‌های چندجمله‌ییهای از درجهٔ بالاتر از دو هستند، شناخته شده نیست. در واقع، بسط کسر مسلسل برای هر عدد جبری از درجهٔ بالا ناشناخته است. مثلاً، حتی نمی‌دانیم که خارج‌قسمتهای جزئی $\sqrt[3]{2}$ کراندار هستند یا نیستند.

بعکس، بسط کسر مسلسل بعضی از اعداد متعالی معلوم است. شاید جالبترین آنها را در ۱۷۳۷ اویلر به‌دست آورده است. فرض می‌کنیم e پایهٔ لگاریتم طبیعی باشد. در این‌صورت

$$e-1 = \langle 1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots \rangle \quad \text{و} \quad \frac{e+1}{e-1} = \langle 2, 6, 10, 14, \ldots \rangle$$

۴. سری نامتناهی زیر را در نظر می‌گیریم

$$\frac{p_0}{q_0} + \left(\frac{p_1}{q_1} - \frac{p_0}{q_0}\right) + \left(\frac{p_2}{q_2} - \frac{p_1}{q_1}\right) + \cdots + \left(\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right) + \cdots,$$

که در آن p_k/q_k معرف همگرای kام عدد گنگ α است. با توجه به (۹.۹)، جمله‌های این سری (از جملهٔ دوم به بعد) یک در میان مثبت و منفی هستند. به‌ازای $k \geq 0$، فرض کنیم $b_0 = p_0/q_0 = [\alpha]$ و $b_{k+1} = p_{k+1}/q_{k+1} - p_k/q_k$؛ از (۷.۹) نتیجه می‌شود که $b_{k+1} = (-1)^k/q_k q_{k+1}$، و چون $q_k \geq k$، دنبالهٔ $(|b_k|)$، بعد از جملهٔ اول، نزولی و همگرا به 0 است.

از این‌رو $\sum_{k=0}^{\infty} b_k$ یک سری متناوب است که nامین مجموع جزئی آن $s_n = b_0 + b_1 + \cdots + b_n$ به روشنی برابر p_n/q_n است. لذا مجموع این سری نامتناهی، بنا به تعریف، برابر $\lim_{n\to\infty}(p_n/q_n)$، یعنی α است ((۱۳.۹) را ببینید). بنابراین داریم

$$\alpha = [\alpha] + \sum_{k=0}^{\infty} \frac{(-1)^k}{q_k q_{k+1}} = [\alpha] + \frac{1}{q_0 q_1} - \frac{1}{q_1 q_2} + \frac{1}{q_2 q_3} - \cdots$$

بجاست خاطرنشان کنیم که این عبارت برای α تنها به مقادیر q_k بستگی دارد و نه به مقادیر p_k. از این‌رو هر همگرای α را می‌توان تنها با استفاده از $[\alpha]$ و دنبالهٔ $\{q_k\}$ به‌دست آورد:

$$\frac{p_n}{q_n} = s_n = [\alpha] + \sum_{k=0}^{n-1} \frac{(-1)^k}{q_k q_{k+1}}.$$

با توجه به قضیه‌های مربوط به سریهای متناوب، به آسانی می‌توان ویژگیهای زیر را برای بسط کسر مسلسل α به‌دست آورد:

(i) زیردنبالهٔ $\{s_{2n}\}$ صعودی اکید و زیردنبالهٔ $\{s_{2n+1}\}$ نزول اکید و هر دو همگرا به α هستند؛ برحسب کسرهای مسلسل، همگراهای با اندیس زوج کمتر از α هستند و متوالیاً به α نزدیکتر می‌شوند، و همگراهای با اندیس فرد بزرگتر از α هستند و متوالیاً به α نزدیکتر می‌شوند ((۹.۹) و (۱۲.۹) را ببینید).

(ii) $|b_{n+2}| < |\alpha - s_n| < |b_{n+1}|$؛ برحسب همگراها، $|\alpha - p_n/q_n| < 1/q_n q_{n+1}$ (که همان (۳۳.۹) است)، و $|\alpha - p_{n+1}/q_{n+1}| < |\alpha - p_n/q_n|$، یعنی، همگراهای α متوالیاً به α نزدیکتر می‌شوند ((۳۴.۹) را ببینید).

وقتی α گویا باشد بحث بالا (با تغییرات جزئی) نیز به‌خوبی به‌کار می‌رود.

شرح مختصری از زندگینامه

ژوزف لویی لاگرانژ در ۱۷۳۶ در ایتالیا به دنیا آمد و ریاضیات را در دانشگاه تورن (تورینو)[1] فرا گرفت. بر اثر مساهمت اساسی در آنالیز، حساب تغییرات، نظریهٔ معادلات دیفرانسیل، و مکانیک، به سرعت مشهور شد. در ۱۷۶۶، وقتی که اویلر برلین را به قصد سن‌پترزبورگ ترک کرد، لاگرانژ شغل خود را در مدرسهٔ سلطنتی توپخانه در تورن رها کرد تا تصدی ریاست بخش ریاضی آکادمی برلین را به عهده بگیرد. (زمانی که اویلر برلین را ترک گفت. فردریک کبیر به لاگرانژ نوشت که «بزرگترین پادشاه اروپا» میل دارد که «بزرگترین ریاضیدان اروپا» را در دربار خود داشته باشد.ـم.) بعد از

1. Turin

وفات اویلر در ۱۷۸۳، لاگرانژ بزرگترین ریاضیدان اروپا به‌شمار می‌آمد. در ۱۷۸۷، دعوت لویی شانزدهم را برای پیوستن به آکادمی فرانسه پذیرفت.

لاگرانژ کارهای مهمی در بسیاری از سطوح ریاضی انجام داد، قابل توجه‌ترین آنها در مکانیک، جبر، و نظریهٔ اعداد است. بیشتر کارهای لاگرانژ در نظریه اعداد در خلال نیمهٔ اول اقامتش در برلین، از ۱۷۶۶ تا ۱۷۷۷، انجام گرفت. تحقیقات وی در نظریهٔ اعداد از جمله انتشار اولین اثبات قضیهٔ ویلسن و اثبات این مطلب است که هر عدد صحیح مثبت را می‌توان به‌صورت مجموع چهار مربع نمایش داد. (این قضیه را باشه و فرما حدس زده بودند و حرکت به سمت یک اثبات توسط اویلر انجام شده بود.) لاگرانژ نظریهٔ مقدماتی کسرهای مسلسل را بسط داد و از آن برای اثبات وجود جواب برای معادلهٔ پِل استفاده کرد. گذشته از آن لاگرانژ کارهای مهمی در تجزیهٔ صورتهای درجهٔ دوم انجام داد. تحقیقاتش در جبر شامل قضیه‌هایی در نظریهٔ معادلات، نظریهٔ گروهها، و نظریهٔ همنهشتیهای چندجمله‌یی است.

در دوران پُر آشوب انقلاب فرانسه لاگرانژ هیچ کار ریاضی انجام نداد. در ۱۷۹۳ ریاست کمیسیون مأمور اصلاح اوزان و مقیاسهای فرانسه به وی واگذار شد، و لاگرانژ معمار بزرگ دستگاه متریک به‌شمار می‌آید. ناپلئون مقام سناتوری امپراتوری را به وی اعطا کرد. (ناپلئون ارزیابی خود از لاگرانژ را در این جمله خلاصه کرده است «لاگرانژ برج رفیع علوم ریاضی است.ـم.»)

لاگرانژ در ۱۸۱۳ بدرود حیات گفت و در آرامگاه ویژهٔ مردان نامی، پانتئون، به خاک سپرده شد.

مراجع

Claude Brezinski, *History of Continued Fractions and Padé Approximants*, Springer-Verlag, New York, 1991.

این تاریخ نه تنها در کاربرد کسرهای مسلسل در نظریهٔ اعداد بحث می‌کند، بلکه بسیاری از کاربردهای آن را در معادلات دیفرانسیل، نظریهٔ احتمال، و تقریب توابع نیز مورد رسیدگی قرار می‌دهد. کتاب به تفصیل از منابعی نقل می‌کند که پیدا کردن آنها جز، در این کتاب مشکل است، و دارای کتابنامه‌ای چشمگیر است.

C. D. Olds, *Continued Fractions*, Random House, New York, 1963.

این یک کتاب قویاً خواندنی است، که با سبکی روان نوشته شده و دارای مثالهای عددی تفصیلی فراوان است، اغلب مطالب مهم این فصل، و یک بحث اساسی از معادلهٔ پل را در بردارد. کسرهای مسلسل قابل فهمترین کتاب در این زمینه به زبان انگلیسی است و به‌عنوان مکملی برای این عرضهٔ فشردهٔ ما به‌شدت توصیه می‌شود.

۱۰

معادلهٔ پِل

همان‌گونه که در فصل قبل اشاره شد، یافتن تقریب گویای خوب برای یک عدد گنگ ارتباط نزدیکی با بسط کسر مسلسل آن عدد گنگ دارد. حدود ۴۰۰ سال ق. م.، ریاضیدانان هندی و یونانی تقریبهای ۱۷/۱۲ و ۵۷۷/۴۰۸ را برای $\sqrt{۲}$ به‌دست دادند. (این اعداد، به‌ترتیب، همگراهای سوم و چهارمِ بسط کسر مسلسل $\sqrt{۲}$ هستند.) در سدهٔ سوم ق. م.، ارشمیدس $\sqrt{۳}$ را با ۲۶۵/۱۵۳ (همگرای هشتم) و ۱۳۵۱/۷۸۰ (همگرای یازدهم) تقریب زد.

مسألهٔ یافتن تقریبهای گویا برای $\sqrt{d}$، که در آن d عدد صحیح مثبتی است که مربع کامل نیست، به‌طور طبیعی به معادلهٔ دیوفانتی $x^۲ - dy^۲ = ۱$ منجر می‌شود، زیرا اگر جفت (x, y) جوابی از این معادله با $y \neq ۰$ باشد، آنگاه $(x/y)^۲ = d + ۱/y^۲$، و لذا وقتی y بزرگ باشد، x/y تقریب خوبی برای $\sqrt{d}$ است. (تئونِ[1] ازمیری ریاضیدان یونانی سدهٔ دوم، توانست جوابهای معادلهٔ $x^۲ - xy^۲ = \pm ۱$ را با استفاده از یک رابطهٔ بازگشتی تولید کند.) شاید به دلیل یک

1. Thon of Smyrna

ارجاع نادرستِ اویلر، معادلهٔ $x^۲ - dy^۲ = ۱$ به معادلهٔ پل معروف شده است، با اینکه، جان پل[1] (۱۶۸۵ـ۱۶۱۱) ریاضیدان انگلیسی چندان در این مسأله کار نکرده بوده است. یکی از قدیمی‌ترین و مشهورترین جای پیدایش معادلهٔ پل در مسألهٔ گلهٔ ارشمیدس است، که به معادلهٔ $x^۲ - ۴۷۲۹۴۹۴y^۲ = ۱$ منجر می‌شود. کوچکترین جواب مثبت که در ۱۸۸۰ پیدا شد، مقدار y آن ۴۱ رقم دارد.

یک بررسی مفصل از معادلهٔ پل در کارهای ریاضیدانان هندی برهمگوپته (سدهٔ هفتم) و بهاسکره (سدهٔ دوازدهم) دیده می‌شود. نخستین ریاضیدان اروپایی که یک تحقیق جدی از معادلهٔ پل به عمل آورد فرما بود. فرما در ۱۶۵۷، جان والیس[2] (۱۷۰۳ـ۱۶۱۶)، یکی از برجسته‌ترین ریاضیدانان انگلیسی پیش از آیزک نیوتن و لرد ویلیام برونکر[3] (۱۶۸۴ـ۱۶۲۰) پشتیبان والیس را برای حل معادلات $x^۲ - ۶۱y^۲ = ۱$ و $x^۲ - ۱۰۹y^۲ = ۱$ به مبارزه طلبید. در پاسخ به فرما، برونکر یک روش بسیار کارآمد برای حل معادلهٔ پل ارائه داد، که در مورد $x^۲ - ۱۰۹y^۲ = ۱$، جوابی که مقدار x آن ۱۵ رقم دارد، به‌دست می‌دهد. همان‌گونه که اویلر در ۱۷۵۹ متوجه شد، روش برونکر مشابه الگوریتم تعیین بسط کسر مسلسل $\sqrt{d}$ است. (در واقع، یک روند اساساً هم‌ارز، حدود پنج سده جلوتر، در کارهای بهاسکره دیده می‌شود.) اویلر بسط کسر مسلسل $\sqrt{d}$ را برای یافتن کوچکترین جواب مثبت $x^۲ - dy^۲ = ۱$ به‌کار برد و نشان داد که چگونه می‌توان جوابهای دیگر را از یک جواب مفروض با یک رابطهٔ بازگشتی تولید کرد.

والیس و فرما هر دو حدس زدند، و به درست، که معادلهٔ پل جواب دارد، در واقع بی‌نهایت جواب دارد. در ۱۷۶۸، لاگرانژ نخستین اثبات کامل این قضیه را به چاپ رساند و نشان داد که جوابها از بسط کسر مسلسل $\sqrt{d}$ به‌دست می‌آیند. هر چند که اویلر یک دهه جلوتر این ارتباط را دریافته بود، ولی لاگرانژ نخستین کسی بود که با استفاده از کسرهای مسلسل، در یک سری از سه مقاله که از ۱۷۶۸ تا ۱۷۷۰ به آکادمی برلین ارائه شدند، یک بررسی دقیق از معادلهٔ پل به عمل آورد.

قضیه‌هایی برای فصل ۱۰

معادلهٔ پل $x^۲ - dy^۲ = ۱$

در سرتاسر این فصل، d معرّف یک عدد صحیح مثبت است که مربع کامل نیست. همان‌گونه که پیش از این ملاحظه شد، تکنیک به‌کار رفته برای حل $x^۲ - dy^۲ = ۱$ توسط بهاسکره، برونکر، و لاگرانژ با روش تعیین بسط کسر مسلسل $\sqrt{d}$ هم‌ارز است. در این بخش نشان خواهیم داد که به‌ازای

1. John Pell 2. John Wallis 3. William Brouncker

هر انتخاب d معادلهٔ پل بی‌نهایت جواب صحیح دارد، که تمام جوابهای مثبت در میان همگراهای $\sqrt{d}$ یافت می‌شوند، و می‌توان تمام جوابهای مثبت را مستقیماً از کوچکترین جواب مثبت تولید کرد.

بنابر (۳۱.۹)، یک عدد گنگ درجهٔ دوم α دارای یک کسر مسلسل دوره‌یی محض است اگر و تنها اگر α ساده شده باشد، یعنی، اگر $\alpha > ۱$ و مزدوجش α' در $-۱ < \alpha' < ۰$ صدق کند. گرچه $\sqrt{d}$ ساده‌شده نیست، به آسانی بررسی می‌شود که گنگ درجهٔ دوم $[\sqrt{d}] + \sqrt{d}$ ساده شده است. (به‌وضوح دیده می‌شود که مزدوجش $\sqrt{d} - [\sqrt{d}]$ است.) می‌توان این مطلب را برای بیان بسط کسر مسلسل $\sqrt{d}$ به‌کار برد.

(۱.۱۰) قضیه. بسط کسر مسلسل $\sqrt{d}$ به‌صورت

$$\langle a_۰ \overline{a_۱, a_۲, a_۳, \ldots, a_۳, a_۲, a_۱, ۲a_۰} \rangle$$

است که $a_۰ = [\sqrt{d}]$.

برهان. فرض کنیم $a_۰ = [\sqrt{d}]$. اگر $\alpha = [\sqrt{d}] + \sqrt{d}$، آنگاه α یک بسط دوره‌یی محض دارد، و اولین خارج‌قسمت جزئی آن با $[\alpha] = ۲[\sqrt{d}] = ۲a_۰$ برابر است، لذا

$$\begin{aligned} \alpha = [\sqrt{d}] + \sqrt{d} &= \langle \overline{۲a_۰, a_۱, a_۲, \ldots, a_n} \rangle \\ &= \langle ۲a_۰, a_۱, a_۲, \ldots, a_n, \overline{۲a_۰, a_۱, a_۲, \ldots, a_n} \rangle \end{aligned}$$

بنابراین اگر $[\sqrt{d}] = a_۰$ را از دو طرف کم کنیم، داریم

$$\sqrt{d} = \langle a_۰, \overline{a_۱, a_۲, \ldots, a_n, ۲a_۰} \rangle .$$

سرانجام، نشان می‌دهیم که خارج‌قسمتهای جزئی $a_۱$، $a_۲$، ...، a_n «متقارن»اند، یعنی، $a_۱ = a_n$، $a_۲ = a_{n-۱}$، ...، $a_n = a_۱$. بنابر (۳۱.۹)، داریم

$$-۱/\alpha' = \frac{۱}{\sqrt{d} - [\sqrt{d}]} = \langle \overline{a_n, a_{n-۱}, \ldots, a_۲, a_۱, ۲a_۰} \rangle .$$

همچنین آشکار است که $\sqrt{d} - [\sqrt{d}] = \langle ۰, \overline{a_۱, a_۲, \ldots, a_n, ۲a_۰} \rangle$، که از آن به آسانی $۱/(\sqrt{d} - [\sqrt{d}]) = \langle \overline{a_۱, a_۲, \ldots, a_n, ۲a_۰} \rangle$ نتیجه می‌شود. بنابراین

$$\langle \overline{a_۱, a_۲, \ldots, a_n, ۲a_۰} \rangle = \langle \overline{a_n, a_{n-۱}, \ldots, a_۲, a_۱, ۲a_۰} \rangle$$

و از این‌رو $a_۱ = a_n$، $a_۲ = a_{n-۱}$، ....

توضیح. ۱. دورهٔ $\sqrt{d}$ بعد از اولین جمله شروع می‌شود، و خارج‌قسمتهای جزئی (بجز اولی و آخری) یک دنبالهٔ متقارن تشکیل می‌دهند به‌طوری که درونی‌ترین جمله دقیقاً وقتی تکرار می‌شود که طول دوره فرد باشد. مثلاً $\sqrt{۲۹} = \langle ۵, \overline{۲, ۱, ۱, ۲, ۱۰} \rangle$ و $\sqrt{۳۳} = \langle ۵, \overline{۱, ۲, ۱, ۱۰} \rangle$.

۲. تنها خارج‌قسمتهای جزئی $\sqrt{d}$ که با $۲a_۰ = ۲[\sqrt{d}]$ برابرند جمله‌های آخر در یک دوره هستند. (مسألهٔ ۶.۱۰ را ببینید.) لذا وقتی بسط کسر مسلسل $\sqrt{۲۹}$ را محاسبه کنیم، تا جایی به محاسبهٔ خارج‌قسمتهای جزئی a_i نیاز داریم که به مقدار $۲a_۰ = ۲[\sqrt{۲۹}] = ۱۰$ برسیم.

۳. به‌ازای بعضی از مقادیر صحیح مثبت d یک کسر مسلسل به‌صورت $\langle a_۰, \overline{a_۱, a_۲, \ldots, a_۲, a_۱, ۲a_۰} \rangle$ لزوماً بسط $\sqrt{d}$ نیست. ولی، هر کسر مسلسل به این صورت به‌ازای یک عدد گویای $r > ۱$ برابر $\sqrt{r}$ است. مثلاً $\sqrt{۱۳/۲} = \langle ۲, \overline{۱, ۱, ۴} \rangle$ و $\sqrt{۵۶/۳} = \langle ۴, \overline{۳, ۸} \rangle$. (مسألهٔ ۳.۱۰ را ببینید.)

برعکس، اگر $r > ۱$ گویا و r مربع یک عدد گویا نباشد، آنگاه $\sqrt{r}$ به‌صورت $\langle a_۰, \overline{a_۱, a_۲, \ldots, a_۲, a_۱, ۲a_۰} \rangle$ است. ($\sqrt{d}$ را به‌صورت $\sqrt{d}/s$ می‌نویسیم، و در برهان (۱.۱۰) $\sqrt{d}$ را با $\sqrt{d}/s$ جانشین می‌کنیم.)

اگر (r, s) و (u, v) با r، s، u، و v مثبت جوابهای $x^۲ - dy^۲ = ۱$ باشند، آنگاه $r < u$ اگر و تنها اگر $s < v$ (زیرا $u^۲ - r^۲ = d(v^۲ - s^۲)$). لذا اگر جوابهایی با اعداد صحیح مثبت وجود داشته باشند، آنگاه جوابی با کوچکترین مقدار مثبت x وجود دارد، در واقع، در (۶.۱۰) نشان خواهیم داد که $x^۲ - dy^۲ = ۱$ همواره جواب صحیح مثبت دارد.

(۲.۱۰) تعریف. یک جواب (u, v) از $x^۲ - dy^۲ = ۱$ مثبت است هرگاه $u > ۰$ و $v > ۰$. کوچکترین جواب مثبت، یا جواب اصلی، از $x^۲ - dy^۲ = ۱$ جواب مثبت $(x_۱, y_۱)$ است به‌طوری که به‌ازای هر جواب مثبتِ دیگر (u, v)، $x_۱ < u$ و $y_۱ < v$.

به‌طور کلی، اگر جوابهای مثبت به‌گونه‌ای مرتب شوند که مقادیر x (یا مقادیر y) یک دنبالهٔ صعودی تشکیل دهند، آنگاه دومین کوچکترین مقدار x دومین جواب مثبت را تعریف می‌کند، سومین کوچکترین مقدار x سومین جواب مثبت را، و مانند آن.

توضیح. برای مقادیر کوچک d، یک روش مناسب برای تعیین کوچکترین جواب مثبت $x^۲ - dy^۲ = ۱$ آزمون مقادیر مثبت متوالی y است تا اینکه کوچکترین مقداری که به‌ازای آن $dy^۲ + ۱$ مربع کامل شود به‌دست آید.

برای یافتن تمام جوابهای صحیح معادلهٔ پل، به‌وضوح کافی است که تنها جوابهای مثبت را در

نظر بگیریم. قضیهٔ بعد نشان می‌دهد که هر جواب مثبت $x^۲ - dy^۲ = ۱$ در میان همگراهای $\sqrt{d}$ یافت می‌شود.

(۳.۱۰) قضیه. فرض کنیم (p, q) یک جواب مثبت $x^۲ - dy^۲ = ۱$ باشد، در این‌صورت p/q یکی از همگراهای بسط کسر مسلسل $\sqrt{d}$ است.

برهان. می‌نویسیم $p - q\sqrt{d} = ۱/(p + q\sqrt{d})$؛ پس $p/q - \sqrt{d} = ۱/q(p + q\sqrt{d})$. چون روشن است که $p > q\sqrt{d}$، داریم $p + q\sqrt{d} > ۲q\sqrt{d}$، و لذا

$$۰ < \frac{p}{q} - \sqrt{d} < \frac{۱}{۲q^۲\sqrt{d}} < \frac{۱}{۲q^۲}.$$

لذا از (۳۹.۹) نتیجه می‌شود که p/q یک همگرای $\sqrt{d}$ است.

توضیح. اگر (p, q) یک جواب مثبت $x^۲ - dy^۲ = ۱$ باشد، آنگاه $p^۲ = dq^۲ + ۱$، و لذا $p/q > \sqrt{d}$. ازاین‌رو بنابر (۹.۹)، p/q یک همگرای شمارهٔ فرد $\sqrt{d}$ است.

عکس (۳.۱۰) برقرار نیست: هر همگرای $\sqrt{d}$ جوابی از $x^۲ - dy^۲ = ۱$ تولید نمی‌کند. کدام همگراها جواب ارائه می‌دهند؟ می‌توان پاسخ را برحسب طول دوره ارائه داد.

(۴.۱۰) لم. گیریم p_k/q_k همگرای kام $\sqrt{d}$ باشد، و فرض می‌کنیم r_k و s_k مانند (۲۴.۹) تعریف شوند. در این‌صورت، به‌ازای هر $k \geq ۰$،

$$\frac{p_k + q_k\sqrt{d}}{p_{k-۱} + q_{k-۱}\sqrt{d}} = \frac{r_{k+۱} + \sqrt{d}}{s_k}.$$

برهان. اثبات به استقرا، روی k. به‌ازای $k = ۰$ داریم $r_۰ = ۰$ و $s_۰ = ۱$، زیرا $\sqrt{d} = (۰ + \sqrt{d})/۱$؛ لذا $r_۱ = a_۰ s_۰ - r_۰ = a_۰$. بنابراین، طرف راست برابر $a_۰ + \sqrt{d}$، و طرف چپ برابر $(p_۰ + q_۰\sqrt{d})/(p_{-۱} + q_{-۱}\sqrt{d}) = a_۰ + \sqrt{d}$ است.

حال فرض کنیم حکم به‌ازای $k \geq ۰$ برقرار باشد. چون $p_{k+۱} = a_{k+۱}p_k + p_{k-۱}$ و $q_{k+۱} = a_{k+۱}q_k + q_{k-۱}$، در نتیجه

$$p_{k+۱} + q_{k+۱}\sqrt{d} = a_{k+۱}(p_k + q_k\sqrt{d}) + p_{k-۱} + q_{k-۱}\sqrt{d}.$$

با تقسیم دو طرف بر $p_k + q_k\sqrt{d}$ و بنابر فرض استقرا، داریم

$$\frac{p_{k+1} + q_{k+1}\sqrt{d}}{p_k + q_k\sqrt{d}} = a_{k+1} + \frac{p_{k-1} + q_{k-1}\sqrt{d}}{p_k + q_k\sqrt{d}} = a_{k+1} + \frac{s_k}{r_{k+1} + \sqrt{d}}$$

$$= a_{k+1} + s_k\frac{\sqrt{d} - r_{k+1}}{d - r_{k+1}^2} = a_{k+1} + \frac{\sqrt{d} - r_{k+1}}{s_{k+1}}$$

$$= \frac{a_{k+1}s_{k+1} - r_{k+1} + \sqrt{d}}{s_{k+1}} = \frac{r_{k+2} + \sqrt{d}}{s_{k+1}}$$

که حکم با $k+1$ به جای k است.

(۵.۱۰) قضیه. فرض کنیم بسط کسر مسلسل $\sqrt{d}$ دوره‌ای به طول m داشته باشد. اگر p_k/q_k همگرای kام $\sqrt{d}$ باشد، و r_k، s_k مانند (۲۴.۹) تعریف شوند، آنگاه

(i) به‌ازای هر $k \geq 0$، $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k s_k$؛

(ii) به‌ازای هر $k \geq 0$، $s_k > 0$؛

(iii) $s_k = 1$ اگر و تنها اگر $m|k$.

برهان. (i) با استفاده از لم قبل و مزدوج‌گیری، به‌ازای هر $i \geq 0$ داریم

$$\frac{p_i - q_i\sqrt{d}}{p_{i-1} - q_{i-1}\sqrt{d}} = \frac{r_{i+1} - \sqrt{d}}{s_i} \quad \text{و} \quad \frac{p_i + q_i\sqrt{d}}{p_{i-1} + q_{i-1}\sqrt{d}} = \frac{r_{i+1} + \sqrt{d}}{s_i}$$

اگر دو عبارت را در هم ضرب کنیم و $d - r_{i+1}^2 = s_i s_{i+1}$ را به‌کار بریم، داریم

$$\frac{p_i^2 - dq_i^2}{p_{i-1}^2 - dq_{i-1}^2} = -\frac{s_{i+1}}{s_i}.$$

اگر حاصلضرب عبارت بالا را از $i = 0$ تا $i = k-1$ در نظر بگیریم، پس از ساده کردن و استفاده از $p_{-1} = 1$، $q_{-1} = 0$، و $s_0 = 1$، عبارت $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k s_k$ را به‌دست می‌آوریم.

(ii) از (۹.۹) و تعریف کسر مسلسل نامتناهی نتیجه می‌شود که هر همگرای فرد $\sqrt{d}$ بزرگتر از $\sqrt{d}$ و هر همگرای زوج کوچکتر از $\sqrt{d}$ است. از این‌رو $(p_i^2 - dq_i^2)/(p_{i-1}^2 - dq_{i-1}^2)$ همواره منفی، و لذا s_{i+1}/s_i همواره مثبت است. چون $s_0 = 1$، در نتیجه به‌ازای هر $k \geq 0$، $s_k > 0$.

(iii) فرض کنیم m طول دورهٔ $\sqrt{d}$ باشد. بنابر (۱.۱۰)، بسط کسر مسلسل $\sqrt{d}$ به‌صورت زیر است

$$\sqrt{d} = \langle a_0, \overline{a_1, \dots, a_{m-1}, 2a_0} \rangle .$$

اگر α_k را مانند (۱۷.۹) تعریف کنیم، آنگاه

$$[\sqrt{d}] + \sqrt{d} = \alpha_m = \alpha_{2m} = \alpha_{3m} = \cdots .$$

بنابر (iii.۲۴.۹)، $\alpha_k = (r_k + \sqrt{d})/s_k$، و لذا به‌ازای هر $j \geq 1$، $s_{jm} = 1$.

حال، فرض می‌کنیم $k \geq 1$ وجود داشته باشد که $s_k = 1$. چون α_k دارای بسط کسر مسلسل دوره‌یی محض است، (۳۱.۹) ایجاب می‌کند که α_k ساده شده باشد، و لذا $-1 < \alpha'_k < 0$. اما $\alpha'_k = (r_k - \sqrt{d})/s_k = r_k - \sqrt{d}$، و لذا $0 < \sqrt{d} - r_k < 1$، یعنی، $r_k = [\sqrt{d}]$. از آنجا $\alpha_k = [\sqrt{d}] + \sqrt{d}$، و لذا k مضربی از دورهٔ $[\sqrt{d}] + \sqrt{d}$، یعنی، مضربی از m است. این، برهان را کامل می‌کند.

توضیحات. ۱. چون $\sqrt{d}$ بسط کسر مسلسل دوره‌یی دارد، خارج‌قسمتهای جزئی q_k بعد از $m+1$ جمله تکرار می‌شوند، که در آن m طول دورهٔ $\sqrt{d}$ است، و لذا اعداد r_k و s_k که در (۳۴.۹) تعریف شدند نیز بعد از $m+1$ جمله تکرار می‌شوند. (توضیح محاسبه‌یی بعد از (۲۴.۹) را ببینید.) لذا به‌ازای هر $i = 1, 2, 3, \dots$، $r_i = r_{m+i}$ و $s_i = s_{m+i}$.

۲. برای $\sqrt{d}$، اعداد صحیح r_k و s_k در نابرابریهای $0 < r_k < \sqrt{d}$ و $0 < s < k < 2\sqrt{d}$ صدق می‌کنند. (مسألهٔ ۱.۱۰ را ببینید.)

(۶.۱۰) قضیه. فرض می‌کنیم بسط کسر مسلسل $\sqrt{d}$ دوره‌یی به طول m داشته باشد.

(i) اگر m زوج باشد، تمام جوابهای مثبت $x^2 - dy^2 = 1$ عبارت‌اند از

$$x = p_{jm-1}, \qquad y = q_{jm-1}, \qquad j = 1, 2, 3, \dots$$

(ii) اگر m فرد باشد، تمام جوابهای مثبت $x^2 - dy^2 = 1$ عبارت‌اند از

$$x = p_{2jm-1}, \qquad y = q_{2jm-1}, \qquad j = 1, 2, 3, \dots$$

برهان. بنابر (۳.۱۰)، تمام جوابهای مثبت $x^2 - dy^2 = 1$ از یک همگرای $\sqrt{d}$ تولید می‌شوند. اگر (p_k, q_k) جواب مثبتی باشد، از (۵.۱۰) نتیجه می‌شود که k فرد است و $m | k+1$، پس $j \geq 1$ وجود دارد به‌طوری که $k = jm - 1$. اگر m زوج باشد، هر مقدار j قابل قبول است، حال آنکه اگر m فرد باشد، j زوج است.

(۷.۱۰) نتیجه. معادلهٔ $x^۲ - dy^۲ = ۱$ بی‌نهایت جواب صحیح مثبت دارد. اگر m طول دورهٔ $\sqrt{d}$ باشد، آنگاه جواب اصلی $(p_{m-۱}, q_{m-۱})$ است اگر m زوج و $(p_{۲m-۱}, q_{۲m-۱})$ است هرگاه m فرد باشد.

(۸.۱۰) مثال. برای یافتن جواب اصلی $x^۲ - ۲۹y^۲ = ۱$، ابتدا جدول زیر را برای یافتن کسر مسلسل $\sqrt{۲۹}$ تشکیل می‌دهیم:

k	۰	۱	۲	۳	۴	۵
r_k	۰	۵	۳	۲	۳	۵
s_k	۱	۴	۵	۵	۴	۱
a_k	۵	۲	۱	۱	۲	۱۰

لذا $\sqrt{۲۹} = \langle ۵, \overline{۲, ۱, ۱, ۲, ۱۰} \rangle$. در اینجا، طول دوره $m = ۵$ است، لذا بنابر (۷.۱۰)، جواب اصلی $(p_۹, q_۹)$ است. برای تعیین جواب اصلی، جدول زیر را می‌سازیم:

k	-۱	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹
a_k		۵	۲	۱	۱	۲	۱۰	۲	۱	۱	۲
p_k	۱	۵	۱۱	۱۶	۲۷	۷۰	۷۲۷	۱۵۲۴	۲۲۵۱	۳۷۷۵	۹۸۰۱
q_k	۰	۱	۲	۳	۵	۱۳	۱۳۵	۲۸۳	۴۱۸	۷۰۱	۱۸۲۰

لذا کوچکترین جواب مثبت $x^۲ - ۲qy^۲ = ۱$ برابر است با $x = p_۹ = ۹۸۰۱$، $y = q_۹ = ۱۸۲۰$.

اکنون به مسألهٔ یافتن جوابهای دیگر، وقتی که جواب اصلی معلوم است، باز می‌گردیم. در مثال بالا، بنابر (ii.۶.۱۰) جواب مثبت بعدی $(p_{۱۹}, q_{۱۹})$ است. می‌توانیم جدول را بسط دهیم و همگراهای دیگر را حساب کنیم تا به $p_{۱۹}$ و $q_{۱۹}$ برسیم، اما روش ساده‌تری برای یافتن جوابهای دیگر وجود دارد، که در (۱۰.۱۰) بیان خواهد شد، لم زیر را لازم داریم.

(۹.۱۰) لم. فرض می‌کنیم $(a_۱, b_۱)$ و $(a_۲, b_۲)$ جوابهای دلخواه (نه لزوماً مثبت) از $x^۲ - dy^۲ = ۱$ باشند. اعداد صحیح r و s را چنین تعریف می‌کنیم

$$(a_۱ + b_۱\sqrt{d})(a_۲ + b_۲\sqrt{d}) = r + s\sqrt{d}.$$

در این‌صورت، (r,s) نیز جوابی از $x^۲-dy^۲=۱$ است. اگر $(a_۱,b_۱)$ و $(a_۲,b_۲)$ جوابهای مثبت باشند، آنگاه (r,s) نیز جواب مثبت است.

برهان. به آسانی بررسی می‌شود که $r=a_۱a_۲+b_۱b_۲d$ و $s=a_۱b_۲+a_۲b_۱$؛ لذا $(a_۱-b_۱\sqrt{d})(a_۲-b_۲\sqrt{d})=r-s\sqrt{d}$. بنابراین

$$\begin{aligned} r^۲-ds^۲ &= (r+s\sqrt{d})(r-s\sqrt{d}) \\ &= (a_۱+b_۱\sqrt{d})(a_۲+b_۲\sqrt{d})(a_۱-b_۱\sqrt{d})(a_۲-b_۲\sqrt{d}) \\ &= (a_۱^۲-db_۱^۲)(a_۲^۲-db_۲^۲)=۱. \end{aligned}$$

توضیح. برهان بالا به آسانی برای ارائه یک قضیهٔ کلی‌تر قابل تعدیل است: اگر $(a_۱,b_۱)$ جوابی از $x^۲-dy^۲=M$ و $(a_۲,b_۲)$ جوابی از $x^۲-dy^۲=N$ باشد، آنگاه (r,s) جوابی از $x^۲-dy^۲=MN$ است. می‌توان این قضیه را از اتحاد برهمگوپته

$$(r^۲-ds^۲)(u^۲-dv^۲)=(ru\pm svd)^۲-d(rv\pm su)^۲,$$

به‌دست آورد. این اتحاد در سدهٔ هفتم در بررسی برهمگوپته از جوابهای $x^۲-dy^۲=N$ دیده می‌شود.

(۱۰.۱۰) قضیه. فرض کنیم $(x_۱,y_۱)$ جواب اصلی $x^۲-dy^۲=۱$ باشد. در این‌صورت تمام جوابهای مثبت با (x_n,y_n) ارائه می‌شوند، که در آن به‌ازای $n\geq ۱$ اعداد صحیح x_n و y_n با $x_n+y_n\sqrt{d}=(x_۱+y_۱\sqrt{d})^n$ تعریف می‌شوند. همچنین، (x_n,y_n) nامین جواب مثبت است (به معنی (۲.۱۰)).

برهان. از (۹.۱۰) نتیجه می‌شود که (x_n,y_n) یک جواب مثبت است. حال فرض کنیم (r,s) جواب مثبتی باشد. برای ساده کردن نمادگذاری، قرار می‌دهیم $\beta=r+s\sqrt{d}$، $\alpha_n=x_n+y_n\sqrt{d}$، و $\alpha_n'=x_n-y_n\sqrt{d}$. داریم $\alpha_n\alpha_n'=x_n^۲-dy_n^۲=۱$، و $\alpha_n'=۱/\alpha_n>۰$. همچنین، به‌ازای هر n، $\alpha_n<\alpha_{n+۱}$، زیرا $\alpha_n=\alpha_۱^n$ و $\alpha_۱>۱$؛ لذا $n\geq ۱$ وجود دارد به‌طوری که $\alpha_n<\beta\leq\alpha_{n+۱}$. با ضرب این نابرابری در α_n' داریم $۱<\beta\alpha_n'\leq\alpha_{n+۱}\alpha_n'=(\alpha_۱\alpha_n)\alpha_n'=\alpha_۱$.

اگر $\tau=\beta\alpha_n'$، آنگاه آشکار است که، به‌ازای اعداد صحیح a و b، $\tau=a+b\sqrt{d}$ (برهان (۹.۱۰) را ببینید). چون $(x_n,-y_n)$ جوابی از $x^۲-dy^۲=۱$ است، لم قبل ایجاب می‌کند که (a,b) نیز جواب باشد.

چون $\tau > ۱$ و $\tau\tau' = a^۲ - db^۲ = ۱$، داریم $۰ < \tau' < ۱$؛ بنابراین $۱ < a + b\sqrt{d}$ و $۰ < a - b\sqrt{d} < ۱$. با جمع و تفریق این دو نابرابری، می‌بینیم که a و b مثبت هستند. لذا (a, b) جواب مثبتی است که $a + b\sqrt{d} \le x_۱ + y_۱\sqrt{d}$، و بنابراین، چون $(x_۱, y_۱)$ کوچکترین جواب مثبت است، داریم $a = x_۱$ و $b = y_۱$. لذا $\beta = \alpha^{n+۱}$.

سرانجام، از تعریف x_n و y_n آشکار است که $\cdots < x_۳ < x_۲ < x_۱$ و $\cdots < y_۳ < y_۲ < y_۱$. چون به‌ازای $n \ge ۱$، تمام جوابهای مثبت با (x_n, y_n) ارائه می‌شوند، از تعریف (۲.۱۰) نتیجه می‌شود که (x_n, y_n) جواب مثبت nام است.

توضیح. ۱. اگر در (۱۰.۱۰) مقدار n را منفی (یا صفر) اختیارکنیم جوابهای نامنفی حاصل می‌شوند. در واقع، به‌ازای یک عدد صحیح مناسبِ n، هر جواب $x^۲ - dy^۲ = ۱$ به‌صورت (x_n, y_n) یا $(-x_n, -y_n)$ است. (مسألهٔ ۲۹.۱۰ را ببینید.)

۲. اگر (۶.۱۰) را به‌کار بریم، نتیجه می‌شود که $(x_n, y_n) = (p_{nm-۱}, q_{nm-۱})$ یا $(x_n, y_n) = (p_{۲nm-۱}, q_{۲nm-۱})$ برحسب آنکه m (طول دورهٔ $\sqrt{d}$) زوج یا فرد باشد.

(۱۱.۱۰) فرع. اعداد صحیح x_n و y_n که در (۱۰.۱۰) تعریف شدند در رابطه‌های بازگشتی زیر صدق می‌کنند:

$$x_{n+۱} = x_۱x_n + y_۱y_nd, \qquad y_{n+۱} = x_۱y_n + y_۱x_n$$

برهان. این رابطه‌ها فوراً از (۱۰.۱۰) با توجه به رابطهٔ زیر نتیجه می‌شود:

$$\begin{aligned} x_{n+۱} + y_{n+۱}\sqrt{d} &= (x_۱ + y_۱\sqrt{d})(x_۱ + y_۱\sqrt{d})^n = (x_۱ + y_۱\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= (x_۱x_n + y_۱y_nd) + (x_۱y_n + y_۱x_n)\sqrt{d}. \end{aligned}$$

(۱۲.۱۰) مثال. در (۸.۱۰)، نشان دادیم که جواب اصلی $x^۲ - ۲۹y^۲ = ۱$ عبارت است از $(p_۹, q_۹) = (۹۸۰۱, ۱۸۲۰)$. برای یافتن جواب مثبت بعدی رابطه‌های بازگشتی (۱۱.۱۰) را با $n = ۱$ به‌کار می‌بریم، لذا

$$\begin{aligned} x_۲ &= ۹۸۰۱ \times ۹۸۰۱ + ۱۸۲۰ \times ۱۸۲۰ \times ۲۹ = ۱۹۲۱۱۹۲۰۱ \\ y_۲ &= ۹۸۰۱ \times ۱۸۲۰ + ۱۸۲۰ \times ۹۸۰۱ = ۳۵۶۷۵۶۴۰. \end{aligned}$$

به‌ویژه، نتیجه می‌شود که هیچ جواب مثبت از $x^۲ - ۲۹y^۲ = ۱$ با x بین ۹۸۰۱ و ۱۹۲۱۱۹۲۰۱ وجود ندارد. بنابر (۶.۱۰)، جواب بعد از $(p_۹, q_۹)$ عبارت است از $(p_{۱۹}, q_{۱۹})$، و لذا $p_{۱۹} = ۱۹۲۱۱۹۲۰۱$ و $q_{۱۹} = ۳۵۶۷۵۶۴۰$.

معادلهٔ $x^۲ - dy^۲ = -۱$

در این بخش، به بررسی معادلهٔ وابستهٔ $x^۲ - dy^۲ = -۱$ می‌پردازیم. یک استدلال که واقعاً با برهان (۳.۱۰) یکی است نشان می‌دهد که هر جواب این معادله نیز به‌صورت (p, q) است، که در آن p/q یک همگرای $\sqrt{d}$ است (مسألهٔ ۳۳.۱۰ را ببینید). از (۵.۱۰) نتیجه می‌شود که (p_k, q_k) یک جواب است اگر و تنها اگر $m|k+۱$. لذا به‌ازای یک $j \geq ۱$، $k = jm - ۱$، و از این‌رو m فرد است. بنابراین، از ترکیب با (۶.۱۰) داریم:

(۱۳.۱۰) قضیه. فرض کنیم m طول دورهٔ $\sqrt{d}$ باشد، و فرض می‌کنیم p_k/q_k همگرای kام $\sqrt{d}$ را نشان دهد.

(i) اگر m زوج باشد، معادلهٔ $x^۲ - dy^۲ = -۱$ جوابی ندارد.

(ii) اگر m فرد باشد، تمام جوابهای مثبت $x^۲ - dy^۲ = -۱$ به‌ازای $j = ۱, ۳, ۵, \ldots$ با $x = p_{jm-۱}$ و $y = q_{jm-۱}$، و تمام جوابهای مثبت $x^۲ - dy^۲ = ۱$ به‌ازای $j = ۲, ۴, ۶, \ldots$؛ $x = p_{jm-۱}$ و $y = q_{jm-۱}$ داده می‌شوند. $(p_{m-۱}, q_{m-۱})$ کوچکترین جواب مثبت $x^۲ - dy^۲ = -۱$، و $(p_{۲m-۱}, q_{۲m-۱})$ کوچکترین جواب مثبت $x^۲ - dy^۲ = ۱$ است.

درست همانند حالت $x^۲ - dy^۲ = ۱$، می‌توان جوابهای دیگر معادلهٔ $x^۲ - dy^۲ = -۱$ را از کوچکترین جواب مثبت آن بدون محاسبهٔ همگراهای اضافی از $\sqrt{d}$ به‌دست آورد. در واقع، می‌توان جوابهای هر دو معادله را به روش زیر مشخص کرد.

(۱۴.۱۰) قضیه. فرض کنیم $x^۲ - dy^۲ = -۱$ دارای جواب باشد، و فرض می‌کنیم (r, s) کوچکترین جواب مثبت آن باشد. به‌ازای $n \geq ۱$، اعداد صحیح x_n و y_n را با رابطهٔ $x_n + y_n\sqrt{d} = (r + s\sqrt{d})^n$ تعریف می‌کنیم. در این صورت اگر n فرد باشد، (x_n, y_n) تمام جوابهای $x^۲ - dy^۲ = -۱$، و اگر n زوج باشد، (x_n, y_n) تمام جوابهای $x^۲ - dy^۲ = ۱$ را به‌دست می‌دهند. به‌ویژه، $(x_۲, y_۲)$ جواب اصلی $x^۲ - dy^۲ = ۱$ است.

برهان. ابتدا نشان می‌دهیم که $(x_۲, y_۲)$ جواب اصلی $x^۲ - dy^۲ = ۱$ است. فرض کنیم (g, h) کوچکترین جواب مثبت $x^۲ - dy^۲ = ۱$ را نشان دهد؛ لذا با توجه به (۱۳.۱۰) داریم $r + s\sqrt{d} < g + h\sqrt{d}$. با توجه به اتحاد برهمگوپته آشکار است که $(x_۲, y_۲)$ یک جواب مثبت

$x^۲-dy^۲=۱$ است، و لذا، بنابر (۱۰.۱۰)، به‌ازای یک $n \geq ۱$، $x_۲+y_۲\sqrt{d}=(g+h\sqrt{d})^n$. اگر n زوج باشد، مثلاً $n=۲k$، آنگاه $(r+s\sqrt{d})^۲=(g+h\sqrt{d})^{۲k}$ و لذا $r+s\sqrt{d}=(g+h\sqrt{d})^k$. چون $r+s\sqrt{d}<g+h\sqrt{d}$، داریم $k=۰$، یعنی، $r+s\sqrt{d}=۱$، که غیرممکن است. لذا n فرد است. اگر $n=۲k+۱$، آنگاه $(r+s\sqrt{d})^۲=(g+h\sqrt{d})^{۲k+۱}$)، و چون $r+s\sqrt{d}<g+h\sqrt{d}$، نتیجه می‌شود که $(g+h\sqrt{d})^{۲k}<r+s\sqrt{d}<g+h\sqrt{d}$. بنابراین $k=۰$، و لذا $x_۲+y_۲\sqrt{d}=g+h\sqrt{d}$، از آنجا $x_۲=g$ و $y_۲=h$.

چون $(x_۲,y_۲)$ جواب اصلی $x^۲-dy^۲=۱$ است، (۱۰.۱۰) ایجاب می‌کند که تمام جوابهای مثبت $x^۲-dy^۲=۱$ با (x_n,y_n) که n زوج است داده شوند.

اگر n فرد باشد، از «توضیح» بعد از (۹.۱۰) نتیجه می‌شود که (x_n,y_n) جواب مثبتی از $x^۲-dy^۲=-۱$ است. حال نشان می‌دهیم که هر جواب مثبتِ (u,v) از $x^۲-dy^۲=-۱$ به‌صورت (x_n,y_n) است که n فرد است. می‌نویسیم $(r+s\sqrt{d})(u+v\sqrt{d})=a+b\sqrt{d}$؛ لذا بنابر اتحاد برهمگوپته، (a,b) یک جواب مثبت $x^۲-dy^۲=۱$ است، بنابراین به‌ازای یک عدد زوج $k \geq ۲$، $a+b\sqrt{d}=(r+s\sqrt{d})^k$، ولذا $u+v\sqrt{d}=(r+s\sqrt{d})^{k-۱}=x_{k-۱}+y_{k-۱}\sqrt{d}$، که $k-۱$ فرد است. در نتیجه $u=x_{k-۱}$ و $v=y_{k-۱}$، که برهان را کامل می‌کند.

عموماً، بیان $(r+s\sqrt{d})^n$ به‌صورت $u+v\sqrt{d}$ تقریباً اتلاف وقت است. قضیهٔ زیر یک روش آسان جهت استفاده در حسابگر برای یافتن جوابهای مثبت دیگر $x^۲-dy^۲=۱$ (و $x^۲-dy^۲=-۱$ اگر جواب داشته باشد) هرگاه کوچکترین جواب مثبت معین باشد، به‌دست می‌دهد. برای یک برهان، مسألهٔ ۳۷.۱۰ را ببینید.

(۱۵.۱۰) قضیه. فرض کنیم (r,s) کوچکترین جواب مثبت $x^۲-dy^۲=-۱$ باشد اگر معادله جواب داشته باشد؛ در غیر این صورت، فرض می‌کنیم (r,s) کوچکترین جواب مثبت $x^۲-dy^۲=۱$ باشد. به‌ازای $n \geq ۱$، اعداد صحیح مثبت x_n و y_n را با $x_n+y_n\sqrt{d}=(r+s\sqrt{d})^n$ تعریف می‌کنیم. در این‌صورت، x_n نزدیکترین عدد صحیح به $(r+s\sqrt{d})^n/۲$، و y_n نزدیکترین عدد صحیح به $x_n\sqrt{d}$ است.

(۱۶.۱۰) مثال. به (۸.۱۰) مراجعه شود. چون $\sqrt{۲۹}$ دارای دوره‌ای به طول ۵ است، از (۱۳.۱۰) نتیجه می‌شود که $(p_۴,q_۴)=(۷۰,۱۳)$. کوچکترین جواب مثبت $x^۲-۲۹y^۲=-۱$ است؛ لذا بنابر نمادگذاری (۱۵.۱۰)، داریم $(r,s)=(۷۰,۱۳)$. از دو قضیهٔ قبل نتیجه می‌شود که $(x_۲,y_۲)=(۹۸۰۱,۱۸۲۰)$ کوچکترین جواب مثبت $x^۲-۲۹y^۲=-۱$ است، زیرا $x_۲$

نزدیکترین عدد صحیح به $(۷۰ + ۱۳\sqrt{۲۹})^۲/۲$ - یعنی ۹۸۰۱- و $y_۲ = ۱۸۲۰$، نزدیکترین عدد صحیح به $x_۲/\sqrt{۲۹} = ۹۸۰۱/\sqrt{۲۹}$ است. (از (ii.۱۳.۱۰) یا (ii.۶.۱۰) نتیجه می‌شود که $p_۹ = ۹۸۰۱$، $q_۹ = ۱۸۲۰$.) همچنین، جواب مثبت بعدی $x^۲ = ۲۹y^۲ = -۱$ بعد از $(۷۰, ۱۳)$ عبارت است از $(x_۳, y_۳) = (۱۳۷۲۲۱۰, ۲۵۴۸۱۳)$، زیرا نزدیکترین عدد صحیح به $(۷۰ + ۱۳\sqrt{۲۹})^۳/۲$ عدد ۱۳۷۲۲۱۰ و نزدیکترین عدد صحیح به $۱۳۷۲۲۱۰/\sqrt{۲۹}$ عدد ۲۵۴۸۱۳ است. (لذا $p_{۱۴} = x_۳ = ۱۳۷۲۲۱۰$ و $q_{۱۴} = y_۳ = ۲۵۴۸۱۳$.)

سرانجام، بررسی کنید که نزدیکترین عدد صحیح به $(۷۰ + ۱۳\sqrt{۲۹})^۴/۲$ عدد ۱۹۲۱۱۹۲۰۱، و نزدیکترین عدد صحیح به $۱۹۲۱۱۹۲۰۱/\sqrt{۲۹}$ عدد ۳۵۶۷۵۶۴۰ است. لذا جواب مثبت بعدی $x^۲ - ۲۹y^۲ = ۱$ بعد از $(۹۸۰۱, ۱۸۲۰)$ عبارت است از $(x_۴, y_۴) = (۱۹۲۱۱۹۲۰۱, ۳۵۶۷۵۶۴۰)$. به‌ویژه، داریم $p_{۱۹} = x_۴ = ۱۹۲۱۱۹۲۰۱$ و $q_{۱۹} = y_۴ = ۳۵۶۷۵۶۴۰$. (ضمناً، با توجه به (۳۳.۹)، نتیجه می‌شود که همگرای $p_{۱۹}/q_{۱۹}$ عدد $\sqrt{۲۹}$ را به‌خوبی تا ۱۵ رقم اعشار تقریب می‌زند.)

معادلهٔ $x^۲ - dy^۲ = N$

فرض می‌کنیم N عدد صحیح غیرصفرِ ثابتی باشد. اگر d منفی باشد، آنگاه $x^۲ - dy^۲ = N$ تنها تعداد متناهی جواب می‌تواند داشته باشد، زیرا $|x| \le \sqrt{N}$ و $|y| \le \sqrt{N/|d|}$. اگر d یک مربع کامل باشد، مثلاً $d = k^۲$، آنگاه داریم $(x + ky)(x - ky) = N$، و مجدداً تعداد متناهی جواب وجود دارد، زیرا تنها تعداد متناهی روش برای تجزیهٔ N وجود دارد. بنابراین فرض می‌کنیم که d یک عدد صحیح مثبتی است که مربع کامل نیست.

به‌ازای یک عدد مثبت N، معادلهٔ $x^۲ - dy^۲ = \pm N$ در ارتباط با یافتن تقریبهای گویای $\sqrt{d}$ وقتی که d یک مربع کامل نیست، در ریاضیات یونان باستان، پیدا می‌شود. در سدهٔ هفتم، برهمگوپته معادلهٔ $x^۲ - dy^۲ = \pm ۱$ را مورد بررسی قرار داده و اتحاد زیر را بیان داشته است:

$$(x^۲ - dy^۲)(z^۲ - dt^۲) = (xz \pm dyt)^۲ - d(xt \pm yz)^۲,$$

و این، به‌ویژه، نشان می‌دهد که از ضرب یک جواب $x^۲ - dy^۲ = N$ (مانند بالا) در یک جواب $x^۲ - dy^۲ = ۱$ جواب دیگری از $x^۲ - dy^۲ = N$ حاصل می‌شود. چون معادلهٔ پل، $x^۲ - dy^۲ = ۱$، بی‌نهایت جواب دارد، لذا اگر $x^۲ - dy^۲ = N$ جوابی داشته باشد، تعداد جوابهای آن بی‌نهایت است.

(۱۷.۱۰) قضیه. اگر معادلهٔ $x^۲ - dy^۲ = N$ یک جواب صحیح مثبت داشته باشد، آنگاه بی‌نهایت جواب دارد.

در حالت کلی، این بررسی که چه وقت $x^۲ - dy^۲ = N$ جواب دارد بسیار پیچیده‌تر از حالت $N = ۱$ است. مثلاً، به‌ازای یک مقدار مفروض N، لازم نیست که جواب از همگرای $\sqrt{d}$ تولید شود: فقط N را $a^۲ - db^۲$ اختیار کند، که در آن a و b اعداد صحیح دلخواهند. ولی، به‌ازای بعضی از مقادیر N، جوابها از همگرای $\sqrt{d}$ حاصل می‌شوند. (مسألهٔ ۵۸.۱۰ را برای برهانی از قضیهٔ زیر ببینید.)

(۱۸.۱۰) قضیه. اگر $|N| < \sqrt{d}$ و (r, s) جواب مثبتی از $x^۲ - dy^۲ = N$ باشد، آنگاه r/s یکی از همگراهای بسط کسر مسلسل $\sqrt{d}$ است.

توضیح. ۱. لزومی ندارد که اعداد صحیح r و s نسبت به هم اول باشند. اگر نباشند، فرض می‌کنیم $e = (r, s)$؛ در این صورت به‌ازای یک $k \geq ۰$ داریم $r/e = p_k$ و $s/e = q_k$، که p_k/q_k همگرایی از $\sqrt{d}$ است. مثلاً، $(۱۰, ۲)$ یک جواب $x^۲ - ۲۴y^۲ = ۴$ است، و به آسانی دیده می‌شود که ۵/۱ همگرای $p_۱/q_۱$ از $\sqrt{۲۴}$ است.

۲. مقادیری از N با $|N| > \sqrt{d}$ می‌توانند وجود داشته باشند که به‌ازای آنها نیز نتیجهٔ قضیهٔ قبل برقرار باشد. مثلاً، (۱۹/۴) جوابی از $x^۲ - ۲۳y^۲ = -۷$ است، و ۱۹/۴ همگرای چهارم $\sqrt{۲۳}$ است.

این بخش را با شرحی دربارهٔ تولید جوابهای دیگر معادلهٔ $x^۲ - dy^۲ = N$ از یک جواب مفروض خاتمه می‌دهیم. در ابتدای این بخش نشان دادیم که یک جواب از $x^۲ - dy^۲ = ۱$ و یک جواب از $x^۲ - dy^۲ = N$ با هم یک جواب دیگر از $x^۲ - dy^۲ = N$ را تولید می‌کنند. به‌ویژه، اگر $(x_۱, y_۱)$ جواب اصلی $x^۲ - dy^۲ = ۱$ باشد و (u, v) کوچکترین جواب مثبت $x^۲ - dy^۲ = N$، آنگاه اعداد صحیح x_n و y_n با تعریف زیر

$$x_n + y_n\sqrt{d} = (u + v\sqrt{d})(x_۱ + y_۱\sqrt{d})^n$$

جواب دیگری از $x^۲ - dy^۲ = N$ را به‌دست می‌دهند، اما ممکن است که (x_n, y_n) همهٔ جوابهای مثبت $x^۲ - dy^۲ = N$ را ارائه ندهند. مثالی از این نوع در مسألهٔ ۶۲.۱۰ آمده است.

یک مشکل کار این است که در طی یک دوره از $\sqrt{d}$، ممکن است مقدار معینی از s_k چندین بار اختیار شود، و لذا ممکن است تنها در یک دوره چند جواب از $x^۲ - dy^۲ = N$ وجود داشته باشد. در واقع، به‌ازای $n = ۲$، فرمول بالا جواب $(x_۲, y_۲)$ از $x^۲ - dy^۲ = N$ را به‌دست می‌دهد که اولین جواب در دورهٔ بعدی است، و لذا در دورهٔ خودش جوابهای دیگر را کنار می‌زند. اما اگر در یک دوره تنها یک جواب وجود داشته باشد (یعنی، فقط به‌ازای یک مقدار k، $N = (-۱)^k s_k$)، آنگاه فرمول بالا همهٔ جوابهای مثبت $x^۲ - dy^۲ = N$ را تولید خواهد کرد.

می‌توان نشان داد که به‌ازای هر عدد غیرصفر N، یک گردایهٔ متناهی از جوابهای $x^۲-dy^۲=N$ وجود دارد به‌طوری که می‌توان هر جواب را از ضرب یکی از این جوابها در یک جواب $x^۲-dy^۲=۱$ به‌دست آورد. (مسألهٔ ۶۳.۱۰ را ببینید.)

معادلهٔ پِل و مجموعهای دو مربع

برای به‌دست آوردن نمایشهای اولیه به‌صورت مجموع دو مربع از اعداد صحیح d که به‌ازای آنها معادلهٔ $x^۲-dy^۲=-۱$ جواب غیر نمایان دارد، می‌توان نظریه‌ای را که برای یافتن جوابهای معادلهٔ پِل بسط داده شده، به‌کار برد. به‌ویژه، روش مذکور در زیر نمایشهای اولیهٔ هر عدد اول به‌صورت $۴k+۱$ را به‌دست خواهد داد. ابتدا قضیهٔ زیر را اثبات می‌کنیم:

(۱۹.۱۰) قضیه. فرض می‌کنیم p عدد اولی به‌صورت $۴k+۱$ باشد. در این‌صورت معادلهٔ $x^۲-py^۲=-۱$ جواب دارد؛ به عبارت هم‌ارز با آن، طول دورهٔ $\sqrt{p}$ فرد است. به‌طور کلی، به‌ازای هر عدد صحیح فرد n طول دورهٔ تناوب $\sqrt{p^n}$ فرد است.

برهان. فرض کنیم (u,v) کوچکترین جواب مثبت $x^۲-py^۲=۱$ باشد. چون $u^۲-pv^۲=۱$ و $p\equiv ۱(\bmod ۴)$، داریم $u^۲-v^۲\equiv ۱(\bmod ۴)$، و لذا u فرد و v زوج است. اکنون $u^۲-pv^۲=۱$ اگر و تنها اگر $(u+۱)(u-۱)=pv^۲$. توجه داریم که $u+۱$ و $u-۱$ زوج‌اند و تفاضلشان ۲ است، و لذا $(u+۱,u-۱)=۲$. قرار می‌دهیم $v=۲w$ و $u+۱=۲t$؛ پس $t(t-۱)pw^۲$. دو حالت برای بررسی وجود دارند: یا t به‌صورت $r^۲$ و $t-۱$ به‌صورت $ps^۲$ است، یا $t=ps^۲$ و $t-۱=r^۲$. در حالت اول، داریم $r^۲-ps^۲=t-(t-۱)=۱$؛ اما $r<u$، و این با این واقعیت که (u,v) کوچکترین جواب مثبت $u^۲-pv^۲=۱$ است تناقض دارد. لذا $t=ps^۲$ و $t-۱=r^۲$؛ در این‌صورت $r^۲-ps^۲=(t-۱)-t=-۱$. اصولاً همین استدلال برای p^n کارساز است.

توضیح. جواب (r,s) که در برهان قبل به‌دست آمد در واقع کوچکترین جواب مثبت $x^۲-py^۲=-۱$ است. برای اثبات این امر، توجه کنید که بنابر (۱۴.۱۰)، به‌ازای یک عدد صحیح مثبت فرد n داریم $r+s\sqrt{d}=(p_{m-۱}+q_{m-۱}\sqrt{d})^n$، و

$$u+v\sqrt{d}=(p_{m-۱}+q_{m-۱}\sqrt{d})^۲$$

چون $r+s\sqrt{d}<u+v\sqrt{d}$، در نتیجه $n=۱$.

تکنیکی که در قضیهٔ بعد ذکر می‌شود روشی است که توسط لاگرانژ در ۱۸۰۸ برای نوشتن

یک عدد اول $۴k+۱$ به‌صورت مجموع دو مربع به‌کار رفته است. ولی برای هر عدد مثبت d که $\sqrt{d}$ دارای طول دورهٔ فرد باشد، هم به‌خوبی کاربرد دارد. (یک مثال که این روش در آن به‌کار می‌رود در مسألهٔ ۶۷.۱۰ ارائه شده است.)

(۲۰.۱۰) قضیه. فرض کنیم d عدد صحیح مثبتی باشد که مربع کامل نیست، و فرض می‌کنیم طول دورهٔ تناوب $\sqrt{d}$ فرد باشد. در این‌صورت d یک نمایش اولیه به‌صورت مجموع دو مربع متباین دارد. به‌ویژه، هر عدد اول به‌صورت $۴k+۱$ مجموع دو مربع متباین است.

برهان. چون طول دورهٔ $\sqrt{d}$ فرد است، بسط کسر مسلسل $\sqrt{d}$ به‌صورت

$$\langle a_۰, \overline{a_۱, a_۲, \ldots, a_k, a_k, \ldots, a_۲, a_۱, ۲a_۰} \rangle$$

است، که در آن جمله‌های میانی دورهٔ تناوب تکرار می‌شوند (توضیح ۱ بعد از (۱.۱۰) را ببینید). بنابر (۱۹.۹)، $a_{k+۱} = \langle \overline{a_k, a_{k-۱}, \ldots, a_۱, ۲a_۰, a_۱, \ldots, a_{k-۱}, a_k} \rangle$. بنابر (۲۴.۹)، اگر $\alpha = \alpha_{k+۱}$، $r = r_{k+۱}$، و $s = s_{k+۱}$، آنگاه مزدوج α عبارت است از $\alpha' = (r - \sqrt{d})/s$، و لذا $\alpha\alpha' = (r^۲ - d)/s^۲$.

اگر جمله‌های دورهٔ α را به‌ترتیب عکس بنویسیم، روشن است که عدد گنگ حاصل، β، در $\beta = \alpha$ صدق می‌کند، و لذا بنابر (۳۱.۹)، $\beta = -۱/\alpha'$. از این‌رو $\alpha\alpha' = -۱$ و بنابراین $(r^۲ - d)/s^۲ = -۱$، یعنی، $d = r^۲ + s^۲$.

سرانجام، ثابت می‌کنیم $(r, s) = ۱$. چون $d = r^۲ + s^۲$ و $s_k s_{k+۱} = d - r_{k+۱}^۲ = s_{k+۱}^۲$، داریم $s_k = s_{k+۱}$. اگر p عدد اولی باشد که r و s را بشمارد، آنگاه p عدد d را نیز می‌شمارد. چون $p|d$ و $p|s_k$، (i.۵.۱۰) ایجاب می‌کند که $p|p_{k-۱}^۲$، و لذا $p|p_{k-۱}$؛ با استدلال مشابه، از $p|d$ و $p|s_{k+۱}$ نتیجه می‌شود $p|p_k$. اما بنابر (۷.۹)، $p_k q_{k-۱} - p_{k-۱} q_k = (-۱)^{k-۱}$، و لذا بایستی $p| \pm ۱$، که یک تناقض است. بنابراین $(r, s) = ۱$.

توضیح. عکس قضیهٔ (۲۰.۱۰) درست نیست: اگر عدد صحیح مثبت d نمایشهای اولیه داشته باشد، لازم نیست که $\sqrt{d}$ دوره‌ای با طول فرد داشته باشد. (مسألهٔ ۶۸.۱۰ را ببینید.)

یک کاربرد: تجزیهٔ اعداد بزرگ

اگر $p_{k-۱}/q_{k-۱}$ یک همگرای بسط کسر مسلسل $\sqrt{d}$ باشد، (i.۵.۱۰) ایجاب می‌کند که $p_{k-۱}^۲ - dq_{k-۱}^۲ = (-۱)^k s_k$. گاهی اتفاق می‌افتد که به‌ازای یک مقدار زوج k، s_k

مربع کامل باشد، و این امر پایهٔ یک الگوریتم کارآمد برای تجزیهٔ اعداد بزرگ است، که بعداً ذکر می‌کنیم.

(۲۱.۱۰) بحث. فرض کنیم N یک عدد صحیح مثبت فرد باشد. اگر بتوان N را به‌صورت $a^۲ - b^۲$ با $a - b \neq ۱$ نوشت، آنگاه N مرکب است و می‌توان آن را به‌صورت $(a-b)(a+b)$ تجزیه کرد. این تکنیک، که به تجزیهٔ فرما معروف است، خیلی کارآمد نیست زیرا به یافتن مربعی به‌صورت $a^۲ - N$ نیاز دارد، و این نیز اگر N مرکب باشد ممکن است امتحان کردن تا $N/۶$ مقدار a را لازم داشته باشد.

ولی، شرط ضعیفتری وجود دارد که آن نیز به تجزیهٔ N منجر می‌شود. فرض کنیم اعداد صحیح مثبت a و b وجود داشته باشند به‌طوری که

$$a^۲ \equiv b^۲ (\mathrm{mod}\, N) \quad \text{با} \quad b < a < N \quad \text{و} \quad a + b \neq N$$

پس $a^۲ - b^۲ = (a-b)(a+b)$ بر N بخشپذیر است، و محدودیتهای a و b ایجاب می‌کنند که نه $a-b$ بر N بخشپذیر باشد و نه $a+b$. حال، الگوریتم اقلیدسی را برای یافتن $d_۱ = (a-b, N)$ و $d_۲ = (a+b, N)$ به‌کار می‌بریم. آشکار است که $d_۱$ و $d_۲$ مقسوم‌علیه‌های سرهٔ N، یعنی $۱ < d_۱ < N$ و $۱ < d_۲ < N$، هستند. (مسألهٔ ۷۲.۱۰ را ببینید.)

همنهشتی $x^۲ \equiv y^۲ (\mathrm{mod}\, N)$ به همنهشتی لژاندر معروف است. لذا مسألهٔ تجزیهٔ N به یافتن جوابهایی از همنهشتی لژاندر که مقسوم‌علیه‌های غیرنمایان N را تولید می‌کنند، تحویل می‌شود. روشی که برای پیدا کردن آنها به‌کار می‌بریم روش تجزیهٔ لژاندر نامیده می‌شود و از بسط کسر مسلسل $\sqrt{N}$ استفاده می‌کند. (روش لژاندر خانواده‌ای از الگوریتم تجزیه است که کسرهای مسلسل را به‌کار می‌برند. «توضیحات» آخر فصل را ببینید.)

(۲۲.۱۰) روش تجزیهٔ لژاندر. گیریم N عدد صحیح مثبت فردی باشد که مربع کامل نیست. فرض می‌کنیم $d = N$ و اعداد صحیح r_k و s_k را مانند (۲۴.۹) تعریف می‌کنیم. در این‌صورت، بنابر (i.۵.۱۰)،

$$p_{k-۱}^۲ - N q_{k-۱}^۲ = (-۱)^k s_k,$$

یعنی،

$$p_{k-۱}^۲ \equiv (-۱)^k s_k (\mathrm{mod}\, N).$$

اگر k زوج باشد و s_k مربع کامل باشد، مثلاً $s_k = c^2$، آنگاه

$$x \equiv p_{k-1} \pmod N \quad \text{و} \quad y \equiv c \pmod N$$

جوابی از همنهشتی لژاندر است. اگر این یک جواب نمایان باشد، یعنی، اگر $p_{k-1} \equiv \pm c \pmod N$، آنگاه روش مذکور در بالا تنها عاملهای نمایان ۱ و N را تولید می‌کند. اما اگر $p_{k-1} \not\equiv \pm c \pmod N$، آنگاه این روش مقسوم‌علیه‌های سره را به‌دست می‌دهد. (مسائل ۷۲.۱۰ و ۷۸.۱۰ را ببینید.)

می‌توان روش تجزیهٔ لژاندر را به‌ترتیب زیر خلاصه کرد:

۱. فرض می‌کنیم N عدد صحیح مثبت فردی باشد که مربع کامل نیست. ابتدا r_k، s_k، a_k، و p_k را محاسبه می‌کنیم. می‌توان این کار را در یک جدول انجام داد. (مثال زیر را ببینید.) توجه کنید که محاسبهٔ q_k لازم نیست. برای حفظ اعداد در اندازهٔ قابل کنترل، به محض آنکه مقادیر p_n از N تجاوز کردند بایستی به پیمانهٔ N تحویل شوند.

۲. وقتی یک s_k با kی زوج به‌دست آمد، بررسی می‌کنیم که s_k مربع کامل است یا نیست، (از s_kها با kی فرد صرف‌نظر می‌کنیم.)

۳. اگر $s_k = c^2$ و $p_{k-1} \not\equiv \pm c \pmod N$، فرض می‌کنیم $a = p_{k-1}$ و $b = c$. (اگر $p_{k-1} \equiv \pm c \pmod N$، s_kی بعدی را که مربع کامل است جستجو می‌کنیم.)

۴. الگوریتم اقلیدسی را برای یافتن $d_1 = (a-b, N)$ و $d_2 = (a+b, N)$ به‌کار می‌بریم. در این‌صورت d_1 و d_2 مقسوم‌علیه‌های سرهٔ N هستند. در واقع، $d_1 d_2 = N$ (مسألهٔ ۷۷.۱۰ را ببینید)؛ لذا، مثلاً، برای یافتن d_1، کاربرد الگوریتم اقلیدسی تنها یک بار ضرورت پیدا می‌کند؛ سپس روشن است که $d_2 = N/d_1$.

۵. اگر d_1 یا d_2 مرکب باشند، می‌توان این روند را برای یافتن عاملهای بیشتری از N تکرار کرد.

توضیح. ممکن است اتفاق بیفتد که دورهٔ تناوب $\sqrt{N}$ خیلی کوتاه باشد؛ مثلاً، به‌ازای هر $n \geq 1$ $\sqrt{n^2+1} = \langle n, \overline{2n} \rangle$. اگر چنین باشد، احتمال یافتن مربعهای به دردخور در میان s_k کم است. در این حالت، برای افزایش طول دورهٔ تناوب ، می‌توان N را در عدد صحیح دیگری، به نام عامل تقویت‌کننده، ضرب کرد. (مسائل ۸۱.۱۰ تا ۸۳.۱۰ را ببینید.)

می‌توان این تکنیک را حتی اگر دورهٔ تناوب $\sqrt{N}$ طولانی باشد نیز به‌کار برد، اما الگوریتم تجزیه هیچ مربع به‌دردخوری، مثلاً، برای نخستین ۵۰۰ مقدار s_k تولید نمی‌کند. اگر این اتفاق بیفتد، می‌توانیم یک عامل تقویت‌کننده به‌کار بریم و روند را مجدداً شروع کنیم.

(۲۳.۱۰) مثال. روش تجزیهٔ لژاندر را برای عدد نسبتاً کوچک $N = ۷۶۱۸۳$ نشان می‌دهیم؛ یک مقدار خیلی بزرگتر N در مسألهٔ ۷۶.۱۰ مورد استفاده قرارگرفته است. (دلیل انتخاب ۷۶۱۸۳ این است که طول دورهٔ تناوبش فقط ۲۰ است. دورهٔ تناوب عدد به‌کار رفته در مسألهٔ ۷۶.۱۰ دارای ۱۱۷۸ جمله است!) جدول زیر را می‌سازیم:

k	۰	۱	۲	۳	۴	۵	۶
r_k	۰	۲۷۶	۲۷۰	۱۹۹	۲۶۹	۲۷۰	۲۶۶
s_k	۱	۷	۴۶۹	۷۸	۴۹	۶۷	۸۱
a_k	۲۷۶	۷۸	۱	۶	۱۱	۸	۶
p_k	۲۷۶	۲۱۵۲۹	۲۱۸۰۵	(۷۶۱۷۶)	(۲۱۷۲۸)	(۲۱۴۵۱)	

اعداد درون پرانتزها کوچکترین مانده‌های مثبت p_k به پیمانهٔ ۷۶۱۸۳ را به‌دست می‌دهند، مثلاً، $۲۱۵۲۹ + ۲۱۸۰۵ \times ۶ \equiv ۷۶۱۷۶ \pmod{۷۶۱۸۳}$. ما باز هم فرمول

$$p_{k+۱} = a_{k+۱}p_k + p_{k-۱}$$

را به‌کار می‌بریم، اما هر موقع که ممکن باشد، کوچکترین ماندهٔ مثبت یک عدد را به‌کار می‌بریم.

نخستین s_k که مربع کامل است $s_۴ = ۴۹$ است؛ بنابراین، $p_۴^۲ \equiv s_۴ \pmod{۷۶۱۸۳}$، یعنی، $(۷۶۱۷۶)^۲ \equiv ۷^۲ \pmod{۷۶۱۸۳}$. ولی، چون $-۷ \equiv ۷۶۱۷۶ \pmod{۷۶۱۸۳}$، روش تجزیهٔ لژاندر مقسوم‌علیه‌های سره از ۷۶۱۸۳ تولید نمی‌کند.

s_kی بعدی که مربع کامل است $s_۶ = ۸۱$ است؛ لذا $p_۵^۲ \equiv s_۶ \pmod{۷۶۱۸۳}$، در نتیجه $(۲۱۴۵۱)^۲ \equiv ۹^۲ \pmod{۷۶۱۸۳}$. چون

$$(۲۱۴۵۱ - ۹, ۷۶۱۸۳) = (۲۱۴۴۲, ۷۶۱۸۳) = ۷۱$$

و $(۲۱۴۶۰, ۷۶۱۸۳) = (۲۱۴۵۱ + ۹, ۷۶۱۸۳) = ۱۰۷۳$، از اینجا نتیجه می‌شود که ۷۱ و ۱۰۷۳ مقسوم‌علیه‌های ۷۶۱۸۳ هستند. در واقع، $۷۶۱۸۳ = ۷۱ \times ۱۰۷۳$. (ولی، عدد ۱۰۷۳ اول نیست؛ $۱۰۷۳ = ۲۹ \times ۳۷$.)

توضیح. اگر m طول دورهٔ تناوب $\sqrt{N}$ باشد، آنگاه $s_m = ۱$. در این مثال، چون $m = ۲۰$ زوج است، داریم $p_۱۹^۲ \equiv s_۲۰ \pmod{۷۶۱۸۳}$، یعنی، $(۶۱۷۸)^۲ \equiv ۱ \pmod{۷۶۱۸۳}$، که ایجاب می‌کند ۳۷ و ۲۰۵۹ مقسوم‌علیه‌های ۷۶۱۸۳ باشند. ولی، در حالت کلی، استفاده از

$s_m = ۱$ برای جستجوی عاملهای N عملی نیست، زیرا s_m آخرین درایه در یک دورهٔ تناوبی است که ممکن است بسیار طولانی باشد و لذا مقدار زیادی محاسبه برای یافتن $p_{m-۱}$ لازم دارد.

سرانجام اشاره می‌کنیم که می‌توان مقادیر زوج s_k را که مربع نیستند برای تجزیهٔ N به‌کار برد. اگر $s_i = s_j = a$، که i و j همپایگی واحدی دارند (یعنی یا هر دو زوج‌اند، یا هر دو فرد)، آنگاه $(p_i p_j) \equiv (-۱)^{i+j} s_i^۲ = a^۲ (\mathrm{mod}\, N)$، و لذا می‌توان روش تجزیهٔ لژاندر را به‌کار برد. وقتی m زوج است، داریم $s_{m-k} = s_k$، و لذا می‌توانیم این تکنیک را با شروع از درونی‌ترین جفت از مقادیر s_k به‌کار بریم، سپس جفت متقارن بعدی، و قس‌علیهذا.

وقتی دورهٔ تناوب خیلی طولانی نباشد این روش کارایی خوبی دارد، زیرا در این حالت، ممکن است مربعهای قابل استفادهٔ زیاد (یا هیچ) برای کارکردن با آنها وجود نداشته باشند. یک مثال که از این روند استفاده می‌کند در تمرین ۸۴.۱۰ آمده است.

مسأله‌ها و راه‌حلها

بسط کسر مسلسل $\sqrt{d}$

۱.۱۰ فرض می‌کنیم $\alpha = \sqrt{d}$ (که d یک مربع کامل نیست)، و α_k، r_k، و s_k را مانند قضیهٔ ۲۴.۹ تعریف می‌کنیم. ثابت کنید به‌ازای هر $k \geq ۱$، $۰ < r_k < \sqrt{d}$ و $۰ < s_k < ۲\sqrt{d}$. (راهنمایی: از (۵.۱۰) استفاده کنید.)

حل. بنابر (ii.۵.۱۰)، به‌ازای هر k، $s_k > ۰$، و $۰ < s_k < (d - r_k^۲)/s_{k-۱}$ ایجاب می‌کند که $r_k < \sqrt{d}$. حال فرض می‌کنیم $r_{k-۱} < \sqrt{d}$ پس $۰ \leq r_{k-۱} \leq a_{k-۱} s_{k-۱} \leq s_{k-۱}$، زیرا $r_k = a_{k-۱} s_{k-۱} - r_{k-۱}$. بنابر (۲۴.۹)، $s_k = (d - r_k^۲)/s_{k-۱}$؛ لذا

$$۱ > \alpha_{k-۱} - a_{k-۱} = ۱/\alpha_k = s_k/(\sqrt{d} + r_k) = (\sqrt{d} - r_k)/s_{k-۱} \geq \sqrt{d}/s_{k-۱} > ۱$$

که یک تناقض است. لذا $r_k > ۰$.

سرانجام، $r_{k+۱} = a_k s_k - r_k$ ایجاب می‌کند که

$$s_k = (r_k + r_{k+۱})/a_k \leq r_k + r_{k+۱} < ۲\sqrt{d}$$

و لذا $s_k < ۲\sqrt{d}$.

۲.۱۰ مسألهٔ قبل را برای به‌دست آوردن یک کران بالا برای طول دورهٔ تناوب $\sqrt{d}$ به‌کار برید. (راهنمایی: از (iii.۲۴.۹) استفاده کنید.)

حل. حداکثر $[\sqrt{d}]$ مقدار برای r_k و $[۲\sqrt{d}]$ مقدار برای s_k وجود دارند؛ لذا حداکثر $[\sqrt{d}][۲\sqrt{d}] < d^۲$ جفت متمایز r_k، s_k وجود دارند. بنابراین اعداد صحیح مثبت i و j با $i < j \le ۲d$ وجود دارند به‌طوری که $r_i = r_j$ و $s_i = s_j$. از (iii.۲۴.۹) نتیجه می‌شود که $\alpha_i = \alpha_j$، و لذا به‌ازای هر $t \ge ۰$، $\alpha_{i+t} = \alpha_{j+t}$. در نتیجه، مقسوم‌علیه‌های جزئی $\sqrt{d}$ تکرار می‌شوند، و طول دورهٔ تناوب $\sqrt{d}$ باید کوچکتر از $۲d$ باشد.

توضیح. در واقع، طول دورهٔ تناوب $\sqrt{d}$ کوچکتر از $۰٫۷۲\sqrt{d}\log d$ و اغلب بسیار کوتاهتر است.

۳.۱۰ فرض می‌کنیم $\alpha = \langle a_۰, \overline{a_۱, a_۲, \ldots, a_۲, a_۱, ۲a_۰}\rangle$، که در آن دنبالهٔ $a_۱$، $a_۲$، ...، $a_۲$، $a_۱$ از خارج‌قسمتهای جزئی متقارن است. ثابت کنید که $\alpha = \sqrt{r}$، که در آن r یک عدد گویای بزرگتر از ۱ است. (راهنمایی: (۳۱.۹) را به‌کار برید.)

حل. چون α یک بسط کسر مسلسل دوره‌یی دارد، α یک گنگ درجهٔ دوم است. فرض کنیم $\alpha = (a + \sqrt{d})/b$؛ پس $\alpha = a_۰ + ۱/\beta$، که $\beta = \langle \overline{a_۱, a_۲, \ldots, a_۲, a_۱, ۲a_۰}\rangle$، و لذا $-۱/\beta' = \langle \overline{۲a_۰, a_۱, a_۲, \ldots, a_۲, a_۱}\rangle = a_۰ + \alpha$، (۳۱.۹). اما بنابر $-۱/\beta' = a_۰ - \alpha'$. لذا $a_۰ + \alpha = a_۰ - \alpha'$، یعنی، $\alpha + \alpha' = ۰$. بلافاصله نتیجه می‌شود که $a = ۰$ و $\alpha = \sqrt{d}/b = \sqrt{d/b^۲}$. فرض کنیم $r = d/b^۲$. چون بایستی $۲a_۰$ مثبت باشد، داریم $a_۰ \ge ۱$، و لذا $r > ۱$.

◁ **۴.۱۰** فرض می‌کنیم $\sqrt{d} = \langle a_۰, \overline{a_۱, \ldots, a_{m-۱}, ۲a_۰}\rangle$، و r_k و s_k را مانند (۲۴.۹) تعریف می‌کنیم. ثابت کنید که مقادیر r_k و s_k درون هر دورهٔ تناوب متقارن هستند. به‌ویژه، اگر m طول دورهٔ تناوب $\sqrt{d}$ باشد، ثابت کنید $s_i = s_{m-i}$ $(i = ۰, ۱, ۲, \ldots, m)$ و $r_{i+۱} = r_{m-i}$ $(i = ۰, ۱, ۲, \ldots, m-۱)$. به‌طور کلی، به‌ازای هر $t \ge ۰$، و به‌ازای مقادیر i در بالا

$$s_{tm+i} = s_{tm+m-i} \quad \text{و} \quad r_{tm+i+۱} = r_{tm+m-i}$$

حل. اثبات به استقرا بر i. با توجه به (۱.۱۰)، می‌توانیم بنویسیم

$$\sqrt{d} = \langle a_۰, \overline{a_۱, a_۲, \ldots, a_۱, ۲a_۰}\rangle$$

که در آن $a_1 = a_{m-1}$ ، $a_2 = a_{m-2}$ ، ... . اگر $\alpha_k = \langle a_k, a_{k+1}, \ldots \rangle$، آنگاه بنابر (iii.۲۴.۹)، $\alpha_k = (r_k + \sqrt{d})/s_k$. بنابر دوره‌یی بودن $\alpha_1 = \alpha_{m+1}$ و لذا $r_1 = r_{m+1}$، $s_1 = s_{m+1}$. با استفاده از (iii.۵.۱۰)، داریم $s_0 = s_m = 1$.

برای اینکه نشان دهیم $r_1 = r_m$، توجه داریم که $r_1 = a_0 s_0 - r_0$، و لذا $r_1 = a_0$ زیرا $r_0 = 0$. بنابر دوره‌یی بودن، داریم $\alpha_1 = \alpha_{m+1}$، یعنی، $(r_1 + \sqrt{d})/s_1 = (r_{m+1} + \sqrt{d})/s_{m+1}$. بنابراین $(s_{m+1} - s_1)\sqrt{d} = s_1 r_{m+1} - s_{m+1} r_1$، و چون $\sqrt{d}$ گنگ است، داریم $s_1 = s_{m+1}$، و لذا $r_1 = r_{m+1}$. بنابه تعریف، $a_m s_m - r_m = r_{m+1}$؛ چون $a_m = 2a_0 = 2r_1$ و $r_1 = r_{m+1}$، نتیجه می‌شود که $2r_1 - r_m = r_1$، یعنی، $r_1 = r_m$. لذا هر دو معادله به‌ازای $i = 0$ برقرارند.

حال فرض می‌کنیم که به‌ازای یک $i \geq 0$ داریم $s_i = s_{m-i}$ و $r_{i+1} = r_{m-i}$. بنابه تعریف ((۲۴.۹) را ببینید)، داریم $(d - r_{i+1}^2)/s_i = s_{i+1}$، و لذا $(d - r_{m-1}^2)/s_{m-1} = s_{i+1}$. چون $(d - r_{m-i}^2)/s_{m-i} = s_{m-i-1}$ ((۲۴.۹) را ببینید)، نتیجه می‌شود که $s_{i+1} = s_{m-(i+1)}$، و لذا معادلهٔ اول به‌ازای $i + 1$ ثابت می‌شود.

اکنون معادلهٔ دوم را به‌ازای $i + t$ ثابت می‌کنیم، یعنی $r_{i+2} = r_{m-(i+1)}$. بنابه تعریف، $r_{i+2} = a_{i+1} s_{i+1} - r_{i+1}$. چون $s_{i+1} = s_{m-(i+1)}$، $a_{i+1} = a_{m-(i+1)}$، و $r_{i+1} = r_{m-i}$ (فرض استقرا)، در نتیجه، $r_{i+2} = a_{m-(i+1)} s_{m-(i+1)} - r_{m-i} = r_{m-(i+1)}$.

سرانجام، نتیجهٔ کلیتر از معادله‌های بالا و دوره‌یی بودن بسط کسر مسلسل $\sqrt{d}$ نتیجه می‌شود. چون $a_{tm+i} = \alpha_i$ و $\alpha_{tm+m-i} = \alpha_{m-i}$، داریم $s_{tm+i} = s_i = s_{m-i} = s_{tm+m-i}$؛ با روشی مشابه $\alpha_{tm+i+1} = \alpha_{i+1}$ و $\alpha_{tm+m-i} = \alpha_{m-i}$ ایجاب می‌کنند که

$$r_{tm+i+1} = r_{i+1} = r_{m-i} = r_{tm+m-i}$$

۵.۱۰ فرض کنید $\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0} \rangle$. اگر $k \leq m - 1$، ثابت کنید $a_k \leq a_0$. (راهنمایی: از (۲۴.۹) و مسألهٔ ۱.۱۰ استفاده کنید.)

حل. می‌توانیم فرض کنیم $k \geq 1$، α_k، r_k، و s_k را مانند (۲۴.۹) تعریف می‌کنیم؛ پس $a_k = (r_k + \sqrt{d})/s_k$ و $s_k = [\alpha_k]$. بنابر (۵.۱۰)، $s_k \geq 2$ زیرا $k < m$ طول دورهٔ تناوب $\sqrt{d}$ است). همچنین، مسأله ۱.۱۰ ایجاب می‌کند که $0 < r_k < \sqrt{d}$. از این‌رو $\alpha_k < (2\sqrt{d})/2 = \sqrt{d}$، و لذا $a_k = [\alpha_k] \leq [\sqrt{d}] = a_0$.

۶.۱۰ فرض می‌کنیم $\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0} \rangle$. اگر kای وجود داشته باشد که

$a_k = ۲a_۰$، آیا بایستی k مضربی از m (طول دورهٔ تناوب $\sqrt{d}$) باشد؟ (مسألهٔ قبل را به‌کار برید.)

حل. آری؛ مستقیماً از مسألهٔ قبل نتیجه می‌شود، زیرا هر جملهٔ دوره بجز آخری بایستی نابزرگتر از $a_۰$ باشد. لذا $a_k = ۲a_۰$ اگر و تنها اگر a_k آخرین جمله در دورهٔ تناوب باشد، یعنی، اگر و تنها اگر k مضربی از m باشد.

◁ **۷.۱۰** ثابت کنید بسط کسر مسلسل $\sqrt{d}$ دارای دورهٔ تناوبی به طول ۱ است اگر و تنها اگر $n \geq ۱$ وجود داشته باشد به‌طوری که $d = n^۲ + ۱$.

حل. بنابر مسألهٔ ۲۴.۹، اگر $d = n^۲ + ۱$، آنگاه $\sqrt{d} = \langle n, \overline{۲n} \rangle$. حال فرض می‌کنیم که بسط کسر مسلسل $\sqrt{d}$ دورهٔ تناوبی به طول ۱ داشته باشد؛ پس بنابر (۱.۱۰)، $\sqrt{d} = \langle n, \overline{۲n} \rangle$. فرض کنیم $\alpha = \langle \overline{۲n} \rangle$؛ لذا $\alpha = ۲n + ۱/\alpha$، یعنی، $\alpha^۲ - ۲n\alpha + ۱ = ۰$. از این‌رو $\alpha = n + \sqrt{n^۲ + ۱}$، و لذا

$$\sqrt{d} = n + ۱/\alpha = n + (\sqrt{n^۲ + ۱} - n) = \sqrt{n^۲ + ۱}$$

◁ **۸.۱۰** ثابت کنید که با اثبات مطلب زیر دورهٔ تناوب $\sqrt{d}$ می‌تواند به‌دلخواه طولانی شود: اگر m عدد صحیح مثبتی باشد، عدد صحیح مثبت d، که مربع کامل نیست، وجود دارد به‌طوری که m طول دورهٔ تناوب $\sqrt{d}$ است.

حل. روش کار را با تولید یک عدد صحیح مثبت d به‌طوری که طول دورهٔ تناوب $\sqrt{d}$ برابر ۵ باشد نشان می‌دهیم. فرض کنیم n یک عدد صحیح مثبت باشد، و تعریف می‌کنیم $\alpha = \langle n\overline{۲, ۲, ۲, ۲, ۲n} \rangle$؛ لذا بنابر (۱۴.۹)، $\alpha = n + ۱/\langle ۲, ۲, ۲, ۲, n + \alpha \rangle$. از (۴.۹) نتیجه می‌شود که $\alpha - n = ((n+\alpha)q_۳ + q_۲)/((n+\alpha)p_۳ + p_۲)$، که در آن p_i/q_i همگراهای $\langle ۲, ۲, ۲, ۲ \rangle$ هستند. به آسانی بررسی می‌شود که به‌ازای $i = ۱, ۲, ۳, ۴$، $q_i = p_{i-۱}$. می‌توان معادلهٔ $\alpha - n$ در فوق را به‌صورت زیر نوشت

$$(\alpha - n)(n + \alpha)p_۳ + (\alpha - n)p_۲ = (n + \alpha)q_۳ + q_۲;$$

چون $p_۲ = q_۳$ و $p_۳ = q_۴$، معادله به‌صورت زیر ساده می‌شود

$$(\alpha^۲ - n^۲)q_۴ = ۲nq_۳ + q_۲ \qquad (۱)$$

اگر $n = q_۴ + ۱$، آنگاه

$$۲nq_۳ + q_۲ = ۲(q_۴ + ۱)q_۳ + q_۲ = ۲q_۴q_۳ + ۲q_۳ + q_۲ = q_۴(۲q_۳ + ۱)\,.$$

لذا (۱) به $\alpha^۲ = (q_۴+۱)^۲+۲q_۳+۱$ تبدیل می‌شود. قرار می‌دهیم $d = (q_۴+۱)^۲+۲q_۳+۱$؛ لذا $\sqrt{d} = \alpha = \langle q_۴ + ۱, \overline{۲, ۲, ۲, ۲, ۲, (q_۴ + ۱)}\rangle$.

به‌طور کلی، برای به‌دست آوردن d به‌طوری که $\sqrt{d}$ دارای دورهٔ تناوبی به طول m باشد، روند بالا را با جانشین کردن $\langle ۲, ۲, ۲, \ldots, ۲$ (m تا ۲) به جای $\langle ۲, ۲, ۲, ۲\rangle$، پی می‌گیریم. سپس $q_{m-۱}$ جانشین $q_۴$ می‌شود، و $\sqrt{d} = \langle q_{m-۱} + ۱, \overline{۲, ۲, \ldots, ۲, ۲, (q_{m-۱} + ۱)}\rangle$ دورهٔ تناوبی به طول m دارد.

۹.۱۰ فرض می‌کنیم p_k/q_k معرّف همگرای kام $\sqrt{۲}$ باشد، اگر $k \geq ۱$، ثابت کنید p_k هرگز مربع نیست. (راهنمایی: مسألهٔ ۲۲.۸ را به‌کار برید.)

حل. چون $\sqrt{۲} = \langle ۱, \overline{۲}\rangle$ دورهٔ تناوبی به طول ۱ دارد، از (۱۳.۱۰) نتیجه می‌شود که به‌ازای هر $k \geq ۰$، $p_k^۲ - ۲q_k^۲ = \pm ۱$. حال فرض می‌کنیم kای وجود داشته باشد که $p_k = x^۲$، و قرار می‌دهیم $q_k = y$؛ پس $x^۴ - ۲y^۲ = \pm ۱$. اما بنابر مسألهٔ ۲۲.۸، معادلهٔ $x^۴ - ۲y^۲ = ۱$ جواب صحیح مثبت ندارد، و $x^۴ - ۲y^۲ = -۱$ تنها یک جواب مثبت دارد، یعنی $x = y = ۱$. در این حالت داریم $p_k = q_k = ۱$، و لذا $k = ۰$.

معادلهٔ پِل $x^۲ - dy^۲ = ۱$

۱۰.۱۰ نخستین سه جواب مثبت $x^۲ - ۱۳y^۲ = ۱$ را به‌دست آورید.

حل. چون $\sqrt{۱۳} = \langle ۳, \overline{۱, ۱, ۱, ۱, ۶}\rangle$، (۶.۱۰) ایجاب می‌کند که جواب اصلی $(p_۹, q_۹) = (۶۴۹۱۸۰)$ باشد، حال (۱۰.۱۰) را برای تولید جوابهای دیگر به‌کار می‌بریم. چون $(۶۴۹ + ۱۸۰\sqrt{۱۳})^۲ = ۸۴۲۴۰۱ + ۲۳۳۶۴۰\sqrt{۱۳}$ و

$$\begin{aligned}(۶۴۹ + ۱۸۰\sqrt{۱۳})^۳ &= (۶۴۹ + ۱۸۰\sqrt{۱۳})^۲(۶۴۹ + ۱۸۰\sqrt{۱۳})\\ &= (۸۴۲۴۰۱ + ۲۳۳۶۴۰\sqrt{۱۳})(۶۴۹ + ۱۸۰\sqrt{۱۳})\\ &= ۱۰۹۳۴۳۵۸۴۹ + ۳۰۳۲۶۴۵۴۰\sqrt{۱۳}\end{aligned}$$

دو جواب بعدی عبارت اند از $(۸۴۲۴۰۱, ۲۳۳۶۴۰)$ و $(۱۰۹۳۴۳۵۸۴۹, ۳۰۳۲۶۴۵۴۰)$.

۱۱.۱۰ صورت کلی یک جواب مثبت $x^۲ - ۲۱y^۲ = ۱$ را برحسب همگراهای $\sqrt{۲۱}$ به‌دست آورید، و جواب اصلی را تعیین کنید.

حل. بررسی کنید که $\sqrt{۲۱} = \langle ۴, \overline{۱, ۱, ۲, ۱, ۱, ۸} \rangle$؛ لذا طول دورهٔ تناوب ۶ است. بنابر (۶.۱۰)، تمام جوابها به‌ازای $j \geq ۱$ عبارت‌اند از $x = p_{۶j-۱}$، $y = p_{۶j-۱}$، که p_k/q_k همگرای kام $\sqrt{۲۱}$ است. $(p_۵, q_۵) = (۵۵, ۱۲)$ جواب اصلی است.

۱۲.۱۰ فرض می‌کنیم (u, v) یک جواب مثبت $x^۲ - ۲y^۲ = ۱$ باشد. ثابت کنید که u بر هیچ عدد اولی به‌صورت $۸k + ۵$ یا $۸k + ۷$ بخشپذیر نیست.

حل. چون $u^۲ = ۲v^۲ + ۱$ فرد است، هر عامل اول u فرد است. اگر p اول و $p|u$، آنگاه $-۲v^۲ \equiv ۱ (\mathrm{mod}\, p)$، و لذا $(-۲v^۲/p) = (-۲/p) = ۱$. لذا، بنابر (۱۳.۵)، p به‌صورت $۸k + ۱$ یا $۸k + ۳$ است.

۱۳.۱۰ فرض می‌کنیم طول دورهٔ تناوب $\sqrt{d}$ فرد باشد. ثابت کنید که به‌ازای بی‌نهایت مقدار k طول دورهٔ تناوب $\sqrt{k^۲d}$ برابر ۱ است. (راهنمایی: بنابر مسألهٔ ۲۴.۹، $\sqrt{n^۲ + ۱} = \langle n, \overline{۲n} \rangle$).

حل. چون $\sqrt{n^۲ + ۱} = \langle n, \overline{۲n} \rangle$، کافی است نشان دهیم که به‌ازای بی‌نهایت مقدار k و n، $k^۲d = n^۲ + ۱$. اما، این همان معادلهٔ $n^۲ - dk^۲ = -۱$ است که بنابر (۱۳.۱۰)، تعداد نامتناهی جواب دارد.

۱۴.۱۰ فرض می‌کنیم که d مربع کامل نباشد. ثابت کنید که به‌ازای بی‌نهایت مقدار k، طول دورهٔ تناوب $\sqrt{k^۲d}$ برابر ۲ است. (راهنمایی: از مسألهٔ ۲۵.۹ استفاده کنید.)

حل. بنابر مسألهٔ ۲۵.۹، $\sqrt{n^۲ - ۱} = \langle n - ۱, \overline{۱, ۲n - ۲} \rangle$. لذا، کافی است نشان دهیم که معادلهٔ $k^۲d = n^۲ - ۱$، یعنی $n^۲ - dk^۲ = ۱$ به‌ازای تعداد نامتناهی k و n جواب دارد. اما بنابر (۷.۱۰) به‌ازای هر d، این معادله بی‌نهایت جواب دارد.

۱۵.۱۰ فرض می‌کنیم k عدد صحیح مثبتی باشد. ثابت کنید $x^۲ - dy^۲ = ۱$ بی‌نهایت جواب دارد که y مضربی از k است.

حل. فرض کنیم $D = k^۲d$؛ پس (۷.۱۰) ایجاب می‌کند که $x^۲ - Dy^۲ = ۱$ بی‌نهایت جواب داشته باشد. فرض می‌کنیم (a, b) یک جواب دلخواه از $x^۲ - dy^۲ = ۱$ باشد. چون

می‌توان $x^۲ - Dy^۲ = ۱$ را به‌صورت $x^۲ - d(ky)^۲ = ۱$ نوشت، در نتیجه (a, kb) جوابی از $x^۲ - dy^۲ = ۱$ است، و مسأله ثابت می‌شود.

۱۶.۱۰ فرض می‌کنیم p_i/q_i همگرای kام $\sqrt{d}$ باشد. اگر k عدد صحیح مثبتی باشد، به کمک مسألهٔ قبل نشان دهید که به‌ازای بی‌نهایت مقدار i، $k|q_i$.

حل. مسألهٔ ۱۵.۱۰ نشان می‌دهد که k تعداد نامتناهی y از جوابهای $x^۲ - dy^۲ = ۱$ را می‌شمارد. اما بنابر (۳.۱۰) هر جواب به‌صورت (p_i, q_i) است، و لذا نتیجه حاصل می‌شود.

۱۷.۱۰ فرض می‌کنیم $(x_۱, y_۱)$ جواب اصلی $x^۲ - dy^۲ = ۱$ باشد، و x_n و y_n را با $x_n + y_n\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n$ تعریف می‌کنیم. ثابت کنید به‌ازای هر عدد صحیح مثبت t، $y_n|y_{tn}$.

حل. داریم

$$x_{tn} + y_{tn}\sqrt{d} = (x_۱ + y_۱\sqrt{d})^{tn} = ((x_۱ + y_۱\sqrt{d})^n)^t = (x_n + y_n\sqrt{d})^t$$

اگر به کمک قضیهٔ دوجمله‌یی $(x_n + y_n\sqrt{d})^t$ را بسط دهیم، می‌بینیم که هر جمله بجز اولی عامل y_n دارد، و لذا $y_n|y_{tn}$.

◁ **۱۸.۱۰** بنابر (۱۰.۱۰)، هر جواب مثبت $x^۲ - dy^۲ = ۱$ به‌صورت (x_n, y_n) است، که در آن $x_n + y_n\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n$ و $(x_۱, y_۱)$ جواب اصلی است. ثابت کنید بی‌نهایت عدد اول p وجود دارد به‌طوری که به‌ازای بی‌نهایت مقدار n، $p|x_n$. (راهنمایی: از مسألهٔ ۱۵.۱۰ استفاده کنید.)

حل. ابتدا نشان می‌دهیم که به‌ازای هر گردایهٔ متناهی $\{p_۱, p_۲, \ldots, p_j\}$ از اعداد اول، یک عدد اول p ناواقع در گردایه و یک عدد صحیح n وجود دارند به‌طوری که $p|x_n$. قرار می‌دهیم $P = p_۱, p_۲, \ldots, p_j$ و تعریف می‌کنیم $D = dP^۲$. بنابر مسألهٔ ۱۵.۱۰ y_mی وجود دارد به‌طوری که $P|y_m$. چون x_m و y_m نسبت به هم اول‌اند، نتیجه می‌شود که هیچ‌کدام از $p_۱$، $p_۲$، ...، p_j نمی‌توانند x_m را بشمارند، و لذا عدد اولی مانند p ناواقع در گردایه وجود دارد که x_m را می‌شمارد.

اکنون ثابت می‌کنیم که اگر $p|x_m$، آنگاه به‌ازای بی‌نهایت مقدار i، $p|x_i$. بنابر مسألهٔ ۱۵.۱۰، به‌ازای بی‌نهایت مقدار n، $p|y_n$. اما $(x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) = x_{m+n} + y_{m+n}\sqrt{d}$،

که $x_{m+n} = x_m x_n + y_m y_n d$. لذا، اگر $p|y_n$، آنگاه $p|m+n$. (در واقع، با توجه به مسألهٔ ۱۷.۱۰، اگر $p|y_n$، آنگاه به‌ازای هر $t \geq 1$، $p|x_{m+tn}$.) بنابراین، هر عامل اول x_m، تعداد نامتناهی x_i را می‌شمارد.

مسألهٔ زیر نشان می‌دهد که می‌توان همهٔ مقادیر p_k و q_k را محاسبه کرد هرگاه مقادیرشان در اولین دورهٔ تناوب معلوم باشند.

۱۹.۱۰ گیریم p_i/q_i همگرای iام $\sqrt{d}$ باشد، و فرض می‌کنیم m طول دورهٔ تناوب $\sqrt{d}$ باشد. ثابت کنید که به‌ازای هر $i \geq -1$، $p_{i+m} + q_{i+m}\sqrt{d} = (p_i + q_i\sqrt{d})(p_{m-1} + q_{m-1}\sqrt{d})$. (راهنمایی: (۴.۱۰) را به‌کار برید.)

حل. نشان می‌دهیم که $(p_{i+m} + q_{i+m}\sqrt{d})/(p_i + q_i\sqrt{d})$ ثابت است؛ پس با قرار دادن $i = -1$ نسبت با $p_{m-1} + q_{m-1}\sqrt{d}$ برابر است، زیرا $p_{-1} = 1$ و $q_{-1} = 0$.

بنابر دوره‌یی بودن، $r_{i+m+1} = r_{i+1}$ و $s_{i+m} = s_i$. فرض می‌کنیم $\beta_k = p_k + q_k\sqrt{d}$. با استفاده از (۴.۱۰) داریم

$$\frac{\beta_{i+m}}{\beta_{i+m-1}} = \frac{r_{i+m+1} + \sqrt{d}}{s_{i+m}} = \frac{r_{i+1} + \sqrt{d}}{s_i} = \frac{\beta_i}{\beta_{i-1}}.$$

بنابراین $\beta_{i+m}/\beta_i = \beta_{i+m-1}/\beta_{i=1}$، و قضیه حاصل می‌شود.

۲۰.۱۰ با استفاده از مسألهٔ قبل ثابت کنید اگر طول دورهٔ تناوب $\sqrt{d}$ برابر m باشد، آنگاه به‌ازای هر عدد صحیح مثبت k، $p_{km-1} + q_{km-1}\sqrt{d} = (p_{m-1} + q_{m-1}\sqrt{d})^k$.

حل. مسأله برای $k = 1$ بدیهی است. بنابراین، کافی است نشان دهیم که به‌ازای هر عدد صحیح مثبت j،

$$p_{(j+1)m-1} + q_{(j+1)m-1}\sqrt{d} = (p_{jm-1} + q_{jm-1}\sqrt{d})(p_{m-1} + q_{m-1}\sqrt{d}).$$

با قرار دادن $i = jm - 1$ در مسألهٔ قبل، رابطهٔ بالا فوراً به‌دست می‌آید.

◁ **۲۱.۱۰** فرض می‌کنیم p_i/q_i همگرای iام $\sqrt{d}$ باشد. ثابت کنید به‌ازای هر عدد مفروض p_i، بی‌نهایت مقدار از j وجود دارند به‌طوری که p_j مضربی از p_i است. (راهنمایی: مسألهٔ ۱۹.۱۰، را به‌کار برید.)

حل. فرض می‌کنیم (x_n, y_n) امین جواب مثبت معادلهٔ $x^۲ - dy^۲ = ۱$ باشد. پس به‌ازای هر $i \geq ۱$، مسألهٔ ۱۹.۱۰، قضیه‌های (۶.۱۰) و (۱۰.۱۰) نشان می‌دهند که

$$p_{i+tm} + q_{i+tm}\sqrt{d} = (p_i + q_i\sqrt{d})(x_t + y_t\sqrt{d})$$

و لذا $p_{i+tm} = x_t p_i + dy_t q_i$. بنابر نتیجهٔ مسألهٔ ۱۵.۱۰، بی‌نهایت t وجود دارد به‌طوری که $p_i | y_t$، و به‌ازای هر چنین t داریم $p_i | p_{i+tm}$.

۲۲.۱۰ (الف) ثابت کنید که حاصلضرب $(r + s\sqrt{d})(u + v\sqrt{d})$ نیز به‌صورت $x + y\sqrt{d}$ است.

(ب) یادآور می‌شویم که مزدوج $\gamma = x + y\sqrt{d}$ برابر است با $\gamma' = x - y\sqrt{d}$. ثابت کنید که $(\alpha\beta)' = \alpha'\beta'$ (یعنی، مزدوج حاصلضرب برابر حاصلضرب مزدوجهاست). به‌ویژه، نشان دهید که مزدوج $(r + s\sqrt{d})^n$ برابر است با $(r - s\sqrt{d})^n$.

حل. (الف) $(r + s\sqrt{d})(u + v\sqrt{d}) = (ru + svd) + (rv + su)\sqrt{d}$.
(ب) قرار می‌دهیم $\alpha = r + s\sqrt{d}$ و $\beta = u + v\sqrt{d}$. بنابر (الف)، داریم

$$(\alpha\beta)' = (ru + svd) - (ru + su)\sqrt{d} = (r - s\sqrt{d})(u - v\sqrt{d}) = \alpha'\beta'$$

یک استدلال آسان استقرایی نشان می‌دهد که مزدوج حاصلضرب n عامل برابر است با حاصلضرب مزدوجها. به‌ویژه، مزدوج $(r + s\sqrt{d})^n$ برابر است با $(r - s\sqrt{d})^n$.

۲۳.۱۰ فرض می‌کنیم $(x_۱۰, y_۱۰)$ و همین جواب مثبت $x^۲ - ۳y^۲ = ۱$ باشد. (الف) تعیین کنید که $x_۱۰ + y_۱۰\sqrt{۳}$ بین ۵۰۰۰۰۰ و ۶۰۰۰۰۰ هست یا نه. (ب) از (۱۵.۱۰) برای یافتن $x_۱۰$ و $y_۱۰$ استفاده کنید.

حل. (الف) چون $\sqrt{۳} = \langle ۱, \overline{۱, ۲} \rangle$، طول دورهٔ تناوب $m = ۲$، و لذا، بنابر (۶.۱۰)، جواب اصلی $(p_۱, q_۱) = (۲, ۱)$. با کاربرد (۱۰.۱۰) و توضیح ۲ بعد از آن، داریم

$$x_۱۰ + y_۱۰\sqrt{۳} = (۲ + \sqrt{۳})^{۱۰} = ۵۲۴۱۷۴$$

(تا نزدیکترین عدد صحیح).

بنابر (۱۵.۱۰)، $x_۱۰$ نزدیکترین عدد صحیح به $۲/۲(۲ + \sqrt{۳})^{۱۰}$، یعنی، ۲۶۲۰۸۷ است. لذا $y_۱۰ = ۱۵۱۳۱۶$، نزدیکترین عدد صحیح به $x_۱۰/\sqrt{۳}$.

۲۴.۱۰ از (۱۵.۱۰) برای یافتن p_7/q_7، یعنی، همگرای هفتم $\sqrt{۲۰}$ استفاده کنید.

حل. داریم $\sqrt{۲۰} = \langle ۴, \overline{۲, ۸} \rangle$؛ لذا $(p_1, q_1) = (۹, ۲)$ جواب اصلی $x^۲ - ۲۰y^۲ = ۱$ است. بنابر (۶.۱۰)، (p_7, q_7) چهارمین جواب مثبت، یعنی، $(x_۴, y_۴)$ است. از این‌رو، بنابر (۱۵.۱۰)، $x_۴$ برابر است با ۵۵۱۸۴۱، نزدیکترین عدد صحیح به $(۹ + ۲\sqrt{۲۰})^۴/۲$؛ لذا $y_۴ = ۱۱۵۹۲$، نزدیکترین عدد صحیح به $x_۴/\sqrt{۲۰}$. بنابراین $p_7/q_7 = ۵۱۸۴۱/۱۱۵۹۲$.

◁ **۲۵.۱۰** فرض می‌کنیم (a, b) جواب اصلی $x^۲ - dy^۲ = ۱$ باشد.

(الف) ثابت کنید $۰ < a - b\sqrt{d} < \sqrt{۲} - ۱$.

(ب) فرض می‌کنیم طول دورهٔ تناوب $\sqrt{d}$ برابر m باشد. ثابت کنید $۰ > a - b\sqrt{d} < ۱/m$ اگر m زوج باشد و $۰ < a - b\sqrt{d} < ۱/۲m$ فرد باشد. (راهنمایی: (۳۳.۹) را به‌کار برید.)

حل. (الف) چون $a > b$، داریم $a + b\sqrt{d} > ۱ + \sqrt{d} \geq ۱ + \sqrt{۲}$. لذا

$$a - b\sqrt{d} = ۱/(a + b\sqrt{d}) < ۱/(۱ + \sqrt{۲}) = \sqrt{۲} - ۱$$

آشکار است که $a - b\sqrt{d}$ مثبت است، زیرا $(a + b\sqrt{d})(a - b\sqrt{d}) = a^۲ - db^۲ = ۱$.

(ب) بنابر (۶.۱۰)، $a = p_{m-۱}$، $b = q_{m-۱}$ یا $a = p_{۲m-۱}$، $b = q_{۲m-۱}$، برحسب آنکه m زوج یا فرد باشد. ابتدا فرض می‌کنیم m زوج باشد. بنابر (۳۳.۹)، داریم

$$a - b\sqrt{d} = b|\sqrt{d} - a/b| < q_{m-۱} \times ۱/(q_{m-۱}q_m) = ۱/q_m \leq ۱/m$$

زیرا $q_m \geq m$ (توضیح بعد از (۳.۹) را ببینید). با استدلالی مشابه، اگر m فرد باشد،آنگاه $a - b\sqrt{d} < ۱/q_{۲m} \leq ۱/۲m$.

۲۶.۱۰ ثابت کنید که مجموع نخستین n عدد صحیح به‌ازای تعداد نامتناهی عدد زوج n و به‌ازای تعداد نامتناهی عدد فرد n مربع کامل است. نخستین شش چنین عدد n را پیدا کنید.

حل. می‌دانیم $۱ + ۲ + \cdots + n = n(n+۱)/۲$؛ لذا می‌خواهیم که $n(n+۱) = ۲a^۲$. چون $(n, n+۱) = ۱$، اگر n زوج باشد، اعداد r و s را جستجو می‌کنیم به‌طوری که $n = ۲r^۲$ و $n + ۱ = s^۲$. از این‌رو $s^۲ = n + ۱ = ۲r^۲ + ۱$، و لذا r و sهایی را لازم داریم که $s^۲ - ۲r^۲ = ۱$، و این معادله بنابر (۷.۱۰) بی‌نهایت جواب دارد. با دلیلی مشابه، اگر n فرد باشد، r و sهایی را جستجو می‌کنیم که $n + ۱ = ۲r^۲$ و $n = s^۲$، یعنی، r و sهایی که $s^۲ - ۲r^۲ = -۱$، که این معادله نیز بنابر (۱۳.۱۰) بی‌نهایت جواب دارد.

بنابر (۱۳.۱۰)، نخستین سه جواب $x^۲ - ۲y^۲ = -۱$ عبارت‌اند از $(۱, ۱)$، $(۷, ۵)$، و $(۴۱, ۲۹)$، که از آنجا مقادیر ۱، ۴۹، و ۱۶۸۱ برای n به‌دست می‌آیند. همچنین، نخستین سه جواب $x^۲ - ۲y^۲ = ۱$ عبارت‌اند از $(۳, ۲)$، $(۱۷, ۱۲)$، و $(۹۹, ۷۰)$، که برای n مقادیر ۸، ۲۲۸، و ۹۸۰۰ را به‌دست می‌دهند.

۲۷.۱۰ فرض کنید (a, b) یک جواب دلخواه $x^۲ - dy^۲ = ۱$ باشد. ثابت کنید (a, b) یا جواب مثبت است اگر و تنها اگر $a + b\sqrt{d} > ۱$.

حل. اگر (a, b) یک جواب مثبت باشد، آنگاه $a + b\sqrt{d} \geq ۱ + \sqrt{d} > ۱$. حال، فرض می‌کنیم $a + b\sqrt{d} > ۱$. روشن است که a و b هر دو نمی‌توانند منفی باشند. اگر دقیقاً یکی از a و b نابزرگتر از ۰ باشد، آنگاه $|a - b\sqrt{d}| \geq |a + b\sqrt{d}|$، و لذا $|a - b\sqrt{d}||a + b\sqrt{d}| < ۱$، که با $a^۲ - dy^۲ = ۱$ تناقض دارد. در نتیجه a و b مثبت هستند.

۲۸.۱۰ آیا $x^۲ - ۲۳y^۲ = ۱$ جواب مثبتی با $۲۴ < x < ۱۱۵۱$ دارد؟

حل. نَه. چون $\sqrt{۲۳} = \langle ۴, \overline{۱, ۳, ۱, ۸} \rangle$، (۶.۱۰) ایجاب می‌کند که $(p_۳, q_۳) = (۲۴, ۵)$ جواب اصلی باشد. با توجه به (۱۰.۱۰)، چون $(۲۴ + ۵\sqrt{۲۳})^۲ = ۱۱۵۱ + ۲۴۰\sqrt{۲۳}$، جواب مثبت بعدی $(۱۱۵۱, ۲۴۰)$ است.

۲۹.۱۰ فرض می‌کنیم n عدد صحیحی (مثبت، منفی، یا صفر) باشد، و x_n و y_n را مانند (۱۰.۱۰) تعریف می‌کنیم. ثابت کنید که هر جواب $x^۲ - dy^۲ = ۱$ (با منظور کردن تمام تغییرات علامتها) به‌صورت (x_n, y_n) یا $(-x_n, -y_n)$ است.

حل. به‌ازای $n = ۰$، داریم $x_۰ + y_۰\sqrt{d} = ۱$، و لذا $x_۰ = ۱$، $y_۰ = ۰$. از این‌رو، جوابهای نمایان $(۱, ۰)$ و $(-۱, ۰)$ دقیقاً به‌ترتیب عبارت‌اند از $(x_۰, y_۰)$ و $(-x_۰, -y_۰)$. حال فرض می‌کنیم (r, s) جواب مثبت دلخواهی از $x^۲ - dy^۲ = ۱$ باشد. لذا، بنابر (۱۰.۱۰)، عدد صحیح مثبت n وجود دارد که $r = x_n$ و $s = y_n$، و جواب $(-r, -s)$ همان $(-x_n, -y_n)$ است.

چون $(x_۱ + y_۱\sqrt{d})(x_۱ - y_۱\sqrt{d}) = ۱$، داریم $x_۱ - y_۱\sqrt{d} = (x_۱ + y_۱\sqrt{d})^{-۱}$، و بنابراین $(x_{-n}, y_{-n}) = (x_۱ + y_۱\sqrt{d})^{-n} = x_n - y_n\sqrt{d}$. لذا جواب $(r_۱ - s)$ با (x_{-n}, y_{-n}) و جواب $(-r, s)$ با $(-x_{-n}, -y_{-n})$ برابرند.

وقتی که معادلهٔ دیوفانتی $x^۲ - dy^۲ = ۱$ را حل می‌کنیم، نقاط مشبکه‌ای (یعنی، نقاط با مختصات صحیح) روی هذلولی $x^۲ - dy^۲ = ۱$ را به‌دست می‌آوریم. به ارتباط نزدیک بین

فرمولهای به‌دست آمده در مسألهٔ بعد و فرمولهای معمولی $\cosh(a+b)$ و $\sinh(a+b)$، همچنین، $\cos(a+b)$ و $\sin(a+b)$، توجه کنید.

۳۰.۱۰ فرض می‌کنیم m و n اعداد صحیح مثبت باشند، و به‌ازای هر k، x_k, y_k را مطابق با (۱۰.۱۰) تعریف می‌کنیم. نشان دهید که $x_{m+n} = x_m x_n + y_m y_n d$ و

$$y_{m+n} = x_m y_n + y_m x_n$$

حل. داریم

$$\begin{aligned} x_{m+n} + y_{m+n}\sqrt{d} = (x_1 + y_1\sqrt{d})^{m+n} &= (x_1 + y_1\sqrt{d})^m (x_1 + y_1\sqrt{d})^n \\ &= (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= x_m x_n + y_n y_n d + (x_m y_n + y_m x_n)\sqrt{d} \end{aligned}$$

و نتیجه حاصل می‌شود.

توضیح. همین‌که x_1 و y_1 را بدانیم، می‌توانیم از این مسأله برای محاسبهٔ x_k و y_k به‌ازای مقادیر بزرگ k، با به‌کار بردن روش مربع کردن مکرر برای یافتن توانها، استفاده کنیم، مثلاً، برای یافتن x_{130} و y_{130}، ابتدا x_2، y_2، سپس x_4، y_4 با فرض $m = n = 2$، بعد x_8 و y_8، ...، و سرانجام x_{130}، y_{130} با فرض $m = 128$ و $n = 2$ را پیدا می‌کنیم.

۳۱.۱۰ گیریم (x_k, y_k) kامین جواب $x^2 - dy^2 = 1$ باشد. نشان دهید که

$$x_{2k}/y_{2k} = (x_k/y_k + dy_k/x_k)/2$$

(راهنمایی: مسألهٔ قبل را ببینید.)

حل. بنابر مسألهٔ ۳۰.۱۰، $x_{2k} = x_k^2 + y_k^2 d$ و $y_{2k} = 2x_k y_k$. پس از تقسیم این دو رابطه و ساده کردن نتیجه به‌دست می‌آید.

توضیح. اعداد گویای r_n را چنین تعریف می‌کنیم $r_0 = x_1/y_1$، $r_1 = x_2/y_2$، $r_2 = x_4/y_4$، $r_3 x_8/y_8$، و مانند آن. مسألهٔ قبل نشان می‌دهد که به‌طور کلی، $r_{n+1} = (r_n + d/r_n)/2$. اگر روش نیوتن، تکنیکی در حساب دیفرانسیل و انتگرالِ سال اول، را با شروع از تخمین $\sqrt{d} \approx x_1/y_1$ به‌کار بریم، r_iها دقیقاً تقریبهایی برای $\sqrt{d}$ هستند که به‌دست می‌آوریم. روش نیوتن برای ریشه‌های دوم توسط کاتالدی[1] در ۱۶۱۳ به‌طورکامل تشریح شده است.

1. Cataldi

۳۲.۱۰ ثابت کنید بی‌نهایت سه‌تایی از اعداد صحیح متوالی وجود دارد که هر یک مجموع دو مربع است. سه تا از این سه‌تاییها را به‌دست آورید.

حل. بنابر (۷.۱۰)، معادلهٔ $x^۲ - xy^۲ = ۱$ بی‌نهایت جواب مثبت دارد. اگر (a, b) یک جواب مثبت باشد، قرار می‌دهیم $n = a^۲$. پس $n + ۱ = a^۲ + ۱$ که واضح است مجموع دو مربع است، و $n - ۱ = ۲b^۲$ نیز چنین است. نخستین سه جواب مثبت عبارت‌اند از $(۲, ۳)$، $(۱۲, ۱۷)$، و $(۷۰, ۹۹)$، که به‌ترتیب، سه‌تاییهای ۸، ۹، ۱۰؛ ۲۸۸، ۲۸۹، ۲۹۰؛ و ۹۸۰۰، ۹۸۰۱، ۹۸۰۲ را به‌دست می‌دهند.

معادلهٔ $x^۲ - dy^۲ = -۱$

۳۳.۱۰ فرض می‌کنیم (p, q) یک جواب مثبت $x^۲ - dy^۲ = -۱$ باشد. ثابت کنید p/q یکی از همگراهای $\sqrt{d}$ است.

حل. چون $p^۲ - dq^۲ = -۱$، داریم $p - q\sqrt{d} = -۱/(p + q\sqrt{d})$؛ لذا

$$p/q - \sqrt{d} = -۱/q(p + q\sqrt{d})$$

آشکار است که $p \geq q$، و لذا $p + q\sqrt{d} > ۲q$. از این‌رو $|p/q - \sqrt{d}| < ۱/q(۲q) = ۱/۲q^۲$. اکنون از (۳۹.۹) نتیجه می‌شود که p/q یک همگرای $\sqrt{d}$ است.

۳۴.۱۰ فرض می‌کنیم r و s اعداد صحیح باشند، و x_n و y_n را با

$$(x_n + y_n\sqrt{d}) = (r + s\sqrt{d})^n$$

تعریف می‌کنیم. ثابت کنید که $x_n = ((r + s\sqrt{d})^n + (r - s\sqrt{d})^n)/۲$ و $y_n = ((r + s\sqrt{d})^n - (r - s\sqrt{d})^n)/۲$. (راهنمایی: از مسألهٔ ۲۲.۱۰ استفاده کنید.)

حل. مزدوج $x_n + y_n\sqrt{d}$ بنابه تعریف $x_n - y_n\sqrt{d}$ است، لذا بنابر قسمت (ب) از مسألهٔ ۲۲.۱۰ داریم $x_n - y_n\sqrt{d} = (r - s\sqrt{d})^n$. اکنون برابریها مستقیماً نتیجه می‌شوند.

۳۵.۱۰ رابطه‌های بازگشتی داده شده در (۱۱.۱۰) را برای یافتن نخستین سه جواب مثبت $x^۲ - ۱۰y^۲ = -۱$ و $x^۲ - ۱۰y^۲ = ۱$ به‌کار برید.

حل. بررسی کنید که $(۳, ۱)$ کوچکترین جواب مثبت $x^۲ - ۱۰y^۲ = -۱$ است؛ لذا بنابر (۱۱.۱۰)، $x_{n+۱} = ۳x_n + ۱۰y_n$ و $y_{n+۱} = x_n + ۳y_n$. با توجه به (۱۴.۱۰)، نخستین سه

جواب مثبت $x^۲ - ۱۰y^۲ = -۱$ به‌ازای n مساوی ۱، ۳، و ۵ با (x_n, y_n)، و نخستین سه جواب مثبت $x^۲ - ۱۰y^۲ = ۱$ متناظر با n مساوی ۲، ۴، و ۶ هستند. با استفاده از رابطه‌های بازگشتی بالا، داریم $(x_۲, y_۲) = (۱۹, ۶)$؛ $(x_۳, y_۳) = (۱۱۷, ۳۷)$؛ $(x_۴, y_۴) = (۷۲۱, ۲۲۸)$؛ $(x_۵, y_۵) = (۴۴۴۳, ۱۴۰۵)$؛ و $(x_۶, y_۶) = (۲۷۳۷۹, ۸۶۵۸)$.

۳۶.۱۰ (الف) با استفاده از (۱۵.۱۰)، نخستین دو جواب مثبت $x^۲ - ۴۱y^۲ = ۱$ و $x^۲ - ۴۱y^۲ = -۱$ را به‌دست آورید.

(ب) از قسمت (الف) برای تعیین مقدار k به‌طوری که $q_k = ۱۳۱۱۳۶۰$ استفاده کنید.

(ج) (۱۳.۱۰)، (۱۴.۱۰)، و (۱۵.۱۰) را برای یافتن $p_{۱۴}/q_{۱۴}$ به‌کار برید. (این همگرا را مستقیماً محاسبه نکنید.)

حل. (الف) داریم $\sqrt{۴۱} = \langle ۶, \overline{۲, ۲, ۱۲} \rangle$ (رسیدگی کنید)؛ لذا طول دورهٔ تناوب $\sqrt{۴۱}$ برابر است با $m = ۳$. بنابراین، کوچکترین جواب مثبت $x^۲ - ۴۱y^۲ = -۱$ عبارت است از $(x_۱, y_۱) = (p_۲, q_۲) = (۳۲, ۵)$. x_n و y_n را با $x_n + y_n\sqrt{۴۱} = \gamma^n$ تعریف می‌کنیم، که در آن $\gamma = ۳۲ + ۵\sqrt{۴۱}$؛ در این‌صورت بنابر (۱۳.۱۰)، تمام جوابهای $x^۲ - ۴۱y^۲ = -۱$ با (x_n, y_n) که n فرد است و تمام جوابهای $x^۲ - ۴۱y^۲ = ۱$ با (x_n, y_n) که n زوج است، داده می‌شوند. لذا اگر (۱۵.۱۰) را به‌کار بریم، دومین جواب مثبت $x^۲ - ۴۱y^۲ = -۱$ عبارت است از $(x_۳, y_۳) = (۱۳۱۱۶۸, ۲۰۴۸۵)$ زیرا ۱۳۱۱۶۸ نزدیکترین عدد صحیح به $\gamma^۳/۲$ است و ۲۰۴۸۵ نزدیکترین عدد صحیح به $۱۳۱۱۶۸/\sqrt{۴۱}$.

$(x_۲, y_۲) = (۲۰۴۹, ۳۲۰)$ کوچکترین جواب مثبت $x^۲ - ۴۱y^۲ = ۱$ است، زیرا ۲۰۴۹ نزدیکترین عدد صحیح به $\gamma^۳/۲$ است و ۳۲۰ نزدیکترین عدد صحیح به $۲۰۴۹/\sqrt{۴۱}$. همچنین، نزدیکترین عدد صحیح به $\gamma^۴/۲$ عدد ۸۳۹۶۸۰۱ و نزدیکترین عدد صحیح به $۸۳۹۶۸۰۱/\sqrt{۴۱}$ عدد ۱۳۱۱۳۶۰ است، لذا جواب مثبت بعدی $(x_۴, y_۴) = (۸۳۹۶۸۰۱, ۱۳۱۱۳۶۰)$ است.

(ب) مقدار y در دومین جواب مثبت $x^۲ - ۴۱y^۲ = ۱$ عدد ۱۳۱۱۳۶۰ است. اما بنابر (۱۳.۱۰) دومین جواب با $(p_{۱۱}, q_{۱۱})$ نیز ارائه می‌شود. لذا $q_{۱۱} = ۱۳۱۱۳۶۰$؛ و از آنجا $k = ۱۱$.

(ج) بنابر (۱۳.۱۰)، $(p_{۱۴}, q_{۱۴})$ سومین جواب مثبت $x^۲ - ۴۱y^۲ = -۱$ است، که بنابر (۱۴.۱۰) یا $(x_۵, y_۵)$ برابر است. اگر (۱۵.۱۰) را به‌کار بریم، $x_۵ = ۵۳۷۵۲۶۴۳۲$ و $y_۵ = ۸۳۹۴۷۵۲۵$ را به‌دست می‌آوریم. لذا $p_{۱۴}/q_{۱۴} = ۵۳۷۵۲۶۴۳۲/۸۳۹۴۷۵۲۵$ (که ضمناً، $\sqrt{۴۱}$ را تا ۱۶ رقم اعشار به‌خوبی تقریب می‌زند.)

۳۷.۱۰ قضیهٔ ۱۵.۱۰ را اثبات کنید: فرض کنیم (r,s) کوچکترین جواب مثبت $x^۲-dy^۲=-۱$ باشد هرگاه معادله جواب داشته باشد؛ در غیر این‌صورت فرض می‌کنیم (r,s) کوچکترین جواب مثبت $x^۲-dy^۲=۱$ باشد. به‌ازای $n\geq ۱$، اعداد صحیح مثبت x_n و y_n را با $x_n+y_n\sqrt{d}=(r+s\sqrt{d})^n$ تعریف می‌کنیم. در این‌صورت، x_n نزدیکترین عدد صحیح به $(r+s\sqrt{d})^n/۲$ و y_n نزدیکترین عدد صحیح به $x_n/\sqrt{d}$ است. (راهنمایی: از مسألهٔ ۳۴.۱۰ استفاده کنید.)

حل. در هر دو حالت داریم $|r^۲-ds^۲|=۱$، و لذا $(r+s|r-s\sqrt{d}|=۱$. پس، $|r-s\sqrt{d}|=۱/(r+s\sqrt{d})<۱/۲$، زیرا $r+s\sqrt{d}>۲$. مسألهٔ ۳۴.۱۰ نشان می‌دهد که به‌ازای هر $n\geq ۱$، $x_n=((r+s\sqrt{d})^n+(r-s\sqrt{d})^n)/۲$، لذا $|x_n-(r_s\sqrt{d})^n/۲|=|r-s\sqrt{d}|^n/۲<۱/۴$، بنابراین، x_n نزدیکترین عدد صحیح به $(r+s\sqrt{d})^n/۲$ است.

چون $|x_n-y_n\sqrt{d}|=|r-s\sqrt{d}|^n<۱/۲$، داریم $|y_n-x_n/\sqrt{d}|<۱/۲\sqrt{۲}<۱/۲$، و لذا y_n نزدیکترین عدد صحیح به $x_n/\sqrt{d}$ است.

توضیح. اگر از نتیجهٔ قبل برای یافتن جوابهای متوالی در یک حسابگر برنامه‌پذیر استفاده کنید، متوجه می‌شوید که نزدیکترین عدد صحیح به x به‌وضوح $[x+۱/۲]$ است.

۳۸.۱۰ (الف) با تجسس، یک جواب مثبت $x^۲-۹۹y^۲=۱$ را به‌دست آورید.

(ب) بدون یافتن بسط کسر مسلسل $\sqrt{۹۹}$، ثابت کنید که $x^۲-۹۹y^۲=-۱$ جواب صحیح مثبت ندارد.

حل. به آسانی دیده می‌شود که $(۱۰,۱)$ یک جواب $x^۲-۹۹y^۲=۱$ است. با توجه به (۱۴.۱۰)، چون (به‌وضوح) $\ldots<x_۳<x_۲<x_۱$ و $\ldots<y_۳<y_۲<y_۱$، لذا هر جواب مثبت (a,b) از $x^۲-۹۹y^۲=-۱$ بایستی در $a<۱۰$ و $b<۱$ صدق کند، که ممکن نیست. (همین نتیجه از مسألهٔ ۳۳.۱۰ و اینکه $\ldots<q_۳<q_۲<q_۱$، نیز به‌دست می‌آید. توضیح بعد از (۳.۹) را ببینید.)

به روش دیگر، اگر (x,y) یک جواب $x^۲-۹۹y^۲=-۱$ باشد، آنگاه $x^۲\equiv -۱(\mathrm{mod}\ ۳)$، که ممکن نیست، لذا معادله جواب ندارد.

۳۹.۱۰ مسألهٔ ۲۰.۱۰ را برای اثبات قضیه‌های ۱۰.۱۰ و ۱۳.۱۰ به‌کار برید.

حل. فرض کنیم (p,q) یک جواب مثبت $x^۲ - dy^۲ = \pm ۱$ باشد؛ لذا، بنابر (۳.۱۰) و مسألهٔ ۳۳.۱۰، p/q یک همگرای بسط کسر مسلسل $\sqrt{d}$ است. اگر m دورهٔ تناوب این بسط باشد، بنابر (۵.۱۰)، عدد صحیحی چون j وجود دارد به‌طوری که $p = p_{jm-۱}$ و $q = q_{jm-۱}$. از مسألهٔ ۲۰.۱۰ نتیجه می‌شود که $p + q\sqrt{d} = (p_{m-۱} + q_{m-۱}\sqrt{d})^j$. از ضرب این عبارت در مزدوجش داریم $p^۲ - dq^۲ = (p_{m-۱}^۲ - dq_{m-۱}^۲)^j$.

اگر m فرد باشد، بنابر (i.۵.۱۰) $p_{m-۱}^۲ - dq_{m-۱}^۲ = -۱$؛ لذا (p,q) جوابی از $x^۲ - dy^۲ = -۱$ است هرگاه j فرد باشد و جوابی از $x^۲ - dy^۲ = ۱$ است اگر j زوج باشد، به‌ویژه، اگر (p,q) جوابی از $x^۲ - dy^۲ = ۱$ باشد، آنگاه $p + q\sqrt{d}$ توانی از $(p_{m-۱} + q_{m-۱}\sqrt{d})^۲$ است. اگر m زوج باشد، آنگاه به همین دلیل، نتیجه می‌گیریم که $p + q\sqrt{d}$ توانی از $p_{m-۱} + q_{m-۱}\sqrt{d}$ است.

۴۰.۱۰ ثابت کنید که بی‌نهایت عدد صحیح زوج و بی‌نهایت عدد صحیح فرد n وجود دارند به‌طوری که $n^۲ + (n+۱)^۲$ مربع کامل است. نخستین پنج n را به‌دست آورید. (راهنمایی: ابتدا نشان دهید که $n^۲ + (n+۱)^۲ = k^۲$ با $(۲n+۱)^۲ - ۲k^۲ = -۱$ هم‌ارز است.)

حل. اگر معادلهٔ $n^۲ + (n+۱)^۲ = k^۲$ را در ۲ ضرب کنیم و مربع را کامل کنیم، معادلهٔ هم‌ارز $(۲n+۱)^۲ - ۲k^۲ = -۱$ را به‌دست می‌آوریم. چون $\sqrt{۲} = \langle ۱, \overline{۲} \rangle$ دارای دورهٔ تناوب فرد است، این معادله بی‌نهایت جواب دارد.

چون $(۱, ۱)$ کوچکترین جواب مثبت است، (۱۴.۱۰) ایجاب می‌کند که همهٔ جوابهای مثبت با $(۱+\sqrt{۲})^t$، که t عدد صحیح مثبت فردی است، یا به‌طور هم‌ارز، با $(۱+\sqrt{۲})(۳+۲\sqrt{۲})^s$ که s عدد صحیح نامنفی است، ارائه شوند. لذا اگر (a,b) یک جواب باشد، $(۳a+۴b, ۲a+۳b)$ جواب بعدی است. $۳a$ مؤلفهٔ اول به پیمانهٔ ۴ است، لذا اگر با $a = ۲n+۱$ شروع کنیم و توجه کنیم که $b = k$ و a آنگاه به‌طور متوالی داریم

$$۲n+۱ \equiv ۱, ۳, ۱, ۳, \ldots \pmod ۴ .$$

لذا مقادیر متناظر n به تناوب زوج و فرد هستند.

اکنون (۱۵.۱۰) را به‌کار می‌گیریم: چون تمام جوابهای مثبت با $(۱+\sqrt{۲})^t$ ارائه می‌شوند که t فرد است، لذا نخستین پنج مقدار مثبت n، با t مساوی ۳، ۵، ۷، ۹، و ۱۱ متناظر است، که عبارت‌اند از n مساوی ۳، ۲۰، ۱۱۹، ۶۹۶، و ۴۰۵۹. (با انتخاب $(a,b) = (۱, ۱)$ و محاسبهٔ مقادیر متوالی $(۳a+۴b, ۲a+۳b)$ نیز می‌توان این مقادیر را به‌دست آورد.)

توضیح. این مسأله نشان می‌دهد که بی‌نهایت سه‌تایی فیثاغورسی اولیهٔ (x, y, z) که x و y اعداد صحیح متوالی هستند و y زوج است، وجود دارند. با مسألهٔ ۱۳.۸ مقایسه کنید.

۴۱.۱۰ فرض کنید $k \geq ۲$. با نشان دادن اینکه معادلهٔ $x^۲ - (k^۲ - ۱)y^۲ = -۱$ حلپذیر نیست، ثابت کنید که بسط کسر مسلسل $\sqrt{k^۲ - ۱}$ دورهٔ تناوب زوج دارد.

حل. روشن است که $(k, ۱)$ یک جواب مثبت $x^۲ - (k^۲ - ۱)y^۲ = ۱$ است. مانند مسألهٔ ۳۸.۱۰ استدلال می‌کنیم: اگر (a, b) کوچکترین جواب مثبت $x^۲ - (k^۲ - ۱)y^۲ = -۱$ باشد، آنگاه $a < k$ و $b > ۱$، که غیرممکن است. از این‌رو، هیچ جوابی وجود ندارد، و لذا، بنابر (۱۳.۱۰)، طول دورهٔ تناوب $\sqrt{k^۲ - ۱}$ زوج است.

راه حل دیگر. چون $-۱ \equiv ۰ \text{ یا } ۱ \pmod ۴$، $k^۲ \equiv ۰ \text{ یا } ۱ \pmod ۴$، پس $x^۲ - (k^۲ - ۱)y^۲$ به پیمانهٔ ۴ همنهشت با ۰، ۱، یا ۲ است و لذا هرگز همنهشت با -۱ نمی‌شود.

۴۲.۱۰ با استدلالی نظیر استدلال راه‌حل مسألهٔ قبل نشان دهید که طول دورهٔ تناوب $\sqrt{k^۲ + ۱}$ فرد است.

حل. چون روشن است که $(k, ۱)$ یک جواب $x^۲ - (k^۲ + ۱)y^۲ = -۱$ است، بنابر (۱۳.۱۰)، نتیجه حاصل است.

۴۳.۱۰ $(۸۹, ۳)$ جواب اصلی $x^۲ - ۸۸۰y^۲ = ۱$ است. بدون محاسبهٔ بسط کسر مسلسل $\sqrt{۸۸۰}$، تعیین کنید که $x^۲ - ۸۸۰y^۲ = -۱$ جواب مثبت دارد یا نه. آیا طول دورهٔ تناوب $\sqrt{۸۸۰}$ فرد است یا زوج؟

حل. اگر (a, b) یک جواب $x^۲ - ۸۸۰y^۲ = -۱$ باشد، آنگاه $a < ۸۹$ و $b < ۳$ (راه حل تمرین ۳۸.۱۰ را ببینید). نه $y = ۱$ و نه $y = ۲$ جوابی به‌دست نمی‌دهند. لذا $x^۲ - ۸۸۰y^۲ = -۱$ حلپذیر نیست. از این‌رو بنابر (۱۳.۱۰) نتیجه می‌شود که طول دورهٔ تناوب $\sqrt{۸۸۰}$ زوج است.

به طریق دیگر، می‌توانیم به کمک همنهشتی نشان دهیم که $x^۲ - ۸۸۰y^۲ = -۱$ حلپذیر نیست. به‌طورکلی، $x^۲ - ۴dy^۲ = -۱$ حلپذیر نیست، زیرا $x^۲ \equiv -۱ \pmod ۴$ جواب ندارد.

۴۴.۱۰ اگر d عامل اولی به‌صورت $۴k + ۳$ داشته باشد، ثابت کنید که طول دورهٔ تناوب $\sqrt{d}$ زوج است.

حل. فرض می‌کنیم عدد اول q که به‌صورت $4k+3$ است d را بشمارد. لذا از $x^2-dy^2=-1$ نتیجه می‌شود که $x^2\equiv -1 \pmod q$. از این‌رو، -1 یک ماندهٔ درجهٔ دوم q است، که با (۱۱.۵) تناقض دارد. چون $x^2-dy^2=-1$ حلپذیر نیست، از (۱۳.۱۰) نتیجه می‌شود که طول دورهٔ تناوب $\sqrt{d}$ زوج است.

۴۵.۱۰ بدون محاسبهٔ بسط کسر مسلسل $\sqrt{9943}$، زوج یا فرد بودن طول دورهٔ تناوبش را تعیین کنید.

حل. چون $9943\equiv 3 \pmod 4$، مسألهٔ قبل ایجاب می‌کند که معادلهٔ $x^2-9943y^2=-1$ حلپذیر نباشد. لذا بنابر (۱۳.۱۰) دورهٔ تناوب $\sqrt{9943}$ زوج است.

۴۶.۱۰ اگر $x^2-dy^2=-1$ حلپذیر باشد و (r,s) کوچکترین جواب مثبت آن باشد، ثابت کنید که $(2r^2+1, 2rs)$ جواب اصلی $x^2-dy^2=1$ است.

حل. اگر a و b با $(r+s\sqrt{d})^2=a+b\sqrt{d}$ تعریف شوند، از (۱۴.۱۰) نتیجه می‌شود که (a,b) جواب اصلی $x^2-dy^2=1$ است. چون $r^2-ds^2=-1$، داریم

$$a-r^2+ds^2=r^2+(r^2+1)=2r^2+1$$

و $b=2rs$.

۴۷.۱۰ به کمک (۱۴.۸) نشان دهید که اگر $x^2-dy^2=-1$ دارای جواب باشد، آنگاه d یک نمایش اولیه به‌صورت مجموع دو مربع دارد.

حل. فرض کنیم $s^2-dt^2=-1$، پس $s^2\equiv -1 \pmod d$. لذا بنابر (۱۴.۸)، اعداد متباین a و b وجود دارند به‌طوری که $sa\equiv b \pmod d$ و $d=a^2+b^2$.

توضیح. همین نتیجه در قضیهٔ ۲۰.۱۰، با استفاده از ویژگیهای بسط کسر مسلسل $\sqrt{d}$ ثابت شده است. در آن قضیه، نمایش صریحی از d به‌صورت مجموع دو مربع به‌دست می‌آوریم. برای روش دیگر، که در آن کسرهای مسلسل نیز به‌کار می‌روند، مسألهٔ ۱۰.۹ را ببینید.

۴۸.۱۰ اگر p اول باشد، ثابت کنید که $x^4-361y^4=-p$ جواب صحیح مثبت ندارد.

حل. اگر (a,b) جوابی باشد، آنگاه $(a^2-19b^2)(a^2+19b^2)=-p$، و لذا $a^2+19b^2=p$، $a^2-19b^2=-1$. اما آخری جواب ندارد، زیرا بنابر (۱۱.۵)، $a^2\equiv -1 \pmod{19}$ برقرار نیست.

۴۹.۱۰ گیریم (u,v) جواب اصلی $x^۲ - dy^۲ = ۱$ باشد، و فرض می‌کنیم اعداد صحیح مثبت r و s وجود دارند به‌طوری که $(r+s\sqrt{d})^۲ = u+v\sqrt{d}$. ثابت کنید که (r,s) یک جواب مثبت $x^۲ - dy^۲ = -۱$ است، و در واقع کوچکترین جواب مثبت است. (راهنمایی: ابتدا نشان دهید $r^۲ - ds^۲ = \pm ۱$. سپس (۱۴.۱۰) را به‌کار برید.)

حل. از بسط $(r+s\sqrt{d})^۲$ نتیجه می‌گیریم $u = r^۲ + ds^۲ > r^۲ \geq r$. آشکار است که

$$(r^۲ - ds^۲)^۲ = (r+s\sqrt{d})^۲(r-s\sqrt{d})^۲ = (u+v\sqrt{d})(u-v\sqrt{d}) = ۱$$

لذا $r^۲ - ds^۲ = \pm ۱$. رابطهٔ $r^۲ - ds^۲ = ۱$ برقرار نیست، زیرا $r < u$ و (u,v) کوچکترین جواب مثبت $x^۲ - dy^۲ = ۱$ است. لذا $r^۲ - ds^۲ = -۱$.

حال، فرض می‌کنیم (a,b) کوچکترین جواب مثبت $x^۲ - dy^۲ = -۱$ باشد. بنابر (۱۴.۱۰)، $(a+b\sqrt{d})^۲ = (a+b\sqrt{d})^۲$، و لذا $u+v\sqrt{d} = (r+s\sqrt{d})^۲$. پس $r+s\sqrt{d} = a+b\sqrt{d}$، زیرا هر دو عدد مثبت‌اند، و لذا $r=a$ و $s=b$. بنابراین (r,s) کوچکترین جواب مثبت $x^۲ - dy^۲ = -۱$ است.

معادلهٔ $x^۲ - dy^۲ = N$

۵۰.۱۰ فرض می‌کنیم N یک عدد صحیح نامنفی باشد. اگر d منفی یا d یک مربع کامل باشد، ثابت کنید که معادلهٔ $x^۲ - dy^۲ = N$ تعداد متناهی جواب دارد.

حل. فرض می‌کنیم $d > ۰$. اگر $N < ۰$، روشن است که جوابی وجود ندارد، و اگر $N > ۰$ باید داشته باشیم $|x| \leq \sqrt{N}$ و $|y| \leq \sqrt{N/|d|}$. حال فرض می‌کنیم d مربع کامل باشد، مثلاً $d = m^۲$؛ پس $x^۲ - dy^۲ = (x+my)(x-my) = N$. لذا $x+my = r$ و $x-my = s$، که $N = rs$. از آنجا که به تعداد متناهی روش می‌توان N را تجزیه کرد، در نتیجه $x^۲ - dy^۲ = N$ تعداد متناهی جواب دارد.

۵۱.۱۰ فرض می‌کنیم (r,s) یک جواب مثبت $x^۲ - dy^۲ = M$ باشد و (u,v) یک جواب مثبت $x^۲ - dy^۲ = N$. (a,b) را با $a+b\sqrt{d} = (r+s\sqrt{d})(u+v\sqrt{d})$ تعریف می‌کنیم؛ لذا $a = ru+svd$ و $b = rv+su$. ثابت کنید که (a,b) یک جواب مثبت $x^۲ - dy^۲ = MN$ است.

حل. به آسانی بررسی می‌شود که $a-b\sqrt{d} = (r-s\sqrt{d})(u-v\sqrt{d})$. لذا

$$a^۲ - db^۲ = (a+b\sqrt{d})(a-b\sqrt{d}) = (r^۲ - ds^۲)(u^۲ = dv^۲) = MN$$

و از این دو، (a,b) جوابی از $x^۲ - dy^۲ = MN$ است. (این همان اتحاد برهمگوپته است.)

۵۲.۱۰ مسألهٔ قبل را برای یافتن سه جواب مثبت $x^۲ - ۱۰y^۲ = ۳۱$ به‌کار برید.

حل. با تجسس پیدا می‌کنیم که $(۳,۲)$ یک جواب $x^۲ - ۱۰y^۲ = -۳۱$ است. چون $\langle ۳,\overline{۶}\rangle = \sqrt{۱۰}$، دورهٔ تناوب $\sqrt{۱۰}$ فرد است، و لذا $x^۲ - ۱۰y^۲ = -۱$ حلپذیر است. بنابر (۱۳.۱۰) (یا با تجسس)، پیدا می‌کنیم که $(p_۰,q_۰) = (۳,۱)$، کوچکترین جواب مثبت است. برای سهولت، "ضرب" زیر را تعریف می‌کنیم: $(r,s)(u,v) = (ru+svd, rv+su)$. در این‌صورت، بنابر (۱۴.۱۰)، دو جواب مثبت بعدی عبارت‌اند از $(x_۲,y_۲) = (۳,۱)(۳,۱) = (۱۹,۶)$ و $(x_۳,y_۳) = (۳,۱)(۱۹,۶) = (۱۱۷,۳۷)$. (می‌توان این جوابها را با محاسبهٔ همگراهای $\sqrt{۱۰}$ نیز به‌دست آورد، زیرا $(x_۲,y_۲) = (q_۱,q_۱)$ و $(x_۳,y_۳) = (p_۲,q_۲)$.)

اگر هر یک از این جوابهای $x^۲ - ۱۰y^۲ = -۱$ را در جواب $(۳,۲)$ از $x^۲ - ۱۰y^۲ = -۳۱$ ضرب کنیم، جوابهای $(۲۹,۹)$، $(۱۱۷,۵۶)$، و $(۱۰۹۱,۳۴۵)$ از $x^۲ - ۱۰y^۲ = ۳۱$ را به‌دست می‌آوریم.

۵۳.۱۰ (الف) با این فرض که $(۱۳,۲)$ یک جواب $x^۲ - ۴۱y^۲ = ۵$ است، جواب دیگری از آن را به‌دست آورید. (راهنمایی: مسأله‌های ۳۶.۱۰ و ۵۱.۱۰ را به‌کار برید.)

(ب) دو جواب از $x^۲ - ۴۱y^۲ = -۵$ را پیدا کنید.

حل. (الف) کافی است که یک جواب مفروض $x^۲ - ۴۱y^۲ = ۵$ را در یک جواب $x^۲ - ۴۱y^۲ = ۱$، بر طبق فرمول داده شده در مسألهٔ ۵۱.۱۰ "ضرب" کنیم. بنابر مسألهٔ ۳۶.۱۰، $(۲۰۴۹,۳۲۰)$ یک جواب $x^۲ - ۴۱y^۲ = ۱$ است. از این‌رو

$$(۱۳,۲)(۲۰۴۹,۳۲۰) = (۱۳\times ۲۰۴۹ + ۲\times ۳۲۰\times ۴۱, ۱۳\times ۳۲۰ + ۲\times ۲۰۴۹)$$
$$= (۵۲۸۷۷,۸۲۵۸)$$

و لذا $(۵۲۸۷۷,۸۲۵۸)$ نیز یک جواب $x^۲ - ۴۱y^۲ = ۵$ است.

(ب) با استفاده از روند کار در (الف)، $(۲,۱۳)$ را در جوابهای $(۳۲,۵)$ و $(۱۳۱۱۶۸,۲۰۴۸۵)$ از $x^۲ - ۴۱y^۲ = -۱$ (مسألهٔ ۳۶.۱۰ را ببینید) "ضرب" می‌کنیم. از آنجا جوابهای زیر از $x^۲ - ۴۱y^۲ = -۵$ به‌دست می‌آیند:

$$(۱۳,۲)(۱۳۱۱۶۸,۲۰۴۸۵) = (۳۳۸۴۹۵۴,۵۲۸۶۴۱)$$

و

$$(۱۳, ۲)(۳۲, ۵) = (۸۲۶, ۱۲۹)$$

۵۴.۱۰ با به‌کار بردن مسألهٔ ۵۱.۱۰، سه جواب مثبت از $x^۲ - ۲۹y^۲ = ۵$ را به‌دست آورید به‌طوری که y هر جواب در $y > ۴۰۰۰۰$ صدق کند. (راهنمایی: مثال (۱۶.۱۰) را ببینید.)

حل. با تجسس پیدا می‌کنیم که $(۱۱, ۲)$ یک جواب (در واقع، کوچکترین جواب مثبت) از $x^۲ - ۲۹y^۲ = ۵$ است. بنابر مثال ۱۶.۱۰، $(۹۸۰۱, ۱۸۲۰)$ یک جواب $x^۲ - ۲۹y^۲ = ۱$ است؛ لذا اگر روند حل مسألهٔ قبل را دنبال کنیم، نتیجه می‌شود که

$$(۱۱, ۲)(۹۸۰۱, ۱۸۲۰) = (۲۱۳۳۷۱, ۳۹۶۲۲)$$

یک جواب $x^۲ - ۲۹y^۲ = ۵$ است.

برای یافتن جواب سومی که y آن در $y < ۴۰۰۰۰$ صدق کند، توجه می‌کنیم که ضرب یک جواب از $x^۲ - ۲۹y^۲ = -۱$ در جوابی از $x^۲ - ۲۹y^۲ = -۵$ نیز جوابی از $x^۲ - ۲۹y^۲ = ۵$ به‌دست می‌دهد. بنابر مثال (۸.۱۰)، $(۷۰, ۱۳)$ جوابی از $x^۲ - ۲۹y^۲ = -۱$ است، و چون $|-۵| < \sqrt{۲۹}$، (۱۸.۱۰) ایجاب می‌کند که جوابهای $x^۲ - ۲۹y^۲ = -۵$ در بین همگراهای $\sqrt{۲۹}$ یافت شوند. به آسانی دیده می‌شود که $(۱۶, ۳)$ جوابی از $x^۲ - ۲۹y^۲ = -۵$ است، و لذا $(۲۲۵۱, ۴۱۸) = (۷۰, ۱۳)(۱۶, ۳)$ نیز یک جواب $x^۲ - ۲۹y^۲ = ۵$ است.

۵۵.۱۰ فرض می‌کنیم $x^۲ - dy^۲ = N$ دارای جواب مثبت باشد. اگر طول دورهٔ تناوب $\sqrt{d}$ فرد باشد، ثابت کنید که $x^۲ - dy^۲ = -N$ نیز جواب صحیح مثبت دارد.

حل. چون دورهٔ تناوب $\sqrt{d}$ فرد است، بنابر (۱۳.۱۰) معادلهٔ $x^۲ - dy^۲ = -۱$ جوابی مانند (u, v) دارد. فرض کنیم (a, b) یک جواب $x^۲ - dy^۲ = N$ باشد، و r و s را با $r = au + bvd$ و $s = av + bu$ تعریف می‌کنیم. در این‌صورت بنابر اتحاد برهمگوپته، (r, s) جوابی از $x^۲ - dy^۲ = -N$ است.

۵۶.۱۰ اثبات یا رد کنید: اگر $x^۲ - dy^۲ = N$ حلپذیر نباشد، آنگاه $x^۲ - dy^۲ = -N$ حلپذیر است.

حل. درست نیست. مثلاً، اگر طول دورهٔ تناوب $\sqrt{d}$ فرد باشد، مسألهٔ قبل نشان می‌دهد که یک معادله جواب دارد اگر و تنها اگر دیگری جواب داشته باشد.

۵۷.۱۰ اثبات یا رد کنید: اگر $1 < |N| < \sqrt{d}$ و $x^2 - dy^2 = N$ حلپذیر باشد، آنگاه $x^2 - dy^2 = -N$ نیز حلپذیر است.

حل. درست نیست. مثلاً، $(9, 2)$ جواب $x^2 - 21y^2 = -3$ است، اما $x^2 - 21y^2 = 3$ جواب ندارد، زیرا اگر $a^2 - 21b^2 = 3$، آنگاه $a^2 \equiv 3 \pmod 7$، که یک تناقض است، زیرا، $(3/7) = -1$.

۵۸.۱۰ ◁ قضیهٔ ۱۸.۱۰ را ثابت کنید: اگر $|N| < \sqrt{d}$ و (r, s) یک جواب مثبت $x^2 - dy^2 = N$ باشد، آنگاه r/s یکی از همگراهای بسط کسر مسلسل $\sqrt{d}$ است. (راهنمایی: برای $N > 0$ مانند برهان (۳.۱۰) شروع کنید و (۳۹.۹) را به‌کار برید. برای $N < 0$، d را با $1/d$ تعویض کنید و مسألهٔ ۲۱.۹ را به‌کار برید.)

حل. ابتدا فرض می‌کنیم $N > 0$. پس داریم $r/s - \sqrt{d} = N/(s(r + s\sqrt{d}))$. چون $N > 0$، پس $r - s\sqrt{d} > 0$، و لذا $r > s\sqrt{d}$. بنابراین،

$$0 < r/s - \sqrt{d} < \sqrt{d}/s(2s\sqrt{d}) = 1/2s^2$$

از (۳۹.۹) نتیجه می‌شود که r/s یک همگرای $\sqrt{d}$ است.

حال، فرض می‌کنیم $N < 0$، از تقسیم معادلهٔ $r^2 - dy^2 = N$ بر $-1/d$ داریم $-N/d = (1/d)r^2 - s^2$، که در آن $-N/d > 0$. اگر مانند بالا استدلال کنیم رابطهٔ $s/r - \sqrt{1/d} = -N/dr(s + r\sqrt{1/d})$ را به‌دست می‌آوریم، و چون $s > r\sqrt{1/d}$، نتیجه می‌شود که $0 < s/r - \sqrt{1/d} < 1/2r^2$. بنابراین s/r یک همگرای $1/\sqrt{d}$ است، و لذا بنابر مسألهٔ ۲۱.۹، r/s یک همگرای $\sqrt{d}$ است.

۵۹.۱۰ گیریم d یک عدد صحیح مثبت باشد که مربع کامل نیست، و فرض می‌کنیم d بر عدد اول q که به‌صورت $4k + 3$ است بخشپذیر باشد. اگر $(N, d) = 1$ و $x^2 - dy^2 = N$ جواب داشته باشد، ثابت کنید $x^2 - dy^2 = -N$ جواب ندارد.

حل. فرض می‌کنیم a و b اعداد صحیحی باشند که $a^2 - ab^2 = N$؛ پس $a^2 \equiv N \pmod q$، و چون $(N, q) = 1$، پس N یک ماندهٔ درجهٔ دوم q است، یعنی، $(N/q) = 1$. اگر اعداد صحیح r و s وجود داشته باشند به‌طوری که $r^2 - ds^2 = -N$، آنگاه $r^2 \equiv -N \pmod q$ و لذا $(-N/q) = 1$. اما در این‌صورت ، $(-N/q) = (-1/q)(N/q) = (-1/q) = 1$،

و این یک تناقض است، زیرا ۱− یک ماندهٔ درجهٔ دوم از اعداد اول به‌صورت $4k+3$ نیست ((۱۱.۵) را ببینید).

۶۰.۱۰ اگر p_k/q_k یک همگرای $\sqrt{d}$ باشد و (p_k, q_k) یک جواب $x^2 - dy^2 = N$، ثابت کنید $|N| < 2\sqrt{d}$. (لذا، اگر (a,b) یک جواب مثبت $x^2 - dy^2 = N$ باشد و $N > 2\sqrt{d}$، آنگاه a/b نمی‌تواند یک همگرای $\sqrt{d}$ باشد.) (راهنمایی: (۵.۱۰) و مسألهٔ ۱.۱۰ را به‌کار برید.)

حل. با توجه به (۵.۱۰)، $k \geq 0$ وجود دارد به‌طوری که $|N| = s_k$، و چون بنابر مسألهٔ ۱.۱۰ داریم $s_k < 2\sqrt{d}$، لذا $|N| < 2\sqrt{d}$.

۶۱.۱۰ اگر $d = 153$ و $0 < N < \sqrt{d}$، نشان دهید که امکان حلپذیری هر دو معادلهٔ $x^2 - dy^2 = N$ و $x^2 - dy^2 = -N$ وجود دارد، گرچه $x^2 - dy^2 = -1$ حلپذیر نیست.

حل. به آسانی بازبینی می‌شود که $\sqrt{153} = \langle 12, \overline{2, 1, 2, 2, 2, 1, 2, 24} \rangle$. از این‌رو طول دورهٔ تناوب ۸ است، و لذا بنابر (۱۳.۱۰)، $x^2 - dy^2 = -1$ حلپذیر نیست. ولی، $s_1 = s_4 = 9$، و چون $s_k = (-1)^k s_k$، $p_{k-1}^2 - q_{k-1}^2$، در نتیجه $x^2 - dy^2 = 9$ و $x^2 - dy^2 = -9$ هر دو حلپذیرند.

به‌طور کلی، اگر طول دورهٔ تناوب $\sqrt{d}$ زوج باشد و اندیسهای i و j که یکی زوج و دیگری فرد است وجود داشته باشند به‌طوری که $s_i = s_j$، آنگاه، با انتخاب $N = s_i$، دو معادلهٔ $x^2 - dy^2 = N$ و $x^2 - dy^2 = -N$ حلپذیرند ولی $x^2 - dy^2 = -1$ حلپذیر نیست.

توضیح. نخستین سه مقدار d با این ویژگی عبارت‌اند از ۱۵۳، ۲۶۱، ۳۶۹؛ نخستین سه مقدار زوج عبارت‌اند از ۲۱۲، ۲۳۴، و ۲۴۴. اگر یک برنامهٔ رایانه‌یی برای یافتن چنین dهایی نوشته شود، به نظر می‌رسد که داده‌های آغازی مشخص می‌کنند که مقدار متناظر N یک مربع است (مثلاً، اگر $d = 153$، آنگاه $N = 9$). ولی، همیشه این‌گونه نیست؛ نخستین عدد زوج d با Nی که مربع نیست $d = 446$ است ($s_3 = s_6 = 15$)، و نخستین عدد فرد d با Nی که مربع نیست $d = 657$ است ($s_3 = s_6 = 27$).

۶۲.۱۰ فرض می‌کنیم (x_1, y_1) جواب اصلی $x^2 - dy^2 = 1$ باشد، و فرض می‌کنیم (u, v) کوچکترین جواب مثبت $x^2 - dy^2 = N$ باشد. u_n و v_n را با رابطهٔ زیر تعریف می‌کنیم

$$u_n + v_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n (u + v\sqrt{d}).$$

از مسألهٔ ۵۱.۱۰ نتیجه می‌شود که (u_n, v_n) نیز یک جواب مثبت $x^۲ - dy^۲ = N$ است. با مثالی نشان دهید که تمام جوابهای مثبت لزوماً به‌صورت (u_n, v_n) نیستند؛ به‌ویژه، نشان دهید که $(x_۱, y_۱)$ لزوماً جواب مثبت بعدی پس از (u, v) نیست. (راهنمایی: $x^۲ - ۲۳y^۲ = -۷$ را در نظر بگیرید.)

حل. اگر s_k را برای $\sqrt{۲۳}$ محاسبه کنیم (۲۴.۹) مانند (۲۴.۹) تعریف می‌شود)، برای kهای فرد داریم $s_k = ۷$. باکاربرد (۵.۱۰) نتیجه می‌شود که $(p_۰, q_۰) = (۴, ۱)$، $(p_۲, q_۲) = (۱۹, ۴)$، و $(p_۴, q_۴) = (۲۱۱, ۴۴)$، ... همگی جوابهای $x^۲ - ۲۳y^۲ = -۷$ هستند. $(۲۴, ۵)$ جواب اصلی $x^۲ - ۲۳y^۲ = ۱$، به آسانی به‌دست می‌آید، اما چون

$$(۲۴ + ۵\sqrt{۲۳})(۴ + \sqrt{۲۳}) = ۲۱۱ + ۴۴\sqrt{۲۳}$$

آشکار است که جواب $(۱۹, ۴)$ جا افتاده است و با این روش تولید نمی‌شود.

جواب (a, b) از $x^۲ - dy^۲ = N$ اولیه خوانده می‌شود، هرگاه a و b نسبت به هم اول باشند. اگر (a, b) یک جواب اولیه باشد، آنگاه گوییم که (a, b) به ردهٔ C_s تعلق دارد هرگاه $a \equiv sb \pmod{N}$. $(0 \le s < |N|)$. (بدون آنکه به کلیت کار خللی وارد آید، فرض می‌کنیم که s.) مسألهٔ بعد نشان می‌دهد که جوابهای متعلق به یک رده را به روش آسانی می‌توان از یکدیگر به‌دست آورد.

◁ **۶۳.۱۰** فرض می‌کنیم $(a_۱, b_۱)$ و $(a_۲, b_۲)$ جوابهای اولیهٔ $x^۲ - dy^۲ = N$ باشند که هر دو به ردهٔ C_s تعلق دارند. ثابت کنید جواب (u, v) از معادلهٔ $x^۲ - dy^۲ = ۱$ وجود دارد به‌طوری که $a_۱ + b_۱\sqrt{d} = (a_۱ + b_۱\sqrt{d})(u + v\sqrt{d})$. (راهنمایی: $a_۲ + b_۲\sqrt{d}$ را بر $a_۱ + b_۱\sqrt{d}$ تقسیم کنید.)

حل. با گویا کردن مخرج، داریم

$$\frac{a_۲ + b_۲\sqrt{d}}{a_۱ + b_۱\sqrt{d}} = \frac{(a_۲ + b_۲\sqrt{d})(a_۱ - b_۱\sqrt{d})}{a_۱^۲ - db_۱^۲}$$

$$= \frac{a_۱a_۲ - db_۱b_۲}{N} + \frac{a_۱b_۲ - b_۱a_۲}{N}\sqrt{d}.$$

فرض کنیم $u = (a_۱a_۲ - db_۱b_۲)/N$ و $v = (a_۱b_۲ - b_۱a_۲)/N$؛ پس،

$$a_۲ + b_۲\sqrt{d} = (a_۱ + b_۱\sqrt{d})(u + v\sqrt{d})$$

پس از مزدوج‌گیری و ضرب داریم $(a_1^2 - db_1^2)(u^2 - dv^2) = a_2^2 - db_2^2$، و بنابراین $N = N(u^2 - dv^2)$، یعنی، $u^2 - dv^4 = 1$. باقی می‌ماند که نشان دهیم u و v اعداد صحیح هستند.

با توجه به اینکه $a_1 \equiv sb_1 \pmod N$ و $a_1^2 - db_1^2 = N$، پیدا می‌کنیم

$$b_1^2(s^2 - d) \equiv 0 \pmod N$$

چون جواب (a_1, b_1) اولیه است، پس $(b_1, N) = 1$، و لذا $s^2 - d \equiv 0 \pmod N$. از این‌رو $a_1a_2 - db_1b_2 \equiv b_1b_2(s^2 - d) \equiv 0 \pmod N$، و بنابراین $a_1a_2 - db_1b_2$ بر N بخشپذیر است، یعنی u یک عدد صحیح است. چون $a_1b_2 - b_1a_2 \equiv sb_1b_2 - b_1sb_2 = 0 \pmod N$، v نیز عدد صحیح است. این برهان را کامل می‌کند.

توضیح. به‌ازای هر N، حداکثر $|N|$ رده از جوابهای اولیهٔ $x^2 - dy^2 = N$ وجود دارند. اگر در هر رده جوابی به‌دست آوریم، آنگاه می‌توانیم تمام جوابهای اولیه را با "ضرب" در یک جواب $x^2 - dy^2 = 1$ پیدا کنیم.

۶۴.۱۰ ثابت کنید هر جواب $x^2 - dy^2 = N$ به‌صورت (mA, mB) است که در آن (A, B) یک جواب اولیهٔ $x^2 - dy^2 = N/m^2$ است.

حل. فرض می‌کنیم (a, b) یک جواب $x^2 - dy^2 = N$ باشد، و فرض می‌کنیم $m = (a, b)$. قرار می‌دهیم $a = mA$ و $b = mB$؛ روشن است که $(A, B) = 1$. با مقدارگذاری در معادله داریم $m^2A^2 - dm^2B^2 = N$. لذا $m^2|N$، و (A, B) یک جواب اولیهٔ $x^2 - dy^2 = N/m^2$ است.

۶۵.۱۰ ثابت کنید $x^2 - 1999y^2 = -2$ جواب صحیح مثبت ندارد. (راهنمایی: (i.۱۳.۵) را به‌کار برید و توجه کنید که ۱۹۹۹ اول است.)

حل. هر جواب مثبت (a, b) بایستی در $a^2 \equiv -2 \pmod{1999}$ صدق کند، که ممکن نیست، زیرا ۱۹۹۹ به‌صورت $8k - 1$ است و بنابر (i.۱۳.۵)، -2 یک نامانده‌ٔ درجهٔ دوم از چنین عدد اولی است.

۶۶.۱۰ اگر $N = \pm1, \pm2, \pm3, \pm4$، ثابت کنید $x^4 - 9y^4 = N$ جواب صحیح مثبت ندارد.

حل. $x^4 - 9y^4$ را به‌صورت $(x^2 - 3y^2)(x^2 + 3y^2)$ تجزیه می‌کنیم و توجه می‌کنیم که اگر x و y مثبت باشند، $x^2 + 3y^2 \geq 4$. چون $x^2 - 3y^2$ بایستی عدد صحیح باشد، لذا

وقتی که $N = \pm ۱, \pm ۲, \pm ۳$ معادله جواب ندارد. اگر $(x^۲ - ۳y^۲)(x^۲ + ۳y^۲) = \pm ۴$، بایستی $x^۲ + ۳y^۲ = ۴$ و لذا $x = y = ۱$. اما در این‌صورت $x^۲ - ۳y^۲ = -۲$، که $x^۴ = ۹y^۴ = -۸$ را به ما می‌دهد.

معادلهٔ پل و مجموعهای دو مربع

۶۷.۱۰ نشان دهید که ۱۱۵۲۰۲ مجموع دو مربع متباین است، و با استفاده از تکنیک بیان‌شده در برهان (۲۰.۱۰)، یک نمایش اولیه برای ۱۱۵۲۰۲ به‌دست آورید.

حل. ابتدا با استفاده از تکنیکی که به اختصار در فصل ۹ شرح داده شد، بررسی کنید که $\sqrt{۱۱۵۲۰۲} = \langle ۳۳۹, \overline{۲, ۲, ۲, ۲, ۲, ۲, ۶۷۸} \rangle$. لذا طول دورهٔ تناوب فرد است و بنابر (۲۰.۱۰)، ۱۱۵۲۰۲ نمایشهای اولیه دارد. اکنون روش به‌کار رفته در برهان (۲۰.۱۰) را اختیار می‌کنیم. فرض می‌کنیم $\alpha_۴ = \langle \overline{۲, ۲, ۲, ۶۷۸, ۲, ۲, ۲} \rangle$. چون

$$\alpha_۰ = \sqrt{۱۱۵۲۰۲} = (۰ + \sqrt{۱۱۵۲۰۲})/۱$$

و $a_۰ = [\sqrt{۱۱۵۲۰۲}] = ۳۳۹$، می‌توانیم از (۲۴.۹) برای ساختن جدول زیر استفاده کنیم:

k	۰	۱	۲	۳	۴
r_k	۰	۳۳۹	۲۲۳	۲۴۳	۲۳۹
s_k	۱	۲۸۱	۲۳۳	۲۴۱	۲۴۱
a_k	۳۳۹	۲	۲	۲	

لذا بنابر (iii.۲۴.۹)، داریم $\alpha_۴ = (۲۳۹ + \sqrt{۱۱۵۲۰۲})/۲۴۱$، و بنابراین،

$$۱۱۵۲۰۲ = ۲۳۹^۲ + ۲۴۱^۲$$

◁ **۶۸.۱۰** با یافتن یک عدد صحیح مثبت (غیر مربع) d به‌طوری که مجموع دو مربع متباین و طول دورهٔ تناوب $\sqrt{d}$ زوج باشد، نشان دهید که عکس قضیهٔ ۲۰.۱۰ برقرار نیست.

حل. چند مثال: $\sqrt{۳۴} = \langle ۵, \overline{۱, ۴, ۱, ۱۰} \rangle$ و $۳۴ = ۳^۲ + ۵^۲$. همچنین،

$$\sqrt{۶۵۰} = \langle ۲۵, \overline{۲, ۵۰} \rangle$$

چون $۶۵۰ = ۲ \times ۵^۲ \times ۱۳$، (۱۵.۸) ایجاب می‌کند که ۶۵۰ نمایشهای اولیه داشته باشد (یعنی، $۲۳^۲ + ۱۱^۲$ و $۱۹^۲ + ۱۷^۲$). سرانجام، بررسی کنید که $\sqrt{۹۴۹۰} = \langle ۹۷, ۲, ۲, ۲, ۱۹۴ \rangle$؛ چون $۹۴۹۰ = ۲ \times ۵ \times ۱۳ \times ۷۳$، از (۱۵.۸) نتیجه می‌شود که ۹۴۹۰ یک نمایش اولیه دارد.

۶۹.۱۰ فرض کنیم d نمایش اولیه ندارد؛ به عبارت دیگر، فرض کنیم d یا بر ۴ یا بر عدد اولی به‌صورت $۴k + ۳$ بخشپذیر باشد ((۱۵.۸) را ببینید). در این‌صورت، از (۲۰.۱۰) نتیجه می‌شود که طول دورهٔ تناوب $\sqrt{d}$ زوج است. از این مطلب استفاده کنید و نشان دهید که طول دورهٔ تناوب هر یک از اعداد $\sqrt{۵۳۹۷۸۴}$ و $\sqrt{۱۶۷۲۵۱۳۸}$ زوج است.

حل. روشن است که، ۵۳۹۷۸۴ بر ۴ بخشپذیر است، لذا بنابر (۱۵.۸)، نمایش اولیه‌ای موجود نیست. (اما نمایشهای غیراولیه وجود دارند. چرا؟) از این‌رو، بنابر (۲۰.۱۰)، دورهٔ $\sqrt{۵۳۹۷۸۴}$ زوج است.

چون مجموع ارقام عدد ۱۶۷۲۵۱۳۸ بر ۳ بخشپذیر است ولی مضرب ۹ نیست، پس این عدد بر ۳ بخشپذیر است ولی بر ۹ بخشپذیر نیست. لذا (۹.۸) ایجاب می‌کند که اصلاً نمایشی وجود نداشته باشد. از این‌رو، طول دورهٔ تناوب $\sqrt{۱۶۷۲۵۱۳۸}$ زوج است.

۷۰.۱۰ فرض می‌کنیم p عدد اولی به‌صورت $۸k+۵$ باشد. نشان دهید که معادلهٔ $x^۲ - ۲py^۲ = -۱$ جواب دارد (یا هم‌ارز با آن، طول دورهٔ تناوب $\sqrt{۲p}$ فرد است). (راهنمایی: از برهان (۱۹.۱۰) تبعیت کنید، و (۱۲.۵) و (۱۳.۵) را به‌کار برید.)

حل. فرض کنیم (u, v) کوچکترین جواب صحیح مثبت $x^۲ - ۲py^۲ = ۱$ باشد. روشن است که، u فرد و v زوج است. اما $u^۲ - ۲pv^۲ = ۱$ اگر و تنها اگر $۲pv^۲ = (u-۱)(u+۱)$. چون $u+۱$ و $u-۱$ هر دو زوج‌اند و تفاضلشان ۲ است، پس $(u+۱, u-۱) = ۲$. فرض کنیم $v = ۲w$ و $u+۱ = ۲t$؛ پس $t(t-۱) = ۲pw^۲$. چهار حالت برای بررسی وجود دارد: (i) t به‌صورت $۲r^۲$ و $t-۱$ به‌صورت $ps^۲$؛ (ii) $t = ps^۲$ و $t-۱ = ۲r^۲$؛ (iii) $t = r^۲$ و $t-۱ = ۲ps^۲$؛ و (iv) $t = ۲ps^۲$ و $t-۱ = r^۲$.

در حالت (i)، داریم $۲r^۲ - ps^۲ = t - (t-۱) = ۱$. از آنجا ۲ یک ماندهٔ درجهٔ دوم p است، که با (۱۲.۵) تناقض دارد. در حالت (ii)، داریم $ps^۲ - ۲r^۲ = ۱$، و لذا ۲− یک ماندهٔ درجهٔ دوم p است، که با (i.۱۳.۵) تناقض دارد. در حالت (iii)، داریم $r^۲ - ۲ps^۲ = ۱$؛ اما $r < u$، و این یا اینکه (u, v) کوچکترین جواب مثبت $u^۲ - ۲pv^۲ = ۱$ است تناقض دارد.

لذا حالت (iv) باقی می‌ماند، یعنی $t = ۲ps^۲$ و $t - ۱ = r^۲$، و بنابراین،

$$r^۲ - ۲ps^۲ = (t - ۱) - t = -۱$$

توضیح. اگر p به‌صورت $۸k + ۱$ باشد، ممکن است طول دورهٔ تناوب $\sqrt{۲p}$ زوج باشد. مثلاً، برای $p = ۱۷$ چنین است (مسألهٔ ۶۸.۱۰ را ببینید).

در مسألهٔ بعد قسمتی از قانون تقابل مربعی با استفاده از معادلهٔ پِل ثابت می‌شود.

۷۱.۱۰ فرض می‌کنیم p و q اعداد اول به‌صورت $۴k + ۳$ باشند. با در نظر گرفتن کوچکترین جواب مثبت $x^۲ - pqy^۲ = ۱$، نشان دهید که p یک ماندهٔ درجهٔ دوم q است اگر و تنها اگر q یک ماندهٔ درجهٔ دوم p نباشد. (راهنمایی: از برهان (۱۹.۱۰) پیروی کنید.)

حل. فرض می‌کنیم (u, v) کوچکترین جواب مثبت $x^۲ - ۲pqy^۲ = ۱$ باشد. اگر همان استدلال برهان (۱۹.۱۰) را بکار بریم، به معادلهٔ $t(t - ۱) = pqw^۲$ می‌رسیم. چهار حالت برای بررسی وجود دارد: (i) t به‌صورت $r^۲$ و $t - ۱$ به‌صورت $pqs^۲$ است؛ (ii) $t = pqs^۲$ و $t - ۱ = r^۲$؛ (iii) $t = pr^۲$، $t - ۱ = qs^۲$؛ و (iv) $t = qs^۲$ و $t - ۱ = pr^۲$.

در حالت (i)، $r^۲ - pqs^۲ = ۱$ را به‌دست می‌آوریم؛ اما $r < u$، و این با اینکه (u, v) کوچکترین جواب مثبت $u^۲ - pqv^۲ = ۱$ است تناقض دارد. در حالت (ii)، داریم $r^۲ - pqs^۲ = -۱$. از آنجا -۱ یک ماندهٔ درجهٔ دوم p است، که با (۱۱.۵) تناقض دارد. در حالت (iii)، داریم $pr^۲ - qs^۲ = ۱$؛ لذا p یک ماندهٔ درجهٔ دوم q است. چون $-qs^۲ \equiv ۱ \pmod p$ و -۱ یک نامانده درجهٔ دوم p است، پس q یک نامانده درجهٔ دوم p است. در حالت (iv) نیز به طریق مشابه می‌توانیم نشان دهیم که q یک ماندهٔ p و p یک نامانده q است. چون تنها حالتهای (iii) و (iv) امکان‌پذیر هستند، نتیجه می‌شود که p یک ماندهٔ q است اگر و تنها اگر q یک نامانده p باشد.

یک کاربرد: تجزیهٔ اعداد بزرگ

۷۲.۱۰ (الف) فرض می‌کنیم $a^۲ \equiv b^۲ \pmod N$، با $۰ < b < a < N$ و $a + b \neq N$. قرار می‌دهیم $d_۱ = (a - b, N)$ و $d_۲ = (a + b, N)$. ثابت کنید $d_۱$ و $d_۲$ مقسوم‌علیه‌های سرهٔ N هستند.

(ب) اگر در قسمت (الف)، $a + b = N$، آیا $d_۱$ و $d_۲$ همواره مقسوم‌علیه‌های نمایان ۱ و N از N را به‌دست می‌دهند؟

حل. (الف) چون $1 < a - b < N$، روشن است که $d_1 = N$ برقرار نیست. همچنین، چون $2 < a + b < 2N$ و $a + b \neq N$، $d_2 = N$ را نمی‌توانیم داشته باشیم. باقی می‌ماند نشان دهیم که $d_1 = 1$ یا $d_2 = 1$ برقرار نیستند. اگر $d_1 = 1$، آنگاه $a + b \equiv 0 \pmod{N}$، که با $d_1 \neq N$ تناقض دارد. همچنین، اگر $d_2 = 1$، آنگاه $a - b \equiv 0 \pmod{N}$، که با $d_2 \neq N$ متناقض است.

(ب) نه لزوماً. مثلاً، $12^2 \equiv 3^2 \pmod{15}$ رابطهٔ $d_1 = (9, 15) = 3$ را به‌دست می‌دهد.

۷۳.۱۰ روش تجزیهٔ لژاندر را، که در (۲۲.۱۰) معرفی شده بود، برای یافتن یک مقسوم‌علیه غیرنمایان ۱۵۹۲۵ به‌کار برید.

حل. فرض می‌کنیم $N = 15925$. در این‌صورت بررسی کنید که

$$\sqrt{u} = \langle 126, 5, 6, 1, 4, 3, \ldots \rangle$$

((۲۴.۹) را ببینید). جدول زیر را ترتیب می‌دهیم:

k	۰	۱	۲	۳	۴
r_k	۰	۱۲۶	۱۱۹	۹۷	۸۴
s_k	۱	۴۹	۳۶	۱۸۱	۴۹
a_k	۱۲۶	۵	۶	۱	۴
p_k	۱۲۶	۶۳۱	۳۹۱۲	۴۵۴۳	

حال، s_kها با اندیس زوج k را که مربع کامل هستند جستجو می‌کنیم. چون $s_2 = 6^2$، پس همنهشتی $p_{k-1}^2 \equiv (-1)^k s_k \pmod{N}$ به‌صورت $631^2 \equiv 6^2 \pmod{N}$ است. با استفاده از الگوریتم اقلیدسی داریم $d_1 = (631 - 6, N) = 25$ و $d_2 = (631 + 6, N) = 637$. در واقع، $637 \times 25 = 15925$ (مسألهٔ ۷۷.۱۰ را ببینید). ملاحظه می‌کنید که در این حالت نه d_1 اولی است و نه d_2 ($637 = 49 \times 13$).

می‌توانستیم این تکنیک را برای $s_4 = 7^2$ به‌کار بریم. در این حالت، داریم $d_1 = (4543 - 7, N) = 7$ و $d_2 = (4543 + 7, N) = 2275$.

۷۴.۱۰ روش تجزیهٔ لژاندر را برای تجزیهٔ ۲۲۲۲۳ به‌کار برید.

حل. فرض کنیم $N = 22223$. با استفاده از الگوریتم بیان‌شده در (۲۴.۹) داریم،

$\sqrt{N} = \langle ۱۴۹, \overline{۱۳, ۱, ۱, ۴, ۱, ۱, ۱, ۱, ۱, ۴, ۱, ۱, ۱۳, ۲۹۸} \rangle$. حال جدول زیر را ترتیب می‌دهیم، با این قرار که برای حفظ معقول اندازه‌ها، مقادیر p_k را به پیمانهٔ N بدل می‌کنیم:

k	۰	۱	۲	۳	۴	۵	۶	۷	۸
r_k	۰	۱۴۹	۱۳۷	۲۰	۱۱۹	۱۱۳	۵۰	۷۱	۷۱
s_k	۱	۲۲	۱۵۷	۱۳۹	۵۸	۱۶۳	۱۲۱	۱۴۲	۱۲۱
a_k	۱۴۹	۱۳	۱	۱	۴	۱	۱	۱	۱
p_k	۱۴۹	۱۹۳۸	۲۰۸۷	۴۰۲۵	۱۸۱۸۷	۲۲۲۱۲	۱۸۱۷۶	۱۸۱۶۵	

نخستین s_k با اندیس زوج k که مربع است $s_۶ = ۱۱^۲$، و $p_s \equiv ۲۲۲۱۲ (\mathrm{mod}\, N)$؛ لذا $۲۲۲۱۲^۲ \equiv ۱۱^۲ (\mathrm{mod}\, N)$. اما $N = ۱۱ + ۲۲۲۱۲$، لذا این روش تنها عاملهای نمایان $d_۱ = (۲۲۲۱۲ + ۱۱, N) = N$ و $d_۱ = (۲۲۲۱۲ - ۱۱, N) = ۱$ را به‌دست می‌دهد.

سپس، $s_۸ = ۱۱^۲$ را امتحان می‌کنیم؛ پس $p_۷ \equiv ۱۸۱۶۵ (\mathrm{mod}\, N)$، و چون

$$۱۸۱۶۵ + ۱۱ \neq N$$

انتظار داریم که مقسوم‌علیه‌های سرهٔ N را به‌دست آوریم. در واقع، $d_۱ = (۱۸۱۵۴, N) = ۳۱۳$ و بنابراین $d_۲ = (۱۸۱۷۶, N) = N/۳۱۳ = ۷۱$ (مسألهٔ ۷۷.۱۰ را ببینید). ملاحظه کنید که در این مثال، مقسوم‌علیه‌های ۳۱۳ و ۷۱ هر دو اول‌اند.

دو مسألهٔ بعد بایستی به کمک رایانه انجام گیرند، زیرا در غیر این‌صورت، محاسبهٔ a_k، r_k، s_k، و p_k به‌طور معقول انجام نمی‌شود. یک برنامهٔ سادهٔ رایانه‌یی می‌تواند مربع بودن s_k را با سرعت بررسی کند و سپس به فوریت بزرگترین مقسوم‌علیه مشترک مقسوم‌علیه‌های $d_۱$ و $d_۲$ را محاسبه نماید.

۷۵.۱۰ روش تجزیهٔ لژاندر را برای تجزیهٔ ۶۲۳۸۰۹ به‌کار برید.

حل. فرض می‌کنیم $N = ۶۲۳۸۰۹$. اولین kی زوج که به‌ازای آن s_k مربع است $s_{۱۴} = ۲۷^۲$ است، و $p_{۱۳} \equiv ۶۲۳۷۸۲$. (همهٔ pـمقدارها به پیمانهٔ N تحویل شده‌اند.) ولی، چون $p_{۱۳} + ۲۷ \equiv ۰ (\mathrm{mod}\, N)$، تنها عاملهای نمایان ۱ و N را به‌دست می‌آوریم (مسألهٔ ۷۸.۱۰ را ببینید). لذا s_kی بعدی را امتحان می‌کنیم که k زوج و s_k مربع باشد. داریم $s_{۳۰} = ۴^۲$، با $p_{۲۹} \equiv ۴۶۶۳۶۶$. از آنجا مقسوم‌علیه‌های سرهٔ $d_۱ = (۴۶۶۳۶۲, N) = ۱۹۹۳$ و $d_۲ = (۴۶۶۳۷۰, N) = ۳۱۳$ حاصل می‌شوند. هر دو مقسوم‌علیه اول‌اند، و، در واقع، $N = ۳۱۳ \times ۱۹۹۳$. (در تمرین ۷۷.۱۰ ثابت می‌شود که اگر N فرد باشد، $N = d_۱ d_۲$.)

طول دورهٔ تناوب $\sqrt{N}$ برابر ۷۲۶ است. جالب است توجه کنید که در میان نخستین ۷۲۷ مقدار s_k، تعداد ۲۹ مربع به دردخور وجود دارند، که ۱۵ تای آنها یک تجزیه غیرنمایان از N به‌دست می‌دهند.

۷۶.۱۰ با کاربرد روش تجزیهٔ لژاندر ۲۶۳۳۳۸۳ را تجزیه کنید.

حل. اگر $N = ۲۶۳۳۳۸۳$، آنگاه طول دورهٔ تناوب $\sqrt{N}$ برابر ۱۱۷۸ است، و لذا انتظار داریم که تعداد زیادی s_k که مربع هستند پیدا کنیم. ولی، این مثال نشان می‌دهد که گرچه $\sqrt{N}$ تعداد زیادی s_k (با k فرد) که مربع هستند تولید می‌کند، نخستین چهار چنین s_kایی، یعنی، $s_{۲۴}$، $s_{۴۰}$، $s_{۹۲}$، و $s_{۱۴۴}$، تنها عاملهای نمایان N را به‌دست می‌دهند. این مقادیر از این قرارند ($p_{k-۱}$ به پیمانهٔ N بدل شده است): $s_{۲۴} = ۵۳^۲$، $p_{۲۳} \equiv ۵۳$ ؛ $s_{۴۰} = ۱۱^۲$، $p_{۳۹} \equiv ۲۶۳۳۳۷۳$؛ $s_{۹۲} = ۳۳^۲$، $p_{۹۱} = ۳۳$؛ و $s_{۱۴۴} = ۳^۲$، $p_{۱۴۳} = ۲۶۳۳۳۸۰$. ولی، مربع بعدی یک تجزیه تولید می‌کند: از $s_{۱۷۴} = ۳۹^۲$، $p_{۱۷۳} = ۳۶۴۳۱۱$ داریم $d_۱ = (۳۶۴۲۷۲, N) = ۷۵۸۹$ و $d_۲ = (۳۶۴۳۵۰, N) = ۳۴۷$. هم ۳۴۷ و هم ۷۵۸۹ اول‌اند، و در واقع، $۳۴۷ \times ۷۵۸۹ = ۲۶۳۳۳۸۳$. (اگر N فرد باشد، همواره $N = d_۱d_۲$، مسألهٔ ۷۷.۱۰ را ببینید.)

◁ **۷۷.۱۰** (۲۲.۱۰ را ببینید.) فرض کنید N فرد، و $c^۲ = p_{k-۱}^۲ - Nq_{k-۱}^۲$. (الف) اگر $d_۱ = (p_{k-۱} - c, N)$ و $d_۲ = (p_{k-۱} + c, N)$، ثابت کنید $N = d_۱d_۲$.

(ب) فرض می‌کنیم p^* کوچکترین ماندهٔ نامنفی $p_{k-۱}$ به پیمانهٔ N باشد؛ در این‌صورت $p^* \geq ۱$. اگر $d_۱^* = (p^* - c, N)$ و $d_۲^* = (p^* + c, N)$، ثابت کنید $N = d_۱^*d_۲^*$.

حل. می‌نویسیم $p = p_{k-۱}$؛ پس $(p - c)(p + c) = Nq^۲$. فرض می‌کنیم $N = \pi_۱^{n_۱} \cdots \pi_r^{n_r}$ تجزیهٔ N به اعداد اول باشد؛ از این‌رو، به‌ازای هر i، $\pi_i^{n_i} | (p - c)(p + c)$، و لذا حداقل n_i عامل π_i وجود دارند که بین $p - c$ و $p + c$ توزیع شده‌اند. (حداقل π_i عامل وجود دارند، زیرا قابل تصور است که $q^۲$ نیز شامل عاملهای π_i باشد.) بنابراین، در ساختن $d_۱$ و $d_۲$، حداقل $n_۱$ عامل π_i وجود دارند که بین $d_۱$ و $d_۲$ توزیع شده‌اند، و لذا $d_۱d_۲$ بر N بخشپذیر است.

اکنون نشان می‌دهیم که N بر $d_۱d_۲$ بخشپذیر است. فرض کنیم π عدد اولی باشد که $\pi | d_۱$ و $\pi | d_۲$، فرض می‌کنیم π^a بزرگترین توانی از π باشد که $d_۱d_۲$ را می‌شمارد، و فرض می‌کنیم P حاصلضرب این قبیل π^a باشد. هر π^a عدد $(p - c)(p + c)$ را می‌شمارد. (برای دیدن این

مطلب، ملاحظه کنید که $d_1|p-c$ و $d_2|p+c$، و لذا $d_1d_2|(c-p)(p+c)$ و چون $\pi^a|d_1d_2$، نتیجه حاصل است.) لذا هر π^a عدد Na^2 را می‌شمارد. همچنین، $\pi|2p$ و $\pi|2c$؛ چون $p|N$ و N فرد است، پس π نیز فرد است، و لذا $\pi|p$. اما، بنابر (۷.۹)، $(N,q)=1$، پس $\pi \nmid q$. از این‌رو نتیجه می‌گیریم که $\pi^a|N$. لذا تمام عاملهای π از d_1d_2 در N قرار دارند. با توجه به تعریف P، نتیجه می‌شود که $P|N$.

فرض می‌کنیم π تمام عاملهای اول d_1 یا d_2 (ولی نه هر دو) را طی کند و π^b بزرگترین توان π باشد که d_1d_2 را می‌شمارد؛ حاصلضرب این قبیل π^bها را Q می‌گیریم. آشکار است که P و Q نسبت به هم اول‌اند، و $d_1d_2=PQ$. چون $d_1|N$ و $d_2|N$، بایستی $Q|N$. (می‌نویسیم $Q=Q_1Q_2$، که $(Q_1,Q_2)=1$ و $Q_1|d_1$، $Q_2|d_2$. پس $Q_1|N$ و $Q_2|N$، و لذا $Q=Q_1Q_2|N$.)

بنابراین $P|N$ و $Q|N$، و چون $(P,Q)=1$، پس $PQ|N$، یعنی، $d_1d_2|N$. از طرفی ثابت کردیم که $N|d_1d_2$، لذا $N=d_1d_2$.

(ب) قرار می‌دهیم $p^*=p+Nk$. پس بنابر (۲۲.۱) داریم

$$d_1^*=(p^*-c,N)=(p+Nk-c,N)=(p-c,N)=d_1$$

همچنین $d_2^*=d_2$، و لذا بنابر قسمت (الف)، $d_1^*d_2^*=N$.

۷۸.۱۰ عطف به (۲۲.۱۰) روش تجزیهٔ لژاندر. فرض می‌کنیم N یک عدد صحیح مثبت فرد باشد. اگر k زوج، $s_k=c^2$، و $p_{k-1}\equiv\pm c(\bmod N)$، ثابت کنید که $d_1=(p_{k-1}-c,N)$ و $d_2=(p_{k-1}+c,N)$ (به‌ترتیبی) همان مقسوم‌علیه‌های نمایان ۱ و N از N هستند.

حل. آسانترین راه اثبات این مطلب استفاده از مسألهٔ قبل است. اگر $p=p_{k-1}$، آنگاه $p\equiv\pm c(\bmod N)$ ایجاب می‌کند که یا $p-c$ مضربی از N باشد یا $p+c$. از این‌رو، یا $d_1=N$ یا $d_2=N$، و لذا بنابر مسألهٔ ۷۷.۱۰، به‌ترتیب، $d_2=1$ یا $d_1=1$.

می‌توان مسأله را مستقیماً به‌ترتیب زیر حل کرد: بنابر (i.۵.۱۰) داریم $p^2-Nq^2=c^2$، یعنی، $(p-c)(p+c)=Nq^2$. اگر $p\equiv c(\bmod N)$، آنگاه $d_1=(p-c,N)=N$. اکنون نشان می‌دهیم که $d_2=1$. اگر $\pi|p+c$ و $\pi|N$، آنگاه چون $N|p-c$، پس $\pi|2p$ و چون N فرد است، پس $\pi|p$. فرض کنیم $p-c=mN$، پس $mN(p+c)=Nq^2$، و لذا $m(p+c)=q^2$. چون $\pi|p+c$، در نتیجه $\pi|q$، و این با $(p,q)=1$ تناقض دارد ((۱۷.۹)

را ببینید). پس هیچ عدد اول π هر دو عدد $p+c$ و N را عاد نمی‌کند، یعنی $d_2 = 1$. به روش مشابه، می‌توانیم نشان دهیم که اگر $p \equiv -c \pmod N$، آنگاه $d_2 = N$ و $d_1 = 1$.

۷۹.۱۰ یک عدد زوج N بیابید به‌طوری که $N \neq d_1 d_2$، که در آن d_1 و d_2 مقسوم‌علیه‌های N هستند که از روش تجزیهٔ لژاندر به‌دست می‌آیند. آیا اگر N زوج باشد $N = d_1 d_2$ امکان‌پذیر است؟ (راهنمایی: اعداد $N = 78$ و $N = 48$ را در نظر بگیرید.)

حل. فرض می‌کنیم $N = 78$. پس $\sqrt{78} = \langle 8, \overline{1, 4, 1, 16} \rangle$، و به آسانی دیده می‌شود که $s_4 = 1$، $p_3 = 53$ جوابی از همنهشتی لژاندر است. از آنجا $d_1 = (52, 78) = 26$ و $d_2 = (54, 78) = 6$، به‌طوری که $d_1 d_2 = 2N$.

اگر N زوج باشد $N = d_1 d_2$ امکان‌پذیر است. اگر $N = 48$، آنگاه از $s_1 = 1$، $p_0 = 6$ داریم $d_1 = (6, 48) = 6$ و $d_2 = (8, 48) = 8$. در واقع، به‌ازای یک N، بسته به مقادیر s_k و p_{k-1}، امکان دارد که $d_1 d_2 = N$ یا $d_1 d_2 = 2N$. مثلاً اگر $N = 88$، آنگاه $s_2 = 9$، $p_1 = 19$ ایجاب می‌کند $d_1 d_2 = 2N = 22 \times 8$، حال آنکه از $s_4 = 9$، $p_3 = 47$ نتیجه می‌شود $d_1 d_2 = N = 44 \times 2$.

۸۰.۱۰ با مثالی نشان دهید که اگر N فرد باشد و $a^2 \equiv b^2 \pmod N$، با $0 < b < a < N$ و $a+b \neq N$، آنگاه $d_1 d_2$ لزوماً برابر N نیست، که در آن $d_1 = (a-b, N)$ و $d_2 = (a+b, N)$. چرا برهان مسألهٔ ۷۷.۱۰ در اینجا کاربرد ندارد؟

حل. مثلاً، $21^2 \equiv 6^2 \pmod{135}$ را در نظر می‌گیریم. لذا $d_1 = (15, 135) = 15$ و $d_2 = (27, 135) = 27$، اما $d_1 d_2$ با ۱۳۵ برابر نیست. استدلال به‌کار رفته در حل مسألهٔ ۷۷.۱۰ در اینجا مورد ندارد، زیرا در مسألهٔ ۷۷.۱۰ داریم $p^2 - a^4 = Nq^2$، که در آن p و q نسبت به هم اول‌اند. (لذا، از کاربرد ویژهٔ این مطلب استفاده کرده‌ایم که اگر p/q یک همگرای $\sqrt{N}$ باشد، آنگاه $(p, q) = 1$.) ولی، در این مثال، $3 \times 135 = 21^2 - 6^2$، که ۳ نه با ۲۱ متباین است و نه با ۶.

عاملهای تقویت‌کننده. طول دورهٔ تناوب $\sqrt{N}$ ممکن است بسیار کوتاهتر از آن باشد که تعداد کافی از مقادیر s_k که مربع هستند تولید کند؛ مثلاً، به‌ازای هر $n \geq 1$، $\sqrt{n^2+1} = \langle n, \overline{2n} \rangle$. در حالتهای دیگری، ممکن است که دورهٔ تناوب طولانی باشد اما امکان دارد که شامل هیچ s_kی مربع، مثلاً، در بررسی نخستین ۵۰۰ مقدار، که به تولید عاملهای سرهٔ N منجر می‌شوند، نباشد. در هر دو حالت، می‌توانیم N را در عامل تقویت‌کنندهٔ D ضرب کنیم و سپس روش تجزیهٔ لژاندر

را در مورد $\sqrt{DN}$ به‌کار بریم. برای بسط دورهٔ تناوب $\sqrt{N}$ به یک مقدار قابل توجه، لازم نیست که عامل تقویت‌کننده زیاد بزرگ باشد؛ در واقع، $D = ۳$ و $D = ۵$ معمولاً تجزیهٔ مورد نظر را تولید می‌کنند. اگر D را فرد اختیار کنیم، مسألهٔ ۷۷.۱۰ نشان می‌دهد که برای DN تنها محاسبهٔ $d_۱$ لازم است، زیرا در این‌صورت $d_۲ = DN/d_۱$.

۸۱.۱۰ روش تجزیهٔ لژاندر را با عامل تقویت‌کنندهٔ ۳ برای تجزیهٔ ۱۲۶۷۸۷۷ به‌کار برید. کار را با عامل تقویت‌کنندهٔ ۵ تکرار کنید.

حل. فرض کنیم $N = ۱۲۶۷۸۷۷$؛ پس $\sqrt{N} = \langle ۱۱۲۶, \overline{۲۲۵۲} \rangle$. (در واقع، $N = ۱۱۲۶^۲ + ۱$.) چون طول دورهٔ تناوب است، الگوریتم لژاندر هیچ مقسوم‌علیهٔ سره از N تولید نمی‌کند. اکنون اگر عامل تقویت‌کنندهٔ ۳ را به‌کار بریم، آنگاه $\sqrt{۳N}$ دارای دورهٔ تناوبی به طول ۸۰ است، و روش تجزیهٔ لژاندر (با مقادیر p_k که به پیمانهٔ $۳N$ تحویل شده‌اند) $s_۶ = ۸۴۱ = ۲۹^۲$، $p_۵ = ۱۹۵۰۲۹$ را ارائه می‌دهد. چون $p_۵ \not\equiv \pm ۲۹ (\mathrm{mod}\, ۳N)$، لذا با محاسبهٔ $d_۱ = (۱۹۵۰۰۰۰, ۳N) = ۳۹$ و $d_۲ = ۳N/d_۱ = ۹۷۵۲۹$ مقسوم‌علیه‌های سرهٔ $۳N$ را به‌دست می‌آوریم. لذا N به‌صورت ۹۷۵۲۹×۱۳ تجزیه می‌شود (توجه کنید که ۹۷۵۲۹ اول نیست: $۹۷۵۲۹ = ۱۷ \times ۵۷۳۷$.)

اگر عامل تقویت‌کنندهٔ ۵ را به‌کار بریم، آنگاه $\sqrt{۵N}$ دورهٔ تناوبی به طول ۵۵ دارد، و الگوریتم مورد نظر $s_{۱۲} = ۱۶^۲$، $p_{۱۱} = ۴۸۷۶۴۶۶$ را به‌دست می‌دهد. لذا $d_۱ = (۴۸۷۶۴۶۶ - ۱۶, ۵N) = ۴۸۷۶۴۵$ و از این‌رو $d_۲ = ۵N/d_۱ = ۱۳$. بنابراین N حاصلضرب $d_۱/۵ = ۹۷۵۲۹$ و ۱۳ است.

۸۲.۱۰ فرض می‌کنیم روش تجزیهٔ لژاندر با یک عامل تقویت‌کنندهٔ D که عدد اول فردی است به‌کار رفته باشد، و فرض می‌کنیم که عدد N که بایستی تجزیه شود به D بخشپذیر نباشد. (مثلاً اگر $p = ۳$، امتحان کنید که مجموع ارقام N مضربی از ۳ نباشد.) فرض می‌کنیم P و C مقادیر $p_{k-۱}$ و $\sqrt{s_k}$ برای DN باشند به‌طوری که $p_{k-۱} \not\equiv \pm c (\mathrm{mod}\, DN)$. اگر $d_۱ = (P - C, N)$ و $d_۲ = (P + C, N)$، ثابت کنید که $d_۱ d_۲ = N$.

حل. فرض کنیم $D_۱ = (P - C, DN)$ و $D_۲ = (P + C, DN)$؛ لذا بنابر مسألهٔ ۷۷.۱۰، $D_۱ D_۲ = DN$. چون D اول است، پس دقیقاً یکی از $D_۱$ و $D_۲$ بر D بخشپذیر است. فرض کنیم $D | D_۱$، پس $D \nmid D_۲$ و لذا $D \nmid P + C$. بنابراین

$$D_۲ = (P + C, DN) = (P + C, N) = d_۲$$

همچنین، چون $D \nmid P-C$ و $D \nmid N$ داریم $D_1=(P-C,DN)=D(P-C,N)=Dd_1$. بنابراین $DN = D_1D_2 = Dd_1d_2$، و لذا $N = d_1d_2$. همچنین، اگر $D|D_2$، آنگاه $D_1 = d_1$ و $D_2 = Dd_2$، و لذا $N = d_1d_2$.

توضیح. فرض می‌کنیم $P \not\equiv \pm C \pmod{DN}$. مسألهٔ قبل نشان می‌دهد که اگر عامل تقویت‌کننده عدد اولی باشد که N را نشمارد، آنگاه برای یافتن مقسوم‌علیه‌های N، به جای آنکه ابتدا عاملهای DN را با محاسبهٔ $(P-C,DN)$ یا $(P+C,DN)$ حساب کنیم، کافی است که مستقیماً $(P-C,N)$ یا $(P+C,N)$ را محاسبه نماییم. اگر این مطلب را در مسألهٔ ۸۱.۱۰ به‌کار بریم، برای عامل تقویت‌کنندهٔ ۳، داریم $d_1 = ۱۳$ و $d_2 = ۹۷۵۲۹$؛ و برای عامل تقویت‌کنندهٔ ۵، داریم $d_1 = ۹۷۵۲۹$ و لذا $d_2 = ۱۳$.

۸۳.۱۰ اگر بخواهیم دقیق شویم، کاربرد عامل تقویت‌کنندهٔ D، عاملهای سرهٔ DN را تولید می‌کند. اما ممکن است که این عاملها فقط D یا N باشند و لذا تنها عاملهای نمایان ۱ و N از N را به‌دست دهند. این مطلب را با کاربرد روش تجزیهٔ لژاندر در مورد $N = ۴۰۹۷$ و عامل تقویت‌کنندهٔ $D = ۳$ ثابت کنید.

حل. بررسی می‌کنیم که $\sqrt{N}$ دورهٔ تناوبی به طول ۱ دارد (زیرا $۴۰۹۷ = ۶۴^۲ + ۱$)، اما طول دورهٔ $\sqrt{۳N}$ برابر ۳۴ است. با کاربرد روش تجزیهٔ لژاندر، در مورد $۳N$ داریم $s_۶ = ۲۵$ و $p_۵ = ۴۱۰۲$. لذا برای $۳N$ مقسوم‌علیه‌های $d_۱ = (۴۰۹۷, ۳N) = N$ و $d_۲ = ۳N/d_۱ = ۳$ را به‌دست می‌آوریم، که تنها عاملهای ۱ و N از N را ارائه می‌دهد.

ولی، جفت قابل استفادهٔ بعدی برای $۳N$ عبارت است از $s_{۱۰} = ۱۲۱$ و $p_۹ = ۹۱۶۹$، که $d_۱ = ۲۴۱$ و $d_۲ = ۵۱$ را به‌دست می‌دهد. از آنجا تجزیهٔ غیرنمایان $N = ۲۴۱ \times ۱۷$ به‌دست می‌آید.

۸۴.۱۰ مقادیر غیرمربع s_k را برای تجزیهٔ ۳۴۵۷۹ به‌کار برید. (قسمت آخرِ بخش مربوط به روش تجزیهٔ لژاندر را ببینید.)

حل. فرض کنیم $N = ۳۴۵۷۹$؛ پس

$$\sqrt{N} = \langle ۱۸۵, \overline{۱, ۲۰, ۱, ۷, ۳, ۴, ۲, ۴, ۳, ۷, ۱, ۲۰, ۱, ۳۷۰} \rangle$$

و لذا طول دورهٔ تناوب ۱۴ است. اگر به وسط دورهٔ تناوب برویم، می‌بینیم که $s_۶ = s_۸ = ۷۸$؛ سپس به پیمانهٔ N داریم $p_۵ = ۳۲۵۵۹$ و $p_۷ = ۱۲۳۲۵$. چون $p_۵^۲ \equiv s_۶$ و $p_۷^۲ \equiv s_۸ (\mathrm{mod} N)$،

در نتیجه $(p_۵p_۷)^۲ \equiv s_۶s_۸ (\mathrm{mod}\, N)$، یعنی $۳۸۰^۲ \equiv ۷۸^۲ (\mathrm{mod}\, N)$. از این‌رو، $d_۱ = (۳۸۰ - ۷۸, N) = (۳۰۲, N) = ۱۵۱$، و لذا $d_۲ = N/۱۵۱ = ۲۲۹$. بنابراین ۳۴۵۷۹ به‌صورت ۲۲۹ × ۱۵۱ تجزیه می‌شود.

توضیح. تنها s_kهای مربع قابل استفاده در اولین دورهٔ تناوب، آخرین مقدار، یعنی، $s_{۱۴} = ۱$ است. چون $p_{۱۳} \equiv ۷۰۹۸ (\mathrm{mod}\, N)$، داریم $d_۱ = (۷۰۹۷, N) = ۱۵۱$ و لذا $d_۲ = N/d_۱ = ۲۲۹$.

تمرینهایی برای فصل ۱۰

۱. صورت کلی یک جواب مثبت از $x^۲ - ۱۱y^۲ = ۱$ را برحسب همگراهای $\sqrt{۱۱}$ به‌دست آورید، و کوچکترین جواب مثبت را تعیین کنید.

۲. جواب مثبت یکتای (a, b) از $x^۲ - ۱۴y^۲ = ۱$ را پیدا کنید به‌طوری که $۱۰^۸ < a + b\sqrt{۱۴} < ۱۰^۶$.

۳. چهارمین جواب مثبت $x^۲ - ۷y^۲ = ۱$ را به‌دست آورید.

۴. (الف) کوچکترین جواب مثبت $x^۲ - ۸۹y^۲ = ۱$ و $x^۲ - ۸۹y^۲ = -۱$ را به‌دست آورید.
(ب) جواب مثبت بعدی را در هر معادله تعیین کنید.

۵. چه تعداد از جوابهای مثبت (a, b) از $x^۲ - ۱۳y^۲ = -۱$ در ویژگی زیر صدق می‌کنند:

$$۱۰^۵ < a + b\sqrt{۱۳} < ۱۰^{۱۵}$$

۶. سومین جواب مثبت $x^۲ - ۸y^۲ = ۱$ چیست؟

۷. جواب اصلی $x^۲ - ۵y^۲ = -۱$ برابر $(۲, ۱)$ است. از این جواب برای یافتن همگرای هفتم $p_۷/q_۷$ از $\sqrt{۵}$ استفاده کنید.

۸. اگر (a, b) جواب مثبتی از $x^۲ - ۳y^۲ = ۱$ باشد، ثابت کنید که a بر هیچ عدد اول به‌صورت $۶k + ۵$ بخشپذیر نیست. (راهنمایی: (۱۰.۵) و (۱۳.۵) را به‌کار برید.)

۹. اثبات یا رد کنید: اگر $x^۲ - dy^۲ = -۱$ حلپذیر باشد، آنگاه به‌ازای هر عدد فرد $n \geq ۱$ معادلهٔ $d^۲ - d^n y^۲ = -۱$ حلپذیر است.

۱۰. بسط کسر مسلسل $\sqrt{۲۹}$ را حساب، و ثابت کنید که به‌ازای بی‌نهایت مقدار k، طول دورهٔ تناوب $k\sqrt{۲۹}$ برابر ۱ است. (راهنمایی: بنابر مسألهٔ ۲۴.۹، طول دورهٔ تناوب $\sqrt{n^۲ + ۱}$ برابر ۱ است.)

۱۱. بی‌نهایت سه‌تایی از اعداد صحیح متوالی وجود دارند به‌طوری که هر یک مجموع دو مربع است. همهٔ سه‌تاییهایی را که یک عنصرشان بین ۱۰۰۰۰۰ و ۴۰۰۰۰۰ است به‌دست آورید.

۱۲. (الف) با تجسس، کوچکترین جواب مثبت $x^۲ - ۸۹۹y^۲ = ۱$ را پیدا کنید.

(ب) بدون محاسبهٔ بسط کسر مسلسل $\sqrt{۸۹۹}$، بیان کنید که چرا $x^۲ - ۸۹۹y^۲ = -۱$ حلپذیر نیست. آیا طول دورهٔ تناوب $\sqrt{۸۹۹}$ فرد است یا زوج؟

۱۳. ثابت کنید بی‌نهایت عدد صحیح مثبت n وجود دارند به‌طوری که $n/۳ + ۱$ و $n + ۱$ هر دو مربع کامل‌اند. نخستین دو عدد این چنینیِ n را پیدا کنید.

۱۴. با تجسس، کوچکترین جواب مثبت $x^۲ - ۱۴۳y^۲ = ۱$ را پیدا کنید. از این جواب برای تعیین حلپذیری $x^۲ - ۱۴۳y^۲ = -۱$ استفاده کنید.

۱۵. نشان دهید که $x^۲ - ۱۹۹۵y^۲ = -۱$ جواب مثبت ندارد. آیا طول دورهٔ تناوب $\sqrt{۱۹۹۵}$ فرد است یا زوج است؟

۱۶. اثبات یا رد کنید: طول دورهٔ تناوب $\sqrt{۵۰۰۰۰۰۰۷}$ زوج است. (کسر مسلسل $\sqrt{۵۰۰۰۰۰۰۷}$ را محاسبه نکنید!)

۱۷. ثابت کنید که $x^۴ + ۱۲۱y^۴ = -۴۵$ جواب مثبت ندارد. (راهنمایی: ابتدا نشان دهید که طول دورهٔ تناوب $\sqrt{۱۱}$ زوج است.)

◁ ۱۸. نشان دهید که $x^۵ - ۴۴۱y^۴ = -۵۹۹۱$ جواب مثبت ندارد.

۱۹. با امتحان کردن، یک جواب مثبت برای $x^۲ - ۱۲y^۲ = ۱$ و $x^۲ - ۱۲y^۲ = ۱۳$ پیدا کنید. از اینها برای یافتن جواب مثبت دیگری برای $x^۲ - ۱۲y^۲ = ۱۳$ استفاده کنید.

◁ ۲۰. پنج جواب مثبت $x^۲ - ۱۷y^۲ = -۸$ را به‌دست آورید به‌طوری که در هر جواب $y < ۴۰۰۰$.

۲۱. ثابت کنید $x^۲ - ۳۱۱y^۲ = ۵$ جواب مثبت ندارد. (راهنمایی: (۱۳.۵) را به‌کار برید.)

۲۲. حلپذیری $x^۲ - ۳۱۳y^۲ = ۵$ را بررسی کنید.

۲۳. اثبات یا رد کنید: اگر (r, s) جواب مثبتی از $x^۲ - ۵۱۹y^۲ = -۱۴$ باشد، آنگاه r/s یک همگرای $\sqrt{۵۱۹}$ است.

۲۴. تکنیک توصیف‌شده در برهان (۲۰.۱۰) را برای یافتن یک نمایش اولیهٔ ۲۱۴۳۷ به‌صورت مجموع دو مربع به‌کار برید.

۲۵. (۲۰.۱۰) را برای یافتن نمایشی از ۸۴۹۲۲ به‌صورت مجموع دو مربع متباین، به‌کار برید.

۲۶. بدون محاسبهٔ بسط کسر مسلسل $\sqrt{۷۹۳۲۶۸}$ و $\sqrt{۱۷۵۹۲۵۱}$ نشان دهید که طول دورهٔ تناوب آنها زوج است.

۲۷. روش تجزیهٔ لژاندر را برای تجزیهٔ ۴۹۳۸۷ به‌کار برید.

۲۸. روش تجزیهٔ لژاندر را برای یافتن یک مقسوم‌علیه سرهٔ ۲۴۵۶۹ به‌کار برید.

۲۹. با استفاده از روش تجزیهٔ لژاندر عدد ۸۳۷۳۱ را تجزیه کنید.

ملاحظاتی برای فصل ۱۰

۱. می‌توان جوابهای دیگر معادلهٔ پل را یا با استفاده از فرمول بازگشتی (قضیهٔ ۱۱.۱۰ و مسألهٔ ۳۰.۱۰ را ببینید) یا با تعیین نزدیکترین عدد صحیح به $(r+s\sqrt{d})^n$، که در آن (r,s) کوچکترین جواب مثبت است (قضیهٔ ۱۵.۱۰)، به‌دست آورد. از نظر محاسبه، الگوریتم «نزدیکترین عدد صحیح» بر دقت حسابگر یا رایانهٔ مورد استفاده به سرعت برتری می‌جوید. ولی، تعریفهای بازگشتی این محدودیت را ندارند، زیرا تمام محاسبات در حساب اعداد صحیح انجام می‌شوند.

در یک رایانه (برخلاف یک حسابگر)، تفاوت واقعی در سرعت بین دو روش وجود ندارد، اما روش بازگشتی برتری دارد، زیرا حساب با ممیز شناور به‌طور ذاتی وقتی کمتر از حساب اعداد صحیح دارد. به هر حال، اگر یک حسابگر برای یافتن جوابهای دیگر به‌کار رود (مثلاً در یک امتحان)، مفید بودن (۱۵.۱۰) بدیهی است.

۲. وقتی که مقادیر p_{m-1} و q_{m-1} معلوم باشند، قضیه‌های ۱۳.۱۰ و ۱۴.۱۰ نشان می‌دهند که می‌توان مقادیر $p_{jm-1}(j \geq 1)$ را بر طبق رابطهٔ $(p_{m-1}+q_{m-1})^j = p_{jm-1}+q_{jm-1}\sqrt{d}$ محاسبه کرد. در واقع، می‌توان تمام مقادیر p_k و q_k را تعیین نمود هرگاه مقادیرشان در اولین دورهٔ تناوب معلوم باشند:

$$p_{i+m}+q_{i+m}\sqrt{d}=(p_i+q_i\sqrt{d})(p_{m-1}+q_{m-1}\sqrt{d})$$

برای یک برهان از این مطلب، مسألهٔ ۱۹.۱۰ را ببینید.

۳. **تجزیهٔ اعداد بزرگ.** روش تجزیهٔ لژاندر واقعاً یک تکنیک خیلی قدیمی است، که به نیمهٔ دوم سدهٔ هجدهم برمی‌گردد. به هر حال، قبل از اختراع رایانه‌های سریع، واقعاً یک الگوریتم عملی برای استفاده نبود، زیرا در حالت کلی، برای یک عدد بزرگ N، تعداد زیادی محاسبه برای یافتن s_kهایی که مربع کامل هستند ضرورت دارد.

علاوه بر روش تجزیهٔ لژاندر (۲۲.۱۰)، تعداد دیگری الگوریتهای تجزیهٔ بااهمیت، از جمله روش فرما، روش اویلر، و روش گاوس، وجود دارند که مفاهیم مشابه را به‌کار می‌برند (کتاب ه. ریزل[1] را که در مراجع فهرست شده است ببینید). یک کاربرد به‌ویژه مؤثر از الگوریتم کسر مسلسل در روش شانک[2] ظاهر می‌شود. این مطلب نیز در کتاب ریزل، در قسمتی که یک برنامهٔ **پاسکال** برای استفاده از الگوریتم ارائه شده است، بحث می‌شود. سرانجام، به ذکر یک الگوریتم تجزیهٔ منتسب به مورسین[3] و بری‌لارت[4] می‌پردازیم، این الگوریتم نیز روی کسرهای مسلسل پایه‌گذاری شده است و خیلی کارآمد است. برخلاف روش لژاندر و روش شانک، که در آنها مقادیر متوالی s_k

1. H. Riesel 2. Shank 3. Morrison 4. Brillhart

محاسبه می‌شوند تا یک مربع یافت شود، این الگوریتم s_kهای مختلف را ترکیب می‌کند تا یک مربع بسازد، لذا ممکن است وقت خیلی کمتری برای تولید یک تجزیه لازم باشد.

یک برنامهٔ نسبتاً کوتاه کوئیک‌بیسیک[1] که روش تجزیهٔ لژاندر را به‌کار می‌برد و از عاملهای تقویت‌کننده استفاده می‌کند در مقالهٔ «یک روش کسر مسلسل برای تجزیهٔ اعداد بزرگ» توسط رابرت. ا. کوری[2] در مجلهٔ *Pi Mu Epsilon* (مجلد ۹، شمارهٔ ۱، سال ۱۹۸۹) ارائه شده است. این مقاله همچنین شامل جدولی از اعداد بزرگ، عاملهای آنها، تعداد s_kهای مربع که این برنامه تا یافتن تجزیهٔ سره بررسی می‌کند، و اندیسهای k که این تجزیه را تولید می‌کند، است. این برنامه بر روی هر رایانه شخصی سازگار با IBM قابل اجراست.

شرح مختصری از زندگینامه

بهاسکره، معروف به بهاسکره آچریه[3] (بهاسکره دانا)، مشهورترین منجم و ریاضیدان دورهٔ پیش‌مدرن است. در ۱۱۱۴ در شهر بیجاپور از ایالت میسور[4] هندوستان به دنیا آمد. مشهورترین کار بهاسکره، سیدهانته‌شیرومَنی[5]، در ۱۱۵۰ نوشته شد. نخستین دو مجلد، که لیلاوتی[6] و بیجگنیته[7] نامیده می‌شوند، کتابهای درسی در حساب و جبر هستند، و بقیه در ارتباط با ریاضیات نجوم است.* همان‌گونه که در آن دوران معمول بود تمام کار به‌صورت نظم نوشته شده است.

کتاب لیلاوتی شامل حساب پایه‌یی و هندسه است، همچنین، گردایهٔ وسیعی از مسائل تفریحی را که به سبک تخیلی زیبایی نوشته شده است در بردارد. (داستانی، که معلوم نیست راست باشد، وجود دارد که بهاسکره دختری به نام لیلاوتی داشته است که زود بیوه شد. بهاسکره به او ریاضیات آموخت تا از غم او بکاهد و لیلاوتی را به خاطر او نوشت.) بخش آخر این کتاب به معادلات دیوفانتی خطی اختصاص دارد. احتمالاً تمام ریاضیاتِ کتاب لیلاوتی بر برهمگوپته، حدود پانصد سال جلوتر، معلوم بوده است.

کتاب بیجگنیته از نظر ریاضی خیلی پیشرفته است. بیشتر با معادلهٔ پِل $x^2 - dy^2 = 1$ و مسائل دیوفانتی وابسته مربوط می‌شود. این کتاب یک الگوریتم کارآمد برای حل معادلهٔ پِل ارائه می‌دهد، که با روندی که برونکر پانصد سال بعد کشف کرد، ارتباط نزدیکی دارد. همانند برونکر،

1. QuickBasic 2. Robert A. Coury 3. Bhāskarācārya 4. Mysore
5. seddhāntaŝiromeni 6. lilāvati 7. bijaganita

* بهاسکره شش اثر دارد: لیلاوتی (در ریاضیات شامل ۱۳ فصل) بیجگنیته (در جبر شامل ۱۲ فصل)، واشنابهاشیَه (شرحی که خود بهاسکره بر سیدهانته‌شیرومنی نوشته است)، کَرَنکوتوهَلَه (ده بخش در حل مسائل نجومی)، و پَوزَنَه، و سیدهانته‌شیرومنی که از دو جزء تشکیل شده است گنیتادهَیایه (شامل نجوم ریاضی، ۲ فصل) و گُولادهَیایه (در باب کره، ۱۳ فصل). از بیجگنیته دو ترجمهٔ فارسی موجود است، در یکی نام مترجم نامعلوم است و مترجم دوم آقای عطاءالله رشیدی ابن احمد نادر است.

بهاسکره نیز اثبات نکرد که روشش همواره جوابی به‌دست می‌دهد. یکی از مثالهای بیجگنیته $x^۲ - ۶۱y^۲ = ۱$ است. بهاسکره تنها در چند مرحله جواب $x = ۲۲۶۱۵۳۹۸۰$ را به‌دست می‌آورد. در ۱۶۵۷ فرما دقیقاً با همین مسأله فرنیکل را به مبارزه طلبید!

بهاسکره در معادلهٔ پِل، مطابق سنت ریاضی دیرین هندی کار می‌کرد. مثلاً، برهمگوپته می‌دانست که چگونه جوابهای دیگر را می‌توان از جوابهای مفروض تولید کرد. آشکار است که بهاسکره دانشی از جبر داشت که اروپا تا سدهٔ هفدهم به آن نرسیده بود.

بهاسکره در حدود ۱۱۸۵ درگذشت.

مراجع

Leonhard Euler, *Elements of Algebra*, translated by John Hewlett, Springer-Verlag, New York, 1984.

شاید این کتاب بیشتر از سایر کتابهای ریاضی جز اصول اقلیدس خوانده شده است، کتابی است که بیش از ۳۰ بار و به ۶ زبان به چاپ رسیده است. بیشتر کتابهای درسی جبر مقدماتی تولید مستقیم این کتاب هستند، زیرا اعتبار اویلر موجب شد که نمادها، اصطلاحات و انتخاب مباحث او استانده شوند.

چند بخش اول کتاب مقدماتی هستند، و حاوی مطالبی می‌باشند که هنوز هم دروس جبر دبیرستانی را تشکیل می‌دهند. در ثلث آخر کتاب معادلات دیوفانتی مورد بحث قرار می‌گیرند. از جوابهای صحیح معادلات خطی شروع می‌شود و تا مطالعهٔ معادلهٔ پِل، مجموعهای دو مربع، و مسائل مربوط، ادامه می‌یابد. سپس اویلر معادلات $x^۴ + y^۴ = z^۲$ و $x^۳ + y^۳ = z^۳$، و نیز تعدادی مسأله از انواعی را که دیوفانتوس بررسی کرده و جوابهای گویا مورد نظرش بوده، به تفصیل بررسی می‌کند. مطالب کتاب همواره خیلی واضح هستند و هر تکنیک با مثالهای فراوان توصیف شده است.

جبر اویلر با یک مکمل طولانی توسط لاگرانژ، که نظریهٔ کسرهای مسلسل را طرح‌ریزی می‌کند، با یک تحلیل نظری کامل از معادلهٔ پِل، خاتمه می‌یابد. سپس، لاگرانژ یک روندی را برای یافتن تمام جوابهای صحیح معادلات دیوفانتی دومتغیرهٔ درجهٔ دوم ارائه می‌دهد. مطالعهٔ ملحقات لاگرانژ، و در واقع، تمام کتاب، هنوز هم ارزش بسیار زیادی دارد.

Hans Riesel, *Prime Numbers and Computer Methods for Eactorization*, Birkhäuser, Boston, 1987.

ریزل بعضی از الگوریتمهای نظری-عدد پایه‌یی را، با تکیه بر مفاهیمی که برای آزمون اول بودن و تجزیه لازم هستند، بیان می‌دارد. به‌ویژه قسمتهایی از نظریهٔ معادلهٔ پِل را که برای فهمیدن روش تجزیهٔ لژاندر و تکنیکهای وابسته لازم است، به اختصار شرح می‌دهد. مطالعهٔ این کتاب آسان است و بینش خوبی در مورد مطالب محاسبه‌یی ارائه می‌دهد. گردایه‌ای از برنامه‌های رایانه‌یی، از جمله بسته‌بندی کاملی از دقت ـ چندگانه[1] برای اعمال حسابی ابتدایی، یک بخش جالب توجه از کتاب است.

1. complete multiple-precision package

۱۱

اعداد صحیح گاوسی و سایر توسیعهای درجهٔ دوم

ابتدا به بررسی یک مسألهٔ ساده می‌پردازیم: به‌ازای کدام عدد صحیح غیرصفر n معادلهٔ دیوفانتی $x^۲ - y^۲ = n$ جواب دارد، و چند جواب وجود دارد؟ برای رسیدن به پاسخ، چندجمله‌یی $x^۲ - y^۲$ را تجزیه می‌کنیم و معادلهٔ هم‌ارز $(x - y)(x + y) = n$ را به‌دست می‌آوریم.

اگر n فرد باشد، فرض می‌کنیم d یک مقسوم‌علیه (مثبت یا منفی) n باشد. قرار می‌دهیم $x + y = d$ و $x - y = n/d$. در این صورت روشن است که $x = (d + n/d)/۲$ و $y = (d - n/d)/۲$ اعداد صحیح هستند و $x^۲ - y^۲ = n$. علاوه بر این، تمام جفتهای (x, y) از اعداد صحیح که در معادله صدق می‌کنند به این طریق به دست می‌آیند. با این یادآوری که $\tau(k)$ تعداد مقسوم‌علیه‌های مثبت k است، می‌بینیم که تعداد $۲\tau(|n|)$ انتخاب برای d، و لذا $۲\tau(|n|)$ جواب صحیح (مثبت، منفی، یا صفر) برای معادلهٔ $x^۲ - y^۲ = n$ وجود دارد.

مرحلهٔ کلیدی در تحلیل حل معادلهٔ دیوفانتی $x^۲-y^۲=n$ تجزیهٔ $x^۲-y^۲=(x-y)(x+y)$ است. می‌خواهیم که همین منظور را در مورد معادلهٔ $x^۲+y^۲=n$ به‌کار بریم. گرچه چندجمله‌یی $x^۲+y^۲$ روی اعداد حقیقی تجزیه نمی‌شود، ولی تجزیهٔ $x^۲+y^۲=(x-yi)(x+yi)$ را که در آن $i^۲=-۱$، داریم. این مطلب به بررسی ویژگیهای نظری‌ـعددی اعداد مختلط $a+bi$، که در آن a و b اعداد صحیح هستند، منجر می‌شود. بعداً در همین فصل خواهیم دید که کاربرد این چنین اعداد مختلط، که اعداد گاوسی خوانده می‌شوند، چگونه نظریهٔ نمایشها به صورت مجموع دو مربع را کاملاً شفاف می‌سازد.

به نظر می‌رسد که اویلر نخستین کسی باشد که این قبیل توسیعهای اعداد صحیح معمولی را برای اثبات یک نتیجهٔ نظری‌ـعددی به‌کار برده است. درکوشش برای اثبات اینکه $x^۳+y^۳=z^۳$ با شرط $xyz\neq ۰$ جواب صحیح ندارد، اویلر به بررسی تجزیهٔ $z^۳-y^۳=(z-y)(z-y\omega)(z-y\omega^۲)$، که $\omega=(-۱+\sqrt{-۳})/۲$ یک ریشهٔ سوم ۱ است، هدایت شده بود. بدون آنکه به صراحت بیان کند، اویلر فرض کرد که اعداد به‌صورت $a+b\omega$، که a و b اعداد صحیح نیستند، از ویژگیهای تجزیه که بسیار شبیه ویژگیهای تجزیهٔ اعداد صحیح معمولی است، برخوردارند. سپس اویلر یک استدلال نزولی به‌کار می‌برد که حالت $n=۳$ از آخرین قضیهٔ فرما را ثابت می‌کند.

کاربردهای مهم بعدی این قبیل توسیعهای اعداد صحیح در یک سری مقاله در مورد تقابل دو مجذوری توسط گاوس است. این موضوع ساده که $x^۲-۱=(x-۱)(x+۱)$ برای تحلیل مانده‌های درجهٔ دوم مهم است، در مقابل، تجزیه $x^۴-۱=(x-۱)(x+۱)(x-i)(x+i)$ برای بحث در مانده‌های درجهٔ چهارم به‌کار می‌خورد. برای کاربرد مؤثر این تجزیه ابتدا لازم است که ویژگیهای پایه‌یی اعداد صحیح گاوسی تأسیس شود، و گاوس مبادرت به این کار کرد.

در طی سدهٔ نوزدهم، بررسی ویژگیهای «اعداد صحیح» از یک نوع کلیتر، در مطالعهٔ تقابل بالاتر و نیز معادلات دیوفانتی، به‌ویژه آخرین قضیهٔ فرما و صورتهای درجهٔ دوم مهم شد. بعضی از مهمترین ریاضیدانان این دوره، از جمله دیریکله، کومر، آیزنشتاین، ژاکوبی، کرونکر، و ددکیند در این زمینه سهیم هستند. یکی از عرصه‌های پایه‌یی نظریهٔ جدید اعداد نظریهٔ جبری اعداد است که آنها توسعه دادند.

قضیه‌هایی برای فصل ۱۱

اعداد صحیح گاوسی

(۱.۱۱) تعریف. یک عدد صحیح گاوسی عدد مختلطی است به‌صورت $a+bi$، که در آن a و b اعداد صحیح هستند و $i=\sqrt{-۱}$.

آشکار است که هر عدد صحیح معمولی یک عدد صحیح گاوسی است و مجموع، تفاضل، و حاصلضرب اعداد صحیح گاوسی یک عدد صحیح گاوسی است. عموماً حروف کوچک یونانی را برای نشان دادن اعداد صحیح گاوسی به‌کار می‌بریم. در این فصل، اعداد صحیح معمولی اغلب اعداد صحیح گویا خوانده می‌شوند.

(۲.۱۱) تعریفها. (i) فرض کنیم α و β اعداد صحیح گاوسی باشند. گوییم که عدد α عدد β را می‌شمارد اگر یک عدد صحیح گاوسی γ وجود داشته باشد به‌طوری که $\beta = \gamma\alpha$. در این صورت، می‌نویسیم $\alpha|\beta$.

(ii) عدد صحیح گاوسی ϵ یک یکه نامیده می‌شود هرگاه $\epsilon|1$.

(iii) اگر ϵ یک یکه باشد، آنگاه $\epsilon\alpha$ یک وابستهٔ α خوانده می‌شود.

(iv) عدد صحیح گاوسی π یک عدد اول گاوسی است اگر π یکه نباشد، و به‌ازای هر دو عدد صحیح گاوسی α و β اگر $\pi = \alpha\beta$، آنگاه یا α یا β یک یکه باشد.

(v) اگر $\alpha = x + yi$، که x و y اعداد صحیح گویا باشند، آنگاه $\bar{\alpha}$، مزدوج α، عدد صحیح گاوسی $x - yi$ است.

(vi) اگر $\alpha = x + yi$، آنگاه نُرم α عبارت است از

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha} = (x + yi)(x - yi) = x^2 + y^2$$

ویژگی اصلی نُرم که در زیر می‌آید مکرراً مورد استفاده قرار می‌گیرد.

(۳.۱۱) لم. فرض کنیم α و β اعداد صحیح گاوسی باشند. آنگاه $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

برهان. فرض کنیم $\alpha = u + vi$ و $\beta = x + yi$. پس

$$\alpha\beta = (u + vi)(x + yi) = (ux - vy) + (uy + vx)i$$

در نتیجه

$$\mathrm{N}(\alpha\beta) = (ux - vy)^2 + (uy + vx)^2 = (u^2 + v^2)(x^2 + y^2) = \mathrm{N}(\alpha)\mathrm{N}(\beta)\,.$$

توضیح. اتحاد $(ux - vy)^2 + (uy + vx)^2 = (u^2 + v^2)(x^2 + y^2)$ برای همه آشناست؛ قبلاً آن را در فصل ۸ دیده‌ایم، در آنجا نقش مهمی در بیان یک عدد صحیح به‌صورت

مجموع دو مربع ایفا کرد. به‌هر حال، در آن فصل به‌عنوان یک مطلب منفرد ظاهر شد. در اینجا، می‌بینیم که بیان‌کنندهٔ یک ویژگی اصلی نُرم است.

چون $N(x+yi) = x^2 + y^2$، آشکار است که نرم یک عدد صحیح گاوسی یک عدد صحیح گویای نامنفی است و ۰ تنها عدد صحیح گاوسی با نُرم ۰ است. بیان ساده‌ای از یکه‌ها برحسب نُرمشان نیز وجود دارد.

(۴.۱۱) لم. عدد صحیح گاوسی α یک یکه است اگر و تنها اگر $N(\alpha) = 1$. اعداد صحیح گاوسی که یکه هستند عبارت‌اند از ± 1 و $\pm i$.

برهان. اگر $N(\alpha) = 1$، آنگاه $\alpha\bar{\alpha} = 1$؛ به‌ویژه، $|\alpha| 1$ و لذا α یک یکه است. بعکس، اگر α یکه باشد، آنگاه عدد صحیح گاوسی β وجود دارد به‌طوری‌که $\alpha\beta = 1$، و لذا

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$$

چون نُرمهای α و β اعداد صحیح نامنفی هستند، در نتیجه $N(\alpha) = 1$.

فرض می‌کنیم $\alpha = x + yi$، آنگاه $N(\alpha) = x^2 + y^2$. (روشن است که $N(\alpha) = 1$ اگر و تنها اگر $y = 0$ و $x = \pm 1$، $x = 0$ و یا $y = \pm 1$، بنابراین تنها یکه‌های گاوسی عبارت‌اند از ± 1 و $\pm i$.

لم بعد در بسط نظری همان نقش را ایفا می‌کند که الگوریتم تقسیم در فصل ۱ ایفا می‌کرد. به شباهت نزدیک بین چند لم بعد و قضیه‌های پایه‌یی در فصل ۱ توجه شود.

(۵.۱۱) لم (الگوریتم تقسیم). فرض می‌کنیم α و β اعداد صحیح گاوسی باشند و α ناصفر باشد. در این صورت اعداد صحیح گاوسی γ و ρ وجود دارند به‌طوری که $\beta = \gamma\alpha + \rho$ و $N(\rho) < N(\alpha)$.

برهان. فرض می‌کنیم $\beta/\alpha = x + yi$ ، که x و y اعداد حقیقی هستند، و فرض می‌کنیم u و v، به‌ترتیب، نزدیکترین اعداد صحیح به x و y باشند. (این اعداد صحیح ممکن است یکتا نباشند.) تعریف می‌کنیم $\gamma = u + vi$، و قرار می‌دهیم $\rho = \beta - \gamma\alpha$؛ واضح است که، $\beta = \gamma\alpha + \rho$. باقی می‌ماند که ثابت کنیم $N(\gamma) < N(\alpha)$. چون $\beta = (x+yi)\alpha$، داریم $\rho = ((x-u) + (y-v)i)\alpha$. اما $|x-u| \leq 1/2$ و $|y-v| \leq 1/2$، و لذا $N((x-u) + (y-v)i) \leq 1/4 + 1/4 = 1/2$. بنابراین، $N(\rho) \leq 1/2 N(\alpha)$، و نتیجه حاصل می‌شود.

اکنون، مانند فصل ۱، به ساختن نظریه‌ای برای قضیهٔ بزرگترین مقسوم‌علیه مشترک می‌پردازیم. تعریف مقتضی به قرار زیر است.

(۶.۱۱) تعریف. عدد صحیح گاوسی δ یک بزرگترین مقسوم‌علیه مشترک α و β است اگر (i) $\delta|\alpha$ و $\delta|\beta$، و (ii) δ بر هر مقسوم‌علیه مشترک α و β بخشپذیر باشد.

در ادامه ثابت می‌کنیم که بزرگترین مقسوم‌علیه‌های مشترک با تعریف بالا وجود دارند و می‌توان آنها را به‌صورت ترکیب خطی از α و β بیان کرد.

(۷.۱۱) قضیه. اگر α و β اعداد صحیح گاوسی باشند که هر دو صفر نیستند، آنگاه α و β یک بزرگترین مقسوم‌علیه مشترک مانند δ دارند، و می‌توان δ را به صورت $\delta = \lambda\alpha + \mu\beta$ نمایش داد، که در آن λ و μ اعداد صحیح گاوسی هستند.

برهان. فرض کنیم I مجموعهٔ تمام اعداد به‌صورت $\phi\alpha + \psi\beta$ باشد، که در آن ϕ و ψ اعداد صحیح گاوسی را طی می‌کنند. فرض می‌کنیم δ عنصری از I با کوچکترین نُرمِ مثبت باشد، و $\delta = \lambda\alpha + \mu\beta$. نشان می‌دهیم که δ بزرگترین مقسوم‌علیه مشترک α و β است.

ابتدا ثابت می‌کنیم که $\delta|\alpha$. بنابر (۵.۱۱)، داریم $\alpha = \kappa\delta + \rho$، که در آن $\mathrm{N}(\rho) < \mathrm{N}(\delta)$. سپس

$$\rho = \alpha - \kappa\delta = \alpha - \kappa(\lambda\alpha + \mu\beta) = (1 - \kappa\lambda)\alpha + (-\kappa\mu)\beta,$$

و لذا ρ یک ترکیب خطی از α و β است. داریم $\mathrm{N}(\rho) < \mathrm{N}(\delta)$، و این با تعریف δ تناقض دارد مگر اینکه باقیماندهٔ ρ برابر ۰ باشد. لذا نتیجه می‌شود که $\delta|\alpha$؛ به تشابه $\delta|\beta$. آشکار است که اگر $\gamma|\alpha$ و $\gamma|\beta$، آنگاه $\gamma|\lambda\alpha + \mu\beta$ و لذا $\gamma|\delta$. بنابراین، δ بزرگترین مقسوم‌علیه مشترک α و β است.

توضیح. فرض می‌کنیم δ و δ' هر دو بزرگترین مقسوم‌علیه مشترک α و β باشند. چون δ' یک مقسوم‌علیه α و نیز β است، از تعریف بزرگترین مقسوم‌علیه مشترک نتیجه می‌شود که $\delta'|\delta$. با استدلالی مشابه، داریم $\delta|\delta'$. لذا $\mathrm{N}(\delta) \le \mathrm{N}(\delta')$ و $\mathrm{N}(\delta') \le \mathrm{N}(\delta)$، و لذا δ و δ' نُرمهای برابر دارند. چون $\delta'|\delta$، پس $\delta' = \epsilon\delta$، که در آن ϵ یک یکه است، و بنابراین δ' یک وابستهٔ δ است.

برعکس، اگر δ بزرگترین مقسوم‌علیه مشترک α و β باشد و δ' یک وابستهٔ δ باشد، آنگاه δ' نیز بزرگترین مقسوم‌علیه مشترک α و β است. علاوه بر این، اگر δ به‌صورت ترکیب خطی از α و β بیان شده باشد، δ' نیز به‌آسانی به‌صورت ترکیب خطی از α و β بیان می‌شود.

در لم زیر یک ویژگی آشنای اعداد اول معمولی به اعداد اول گاوسی توسعه داده می‌شود و اساساً از همان برهان استفاده می‌شود.

(۸.۱۱) لم. فرض می‌کنیم π یک عدد اول گاوسی باشد، اگر $\pi|\alpha\beta$، آنگاه $\pi|\alpha$ یا $\pi|\beta$.

برهان. اگر $\pi\nmid\alpha$، آنگاه ۱ یک بزرگترین مقسوم‌علیه مشترک π و α است. لذا اعداد صحیح گاوسی λ و μ وجود دارند به‌طوری‌که $\lambda\pi+\mu\alpha=1$. از ضرب β در دو طرف این معادله داریم $\lambda\pi\beta+\mu\alpha\beta=\beta$. چون $\pi|\pi\beta$ و $\pi|\mu\alpha\beta$، در نتیجه $\pi|\beta$.

تجزیهٔ یکتا برای اعداد صحیح گاوسی

ابتدا نشان می‌دهیم که می‌توان اعداد صحیح گاوسی را به حاصلضرب اعداد اول تجزیه کرد.

(۹.۱۱) قضیه. اگر α یک عدد صحیح گاوسی جز $\circ$ یا یکه باشد، می‌توان α را به‌صورت حاصلضرب اعداد اول گاوسی بیان کرد.

برهان.[۱] اثبات به استقرای قوی بر نُرم α است. چون α نه صفر است و نه یکه پس $\mathrm{N}(\alpha)\geq ۲$. اگر $\mathrm{N}(\alpha)=۲$، آنگاه α یک عدد اول گاوسی است و لذا حکم برقرار است (اگر $\alpha=\beta\gamma$، داریم $\mathrm{N}(\alpha)=\mathrm{N}(\beta)N(\gamma)=۲$. پس یا $\mathrm{N}(\beta)=۱$ یا $\mathrm{N}(\gamma)=۱$، و لذا بنابر لم ۴.۱۱، یا β یک یکه است یا γ، در نتیجه بنابر (iv.۲.۱۱)، α یک عدد اول گاوسی است). حال فرض می‌کنیم که $n\geq ۳$ و حکم برای تمام اعداد صحیح گاوسی α که نُرمشان برابر $۲،۳،\ldots،n-۱$ است برقرار باشد، گوییم که حکم برای عدد صحیح گاوسی α که $\mathrm{N}(\alpha)=n$ نیز برقرار است. اگر α یک عدد اول گاوسی باشد، چیزی برای اثبات نداریم. در غیر این‌صورت، اعداد صحیح گاوسی β و γ که هیچ‌یک از آن دو یکه نیست، وجود دارند به‌طوری‌که $\alpha=\beta\gamma$. چون $\mathrm{N}(\alpha)=\mathrm{N}(\beta)\mathrm{N}(\gamma)$ و نه α یک یکه است و نه β، داریم $\mathrm{N}(\beta)<n$ و $\mathrm{N}(\gamma)<n$. لذا بنابر فرض استقرا، می‌توان β و γ را به‌صورت حاصلضرب اعداد اول گاوسی بیان کرد، و بنابراین α نیز حاصلضرب اعداد اول گاوسی است.

برهان کتاب:

اثبات به استقرا بر نُرم α است. فرض می‌کنیم که قضیه برای همهٔ اعداد صحیح گاوسی که نُرمشان کمتر از n است برقرار باشد؛ در این صورت نشان می‌دهیم که قضیه برای اعداد صحیح گاوسی از نُرم n برقرار است. اگر α یک عدد اول گاوسی باشد، چیزی برای اثبات نداریم. در غیر

۱. اثبات ارائه‌شده در متن اصلی ناقص است، لذا مترجم به اصلاح آن پرداخت.

این‌صورت، اعداد صحیح گاوسی β و γ که هیچ‌یک از آن دو یک یکه نیست، وجود دارند به‌طوری‌که $\alpha = \beta\gamma$. اما چون $\mathrm{N}(\alpha) = \mathrm{N}(\beta)\mathrm{N}(\gamma)$ و نه α و نه β یکه نیست، داریم $\mathrm{N}(\beta) < n$ و $\mathrm{N}(\gamma) < n$. لذا بنابر فرض استقرا می‌توان β و γ را به‌صورت حاصلضرب اعداد اول گاوسی بیان کرد، و بنابراین α نیز حاصلضرب اعداد اول گاوسی است.

قضیهٔ بعد نشان می‌دهد که یک قضیهٔ اصلی، نظیر قضیهٔ اصلی حساب، برای اعداد صحیح گاوسی نیز برقرار است.

(۱۰.۱۱) قضیهٔ تجزیهٔ یکتا. اگر α_1، α_2، ... و β_1، ...، β_s اعداد اول گاوسی باشند و ϵ یک یکه باشد و $\alpha_1\alpha_2\cdots\alpha_r = \epsilon\beta_1\beta_2\cdots\beta_s$، آنگاه $r = s$، و می‌توان β_iها را تجدید آرایش کرد به‌طوری‌که به‌ازای هر i، β_i یک وابستهٔ α_i باشد.

برهان. قرار می‌دهیم $\gamma = \alpha_1\alpha_2\cdots\alpha_r$. اگر γ یک عدد اول گاوسی باشد قضیه حاصل است، زیرا در این صورت $r = s = 1$ و $\alpha_1 = \epsilon\beta_1$. در حالت کلی قضیه را به استقرا روی r ثابت می‌کنیم. لذا، فرض می‌کنیم که قضیهٔ تجزیهٔ یکتا برای تمام اعداد صحیح گاوسی که حداقل یک تجزیهٔ به‌صورت حاصلضرب $r-1$ عامل اول (نه لزوماً یکتا) دارند برقرار باشد؛ نشان می‌دهیم که قضیه برای تمام اعداد صحیح گاوسی که نمایشی به‌صورت r عامل اول دارند برقرار است.

فرض می‌کنیم که $\alpha_1\alpha_2\cdots\alpha_r = \epsilon\beta_1\beta_2\cdots\beta_s$. چون α_r حاصلضرب β_iها را می‌شمارد، لذا لااقل یکی از آنها را خواهد شمرد. با تجدید آرایش عاملها در صورت لزوم، می‌توانیم فرض کنیم که $\alpha_r|\beta_s$. چون β_s اول است، بایستی یک وابستهٔ α_r باشد؛ لذا $\beta_s = \epsilon'\alpha_r$، که ϵ' یک یکه است. با حذف α_r از طرفین معادلهٔ

$$\alpha_1\alpha_2\cdots\alpha_r = \epsilon\epsilon'\beta_1\beta_2\cdots\beta_{s-1}\alpha_r$$

داریم

$$\alpha_1\cdots\alpha_{r-1} = \epsilon\epsilon'\beta_1\cdots\beta_{s-1}$$

لذا بنابر فرض استقرا، داریم $r-1 = s-1$، و از آنجا $r = s$. از فرض استقرا همچنین نتیجه می‌شود که می‌توان اعداد β_1، ...، β_{r-1} را تجدید آرایش کرد به‌طوری‌که وابسته‌های α_1، ...، α_{r-1} بشوند، که این قضیه را ثابت می‌کند.

توضیح. قضیهٔ تجزیهٔ یکتا برای اعداد صحیح گاوسی را می‌توان به عبارتی بیان کرد که شباهت بیشتر به قضیهٔ تجزیهٔ یکتای معمولی پیدا کند. اگر $a+bi$ یک عدد صحیح گاوسی

غیرصفر باشد، موقتاً $a+bi$ را مثبت خوانیم اگر $a>0$ و $b\leq 0$. به آسانی بررسی می‌شود که هر عدد صحیح گاوسی غیرصفر دارای یک وابستهٔ مثبتِ یکتاست. در این صورت، هر عدد صحیح گاوسی غیرصفر (صرف‌نظر از ترتیب عاملها) یک نمایش یکتا به‌صورت $\epsilon\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_r^{a_r}$ دارد، که در آن ϵ یک یکه است، π_iها اعداد اول گاوسی متمایزند، و a_iها اعداد صحیح مثبت هستند.

اعداد اول گاوسی

ابتدا توجه می‌کنیم که اگر $\mathrm{N}(\alpha)$ یک عدد اول گویا باشد، α یک عدد اول گاوسی است. زیرا فرض کنیم $\alpha=\beta\gamma$؛ پس $\mathrm{N}(\alpha)=\mathrm{N}(\beta)\mathrm{N}(\gamma)$. بنابراین، اگر $\mathrm{N}(\alpha)$ یک عدد اول گویا باشد، آنگاه $\mathrm{N}(\beta)=1$ یا $\mathrm{N}(\gamma)=1$، و لذا بنابر (۴.۱۱)، یا β یک یکه است یا γ. از تعریف نتیجه می‌شود که α یک عدد اول گاوسی است.

سپس مشاهده می‌کنیم که هر عدد اول گاوسی عدد اول گویایی را می‌شمارد. برای دیدن این مطلب، گیریم π یک عدد اول گاوسی باشد، و فرض می‌کنیم $n=\mathrm{N}(\pi)$. چون $\mathrm{N}(\pi)=\pi\bar{\pi}$، داریم $\pi|n$. حال، n را به‌صورت حاصلضرب اعداد اول گویا بیان می‌کنیم، مثلاً $n=p_1p_2\cdots p_k$. چون $\pi|n$، بنابر (۸.۱۱)، یک i وجود دارد به‌طوری‌که $\pi|p_i$. لذا برای جستجوی اعداد اول گاوسی، کافی است که عاملهای اول گویا را بررسی کنیم.

در اعداد صحیح گاوسی، عدد اول گویای ۲ دارای تجزیهٔ $2=(1+i)(1-i)$ است. چون $1-i$ دارای نُرم ۲ است، که اول‌است، در نتیجه $1-i$ و وابسته‌هایش یعنی $1+i$، $-1+i$، و $-1-i$ اعداد اول گاوسی هستند.

اعداد اول گویای p به‌صورت $4k+3$ نیز اعداد اول گاوسی هستند. زیرا فرض کنیم $p=\alpha\beta$؛ آنگاه $\mathrm{N}(p)=p^2=\mathrm{N}(\alpha|\mathrm{N}\beta)$. اما p نمی‌تواند نُرم یک عدد صحیح گاوسی باشد، زیرا هیچ عدد به‌صورت $4k+3$ مجموع دو مربع نیست. بنابراین، یا $\mathrm{N}(\alpha)$ بایستی ۱ باشد یا $\mathrm{N}(\beta)$، و لذا یا α یک یکه است یا β. در نتیجه p یک عدد اول گاوسی است. از این‌رو، تنها اعداد اول گاوسی که p را می‌شمارند چهار وابسته p هستند.

باقی می‌ماند که اعداد اول به‌صورت $4k+1$ را بررسی کنیم. بنابر (۸.۸)، هر عدد اول به این صورت را می‌توان به‌صورت مجموع دو مربع بیان کرد. اگر $p=u^2+v^2$، آنگاه $p=(u+vi)(u-vi)$. چون نُرمهای $u+vi$ و $u-vi$ اول هستند، پس هرکدام یک عدد اول گاوسی است. در این صورت $u+vi$، $u-vi$، و وابسته‌هایشان تنها اعداد اول گاوسی هستند که p را می‌شمارند.

بحث بالا را می‌توان به‌ترتیب زیر خلاصه کرد.

(۱۱.۱۱) قضیه. عدد صحیح گاوسی π یک عدد اول گاوسی است اگر و تنها اگر یکی از موارد زیر برقرار باشد:

(i) π عدد $i-1$ یا یکی از وابسته‌هایش باشد؛

(ii) π عدد اول گویا به‌صورت $4k+3$ یا یکی از وابسته‌هایش باشد؛

(ii) $\mathrm{N}(\pi)=p$، که در آن p عدد اول گویا به‌صورت $4k+1$ است.

یک کاربرد: اعداد صحیح گاوسی و مجموع دو مربع

اعداد صحیح گاوسی را می‌توان برای ارائهٔ برهانهای دیگری برای تمام قضیه‌های مربوط به نمایشها به‌صورت مجموع دو مربع که در فصل ۸ ثابت شدند، به‌کار برد.

به‌عنوان نخستین مثال، با برهان دیگری ثابت می‌کنیم که هر عدد اول به‌صورت $4k+1$ مجموع دو مربع است. ابتدا نشان می‌دهیم که p یک عدد اول گاوسی نیست. چون -1 یک ماندهٔ درجهٔ دوم p است، عدد صحیح گویای x وجود دارد به‌طوری که $x^2 \equiv -1 \pmod{p}$. از این‌رو $p|x^2+1$ و لذا $p|(x-i)(x+i)$. اگر p یک عدد اول گاوسی باشد، بنابر (۸.۱۱) یا بایستی $p|x-i$ یا $p|x+i$، اما روشن است که، هیچ‌کدام اتفاق نمی‌افتد.

چون p یک عدد اول گاوسی نیست، اعداد صحیح گاوسی α و β که هیچ‌کدام یکه نیستند وجود دارند به‌طوری‌که $p=\alpha\beta$. چون $\mathrm{N}(p)=p^2=\mathrm{N}(\alpha)\mathrm{N}(\beta)$ و هیچ‌کدام از $\mathrm{N}(\alpha)$ و $\mathrm{N}(|\beta)$ برابر ۱ نیستند، لذا $\mathrm{N}(\alpha)=\mathrm{N}(\beta)=p$. بنابراین، اگر $\alpha=u+iv$، آنگاه $p=u^2+v^2$، یعنی p مجموع دو مربع است.

می‌توان قضیهٔ تجزیهٔ یکتا را برای محاسبهٔ $\mathrm{N}(n)$ یعنی تعداد نمایشهای n به صورت مجموع دو مربع، نیز به‌کار برد. ($\mathrm{N}(n)$، یعنی تعداد نمایشها را با $\mathrm{N}(\alpha)$، یعنی نُرم α، اشتباه نکنید.)

(۱۲.۱۱) قضیه. فرض می‌کنیم $n=2^a\prod p_j^{a_j}\prod q_j^{b_j}$، که در آن p_jها اعداد اول به‌صورت $4k+1$ هستند، q_jها اعداد اول به‌صورت $4k+3$، و هر b_j زوج است، در این صورت

$$N(n)=4\prod(a_j+1)$$

(حاصلضربی که هیچ جمله‌ای ندارد برابر ۱ تلقی می‌شود.)

برهان. محاسبهٔ تعداد جفتهای مرتب (u,v) از اعداد صحیح را به‌طوری که $u^2+v^2=n$، یعنی، $(u+vi)(u-vi)=n$ لازم داریم. به‌ازای هر p_j، فرض می‌کنیم c_j و d_j اعداد صحیحی

باشند به‌طوری که $p_j = c_j^2 + d_j^2$. لذا، در اعداد صحیح گاوسی، n دارای تجزیه زیر است

$$n = i^a(1-i)^{2a}\prod(c_j+d_ji)^{a_j}(c_j-d_ji)^{a_j}\prod q_j^{b_j}$$

که در آن i، $1-i$، $c_j \pm d_ji$، و q_j همگی اعداد اول گاوسی هستند.

هر عامل $u+vi$ از n به‌صورت

$$\epsilon(1-i)^t\prod(c_j+d_ji)^{u_j}(c_j-d_ji)^{v_j}\prod q_j^{w_j} \qquad (1)$$

است که در آن ϵ یک یکه است، $0 \le t \le 2a$، $0 \le u_j, v_j \le a_j$، و $0 \le w_j \le b_j$. علاوه بر این، بنابر قضیهٔ تجزیهٔ یکتا، تمام عبارتهای متمایز به‌صورت (۱) به عاملهای متمایز n منجر می‌شوند. با مزدوج‌گیری، می‌بینیم که $u-vi$ دارای نمایش زیر است

$$\bar{\epsilon}(1+i)^t\prod(c_j-d_ji)^{u_j}(c_j+d_ji)^{v_j}\prod q_j^{w_j} \qquad (2)$$

در این صورت، شرط $n = (u+vi)(u-vi)$ ایجاب می‌کند که $n = 2^t\prod p_j^{u_j+v_j}\prod q_j^{2w_i}$؛ لذا $t=a$، $u_j+v_j=a_j$، و $2w_j = b_j$. از آنجا نتیجه‌های زیر به‌دست می‌آید: t و w_j کاملاً به‌وسیلهٔ n معین می‌شوند، به‌ازای هر j دقیقاً a_j+1 انتخاب ممکن برای u_j داریم، و هرگاه u_j انتخاب شده باشد، v_j مشخص می‌شود. سرانجام، چون به وضوح چهار انتخاب برای یکهٔ ϵ در (۱) وجود دارند، در نتیجه $4\prod(a_j+1)$ انتخاب برای $u+v_i$ وجود دارند. این برهان را کامل می‌کند.

تجزیه در اعداد صحیح گاوسی نگاه دیگری بر نمایشهای n به‌صورت مجموع دو مربع متباین دارد. برهانی از (۱۸.۸) بر پایهٔ اعداد صحیح گاوسی ارائه می‌دهیم.

(۱۳.۱۱) قضیه. فرض کنیم $n = p_1^{a_1}\cdots p_r^{a_r}$، که در آن p_1، p_2، ...، p_r اعداد اول متمایز به‌صورت $4k+1$ هستند. در این صورت n و $2n$ هر کدام دقیقاً 2^{r+2} نمایش اولیه به‌صورت مجموع دو مربع دارند.

برهان. قضیه را برای n ثابت می‌کنیم؛ برهان برای $2n$ نیز مشابه همین است. به‌ازای هر j، فرض می‌کنیم $p_j = (c_j+d_ji)(c_j-d_ji)$. برهان (۱۲.۱۱) نشان می‌دهد که نمایشهای n به‌صورت u^2+v^2 با فرض $u+iv = \epsilon\prod(c_j+d_ji)^{u_j}(c_j-d_ji)^{v_j}$، که در آن ϵ یک یکه است و $u_j+v_j=a_j$، به دست می‌آیند. اگر $0 < u_j < a_j$، آنگاه $(c_j+d_ji)(c_j-d_ji)$

عدد $u+vi$ را می‌شمارد، لذا $p_j|u+vi$. با مزدوج‌گیری، داریم $p_j|2u$ و $p_j|2v$. و چون p_j فرد است، پس $p_j|u$ و $p_j|v$. لذا یک نمایش اولیه به‌دست نمی‌آوریم.

لذا، به‌ازای هر j، بایستی یا $u_j=0$ یا $u_j=a_j$ را انتخاب کنیم، تا یک نمایش اولیه از n به دست آید. زیرا، در غیر این‌صورت اگر ρ عدد اولی باشد که u و v را بشمارد؛ آنگاه $p|n$، و لذا یک j وجود دارد به‌طوری‌که $p=p_j$. بنابراین، c_j+d_ji و c_j-d_ji هرکدام عدد $u+vi$ را می‌شمارند، که ممکن نیست، زیرا اگر $u_j=0$، آنگاه c_j+d_ji عدد $u+vi$ را نمی‌شمارد، و اگر $u_j=a_j$، آنگاه c_j-d_ji عدد $u+vi$ را نمی‌شمارد.

در نتیجه به‌ازای هر j، دو انتخاب $u_j=0$ یا $u_j=a_j$ را داریم، که در مجموع 2^r انتخاب ارائه می‌دهند. از طرفی، چون چهار انتخاب برای ϵ وجود دارند، در نتیجه تعداد کل نمایشهای اولیه 2^{r+2} است.

یک کاربرد از اعداد صحیح گاوسی در معادلات دیوفانتی

قبلاً اعداد صحیح گاوسی را برای بررسی معادلهٔ دیوفانتی $n=x^2+y^2$ به‌کار برده‌ایم. در این بخش، مثال دیگری ارائه می‌دهیم. ابزار اصلی، مشابه مطلب آشنای مربوط به اعداد صحیح است که در زیر می‌آید.

(۱۴.۱۱) قضیه. اگر α، β، و γ اعداد صحیح گاوسی، $(\alpha,\beta)=1$، و $\alpha\beta=\gamma^n$، آنگاه یکهٔ ϵ و عدد صحیح گاوسی δ وجود دارند به‌طوری‌که $\alpha=\epsilon\delta^n$.

برهان. قضیهٔ تجزیهٔ یکتا را با آن صورتی به‌کار می‌بریم که می‌گوید: (صرف‌نظر از ترتیب جمله‌ها) به عدد صحیح گاوسی غیرصفر را می‌توان به طور یکتا به‌صورت ضرب یک یکه در حاصلضرب اعداد اول گاوسی «مثبت» بیان کرد. («توضیح» بعد از (۱۰.۱۱) را ببینید.) قرار می‌دهیم

$$\alpha=\epsilon_a\prod\pi_j^{a_j}\quad،\beta=\epsilon_b\prod\pi_j^{b_j}\quad،\gamma=\epsilon_c\prod\pi_j^{c_j}$$

چون $\alpha\beta=\gamma^n$، به‌ازای هر j داریم $a_j+b_j=nc_j$. همچنین، چون α و β نسبت به هم اول‌اند، هیچ عدد اول گاوسی نمی‌تواند هم در تجزیهٔ α و هم در تجزیهٔ β ظاهر شود؛ لذا به‌ازای هر j داریم $a_j=0$ یا $a_j=nc_j$. در نتیجه، هر a_j مضربی از n است، لذا α برابر است با یک یکه در توان nام عددی.

مثال. ویژگیهای اعداد صحیح گاوسی را برای یافتن تمام جوابهای معادلهٔ دیوفانتی $x^2+1=y^3$ یا، هم‌ارز با آن، $(x+i)(x-i)=y^3$ به‌کار می‌بریم. ابتدا ثابت می‌کنیم که اگر x و y یک جواب

باشد، آنگاه $x+j$ و $x-i$ نسبت به هم اول‌اند. اگر چنین نباشد، عدد اول گاوسی π وجود دارد که $\pi|(x+i)-(x-i)$ و $x-i$ را می‌شمارد؛ در این صورت $\pi|2$، زیرا $x+i$. گوییم x زوج است، زیرا اگر x فرد باشد، آنگاه $x^2+1\equiv 2 \pmod 4$، ولی هیچ مکعبی نمی‌تواند همنهشت با ۲ به پیمانهٔ ۴ باشد. پس x زوج است. چون x زوج است، داریم $\pi|x$؛ از طرفی، بنابه فرض $\pi|x+1$، لذا $\pi|i$، که ممکن نیست.

بنابر (۱۴.۱۱)، می‌توان $x+i$ را به‌صورت $\epsilon\delta^3$ نوشت، که ϵ یک یکه است. اما به‌آسانی دیده می‌شود که به‌ازای هر یکهٔ ϵ، داریم $\epsilon=\epsilon^3$، لذا $x+i=(\epsilon\delta)^3$. اگر

$$x+i=(u+vi)^3=(u^3-3uv^2)+(3u^2v-v^3)i$$

آنگاه $x=u^3-3uv^2$ و $3u^2v-v^3=1$.

چون $v(3u^2-v^2)=1$، پس $v=\pm 1$. اگر $v=1$، آنگاه $3u^2-v^2=1$ و لذا $3u^2=2$، که ممکن نیست. اگر $v=-1$، آنگاه $3u^2-v^2=-1$، و از آنجا $u=0$. از این‌رو $x=0$، و لذا $y=1$. در نتیجه تنها جواب صحیح معادلهٔ دیوفانتی $x^2+1=y^3$ عبارت است از $x=0$، $y=1$. (برای مثالهای بیشتر، مسائل ۱۱ـ۳۰ و ۱۱ـ۳۱ را ببینید.)

اعداد صحیح $Q(\sqrt{d})$

(۱۵.۱۱) تعریف. فرض کنیم $d\neq 1$، و فرض می‌کنیم d خالی از مربع باشد. در این صورت $Q(\sqrt{d})$ مجموعهٔ تمام اعداد به‌صورت $x+y\sqrt{d}$ است، که در آن x و y اعداد گویا هستند. عدد $x+y\sqrt{d}$ یک عدد صحیح از $Q\sqrt{d}$ خوانده می‌شود اگر یا (i) $d\equiv 3 \pmod 4$ یا ۲ و x و y اعداد صحیح معمولی باشند یا (ii) $d\equiv 1 \pmod 4$ و x و y هر دو عدد صحیح باشند یا هر یک نصف یک عدد صحیح فرد باشد.

توضیحات. ۱. وقتی $d\equiv 1 \pmod 4$، می‌توان تعریف یک عدد صحیح از $Q(\sqrt{d})$ را به طریق زیر با انگیزه تلقی کرد: یک عدد مختلط α را یک عدد صحیح جبری خوانیم هرگاه α ریشه‌ای از یک چندجمله‌یی با ضرایب صحیح و ضریب پیشرو ۱ باشد. اگر $\alpha\epsilon(\sqrt{d})$، اثبات اینکه α یک عدد صحیح جبری است اگر و تنها اگر به معنی تعریف قبل α یک عدد صحیح از $Q(\sqrt{d})$ باشد، مشکل نیست (مسائل ۱۱ـ۴۱ و ۱۱ـ۴۲ را ببینید).

۲. اگر $d\equiv 1 \pmod 4$، اعداد صحیح $Q(\sqrt{d})$ دقیقاً اعداد مختلط به‌صورت $x+y\omega$ هستند، که در آن x و y اعداد صحیح معمولی هستند و $\omega=(1+\sqrt{d})/2$.

در آنچه در زیر می‌آید، لازم است بدانیم که اگر d مربع عدد صحیحی نباشد، $\sqrt{d}$ گنگ است. اثبات یک قضیهٔ کلیتر به آسانی صورت می‌گیرد.

(۱۶.۱۱) قضیه. فرض می‌کنیم $P(x)$ یک چندجمله‌یی با ضرایب صحیح و ضریب پیشرو ۱ باشد. اگر z عدد گویایی باشد به‌طوری‌که $P(z) = ۰$، آنگاه z یک عدد صحیح است. به‌ویژه، اگر عدد صحیح d مربع کامل نباشد $\sqrt{d}$ گنگ است.

برهان. گیریم $P(x) = x^k + a_{k-۱}x^{k-۱} \cdots + a_۱x + a_۰$، و فرض می‌کنیم به‌ازای عدد گویای z، $P(z) = ۰$. می‌توانیم فرض کنیم که $z = s/t$، که در آن t مثبت و $(s,t) = ۱$. نشان می‌دهیم که $t = ۱$.

با گذاشتن s/t به‌جای z و ضرب در t^k، داریم

$$a_{k-۱}s^{k-۱} + a_{k-۲}s^{k-۲}t^۲ + \cdots + a_۱st^{k-۱} + a_۰t^k = -s^k$$

آشکار است که طرف چپ بر t بخشپذیر است، لذا $t|s^k$. چون $(s,t) = ۱$، در نتیجه $t = ۱$.

سرانجام، برای اثبات اینکه $\sqrt{d}$ گویا نیست مگر آنکه d یک مربع کامل باشد، توجه می‌کنیم که $\sqrt{d}$ ریشهٔ معادلهٔ چندجمله‌یی $x^۲ - d = ۰$ است.

توضیح. اگر α عنصری از $Q(\sqrt{d})$ باشد، آنگاه اعداد گویای x و y که به‌طور یکتا تعیین می‌شوند وجود دارند و به‌طوری‌که $\alpha = x + y\sqrt{d}$. این مطلب یک نتیجهٔ بلافصل از (۱۶.۱۱) است.

اعمال حسابی ابتدایی. به آسانی دیده می‌شود که اگر α و β در $Q(\sqrt{d})$ باشند، آنگاه $\alpha \pm \beta$ و $\alpha\beta$ نیز در $Q(\sqrt{d})$ هستند. همچنین، اگر $\beta \neq ۰$، و α در $Q(\sqrt{d})$ باشد، آنگاه α/β در $Q(\sqrt{d})$ است. برای اثبات این مطلب کافی است نشان دهیم که $۱/\beta$ در $Q(\sqrt{d})$ است.

فرض کنیم $\beta = s + t\sqrt{d}$، که در آن s و t اعداد گویا هستند. اگر $t = ۰$، آنگاه β گویاست و نتیجه برقرار است. اگر $t \neq ۰$، آنگاه $s - t\sqrt{d} \neq ۰$، زیرا اگر $s - t\sqrt{d} = ۰$، آنگاه $\sqrt{d} = s/t$، که با (۱۶.۱۱) تناقض دارد. بنابراین

$$\frac{۱}{s + t\sqrt{d}} = \frac{s - t\sqrt{\alpha}}{(s + t\sqrt{\alpha})(s - t\sqrt{d})} = \frac{s}{s^۲ - dt^۲} + \frac{-t}{s^۲ - dt^۲}\sqrt{d},$$

و لذا $۱/\beta$ در $Q(\sqrt{d})$ است.

قبلاً حالت $d = -1$ را به تفصیل بررسی کرده‌ایم؛ اعداد صحیح $Q(\sqrt{-1})$ همان اعداد صحیح گاوسی هستند. اکنون که اختصار اعمال حسابی پایه‌یی $Q(\sqrt{d})$ را شرح می‌دهیم. تعریفهای اصلی تقریباً نظیر تعریفهای متناظر برای اعداد صحیح گاوسی هستند.

(۱۷.۱۱) تعریفها. (i) فرض کنیم α، β اعداد صحیحی از $Q(\sqrt{d})$ باشند. گوییم $\alpha|\beta$ اگر عدد صحیح γ از $Q(\sqrt{d})$ وجود داشته باشد به‌طوری‌که $\beta = \gamma\alpha$.

(ii) عدد صحیح ϵ از $Q(\sqrt{d})$ یک یکه خوانده می‌شود هرگاه $\epsilon|1$. اگر یکهٔ ϵ وجود داشته باشد به‌طوری‌که $\beta = \epsilon\alpha$، آنگاه β یک وابستهٔ α نامیده می‌شود.

(iii) عدد صحیح π از $Q(\sqrt{d})$ اول است اگر π یکه نباشد، و به‌ازای هر عدد صحیح α و β از $Q(\sqrt{d})$ اگر $\pi = \alpha\beta$، آنگاه یا α یک یکه باشد یا β.

(iv) اگر x و y اعداد گویا باشند، آنگاه $x - y\sqrt{d}$ مزدوج $x + y\sqrt{d}$، و $x^2 - dy^2$ نُرم $x + y\sqrt{d}$ است. نماد $\bar{\alpha}$ را برای مزدوج α، و $\mathrm{N}(x + y\sqrt{d})$ را برای نُرم $x + y\sqrt{d}$ به‌کار می‌بریم.

توضیح. در فصل ۹ مزدوج α برای $d > 0$ تعریف و با α' نشان داده شد. $\bar{\alpha}$ را به‌کار بردیم تا تأکید کنیم که این تعمیمی از مفهوم مزدوج مختلط است.

در قضیهٔ بعد بعضی از نتایج مربوط به یکه‌ها، وابسته‌ها، مزدوجها، و نُرم بیان می‌شوند. همهٔ برهانها ساده هستند.

(۱۸.۱۱) قضیه. (i) اگر ϵ و ϵ' یکه باشند، آنگاه $\epsilon\epsilon'$ و $1/\epsilon$ نیز یکه هستند.

(ii) اگر α و β عناصری از $Q(\sqrt{d})$ باشند، آنگاه $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)|\mathrm{N}(\beta)$.

(iii) اگر α عدد صحیحی از $Q(\sqrt{d})$ باشد، آنگاه α یک یکه است اگر و تنها اگر $\mathrm{N}(\alpha) = \pm 1$.

(iv) اگر α و β در $Q(\sqrt{d})$ باشند، آنگاه $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$.

(v) اگر $\alpha|\beta$، آنگاه $\mathrm{N}(\alpha)|\mathrm{N}(\beta)$.

(vi) اگر α عدد صحیحی از $Q(\sqrt{d})$ باشد و $\mathrm{N}(\alpha) = \pm p$، که در آن p یک عدد اول گویاست، آنگاه α اول است.

تا این مرحله، نتایج حاصل ویژگیهای استانداردِ اعداد صحیح گاوسی را به وقت نمایان می‌سازند. همچنین به‌آسانی می‌توان ثابت کرد که هر عدد صحیح از $Q(\sqrt{d})$ را که 0 یا یک یکه نیست می‌توان به صورت حاصلضرب اعداد اول بیان کرد. برهان تقریباً همین برهان (۹.۱۱) است، تنها

اختلاف عمده این است که چون نُرمها در $Q(\sqrt{d})$ می‌توانند منفی شوند، قضیه را به استقرا روی قدرمطلق نُرم اثبات می‌کنیم.

ولی، همان‌گونه که مثال زیر نشان می‌دهد، در حالت کلی تجزیهٔ یکتا برای اعداد صحیح $Q(\sqrt{d})$ نداریم.

مثال. نشان می‌دهیم که تجزیهٔ یکتا برای اعداد صحیح $Q(\sqrt{-6})$ برقرار نیست. ابتدا توجه می‌کنیم که یکه‌ها فقط ± 1 هستند. زیرا بنابر (iii. ۱۸.۱۱)، $x + y\sqrt{-6}$ یک یکه است اگر و تنها اگر $x^2 + 6y^2 = 1$، و تنها جوابهای صحیح این معادله عبارت‌اند از $x = \pm 1$، و $y = 0$.

سپس مشاهده می‌کنیم که $10 = 2 \times 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$؛ روشن است که نه $2 + \sqrt{-6}$ یک وابستهٔ ۲ یا ۵ است و نه $2 - \sqrt{-6}$. نشان می‌دهیم که ۲، ۵، و $2 \pm \sqrt{-6}$ همگی اول‌اند، و لذا ۱۰ دارای دو نمایش اساساً متفاوت به‌صورت حاصلضرب اعداد اول است.

نه ۲ و نه ۵ نمی‌توانند نُرم یک عدد صحیح از $Q\sqrt{-6}$ باشند، زیرا

$$\mathrm{N}(x + y\sqrt{-6}) = x^2 + 6y^2$$

و $x^2 + 6y^2$ نمی‌تواند مقادیر ۲ یا ۵ را اختیار کند. اکنون ثابت می‌کنیم که ۲ اول است. اگر $\alpha\beta = 2$، با نُرم‌گیری داریم $\mathrm{N}(\alpha)\mathrm{N}(\beta) = 4$؛ لذا $\mathrm{N}(\alpha) | 4$. چون $\mathrm{N}(\alpha) \neq 2$، باید داشته باشیم $\mathrm{N}(\alpha) = 1$ یا $\mathrm{N}(\alpha) = 4$، و بنابراین یا α یک یکه است یا β. به همین روش اساساً می‌توان نشان داد که ۵ و $2 \pm \sqrt{-6}$ اول‌اند.

همچنین، اعداد صحیح $Q(\sqrt{-6})$ لزوماً بزرگترین مقسوم‌علیه مشترک ندارند. مثلاً، فرض کنیم $\alpha = 10$ و $\beta = 5\sqrt{-6}$. اگر α و β دارای یک بزرگترین مقسوم‌علیه مشترک مانند δ باشند، آنگاه $\mathrm{N}(\delta)$ یک مقسوم‌علیه مشترک $\mathrm{N}(\alpha)$ و $\mathrm{N}(\beta)$ است، لذا $\mathrm{N}(\delta) | 50$. از طرفی $2 + \sqrt{-6}$ یک مقسوم‌علیه مشترک α و β است، زیرا $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$ و $5\sqrt{-6} = (2 + \sqrt{-6})(3 + \sqrt{-6})$. همچنین، آشکار است که ۵ نیز یک مقسوم‌علیه مشترک α و β است. از این‌رو $\mathrm{N}(5)$ و $\mathrm{N}(2 + \sqrt{-6})$ هر کدام $\mathrm{N}(\delta)$ را می‌شمارند، و لذا $\mathrm{N}(\delta) | 50$. در نتیجه $\mathrm{N}(\delta) = 50$: اما این ممکن نیست، زیرا به آسانی بررسی می‌شود که معادلهٔ $x^2 + 6y^2 = 50$ جواب صحیح ندارد.

توضیح. تجزیهٔ یکتا برای اعداد صحیح $Q(-\sqrt{5})$ نیز برقرار نیست؛ مسألهٔ ۱۱ـ۴۸ را ببینید.

در چند حالت، با کاربرد اساساً همان برهان مربوط به اعداد صحیح گاوسی، می‌توان یک قضیهٔ تجزیهٔ یکتا برای اعداد صحیح $Q(\sqrt{d})$ اثبات کرد.

(۱۹.۱۱) تعریف. $Q(\sqrt{d})$ اقلیدسی است اگر به‌ازای هر عدد صحیح α و β از $Q(\sqrt{d})$ با $\alpha \neq 0$، اعداد صحیح γ و ρ از $Q(\sqrt{d})$ وجود داشته باشند به‌طوری‌که $\beta = \gamma\alpha + \rho$ و $0 \leq \mathrm{N}(\rho) < \mathrm{N}(\alpha)$.

الگوریتم تقسیم معمولی به‌عنوان یک مبنا برای فصل ۱ به‌کار رفت، و از یک مشابه نزدیک (لم ۵.۱۱) درگسترش ویژگیهای تجزیهٔ اعداد صحیح گاوسی استفاده شد. اساساً همان الگوریتم تقسیم در تعریف بالا از «اقلیدسی» ساخته شد.

به شرطی که $Q(\sqrt{d})$ اقلیدسی باشد، می‌توان نتایج پایه‌ای اعداد صحیح گاوسی را دقیقاً به همان روش برای اعداد صحیح $Q(\sqrt{d})$ بیان و اثبات کرد.

(۲۰.۱۱) تجزیهٔ یکتا برای $Q(\sqrt{d})$. فرض می‌کنیم $Q(\sqrt{d})$ اقلیدسی باشد. فرض می‌کنیم $\alpha_1\alpha_2\cdots\alpha_r = \epsilon\beta_1\beta_2\cdots\beta_s$، که در آن α_i و β_i اعداد اولِ $Q(\sqrt{d})$ هستند و ϵ یک یکه است. در این صورت $r = s$، و می‌توان β_iها را تجدید آرایش کرد به‌طوری‌که به‌ازای هر i، β_i یک وابستهٔ α_i باشد.

با توجه به (۲۰.۱۱)، طبیعی است سعی کنیم هر تعداد ممکن d که به‌ازای آنها $Q(\sqrt{d})$ اقلیدسی است به‌دست آوریم. متأسفانه، $Q(\sqrt{d})$ به‌ندرت اقلیدسی است. می‌توان برهان (۵.۱۱) را با اندک تغییری به‌کار برد و نشان داد که $Q(\sqrt{d})$ به‌ازای $d = \pm 2$ و ± 3 برای d اقلیدسی است (مسألهٔ ۵۶.۱۱ را ببینید). در واقع، اثبات اینکه تنها مقادیری از اعداد منفی و خالی از مربع d که به‌ازای آنها $Q(\sqrt{d})$ اقلیدسی است عبارت‌اند از -1، -2، -3، -7، و -11 دشوار نیست. همچنین، معلوم شده است که تنها مقادیری از عدد مثبتِ خالی از مربع d که به‌ازای آنها $Q(\sqrt{d})$ اقلیدسی است عبارت‌اند از اعداد صحیح معمولی ۱، ۲، ۳، ۵، ۶، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۱، ۲۹، ۳۳، ۳۷، ۴۱، ۵۷، ۷۳.

توضیحات. ۱. تجزیهٔ یکتا برای اعداد صحیح $Q(\sqrt{-3})$ برقرار است (قضیهٔ ۲۰.۱۱ و مسألهٔ ۵۶.۱۱ را ببینید)، ولی برای مجموعهٔ اعداد به‌صورت $x + y\sqrt{-3}$، که x و y اعداد صحیح معمولی هستند، برقرار نیست (مسألهٔ ۴۷.۱۱ را ببینید).

۲. حتی اگر $Q(\sqrt{d})$ اقلیدسی نباشد امکان دارد که اعداد صحیح $Q(\sqrt{d})$ دارای تجزیهٔ یکتا باشند؛ برای تفصیل بیشتر توضیحات فصل را ببینید.

اعداد اول $Q(\sqrt{d})$ و معادلات دیوفانتی

در ادامه به این مسأله می‌پردازیم که کدام اعداد اول p را می‌توان به‌صورت $p = x^2 + 2y^2$، که x و y اعداد صحیح هستند، نمایش داد. فرما پاسخ این سؤال را می‌دانست، اما روشن نیست که

برهانی داشته است. روشن است که، ۲ چنین نمایشی دارد، و لذا فرض می‌کنیم p فرد باشد.

فرض کنیم $p = x^2 + 2y^2$. چون x فرد است، داریم $x^2 \equiv 1 \pmod 8$. همچنین، چون $2y^2 \equiv 0 \pmod 8$ یا $2y^2 \equiv 4 \pmod 8$، در نتیجه $p \equiv 1 \pmod 8$ یا $p \equiv 3 \pmod 8$. لذا نمی‌توان اعداد اول $8k + 5$ یا $8k + 7$ را به‌صورت $x^2 + 2y^2$ نمایش داد. نشان خواهیم داد که اعداد اول $8k + 1$ یا $8k + 3$ را می‌توان به‌صورت $x^2 + 2y^2$ نمایش داد.

فرض کنیم p یک عدد اول (گویا) به‌صورت $8k + 1$ یا $8k + 3$ باشد. بنابر (i.۱۳.۵)، -2 یک ماندهٔ درجهٔ دوم p است، و لذا عدد صحیح x وجود دارد به‌طوری که $x^2 \equiv -2 \pmod p$، پس $p | (x + \sqrt{-2})(x - \sqrt{-2})$. چون $Q(\sqrt{-2})$ اقلیدسی است، نظیر لم (۸.۱۱) برقرار است. از این‌رو، اگر p در $Q(\sqrt{-2})$ اول باشد، خواهیم داشت $p | x - \sqrt{-2}$ یا $p | x + \sqrt{-2}$. اما روشن است که $p | (x \pm \sqrt{-2})$، لذا p اول نیست.

بنابراین اعداد صحیح α و β از $Q(\sqrt{-2})$، که هیچ‌کدام یک یکه نیستند، وجود دارند به‌طوری‌که $p = \alpha\beta$. با نُرم‌گیری داریم $p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$، و لذا $\mathrm{N}(\alpha) = p$. اگر $\alpha = x + y\sqrt{-2}$، آنگاه داریم $p = \mathrm{N}(\alpha) = x^2 + 2y^2$، و لذا p قابل نمایش به‌صورت $x^2 + 2y^2$ است. بنابراین قضیهٔ زیر را ثابت کرده‌ایم:

(۲۱.۱۱) قضیه. عدد اول p قابل نمایش به‌صورت $p = x^2 + 2y^2$ است اگر و تنها اگر $p = 2$ یا $p \equiv 1$ یا $3 \pmod 8$.

همچنین، می‌توانیم تمام اعداد صحیحی را که نمایشی به‌صورت $x^2 + 2y^2$ دارند مشخص کنیم، تعداد نمایشها را به‌دست آوریم، و مانند آن. استدلالها اساساً با استدلالهای نظیر برای $x^4 + y^2$ که در (۱۲.۱۱) و (۱۳.۱۱) ارائه شده‌اند یکی هستند.

(۲۲.۱۱) قضیه. عدد صحیح مثبت n قابل نمایش به‌صورت $x^2 + 2y^2$ است اگر و تنها اگر $n = 2^a \prod p_j^{a_j} \prod q_j^{b_j}$، که در آن هر p_j عدد اولی است به‌صورت $8k + 1$ یا $8k + 3$، هر q_j عدد اولی به‌صورت $8k + 5$ یا $8k + 7$، و هر b_j زوج است. اگر n قابل نمایش باشد، آنگاه دارای $2 \prod (a_j + 1)$ نمایش است.

یک استدلال اساساً واحد برای $x^2 + 3y^2$ کارساز است. می‌توان مفاهیم مشابه را برای نمایشها توسط $x^2 - dy^2$ به‌کار برد، که d یک عدد صحیح خالی از مربع است به‌طوری‌که اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا دارند. اگر تجزیهٔ یکتا نداشته باشیم، مسأله بسیار دشوارتر است.

می‌توان کاربردهای دیگری از حساب $Q(\sqrt{d})$ در معادلات دیوفانتی را در مسأله‌های ۵۷.۱۱ و ۵۸.۱۱ مشاهده کرد.

یکه‌های $Q(\sqrt{d})$

در این بخش، یکه‌های $Q(\sqrt{d})$ را که در آن d خالی از مربع است بررسی می‌کنیم. بررسی $d < 0$ آسان است، ولی وضعیت برای $d > 0$ پیچیده‌تر است.

فرض کنیم d منفی باشد. چون d خالی از مربع است، پس همنهشت با ۱، ۲، یا ۳ به پیمانهٔ ۴ است. اگر $d \not\equiv 1 \pmod 4$، آنگاه هر عدد صحیح α از $Q(\sqrt{d})$ به‌صورت $x + y\sqrt{d}$ است، که در آن x و y اعداد صحیح هستند. ملاحظه می‌کنید که $\mathrm{N}(\alpha) = x^2 + |d|y^2$. اگر $d \le -2$، آنگاه $x^2 + |d|y^2 \ge x^2 + 2y^2$. چون بجز $y = 0$ داریم $x^2 + 2y^2 \ge 2$، پس ± 1 تنها عناصر با نُرم ۱ هستند. اگر $d = -1$، آنگاه یکه‌ها عبارت‌اند از ± 1 و $\pm i$.

حال فرض می‌کنیم $d \equiv 1 \pmod 4$. همانند بند بالا، می‌توانیم نشان دهیم که تنها یکه‌های صورت $x + y\sqrt{d}$ که x و y اعداد صحیح‌اند اعداد ± 1 هستند. سپس یکه‌های صورت $\alpha = (x + y\sqrt{d})/2$ را که در آن x و y فرد هستند، جستجو می‌کنیم. با نُرم‌گیری، می‌بینیم که α یک یکه است اگر و تنها اگر $x^2 + |d|y^2 = 4$. اگر $d \le -7$ آنگاه $x^2 + |d|y^2 > 4$ مگر آنکه $y = 0$؛ به‌ویژه، y فرد نیست. سرانجام، فرض می‌کنیم $d = -3$؛ در این صورت جوابها فرد معادلهٔ دیوفانتی $x^2 + 3y^2 = 4$ را جستجو می‌کنیم. روشن است که $x = \pm 1$، $y = \pm 1$ جوابها هستند. می‌توانیم این حالت را در قضیهٔ زیر خلاصه کنیم:

(۲۳.۱۱) قضیه. فرض کنیم $d < 0$ خالی از مربع باشد، یکه‌های $Q(\sqrt{d})$ برابرند با ± 1 مگر آنکه $d = -1$ یا $d = -3$. اگر $d = -1$، یکه‌ها ± 1 و $\pm i$، و اگر $d = -3$، یکه‌ها ± 1، $\pm(1 + \sqrt{-3})/2$، و $\pm(1 - \sqrt{-3})/2$ هستند.

دیدیم که اگر $d < 0$، $Q(\sqrt{d})$ تنها تعداد متناهی، معمولاً دو، یکه دارد. وقتی d مثبت باشد وضعیت کاملاً متفاوت است. بنابر (iii.۱۸.۱۱)، اگر $x^2 - dy^2 = \pm 1$، آنگاه $x + y\sqrt{d}$ یک یکه از $Q(\sqrt{d})$ است. اما قضیهٔ ۷.۱۰ نشان می‌دهد که معادلهٔ پِل $x^2 - dy^2 = 1$ بی‌نهایت جواب صحیح دارد، و بنابراین $Q(\sqrt{d})$ دارای تعداد نامتناهی یکه است.

قضیهٔ بعد شرح کاملی از یکه‌ها در حالت $d > 1$ به‌دست می‌دهد.

(۲۴.۱۱) قضیه. اگر $d > 1$، یکهٔ یکتای $\epsilon > 1$ از $Q(\sqrt{d})$ وجود دارد به‌طوری که هر یکه به‌صورت $\pm\epsilon^n$ است، که در آن n یک عدد صحیح، مثبت، منفی، یا صفر است. (یکهٔ ϵ یکهٔ اصلی $Q(\sqrt{d})$ خوانده می‌شود.)

برهان. ابتدا نشان می‌دهیم که اگر λ یک یکه بجز ± 1 باشد، یکی از مقادیر λ، $1/\lambda$، $-\lambda$،

یا $-۱/\lambda$ به‌صورت $u+v\sqrt{d}$ است، که در آن u و v مثبت‌اند. برحسب آنکه $\mathrm{N}(\lambda)=۱$ یا $\mathrm{N}(\lambda)=-۱$، دو حالت برای بررسی وجود دارد.

قرار می‌دهیم $\lambda=a+b\sqrt{d}$؛ و ابتدا فرض می‌کنیم که $\mathrm{N}(\lambda)=۱$. با تغییر علامت λ در صورت لزوم، می‌توانیم فرض کنیم که $a>۰$. اگر $b>۰$، آنگاه خود λ صورت مناسب را داراست. در غیر این‌صورت، $۱/\lambda=\bar{\lambda}/\lambda\bar{\lambda}=\bar{\lambda}=a-b\sqrt{d}$، و بنابراین $۱/\lambda=a+(-b)\sqrt{d}$، که در آن a و $-b$ مثبت‌اند.

حال، فرض می‌کنیم که $\mathrm{N}(\lambda)=-۱$. با تغییر علامت λ در صورت لزوم، می‌توانیم فرض کنیم که $b>۰$. اگر $a>۰$، کار تمام است. اگر نه، $۱/\lambda=\bar{\lambda}/\lambda\bar{\lambda}=-\bar{\lambda}=-a+b\sqrt{d}$، و لذا $۱/\lambda$ صورت مناسب است.

بنابراین کافی است یکه‌های λ به‌صورت $u+v\sqrt{d}$ را، که u و v مثبت‌اند بررسی کنیم. آشکار است که این چنین یکه بزرگتر از ۱ است، و تمام یکه‌های بزرگتر از ۱ به این صورت هستند، زیرا $-\lambda$، $۱/\lambda$، و $-۱/\lambda$ نمی‌توانند به این صورت باشند. وجود یکه‌های به این صورت از (۷.۱۰) نتیجه می‌شود.

به‌ازای هر عدد حقیقی x، تنها تعداد متناهی عدد صحیح به‌صورت $u+v\sqrt{d}$ با u و v مثبت و $۱<u+\sqrt{d}\le x$ از $Q(\sqrt{d})$ وجود دارند. بنابراین یک کوچکترین یکهٔ $\epsilon>۱$ وجود دارد. نشان می‌دهیم که ϵ یکهٔ اصلی است.

کافی است نشان دهیم که هر یکهٔ $\lambda>۱$ توانی از ϵ است. آشکار است که λ بین دو توان متوالی ϵ واقع می‌شود. فرض کنیم $\epsilon^n<\lambda\le\epsilon^{n+۱}$؛ در این صورت λ/ϵ^n یک یکهٔ بزرگتر از ۱ است. اگر $\lambda\ne\epsilon^{n+۱}$، آنگاه $\lambda/\epsilon^n<\epsilon$، و این مطلب با کوچکترین یکهٔ بزرگتر از ۱ بودن ϵ تناقض دارد. لذا $\lambda=\epsilon^{n+۱}$، و قضیه ثابت می‌شود.

توضیحات. ۱. اگر $d\equiv ۲ \pmod ۴$ یا ۳، آنگاه یکه‌های $Q(\sqrt{d})$ دقیقاً از جوابهای معادلهٔ پل $x^۲-dy^۲=\pm ۱$ حاصل می‌شوند، و لذا قضیهٔ ۲۴.۱۱ نتیجهٔ بلافصل قضیه‌های فصل ۱۰ خواهد بود. به‌ویژه، یکهٔ اصلی $Q(\sqrt{d})$ عدد $a+b\sqrt{d}$ است، که در آن (a,b) کوچکترین جواب مثبت $x^۲-dy^۲=-۱$ است، اگر حلپذیر باشد، و الّا کوچکترین جواب مثبت $x^۲-dy^۲=۱$ است.

۲. وقتی $d\equiv ۱ \pmod ۴$، وضعیت پیچیده‌تر است زیرا اعداد صحیح $Q(\sqrt{d})$ به‌صورت $(x+y\sqrt{d})/۲$ نیز می‌توانند باشند، که در آن x و y اعداد صحیح فرد هستند. در این حالت، چون $\mathrm{N}((x+y\sqrt{d})/۲)=(x^۲-dy^۲)/۴$، یکهٔ اصلی $Q(\sqrt{d})$ عدد $(a+y\sqrt{d})/۲$ است، که

در آن (a,y) کوچکترین جواب مثبت $x^۲-dy^۲=-۴$ است. اگر این معادله حلپذیر باشد، در غیر این‌صورت کوچکترین جواب مثبت $x^۲-dy^۲=۴$ است. (معادلهٔ $x^۲-dy^۲=۴$ همواره حلپذیر است: اگر (u,v) یک جواب $x^۲-dy^۲=۱$ باشد، آنگاه $(۲u,۲v)$ یک جواب $x^۲-dy^۲=۴$ خواهد بود).

مثالها. (الف) فرض کنیم $d=۳$. معادلهٔ $x^۲-۳y^۲=-۱$ حلپذیر نیست، زیرا همنهشتی $x^۲\equiv -۱ \pmod ۳$ جواب ندارد. بنابراین یکهٔ اصلی $Q(\sqrt{۳})$ عدد $۲+\sqrt{۳}$ است، زیرا $(۲,۱)$ جواب اصلی $x^۲-۳y^۲=۱$ است.

(ب) اگر $d=۱۰$، آنگاه $d\equiv ۲ \pmod ۴$ و $(۳,۱)$ کوچکترین جواب مثبت $x^۲-۱۰y^۲=-۱$ است. لذا $۳+\sqrt{۱۰}$ یکهٔ اصلی $Q(\sqrt{۱۰})$ است.

(ج) فرض کنیم $d=۵$. چون $d\equiv ۱ \pmod ۴$، یکهٔ اصلی $Q(\sqrt{۵})$ عدد $(a+b\sqrt{۵})/۲$ است، که در آن (a,b) کوچکترین جواب مثبت $x^۲-۵y^۲=-۴$ است. اگر این معادله حلپذیر باشد، در غیر این‌صورت، کوچکترین جواب مثبت $x^۲-۵y^۲=۴$ است. آشکار است که $(۱,۱)$ کوچکترین جواب مثبت $x^۲-۵y^۲=-۴$ است، و لذا $(۱+\sqrt{۵})/۲$ یکهٔ اصلی $Q(\sqrt{۱۰})$ است.

مسأله‌ها و راه‌حلها

اعداد صحیح گاوسی و اعداد اول گاوسی

۱.۱۱ آیا ۷ عدد $(۴+۵i)(۸-i)$ را می‌شمارد؟

حل. نه. یا با محاسبهٔ حاصلضرب $(۴+۵i)(۸-i)$ مستقیماً می‌توان دید که ۷ آن را نمی‌شمارد، یا ملاحظه کنید که نُرم $(۴+۵i)(۸-i)$ برابر ۶۵×۴۱ است، که بر نُرم ۷ بخشپذیر نیست.

۲.۱۱ به‌ازای کدام‌یک از اعداد صحیح گاوسی α، مزدوج $\bar{\alpha}$ یک وابستهٔ α است؟

حل. اگر $\alpha=s+ti$، آنگاه $\bar{\alpha}=s-ti$. می‌خواهیم که $s-ti$ یکی از اعداد $s+ti$، $-t+si$، $-s-ti$، یا $t-si$ باشد. برای حالت اول، لازم است که $t=۰$؛ برای حالت دوم، $s=-t$؛ برای حالت سوم، $s=۰$؛ و برای حالت چهارم، $s=t$. لذا α به‌صورت a، $a(۱-i)$، ai، یا $a(۱+i)$ است، که a یک عدد صحیح گویاست.

۳.۱۱ فرض کنید $\alpha=۳+۴i$ و $\beta=۴۰+۱۰i$. با به‌کار بردن روند بیان‌شده در برهان (۵.۱۱)، اعداد صحیح گاوسی γ و ρ را بیابید به‌طوری‌که $\beta=\gamma\alpha+\rho$ و $N(\rho)<N(\alpha)$.

حل. نمادگذاری (۵.۱۱) را به‌کار می‌بریم. فرض کنیم $\beta/\alpha = x + yi$. با «گویا کردن» مخرج داریم $x = ۱۶۰/۲۵$ و $y = -۱۳۰/۲۵$. از این‌رو، نزدیکترین عدد صحیح به x و y عبارت‌اند از $u = ۶$ و $v = -۵$، و لذا $\gamma = ۶ - ۵i$ را انتخاب می‌کنیم. بنابراین، $\rho = \beta - \gamma\alpha = ۲ + i$.

۴.۱۱ راست یا دروغ: اگر α و β اعداد صحیح گاوسی باشند و $\mathrm{N}(\alpha)|\mathrm{N}(\beta)$، آنگاه $\alpha|\beta$.

حل. در حالت کلی برقرار نیست. مثلاً اگر $\alpha = ۲ + i$ و $\beta = ۲ - i$، آنگاه هر یک از α و β دارای نُرم ۵ است، اما $\alpha \nmid \beta$. (می‌توان این مطلب را مستقیماً با تقسیم کردن بررسی کرد، یا توجه کرد که نُرم α و β اول است، و لذا α و β اول هستند، اما وابسته نیستند.)

۵.۱۱ فرض کنیم $a + bi$ یک عدد صحیح گاوسی باشد. ثابت کنید $۱ + i$ عدد $a + bi$ را می‌شمارد اگر و تنها اگر a و b هر دو مزدوج یا هر دو فرد باشند.

حل. با تقسیم $a + bi$ بر $۱ + i$، و «گویا کردن مخرج» به دست آوریم

$$\frac{a+bi}{۱+i} = \frac{a+bi}{۱+i}\frac{۱-i}{۱-i} = \frac{a+b}{۲} + \frac{b-a}{۲}i.$$

اما $a + b$ زوج است اگر و تنها اگر a و b دارای زوجیت یکسان باشند، همین مطلب در مورد $b - a$ نیز صادق است. لذا $(a + bi)/(۱ + i)$ یک عدد صحیح گاوسی است اگر و تنها اگر a و b هر دو زوج یا هر دو فرد باشند.

برهان دیگر. به آسانی دیده می‌شود که $\mathrm{N}(a + bi)$ زوج است اگر و تنها اگر a و b دارای زوجیت یکسان باشند. چون تنها اعداد اول گاوسی با نُرم زوج، $i + ۱$ و وابسته‌اش می‌باشند، مسأله ثابت می‌شود.

۶.۱۱ بررسی معادلهٔ دیوفانتی $x^۲ - y^۲ = n$ را که در ابتدای فصل ارائه شد با بحث در حالتی‌که n زوج است کامل کنید.

حل. جوابهای صحیح $x^۲ - y^۲ = n$ را که در آن n عدد صحیح زوج غیرصفری است به‌دست می‌آوریم. چون $x^۲ - y^۲ = (x - y)(x + y)$ و $x - y$ و $x + y$ همواره زوجیت یکسان دارند، لذا $(x - y)(x + y)$ تنها وقتی زوج است که $x - y$ و $x + y$ هر دو زوج باشند. لذا اگر $x^۲ - y^۲ = n$، آنگاه n بایستی مضرب ۴ باشد. اگر $n = ۴m$، آنگاه هر یک از $x - y$ و $x + y$ دو برابر یک مقسوم‌علیه m است. اگر d یک مقسوم‌علیه (مثبت یا منفی) از m باشد، قرار می‌دهیم $x + y = ۲d$ و $x - y = ۲m/d$. در این صورت، دیده می‌شود که $x = d + m/d$

و $y = d - m/d$ اعداد صحیح هستند، و $x^۲ - y^۲ = n$. علاوه‌بر این، تمام جفتهای (x, y) که در معادله صدق می‌کنند از این طریق به دست می‌آیند. تعداد $۲\tau(|m|)$ انتخاب برای d وجود دارد، و لذا اگر n زوج باشد، معادلهٔ $x^۲ - y^۲ = n$ دارای $۲\tau(|m|)$ جواب است.

۷.۱۱ راست یا دروغ: اگر $a + bi$ یک عدد اول گاوسی باشد، $a - bi$ نیز یک عدد اول گاوسی است. $b + ai$ چطور؟

حل. ادعا درست است. اگر $a - bi = (s + ti)(u + vi)$، که در آن نه $s + ti$ یک یکه است و نه $u + vi$، آنگاه با مزدوج‌گیری داریم $a + bi = (s - ti)(u - vi)$، و نه $s - ti$ یک یکه است و نه $u - vi$.

اگر $a + bi$ یک عدد اول گاوسی باشد، آنگاه $a - bi$ نیز هست. چون $b + ai = -i(a - bi)$، لذا $b + ai$ وابستهٔ یک عدد اول گاوسی و لذا یک عدد اول گاوسی است.

۸.۱۱ کدام‌یک از اعداد زیر اعداد اول گاوسی هستند؟ $۴i + ۳$، $۴i - ۳$، $۵i$، $-۱۱i$.

حل. بنابر (۱۱.۱۱)، اعداد اول گاوسی عبارت‌اند از $i + ۱$ و وابسته‌هایش، اعداد اول گویایی به‌صورت $۴k + ۳$ و وابسته‌هایشان، و اعداد به‌صورت $a + bi$، که در آن $a^۲ + b^۲$ عدد اولی به‌صورت $۴k + ۱$ است. روشن است که، $۴i + ۳$ هیچ‌کدام از اینها نیست، زیرا نُرم $۴i + ۳$ برابر $۵^۲ = ۲۵$ است، و ۵ عدد اولی به‌صورت $۴k + ۱$ است. در واقع، به آسانی دیده می‌شود که $۴i + ۳ = (۲ + i)^۲$. به دلیل مشابه، $۴i - ۳$ نیز عدد اول گاوسی نیست. $۵i$ اول گاوسی نیست، زیرا به آسانی دیده می‌شود که ۵ بر عدد اول $i + ۲$ بخشپذیر است. سرانجام، $-۱۱i$ یک عدد اول گاوسی است، زیرا وابستهٔ ۱۱ است که عدد اول گویایی به‌صورت $۴k + ۳$ است.

۹.۱۱ ثابت کنید بی‌نهایت عدد اول گاوسی به‌صورت $a + bi$؛ $a \neq ۰$ و $b \neq ۰$ وجود دارد.

حل. فرض کنیم p عدد اول گویایی به‌صورت $۴k + ۱$ باشد، در این صورت p نمایشی به‌صورت مجموع دو مربع غیرصفر مانند $a^۲ + b^۲$ دارد. قرار می‌دهیم $\pi = a + bi$. روشن است که، ۲های متمایز πهای متمایز به‌دست می‌دهند، و بنابر مسألهٔ ۵ـ۲۳، بی‌نهایت عدد اول به‌صورت $۴k + ۱$ وجود دارد، بنابراین بی‌نهایت عدد اول گاوسی به این صورت مشخص وجود دارد.

۱۰.۱۱ فرض می‌کنیم نُرم γ برابر $q^۲$ باشد، که در آن q عدد اولی به‌صورت $۴k + ۳$ است. آیا γ یک عدد اول گاوسی است؟

حل. فرض کنیم $\gamma = \alpha\beta$. اگر $N(\gamma) = q^2$ که q یک عدد اول گویاست، آنگاه $N(\alpha)$ برابر ۱، q، یا q^2 است. اما اگر q به‌صورت $4k+3$ باشد، $N(\alpha) = q$ برقرار نیست، زیرا هیچ عددی به این صورت مجموع دو مربع نیست. لذا $N(\alpha) = 1$ یا $N(\alpha) = q^2$، و بنابراین یا α یک یکه است یا β. لذا γ یک عدد اول گاوسی است.

۱۱.۱۱ $3+i$ و $6+7i$ را به‌صورت حاصلضرب اعداد اول گاوسی بیان کنید.

حل. چون نُرم $3+i$ برابر ۱۰ است، لذا تنها مقسوم‌علیه‌های اولِ ممکن برای $3+i$ مقسوم‌علیه‌های اول ۲ و ۵، یعنی وابسته‌های $1+i$ و $2 \pm i$ هستند. $3+i$ را بر $1+i$ تقسیم می‌کنیم (این آسانترین راه گویاکردن مخرج است، یعنی صورت و مخرج را در $1-i$ ضرب کنیم)؛ لذا $3+i = (1+i)(2-i)$.

نُرم $6+7i$ برابر $85 = 5 \times 17$ است. چون ۵ و ۱۷ اعداد اول به‌صورت $4k+1$ هستند، لذا تنها مقسوم‌علیه‌های اول گاوسی $6+7i$ عبارت‌اند از $2 \pm i$، $4 \pm i$، و وابسته‌هایشان. اگر $6+7i$ را بر $2+i$ تقسیم کنیم، می‌بینیم که خارج‌قسمت یک عدد صحیح گاوسی نیست. اگر بر $2-i$ تقسیم کنیم خارج‌قسمت $1+4i$ را به‌دست می‌آوریم، که دارای نُرم ۱۷ است و لذا اول است. بنابراین، $6+7i = (2-i)(1+4i)$ تجزیهٔ $6+7i$ به اعداد اول است.

۱۲.۱۱ $60+105i$ را به‌صورت حاصلضرب اعداد اول گاوسی بنویسید.

حل. چون $60+105i = 15(4+7i)$، کافی است ۱۵ و $4+7i$ را تجزیه کنیم. داریم $15 = 3(2+i)(2-i)$، و هر عامل اول است. چون $N(4+7i) = 65 = 5 \times 13$، $4+7i$ یا بر $2+i$ بخشپذیر است یا بر $2-i$. می‌بینیم که $4+7i = (2+i)(3+2i)$، و چون نُرم هر عامل اول است، پس $4+7i$ اول است. لذا $60+105i = 3(2+i)^2(2-i)(3+2i)$ یکی از تجزیه‌های $60+105i$ به اعداد اول است.

۱۳.۱۱ یک تجزیه به اعداد اول از $239+i$ به دست آورید.

حل. چون $N(239+i)$ زوج است، پس $239+i$ بر $1+i$ بخشپذیر است. اگر عمل تقسیم را انجام دهیم خارج قسمت $120+119i$ را به‌دست می‌آوریم. چون

$$N(120+119i) = 28561 = 13^4$$

لذا عاملهای اول با نُرم ۱۳ را جستجو می‌کنیم. عاملهای ممکن عبارت‌اند از $3 \pm 2i$ (و وابسته‌هایشان). توجه می‌کنیم که $60+105i$ نمی‌تواند بر $3+2i$ و $3-2i$ هر دو بخشپذیر

باشد، زیرا در غیر این صورت، بر ۱۳ بخشپذیر خواهد شد، که این طور نیست. اگر بر $۲i+۳$ تقسیم کنیم، داریم

$$۱۲۰+۱۱۹i=(۳+۲i)(۴۶+۹i)=(۳+۲i)^۲(۱۲-۵i)=(۳+۲i)^۳(۲-۳i)$$

لذا $(۳+۲i)^۴=-i(۱۲۰+۱۱۹i)$، و از این‌رو $(۳+۲i)^۴(۱-i)=۲۳۹+i$ یک تجزیه به اعداد اول از $۲۳۹+i$ است.

۱۴.۱۱ چه تعداد عدد صحیح گاوسی دارای نُرم ۱۸۰۰ هستند؟ چه تعداد از اینها عدد صحیح گویا هستند؟

حل. نُرم یک عدد صحیح گویای n برابر $n^۲$ است، لذا نُرم هیچ عدد صحیح گویا برابر ۱۸۰۰ نمی‌شود. تعیین تعداد اعداد صحیح گاوسی با نُرم ۱۸۰۰، به تعیین تعداد جوابهای معادلهٔ دیوفانتی $u^۲+v^۲=۱۸۰۰$ برمی‌گردد. اما $۱۸۰۰=۲^۳\times۳^۲\times۵^۲$، و لذا بنابر (۱۲.۱۱)، تعداد $۴\times(۲+۱)=۱۲$ عدد صحیح گاوسی با نُرم ۱۸۰۰ وجود دارد.

۱۵.۱۱ تمام اعداد صحیح گاوسی با نُرم ۱۶۹ را به‌دست آورید.

حل. حل معادلهٔ $(u-vi)(u-vi)=۱۶۹$ را لازم داریم. چون $۱۶۹=۱۳^۲$ و $۱۳=۲^۲+۳^۲$، لذا ۱۶۹ دارای تجزیه به عوامل اول به صورت $(۲+۳i)^۲(۲-۳i)^۲=۱۶۹$ است. لذا $u+vi=\epsilon(۲+۳i)^k(۲-۳i)^{۲-k}$، که ϵ یک یکه است و $۰\le k\le ۲$ (برهان (۱۲.۱۱) را ببینید). اگر بگیریم $\epsilon=۱$، نتیجه می‌گیریم که $u+vi$ یکی از اعداد $۱۲i-۵$، ۱۳، یا $۱۲i+۵-$ است؛ اگر سایر یکه‌ها را اختیار کنیم وابسته‌های اینها به‌دست می‌آیند. لذا اعداد صحیح گاوسی با نُرم ۱۶۹ عبارت‌اند از: $۱۲i-۵-$، $۵i-۱۲$، $۱۲i+۵$، $۵i+۱۲-$، ۱۳، $۱۳i$ ، $۱۳-$، $۱۳i-$، $۱۲i+۵-$، $۵i-۱۲-$، $۱۲i-۵$، و $۵i+۱۲$.

۱۶.۱۱ فهرستی از تمام اعداد اول گاوسی که نُرمشان از ۶۰ تجاوز نمی‌کند فراهم کنید. برای آنکه این فهرست کوتاهتر باشد، تنها یکی از π، $-\pi$، $i\pi$، و $-i\pi$ را فهرست کنید.

حل. روشن است که، $۱+i$ یک چنین عدد اولی است. سپس تمام اعداد اول گویای p به‌صورت $۴k+۳$ را که $p^۲\le ۶۰$ فهرست می‌کنیم؛ اینها ۳ و ۷ هستند. بعد به جستجوی تمام اعداد اول p به‌صورت $۴k+۱$ با $p\le ۶۰$ می‌پردازیم و هر یک را به صورت مجموع دو مربع بیان می‌کنیم. در هر مرحله، دو عدد اول، به‌صورت جفتهای مزدوج، به دست می‌آوریم. اینها عبارت‌اند از $i\pm ۲$، $۲i\pm ۳$، $۴\pm ۲i$، $۵\pm i$، $۶\pm ۴i$، $۵\pm ۲i$، و $۷\pm ۲i$.

۱۷.۱۱ معادلهٔ $x+y+z=xyz=1$ را در اعداد صحیح گاوسی حل کنید.

حل. چون $xyz=1$، تمام متغیرها یکه‌اند و لذا بایستی از ± 1، $\pm i$ انتخاب شوند. همچنین، یا همهٔ آنها حقیقی هستند یا دقیقاً یکی حقیقی است. اگر همگی حقیقی باشند، آنگاه از $x+y+z=1$ نتیجه می‌شود که دوتای آنها برابر 1 و دیگری -1 است، و این با $xyz=1$ تناقض دارد. لذا دقیقاً دو تا از x، y، و z موهومی هستند، و چون $x+y+z=1$، این دو بایستی i و $-i$ باشند؛ سپس $xyz=1$ ایجاب می‌کند که سومین عدد 1 باشد. بنابراین جوابها شش جایگشت $(1,i,-i)$ هستند.

۱۸.۱۱ یک بزرگترین مقسوم‌علیه مشترک از $6i+4$ و $6i-4$ به‌دست آورید.

حل. کافی است که یک بزرگترین مقسوم‌علیه مشترک از $3i+2$ و $3i-2$ پیدا کنیم. نُرم هر یک از اینها ۱۳ است، که اول است، لذا $3i+2$ و $3i-2$ اول‌اند. واضح است که، آنها وابسته نیستند، و لذا ۲ یک بزرگترین مقسوم‌علیه مشترک $6i+4$ و $6i-4$ است.

۱۹.۱۱ (الف) نشان دهید که $3i+10$ یک بزرگترین مقسوم‌علیه مشترک $47i-25$ و $16i+17$ است. (ب) $47i-25$ و $16i+17$ را به‌صورت حاصلضرب اعداد اول گاوسی بیان کنید.

حل. (الف) (ب)، هر یک از $47i-25$ و $16i+17$ را بر $3i+10$ تقسیم می‌کنیم (یک راه مناسب برای انجام این کار گویا کردن مخرج با ضرب «بالا» و «پایین» در $3i-10$ است). خارج‌قسمتها به‌ترتیب عبارت‌اند از $5i-1$ و $i+2$. عامل $5i-1$ را تجزیه می‌کنیم، توجه می‌کنیم که چون -1 و 5 فرد هستند $5i-1$ بر $i+1$ بخشپذیر است. داریم $5i-1=(1+i)(2+3i)$، و لذا $-25+47i=(1+i)(2+3i)(10+3i)$. چون نُرم هر عامل اول است، پس یک تجزیه به اعداد اول از $47i-25$ به‌دست آورده‌ایم. همچنین، $16i+17=(2+i)(10+3i)$، و چون نُرم هر عامل اول است، یک تجزیه به اعداد اول از $16i+17$ یافته‌ایم. چون $i+2$ یک وابسته از $1+i$ یا $3i+2$ نیست، لذا $3i+10$ یک بزرگترین مقسوم‌علیه مشترک $47i-25$ و $16i+17$ است.

◁ **۲۰.۱۱** عطف به تعریف (۶.۱۱) نشان دهید که γ یک بزرگترین مقسوم‌علیه مشترک α و β است اگر و تنها اگر γ یک مقسوم‌علیه مشترک باشد، و به‌ازای هر مقسوم‌علیه λ، $N(\lambda)\le N(\gamma)$.

حل. اگر γ یک یزرگترین مقسوم‌علیه مشترک α، β، λ یک مقسوم‌علیه مشترک باشد، آنگاه

$\gamma \not| \lambda$. از این‌رو $N(\lambda)|N(\gamma)$ و لذا $N(\lambda)N(\gamma)$. بعکس، فرض کنیم که λ یک مقسوم‌علیه مشترک α و β با نُرم ماکسیمم باشد، و فرض می‌کنیم δ یک بزرگترین مقسوم‌علیه مشترک α و β برطبق تعریف (۶.۱۱) باشد. لذا $\gamma|\delta$؛ فرض کنیم $\gamma = \mu\delta$. چون در میان مقسوم‌علیه‌های مشترک، نُرم γ ماکسیمم است، در نتیجه $N(\mu) = ۱$ و لذا μ یک یکه است. بنابراین γ یک بزرگترین مقسوم‌علیه مشترک α و β است («توضیح» بعد از (۷.۱۱) را ببینید).

توضیح. تعریف بزرگترین مقسوم‌علیه مشترک که در این فصل به‌کار می‌بریم یکی از ویژگیهای مقسوم‌علیه مشترک معمولی دو عدد صحیح گویاست ((۶.۱) را ببینید). تعریف جدید از نظر جبری طبیعی‌تر است و حتی در وضعیتهایی که هیچ مفهوم روشنی از اندازه وجود ندارد دارای معنی است.

۲۱.۱۱ اثبات یا رد کنید: اگر α و β دو عدد صحیح گاوسی باشند و δ یک بزرگترین مقسوم‌علیه مشترک α و β باشد، آنگاه $\bar{\delta}$ یک بزرگترین مقسوم‌علیه مشترک $\bar{\alpha}$ و $\bar{\beta}$ است.

حل. درست است. چون $\alpha|\delta$، لذا γای وجود دارد به‌طوری‌که $\alpha = \gamma\delta$، و از این‌رو، $\bar{\alpha} = \bar{\gamma}\bar{\delta}$. در نتیجه $\bar{\alpha}|\bar{\delta}$؛ با استدلالی مشابه، $\bar{\beta}|\bar{\delta}$، لذا $\bar{\delta}$ یک مقسوم‌علیه مشترک $\bar{\alpha}$ و $\bar{\beta}$ است. حال، فرض کنیم $\bar{\mu}$ یک مقسوم‌علیه مشترک $\bar{\alpha}$ و $\bar{\beta}$ باشد. به آسانی دیده می‌شود که μ یک مقسوم‌علیه مشترک α و β است، و لذا $\mu|\delta$، زیرا δ بزرگترین مقسوم‌علیه مشترک α و β است. اما در این صورت $\bar{\mu}|\bar{\delta}$، و بنابراین $\bar{\delta}$ یک بزرگترین مقسوم‌علیه مشترک $\bar{\alpha}$ و $\bar{\beta}$ است.

حل دیگر. بنابر برهان (۷.۱۱)، می‌دانیم که δ یک عنصر با کوچکترین نُرم است که می‌تواند به‌صورت ترکیب خطی α و β نوشته شود. با مزدوج‌گیری، معلوم می‌شود که $\bar{\delta}$ یک عنصر با نُرم مثبت کمین است که می‌تواند به‌صورت ترکیب خطی $\bar{\alpha}$ و $\bar{\beta}$ نمایش داده شود.

۲۲.۱۱ اگر اعداد صحیح گویای a و b به معنی معمول متباین باشند، نشان دهید که به‌صورت اعداد صحیح گاوسی نیز متباین‌اند.

حل. چون a و b نسبت به هم اول‌اند، اعداد صحیح (گویای) u و v وجود دارند به‌طوری‌که $au + bv = ۱$. بنابراین اگر عدد صحیح گاوسی λ اعداد a و b را بشمارد، آنگاه λ عدد ۱ را می‌شمارد، و لذا λ یک یکه است. بنابراین تنها مقسوم‌علیه‌های مشترکِ گاوسی a و b یکه‌ها هستند، و لذا a و b به‌عنوان اعداد صحیح گاوسی نسبت به هم اول‌اند.

۲۳.۱۱ اگر $n = ۲^۲ \times ۳^۳ \times ۵^۵$، تعیین کنید چه تعداد عدد صحیح گاوسی عدد n را می‌شمارند.

حل. یک تجزیه به اعداد اول از n به‌صورت $\epsilon\prod\pi_i^{a_i}$ را به‌دست می‌آوریم که در آن ϵ یک یکه است و اگر $i\neq j$ عدد π_i یک وابستهٔ π_j نیست (این مطلب برای یک شمارش درست مهم است). در این حالت داریم $n=-(1+i)^{4}3^{3}(1+2i)^{5}(1-2i)^{2}$. بنابر تجزیهٔ یکتا، هر مقسوم‌علیه n یک نمایش یکتا به‌صورت $\epsilon(1+i)^{a}3^{b}(1+2i)^{c}(1-2i)^{d}$ دارد، که در آن ϵ یک یکه است و a، b، c، و d اعداد صحیح نامنفی هستند به‌طوری که $a\leq 4$، $b\leq 3$، و $d\leq 5$. تعداد ۴ انتخاب برای ϵ، ۵ انتخاب برای a، و مانند آن وجود دارند. لذا تعداد کل مقسوم‌علیه‌ها عبارت است از $4\times 5\times 4\times 6^{2}=2880$.

اگر α، β، و μ اعداد صحیح گاوسی با $\mu\neq 0$ باشند، گوییم که $\alpha\equiv\beta(\mathrm{mod}\,\mu)$ اگر $\mu|\alpha-\beta$. یک دستگاه کامل مانده‌ها به پیمانهٔ μ مجموعه‌ای مانند S از اعداد صحیح گاوسی است که به پیمانهٔ μ با یکدیگر ناهمنهشت‌اند، به‌طوری‌که هر عدد صحیح گاوسی با یک عنصر S همنهشت به پیمانهٔ μ است. شش مسألهٔ بعد در مورد همنهشتیهای به پیمانهٔ یک عدد صحیح گاوسی هستند.

۲۴.۱۱ همنهشتیهای خطی زیر را حل کنید: (الف) $2x\equiv 1+3i(\mathrm{mod}\,11)$؛
(ب) $2x\equiv 1+3i(\mathrm{mod}\,3+8i)$.

حل. (الف) مطابق معمول طرفین همنهشتی را در یک وارون (معمولی) ۲ به پیمانهٔ ۱۱ ضرب می‌کنیم. مثلاً با ضرب در ۶ داریم $x\equiv 6+18i(\mathrm{mod}\,11)$، و لذا، مثلاً، $7i+6$ یک جواب است.

(ب) می‌خواهیم همنهشتی را در یک عدد صحیح گاوسی مانند α ضرب کنیم به‌طوری که $2\alpha\equiv 1(\mathrm{mod}\,3+8i)$. چون $(3+8i)(3-8i)=73$، کافی است که α در $2\alpha\equiv 1(\mathrm{mod}\,73)$ صدق کند، و آشکار است که $\alpha=37$ کارساز است. از این‌رو، $x\equiv 37+111i(\mathrm{mod}\,3+8i)$ را به‌دست می‌آوریم. اما $37+111i=14(3+8i)-(5+i)$، لذا یک پاسخ ساده‌تر $x\equiv -(5+i)(\mathrm{mod}\,3+8i)$ است.

۲۵.۱۱ فرض کنید α و $\mu\neq 0$ اعداد صحیح گاوسی متباین باشند. ثابت کنید عدد صحیح گاوسی ξ وجود دارد به‌طوری‌که $\alpha\xi\equiv 1(\mathrm{mod}\,\mu)$.

حل. چون ۱ بزرگترین مقسوم‌علیه مشترک α و μ است، (۷.۱۱) ایجاب می‌کند که اعداد صحیح گاوسی κ و λ وجود داشته باشند به‌طوری که $\kappa\alpha+\lambda\mu=1$. اگر قرار دهیم $\xi=\kappa$، آنگاه $\alpha\xi\equiv 1(\mathrm{mod}\,\mu)$.

۲۶.۱۱ فرض کنید اعداد صحیح گاوسی μ و ν نسبت به هم اول باشند. اگر α و β اعداد صحیح گاوسی باشند، ثابت کنید دستگاه همنهشتیهای

$$x \equiv \alpha (\mathrm{mod}\, \mu), \quad x \equiv \beta (\mathrm{mod}\, \nu)$$

حلپذیر است، و جواب آن به پیمانهٔ $\mu\nu$ یکتاست. (راهنمایی: مسألهٔ ۲۵.۱۱ و برهان قضیهٔ باقیماندهٔ چینی را ببینید.)

حل. بنابر مسألهٔ قبل، اعداد صحیح گاوسی γ و δ وجود دارند به‌طوری‌که $\gamma\nu \equiv ۱ (\mathrm{mod}\, \mu)$ و $\delta\mu \equiv ۱ (\mathrm{mod}\, \nu)$. به آسانی دیده می‌شود که $x = \gamma\nu\alpha + \delta\mu\beta$ در هر دو همنهشتی صدق می‌کند. اگر y نیز در هر دو همنهشتی صدق کند، آنگاه $x - y$ بر μ و ν و لذا بر $\mu\nu$ بخشپذیر است (تجزیه به اعداد اولِ $x - y$ را ملاحظه کنید). بنابراین دقیقاً یک جواب به پیمانهٔ $\mu\nu$ وجود دارد.

۲۷.۱۱ فرض می‌کنیم m یک عدد صحیح مثبت باشد. نشان دهید که هر دستگاه کامل ماندهها به پیمانهٔ m دارای $m^۲$ عنصر است.

حل. آشکار است که هر دو دستگاه کامل ماندهها به پیمانهٔ m دارای یک تعداد عنصر هستند. لذا کافی است که یک دستگاه کامل ماندهها با $m^۲$ عنصر به دست آوریم. فرض کنیم S مجموعهٔ تمام اعداد صحیح گاوسی به‌صورت $u + iv$ باشد که در آن $۰ \le u, v \le m - ۱$؛ روشن است که S دارای $m^۲$ عنصر است. اگر $\alpha = s + ti$ یک عدد صحیح گاوسی باشد، فرض می‌کنیم که $s_۰$، $t_۰$ به‌ترتیب، کوچکترین ماندههای نامنفی s و t به پیمانهٔ m باشند. در این صورت $s_۰ + t_۰ i$ متعلق به S است و با α به پیمانه m همنهشت است. اگر $\alpha = u + vi$ و $\alpha' = u' + v'i$ عناصری از S باشند و $m|\alpha - \alpha'$، آنگاه m هر یک از $u - u'$ و $v - v'$ را می‌شمارد. اما چون $۰ \le u, u' \le m - ۱$، نتیجه می‌شود که $u = u'$. با استدلالی مشابه $v = v'$، و لذا عناصر متمایز S به پیمانهٔ m ناهمنهشت‌اند.

◁ **۲۸.۱۱** فرض می‌کنیم π یک عدد اول گاوسی باشد به‌طوری که $\mathrm{N}(\pi)$ عدد اولی مانند p به‌صورت $۴k + ۱$ باشد. ثابت کنید هر دستگاه کامل ماندهها به پیمانهٔ π دارای p عنصر است (راهنمایی: مسألههای ۲۶.۱۱ و ۲۷.۱۱ را به‌کار برید.)

حل. به آسانی دیده می‌شود که π و $\bar{\pi}$ نسبت به هم اول‌اند، زیرا آنها وابسته نیستند و π هیچ مقسوم‌علیه سره ندارد. فرض می‌کنیم P، A، و B به‌ترتیب دستگاههای کامل ماندهها به پیمانهٔ p، π، و $\bar{\pi}$ باشند. اگر A دارای k عنصر باشد، آنگاه β نیز k عنصر دارد. بنابر مسألهٔ ۲۶.۱۱،

هر جفت α، β، که $\alpha \epsilon A$ و $\beta \epsilon B$، یک عنصر یکتا مانند γ از P را معین می‌کند به‌طوری‌که $\gamma \equiv \alpha (\mathrm{mod}\, \pi)$ و $\gamma \equiv \beta (\mathrm{mod}\, \bar{\pi})$. علاوه بر این، هر عنصر P به همین روش تولید می‌شود. لذا P دارای k^2 عنصر است. از طرف دیگر، بنابر مسألهٔ ۲۷.۱۱، P دارای p^2 عنصر است، و لذا $k = p$.

توضیح. اساساً به همین روش می‌توان نشان داد که هر دستگاه کامل مانده‌ها به پیمانهٔ π^n دارای p^n عنصر است. سپس با استفاده از قضیهٔ باقیماندهٔ چینی، ثابت کرد که اگر μ یک عدد صحیح گاوسی غیرصفر باشد، آنگاه هر دستگاه کامل مانده‌ها به پیمانهٔ μ دارای $\mathrm{N}(\mu)$ عنصر است.

۲۹.۱۱ (یک مشابه گاوسی قضیهٔ فرما.) فرض می‌کنیم π یک عدد اول گاوسی باشد، و فرض کنید α بر π بخشپذیر نباشد. نشان دهید $\alpha^{\mathrm{N}(\pi)-1} \equiv 1 (\mathrm{mod}\, \pi)$. (راهنمایی: مسأله‌های ۲۷.۱۱ و ۲۸.۱۱ را به‌کار برید، یا از قضیهٔ دوجمله‌یی استفاده کنید.)

حل. اگر π برابر با $i + 1$ یا یکی از وابسته‌هایش باشد، بررسی مسأله آسان است. بنابراین می‌توانیم فرض کنیم که یا π یک عدد اول گویا به‌صورت $4k + 3$ است یا یک عامل اول از یک عدد اول گویا به‌صورت $4k + 1$. فرض می‌کنیم β_0، β_1، ...، β_n یک دستگاه کامل مانده‌ها با $\beta_0 = 0$ باشد. بنابر مسأله‌های ۲۷.۱۱ و ۲۸.۱۱، $n = \mathrm{N}(\pi) - 1$. حال $\alpha\beta_1$، $\alpha\beta_2$، ...، $\alpha\beta_n$ را در نظر می‌گیریم. به آسانی دیده می‌شود که هیچ دو تا از اینها همنهشت به پیمانهٔ π نیستند. لذا، به‌ترتیبی، با β_1، β_2، ...، β_n به پیمانهٔ π همنهشت‌اند. از ضرب آنها در هم داریم

$$(\alpha\beta_1)(\alpha\beta_2)\cdots(\alpha\beta_n) \equiv \beta_1\beta_2\cdots\beta_n (\mathrm{mod}\, \pi).$$

اگر طرفین همنهشتی بالا را بر $\beta_1\beta_2\cdots\beta_n$ تقسیم کنیم، خواهیم داشت $\alpha^n \equiv 1 (\mathrm{mod}\, \pi)$، که همان قضیهٔ مورد نظر است.

برهان دیگر: حکم هم‌ارز آن را ثابت می‌کنیم که به‌ازای هر عدد صحیح گاوسی α $\alpha^{\mathrm{N}(\pi)} \equiv \alpha (\mathrm{mod}\, \pi)$. برای $\alpha = 0$ قضیه روشن است. سپس نشان می‌دهیم که اگر مسأله برای α برقرار باشد، آنگاه برای β، که $\beta = \alpha \pm 1$ یا $\beta = \alpha \pm i$ نیز برقرار است. استدلالها در هر چهار حالت خیلی شبیه یکدیگر هستند، لذا فرض می‌کنیم $\beta = \alpha + i$. با استفاده از قضیهٔ دوجمله‌یی و با توجه به اینکه اگر p اول باشد و $1 \leq k \leq p - 1$ آنگاه ضریب دوجمله‌یی $\binom{p}{k}$ مضرب p است، داریم $(\alpha + i)^{\mathrm{N}(\pi)} \equiv \alpha^{\mathrm{N}(\pi)} + i^{\mathrm{N}(\pi)} \equiv \alpha + i^{\mathrm{N}(\pi)} (\mathrm{mod}\, \pi)$. باقی می‌ماند نشان دهیم $i^{\mathrm{N}(\pi)} \equiv i (\mathrm{mod}\, \pi)$. اگر $\mathrm{N}(\pi) = 2$ لازم است تحقیق کنیم که $\pi | 1 + i$، که بدیهی است. در سایر حالتها، $\mathrm{N}(\pi)$ به‌صورت $4k + 1$ است، و $i^{4k+1} = i$.

توضیح. اثبات مشابه قضیهٔ ویلسن نیز دشوار نیست.

۳۰.۱۱ با استفاده از تجزیهٔ $x^۲+y^۲=(x+yi)(x-yi)$ ثابت کنید هر سه‌تایی اولیه فیثاغورسی $(x_۱,y_۱,z)$ با فرض زوج بودن y به‌صورت $x=a^۲-b^۲$، $y=۲ab$، $z=a^۲+b^۲$ است که اعداد صحیح a و b نسبت به هم اول‌اند.

حل. تجزیهٔ $z^۲=(x+yi)(x-yi)$ را در نظر می‌گیریم. نشان می‌دهیم که $x+yi$ و $x-yi$ نسبت به هم اول‌اند. هر عدد اول گاوسی π که این دو عدد را بشمارد مجموع و تفاضلشان و لذا $۲x$ و $۲y$ را می‌شمارد. چون هیچ عدد اول گویایی هم x و هم y را نمی‌شمارد، باید داشته باشیم $\pi|۲$، و لذا π یک وابستهٔ $i+۱$ است. از این‌رو $\pi|x^۲+y^۲$ و $\pi|(۱+i)^۲$، یعنی، $\pi|۲i$. این ممکن نیست، زیرا z فرد است. پس $x+yi$ و $x-yi$ نسبت به هم اول‌اند.

لذا بنابر (۱۴.۱۱)، $x+yi$ به‌صورت $\epsilon\delta^۲$ است، که ϵ یک یکه است. قرار می‌دهیم $\delta=a+bi$؛ پس $x+yi=\epsilon((a^۲-b^۲)+۲abi)$. چون x فرد و y زوج است، بایستی داشته باشیم $a^۲-b^۲=\pm x$ و $۲ab=\pm y$. توجه داریم که $(a,b)=۱$، زیرا اگر $d|a$ و $d|b$، آنگاه d اعداد $x+yi$ و $x-yi$ را می‌شمارد. اما $x+yi$ و $x-yi$ نسبت به هم اول‌اند، پس $d=۱$. اکنون با تعویض نقشهای a و b (در صورت لزوم) و انتخاب علامتهای مناسب برای a و b قضیه ثابت می‌شود.

۳۱.۱۱ برای تمام جوابهای معادلهٔ $x^۲+y^۲=z^۳$، که در آن $(x,y)=۱$ و یکی از x و y زوج و دیگری فرد است. یک «فرمول» به‌دست دهید.

حل. می‌خواهیم که $(x+yi)(x-yi)=z^۳$، مانند مسألهٔ قبل، می‌توانیم نشان دهیم که $x+yi$ و $x-yi$ نسبت به هم اول‌اند. لذا بنابر (۱۴.۱۱)، یک یکه ϵ و یک عدد صحیح گاوسی δ وجود دارند به‌طوری‌که $x+yi=\epsilon\delta^۳$. از آنجا که هر یکه یک مکعب کامل است، در واقع، می‌توانیم فرض کنیم که $x+yi=\delta^۳$. اگر $\delta=a+bi$، آنگاه داریم $x+yi=a^۳-۳ab^۲+(۳a^۲b-b^۳)i$، و لذا $x=a^۳-۳ab^۲$، $y=۳a^۲b-b^۳$. چون $z^۳=(a+bi)^۳(a-bi)^۳$، داریم $z=a^۲+b^۲$.

برای آنکه $(x,y)=۱$، اعداد a و b بایستی طوری انتخاب شوند که نسبت به هم اول باشند. همچنین، برای آنکه x و y زوجیت مخالف داشته باشند، بایستی a و b نیز از زوجیت مخالف انتخاب شوند. نشان می‌دهیم که با این انتخاب، x و y نسبت به هم اول‌اند. زیرا اگر عدد اول p اعداد x و y را بشمارد، آنگاه $p|ay-۳bx$، یعنی $p|۸ab^۳$؛ چون p فرد است، $p|a$ یا $p|b$. اما

اگر $p|a$، آنگاه چون $p|۳a^۲b - b^۳$، داریم $p|b$، و این با انتخاب a و b تناقض دارد. به همین طریق، $p|b$ نیز به یک تناقض منجر می‌شود. لذا همهٔ جوابهای معادلهٔ $x^۲ + y^۲ = z^۳$، که در آن $(x, y) = ۱$ و یکی‌از x و y زوج دیگری فرد است، با $x = a^۳ - ۳ab^۲$، $y = ۳a^۲b - b^۳$، و $z = a^۲ + b^۲$ داده می‌شوند، که در آنها a و b اعداد صحیح متباین و یکی زوج دیگری فرد است.

اعمال حسابی $Q(\sqrt{d})$

۳۲.۱۱ اگر $\alpha|\beta$ و $|\mathrm{N}(\alpha)| = |\mathrm{N}(\beta)|$، ثابت کنید که β یک وابستهٔ α است.

حل. اگر $\beta = ۰$ مسأله روشن است. اگر $\beta \neq ۰$، فرض می‌کنیم $\beta = \gamma\alpha$. چون $\mathrm{N}(\beta) = \mathrm{N}(\gamma)\mathrm{N}(\alpha)$ و $|\mathrm{N}(\alpha)| = |\mathrm{N}(\beta)|$، نتیجه می‌شود که $|\mathrm{N}(\gamma)| = ۱$، و لذا γ یک یکه است.

۳۳.۱۱ اگر β یک وابستهٔ α باشد، نشان دهید که α نیز یک وابستهٔ β است.

حل. بنابه تعریف، β یک وابستهٔ α است اگر و تنها اگر یک یکه ϵ یک یکه وجود داشته باشد به‌طوری که $\beta = \epsilon\alpha$. اما اگر ϵ یک یکه باشد و $\epsilon' = ۱/\epsilon$، آنگاه $\epsilon\epsilon' = ۱$ و لذا ϵ' یک یکه است. واضح است که، $\alpha = \epsilon'\beta$، و لذا α یک وابستهٔ β است.

۳۴.۱۱ گیریم m یک عدد صحیح گویای خالی از مربع باشد، و فرض می‌کنیم α و β اعداد صحیح در $Q(\sqrt{m})$ با نُرم برابر باشند. آیا همواره β یک وابستهٔ α یا یک وابستهٔ مزدوج α است؟

حل. نه، و می‌توانیم مثالهایی در اعداد صحیح گاوسی پیدا کنیم. چون $۴^۲ + ۳^۲ = ۵^۲ = ۲۵$، لذا ۲۵ مساوی نُرم ۵ و نیز نُرم $۴i + ۳$ است. روشن است که، $۴i + ۳$ نه یک وابستهٔ ۵ است و نه مزدوج یک وابستهٔ ۵.

۳۵.۱۱ تعیین کنید که کدام‌یک از اعداد زیر در $Q(\sqrt{-۵})$ اول هستند. (الف) $۴\sqrt{-۵} + ۳$؛ (ب) $\sqrt{-۵} - ۷$؛ (ج) ۱۹۹۷. (توجه کنید که ۱۹۹۷ یک عدد اول گویاست.)

حل. (الف) چون نُرم $۴\sqrt{-۵} + ۳$ برابر ۸۳ و ۸۳ یک عدد اول گویاست، پس $۴\sqrt{-۵} + ۳$ اول است.

(ب) نُرم $\sqrt{-۵} - ۷$ برابر ۵۴ است، و لذا تنها مقسوم‌علیه‌های غیرنمایان ممکن از $\sqrt{-۵} - ۷$ دارای نُرم ۲، ۳، ۶، ۹، ۱۸، یا ۲۷ هستند. اگر در جستجوی مقسوم‌علیه غیرنمایان با کوچکترین نُرم باشیم، لازم است که فقط ۲، ۳، و ۶ را به‌عنوان شِقهای ممکن برای نُرم بررسی کنیم. نُرم

$a+b\sqrt{-۵}$ برابر $a^۲+۵b^۲$ است، که به‌وضوح هرگز ۲ و ۳ نمی‌شود. اعداد صحیح با نُرم ۶ عبارت‌اند از $\sqrt{-۵}+۱$، $\sqrt{-۵}-۱$، و منفیهای آنها. اگر $\sqrt{-۵}-۷$ را بر $\sqrt{-۵}-۱$ تقسیم کنیم (با گویا کردن مخرج)، می‌بینیم که خارج‌قسمت یک عدد صحیح از $Q(\sqrt{-۵})$ است، و لذا $\sqrt{-۵}-۷$ اول نیست.

(ج) چون $N(۱۹۹۷)=۱۹۹۷^۲$، تنها مقسوم‌علیه‌های غیرنمایان ۱۹۹۷ اعداد با نُرم ۱۹۹۷ هستند. می‌توانیم با شمارش بررسی کنیم که هیچ عدد صحیح از $Q(\sqrt{-۵})$ دارای نُرم ۱۹۹۷ نیست، اما راه آسانتری وجود دارد. اگر $a^۲+۵b^۲=۱۹۹۷$، آنگاه ۱۹۹۷ یک ماندهٔ درجهٔ دوم از ۵ است. چون $(۱۹۹۷/۵)=(۲/۵)=-۱$، اعداد صحیح a و b وجود ندارند به‌طوری‌که $a^۲+۵b^۲=۱۹۹۷$، و لذا ۱۹۹۷ اول است.

۳۶.۱۱ آیا ۴۱ یک عدد اول در $Q(\sqrt{۱۳})$ است؟

حل. اگر $۴۱=\alpha\beta$، آنگاه $N(۴۱)=۴۱^۲=N(\alpha)|N(\beta)$. بنابراین بایستی هر مقسوم‌علیه غیرنمایان ۴۱ دارای نُرم ±۴۱ باشد، لذا یا جوابهای صحیح $x^۲-۱۳y^۲=\pm۴۱$ را جستجو می‌کنیم یا اعداد صحیح فرد x و y را به‌طوری‌که $(x/۲)^۲-۱۳(y/۲)^۲=\pm۴۱$. ابتدا معادلهٔ $x^۲-۱۳y^۲=\pm۴۱$ را در نظر می‌گیریم. اگر این معادله جواب داشته باشد، آنگاه ±۴۱ یک ماندهٔ درجهٔ دوم از ۱۳ است، زیرا $x^۲\equiv\pm۴۱ \pmod{۱۳}$. مطابق معمول نمادهای لژاندر را محاسبه می‌کنیم. در هر دو حالت -۱ به‌دست می‌آید، و لذا معادلهٔ $x^۲-۱۳y^۲=\pm۴۱$ جواب صحیح ندارد. همین استدلال اساساً برای معادلهٔ $(x/۲)^۲-۱۳(y/۲)^۲=\pm۴۱$ نیز کارساز است. لذا ۴۱ در $Q(\sqrt{۱۳})$ اول است.

۳۷.۱۱ $\sqrt{۱۴}$ را به‌صورت حاصلضرب دو عدد اول در $Q(\sqrt{۱۴})$ بنویسید.

حل. چون $\sqrt{۱۴}$ دارای نُرم -۱۴ است، لذا برای یافتن مقسوم‌علیه‌های سَره $\sqrt{۱۴}$ توجه خود را به اعداد با نُرم ±۲ یا ±۷ معطوف می‌کنیم. توجه می‌کنیم که نُرم $۴+\sqrt{۱۴}$ برابر ۲ است و اینکه $-۷+۲\sqrt{۱۴}=(۴+\sqrt{۱۴})/\sqrt{۱۴}$. لذا تجزیهٔ $\sqrt{۱۴}=(۴+\sqrt{۱۴})(-۷+۲\sqrt{۱۴})$ را داریم. چون قدرمطلق نُرم هر عامل اول است، لذا هر عامل اول است.

توضیح. تجزیه‌ای را که پیدا کرده‌ایم بی‌نهایت صورت غیراساسی تولید می‌کند، زیرا بی‌نهایت یکه وجود دارد، و با ضرب یک عامل در ϵ و تقسیم دیگری بر ϵ تجزیه‌ای که به نظر متفاوت است به‌دست می‌آوریم.

۳۸.۱۱ $۱۱\sqrt{-۷}+۳۳$ را به‌صورت حاصلضرب اعداد اول در $Q(\sqrt{-۷})$ بیان کنید. (توجه کنید که $-۷ \equiv (\bmod ۴)$).

حل. می‌نویسیم $۱۱\sqrt{-۷}+۳۳ = ۱۱(۳+\sqrt{-۷})$. چون $۱۱ = ۲^۲ + ۱^۲ \times ۷$، داریم $۱۱ = (۲+\sqrt{-۷})(۲-\sqrt{-۷})$. اعداد صحیح $۲ \pm \sqrt{-۷}$ اول‌اند، زیرا نُرم هر کدام اول است. اکنون $۳+\sqrt{-۷}$ را تجزیه می‌کنیم. چون $۲/(۳+\sqrt{-۷})$ عدد صحیحی در $Q(\sqrt{-۷})$ است، پس ۲ بر $۳+\sqrt{-۷}$ بخشپذیر است. همچنین، ۲ مساوی حاصلضرب $۲/(۱+\sqrt{-۷})$ و $۲/(۱-\sqrt{-۷})$ است، که هر دو اول‌اند، زیرا نُرم هرکدام اول است. باقی می‌ماند که $۲/(۳+\sqrt{-۷})$ را بررسی کنیم. چون $\mathrm{N}((۳+\sqrt{-۷})/۲) = ۴$، هر مقسوم‌علیه سره $۲/(۳+\sqrt{-۷})$ دارای نُرم ۲ است. از این‌رو، با جستجویی که محدود است، به آسانی دیده می‌شود که $۲/(۳+\sqrt{-۷})$ حاصلضرب $۲/(۱-\sqrt{-۷})$ و $۲/(۱+\sqrt{-۷})$ است.

۳۹.۱۱ اول بودن ۹۷ را در $Q\sqrt{۱۱۹}$ بررسی کنید.

حل. نُرم ۹۷ برابر $۹۷^۲$ است. لذا اگر $\alpha\beta = ۹۷$، آنگاه $\mathrm{N}(\alpha)\mathrm{N}(\beta) = ۹۷^۲$. با اثبات اینکه به‌ازای هر عدد صحیح γ از $Q(\sqrt{۱۱۹})$ تساوی $\mathrm{N}(\gamma) = \pm ۹۷$ برقرار نیست، نشان می‌دهیم که نُرم یکی از عاملها ± ۱ است (یعنی، یکی از عاملهای یک یکه است). فرض کنیم $\gamma = u + v\sqrt{۱۱۹}$، که در آن u و v اعداد صحیح گویا هستند. در این صورت $\mathrm{N}(\gamma) = \pm ۹۷$ اگر و تنها اگر $u^۲ - ۱۱۹v^۲ = \pm ۹۷$. با توجه به $۱۱۹ = ۷ \times ۱۷$ دو حالت پیش می‌آید که هر دو را رد می‌کنیم. اگر $u^۲ - ۱۱۹v^۲ = ۹۷$، آنگاه $u^۲ \equiv ۹۷ (\bmod ۷)$، یعنی، $u^۲ \equiv -۱ (\bmod ۷)$، که ممکن نیست، زیرا -۱ یک ماندهٔ درجهٔ دوم ۷ نیست. اگر $u^۲ - ۱۱۹v^۲ = -۹۷$، آنگاه $u^۲ \equiv -۹۷ (\bmod ۱۷)$، یعنی، $u^۲ \equiv ۵ (\bmod ۱۷)$. این نیز ممکن نیست، زیرا $(۲/۵) = (۵/۱۷)(۱۷/۵) = -۱$.

۴۰.۱۱ اگر $۵|d$، ثابت کنید ۲ در $Q(\sqrt{d})$ اول است.

حل. ابتدا حالت $d \not\equiv ۱ (\bmod ۴)$ را در نظر می‌گیریم. اعداد صحیح $Q(\sqrt{d})$ به‌صورت $a + b\sqrt{d}$ هستند که a و b اعداد صحیح‌اند. چون $\mathrm{N}(۲) = ۴$، هر مقسوم‌علیه سرهٔ ۲ دارای نُرم ± ۲ است. اگر $a^۲ - db^۲ = \pm ۲$ و $۵|d$، آنگاه $a^۲ \equiv \pm ۲ (\bmod ۵)$، که غیرممکن است.

اگر $d \equiv ۱ (\bmod ۴)$، اعداد صحیح به‌صورت $(a+b\sqrt{d})/۲$ با a و b فرد نیز وجود دارند. اگر یک چنین عدد صحیح دارای نُرم ± ۲ باشد، آنگاه $a^۲ - db^۲ = \pm ۸$. اگر $۵|d$، آنگاه داریم $a^۲ \equiv \pm ۳ (\bmod ۵)$، که ممکن نیست.

۴۱.۱۱ فرض می‌کنیم d، u، و v اعداد صحیح باشند. (الف) ثابت کنید $u+v\sqrt{d}$ یک ریشهٔ معادلهٔ $x^۲+bx+c=۰$ است، که در آن b و c اعداد صحیح‌اند. (ب) اگر $d\equiv ۱ \pmod ۴$ و u و v فرد باشند. نشان دهید که $(u+v\sqrt{d})/۲$ یک ریشهٔ معادله‌ای به‌صورت $x^۲+bx+c=۰$ است، که در آن b و c اعداد صحیح هستند.

حل. (الف) چندجمله‌یی

$$P(x)=(x-(u+v\sqrt{d}))(x-(u-v\sqrt{d}))=x^۲-۲ux+u^۲-dv^۲$$

به‌صورت مورد نظر است، و روشن است که، $P(u+v\sqrt{d})=۰$. (ب) فرض می‌کنیم

$$P(x)=(x-(u+v\sqrt{d})/۲)(x-(u-\sqrt{d})/۲)=x^۲-ux+(u^۲-dv^۲)/۴$$

چون u و v فرد هستند و $d\equiv ۱ \pmod ۴$، $u^۲-dv^۲$ مضربی است از ۴، و لذا $P(x)$ دارای ضرایب صحیح است.

۴۲.۱۱ گیریم $d\neq ۱$ یک عدد صحیح خالی از مربع باشد، و فرض می‌کنیم r و $s\neq ۰$ اعداد گویا باشند. اگر $\alpha=r+s\sqrt{d}$ یک ریشهٔ معادلهٔ چندجمله‌یی $x^۲+bx+c=۰$ باشد، که b و c اعداد صحیح هستند، نشان دهید که اگر $d\equiv ۲ \pmod ۴$ یا $d\equiv ۳ \pmod ۴$، آنگاه r و s اعداد صحیح هستند. اگر $d\equiv ۱ \pmod ۴$، ثابت کنید که یا r و s هر دو صحیح‌اند، یا $۲r$ و $۲s$ هر دو عدد صحیح فردند.

حل. اگر $r+s\sqrt{d}$ یک ریشهٔ معادلهٔ $x^۲+bx+c=۰$ باشد، آنگاه $r-s\sqrt{d}$ نیز یک ریشهٔ این معادله است، و چون $s\neq ۰$، این دو ریشه متمایزند. مجموع دو ریشه یعنی $۲r$ برابر $-b$ و حاصلضربشان $r^۲-ds^۲$ مساوی c است. با جایگزینی، داریم $۴ds^۲=b^۲-۴c$. فرض کنیم $۲s=m/n$، که در آن m و n دو عدد صحیح متباین‌اند؛ لذا $dm^۲=n^۲(b^۲-۴c)$. چون m و n نسبت به هم اول‌اند، در نتیجه $n^۲|d$. چون d خالی از مربع است، داریم $n^۲=۱$، و لذا $۲s$ یک عدد صحیح است.

اگر $۲s=v$، آنگاه $b^۲-dv^۲=۴c$، و لذا $b^۲-dv^۲\equiv ۰ \pmod ۴$. اگر $d\equiv ۳ \pmod ۴$ یا $d\equiv ۲ \pmod ۴$، به آسانی دیده می‌شود که b و v زوج‌اند، و لذا r و s اعداد صحیح‌اند. اگر $d\equiv ۱ \pmod ۴$ و b و v هر دو زوج نباشند، هر دو بایستی فرد باشند، لذا $۲r$ و $۲s$ هر دو فردند.

۴۳.۱۱ اگر d منفی باشد، نشان دهید که همهٔ یکه‌های $Q(\sqrt{d})$ توانهایی از یکی از یکه‌ها هستند.

حل. یکه‌ها در (۲۳.۱۱) تشریح شده‌اند. توجه کنید که آنها توانهایی از -1 هستند، مگر آنکه $d=-1$ یا $d=-3$. اگر $d=-1$، یکه‌ها توانهایی از i (همچنین از $-i$) هستند. اگر $d=-3$، به آسانی دیده می‌شود که یکه‌ها توانهایی از $(1+\sqrt{-3})/2$ (همچنین از $(1-\sqrt{-3})/2$) هستند.

۴۴.۱۱ آیا در $Q(\sqrt{2})$ یکه‌ای بین ۱ و ۱۰ وجود دارد؟ اگر چنین است، آنها را بیابید. اگر چنین نیست، توضیح دهید که چرا هیچ عددی وجود ندارد.

حل. به آسانی می‌توان تحقیق کرد که $1+\sqrt{2}$ یک یکه است. $1+\sqrt{2}$ یکهٔ اصلی، زیرا بنابر برهان (۲۴.۱۱)، هر یکهٔ بزرگتر از ۱ به‌صورت $a+b\sqrt{2}$ است، که a و b مثبت‌اند. اما اگر δ یا $1+\sqrt{2}<\delta<1$ به آن صورت باشد، آنگاه $\delta=2$، لذا δ یک یکه نیست. رابطهٔ $1<(1+\sqrt{2})^n<10$ تنها به‌ازای $n=1$ و $n=2$ برقرار است. لذا یکه‌های بین ۱ و ۱۰ عبارت‌اند از $1+\sqrt{2}$ و $3+2\sqrt{2}$.

۴۵.۱۱ اگر π_1 و π_2 اعداد اول در $Q(\sqrt{d})$ باشند و $\pi_1|\pi_2$، ثابت کنید که π_1 و π_2 وابسته‌اند.

حل. فرض کنیم $\pi_2=\alpha\pi_1$. چون π_1 اول است، یکی از α و π_1 یک یکه است. چون π_1 اول است، نمی‌تواند یکه باشد. لذا α یک یکه است، و بنابراین π_1 و π_2 وابسته‌اند.

۴۶.۱۱ اگر m و n اعداد صحیح گویای متمایز خالی از مربع باشند، نشان دهید که $Q(\sqrt{m})\neq Q(\sqrt{n})$.

حل. بدون آنکه به کلیت استدلال خللی وارد آید، می‌توانیم فرض کنیم که $n\neq 1$. با نشان دادن اینکه $\sqrt{n}$ عنصری از $Q(\sqrt{m})$ نیست ثابت می‌کنیم که دو هیئت متمایزند. بعکس، فرض کنیم $\sqrt{n}$ عنصری از $(\sqrt{m})$ باشد، لذا اعداد گویای s و t وجود دارند به‌طوری که $\sqrt{n}=s+t\sqrt{m}$، و چون $\sqrt{n}$ گویا نیست، $t\neq 0$.

اگر $\sqrt{n}=s+t\sqrt{m}$، آنگاه $\sqrt{n}-t\sqrt{m}=s$. پس از مربع کردن و ساده کردن، داریم $\sqrt{mn}=(n+t^2m-s^2)/2t$؛ لذا $\sqrt{mn}$ یک عدد گویاست. با نشان دادن اینکه mn یک مربع کامل نیست. ثابت می‌شود که mn عدد گویا نیست. اگر عدد اولی مانند p وجود داشته باشد که یکی از m یا n را بشمارد و دیگری را نشمارد، آنگاه چون m و n خالی از مربع هستند، mn یکی مربع کامل نیست. اگر تمام اعداد اولی که یا m یا n را می‌شمارند دیگری را نیز بشمارند، آنگاه $m=-n$، زیرا m و n متمایزند، و مجدداً mn یک مربع کامل نیست.

۴۷.۱۱ (الف) فرض می‌کنیم $\alpha = (۷ + \sqrt{۳})/۲$ و $\beta = ۱ + ۲\sqrt{-۳}$. تحقیق کنید که $\alpha\bar{\alpha} = \beta\bar{\beta} = ۱۳$. چرا این مطلب ویژگی تجزیهٔ یکتا در $Q(\sqrt{-۳})$ را نقض نمی‌کند؟

(ب) فرض می‌کنیم W مجموعهٔ اعدادی به‌صورت $x + y\sqrt{-۳}$ باشد، که در آن x و y اعداد صحیح‌اند. نشان دهید که تجزیهٔ یکتا در W برقرار نیست. (ولی، تجزیهٔ یکتا در $Q(\sqrt{-۳})$ برقرار است. (۲۰.۱۱) و مسألهٔ ۵۶.۱۱ را ببینید.)

حل. (الف) چون نُرمهای عاملهای مفروض اول‌اند، پس عاملها اول‌اند. اما یک محاسبهٔ کوتاه نشان می‌دهد که $\alpha/\beta = (۱ - \sqrt{-۳})/۲$. چون $(۱ - \sqrt{-۳})/۲$ یک یکه است، این بدان معنی است که α و β وابسته‌اند. با مزدوج‌گیری می‌بینیم که $\bar{\alpha}$ و $\bar{\beta}$ نیز وابسته‌اند. لذا دو تجزیهٔ مفروض اساساً یکی هستند.

(ب) داریم $(۱ - \sqrt{-۳})(۱ + \sqrt{-۳}) = ۲ \times ۲$. چون ۲ و $۱ \pm \sqrt{-۳}$ دارای نُرم ۴ هستند، بایستی هر مقسوم‌علیه غیرنمایان آنها دارای نُرم ۲ باشد. اما معادلهٔ $x^۲ + ۳y^۲ = ۲$ جواب صحیح ندارد، و لذا W هیچ عنصری با نُرم ۲ ندارد. در نتیجه ۲ و $۱ \pm \sqrt{-۳}$ در W اول‌اند. اما $۱ + \sqrt{-۳}$ یک وابستهٔ ۲ در W نیست زیرا $(۱ + \sqrt{-۳})/۲$ عنصری از W نیست، و لذا تجزیهٔ یکتا در W برقرار نیست.

۴۸.۱۱ نشان دهید که $Q(\sqrt{-۵})$ ویژگی تجزیهٔ یکتا را ندارد.

حل. داریم $(۱ - \sqrt{-۵})(۱ + \sqrt{-۵}) = ۲ \times ۳ = ۶$. نشان می‌دهیم که ۲، ۳ و $۱ \pm \sqrt{-۵}$ اول‌اند، و چون به‌وضوح هیچ دو تا از اینها وابسته نیستند، ثابت می‌شود که تجزیهٔ یکتا را نداریم. چون ۲، ۳، و $۱ \pm \sqrt{-۵}$ به‌ترتیب، دارای نُرم ۴، ۹، و ۶ هستند، لذا برای اینکه نشان دهیم مقسوم‌علیه غیرنمایان ندارند، کافی است نشان دهیم که اعداد صحیح با نُرم ۲ یا ۳ وجود ندارند. این بدیهی است.

۴۹.۱۱ آیا اعداد صحیح $Q(\sqrt{-۱۴})$ به‌طور یکتا به‌صورت حاصلضرب اعداد اول تجزیه می‌شوند؟ اگر چنین است، ثابت کنید؛ اگر نیست، توضیح دهید که چرا نیست.

حل. داریم $(۱ - \sqrt{-۱۴})(۱ + \sqrt{-۱۴}) = ۳ \times ۵ = ۱۵$. نشان می‌دهیم که تمام این عاملها اول‌اند. چون به‌وضوح $۱ + \sqrt{-۱۴}$ وابستهٔ ۳ یا ۵ نیست، این نشان می‌دهد که اعداد صحیح $Q(\sqrt{-۱۴})$ ویژگی تجزیهٔ یکتا را ندارند.

چون $N(۳) = ۹$، لذا برای نشان دادن اینکه ۳ اول است، کافی است نشان دهیم که هیچ عدد صحیح با نُرم ۳ در $Q(\sqrt{-۱۴})$ وجود ندارد. این بدیهی است، زیرا نُرم $a + b\sqrt{-۱۴}$

برابر $a^۲ + ۱۴b^۲$ است، و $a^۲ + ۱۴b^۲ = ۳$ جواب صحیح ندارد. استدلال تقریباً یکسان نشان می‌دهد که ۵ اول است. به تشابه، اگر $\alpha\beta = ۱ \pm \sqrt{-۱۴}$، که α و β هیچ‌کدام یکه نیستند، آنگاه نُرمهای α و β عبارت‌اند از ۳ یا ۵، که ممکن نیست.

۵۰.۱۱ نشان دهید که $Q(\sqrt{۱۵})$ ویژگی تجزیهٔ یکتا را دارا نیست.

حل. ملاحظه می‌کنید که ۲ عدد $(۱ - \sqrt{۱۵})(۱ + \sqrt{۱۵})$ را می‌شمارد ولی ۲ نه $۱ + \sqrt{۱۵}$ را می‌شمارد و نه $۱ - \sqrt{۱۵}$ را. این با تجزیهٔ یکتا ناسازگار است هرگاه نشان دهیم که ۲ در $Q(\sqrt{۱۵})$ اول است.

هر مقسوم‌علیه غیرنمایان ۲ بایستی دارای نُرم ± ۲ باشد. اما $u^۲ - ۱۵v^۲ = \pm ۲$ برقرار نیست، زیرا از آنجا $u^۲ \equiv \pm ۲ \pmod ۵$ به دست می‌آید، که ممکن نیست. لذا ۲ اول است، و مسأله ثابت می‌شود.

۵۱.۱۱ $۴۱ \times ۳۱ \times ۳$ را به‌صورت حاصلضرب اعداد اولِ $Q(\sqrt{-۲})$ بیان کنید. نشان دهید که عاملها به‌طور مسلم اول هستند.

حل. می‌توانیم نظریهٔ (۲۲.۱۱) را به‌کار بریم، اما به‌جای آن، مستقیماً عمل می‌کنیم. ملاحظه می‌کنید که نُرمهای ۳، ۳۱، و ۴۱ عبارت‌اند از $۳^۲$، $۳۱^۲$، و $۴۱^۲$، و لذا هر مقسوم‌علیه سره دارای نُرمهای ۳، ۳۱، و ۴۱ است. به‌آسانی دیده می‌شود که $(\sqrt{-۲} - ۱)(\sqrt{-۲} + ۱) = ۳$، هیچ عددی دارای نُرم ۳۱ نیست، و اینکه $(۳ - ۴\sqrt{-۲})(۳ + ۴\sqrt{-۲}) = ۴۱$. چون عددی با نُرم ۳۱ وجود ندارد، پس ۳۱ اول است، و چون $۱ + \sqrt{-۲}$ و $۳ \pm \sqrt{-۲}$ همگی نُرمِ اول دارند، پس اول‌اند. لذا تجزیهٔ اعداد اول زیر را داریم

$$۳ \times ۳۱ \times ۴۱ = ۳۱(۱ + \sqrt{-۲})(۱ - \sqrt{-۲})(۳ + ۴\sqrt{-۲})(۳ - ۴\sqrt{-۲})$$

۵۲.۱۱ تمام نمایشهای $n = ۲ \times ۱۱ \times ۱۷ \times ۲۵$ به‌صورت $x^۲ + ۲y^۲$ را به‌دست آورید.

حل. چون ۱۱ و ۱۷ اعداد اول به‌صورت $۸k + ۱$ یا $۸k + ۳$ هستند، و ۵ به‌صورت $۸k + ۵$ و با توان زوج است، از (۲۲.۱۱) نتیجه می‌شود که n دارای نمایشهایی به‌صورت $x^۲ + ۲y^۲$ است. در واقع، n دارای $۸ = (۱ + ۱)(۱ + ۱)۲$ چنین نمایشی است. در هر نمایش، بایستی ۵ اعداد x و y را بشمارد، زیرا ۵ در $Q(\sqrt{-۲})$ اول است، و لذا اگر $۵|x^۴ + ۲y^۲$، آنگاه ۵ عدد $x + y\sqrt{-۲}$ یا $x - y\sqrt{-۲}$ و لذا هر دو را می‌شمارد. بنابراین کافی است که $۲ \times ۱۱ \times ۱۷$

را نمایش دهیم. اگر $۲ \times ۱۱ \times ۱۷$ را به‌صورت حاصلضرب اعداد اولِ $Q(\sqrt{-۲})$ تجزیه کنیم داریم

$$۲ \times ۱۱ \times ۱۷ = -(\sqrt{-۲})^۲(۳+\sqrt{-۲})(۳-\sqrt{-۲})(۳+۲\sqrt{-۲})(۳-۲\sqrt{-۲})$$

می‌خواهیم که این عبارت را به‌صورت $\alpha\bar{\alpha}$ بیان کنیم. برای انجام این کار اساساً دو روش وجود دارد: α را به یکی از دو صورت زیر حساب می‌کنیم $\alpha = \sqrt{-۲}(۳+\sqrt{-۲})(۳+۲\sqrt{-۲})$ یا $\alpha = \sqrt{-۲}(۳+\sqrt{-۲})(۳-۲\sqrt{-۲})$. اولی نمایش $۲ \times ۱۱ \times ۱۷ = ۱۸^۲ + ۲ \times ۵^۲$ را ارائه می‌دهد، و دومی نمایش $۲ \times ۱۳^۲ + ۶^۲$ را. اگر در ۵ ضرب کنیم نمایشهای $n = ۹۰^۲ + ۲ \times ۲۵^۲$ و $n = ۳۰^۲ + ۲ \times ۶۵^۲$ را به‌دست می‌آوریم. با تغییر علامت هرکدام دارای چهار صورت نمایان است.

۵۳.۱۱ فرض می‌کنیم d خالی از مربع است و $Q(\sqrt{d})$ ویژگی تجزیهٔ یکتا را داراست. گیریم p یک عدد اول (گویای) فرد باشد به‌طوری‌که d یک ماندهٔ درجهٔ دوم p است. ثابت کنید p در $Q(\sqrt{d})$ اول نیست. (راهنمایی: به بحث پیش از (۲۱.۱۱) مراجعه کنید.)

حل. چون d یک ماندهٔ درجهٔ دوم p است، یک عدد صحیح x وجود دارد به‌طوری‌که $x^۲ \equiv d \pmod{p}$؛ لذا $p|(x+\sqrt{d})(x-\sqrt{d})$. اگر p در $Q(\sqrt{d})$ اول باشد، آنگاه نتیجه خواهد شد که $p|x+\sqrt{d}$ یا $p|x-\sqrt{d}$، زیرا فرض کرده‌ایم که اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا دارند. اما بدیهی است که p اعداد $x \pm \sqrt{d}$ را نمی‌شمارد.

۵۴.۱۱ ثابت کنید که اعداد صحیح x و y وجود دارند به‌طوری‌که $x^۲ - ۳y^۲ = ۹۷$. (راهنمایی: از مسألهٔ ۵۳.۱۱ استفاده و توجه کنید که $Q(\sqrt{۳})$ ویژگی تجزیهٔ یکتا را داراست.)

حل. با یک محاسبهٔ سادهٔ نماد لژاندر، داریم $(۳/۹۷) = ۱$، و لذا ۳ یک ماندهٔ درجهٔ دوم ۹۷ است. از این‌رو، بنابر مسألهٔ قبل، ۹۷ یک عدد اول در $Q(\sqrt{۳})$ نیست؛ فرض کنیم $۹۷ = \alpha\beta$، که α و β هیچ‌کدام یکه نیستند. سپس، چون $\mathrm{N}(۹۷) = ۹۷^۲$، بایستی $\mathrm{N}(\alpha) = \pm ۹۷$. اگر $\alpha = x + y\sqrt{۳}$، آنگاه $x^۲ - ۳y^۲ = \pm ۹۷$. اما با یک محاسبهٔ ساده به پیمانهٔ ۳ معلوم می‌شود که $x^۲ - ۳y^۲ = -۹۷$ ممکن نیست. در نتیجه $x^۲ - ۳y^۲ = ۹۷$.

۵۵.۱۱ فرض می‌کنیم p عدد اول فردی است که عدد خالی از مربع d را نمی‌شمارد. اگر α یک عدد صحیح در $Q(\sqrt{d})$ باشد، نشان دهید که $\alpha^p \equiv \alpha \pmod{p}$ هر گاه d یک ماندهٔ درجهٔ دوم p باشد، و $\alpha^p \equiv \bar{\alpha} \pmod{p}$ اگر d یک نامانده‌ٔ p باشد. (راهنمایی: $(x+y\sqrt{d})^p$ را بسط دهید. در اینجا $\alpha \equiv \beta \pmod{p}$ به این معنی است که $p|\alpha - \beta$.)

حل. فرض می‌کنیم $\alpha = x + y\sqrt{d}$. حالتی را که x و y اعداد صحیح هستند بررسی می‌کنیم؛ در حالتی که x و y هرکدام نصف یک عدد صحیح فرد هستند استدلال مشابه، همین است. بنابر قضیهٔ دوجمله‌یی داریم

$$(x+y\sqrt{d})^p = x^p + \binom{p}{1} x^{p-1} y\sqrt{d} + \cdots + \binom{p}{p-1} xy^{p-1}(\sqrt{d})^{p-1} + y^p(\sqrt{d})^p$$

با کاربرد قضیهٔ فرما و اینکه به‌ازای هر k جز ۰ و p، $\binom{p}{k} \equiv 0 \pmod p$، پیدا می‌کنیم $(x+y\sqrt{d})^p \equiv x + yd^{(p-1)/2}\sqrt{d} \pmod p$. اکنون مسأله یک نتیجهٔ مستقیم ملاک اویلر است.

◁ **۵۶.۱۱** فرض می‌کنیم d مساوی ± 2 یا ± 3 باشد. اگر α و β اعداد صحیحی در $Q(\sqrt{d})$ باشند که $\alpha \neq 0$، ثابت کنید که اعداد صحیح γ و ρ در $Q(\sqrt{d})$ وجود دارند به‌طوری‌که $\beta = \gamma\alpha + \rho$ و $|\mathrm{N}(\rho)| < |\mathrm{N}(\alpha)|$. (راهنمایی: ۵.۱۱ را ببینید.)

حل. این راه‌حل استدلال به‌کاررفته در (۵.۱۱) را به‌دقت نشان می‌دهد. β را بر α تقسیم می‌کنیم تا $\beta/\alpha = x + y\sqrt{d}$ را که در آن x و y اعداد گویا هستند به‌دست آوریم. فرض می‌کنیم u و v، به‌ترتیب، نزدیکترین اعداد صحیح به x و y باشند، قرار می‌دهیم $\gamma = u + vi$، و $\rho = \beta - \gamma\alpha$. باقی می‌ماند ثابت کنیم $\mathrm{N}(\gamma) < \mathrm{N}(\alpha)$.

چون $\beta = (x+y\sqrt{d})\alpha$، داریم $\rho = ((x-u)+(y-v)\sqrt{d})\alpha$. اما $|x-v| \leq 1/2$ و $|y-v| \leq 1/2$. لذا $|\mathrm{N}((x-u)+(y-v)\sqrt{d}| \leq 1/4 + |d|/4$. بنابراین، اگر $d = \pm 2$، داریم $|\mathrm{N}(\rho)| \leq \frac{3}{4}|\mathrm{N}(\alpha)|$، و برهان کامل می‌شود. برای $d = 3$، با توجه به شرایط $|x-u| \leq 1/2$ و $|y-v| \leq 1/2$، سعی می‌کنیم که قدرمطلق $(x-u)^2 - 3(y-v)^2$ را ماکسیمم سازیم. آشکار است که اگر $|y-v| = 1/2$ و $x-u = 0$ به این ماکسیمم می‌رسیم. از این‌رو، $|\mathrm{N}(\rho)| \leq \frac{3}{4}|\mathrm{N}(\alpha)|$، و مجدداً برهان کامل می‌شود.

حالت $d = -3$ به استدلال بیشتری نیاز دارد، زیرا $\mathrm{N}((1+\sqrt{-3})/2) = 1$. اگر $|x-u| < 1/2$ یا $|y-v| < 1/2$، آنگاه $\mathrm{N}((x-u)+(y-v)\sqrt{-3}) < 1$، و لذا $|\mathrm{N}(\rho)| < |\mathrm{N}(\alpha)|$. اگر اختلاف هر یک از x و y با یک عدد صحیح $1/2$ باشد، آنگاه $(x+y\sqrt{-3})/2$ یک عدد صحیح در $Q(\sqrt{-3})$ است، لذا قرار می‌دهیم $\gamma = (x+y\sqrt{-3})/2$ و $\rho = 0$.

◁ **۵۷.۱۱** تمام جوابهای صحیح معادلهٔ دیوفانتی $x^2 + 2 = y^3$ را بیابید. (راهنمایی: مثال بعد از (۱۴.۱۱) را ببینید. می‌توانید فرض کنید که $Q(\sqrt{-2})$ تجزیهٔ یکتا دارد.)

حل. فرض می‌کنیم $x^۲+۲=y^۳$، و $x^۲+۲$ را به‌صورت $(x+\sqrt{-۲})(x-\sqrt{-۲})$ تجزیه می‌کنیم. هر مقسوم‌علیه مشترک غیرنمایان $x+\sqrt{-۲}$ و $x-\sqrt{-۲}$ عدد $۲\sqrt{-۲}$ را می‌شمارد. اما x فرد است، زیرا اگر زوج باشد، آنگاه $x^۲+۲\equiv ۲ \pmod ۴$، و لذا $x^۲+۴$ نمی‌تواند یک مکعب کامل باشد. بنابراین نُرم هر یک از $x\pm\sqrt{-۲}$ فرد است. چون نُرم هر مقسوم‌علیه غیرنمایان $۲\sqrt{-۲}$ زوج است، در نتیجه $x+\sqrt{-۲}$ و $x-\sqrt{-۲}$ نسبت به هم اول‌اند.

چون $Q(\sqrt{-۲})$ تجزیهٔ یکتا دارد، یک برهان شبیه به برهان (۴.۱۱) نشان می‌دهد که می‌توان $x+\sqrt{-۲}$ را به‌صورت $\epsilon\gamma^۳$ بیان کرد، که ϵ یک یکه است. اما تنها یکه‌ها عبارت‌اند از ± ۱، که هر دو مکعب کامل‌اند، و لذا می‌توانیم $x+\sqrt{-۲}=\gamma^۳$ را اختیار کنیم. اگر $\gamma=a+b\sqrt{-۲}$، آنگاه با مکعب کردن $a+b\sqrt{-۲}$ و برابر قرار دادن آن با $x+\sqrt{-۲}$، داریم $x=a^۳-۶ab^۲$ و $۱=۳a^۲b-۲b^۳$. چون b عدد $۳a^۲b-۲b^۳$ را می‌شمارد، پس $b=\pm ۱$. اگر $b=۱$، آنگاه $a=\pm ۱$، و اگر $b=-۱$، آنگاه معادلهٔ $۳a^۲b-۲b^۳=۱$ جواب ندارد. از این‌رو به‌ازای $b=۱$ و $a=\pm ۱$ داریم $x=a^۳-۶ab^۲=\pm ۵$. بنابراین، تنها جوابهای صحیح $x^۲+۲=y^۳$ عبارت‌اند از $x=\pm ۵$، $y=۳$.

◁ **۵۸.۱۱** جوابهای صحیح معادلهٔ $x^۲+۱۱=y^۳$ را به‌دست آورید. بدون اثبات، فرض کنید که $Q(\sqrt{-۱۱})$ دارای تجزیهٔ یکتاست.

حل. ابتدا توجه می‌کنیم که اگر $x^۲+۱۱=y^۳$، آنگاه x زوج است. زیرا اگر x فرد باشد، آنگاه $x^۲+۱۱\equiv ۴ \pmod ۸$، و لذا $x^۲+۱۱$ نمی‌تواند یک مکعب کامل باشد. همچنین، x بر ۱۱ بخشپذیر نیست، زیرا اگر $۱۱|x$، آنگاه $۱۱|y$ و لذا $y^۳-x^۲$ بر (۲) بخشپذیر است، و این با $y^۳-x^۲=۱۱$ تناقض دارد.

اگر معادله را در $Q(\sqrt{-۱۱})$ تجزیه کنیم داریم $(x+\sqrt{-۱۱})(x-\sqrt{-۱۱})=y^۳$. اگر α یک عامل اول مشترک $x+\sqrt{-۱۱}$ و $x-\sqrt{-۱۱}$ باشد، آنگاه $\alpha|۲\sqrt{-۱۱}$، و چون روشن است که ۲ و $\sqrt{-۱۱}$ اول‌اند، α مساوی ± ۲ یا $\pm\sqrt{-۱۱}$ است. اما $\alpha=\pm ۲$ برقرار نیست، زیرا x زوج است و ۲ عدد $\sqrt{-۱۱}$ را نمی‌شمارد. اگر $\alpha=\pm\sqrt{-۱۱}$، آنگاه $\alpha|x$ و لذا $۱۱|x$، که ممکن نیست. بنابراین $x+\sqrt{-۱۱}$ و $x-\sqrt{-۱۱}$ نسبت به هم اول‌اند. در نتیجه $x+\sqrt{-۱۱}$ و $x-\sqrt{-۱۱}$ هر دو مکعب کامل‌اند. قرار می‌دهیم $x+\sqrt{-۱۱}=\lambda^۳$. چون $-۱۱\equiv ۱ \pmod ۴$، یا (i) $\lambda=a+b\sqrt{-۱۱}$، که a و b اعداد صحیح‌اند، یا (ii) $\lambda=(c+d\sqrt{-۱۱})/۲$، که c و d اعداد صحیح فرد هستند.

در حالت (i)، $x=a^۳-۳۳ab^۲$ و $۳a^۲b-۱۱b^۳=۱$ را به‌دست می‌آوریم. اگر

$۳a^۲b - ۱۱b^۳ = ۱$، آنگاه $b = ۱$ یا $b = -۱$. برای $b = ۱$ داریم $a = \pm ۲$؛ و $b = -۱$ مقدار صحیحی برای a ارائه نمی‌دهد. با جایگزینی در $x = a^۳ - ۳۳ab^۲$، جواب $x = \pm ۵۸$ را به‌دست می‌آوریم؛ لذا $y = ۱۵$.

در حالت (ii)، داریم $x = (c^۳ - ۳۳cd^۲)/۸$ و $(۳a^۲b - ۱۱b^۳)/۸ = ۱$. معادلهٔ $۳c^۲d - ۱۱d^۳ = ۸$ را در نظر می‌گیریم. آشکار است که $d|۸$، و چون d فرد است، پس $d = \pm ۱$. $d = ۱$ جوابی به دست نمی‌دهد، و اگر $d = -۱$، آنگاه $c = \pm ۱$. بنابراین جواب $x = \pm ۴$، $y = ۳$ را به‌دست می‌آوریم.

تمرینهایی برای فصل ۱۱

۱. فرض کنید $\mathrm{N}(\gamma) = ۷۲۹ = ۲۷^۲$. آیا γ یک عدد اول گاوسی است؟

۲. اثبات یا رد کنید: اگر a و b غیر صفر و $a + bi$ یک عدد اول گاوسی باشد، آنگاه $\mathrm{N}(a + bi)$ یک عدد اول گویاست.

۳. ۳۹۰ را به‌صورت حاصلضرب اعداد اول گاوسی بیان کنید.

۴. $۱۸۰i + ۶۰$ را به‌صورت حاصلضرب اعداد اول گاوسی بنویسید.

۵. $۱۷i + ۱۹$ را به حاصلضرب اعداد اول تجزیه کنید.

۶. $۲۴i + ۷$ را به‌صورت حاصلضرب یک یکه و اعداد اول گاوسی $a + bi$ با $a > ۰$ و $b \geq ۰$ بیان کنید.

۷. بزرگترین مقسوم‌علیه مشترک $i + ۱۸$ و $۱۷i - ۶$ را به‌دست آورید.

۸. ملاحظه می‌کنید که ۴۱ نُرم یک عدد اول گاوسی است. عدد صحیح بعدی که نُرم یک عدد اول گاوسی باشد کدام است؟

۹. چه تعداد اعداد صحیح گاوسی دارای نُرم ۱۳۰۰ هستند؟ چندتای اینها مضرب ۵ هستند؟

۱۰. تعداد اعداد صحیح کوچکتر از ۲۰۰ مانند n را بیابید به‌طوری که n نُرم حداقل ۱۲ عدد صحیح گاوسی باشد.

۱۱. فرض می‌کنیم α، β، و γ اعداد اول گاوسی با نُرم فرد باشند. آیا اصلاً رابطهٔ $\alpha + \beta = \gamma$ برقرار است؟ توضیح دهید.

۱۲. چه تعداد عدد گاوسی متفاوت عدد $۱۰^۶$ را می‌شمارند؟

۱۳. همهٔ اعداد صحیح گاوسی با نُرم ۵۷۸ را پیدا کنید.

۱۴. اگر α و β اعداد صحیح گاوسی باشند، ثابت کنید که δ یک بزرگترین مقسوم‌علیه مشترک α و β است اگر و تنها اگر δ بزرگترین مقسوم‌علیه مشترک α و $\beta - \alpha$ باشد.

۱۵. فرض می‌کنیم α، β، و γ اعداد صحیح گاوسی باشند به‌طوری که $\alpha|\gamma$ و $\beta|\gamma$. اگر α و β نسبت به هم اول باشند، نشان دهید که $\alpha\beta|\gamma$. (راهنمایی: (۱۰.۱) را ببینید، یا تجزیهٔ یکتا را به‌کار برید.)

۱۶. فرض می‌کنیم α و β اعداد صحیح گاوسی باشند که نُرمشان نسبت به هم اول‌اند. ثابت کنید α و β نسبت به هم اول‌اند. آیا عکس این مطلب برقرار است؟ توضیح دهید.

۱۷. (ii.۱۸.۱۱) را اثبات کنید: اگر α و β عناصر $Q(\sqrt{d})$ باشند، آنگاه $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

۱۸. (iii.۱۸.۱۱) را ثابت کنید: اگر α یک عدد صحیح در $Q(\sqrt{d})$ باشد، آنگاه α یک یکه است اگر و تنها اگر $\mathrm{N}(\alpha) = \pm ۱$.

۱۹. ثابت کنید که $۲ + \sqrt{-۶}$ در $Q(\sqrt{-۶})$ اول است.

۲۰. نشان دهید که $۱ + \sqrt{۳}$ و $۱ - \sqrt{۳}$ در $Q(\sqrt{۳})$ وابسته هستند.

۲۱. تعیین کنید که کدام‌یک از اعداد زیر در $Q(\sqrt{-۱۳})$ اول‌اند: $۲\sqrt{-۱۳} + ۱$؛ $۳ + \sqrt{-۱۳}$؛ ۴۱.

۲۲. (الف) آیا $\alpha = ۱۱$ در $Q(\sqrt{-۳})$ اول است؟ اگر چنین است، ثابت کنید. اگر چنین نیست، α را به‌صورت حاصلضرب اعداد اول بیان کنید. (ب) به همین سؤال اگر $\alpha = ۲۳$ پاسخ دهید. (توجه کنید که $-۳ \equiv ۱ \pmod ۴$).

۲۳. نشان دهید که $۵ + \sqrt{۱۵}$ در $Q(\sqrt{۱۵})$ اول است.

۲۴. ثابت کنید به‌ازای هر عدد خالی از مربعِ d، بی‌نهایت عدد صحیح در $Q(\sqrt{d})$ وجود دارند که در $Q(\sqrt{d})$ اول‌اند.

۲۵. با بررسی تجزیهٔ ۲۰، نشان دهید که $Q(\sqrt{-۱۹})$ ویژگی تجزیهٔ یکتا ندارد.

۲۶. تمام نمایشهای $۱۲۱ \times ۴۹ \times ۸$ به‌صورت $a^۲ + ۲b^۲$ را، که a و b اعداد صحیح هستند، پیدا کنید.

۲۷. یکه اصلی ϵ در $Q(\sqrt{۱۰۱})$ را بیابید، و ثابت کنید ϵ یکهٔ اصلی است.

۲۸. همهٔ یکه‌های $Q(\sqrt{۳})$ را که بین ۱۰۰ و ۱۰۰۰ قرار دارند پیدا کنید.

ملاحظاتی برای فصل ۱۱

۱. در ۱۸۰۱ گاوس می‌دانست که اعداد صحیح $Q(\sqrt{d})$ به‌ازای d مساوی -۱، -۲، -۳، -۷، -۱۱، -۱۹، -۴۳، -۶۷، و -۱۶۳ تجزیهٔ یکتا دارند. (آنچه او در واقع اثبات کرد یک حکم هم‌ارز دربارهٔ صورتهای درجهٔ دوم بود.) گاوس همچنین حدس زد که اینها تنها dهای خالی از مربعِ منفی با این ویژگی هستند. این حدسیه بیش از ۱۵۰ سال به‌صورت حل‌نشده باقی ماند.

در ۱۹۳۴، ه. هایلبر ون[1] و اِ. ه. لین فوت[2] نشان دادند که حداکثر یک d خالی از مربع منفی دیگر وجود دارد که به‌ازای آن اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا دارند. سرانجام، در ۱۹۶۶، ه.م. استارک[3] ثابت کرد که فهرست گاوس واقعاً کامل است. کمابیش هم‌زمان، آ. بیکر نیز برهانی یافته بود. هر دو برهان فوق‌العاده دشوار هستند.

برای d مثبت، این سؤال که چه وقت تجزیهٔ یکتا داریم ابداً پاسخ داده نشده است. تعداد ۳۷ عدد خالی از مربع مثبت d کمتر از ۱۰۰ وجود دارند که به‌ازای آنها اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا دارند، و فقط به‌ازای ۱۷ تای اینها $Q(\sqrt{d})$ اقلیدسی است. بعکس مورد منفی d، به نظر می‌رسد که تجزیهٔ یکتا وقتی d مثبت است کاملاً مشترک است. ولی، حتی ثابت نشده است که بی‌نهایت عدد خالی از مربع مثبت d وجود دارد به‌طوری‌که اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا داشته باشند.

۲. یک صورت درجهٔ دوم دومجهولی یک چندجمله‌یی $ax^2+bxy+cy^2$ است، که در آن a، b، و c اعداد صحیح اختیار می‌شوند. یکی از مسائل اساسی نظریهٔ صورتهای درجهٔ دوم، که به زبان بهاسکره و فرما برمی‌گردد، تعیین اعداد صحیحی است که قابل نمایش به‌صورت $ax^2+bxy+xy^2$ هستند. برای صورتهای x^2+y^2 و x^2+2y^2 جواب این سؤال را یافته‌ایم ((۲۱.۱۱) را ببینید). با کامل کردن مربع، می‌توان دید که

$$4a(ax^2+bxy+cy^2)=(2ax+by-y\sqrt{d})(2ax+by+y\sqrt{d})$$

که در آن $d=b^2-4ac$. لذا سؤال مربوط به قابلیت نمایش توسط صورتهای درجهٔ دوم ارتباط نزدیکی با تجزیه در $Q(\sqrt{d})$ دارد.

به‌ویژه، صورت x^2-dy^2 را در نظر می‌گیریم. (در قضیهٔ ۲۱.۱۱ حالت $d=-2$ مطرح می‌شود.) با یافتن اعداد اول p که می‌توانند نمایش داده شوند و سپس استفاده اینکه نَرم حاصلضرب برابر حاصلضرب نُرمهاست، مسأله اعداد صحیحی را که قابل نمایش هستند حل کردیم. یافتن pهای نمایش‌پذیر یک کاربرد ساده از تقابل درجهٔ دوم است. این روند وقتی که اعداد صحیح $Q(\sqrt{d})$ تجزیهٔ یکتا دارند کارساز است. (وقتی d مثبت است، بررسی نمایش‌پذیری $-p$ نیز لازم است.) ولی وضعیت همیشه به این آسانی نیست. مثلاً می‌توان ۲۱ را به‌صورت x^2+5y^2 نمایش داد، اما هیچ‌کدام از عاملهای اولش را نمی‌توان. این پدیده ارتباط نزدیکی با این حقیقت دارد که تجزیهٔ یکتا برای اعداد صحیح $Q(\sqrt{-5})$ برقرار نیست.

1. H. Heilbronn 2. E. H. Linfoot 3. H. M. Stark

شرح مختصری از زندگینامه‌ها

ارنست ادوارد کومر[1] در ۱۸۱۰ در آلمان متولد شد و دکترایش را از دانشگاه هاله[2] اخذ نمود. به مدت ۱۰ سال در یک دبیرستان تدریس کرد. لئوپولد کرونکر، که خود ریاضیدان مشهوری شد یکی از شاگردان کومر بود. در ۱۸۵۵ به استادی ریاضیات دانشگاه برلین و دانشکدهٔ جنگ برلین منصوب شد. تا ۳۲ سالگی، کارهای کومر بیشتر به انتگرالهای معین، معادلات دیفرانسیل، و سریها، به‌طور چشمگیرتر توابع ابرهندسی، مربوط می‌شد.

کومر نخستین مساهمت مهم خود در نظریهٔ اعداد را با کاوش در قوانین تقابل بالاتر شروع کرد. با پیگیری کارهای گاوس و ژاکوبی، کومر به مطالعهٔ حساب «اعداد صحیح» در میدان $Q(\alpha)$ که از الحاق یک ریشهٔ غیرنمایان ۱ $= x^n$ به گویاها به دست آمده بود کشیده شد. او ثابت کرد که تجزیهٔ یکتا به‌ازای ۲۳ $= n$ برقرار نیست و «اعداد ایده‌آل» را برای برقراری تجزیهٔ یکتا موفق شد وارد کند. سرانجام، این اعداد ایده‌آل را برای احیای یک قانون تقابل عام به‌کار برد. کومر همچنین ارتباط حساب $Q(\sqrt{d})$ را با نظریهٔ صورتهای درجهٔ دوم خاطرنشان ساخت. صورتهای درجهٔ دوم درکارهای مربوط به نظریهٔ اعدادِ لاگرانژ، لژاندر، وگاوس اساسی بود. از این‌رو کومر پایه‌گذار نظریهٔ اعداد جبری است.

کومر به خاطرکارهایش در آخرین قضیهٔ فرما نیز معروف است. در اینجا نیز، تجزیه در $Q(\sqrt{\alpha})$ را به‌کار برد و سرانجام آخرین قضیهٔ فرما را برای تمام نماهای کمتر از ۱۰۰ ثابت کرد. او یکی از نخستین ریاضیدانانی بودکه نشان داد چگونه مفاهیم جبری «مجرد» را می‌توان برای حل مسائل خاص به‌کاربرد.

کومر در ۱۸۹۳ در برلین درگذشت.

مراجع

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Fourth Edition). (See Chapter 7.)

Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers* (Fifth Edition), John Wiley & Sons, New York, 1991.

از ابتدای چاپ کتاب نیون و تسوکرمن در ۱۹۶۰، این کتاب به‌عنوان یک کتاب درسی در نظریهٔ مقدماتی اعداد معروف بوده است. مطالب چاپ اخیر در یک سطح بالاتر و نظری‌تری نسبت به سایر کتابهای درسی متداول ارائه شده است. به هر حال، بعد ازکسب یک زمینهٔ پایه‌یی در نظریهٔ اعداد، یک کتاب عالی برای مطالعه است و یک بحث نسبتاً کاملی از مطالب این فصل را داراست.

1. Ernst Eduard Kummer 2. Halle

پیوست

جدول ۱. اعداد اول کوچکتر از ۱۰۰۰ و g کوچکترین ریشهٔ اولیهٔ آنها

p	g	p	g	p	g	p	g
2	1	191	19	439	15	709	2
3	2	193	5	443	2	719	11
5	2	197	2	449	3	727	5
7	3	199	3	457	13	733	6
11	2	211	2	461	2	739	3
13	2	223	3	463	3	743	5
17	3	227	2	467	2	751	3
19	2	229	6	479	13	757	2
23	5	233	3	487	3	761	6
29	2	239	7	491	2	769	11
31	3	241	7	499	7	773	2
37	2	251	6	503	5	787	2
41	6	257	3	509	2	797	2
43	3	263	5	521	3	809	3
47	5	269	2	523	2	811	3
53	2	271	6	541	2	821	2
59	2	277	5	547	2	823	3
61	2	281	3	557	2	827	2
67	2	283	3	563	2	829	2
71	7	293	2	569	3	839	11
73	5	307	5	571	3	853	2
79	3	311	17	577	5	857	3
83	2	313	10	587	2	859	2
89	3	317	2	593	3	863	5
97	5	331	3	599	7	877	2
101	2	337	10	601	7	881	3
103	5	347	2	607	3	883	2
107	2	349	2	613	2	887	5
109	6	353	3	617	3	907	2
113	3	359	7	619	2	911	17
127	3	367	6	631	3	919	7
131	2	373	2	641	3	929	3
137	3	379	2	643	11	937	5
139	2	383	5	647	5	941	2
149	2	389	2	653	2	947	2
151	6	397	5	659	2	953	3
157	5	401	3	661	2	967	5
163	2	409	21	673	5	971	6
167	5	419	2	677	2	977	3
173	2	421	2	683	5	983	5
179	2	431	7	691	3	991	6
181	2	433	5	701	2	997	7

جدول ۲. بسط کسر مسلسل $\sqrt{d}$ به‌ازای $d < ۱۰۰$

d	$\sqrt{d}$	d	$\sqrt{d}$
2	$\langle 1,\overline{2}\rangle$	53	$\langle 7,\overline{3,1,1,3,14}\rangle$
3	$\langle 1,\overline{1,2}\rangle$	54	$\langle 7,\overline{2,1,6,1,2,14}\rangle$
5	$\langle 2,\overline{4}\rangle$	55	$\langle 7,\overline{2,2,2,14}\rangle$
6	$\langle 2,\overline{2,4}\rangle$	56	$\langle 7,\overline{2,14}\rangle$
7	$\langle 2,\overline{1,1,1,4}\rangle$	57	$\langle 7,\overline{1,1,4,1,1,14}\rangle$
8	$\langle 2,\overline{1,4}\rangle$	58	$\langle 7,\overline{1,1,1,1,1,1,14}\rangle$
10	$\langle 3,\overline{6}\rangle$	59	$\langle 7,\overline{1,2,7,2,1,14}\rangle$
11	$\langle 3,\overline{3,6}\rangle$	60	$\langle 7,\overline{1,2,1,14}\rangle$
12	$\langle 3,\overline{2,6}\rangle$	61	$\langle 7,\overline{1,4,3,1,2,2,1,3,4,1,14}\rangle$
13	$\langle 3,\overline{1,1,1,1,6}\rangle$	62	$\langle 7,\overline{1,6,1,14}\rangle$
14	$\langle 3,\overline{1,2,1,6}\rangle$	63	$\langle 7,\overline{1,14}\rangle$
15	$\langle 3,\overline{1,6}\rangle$	65	$\langle 8,\overline{16}\rangle$
17	$\langle 4,\overline{8}\rangle$	66	$\langle 8,\overline{8,16}\rangle$
18	$\langle 4,\overline{4,8}\rangle$	67	$\langle 8,\overline{5,2,1,1,7,1,1,2,5,16}\rangle$
19	$\langle 4,\overline{2,1,3,1,2,8}\rangle$	68	$\langle 8,\overline{4,16}\rangle$
20	$\langle 4,\overline{2,8}\rangle$	69	$\langle 8,\overline{3,3,1,4,1,3,3,16}\rangle$
21	$\langle 4,\overline{1,1,2,1,1,8}\rangle$	70	$\langle 8,\overline{2,1,2,1,2,16}\rangle$
22	$\langle 4,\overline{1,2,4,2,1,8}\rangle$	71	$\langle 8,\overline{2,2,1,7,1,2,2,16}\rangle$
23	$\langle 4,\overline{1,3,1,8}\rangle$	72	$\langle 8,\overline{2,16}\rangle$
24	$\langle 4,\overline{1,8}\rangle$	73	$\langle 8,\overline{1,1,5,5,1,1,16}\rangle$
26	$\langle 5,\overline{10}\rangle$	74	$\langle 8,\overline{1,1,1,1,16}\rangle$
27	$\langle 5,\overline{5,10}\rangle$	75	$\langle 8,\overline{1,1,1,16}\rangle$
28	$\langle 5,\overline{3,2,3,10}\rangle$	76	$\langle 8,\overline{1,2,1,1,5,4,5,1,1,2,1,16}\rangle$
29	$\langle 5,\overline{2,1,1,2,10}\rangle$	77	$\langle 8,\overline{1,3,2,3,1,16}\rangle$
30	$\langle 5,\overline{2,10}\rangle$	78	$\langle 8,\overline{1,4,1,16}\rangle$
31	$\langle 5,\overline{1,1,3,5,3,1,1,10}\rangle$	79	$\langle 8,\overline{1,7,1,16}\rangle$
32	$\langle 5,\overline{1,1,1,10}\rangle$	80	$\langle 8,\overline{1,16}\rangle$
33	$\langle 5,\overline{1,2,1,10}\rangle$	82	$\langle 9,\overline{18}\rangle$
34	$\langle 5,\overline{1,4,1,10}\rangle$	83	$\langle 9,\overline{9,18}\rangle$
35	$\langle 5,\overline{1,10}\rangle$	84	$\langle 9,\overline{6,18}\rangle$
37	$\langle 6,\overline{12}\rangle$	85	$\langle 9,\overline{4,1,1,4,18}\rangle$
38	$\langle 6,\overline{6,12}\rangle$	86	$\langle 9,\overline{3,1,1,1,8,1,1,1,3,18}\rangle$
39	$\langle 6,\overline{4,12}\rangle$	87	$\langle 9,\overline{3,18}\rangle$
40	$\langle 6,\overline{3,12}\rangle$	88	$\langle 9,\overline{2,1,1,1,2,18}\rangle$
41	$\langle 6,\overline{2,2,12}\rangle$	89	$\langle 9,\overline{2,3,3,2,18}\rangle$
42	$\langle 6,\overline{2,12}\rangle$	90	$\langle 9,\overline{2,18}\rangle$
43	$\langle 6,\overline{1,1,3,1,5,1,3,1,1,12}\rangle$	91	$\langle 9,\overline{1,1,5,1,5,1,1,18}\rangle$
44	$\langle 6,\overline{1,1,1,2,1,1,1,12}\rangle$	92	$\langle 9,\overline{1,1,2,4,2,1,1,18}\rangle$
45	$\langle 6,\overline{1,2,2,2,1,12}\rangle$	93	$\langle 9,\overline{1,1,1,4,6,4,1,1,1,18}\rangle$
46	$\langle 6,\overline{1,3,1,1,2,6,2,1,1,3,1,12}\rangle$	94	$\langle 9,\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}\rangle$
47	$\langle 6,\overline{1,5,1,12}\rangle$	95	$\langle 9,\overline{1,2,1,18}\rangle$
48	$\langle 6,\overline{1,12}\rangle$	96	$\langle 9,\overline{1,3,1,18}\rangle$
50	$\langle 7,\overline{14}\rangle$	97	$\langle 9,\overline{1,5,1,1,1,1,1,1,5,1,18}\rangle$
51	$\langle 7,\overline{7,14}\rangle$	98	$\langle 9,\overline{1,8,1,18}\rangle$
52	$\langle 7,\overline{4,1,2,1,4,14}\rangle$	99	$\langle 9,\overline{1,18}\rangle$

چهره‌های مهم در تاریخ نظریه اعداد

(برحسب حروف الفبا)

آدامار، ژاک	۱۸۶۵_۱۹۶۳
اراتستن	ح ۲۳۰ ق.م
ارشمیدس	۲۱۲_۲۸۷ ق. م
آریبهطه	ح ۴۷۵_۵۵۰
اقلیدس	۲۸۵_۳۲۳ ق. م
الکرجی	ح ۱۰۹۰
اویلر، لئونهارت	۱۷۰۷_۱۷۸۳
آیزنشتاین، فردینانت	۱۸۲۳_۱۸۵۲
باشه، کلود	۱۵۸۷_۱۶۳۸
براونکر، ویلیام	۱۶۲۰_۱۶۸۴
برهمگوپته	ح ۶۲۵
بومبلی، رافائل	۱۵۲۶_۱۵۷۲
بهاسکره	۱۱۱۴_ح ۱۱۸۵
پل، جان	۱۶۱۰_۱۶۸۵
توئه، آکسل	۱۸۶۳_۱۹۲۲
چبیشف، پافنوتی	۱۸۲۱_۱۸۹۴

چئین، کیوشائو	ح ۱۲۰۲_۱۲۶۱
دیریکله، پترلوژون	۱۸۰۵_۱۸۵۹
دیوفانتوس	ح ۲۵۰
یاکوبی، کارل گوستاف	۱۸۰۴_۱۸۵۱
سون‌ـتسو (تزی)	ح ۲۵۰
فرما، پییردو	۱۶۰۱_۱۶۶۵
فرنیکل، (دوبِسی)، برنار	ح ۱۶۰۲_۱۶۷۵
فیبوناتچی	ح ۱۱۷۵_۱۲۵۰
فیثاغورس	۵۸۵_۵۰۱ ق. م.
کومر، ارنست	۱۸۱۰_۱۸۹۳
گاوس، کارل فریدریش	۱۷۷۷_۱۸۵۵
گولدباخ، کریستیان	۱۶۹۰_۱۷۶۴
لژاندر، آدرین ماری	۱۷۵۲_۱۸۳۳
لوکا، ادوار	۱۸۴۲_۱۸۹۱
لاگرانژ، ژوزف لویی	۱۷۳۶_۱۸۱۳
لامه، گابریل	۱۷۹۵_۱۸۷۰
مِرسِن، مارن	۱۵۸۸_۱۶۴۸
وئرینگ، ادوارد	۱۷۳۴_۱۷۹۳
والیس، جان	۱۶۱۰_۱۷۰۳
ویلسون، جان	۱۷۴۱_۱۷۹۳
وینوگراوف، ایوان ماتوه‌یویچ	۱۸۹۱_۱۹۸۳
واله پوسن، شارل دولا	۱۸۶۶_۱۹۶۲
هاردی، گادفری هرلد	۱۸۷۷_۱۹۴۷
هیلبرت، داویت	۱۸۶۲_۱۹۴۳

چهره‌های مهم در تاریخ نظریه اعداد

(به‌ترتیب زمان)

فیثاغورس	۵۸۵_۵۰۱ ق. م
اقلیدس	۳۲۳_۲۸۵ ق. م
ارشمیدس	۲۸۷_۲۱۲ ق. م
اراتستن	حـ ۲۳۰ ق. م
دیوفانتوس	حـ ۲۵۰ ب. م
سون_تسو	حـ ۲۵۰
آریبهطه	حـ ۵۵۰_۴۷۵
برهمگوپته	حـ ۶۲۵
الکرجی	حـ ۱۰۹۰
بهاسکره	۱۱۱۴_ حـ ۱۱۸۵
فیبوناتچی	حـ ۱۲۵۰_۱۱۷۵
چئین، کیوشائو	حـ ۱۲۶۱_۱۲۰۲
بومبلی، رافائل	۱۵۷۲_۱۵۲۶
باشه، کلود	۱۶۳۸_۱۵۸۷
مِرسِن، مارن	۱۶۴۸_۱۵۸۸
فرما، پییردو	۱۶۶۵_۱۶۰۱

فرنیکل دوبسی، برنار	ح ۱۶۷۵_۱۶۰۲
پل، جان	۱۶۸۵_۱۶۱۰
والیس، جان	۱۷۰۳_۱۶۱۰
براونکر، ویلیام	۱۶۸۴_۱۶۲۰
گلدباخ، کریستیان	۱۷۶۴_۱۶۹۰
اویلر، لئونهارت	۱۷۸۳_۱۷۰۷
وئرینگ، ادوارد	۱۷۹۳_۱۷۳۴
لاگرانژ، ژوزف لویی	۱۸۱۳_۱۷۳۶
ویلسون، جان	۱۷۹۳_۱۷۴۱
لژاندر، آدرین ماری	۱۸۳۳_۱۷۵۲
گاوس، کارل فریدریش	۱۸۵۵_۱۷۷۷
لامه، گابریل	۱۸۷۰_۱۷۹۵
ژاکوبی، کارل گوستاو	۱۸۵۱_۱۸۰۴
دیریکله، پترلوژون	۱۸۵۹_۱۸۰۵
کومر، ارنست	۱۸۹۳_۱۸۱۰
چبیشف، پافنوتی	۱۸۹۴_۱۸۲۱
آیزنشتاین، فردینانت	۱۸۵۲_۱۸۲۳
لوکا، ادوار	۱۸۹۱_۱۸۴۲
هیلبرت، داویت	۱۹۴۳_۱۸۶۲
توئه، آکسل	۱۹۲۲_۱۸۶۳
آدامار، ژاک	۱۹۶۳_۱۸۶۵
واله پوسن، شارل دولا	۱۹۶۲_۱۸۶۶
هاردی، گادفری هرله	۱۹۴۷_۱۸۷۷
وینوگرادوف، ایوان ماتِوِیویچ	۱۹۸۳_۱۸۹۱

فهرست نمادها

حاصلضرب	Π
مجموعیابی	$\sum$
a عدد b را می‌شمارد	$a\|b$
a عدد b را نمی‌شمارد	$a\nmid b$
بزرگترین مقسوم‌علیه مشترک a، b	(a,b)
کوچکترین مضرب مشترک a، b	$[a,b]$
تعداد مقسوم‌علیه‌های مثبتِ n	$\tau(n)$
مجموع مقسوم‌علیه‌های مثبتِ n	$\sigma(n)$
جزء صحیح x	$[x]$
a همنهشت با b به پیمانهٔ m	$a \equiv b (\mathrm{mod}\, m)$
a ناهمنهشت با b به پیمانهٔ m	$a \not\equiv b (\mathrm{mod}\, m)$
تابع ϕ – اویلر	$\phi(n)$
نماد لژاندر	(a/p)
نماد ژاکوبی	(a/m)
مرتبهٔ a	$\mathrm{ord}\, a$
اندیس a	$\mathrm{ind}\, a$
nامین عدد مرسِن	M_n
nامین عدد فرما	F_n

تعداد اعدادِ اولِ نابیشتر از x	$\pi(x)$
تعداد نمایشهای n به‌صورت مجموع دو مربع	$N(n)$
کسر مسلسل متناهی	$< a_0, a_1, a_2, \ldots, a_n >$
همگرای kام	$c_k = p_k/q_k$
کسر مسلسل نامتناهی	$< a_0 a_1, a_2, \ldots >$
کسر مسلسل دوره‌یی	$\langle c_0, c_1, \ldots, c_n, \overline{a_0, a_1, \ldots, a_k} \rangle$
گنگ درجهٔ دوم	$\alpha = (r + \sqrt{d})/s$
مزدوج α	$\alpha' = (r - \sqrt{d})/s$
عدد صحیح گاوسی؛ مزدوج	$a + bi; a - bi$
یکه	ϵ
عدد اول گاوسی	π
نُرم $a + bi$	$\mathrm{N}(a + bi)$
توسیع درجهٔ دوم	$Q(\sqrt{d})$

مراجع

W.W. Adams and L.J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1976.

Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

David M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

Harold Davenport, *The Higher Arithmetic* (Sixth Edition), Cambridge University Press, Cambridge, England, 1992.

Harold M. Edwards, *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

Leonhard Euler, *Elements of Algebra*, translated by John Hewlett, Springer-Verlag, New York, 1984.

Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, translated by Arthur A. Clarke, Yale University Press, New Haven, Connecticut, 1966.

Peter Giblin, *Primes and Programming*, Cambridge University Press, Cambridge, England, 1993.

Emil Grosswald, *Topics from the Theory of Numbers* (Second Edition), Birkhäuser, Boston, 1982.

G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (Fourth Edition), The Clarendon Press, Oxford, England, 1971.

Thomas L. Heath, *The Thirteen Books of Euclid's Elements, Volume II*, Cambridge University Press, Cambridge, England, 1926.

Thomas L. Heath, *Diophantus of Alexandria*, Dover, New York, 1964.

K. Ireland and M.I. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

Victor Klee and Stan Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Mathematical Association of America, Washington, 1991.

Donald E. Knuth, *The Art of Computer Programming, Volume 2* (Second Edition), Addison-Wesley, Reading, Massachussetts, 1981.

Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

William J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, Reading, Massachusetts, 1977.

L.J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

Trygve Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981 (originally published in 1951).

W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientific Publishers, Warsaw, 1986.

Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers* (Fifth Edition), John Wiley & Sons, New York, 1991.

Carl D. Olds, *Continued Fractions*, Random House, New York, 1963.

Oystein Ore, *Number Theory and Its History*, McGraw-Hill, New York, 1948.

Hans Rademacher, *Lectures on Elementary Number Theory*, Blaisdell, New York, 1964.

Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

Paulo Ribenboim, *The Book of Prime Number Records* (Second Edition), Springer-Verlag, New York, 1989.

Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1987.

Kenneth H. Rosen, *Elementary Number Theory and its Applications* (Third Edition), Addison-Wesley, Reading, Massachusetts, 1992.

W. Scharlau and H. Opolka, *From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development*, Springer-Verlag, New York, 1985.

Jacques Sesiano, *Books IV to VII of Diophantus' Arithmetica*, Springer-Verlag, New York, 1982.

Daniel Shanks, *Solved and Unsolved Problems in Number Theory* (Third Edition), Chelsea, New York, 1985.

J.V. Uspensky and M.A. Heaslet, *Elementary Number Theory*, McGraw-Hill, New York, 1939.

I.M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

تاریخی

Eric T. Bell, *Men of Mathematics*, Simon & Schuster, New York, 1965.

Carl B. Boyer and Uta C. Merzbach, *A History of Mathematics* (Second Edition), John Wiley & Sons, New York, 1989.

Claude Brezinski, *History of Continued Fractions and Padé Approximants*, Springer-Verlag, New York, 1991.

David M. Burton, *The History of Mathematics* (Second Edition), Wm. C. Brown, Dubuque, Iowa, 1991.

Leonard Eugene Dickson, *History of the Theory of Numbers* (3 volumes), Chelsea, New York, 1952 (originally published in 1919).

George G. Joseph, *The Crest of the Peacock: Non-European Roots of Mathematics*, Penguin Books, New York, 1991.

Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.

Ulrich Libbrecht, *Chinese Mathematics in the Thirteenth Century*, The MIT Press, Cambridge, Massachusetts, 1973.

James R. Newman, *The World of Mathematics* (4 volumes), Simon & Schuster, New York, 1956.

André Weil, *Number Theory: An approach through history from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.

مقاله های مجلات

Robert A. Coury, "A Continued Fraction Approach for Factoring Large Numbers," *Pi Mu Epsilon Journal*, Vol. 9, No. 1 (1989), 9–12.

David A. Cox, "Introduction to Fermat's Last Theorem," *American Mathematical Monthly*, Vol. 101, No. 1 (1994), 3–14.

Jacques Dutka, "On the Gregorian Revision of the Julian Calendar," *Mathematical Intelligencer*, Vol. 10, No. 1 (1988), 56–64.

M. Ram Murty, "Artin's Conjecture for Primitive Roots," *Mathematical Intelligencer*, Vol. 10, No. 4 (1988), 59–67.

Carl Pomerance, "The Search for Prime Numbers," *Scientific American*, Vol. 247 (1982), 136–147.

V. Frederick Rickey, "Mathematics of the Gregorian Calendar," *Mathematical Intelligencer*, Vol. 7, No. 1 (1985), 53–56.

David E. Rowe, "Gauss, Dirichlet, and the Law of Biquadratic Reciprocity," *Mathematical Intelligencer*, Vol. 10, No. 2 (1988), 13–25.

A. Seidenberg, "The Ritual Origin of Geometry," *Archive for the History of the Exact Sciences*, Vol. 1 (1963), 488–527.

Stan Wagon, "Perfect Numbers," *Mathematical Intelligencer*, Vol. 7, No. 2 (1985), 66–68.

Stan Wagon, "Primality Testing," *Mathematical Intelligencer*, Vol. 8, No. 3 (1986), 58–61.

Stan Wagon, "The Euclidean Algorithm Strikes Again," *American Mathematical Monthly*, Vol. 97, No. 2 (1990), 125–129.

نمایه