وزارت علوم تحقیقات و فناوری
مرکز نشر دانشگاهی

نظریهٔ مقدماتی اعداد

دیوید ام. برتن

ترجمهٔ محمد صادق منتخب

نظریهٔ مقدماتی اعداد

دیوید ام. برتن

ترجمهٔ محمدصادق منتخب

مرکز نشر دانشگاهی

بسم‌الله الرحمن الرحیم

فهرست

عنوان	صفحه

عنوان | صفحه

پیشگفتار

افلاطون گفت: «خدا هندسه‌دان است.» ژاکوبی این جمله را چنین تغییر داد: «خدا حساب‌دان است.» سپس کرونکر آمد و این سخن به یاد ماندنی را باب کرد: «خدا عددهای طبیعی را آفرید، مابقی کار انسان است.»

فلیکس کلاین

هدف از این کتاب ارائهٔ شرح ساده‌ای از نظریهٔ کلاسیک اعداد و برخی از زمینه‌های تاریخی است که نظریهٔ اعداد بر پایهٔ آنها شکل گرفته است. گرچه این کتاب بیشتر برای تدریس در یک درس نیمساله در سطح کارشناسی در نظر گرفته شده، به گونه‌ای طراحی شده است که مناسب مؤسسه‌های تربیت معلم نیز باشد و بتوان از آن در دوره‌های بازآموزی ریاضی نیز استفاده کرد. این کتاب برای کسانی که خود را برای تدریس در دبیرستان آماده می‌کنند و لازم است آشنایی مختصری با نظریهٔ اعداد داشته باشند، بسیار مناسب است.

نظریهٔ اعداد در جهان ریاضیات همیشه موقعیت منحصر به‌فردی داشته است. این امر به‌دلیل اهمیت تاریخی تردید ناپذیر این موضوع است: یکی از معدود رشته‌های علمی است که پیشینهٔ برخی از نتیجه‌های قابل اثبات آن به زمانی می‌رسد که حتی فکر تأسیس دانشگاه یا آکادمی مطرح نبوده است. از دوران باستان، تقریباً در هر سده کشفیات جذاب تازه‌ای دربارهٔ ویژگیهای عددها صورت گرفته است؛ و بسیاری از بزرگان علوم ریاضی، در مقطعی از فعالیتهای خود، در این حیطه از دانش به پژوهش پرداخته‌اند. چرا نظریهٔ اعداد این چنین جاذبهٔ مقاومت ناپذیری در نظر ریاضیدانان برجسته و هزاران ریاضیکار آماتور داشته است؟ یکی از پاسخها مبتنی است بر مقدماتی بودن صورت مسأله‌های آن. گرچه حل بسیاری از مسأله‌های نظریهٔ اعداد فوق‌العاده دشوار است، می‌توان صورت آنها را چنان ساده بیان کرد که حتی علاقه و کنجکاوی کسانی را که آموزش ریاضی

زیادی ندیده‌اند، برانگیزد. برخی از به‌ظاهر ساده‌ترین مسأله‌های آن که سده‌ها در معرض زورآزمایی فکری بوده‌اند، هنوز جزو غامضترین مسأله‌های حل نشده در کل ریاضیات به حساب می‌آیند.

بنابراین، مایهٔ شگفتی است که بسیاری از دانشجویان نظریهٔ اعداد را جدی نمی‌گیرند و آن را مبحث کم ارزشی در حاشیهٔ ریاضیات به حساب می‌آورند. این احساس بدون شک ناشی از این دیدگاه است که نظریهٔ اعداد به‌وضوح بیفایده‌ترین شاخهٔ ریاضیات محض است و نتیجه‌های به‌دست آمده در این زمینه کاربردهای معدودی در مسأله‌های مربوط به جهان واقعی دارند. در روزگاری که حوصلهٔ چندانی برای پرداختن به «علوم نظری» وجود ندارد، معمولاً با دانشجویان ریاضیی برخورد می‌کنیم که از نظریهٔ اعداد چندان چیزی نمی‌دانند، یا اصلاً چیزی نمی‌دانند. این وضعیت واقعاً مایهٔ تأسف است، زیرا نظریهٔ مقدماتی اعداد یکی از بهترین موضوعها برای آموزش اولیهٔ ریاضی است. به آموزش قبلی طولانی نیاز ندارد، محتوای آن مأنوس و آشناست، و بیش از هر شاخهٔ دیگر ریاضیات، روشهای تحقیق در آن مطابق با شیوهٔ رایج در علوم تجربی است. دانشجویی که در این زمینه کار می‌کند، باید تا اندازهٔ زیادی متکی به آزمایش و خطا، همراه با کنجکاوی، شهود، و خلاقیت باشد؛ در هیچ یک از شاخه‌های دیگر ریاضیات، اثبات دقیق تا این اندازه متکی به آزمایشهای طولانی و صبورانه نیست. اگر روند کار گهگاه دچار کندی و دشواری می‌شود، دانشجو می‌تواند خود را با این فکر تسلّی دهد که تقریباً هر ریاضیدان برجسته در زمان گذشته نیز همان مسیر دشوار را پیموده است.

معروف است که می‌گویند هرکس بخواهد به کُنه موضوعی پی ببرد، باید نخست تاریخچهٔ آن را مطالعه کند. در تأیید این نظر، کوشیده‌ایم مطالب را در چارچوب تاریخی قرار دهیم. نکته‌های تاریخی تنیده در لابه‌لای متن، علاوه بر جان بخشیدن به جنبهٔ نظری کتاب، این واقعیت را روشن می‌سازند که نظریهٔ اعداد هنر مرده‌ای نیست، بلکه بر اثر تلاشهای متخصصانِ بسیارش، سرزنده و پویاست. این مطالب تاریخی نشان می‌دهند که این موضوع به روشی گام‌به‌گام ساخته و پرداخته شده است و کار هر فردی که سهمی در آن دارد اساس پژوهش بسیاری افراد دیگر بوده است: در بسیاری موارد، قرنها تلاش لازم بوده تا گام مهمی برداشته شود. همین‌که دانشجو دریابد که چگونه افراد نابغه مسیر کار خلاقه را افتان و خیزان و کورمال کورمال پیموده‌اند تا کم‌کم به نتایجی دست یافته‌اند، از ناشیگری خود در حل تکالیف درسی کمتر دچار سرخوردگی خواهد شد.

اما چند کلمه دربارهٔ تمرینها. بسیاری از بخشها با شمار قابل توجهی تمرین به پایان می‌رسند که از نظر دشواری، از مسأله‌های کاملاً محاسبه‌ای تا مسأله‌های استدلالی مشکل در میان آنها هست. این مسأله‌ها جزئی ضروری از کتاب هستند و لازم است خواننده تمام سعی خود را در حل آنها به کار برد، زیرا هیچ کس نمی‌تواند نظریهٔ اعداد را بدون حل مساله فرا گیرد. تمرینهای محاسبه‌ای،

گسترش دهندهٔ تکنیکهای اساسی متن‌اند و میزان درک مفهومها را محک می‌زنند، و تمرینهای نظری و استدلالی، توان خواننده را در اثبات کردن تقویت می‌کنند. تمرینها علاوه بر اینکه حاوی اطلاعاتی اضافی دربارهٔ مطالب عرضه شدهٔ پیشین هستند، مفهومهای متنوعی معرفی می‌کنند که در داخل متن مورد بحث قرار نگرفته‌اند. کلاً در برابر وسوسهٔ استفاده از تمرین به‌منظور معرفی نتایجی که پس از آن مورد نیازند، مقاومت کرده‌ایم. بنابراین، لازم نیست خواننده روی هر تمرینی به منظور فهم بقیهٔ کتاب کار کند. بیشتر تمرینهایی که حل آنها سر راست به نظر نمی‌رسد، با راهنمایی همراه‌اند.

گرچه کتاب در اصل برای دانشجویان ریاضی نوشته شده است، پیشنیاز رسمی چندانی ندارد؛ مطالعهٔ آن برای هر کسی که زمینه‌ای قوی در ریاضیات دبیرستانی داشته باشد سودمند است. به ویژه، اطلاع از مفهومهای جبر مجرد ضروری نیست. دانشجویانی که درسی در جبر (مثلاً در سطح کتاب آشنایی با جبر جدید نوشتهٔ نیل مک‌کوی[1] یا آشنایی با جبر مجرد جدید به قلم این نویسنده[2]) گذرانده باشند، در مطالعهٔ این کتاب می‌توانند بیشتر مباحث چهار فصل نخست را کنار بگذارند.

با توجه به فهرست مطالب، بدیهی است که محتوای کتاب بیش از آن است که بتوان آن را به گونه‌ای رضایتبخش در یک درس نیمساله عرضه کرد. این امر باعث می‌شود که کتاب برای کلاسهای گوناگونی قابل استفاده باشد، به مدرس امکان می‌دهد مبحثها را طبق ذوق و نظر خود انتخاب کند و به دانشجو نیز امکان مطالعهٔ بیشتر در نظریهٔ اعداد را می‌دهد. تجربه نشان می‌دهد که یک درس متعارف را می‌توان با استفاده از فصلهای ۱ تا ۹ تنظیم کرد؛ چنانچه موقعیت اقتضا کند، بی‌آنکه خللی در پیوستگی مطالب پدید آید، می‌توان بخشهای ۶ـ۲، ۶ـ۳، ۷ـ۴، ۸ـ۴، و ۹ـ۴ را از برنامه حذف کرد. چون چهار فصل آخر کاملاً مستقل از یکدیگرند، می‌توان به دلخواه از آنها استفاده کرد.

این چاپِ تجدید نظر شده در واکنش به اظهار نظرهای بسیاری از استفاده‌کنندگان کتاب فراهم آمده است. تنها تغییر عمدهٔ افزوده شدن مبحث کسرهای مسلسل نامتناهی و معادلهٔ پِل در فصل ۱۳ است. تمرینهایی به بخشهای متعددی از کتاب اضافه شده و تغییرهای جزئی بسیاری هم داده شده است.

مایلیم با اغتنام فرصت از همهٔ ریاضیدانهایی که دستنوشتهٔ این کتاب و صورتهای اصلاح شدهٔ گوناگون آن را مطالعه کردند و پیشنهادهای ذی‌قیمتی ارائه کردند که به بهتر شدن کتاب انجامید، عمیقاً قدردانی کنیم[3]. البته، نویسنده مسؤولیت هرگونه لغزش و کاستی را می‌پذیرد.

دیوید ام. برتن

دارم، نیوهمپشایر، ژانویهٔ ۱۹۸۰

---

1. *Introduction to Modern Algebra* by Neal McCoy.

2. *Introduction to Modern Abstract Algebra* by David M. Burton.

۳. نویسنده در اینجا نام دوازده ریاضیدان را که نظراتشان در اصلاح کتاب مؤثر بوده همراه با نام دانشگاههایشان آورده است که آوردن آنها در ترجمه ضروری تشخیص داده نشد ـ م.

۱

برخی ملاحظات مقدماتی

«عدد در خرافات متولد شد و در راز و رمز پرورش یافت ... اعداد زمانی مبنای دین و فلسفه واقع شدند، و ترفندهای عددی تأثیر فوق‌العاده‌ای بر افراد زود باور داشته است.»

اف. دبلیو. پارکر

۱ـ۱ استقرای ریاضی

نظریهٔ اعداد، حداقل در سطوح ابتداییش، به ویژگیهای عددهای صحیح و به طور اخص به عددهای صحیح مثبت ۱، ۲، ۳، ... (که به اعداد طبیعی نیز معروف‌اند) می‌پردازد. پیشینهٔ این نامگذاری نامناسب به یونانیان اولیه می‌رسد که در قاموس آنها واژهٔ «عدد» فقط به عدد صحیح مثبت اطلاق می‌شد. سابقهٔ آشنایی ما با عددهای طبیعی به اندازه‌ای طولانی است که زمانی کرونکر ریاضیدان معروف اظهار داشت: «خداوند عددهای طبیعی را آفرید، مابقی کار انسان است.» ولی نظریهٔ اعداد نه تنها عطیه‌ای الهی نیست، بلکه سیر رشد طولانی و گاه مرارت باری داشته است، ماجرایی که در صفحات بعدی به آن خواهیم پرداخت.

ما هیچ‌گونه کوششی برای ساختن عددهای صحیح به روش اصل موضوعی نخواهیم کرد، بلکه فرض می‌کنیم که آنها از پیش داده شده‌اند و خوانندهٔ این کتاب با بسیاری از احکام مقدماتی دربارهٔ آنها آشناست. اصل خوشترتیبی را یکی از اینها به حساب می‌آوریم. برای یادآوری، اصل مزبور را بازگو می‌کنیم:

اصل خوشترتیبی هر مجموعهٔ ناتهی S از اعداد صحیح نامنفی دارای کوچکترین عضو است؛ یعنی عدد صحیح aای در S هست که، به‌ازای هر bی متعلق به S، $a \leq b$.

چون این اصل نقش خیلی مهمی در اثباتهای این فصل و فصلهای آینده دارد، در اینجا با استفاده از آن نشان می‌دهیم که مجموعهٔ عددهای صحیح مثبت دارای ویژگی معروف به ویژگی ارشمیدسی است.

قضیهٔ ۱ـ۱ (ویژگی ارشمیدسی). اگر a و b عددهای صحیح مثبت دلخواهی باشند، آنگاه عدد صحیح مثبت nای موجود است به طوری که $na \geq b$.

اثبات. فرض کنید حکم قضیه درست نباشد، یعنی به‌ازای a و b ای و به‌ازای هر عدد صحیح مثبت n، $na < b$. در این صورت مجموعهٔ

$$S = \{b - na | \text{یک عدد صحیح مثبت } n\}$$

فقط متشکل از عددهای صحیح مثبت است. بنا به اصل خوشترتیبی، S دارای کوچکترین عضوی چون $b - ma$ است. توجه کنید که $b - (m + ۱)a$ نیز در S واقع است، زیرا S حاوی همهٔ این‌گونه عددهای صحیح است. به علاوه، داریم

$$b - (m + ۱)a = (b - ma) - a < b - ma$$

که متناقض با انتخاب $b - ma$ به‌عنوان کوچکترین عدد صحیح متعلق به S است. این تناقض ناشی از فرض اولیهٔ ما مبنی بر عدم برقراری ویژگی ارشمیدسی است، پس ثابت شد که این ویژگی برقرار است. □

با استفاده از اصل خوشترتیبی، به آسانی می‌توان اصل استقرای متناهی را نتیجه گرفت. اصل اخیر مبنایی برای روش اثباتی موسوم به «استقرای ریاضی» فراهم می‌کند. اصل استقرای متناهی، به بیان مسامحه‌آمیز حاکی از آن است که اگر مجموعه‌ای از عددهای صحیح مثبت دارای دو ویژگی خاص باشد، آنگاه با مجموعهٔ همهٔ عددهای صحیح مثبت برابر است. به بیانی روشنتر:

قضیهٔ ۱ـ۲ (اصل استقرای متناهی). فرض کنید S مجموعه‌ای از عددهای صحیح مثبت با ویژگیهای زیر باشد

(i) ۱ متعلق به S است، و

(ii) هرگاه عدد صحیح k در S باشد، آنگاه عدد صحیح بعدی یعنی $k+1$ نیز باید در S باشد.

در این صورت S مجموعهٔ همهٔ عددهای صحیح مثبت است.

اثبات. فرض کنید T مجموعهٔ همهٔ عددهای صحیح مثبت غیر متعلق به S است، و نیز فرض کنید T ناتهی است. بنا به اصل خوشترتیبی، T دارای کوچکترین عضو است، که آن را با a نشان می‌دهیم. چون ۱ در S است، قطعاً $a > 1$، و بنابراین $0 < a - 1 < a$. چون a کوچکترین عدد صحیح مثبت موجود در T است، $a-1$ عضو T نیست؛ به عبارت دیگر، $a-1$ متعلق به S است. بنا به فرض، S باید شامل عنصر $a = 1 + (a-1)$ نیز باشد، که متناقض با عضویت a در T است. نتیجه می‌گیریم که مجموعهٔ T تهی است، و در نتیجه S شامل همهٔ عددهای صحیح مثبت است. □

فرمول زیر نمونه‌ای از فرمولهایی است که می‌توان با استقرای ریاضی ثابت کرد:

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(2n+1)(n+1)}{6} \qquad (1)$$

به‌ازای $n = 1, 2, 3, \ldots$. به‌امید آنکه بتوانیم قضیهٔ ۱ـ۲ را در این مورد به کار ببریم فرض می‌کنیم S مجموعهٔ عددهای صحیح مثبت n ای باشد که به‌ازای آنها (۱) برقرار است. ملاحظه می‌کنیم که اگر $n = 1$، فرمول به صورت

$$1^2 = \frac{1(2+1)(1+1)}{6} = 1$$

در می‌آید؛ یعنی، ۱ در S است. حال فرض کنید k متعلق به S باشد (k یک عدد صحیح مثبت ثابت ولی نامشخص است). یعنی

$$1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(2k+1)(k+1)}{6} \qquad (2)$$

برای تعیین مجموع $k+1$ جملهٔ نخست، جملهٔ بعدی، یعنی $(k+1)^2$ را، به طرفین (۲) اضافه می‌کنیم. در این صورت

$$1^2 + 2^2 + \ldots + k^2 + (k+1)^2 = \frac{k(2k+1)(k+1)}{6} + (k+1)^2$$

بعد از عملیاتی جبری، طرف راست به صورت زیر در می‌آید

$$\begin{aligned}(k+۱)\left[\frac{k(۲k+۱)+۶(k+۱)}{۶}\right] &= (k+۱)\left[\frac{۲k^{۲}+۷k+۶}{۶}\right]\\ &= \frac{(k+۱)(۲k+۳)(k+۲)}{۶}\end{aligned}$$

که دقیقاً همان طرف راست (۱) به‌ازای $n = k + ۱$ است. استدلال ما نشان می‌دهد که اگر S شامل عدد صحیح k باشد آنگاه S شامل عدد صحیح $k + ۱$ نیز هست. بنا به قضیهٔ ۱ـ۲ـ۱، S باید شامل همهٔ عددهای صحیح مثبت باشد؛ یعنی، فرمول داده شده به‌ازای $n = ۱, ۲, ۳, \ldots$ برقرار است.

گرچه استقرای ریاضی تکنیک متعارفی برای اثبات احکامی دربارهٔ عددهای صحیح مثبت است، برای صورتبندی این نوع حکمها کارساز نیست. البته اگر بتوانیم در مورد ویژگیی که معتقدیم در حالت کلی برقرار است، «حدسی پخته» بزنیم، آنگاه اغلب می‌توانیم درستی آن را به کمک اصل استقرا بررسی کنیم. به عنوان مثال، برابریهای

$$\begin{aligned}&۱ = ۱\\ &۱ + ۲ = ۳\\ &۱ + ۲ + ۲^{۲} = ۷\\ &۱ + ۲ + ۲^{۲} + ۲^{۳} = ۱۵\\ &۱ + ۲ + ۲^{۲} + ۲^{۳} + ۲^{۴} = ۳۱\\ &۱ + ۲ + ۲^{۲} + ۲^{۳} + ۲^{۴} + ۲^{۵} = ۶۳\end{aligned}$$

را در نظر بگیرید. هدف تعیین قاعده‌ای است که عددهای صحیح طرف راست را نتیجه بدهد. خواننده با اندکی تأمل متوجه خواهد شد که

$$\begin{array}{lll} ۱ = ۲ - ۱, & ۳ = ۲^{۲} - ۱, & ۷ = ۲^{۳} - ۱\\ ۱۵ = ۲^{۴} - ۱, & ۳۱ = ۲^{۵} - ۱, & ۶۳ = ۲^{۶} - ۱\end{array}$$

(توضیح اینکه چگونه می‌توان به این نکته دست یافت، دشوار است، ولی تجربه در این‌گونه موارد مفید واقع می‌شود). الگویی که از این حالتهای معدود به‌دست می‌آید، الهامبخش فرمولی برای

تعیین مقدار عبارت $۱ + ۲ + ۲^۲ + ۲^۳ + \ldots + ۲^{n-۱}$ است؛ یعنی، به‌ازای هر عدد صحیح مثبت n،

$$۱ + ۲ + ۲^۲ + ۲^۳ + \ldots + ۲^{n-۱} = ۲^n - ۱ \qquad (۳)$$

برای اثبات درستی حدسمان، فرض می‌کنیم S مجموعهٔ عددهای صحیح مثبت nای باشد که به‌ازای آنها فرمول (۳) برقرار است. به‌ازای $n = ۱$، (۳) قطعاً برقرار است، پس ۱ متعلق به S است. فرض می‌کنیم (۳) به‌ازای عدد صحیح مثبت kای برقرار باشد. یعنی، به‌ازای این k،

$$۱ + ۲ + ۲^۲ + \ldots + ۲^{k-۱} = ۲^k - ۱$$

و کوشش می‌کنیم درستی فرمول را به‌ازای $k + ۱$ ثابت کنیم. افزودن جملهٔ ۲^k به‌طرفین آخرین رابطهٔ نوشته شده نتیجه می‌دهد

$$\begin{aligned} ۱ + ۲ + ۲^۲ + \ldots + ۲^{k-۱} + ۲^k &= ۲^k - ۱ + ۲^k \\ &= ۲ \times ۲^k - ۱ = ۲^{k+۱} - ۱ \end{aligned}$$

یعنی، فرمول (۳) به‌ازای $n = k + ۱$ برقرار است، و بنابراین $k + ۱$ متعلق به S است؛ یعنی، اگر k در S باشد، $k + ۱$ نیز در S است. پس، بنا به اصل استقرا، S باید مجموعهٔ همهٔ عددهای صحیح مثبت باشد.

تذکر: معمولاً به هنگام استفاده از اثبات استقرایی، برای کوتاه کردن استدلال از مجموعهٔ S نام نمی‌بریم. فقط نشان می‌دهیم که حکم مورد نظر به‌ازای $n = ۱$ درست است، و اگر به‌ازای عدد صحیح k درست باشد، به‌ازای $k + ۱$ نیز درست است.

در اینجا باید هشدار بدهیم که به‌هنگام استفاده از قضیهٔ ۱ـ۲، باید پیش از هرگونه نتیجه‌گیری هر دو شرط آن را ثابت کرد؛ و هیچ کدام به تنهایی کافی نیست. معمولاً اثبات شرط (i) پایهٔ استقرا و اثبات (ii) مرحلهٔ استقرا نامیده می‌شود. فرضهای اتخاذ شده در مرحلهٔ استقرا به فرضهای استقرا معروف‌اند. وضعیت استقرا به ردیفی نامتناهی از مهره‌های دومینو تشبیه شده است که همگی به‌حالت ایستاده بر خطی راست طوری قرار گرفته‌اند که اگر یکی بیفتد، بعدی را نیز می‌اندازد. اگر مهره‌ای هل داده نشود (یعنی، پایهٔ استقرایی در کار نباشد) یا اگر فضای میان دو مهرهٔ متوالی خیلی زیاد باشد (یعنی، مرحلهٔ استقرا برقرار نباشد)، آنگاه همهٔ مهره‌ها نخواهند افتاد.

برقراری مرحلهٔ استقرا لزوماً به درستی عبارتی که می‌خواهیم ثابت کنیم بستگی ندارد. به عنوان مثال، به فرمول نادرست زیر توجه کنید

$$۱ + ۳ + ۵ + \ldots + (۲n - ۱) = n^۲ + ۳ \qquad (۴)$$

فرض کنید که این فرمول به‌ازای $n = k$ برقرار باشد؛ به دیگر سخن،

$$۱ + ۳ + ۵ + \ldots + (۲k - ۱) = k^۲ + ۳$$

در این صورت

$$\begin{aligned} ۱ + ۳ + ۵ + \ldots + (۲k - ۱) + (۲k + ۱) &= k^۲ + ۳ + ۲k + ۱ \\ &= (k + ۱)^۲ + ۳ \end{aligned}$$

که دقیقاً همان سمت راست (۴) به‌ازای $n = k + ۱$ است. پس، اگر فرمول (۴) به‌ازای عدد صحیح داده شده‌ای برقرار باشد، به‌ازای عدد صحیح بعدی نیز برقرارست. ولی، ممکن نیست مقداری برای n پیدا کرد که به‌ازای آن فرمول (۴) برقرار باشد.

صورت دیگری از اصل استقرا وجود دارد که اغلب در مواردی به کار می‌رود که قضیهٔ ۱ـ۲ به خودی خود کارساز به نظر نمی‌رسد. مانند صورت اول، این «دومین اصل استقرای متناهی» نیز دارای دو شرط است که تضمین می‌کنند مجموعهٔ خاصی از عددهای صحیح مثبت در واقع شامل همهٔ عددهای صحیح مثبت است. در این اصل، شرط (i) را حفظ می‌کنیم، ولی به جای شرط (ii)، شرط زیر را می‌گذاریم

(ii′) اگر به‌ازای عدد صحیح مثبت kای همهٔ عددهای ۱، ۲، . . .، k متعلق به S باشند، آنگاه $k + ۱$ نیز باید در S باشد.

اثبات اینکه S شامل همهٔ عددهای صحیح مثبت است به همان شیوهٔ اثبات قضیهٔ ۱ـ۲ صورت می‌گیرد. باز، فرض کنید T مجموعهٔ عددهای صحیح مثبتِ غیر واقع در S است. به فرض ناتهی بودن T، کوچکترین عضو T را n می‌نامیم. در این صورت، بنا به فرض (i)، $n > ۱$. به دلیل کوچکترین بودن n، هیچ یک از عددهای صحیح ۱، ۲، . . .، $n - ۱$ در T نیست، یا اگر بخواهیم این موضوع را به صورت ایجابی بیان کنیم، می‌توان گفت که ۱، ۲، . . .، $n - ۱$ همگی به S تعلق دارند. پس، بنا به ویژگی (ii′)، $n = (n - ۱) + ۱$ در S است، که تناقضی بدیهی است. نتیجه می‌شود که T تهی است.

گرچه «نخستین اصل استقرای متناهی» بیش از دومین اصل به کار می‌رود، مواردی وجود دارند که در آنها دومین اصل کارسازتر است، و خواننده باید با هر دو صورت آشنا باشد. (گاهی برای نشان دادن عضویت $k+۱$ در S، نه تنها به عضویت k در S، بلکه به عضویت همهٔ عددهای صحیح مثبت کوچکتر از k در S احتیاج است.) اصلهای استقرا تا اینجا برای حالتی بیان شده‌اند که استقرا با ۱ آغاز شود. هر یک از اصلهای مزبور را می‌توان طوری تعمیم داد که استقرا از هر عدد صحیح مثبت $n_۰$ای آغاز گردد. در چنین حالتی، حکم به این شکل در می‌آید: « در این صورت S مجموعهٔ همهٔ عددهای صحیح مثبت n، $n \geq n_۰$، است.»

استقرای ریاضی علاوه بر اینکه روشی برای اثبات است، بسیاری اوقات به عنوان روشی برای تعریف نیز به کار می‌رود. مثلاً، روش معمول برای معرفی نماد $n!$ (بخوانید «n فاکتوریل») استفاده از تعریفی استقرایی به شرح زیر است:

(الف) $۱! = ۱$

(ب) اگر $n > ۱$، آنگاه $n! = n \cdot (n-۱)!$

این دو شرط قاعده‌ای معین می‌کنند که به وسیلهٔ آن معنی $n!$ به‌ازای هر عدد صحیح مثبت n مشخص می‌شود. بنابراین، بنا به (الف)، $۱ = !۱$، و بنا به (ب)

$$۲! = ۲ \times ۱! = ۲ \times ۱$$

و باز بنا به (ب)

$$۳! = ۳ \times ۲! = ۳ \times ۲ \times ۱$$

با ادامهٔ این روش، و با استفادهٔ مکرر از شرط (ب)، عددهای $!۱$، $!۲$، $!۳$، ...، $n!$ به طور متوالی تا هر n انتخابی تعریف می‌شوند. در واقع،

$$n! = n \times (n-۱) \dots ۳ \times ۲ \times ۱$$

با استفاده از استقرا می‌توان نشان داد که $n!$، به عنوان تابعی از عددهای صحیح مثبت، موجود و یکتاست؛ ولی این نکته را در این کتاب ثابت نخواهیم کرد.

مناسب است تعریف $n!$ را، با قرارداد $۱ = !۰$، در مورد $n = ۰$ تعمیم دهیم.

مثال ۱ـ۱

برای ارائهٔ اثباتی که نیازمند دومین اصل استقرای متناهی باشد، دنبالهٔ معروف به دنبالهٔ لوکاس

$$۱, ۳, ۴, ۷, ۱۱, ۱۸, ۲۹, ۴۷, ۷۶, \ldots$$

را در نظر می‌گیریم. به استثنای دو جملهٔ نخست، هر جملهٔ دیگر این دنباله مجموع دو جملهٔ قبلی است، بنابراین دنباله را می‌توان به طور استقرایی به صورت

$$\begin{aligned} a_۱ &= ۱ \\ a_۲ &= ۳ \\ a_n &= a_{n-۱} + a_{n-۲} \qquad \text{به‌ازای هر } n \geq ۳ \end{aligned}$$

تعریف کرد. ادعا می‌کنیم که به‌ازای هر عدد صحیح مثبت n، نابرابری

$$a_n < \left(\frac{۷}{۴}\right)^n$$

برقرار است. استدلالی که به کار می‌رود، جالب است زیرا در مرحلهٔ استقرا، برای اثبات برقراری این نابرابری به‌ازای یک مقدار n، لازم است برقراری نابرابری مزبور به‌ازای دو مقدار بلافاصله قبل از آن معلوم باشد.

پیش از همه، به ازای $n = ۱$ و $n = ۲$ داریم

$$a_۲ = ۳ < \left(\frac{۷}{۴}\right)^۲ = \frac{۴۹}{۱۶} \quad \text{و} \quad a_۱ = ۱ < \left(\frac{۷}{۴}\right)^۱ = \frac{۷}{۴}$$

و بنابراین نابرابری مورد بحث در این دو حالت برقرار است. این امر پایه‌ای برای استقرا فراهم می‌کند. در مورد مرحلهٔ استقرا، عدد صحیح kای، $k \geq ۳$، اختیار می‌کنیم و فرض می‌کنیم که نابرابری به‌ازای $n = ۱, ۲, \ldots, k-۱$ برقرار است. پس

$$a_{k-۲} < \left(\frac{۷}{۴}\right)^{k-۲} \quad \text{و} \quad a_{k-۱} < \left(\frac{۷}{۴}\right)^{k-۱}$$

با توجه به نحوهٔ تعریف دنبالهٔ لوکاس، نتیجه می‌گیریم

$$\begin{aligned} a_k = a_{k-۱} + a_{k-۲} &< \left(\frac{۷}{۴}\right)^{k-۱} + \left(\frac{۷}{۴}\right)^{k-۲} \\ &= \left(\frac{۷}{۴}\right)^{k-۲}\left(\frac{۷}{۴}+۱\right) \\ &= \left(\frac{۷}{۴}\right)^{k-۲}\left(\frac{۱۱}{۴}\right) \\ &< \left(\frac{۷}{۴}\right)^{k-۲}\left(\frac{۷}{۴}\right)^{۲} = \left(\frac{۷}{۴}\right)^{k} \end{aligned}$$

چون نابرابری به‌ازای $n = k$، به فرض برقراریش به‌ازای عددهای صحیح ۱، ۲، ...، $k - ۱$ برقرار است، بنا به دومین اصل استقرا نتیجه می‌گیریم که، به‌ازای هر $n \geq ۱$، $a_n < \left(\frac{۷}{۴}\right)^n$. ■

این مثال، صرف نظر از نکات دیگر، نشان می‌دهد که اگر اشیایی به‌طور استقرایی تعریف شوند، استقرای ریاضی وسیلهٔ کارآمدی برای اثبات ویژگیهای آنهاست.

تمرینهای ۱ـ۱

۱. فرمولهای زیر را با استفاده از استقرای ریاضی ثابت کنید

(الف) به‌ازای هر $n \geq ۱$، $$۱ + ۲ + ۳ + \ldots + n = \frac{n(n+۱)}{۲}$$

(ب) به‌ازای هر $n \geq ۱$، $$۱ + ۳ + ۵ + \ldots + (۲n - ۱) = n^۲$$

(پ) به‌ازای هر $n \geq ۱$، $$۱\times۲ + ۲\times۳ + ۳\times۴ + \ldots + n(n+۱) = \frac{n(n+۱)(n+۲)}{۳}$$

(ت) به‌ازای هر $n \geq ۱$، $$۱^۲ + ۳^۲ + ۵^۲ + \ldots + (۲n-۱)^۲ = \frac{n(۴n^۲ - ۱)}{۳}$$

(ث) به‌ازای هر $n \geq ۱$، $$۱^۳ + ۲^۳ + ۳^۳ + \ldots + n^۳ = \left[\frac{n(n+۱)}{۲}\right]^۲$$

۲. اگر $r \neq ۱$، نشان دهید که به‌ازای هر عدد صحیح مثبت n داریم

$$a + ar + ar^۲ + \ldots + ar^n = \frac{a(r^{n+۱} - ۱)}{r - ۱}$$

۳. با استفاده از دومین اصل استقرای متناهی ثابت کنید که به‌ازای هر $n \geq ۱$

$$a^n - ۱ = (a - ۱)(a^{n-۱} + a^{n-۲} + a^{n-۳} + \ldots + a + ۱)$$

[راهنمایی: $a^{n+۱} - ۱ = (a + ۱)(a^n - ۱) - a(a^{n-۱} - ۱)$.]

۴. ثابت کنید که مکعب هر عدد صحیح را می‌توان به صورت تفاضل دو مربع نوشت. [راهنمایی: توجه کنید که برابری

$$n^۳ = (۱^۳ + ۲^۳ + \ldots + n^۳) - (۱^۳ + ۲^۳ + \ldots + (n - ۱)^۳)$$

برقرار است.]

۵. (الف) مقدارهایی از $n \le ۷$ را پیدا کنید که به‌ازای آنها $n! + ۱$ مربع کامل باشد (معلوم نیست که به‌ازای nای، $n > ۷$، $n! + ۱$ مربع کامل باشد).

(ب) رابطه‌های زیر درست‌اند یا نادرست؟ به‌ازای عددهای صحیح مثبت m و n، $(mn)! = m!n!$ و $(m + n)! = m! + n!$.

۶. ثابت کنید که به‌ازای هر عدد صحیح $n \ge ۴$، $n! > n^۲$، ولی به‌ازای هر عدد صحیح $n \ge ۶$، $n! > n^۳$.

۷. با استفاده از استقرای ریاضی ثابت کنید که به‌ازای هر $n \ge ۱$

$$۱(۱!) + ۲(۲!) + ۳(۳!) + \ldots + n(n!) = (n + ۱)! - ۱$$

۸. (الف) ثابت کنید که به‌ازای هر $n \ge ۱$ داریم

$$۲ \times ۶ \times ۱۰ \times ۱۴ \times \ldots \times (۴n - ۲) = \frac{(۲n)!}{n!}$$

(ب) بااستفاده از قسمت (الف)، نابرابری $۲^n(n!)^۲ \le (۲n)!$ را به‌ازای هر $n \ge ۱$ ثابت کنید.

۹. نابرابری برنولی را ثابت کنید: اگر $۱ + a > ۰$، آنگاه به‌ازای هر $n \ge ۱$

$$(۱ + a)^n \ge ۱ + na$$

۱۰. با استقرای ریاضی ثابت کنید که به‌ازای هر $n \ge ۱$

$$\frac{۱}{۱^۲} + \frac{۱}{۲^۲} + \frac{۱}{۳^۲} + \ldots + \frac{۱}{n^۲} \le ۲ - \frac{۱}{n}$$

۱ـ۲ قضیهٔ دو جمله‌ای

ضریبهای دو جمله‌ای $\binom{n}{k}$ ارتباط نزدیکی با نماد فاکتوریل دارند. به‌ازای هر عدد صحیح مثبت n و هر عدد صحیح kای که در $۰ \le k \le n$ صدق کند، این ضریبها چنین تعریف می‌شوند:

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

با حذف $k!$ یا $(n-k)!$، $\binom{n}{k}$ را می‌توان به صورت

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

نوشت. به عنوان مثال، به‌ازای $n = ۸$ و $k = ۳$ داریم

$$\binom{۸}{۳} = \frac{۸!}{۳!۵!} = \frac{۸ \times ۷ \times ۶ \times ۵ \times ۴}{۵!} = \frac{۸ \times ۷ \times ۶}{۳!} = ۵۶$$

همچنین توجه کنید که اگر $k = ۰$ یا $k = n$، کمیت $۰!$ در طرف راست تعریف $\binom{n}{k}$ ظاهر می‌شود؛ چون $۰!$ را برابر ۱ تعریف کرده‌ایم، به‌ازای این مقدارهای خاص k داریم

$$\binom{n}{۰} = \binom{n}{n} = ۱$$

اتحادهای سودمند متعددی در ارتباط با ضریبهای دو جمله‌ای موجودند. یکی از اتحادهای مورد نیاز ما در این کتاب قاعدهٔ پاسکال است:

$$\binom{n}{k} + \binom{n}{k-۱} = \binom{n+۱}{k}, \qquad ۱ \leq k \leq n$$

برای اثبات این اتحاد، اتحاد

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

را در $\frac{n!}{(k-۱)!(n-k)!}$ ضرب می‌کنیم. داریم

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

با توجه به تعریف تابع فاکتوریل، این برابری به این معنی است که

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

که از آن قاعدهٔ پاسکال نتیجه می‌شود.

این رابطه منجر به آرایشی از اعداد، معروف به مثلث پاسکال می‌شود که در آن ضریب دوجمله‌ای $\binom{n}{k}$ به صورت $(k+۱)$امین عدد سطر nام ظاهر می‌شود:

$$\begin{array}{ccccccccccccc}
 & & & & & ۱ & & ۱ & & & & & \\
 & & & & ۱ & & ۲ & & ۱ & & & & \\
 & & & ۱ & & ۳ & & ۳ & & ۱ & & & \\
 & & ۱ & & ۴ & & ۶ & & ۴ & & ۱ & & \\
 & ۱ & & ۵ & & ۱۰ & & ۱۰ & & ۵ & & ۱ & \\
۱ & & ۶ & & ۱۵ & & ۲۰ & & ۱۵ & & ۶ & & ۱ \\
 & & & & & & \cdots & & & & & &
\end{array}$$

قاعدهٔ تنظیم این آرایش روشن است. مرزهای مثلث از ۱ ها تشکیل شده است؛ هر عدد غیر واقع بر مرز، مجموع دو عدد از ردیف قبلی است که به آن نزدیکترند.

در واقع، قضیهٔ دوجمله‌ای فرمولی برای بسط کامل $(a+b)^n$، $n \geq ۱$، به صورت مجموعی از توانهای a و b است. این عبارت در همهٔ سطوح نظریهٔ اعداد به کرات ظاهر می‌شود و بنابراین، می‌ارزد که بیشتر به آن بپردازیم. به‌آسانی می‌توان با ضرب مستقیم ملاحظه کرد که

$$\begin{aligned}
(a+b)^{۱} &= a+b\\
(a+b)^{۲} &= a^{۲}+۲ab+b^{۲}\\
(a+b)^{۳} &= a^{۳}+۳a^{۲}b+۳ab^{۲}+b^{۳}\\
(a+b)^{۴} &= a^{۴}+۴a^{۳}b+۶a^{۲}b^{۲}+۴ab^{۳}+b^{۴}
\end{aligned}$$

و به همین ترتیب. سؤال این است که چگونه می‌توان ضریبها را پیش‌بینی کرد. به طوری که ملاحظه می‌شود، ضریبهای این چند بسط نخست، ردیفهایی متوالی از مثلث پاسکال را تشکیل می‌دهند. از اینجا می‌توان حدس زد که بسط کلی دو جمله‌ای باید به صورت

$$\begin{aligned}
(a+b)^n = \binom{n}{۰}a^n + \binom{n}{۱}a^{n-۱}b + \binom{n}{۲}a^{n-۲}b^{۲}&\\
+\cdots+\binom{n}{n-۱}ab^{n-۱}+\binom{n}{n}a^n&
\end{aligned}$$

و یا به اختصار،

$$(a+b)^n = \sum_{k=۰}^{n}\binom{n}{k}a^{n-k}b^k$$

باشد.

استقرای ریاضی بهترین وسیله برای اثبات این ادعاست. به‌ازای $n = 1$، فرمول حدس زده‌شده به صورت

$$(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b$$

در می‌آید که قطعاً درست است. با فرض اینکه فرمول به‌ازای عدد صحیح ثابت mای برقرار باشد، نشان می‌دهیم که به‌ازای $m+1$ نیز باید برقرار باشد. در شروع کار توجه می‌کنیم که

$$(a+b)^{m+1} = a(a+b)^m + b(a+b)^m$$

تحت فرض استقرا داریم

$$a(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k = a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k$$

و

$$\begin{aligned} b(a+b)^m &= \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^{j+1} \\ &= \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1} \end{aligned}$$

با جمع کردن این عبارتها، به‌دست می‌آوریم

$$\begin{aligned} (a+b)^{m+1} &= a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1} \right] a^{m+1-k} b^k + b^{m+1} \\ &= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k \end{aligned}$$

که فرمول مورد بحث به‌ازای $n = m + 1$ است. به این ترتیب، قضیهٔ دوجمله‌ای به استقرا ثابت می‌شود.

پیش از آنکه بحث دربارهٔ این مفهومها را پایان دهیم، خاطر نشان می‌کنیم که نخستین صورت قابل قبول روش استقرای ریاضی در رساله در باب مثلث حسابی[1]، به قلم بلز پاسکال[2]، ریاضیدان و فیلسوف قرن هفدهم فرانسه دیده می‌شود. این اثر کوتاه در سال ۱۶۵۳ نوشته شد ولی تا سال ۱۶۶۵ چاپ نشد زیرا پاسکال از ریاضیات (در سن ۲۵ سالگی) کناره‌گیری کرد تا استعدادش را وقف تبلیغ مذهب کند. بررسی دقیق او از ویژگیهای ضریبهای دو جمله‌ای به پایه‌گذاری نظریهٔ احتمال کمک کرد.

---

1. Traité du Triangle Arithmetiqué   2. Blaise Pascal

تمرینهای ۱ـ۲

۱. ثابت کنید که به‌ازای $n \geq ۱$

(الف) $$\binom{۲n}{n} = \frac{۱ \times ۳ \times ۵ \times \ldots \times (۲n - ۱)}{n!} ۲^n$$

(ب) $$\binom{۴n}{۲n} = \frac{۱ \times ۳ \times ۵ \times \ldots \times (۴n - ۱)}{[۱ \times ۳ \times ۵ \times \ldots \times (۲n - ۱)]^۲} \binom{۲n}{n}$$

۲. اگر $۲ \leq k \leq n - ۲$، و $n \geq ۴$، نشان دهید که

$$\binom{n}{k} = \binom{n-۲}{k-۲} + ۲\binom{n-۱۱}{k-۱} + \binom{n-۲}{k}$$

۳. درستی هر یک از اتحادهای زیر را به‌ازای $n \geq ۱$ ثابت کنید

(الف) $$\binom{n}{۰} + \binom{n}{۱} + \binom{n}{۲} + \ldots + \binom{n}{n} = ۲^n$$

[راهنمایی: در قضیهٔ دو جمله‌ای قرار دهید $a = b = ۱$.]

(ب) $$\binom{n}{۰} - \binom{n}{۱} + \binom{n}{۲} + \ldots + (-۱)^n \binom{n}{n} = ۰$$

(پ) $$\binom{n}{۱} + ۲\binom{n}{۲} + ۳\binom{n}{۳} + \ldots + n\binom{n}{n} = n۲^{n-۱}$$

[راهنمایی: بعد از بسط دادن $n(۱ + b)^{n-۱}$ با استفاده از قضیهٔ دو جمله‌ای، قرار دهید $b = ۱$؛ همچنین توجه کنید که $n\binom{n-۱}{k} = (k+۱)\binom{n}{k+۱}$.]

(ت) $$\binom{n}{۰} + ۲\binom{n}{۱} + ۲^۲\binom{n}{۲} + \ldots + ۲^n\binom{n}{n} = ۳^n$$

(ث) $$\binom{n}{۰} + \binom{n}{۲} + \binom{n}{۴} + \binom{n}{۶} + \ldots = \binom{n}{۱} + \binom{n}{۳} + \binom{n}{۵} + \ldots = ۲^{n-۱}$$

[راهنمایی: از قسمتهای (الف) و (ب) استفاده کنید.]

(ج) $$\binom{n}{۰} - \frac{۱}{۲}\binom{n}{۱} + \frac{۱}{۳}\binom{n}{۲} - \ldots + \frac{(-۱)^n}{n+۱}\binom{n}{n} = \frac{۱}{n+۱}$$

[راهنمایی: طرف چپ برابر با

$$\frac{1}{n+1}\left[\binom{n+1}{1}-\binom{n+1}{2}+\binom{n+1}{3}-\ldots+(-1)^n\binom{n+1}{n+1}\right]$$

است.]

۴. ثابت کنید که به‌ازای $n \geq 1$

(الف) $\binom{n}{r}<\binom{n}{r+1}$ اگر و تنها اگر $0 \leq r < \frac{1}{2}(n-1)$.

(ب) $\binom{n}{r}>\binom{n}{r+1}$ اگر و تنها اگر $n-1 \geq r > \frac{1}{2}(n-1)$.

(پ) $\binom{n}{r}=\binom{n}{r+1}$ اگر و تنها اگر n عدد صحیح فردی باشد، و $r=\frac{1}{2}(n-1)$.

۵. نشان دهید که به‌ازای $n \geq 1$ هر دو عبارت $\frac{(2n)!}{n!(n+1)!}$ و $\frac{(3n)!}{6^n n!}$ عددهایی صحیح‌اند.

۶. (الف) ثابت کنید که، به‌ازای $n \geq 2$

$$\binom{2}{2}+\binom{3}{2}+\binom{4}{2}+\ldots+\binom{n}{2}=\binom{n+1}{3}$$

[راهنمایی: از استقرا و قاعدهٔ پاسکال استفاده کنید.]

(ب) از قسمت (الف) و اینکه به‌ازای $m \geq 2$، $\binom{m}{2}+\binom{m+1}{2}=m^2$، نتیجه بگیرید

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$$

۷. نشان دهید که به‌ازای $n > 1$

$$1^2+3^2+5^2+\ldots+(2n-1)^2=\binom{2n+1}{3}$$

۸. نابرابری $2^{2n} > \binom{2n}{n} > 2^n$ را به‌ازای $n > 1$ ثابت کنید. [راهنمایی: قرار دهید $x = 2\times4\times6\times\ldots\times(2n)$، $y = 1\times3\times5\times\ldots\times(2n-1)$، $z = 1\times2\times3\times\ldots\times n$، و نشان دهید $x > y > z$، و از آنجا $x^2 > xy > xz$.]

۱ـ۳ نظریهٔ اعداد در آغاز

پیش از اینکه در جزئیات موضوع غرق شویم، لازم است چند کلمه‌ای دربارهٔ منشأ نظریهٔ اعداد توضیح دهیم. نظریهٔ اعداد یکی از قدیمیترین شاخه‌های ریاضیات است؛ هر فرد علاقه‌مندی، با کاوش و جستجو، می‌تواند دریابد که ریشه‌های این نظریه به روزگار فوق‌العاده دوری باز می‌گردد.

هر چند محتمل به‌نظر می‌رسد که یونانیان برخی از مهمترین اطلاعات خود را دربارهٔ ویژگیهای اعداد طبیعی از بابلیها و مصریهای باستان گرفته باشند، نخستین اصول و مبادی یک نظریهٔ واقعی دربارهٔ اعداد عموماً به فیثاغورس و شاگردان او نسبت داده می‌شود.

اطلاعات ما دربارهٔ زندگی فیثاغورس اندک است و خیلی کم می‌توان دربارهٔ او با قاطعیت سخن گفت. براساس دقیقترین برآوردها، او در فاصلهٔ ۵۸۰ و ۵۶۲ پیش از میلاد در جزیرهٔ ساموس[1] در دریای اژه متولد شده است. به نظر می‌رسد که نه تنها در مصر تحصیل کرده، بلکه به طرف شرق حتی تا بابل هم سفر کرده است. فیثاغورس وقتی بعد از سالها سیر و سفر، به وطن بازگشت، در پی مکان مناسبی برای تأسیس یک مکتب برآمد و بالاخره در کروتونا[2]، دهکدهٔ یونانی‌نشین مرفهی واقع در پاشنهٔ چکمهٔ ایتالیای فعلی ساکن شد. مکتب او در چهار زمینهٔ مطالعاتی فعالیت می‌کرد: حساب (به معنی نظریهٔ اعداد، نه فن محاسبه)، موسیقی، هندسه، و نجوم. این تقسیم‌بندی چهارگانهٔ دانش در قرون وسطا به چهارگان یا علوم چهارگانه معروف شد، که بعداً علوم سه‌گانهٔ منطق، دستور زبان، و معانی و بیان نیز به آن اضافه گردید. این دانشهای هفتگانه دروس لازمی به شمار می‌آمد که هر فرد تحصیلکرده می‌بایست آنها را گذرانده باشد.

فیثاغورس شاگردانش را به دوگروه تقسیم کرده بود: شاگردان آزمایشی و مشروط (یا مستمعین) و فیثاغورسیان. مبتدی پس از گذراندن سه سال در کلاس اول، ممکن بود به کلاس دوم راه یابد، و در آنجا اکتشافات مهم مکتب به طور محرمانه به او آموخته می‌شد. فیثاغورسیان فرقه‌ای با روابط برادرانه بودند، از همهٔ وسایل و نعمتهای مادی به اشتراک استفاده می‌کردند، و به قید سوگند متعهد بودند که اسرار بانی مکتب را بروز ندهند. براساس افسانه‌ای، فیثاغورسیِ پرحرفی که از روی خودستایی در انظار عمومی گفته بود دوازده وجهی را به اجسام منتظم کشف شده به وسیلهٔ فیثاغورس افزوده است، به کیفر الهی در سانحهٔ غرق کشتی از میان رفت. برای مدتی فیثاغورسیان مستبد توانستند حکومت محلی کروتونا را در دست بگیرند، ولی قیامی عمومی در ۵۰۱ پیش از میلاد منجر به کشته شدن بسیاری از عضوهای برجستهٔ این گروه شد، و خود فیثاغورس نیز اندکی بعد از آن کشته شد. هرچند نفوذ سیاسی فیثاغورسیان به این ترتیب از بین رفت، توانستند حداقل تا دو قرن دیگر به صورت انجمنی فلسفی و ریاضی به حیات خود ادامه دهند. بالاخره، به صورت یک جمعیت مخفی در آمدند، چیزی منتشر نمی‌کردند و، با تواضع فوق‌العاده‌ای، همهٔ کشفیات خود را به مراد خود نسبت می‌دادند.

فیثاغورسیان معتقد بودند که کلید اسرار جهان در عدد نهفته است و کلاً عقیده داشتند که «همه چیز عدد است». (البته، منظور آنها از عدد، عدد صحیح مثبت بود.) به نظر آنها، برای ادراک منطقی طبیعت، بررسی ویژگیهای اعداد خاصی کافی بود. در مورد خود فیثاغورس، گفته شده

1. Samos   2. Croton

است که او «ظاهراً اهمیت فوق‌العاده‌ای برای مطالعهٔ حساب، که خود آن را به پیش برد و از قلمرو مصارف بازرگانی خارج کرد، قائل بوده است.»

تعلیمات فیثاغورسی آمیزهٔ غریبی از فلسفهٔ کیهانی و رمزگرایی عددی بود، نظریه‌ای مبتنی بر اعتقاد افراطی به رمزآمیز بودن اعداد، که به هر چیز مادی یا معنوی عدد معینی نسبت می‌داد. از نوشته‌هایشان در می‌یابیم که ۱ را نمایندهٔ دلیل و برهان می‌دانستند، زیرا دلیل می‌تواند فقط یک مجموعه از حقایق سازگار تولید کند؛ ۲ به مرد و ۳ به زن نسبت داده شده بود؛ ۴ مظهر فیثاغورسی برای عدالت بود زیرا نخستین عددی است که حاصلضرب دو عددِ برابر است، ۵ با ازدواج یکی گرفته شده بود، زیرا از اجتماع ۲ و ۳ تشکیل شده است، و الی آخر. همهٔ عددهای زوج، بعد از ۲، قابل تجزیه به دو عدد زوج دیگرند، بنابراین، در نظر فیثاغورسیان بارآور و مؤنث و خاکی به حساب می‌آمدند ـ و به طور کلی در مرتبه‌ای پایینتر از عددهای فرد قرار داشتند. فیثاغورسیان، که بیشترشان مرد بودند، عددهای فرد بعد از ۳ را مذکر یا الهی به‌شمار می‌آوردند.

امروز چنین تصوراتی دربارهٔ اعداد یعنی در نظر گرفتن آنها به صورت الگوهای «چیزها» بی‌معنی به نظر می‌رسد، ولی باید در نظر داشت که روشنفکران یونان باستان تا اندازهٔ زیادی مجذوب فلسفه بودند و درست همین اشخاص بودند که به لحاظ علائق روشنفکرانه خود، به پی‌ریزی ریاضیات به عنوان نظامی فکری پرداختند. برای فیثاغورس و مریدانش، ریاضیات تا حد زیادی وسیله‌ای برای نیل به هدفی دیگر، یعنی فلسفه، بود. فقط از زمان تأسیس مکتب اسکندریه است که وارد دوره‌ای می‌شویم که ریاضیات به خودی خود مورد توجه قرار می‌گیرد.

فعلاً قدری از موضوع منحرف می‌شویم تا خاطرنشان کنیم که تصورات رمزگرایانه دربارهٔ ویژگیهای اعداد منحصر به فیثاغورسیان نبود. یکی از مهملترین و در عین حال رایجترین اشکالی که عددشناسی در قرون وسطا به خود گرفت، شبه دانش معروف به گِماتریا[1] بود. با نسبت دادن مقدارهای عددی به حروف الفبا بر پایهٔ نظمی خاص، به هر اسم یا کلمه عددی خاص منسوب می‌شد. از نظر گماتریا، دو کلمه هم‌ارز به حساب می‌آمدند اگر مجموعهای عددهای متناظر با حرفهایشان برابر بودند. همهٔ اینها احتمالاً از دوران یونانیان اولیه منشأ گرفته که در آن دوران ترتیب طبیعی الفبا روش کاملی برای ثبت اعداد به حساب می‌آمد؛ α متناظر با ۱ بود، β متناظر با ۲، و الی آخر. به عنوان مثال، کلمهٔ «آمین» متناظر با $\alpha\mu\eta\nu$ در زبان یونانی است؛ این حروف به ترتیب دارای ارزشهای ۱، ۴۰، ۸، و ۵۰ هستند که به ۹۹ بالغ می‌شوند. در بسیاری از چاپهای قدیمی کتاب مقدس، به جای آمین در انتهای ادعیه عدد ۹۹ به کار رفته است. معروفترین عدد ۶۶۶ بود یعنی «عدد وحش» مذکور در «کتاب مکاشفات». یکی از سرگرمیهای برخی از روحانیان کاتولیک

۱. gematria، نوعی حساب جمل.

در عصر اصلاح دینی[1] تنظیم جدولهایی الفبایی بود که طبق آنها ۶۶۶ متناظر با نام مارتین لوتر می‌شد، و نتیجه می‌گرفتند که او مسیح کاذب است. لوتر نیز به همان شیوه به آنها پاسخ داد یعنی دستگاهی سرهم‌بندی کرد که در آن ۶۶۶ عدد منسوب به پاپِ وقت، لئوی دهم، بود.

در اسکندریه بود، و نه در آتن، که دانشی از اعداد، جدا از دیدگاه رمزگرایانه، شروع به رشد کرد. اسکندریه تا زمان انهدامش در ۶۴۱ میلادی توسط عربها، به مدت هزار سال مرکز فرهنگی و تجارتی دنیای هلنی [=یونانی مآب] بود. (بعد از سقوط اسکندریه، بیشتر علمای آن به قسطنطنیه مهاجرت کردند. در طی ۸۰۰ سال بعدی، در حالی که در غرب خبری از آموزش رسمی نبود، دانشمندان قسطنطنیه آثار ریاضی مکتبهای مختلف یونانی را حفظ کردند.) مرکز علمی اسکندریه، موسوم به موزهٔ اسکندرانی[2]، نیای دانشگاههای امروزی بوده و شاعران و علمای پیشروِ روز را گردهم می‌آورده است؛ در مجاورت آن کتابخانهٔ عظیمی تأسیس شده بود که گفته می‌شود در بهترین دوران خود بیش از ۷۰۰۰۰۰ نسخهٔ خطی داشته است. از میان افراد برجسته‌ای که با این مرکز همکاری می‌کردند، اقلیدس (در حوالی ۳۵۰ پیش از میلاد)، مؤسس «مکتب ریاضیات» جایگاه خاصی دارد. معلوم شده است که او نویسندهٔ کتاب اصول، قدیمیترین رسالهٔ یونانی دربارهٔ ریاضیات که سالم به‌دست ما رسیده است، بوده است. کتاب اصول مجموعه‌ای است از بسیاری از اطلاعات ریاضی موجود در آن زمان که در سیزده قسمت یا مقاله تنظیم شده است. نام اقلیدس به اندازه‌ای با هندسه مترادف است که گاهی فراموش می‌شود که سه مقالهٔ هفتم، هشتم، و نهم از کتاب او به نظریهٔ اعداد اختصاص دارد.

اصول اقلیدس یکی از موفقترین آثار در میان تمام آثار مکتوبِ دنیاست. صرف‌نظر از کتاب مقدس، کمتر کتابی را می‌توان یافت که به اندازهٔ آن منتشر یا مطالعه شده باشد. از زمان نخستین چاپش در ۱۴۸۲ بیش از یکهزار بار تجدید چاپ شده است، و پیش از آن، نسخه‌های خطی این کتاب در بیشتر مراکز آموزش اروپای غربی مقام مرجعیت داشته است. متأسفانه هیچ نسخه‌ای از این کتاب که واقعاً در زمان خود اقلیدس تهیه شده باشد، به‌دست نیامده است؛ نسخه‌های فعلی مبتنی بر نسخهٔ تجدید نظر شده‌ای است که تئون اسکندرانی، یکی از شارحان قرن چهارم بعد از میلاد، فراهم کرده است.

تمرینهای ۱ـ۳

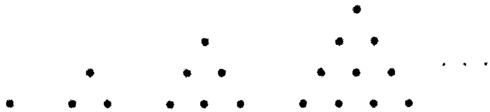
۱. هر یک از عددهای

$$۱ = ۱,\ \ ۳ = ۱ + ۲,\ \ ۶ = ۱ + ۲ + ۳,\ \ ۱۰ = ۱ + ۲ + ۳ + ۴, \ldots$$

۱. جنبشی مذهبی که در قرن شانزدهم به منظور اصلاح کلیسای رُم به وجود آمد ـ م.

2. Alexandrian Museum

تعداد نقطه‌هایی را نشان می‌دهند که می‌توان با فاصله‌های مساوی در یک مثلث متساوی‌الاضلاع چید:



این امر موجب شد که یونانیان باستان عددی را مثلثی بنامند هرگاه مجموع چند عدد صحیح مثبت متوالی باشد که از ۱ آغاز شوند. حکمهای زیر را دربارهٔ عددهای مثلثی ثابت کنید:

(الف) یک عدد مثلثی است اگر و تنها اگر به‌ازای $n \geq 1$ای به صورت $n(n+1)/2$ باشد. (فیثاغورس، در حوالی ۵۵۰ پیش از میلاد).

(ب) عدد صحیح n یک عدد مثلثی است اگر و تنها اگر $8n+1$ مربع کامل باشد. (پلوتارخ، در حوالی ۱۰۰ بعد از میلاد).

(پ) مجموع هر دو عدد مثلثی متوالی یک مربع کامل است. (نیکوماخوس، در حوالی ۱۰۰ بعد از میلاد).

(ت) اگر n عددی مثلثی باشد، آنگاه عددهای $9n+1$، $25n+3$ و $49n+6$ نیز مثلثی هستند. (اویلر، ۱۷۷۵ میلادی).

۲. اگر t_n، nامین عدد مثلثی باشد، ثابت کنید که برحسب ضریبهای دو جمله‌ای داریم

$$t_n = \binom{n+1}{2}, \quad n \geq 1$$

۳. فرمول زیر را برای مجموع عددهای مثلثی که به آریبهطه[1] ریاضیدان هندی (در حوالی ۵۰۰ بعد از میلاد)، نسبت داده شده است، ثابت کنید:

$$t_1 + t_2 + t_3 + \ldots + t_n = \frac{n(n+1)(n+2)}{6}, \quad n \geq 1$$

[راهنمایی: با توجه به اتحاد $t_{k-1} + t_k = k^2$، جمله‌های سمت چپ را دوبه‌دو دسته‌بندی کنید.]

۴. ثابت کنید که مربع هر مضرب فرد ۳ تفاضل دو عدد مثلثی است؛ به طور مشخص نشان دهید

$$9(2n+1)^2 = t_{9n+4} - t_{3n+1}$$

۵. در دنبالهٔ عددهای مثلثی، مطلوب است

1. Aryabhatta

(الف) دو عدد مثلثی که مجموع و تفاضلشان نیز اعدادی مثلثی باشند؛
(ب) سه عدد مثلثی متوالی که حاصلضربشان مربع کامل باشد؛
(پ) سه عدد مثلثی متوالی که مجموعشان مربع کامل باشد.

۶. (الف) اگر عدد مثلثی t_n مربع کامل باشد، نشان دهید که $t_{۴n(n+۱)}$ نیز مربع کامل است.
(ب) با استفاده از قسمت (الف) سه مربع کامل مثال بزنید که عددهایی مثلثی نیز باشند.

۷. نشان دهید که تفاضل مربعهای دو عدد مثلثی متوالی همیشه مکعب است.

۸. ثابت کنید که مجموع عکسهای n عدد مثلثی نخست کمتر از ۲ است؛ یعنی

$$\frac{۱}{۱} + \frac{۱}{۳} + \frac{۱}{۶} + \frac{۱}{۱۰} + \ldots + \frac{۱}{t_n} < ۲$$

[راهنمایی: توجه کنید که $\frac{۲}{n(n+۱)} = ۲\left(\frac{۱}{n} - \frac{۱}{n+۱}\right)$.]

۹. (الف) اگر $n \geq ۱$، $x = ۱/۲\ n(n+۳) + ۱$، $y = n + ۱$، $z = ۱/۲\, n(n+۳)$، اتحاد $t_x = t_y + t_z$ را ثابت کنید و از آن نتیجه بگیرید که تعداد عددهای مثلثی که مجموع دو عدد مثلثی دیگر باشند، نامتناهی است.
(پ) سه عدد مثلثی مثال بزنید که هر یک مجموع دو عدد مثلثی دیگر باشند.

۲

نظریهٔ تقسیم‌پذیری در عددهای صحیح

«عددهای صحیح سرچشمهٔ کل ریاضیات هستند.»

هرمان مینکوفسکی

۲ـ۱ الگوریتم تقسیم

تا اینجا چندین صفحه دربارهٔ عددهای صحیح بحث کرده‌ایم ولی هنوز هیچ یک از ویژگیهای تقسیم‌پذیری را استنتاج نکرده‌ایم. اکنون وقت آن است که این نقص جبران شود. قضیه‌ای وجود دارد که سنگ بنای اصلی کل مطالعهٔ ما در این زمینه است: الگوریتم تقسیم. بیشتر ما با این قضیه آشنا هستیم و مضمون آن به زبان ساده این است که عدد صحیح a را می‌توان بر عدد صحیح b طوری «تقسیم کرد» که اندازهٔ باقیمانده از اندازهٔ b کوچکتر باشد. به بیانی دقیقتر می‌توان گفت:

قضیهٔ ۲ـ۱ (الگوریتم تقسیم). به‌ازای عددهای صحیح a و b، به شرط $b > 0$، عددهای صحیح یکتای q و r وجود دارند به طوری که

$$a = qb + r \quad ، \quad 0 \leq r < b$$

عددهای صحیح q و r، به ترتیب، خارج قسمت و باقیماندهٔ تقسیم a بر b نامیده می‌شوند.

اثبات. با اثبات ناتهی بودن مجموعهٔ

$$S = \{a - xb | a - xb \geq ۰ \text{ و } x \text{ عددی صحیح است}\}$$

آغاز می‌کنیم. برای این کار کافی است مقداری از x ارائه کنیم که $a - xb$ به‌ازای آن نامنفی باشد. چون $b \geq ۱$، داریم $|a|b \geq |a|$، و بنابراین

$$a - (-|a|)b = a + |a|b \geq a + |a| \geq ۰$$

پس به‌ازای $x = -|a|$، $a - xb$ در S واقع می‌شود. این نکته راه را برای کاربردی از اصل خوشترتیبی، که از آن نتیجه می‌گیریم مجموعهٔ S دارای کوچکترین عضو است، هموار می‌کند؛ این عضو را r می‌نامیم. بنا به تعریف S، عدد صحیح qای وجود دارد که

$$r = a - qb, \quad ۰ \leq r$$

نشان می‌دهیم $r < b$. اگر چنین نباشد، باید $r \geq b$ و

$$a - (q + ۱)b = (a - qb) - b = r - b \geq ۰$$

یعنی، عدد صحیح $a - (q + ۱)b$ دارای شکل مناسب برای عضویت در مجموعهٔ S است. ولی، $a - (q + ۱)b = r - b < r$، که متناقض با انتخاب r به عنوان کوچکترین عضو S است. پس، $r < b$.

اکنون به اثبات یکتایی q و r می‌پردازیم. فرض کنید a دارای دو نمایش به‌صورت مطلوب باشد، مثلاً

$$a = qb + r = q'b + r'$$

که در آن $۰ \leq r < b$، $۰ \leq r' < b$. در این صورت $r - r' = b(q - q')$، و چون قدر مطلق حاصلضرب برابر با حاصلضرب قدر مطلقهاست، پس

$$|r' - r| = b|q - q'|$$

از جمع دو نابرابری $-b < -r \leq ۰$ و $۰ \leq r' < b$ نتیجه می‌شود $-b < r' - r < b$ یا، به‌صورت معادل، $|r' - r| < b$. بنابراین، $b|q - q'| < b$، که نتیجه می‌دهد

$$۰ \leq |q - q'| < ۱$$

چون $|q-q'|$ یک عدد صحیح نامنفی است، تنها امکان این است که $|q-q'| = \circ$، یا $q = q'$،
از این نیز نتیجه می‌شود $r = r'$، که به فرایند اثبات پایان می‌دهد. □

گونهٔ کلیتری از الگوریتم تقسیم به این ترتیب به‌دست می‌آید که به جای شرط مثبت بودن b، شرط سادهٔ $b \neq \circ$ را قرار دهیم.

فرع. اگر a و b عددهایی صحیح باشند و $b \neq \circ$، آنگاه عددهای صحیح یکتای q و r وجود دارند به طوری که

$$a = qb + r, \qquad \circ \le r < |b|$$

اثبات. کافی است حالتی را در نظر بگیریم که $b < \circ$. در این صورت $|b| > \circ$ و بنا به قضیهٔ ۲ـ۱، عددهای صحیح یکتای q' و r وجود دارند به طوری‌که

$$a = q'|b| + r, \qquad \circ \le r < |b|$$

چون $|b| = -b$، با انتخاب $q = -q'$ به $a = qb + r$، با ضابطهٔ $\circ \le r < |b|$، می‌رسیم. □

به عنوان مثالی از الگوریتم تقسیم در حالت $b < \circ$، فرض می‌کنیم $b = -۷$. در این صورت، به‌ازای $a = ۱, -۲, ۶۱, -۵۹$ به‌دست می‌آوریم

$$۱ = \circ(-۷) + ۱$$
$$-۲ = ۱(-۷) + ۵$$
$$۶۱ = (-۸)(-۷) + ۵$$
$$-۵۹ = ۹(-۷) + ۴$$

ما بیشتر به کاربردهای الگوریتم تقسیم خواهیم پرداخت تا به خودِ این الگوریتم. به عنوان نخستین مثال، توجه کنید که به‌ازای $b = ۲$، باقیمانده‌ها می‌توانند $\circ$ یا ۱ باشند. اگر $r = \circ$، عدد صحیح a به‌صورت $a = ۲q$ است و زوج نامیده می‌شود؛ اگر $r = ۱$، عدد صحیح a به‌صورت $a = ۲q + ۱$ است و فرد نامیده می‌شود. پس $a^۲$ یا به شکل $(۲q)^۲ = ۴k$ است یا به شکل $(۲q + ۱)^۲ = ۴(q^۲ + q) + ۱ = ۴k + ۱$. نتیجه اینکه باقیماندهٔ تقسیم مربع هر عدد صحیح بر ۴ برابر $\circ$ یا ۱ است.

همچنین می‌توانیم نشان دهیم که: مربع هر عدد صحیح فرد به‌صورت $۸k + ۱$ است. بنابه الگوریتم تقسیم، هر عدد صحیح قابل نمایش به یکی از صورتهای $۴q$، $۴q + ۱$، $۴q + ۲$، $۴q + ۳$ است. در این طبقه‌بندی، فقط عددهای صحیحی که به‌صورت $۴q + ۱$ و $۴q + ۳$اند، فرد هستند. اگر اینها را به توان ۲ برسانیم، به‌دست می‌آوریم

$$(۴q + ۱)^۲ = ۸(۲q^۲ + q) + ۱ = ۸k + ۱$$

و همین‌طور

$$(۴q + ۳)^۲ = ۸(۲q^۲ + ۳q + ۱) + ۱ = ۸k + ۱$$

به عنوان مثال، مربع عدد صحیح فرد ۷ برابر با $۷^۲ = ۴۹ = ۸ \times ۶ + ۱$ است، و مربع ۱۳ برابر با $۱۳^۲ = ۱۶۹ = ۸ \times ۲۱ + ۱$ است.

به طوری که از این ملاحظات برمی‌آید، فایدهٔ الگوریتم تقسیم در این است که اثبات حکمهایی دربارهٔ همهٔ عددهای صحیح را صرفاً با بررسی تعدادی متناهی از حالات امکان‌پذیر می‌کند. این موضوع را با مثال زیر نشان می‌دهیم.

مثال ۲ـ۱

می‌خواهیم نشان دهیم که به‌ازای هر $a \geq ۱$، عبارت $\frac{a(a^۲+۲)}{۳}$ عددی صحیح است. بنا به الگوریتم تقسیم، هر a به‌صورت $۳q$، $۳q + ۱$، یا $۳q + ۲$ است. نخستین حالت از این حالتها را در نظر بگیرید. داریم

$$a(a^۲ + ۲)/۳ = q(۹q^۲ + ۲)$$

که به وضوح عدد صحیحی است. به همین ترتیب، اگر $a = ۳q + ۱$، آنگاه

$$(۳q + ۱)\frac{[(۳q + ۱)^۲ + ۲]}{۳} = (۳q + ۱)(۳q^۲ + ۲q + ۱)$$

و $a(a^۲ + ۲)/۳$ در این حالت نیز عدد صحیحی است. بالاخره، به‌ازای $a = ۳q + ۲$، به‌دست می‌آوریم

$$(۳q + ۲)\frac{[(۳q + ۲)^۲ + ۲]}{۳} = (۳q + ۲)(۳q^۲ + ۴q + ۲)$$

که باز عدد صحیحی است. پس، حکم در همهٔ حالتها ثابت شد. ■

تمرینهای ۲ـ۱

۱. ثابت کنید که اگر a و b عددهایی صحیح باشند و $b > \circ$، آنگاه عددهای صحیح یکتای q و r وجود دارند که در $a = qb + r$، به طوری که $۲b \leq r < ۳b$، صدق کنند.

۲. نشان دهید که هر عدد صحیح به‌صورت $۶k + ۵$، به‌صورت $۳k + ۲$ نیز هست، ولی نه برعکس.

۳. با استفاده از الگوریتم تقسیم نشان دهید که

(الف) مربع هر عدد صحیح یا به‌صورت $۳k$ یا به‌صورت $۳k + ۱$ است

(ب) مکعب هر عدد صحیح به یکی از صورتهای $۹k$، $۹k + ۱$ یا $۹k + ۸$ است

(پ) توان چهارم هر عدد صحیح یا به‌صورت $۵k$ یا به‌صورت $۵k + ۱$ است.

۴. ثابت کنید که $۳a^۲ - ۱$ هرگز مربع کامل نیست. [راهنمایی: تمرین ۳ (الف).]

۵. ثابت کنید که به‌ازای $n \geq ۱$، $n(n + ۱)(۲n + ۱)/۶$ عددی صحیح است. [راهنمایی: بنا به الگوریتم تقسیم، n به یکی از صورتهای $۶k$، $۶k + ۱$، ...، $۶k + ۵$ است؛ حکم را در مورد هر یک از این شش حالت ثابت کنید.]

۶. تحقیق کنید که اگر عدد صحیحی هم مربع و هم مکعب باشد (مانند $۶۴ = ۸^۲ = ۴^۳$)، آنگاه عدد مزبور باید به یکی از دو صورت $۷k$ یا $۷k + ۱$ باشد.

۷. صورت زیر از الگوریتم تقسیم را استنتاج کنید: به‌ازای عددهای صحیح a و b که $b \neq \circ$، عددهای صحیح یکتای q و r وجود دارند به طوری که $a = qb + r$، که در آن $-\frac{۱}{۲}|b| < r \leq \frac{۱}{۲}|b|$. [راهنمایی: نخست بنویسید $a = q'b + r'$، که در آن $\circ \leq r' < |b|$. اگر $\circ \leq r' \leq \frac{۱}{۲}|b|$، قرار دهید $r = r'$ و $q = q'$؛ اگر $\frac{۱}{۲}|b| < r' < |b|$، قرار دهید $r = r' - |b|$ و $q = q' + ۱$ چنانچه $b > \circ$ و $q = q' - ۱$ چنانچه $b < \circ$.]

۸. ثابت کنید که هیچ عدد صحیحی در دنبالهٔ

$$۱۱, ۱۱۱, ۱۱۱۱, ۱۱۱۱۱, \ldots$$

مربع کامل نیست. [راهنمایی: جملهٔ عمومی ۱۱۱...۱۱۱ را می‌توان به صورت $۱۱۱\ldots۱۱۱ = ۱۱۱\ldots۱۰۸ + ۳ = ۴k + ۳$ نوشت.]

۹. نشان دهید که مکعب هر عدد صحیح به‌صورت $۷k$ یا $۷k \pm ۱$ است.

۱۰. نشان دهید که به‌ازای $n \geq ۱$، عدد صحیح $n(۷n^۲ + ۵)$ به‌صورت $۶k$ است.

۱۱. اگر n عدد صحیح فردی باشد، نشان دهید که $n^۴ + ۴n^۲ + ۱۱$ به‌صورت $۱۶k$ است.

۲ـ۲ بزرگترین مقسوم‌علیه مشترک

حالتی که باقیمانده در الگوریتم تقسیم صفر است، اهمیت ویژه‌ای دارد. اکنون به مطالعهٔ این وضعیت می‌پردازیم.

تعریف ۲ـ۱ گوییم عدد صحیح b بر عدد صحیح $a \neq ۰$ تقسیم‌پذیر [بخش‌پذیر] است، و می‌نویسیم $a|b$، اگر عدد صحیح cای موجود باشد به طوری که $b = ac$. برای نشان دادن اینکه b بر a تقسیم‌پذیر [بخش‌پذیر] نیست، می‌نویسیم $a \not| b$.

بنابراین، مثلاً ۱۲− بر ۴ بخش‌پذیر است، زیرا $(-۳)۴ = -۱۲$ ولی، ۱۰ بر ۳ بخش‌پذیر نیست؛ زیرا عدد صحیح cای وجود ندارد که به‌ازای آن تساوی $۳c = ۱۰$ برقرار باشد.

رابطهٔ بخش‌پذیری $a|b$ را می‌توان به صورتهای دیگر نیز بیان کرد. می‌توان گفت که a یک مقسوم‌علیه b است، یا a یک عامل b است، یا a عدد b را می‌شمارد و یا اینکه b یک مضرب a است. توجه کنید که، در تعریف ۲ـ۱، مقسوم‌علیه a محدودیتی دارد: هرگاه نماد $a|b$ مورد استفاده قرار می‌گیرد، فرض بر این است که a مخالف صفر است.

اگر a مقسوم‌علیهی از b باشد، آنگاه b بر $-a$ نیز بخش‌پذیر است در واقع، $b = ac$ نتیجه می‌دهد $b = (-a)(-c)$، و بنابراین، مقسوم‌علیه‌های یک عدد صحیح را همیشه می‌توان به‌صورت زوجهایی نمایش داد. برای تعیین همهٔ مقسوم‌علیه‌های یک عدد صحیح مفروض، کافی است مقسوم‌علیه‌های مثبت آن را به‌دست آوریم و سپس عددهای صحیح منفی متناظر را به آنها اضافه کنیم. به این دلیل، معمولاً بررسی خود را به مقسوم‌علیه‌های مثبت محدود می‌کنیم.

آوردن فهرست برخی از مستقیمترین نتیجه‌های تعریف ۲ـ۱ مفید است (به خواننده بازخاطرنشان می‌کنیم که مقسوم‌علیه‌ها ناصفر فرض می‌شوند، حتی اگر این موضوع تصریح نشده باشد).

قضیهٔ ۲ـ۲ به‌ازای عددهای صحیح a، b، c، حکمهای زیر برقرارند:

(۱) $a|۰$، $۱|a$، $a|a$.

(۲) $a|۱$ اگر و تنها اگر $a = \pm ۱$.

(۳) اگر $a|b$ و $c|d$، آنگاه $ac|bd$.

(۴) اگر $a|b$ و $b|c$، آنگاه $a|c$.

(۵) $a|b$ و $b|a$ اگر و تنها اگر $a = \pm b$.

(۶) اگر $a|b$ و $b \neq ۰$، آنگاه $|a| \leq |b|$.

(۷) اگر $a|b$ و $a|c$، آنگاه به‌ازای عددهای صحیح دلخواه x و y، $a|(bx + cy)$.

اثبات. حکمهای (۶) و (۷) را ثابت می‌کنیم و قسمتهای دیگر را به عنوان تمرین به خواننده وامی‌گذاریم. اگر $a|b$، آنگاه عدد صحیح cای وجود دارد که $ac = b$؛ همچنین، از $b \neq 0$ نتیجه می‌شود $c \neq 0$. با قدر مطلق‌گیری، به‌دست می‌آوریم $|b| = |ac| = |a||c|$. چون $c \neq 0$، نتیجه می‌شود که $|c| \geq 1$، بنابراین $|b| = |a||c| \geq |a|$.

در مورد (۷)، رابطه‌های $a|b$ و $a|c$ تضمین می‌کنند که به‌ازای عددهای صحیح مناسب r و sای، $b = ar$ و $c = as$. ولی در این صورت، به‌ازای هر x و y،

$$bx + cy = arx + asy = a(rx + sy)$$

چون $rx + sy$ عدد صحیحی است، به نتیجهٔ مطلوب یعنی $a|(bx + cy)$ می‌رسیم. □

شایان ذکر است که ویژگی (۷) از قضیهٔ اخیر را می‌توان با استقرا به مجموع بیش از دو جمله تعمیم داد. یعنی، اگر $a|b_k$، $k = 1, 2, \ldots, n$، آنگاه به‌ازای عددهای صحیح دلخواه x_1، x_2، ...، x_n

$$a|(b_1x_1 + b_2x_2 + \ldots + b_nx_n)$$

عملیات اندکی که برای اثبات این تعمیم مورد نیازند به اندازه‌ای سرراست هستند که از ذکر آنها خودداری می‌کنیم.

اگر a و b عددهای صحیح دلخواهی باشند، آنگاه عدد صحیح d مقسوم‌علیه مشترک a و b نامیده می‌شود اگر $d|a$ و $d|b$. چون عدد ۱ مقسوم علیهی از هر عدد صحیح است، مقسوم‌علیه مشترکی از a و b است؛ پس، مجموعهٔ مقسوم‌علیه‌های مشترک مثبت a و b ناتهی است. چون هر عدد صحیحی ۰ را می‌شمارد، اگر $a = b = 0$، آنگاه هر عدد صحیح مقسوم‌علیه مشترکی از a و b است. در این مورد، مجموعهٔ مقسوم‌علیه‌های مشترک مثبت a و b نامتناهی است. ولی، اگر حداقل یکی از a یا b مخالف صفر باشد، تعداد مقسوم‌علیه‌های مشترک مثبت آنها متناهی است. میان اینها، یکی بزرگتر از همه است، که بزرگترین مقسوم‌علیه مشترک a و b نامیده می‌شود. در قالب تعریف، چنین می‌گوییم:

تعریف ۲-۲ فرض کنیم a و b عددهای صحیح داده شده‌ای باشند که حداقل یکی از آنها ناصفر است. بزرگترین مقسوم علیه مشترک a و b، که با $\gcd(a, b)$ نشان داده می‌شود[1]، عدد صحیح مثبت d است به‌طوری که

۱. gcd از حروف اول عبارت انگلیسی greatest common divisor (بزرگترین مقسوم‌علیه مشترک) تشکیل شده و ما برای سهولت کاربرد در فرمولها، همین صورت اختصاری انگلیسی را در ترجمه حفظ کرده‌ایم.ـ م.

(۱) $d|a$ و $d|b$،
(۲) اگر $c|a$ و $c|b$، آنگاه $c \leq d$.

مثال ۲ـ۲

مقسوم‌علیه‌های مثبت ۱۲− عبارت‌اند از ۱، ۲، ۳، ۴، ۶، ۱۲، و مقسوم‌علیه‌های مثبت ۳۰ عددهای ۱، ۲، ۳، ۵، ۶، ۱۰، ۱۵، و ۳۰ هستند؛ پس، مقسوم‌علیه‌های مثبت مشترک ۱۲− و ۳۰ عبارت‌اند از ۱، ۲، ۳، ۶. چون ۶ بزرگترین عدد در میان این عددهای صحیح است، نتیجه می‌شود $\gcd(-۱۲, ۳۰) = ۶$. به روشی مشابه می‌توان نشان داد که

$$\gcd(-۵, ۵) = ۵،\quad \gcd(۸, ۱۷) = ۱ \quad و \quad \gcd(-۸, -۳۶) = ۴ \qquad ■$$

قضیهٔ ۲ـ۳ نشان می‌دهد که $\gcd(a, b)$ را می‌توان به‌صورت ترکیبی خطی از a و b (منظور از ترکیبی خطی از a و b عبارتی به‌صورت $ax + by$ است، که در آن، x و y عددهای صحیحی هستند) نشان داد. به عنوان مثال

$$\gcd(-۱۲, ۳۰) = ۶ = (-۱۲)۲ + ۳۰ \times ۱$$

یا

$$\gcd(-۸, -۳۶) = ۴ = (-۸)۴ + (-۳۶)(-۱)$$

قضیهٔ ۲ـ۳ به‌ازای عددهای صحیح مفروض a و b، که دست کم یکی از آنها صفر نیست، عددهای صحیح x و yای وجود دارند که

$$\gcd(a, b) = ax + by$$

اثبات. مجموعهٔ S متشکل از همهٔ ترکیبهای خطی مثبت a و b را در نظر بگیرید:

$$S = \{au + bv | au + bv > ۰ \text{ ؛}\ u \text{ و } v \text{ عددهایی صحیح‌اند}\}$$

نخست توجه کنید که S تهی نیست. به عنوان مثال، اگر $a \neq ۰$، آنگاه عدد صحیح $|a| = au + b \times ۰$، که در آن، u برحسب مثبت یا منفی بودن a، به ترتیب، ۱ یا ۱− است، در S واقع است. بنا به اصل خوشترتیبی، S باید دارای کوچکترین عضوی چون d باشد. پس بنا به تعریف مجموعهٔ S، عددهای صحیح x و yای وجود دارند که به‌ازای آنها $d = ax + by$. ادعا می‌کنیم که $d = \gcd(a, b)$.

با توسل به الگوریتم تقسیم، می‌توانیم عددهای صحیح q و r را پیدا کنیم به طوری که $a = qd + r$ و $\circ \leq r < d$. در این صورت، r را می‌توان به‌صورت

$$\begin{aligned} r &= a - qd = a - q(ax + by) \\ &= a(\text{۱} - qx) + b(-qy) \end{aligned}$$

نوشت. اگر $r > \circ$، طبق این عبارت لازم می‌آید که r عضوی از S باشد، و این متناقض است با اینکه d کوچکترین عضو S باشد (توجه کنید که $r < d$). پس، $r = \circ$ و بنابراین $a = qd$، یا به بیان دیگر، $d|a$. با استدلالی مشابه، $d|b$ و بنابراین d مقسوم‌علیه مشترکی از a و b است.

حال اگر c مقسوم‌علیه مشترک مثبتی از عددهای صحیح a و b باشد، آنگاه بنا به قسمت (۷) از قضیهٔ ۲ـ۲ می‌توانیم نتیجه بگیریم که $c|(ax + by)$؛ به بیان دیگر، $c|d$. بنا به قسمت (۶) از همان قضیه، $c = |c| \leq |d| = d$، و در نتیجه d بزرگتر از هر مقسوم‌علیه مشترک مثبت دیگر a و b است. بنابراین، با در نظر گرفتن همهٔ این اطلاعات، ملاحظه می‌کنیم که $d = \gcd(a, b)$. □

باید متوجه بود که اثبات فوق صرفاً اثباتی «وجودی» است و روشی عملی برای محاسبهٔ مقادیر x و y ارائه نمی‌کند؛ چنین روشی در آینده ارائه خواهد شد.

با مطالعهٔ دقیق اثبات قضیهٔ ۲ـ۳ معلوم می‌شود که بزرگترین مقسوم‌علیه مشترک a و b را می‌توان کوچکترین عدد صحیح مثبتِ به‌صورت $ax + by$ دانست. حالت $a = \text{۶}$ و $b = \text{۱۵}$ را در نظر بگیرید. در این حالت، S به‌صورت

$$\begin{aligned} S &= \{\text{۶}(-\text{۲}) + \text{۱۵} \times \text{۱}, \text{۶}(-\text{۱}) + \text{۱۵} \times \text{۱}, \text{۶} \times \text{۱} + \text{۱۵} \times \circ, \ldots\} \\ &= \{\text{۳}, \text{۹}, \text{۶}, \ldots\} \end{aligned}$$

در می‌آید. ملاحظه می‌کنیم که ۳ کوچکترین عدد صحیح موجود در S است، بنابراین $\gcd(\text{۶}, \text{۱۵}) = \text{۳}$.

طبیعت عضوهای S در این مثال، الهامبخش نتیجهٔ دیگری است:

فرع. اگر a و b عددهای صحیح مفروضی باشند، که دست‌کم یکی از آنها صفر نیست، آنگاه مجموعهٔ

$$T = \{ax + by \mid \text{عددهایی صحیح‌اند } y \text{ و } x\}$$

دقیقاً مجموعهٔ همهٔ مضربهای $d = \gcd\,(a, b)$ است.

اثبات. چون $d|a$ و $d|b$، می‌دانیم که به‌ازای همهٔ عددهای صحیح x و y، $d|(ax+by)$. پس هر عضو T مضربی از d است. از طرف دیگر، d را می‌توان به‌ازای عددهای صحیح مناسب $x_\circ$ و $y_\circ$ای به صورت $d = ax_\circ + by_\circ$ نوشت، که در نتیجه هر مضرب nd از d به‌صورت

$$nd = n(ax_\circ + by_\circ) = a(nx_\circ) + b(ny_\circ)$$

است. پس nd ترکیبی خطی از a و b است، و، بنا به تعریف، در T واقع است. □

ممکن است ۱ و ۱− تنها مقسوم‌علیه‌های مشترک زوج مفروضی از عددهای صحیح a و b باشند، که در این صورت $\gcd(a,b) = ۱$. به عنوان مثال:

$$\gcd(۲,۵) = \gcd(-۹,۱۶) = \gcd(-۲۷,-۳۵) = ۱$$

این وضعیت آنقدر پیش می‌آید که تعریف زیر را ایجاب می‌کند.

تعریف ۲ـ۳ دو عدد صحیح a و b، که دست‌کم یکی از آنها صفر نیست، متباین [یا نسبت به هم اول] نامیده می‌شوند اگر $\gcd(a,b) = ۱$.

در قضیهٔ زیر عددهای صحیحِ متباین برحسب ترکیبهای خطی مشخص می‌شوند.

قضیهٔ ۲ـ۴ فرض کنید a و b عددهایی صحیح باشند، که دست‌کم یکی از آنها صفر نیست. در این صورت a و b متباین‌اند اگر و تنها اگر عددهای صحیح x و yای وجود داشته باشند که $۱ = ax + by$.

اثبات. اگر a و b نسبت به هم متباین باشند، یعنی $\gcd(a,b) = ۱$، آنگاه بنا به قضیهٔ ۲ـ۳ عددهای صحیح x و yای وجود دارند که $۱ = ax + by$. برعکس، فرض کنید به‌ازای x و yای داریم $۱ = ax + by$، و $d = \gcd(a,b)$. چون $d|a$ و $d|b$، بنا به قضیهٔ ۲ـ۲، $d|(ax+by)$، یا $d|۱$. چون d عدد صحیح مثبتی است، از شرط بخشپذیری اخیر لازم می‌آید $d = ۱$ (به نقش قسمت (۲) از قضیهٔ ۲ـ۲ در اینجا توجه کنید) و حکم مطلوب نتیجه می‌شود. □

از این قضیه، نتیجه‌ای به‌دست می‌آید که در وضعیتهای خاصی مفید است، یعنی

فرع ۱. اگر $\gcd(a,b) = d$، آنگاه $\gcd(a/d, b/d) = ۱$.

اثبات. پیش از آغاز رسمی اثبات باید توجه کنیم که گرچه a/d و b/d ظاهر کسری دارند، در واقع عددهایی صحیح‌اند، زیرا d مقسوم‌علیهی از هر دوی a و b است. اکنون با علم به اینکه $\gcd(a,b)=d$، می‌توان عددهای صحیح x و yای پیدا کرد که $d=ax+by$. با تقسیم هر دو طرف این معادله بر d، عبارت

$$۱=(a/d)x+(b/d)y$$

به‌دست می‌آید. چون a/d و b/d عددهایی صحیح‌اند، می‌توان از قضیهٔ فوق استفاده کرد. نتیجه این است که a/d و b/d متباین هستند.

برای اینکه مثالی از فرع اخیر آورده باشیم، توجه کنید که $\gcd(-۱۲,۳۰)=۶$ و

$$\gcd(-۱۲/۶,\ ۳۰/۶)=\gcd(-۲,۵)=۱$$

که جز این هم انتظاری نداشتیم.

از $a|c$ و $b|c$، بدون در نظر گرفتن شرطی اضافی، همیشه $ab|c$ نتیجه نمی‌شود. به عنوان مثال، $۶|۲۴$ و $۸|۲۴$، ولی $۶\times۸\nmid۲۴$. البته اگر ۶ و ۸ نسبت به هم متباین می‌بودند، این وضعیت پیش نمی‌آمد. با توجه به این نکته است که: □

فرع ۲. اگر $a|c$ و $b|c$ و $\gcd(a,b)=۱$، آنگاه $ab|c$.

اثبات. چون $a|c$ و $b|c$، عددهای صحیح r و sای می‌توان یافت که $c=ar=bs$. به علاوه، چون $\gcd(a,b)=۱$، می‌توانیم به‌ازای عددهای صحیح x و yای بنویسیم $۱=ax+by$. از ضرب رابطهٔ اخیر در c، نتیجه می‌شود

$$c=c\times۱=c(ax+by)=acx+bcy$$

اگر در طرف راست جانشانیهای مناسب به عمل آید، آنگاه

$$c=a(bs)x+b(ar)y=ab(sx+ry)$$

یا، با استفاده از نماد بخشپذیری، $ab|c$.

گرچه قضیهٔ زیر ساده و پیش افتاده به نظر می‌رسد، از اهمیتی اساسی برخوردار است.

قضیهٔ ۲ـ۵ (لم اقلیدس). اگر $a|bc$ و $\gcd(a,b)=۱$، آنگاه $a|c$.

اثبات. دوباره با استناد به قضیهٔ ۲ـ۳ با نوشتن $ax + by = ۱$، که در آن x و y عددهای صحیحی هستند، آغاز می‌کنیم. با ضرب این معادله در c نتیجه می‌شود

$$c = ۱ \times c = (ax + by)c = acx + bcy$$

چون $a|ac$ و $a|bc$، نتیجه می‌شود $a|(acx + bcy)$، و بنابراین $a|c$.

اگر a و b متباین نباشند، حکم لم اقلیدس ممکن است برقرار نباشد. به عنوان مثال: $۱۲|۹ \times ۸$؛ ولی $۱۲ \nmid ۹$ و $۱۲ \nmid ۸$. □

قضیهٔ زیر اغلب به عنوان تعریفی از $\gcd(a,b)$ به کار می‌رود. امتیاز استفاده از آن به عنوان تعریف، استقلال آن از رابطهٔ ترتیبی است؛ بنابراین می‌توان آن را در دستگاههای جبریِ فاقد رابطهٔ ترتیبی به کار برد.

قضیهٔ ۲ـ۶ فرض کنید a و b عددهایی صحیح باشند که دست‌کم یکی از آنها صفر نیست، به‌ازای عدد صحیح مثبت d، $d = gcd(a,b)$ اگر و تنها اگر

(۱) $d|a$ و $d|b$،

(۲) اگر $c|a$ و $c|b$، آنگاه $c|d$.

اثبات. در شروع کار، فرض کنید $d = \gcd(a,b)$. در این صورت، $d|a$ و $d|b$، بنابراین (۱) برقرار است. در پرتو قضیهٔ ۲ـ۳، d را می‌توان به ازای عددهای صحیح x و yای به‌صورت $d = ax + by$ نوشت. بنابراین، اگر $c|a$ و $c|b$، آنگاه $c|(ax + by)$ یا $c|d$. به طور خلاصه، شرط (۲) برقرار است. برعکس، فرض کنید d عدد صحیح مثبتی باشد و در شرطهای داده شده صدق کند. اگر c مقسوم‌علیه مشترک دلخواهی از a و b باشد، آنگاه بنا به شرط (۲) داریم $c|d$. پس $d \geq c$، و در نتیجه d بزرگترین مقسوم‌علیه مشترک a و b است. □

تمرینهای ۲ـ۲

۱. اگر $a|b$، نشان دهید $(-a)|b$، $a|(-b)$، و $(-a)|(-b)$.

۲. با مفروض بودن عددهای صحیح a، b، c و d نشان دهید که

(الف) اگر $a|b$، آنگاه $a|bc$؛

(ب) اگر $a|b$ و $a|c$، آنگاه $a^۲|bc$؛

(پ) $a|b$ اگر و تنها اگر $ac|bc$، که $c \neq ۰$؛

(ت) اگر $a|b$ و $c|d$، آنگاه $ac|bd$.

۳. این حکم را ثابت یا رد کنید: اگر $a|(b+c)$، آنگاه یا $a|b$ یا $a|c$.

۴. با استفاده از استقرای ریاضی هر یک از حکمهای بخشپذیری زیر را به‌ازای $n \geq ۱$ ثابت کنید

(الف) $۸|۵^{۲n}+۷$ [راهنمایی: $۵^{۲(k+۱)}+۷ = ۵^۲(۵^{۲k}+۷)+(۷-۵^۲\times ۷)$]؛

(ب) $۱۵|۲^{۴n}-۱$؛

(پ) $۵|۳^{۳n+۱}+۲^{n+۱}$؛

(ت) $۲۱|۴^{n+۱}+۵^{۲n-۱}$؛

(ث) $۲۴|۲\times ۷^n+۳\times ۵^n-۵$.

۵. ثابت کنید که به‌ازای هر عدد صحیح a، یکی از عددهای صحیح a، $a+۲$ و $a+۴$ بر ۳ بخشپذیر است. [راهنمایی: بنا به الگوریتم تقسیم، عدد صحیح a باید به یکی از صورتهای $۳k$، $۳k+۱$، یا $۳k+۲$ باشد.]

۶. نشان دهید که به‌ازای عدد صحیح a

(الف) $۲|a(a+۱)$، و $۳|a(a+۱)(a+۲)$؛

(ب) $۳|a(۲a^۲+۷)$؛

(پ) اگر a فرد باشد، آنگاه $۳۲|(a^۲+۳)(a^۲+۷)$.

۷. ثابت کنید که اگر هم a و هم b عددهای صحیح فردی باشند، آنگاه $۱۶|a^۴+b^۴-۲$.

۸. ثابت کنید که

(الف) مجموع مربعهای دو عدد صحیح فرد نمی‌تواند مربع کامل باشد؛

(ب) حاصلضرب چهار عدد صحیح متوالی برابر با مربعی کامل منهای ۱ است.

۹. ثابت کنید که تفاضل دو مکعب متوالی هرگز بر ۲ بخشپذیر نیست.

۱۰. نشان دهید که به‌ازای هر عدد صحیح ناصفر a، $\gcd(a,۰)=|a|$، $\gcd(a,a)=|a|$، و $\gcd(a,۱)=۱$.

۱۱. اگر a و b عددهایی صحیح باشند که دست‌کم یکی از آنها مخالف صفر باشد، نشان دهید که

$$\gcd(a,b)=\gcd(-a,b)=\gcd(a,-b)=\gcd(-a,-b)$$

۱۲. ثابت کنید که به‌ازای هر عدد صحیح مثبت n و هر عدد صحیح a، $\gcd(a,a+n)$ بر n بخشپذیر است؛ پس، $\gcd(a,a+۱)=۱$.

۱۳. اگر عددهای صحیح a و b مفروض باشند، ثابت کنید که

(الف) عددهای صحیح x و yای وجود دارند که $c=ax+by$ اگر و تنها اگر $\gcd(a,b)|c$؛

(ب) اگر عددهای صحیح x و yای موجود باشند به طوری که $ax + by = \gcd(a, b)$، آنگاه $\gcd(x, y) = ۱$.

۱۴. نشان دهید که به‌ازای هر عدد صحیح a

(الف) $\gcd(۲a + ۱,\ ۹a + ۴) = ۱$؛

(ب) $\gcd(۵a + ۲,\ ۷a + ۳) = ۱$؛

(پ) اگر a فرد باشد، آنگاه $\gcd(۳a,\ ۳a + ۲) = ۱$.

۱۵. اگر a و b عددهای صحیحی باشند، که دست‌کم یکی از آنها صفر نباشد، ثابت کنید که b بر $\gcd(۲a - ۳b,\ ۴a - ۵b)$ بخشپذیر است؛ و بنابراین، $\gcd(۲a + ۳,\ ۴a + ۵) = ۱$.

۱۶. نشان دهید که به‌ازای هر عدد صحیح فرد a،

$$a^۲ + (a + ۲)^۲ + (a + ۴)^۲ + ۱$$

بر ۱۲ بخشپذیرست.

۱۷. ثابت کنید که به‌ازای هر $n \geq ۰$، $(۲n)!/n!(n + ۱)!$ عددی صحیح است. [راهنمایی: توجه کنید که $\binom{۲n}{n}(۲n + ۱) = \binom{۲n+۱}{n+۱}(n + ۱)$.]

۱۸. ثابت کنید: حاصلضرب هر سه عدد صحیح متوالی بر ۶ بخشپذیر است؛ حاصلضرب هر چهار عدد صحیح متوالی بر ۲۴ بخشپذیر است؛ حاصلضرب هر پنج عدد صحیح متوالی بر ۱۲۰ بخشپذیر است. [راهنمایی: فرع ۲ی قضیهٔ ۲ـ۴ را نگاه کنید.]

۱۹. هر یک از حکمهای زیر را ثابت کنید

(الف) اگر a عدد صحیح دلخواهی باشد، آنگاه $۶|a(a^۲ + ۱۱)$.

(ب) اگر a عدد صحیح فردی باشد، آنگاه $۲۴|a(a^۲ - ۱)$. [راهنمایی: مربع هر عدد صحیح فرد به‌صورت $۸k + ۱$ است.]

(پ) اگر a و b عددهای صحیح فردی باشند، آنگاه $۸|(a^۲ - b^۲)$.

(ت) اگر a عدد صحیحی باشد که بر ۲ و ۳ تقسیم‌پذیر نباشد، آنگاه $۲۴|(a^۲ + ۲۳)$. [راهنمایی: هر عدد صحیح a باید به یکی از صورتهای $۶k$، $۶k + ۱$، ...، $۶k + ۵$ باشد.]

(ج) اگر a عدد صحیح دلخواهی باشد، آنگاه $۳۶۰|a^۲(a^۲ - ۱)(a^۲ - ۴)$.

۲۰. ثابت کنید که بزرگترین مقسوم‌علیه مشترک، ویژگیهای زیر را دارد

(الف) اگر $\gcd(a, b) = ۱$، و $\gcd(a, c) = ۱$، آنگاه $\gcd(a, bc) = ۱$. [راهنمایی: چون به‌ازای x، y، u و vای $ax + by = au + cv = ۱$، پس $۱ = (ax + by)(au + cv) = a(aux + cvx + byu) + bc(yv)$.]

(ب) اگر $\gcd(a,b) = 1$ و $c|a$، آنگاه $\gcd(b,c) = 1$.

(پ) اگر $\gcd(a,b) = 1$، آنگاه $\gcd(ac,b) = \gcd(c,b)$.

(ت) اگر $\gcd(a,b) = 1$ و $c|a+b$، آنگاه $\gcd(a,c) = \gcd(b,c) = 1$. [راهنمایی: قرار دهید $d = \gcd(a,c)$. در این صورت از $d|a$، $d|c$ نتیجه می‌شود که $d|(a+b) - a$، یا $d|b$.]

(ث) اگر $\gcd(a,b) = 1$، $d|ac$ و $d|bc$، آنگاه $d|c$.

(ث) اگر $\gcd(a,b) = 1$، آنگاه $\gcd(a^2,b^2) = 1$. [راهنمایی: نخست نشان دهید که $\gcd(a,b^2) = \gcd(a^2,b) = 1$.]

۲۱. نشان دهید که اگر $d|n$، آنگاه $(2^d - 1)|(2^n - 1)$. [راهنمایی: از اتحاد $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + x + 1)$ استفاده کنید.]

۲ـ۳ الگوریتم اقلیدسی

البته بزرگترین مقسوم‌علیه مشترک دو عدد صحیح را می‌توان با تعیین همهٔ مقسوم‌علیه‌های مشترک مثبت آنها و مشخص کردن بزرگترین آنها به‌دست آورد؛ ولی این‌کار در مورد عددهای بزرگ روش پرزحمتی است. روش کارآمدتری، که متضمن کاربرد مکرر الگوریتم تقسیم است، در مقالهٔ هفتم اصول آمده است. گرچه این روش براساس شواهد تاریخی پیش از اقلیدس ابداع شده است، امروزه به الگوریتم اقلیدسی معروف است.

الگوریتم اقلیدسی را می‌توان چنین توصیف کرد: فرض کنید a و b دوعدد صحیح‌اند که تعیین بزرگترین مقسوم‌علیه مشترک آنها مدنظر است. چون $\gcd(|a|,|b|) = \gcd(a,b)$، بی‌آنکه به کلیت مطلب خللی وارد شود، می‌توان فرض کرد که $a \geq b > 0$. مرحلهٔ نخست، کاربرد الگوریتم تقسیم در مورد a و b است. در این مرحله به‌دست می‌آید

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b$$

اگر $r_1 = 0$، آنگاه $b|a$ و $\gcd(a,b) = b$. اگر $r_1 \neq 0$، b را به r_1 تقسیم می‌کنیم. در این صورت عددهای صحیح r_2 و q_2ای به‌دست می‌آیند که

$$b = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1$$

اگر $r_2 = 0$، توقف می‌کنیم؛ وگرنه با عمل به‌روش قبل به‌دست می‌آوریم

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2$$

این فرآیند تقسیم تا حصول باقیمانده‌ای صفر، مثلاً در مرحلهٔ $(n+1)$ام، که در آن r_{n-1} بر r_n تقسیم می‌شود، ادامه می‌یابد (چون دنبالهٔ نزولی $b > r_1 > r_2 > \ldots \geq 0$ نمی‌تواند بیش از b عدد صحیح داشته باشد، دیر یا زود باقیماندهٔ صفری به‌دست می‌آید).

نتیجه، دستگاه معادله‌های زیر است:

$$
\begin{aligned}
&a = q_1 b + r_1, && 0 < r_1 < b\\
&b = q_2 r_1 + r_2, && 0 < r_2 < r_1\\
&r_1 = q_3 r_2 + r_3, && 0 < r_3 < r_2\\
&\vdots\\
&r_{n-2} = q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1}\\
&r_{n-1} = q_{n+1} r_n + 0,
\end{aligned}
$$

ثابت می‌کنیم که آخرین باقیماندهٔ ناصفر در این فرآیند، یعنی r_n، برابر $\gcd(a,b)$ است. اثبات ما برمبنای لم زیر است.

لم. اگر $a = qb + r$، آنگاه $\gcd(a,b) = \gcd(b,r)$.

اثبات. اگر $d = \gcd(a,b)$، آنگاه از رابطه‌های $d|a$ و $d|b$ نتیجه می‌شود $d|(a-qb)$، یا $d|r$. پس d مقسوم‌علیه مشترکی از b و r است. از طرف دیگر، اگر c مقسوم‌علیه مشترک دلخواهی از b و r باشد، آنگاه $c|(qb+r)$، و در نتیجه $c|a$. یعنی، c مقسوم‌علیه مشترکی از a و b است، بنابراین $c \leq d$. پس، بنا به تعریف $\gcd(b,r)$، $d = \gcd(b,r)$. □

با استفاده از این لم، از دستگاه معادله‌های مزبور به‌سادگی معلوم می‌شود که همان‌طور که ادعا شد داریم

$$\gcd(a,b) = \gcd(b,r_1) = \ldots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$$

گرچه، بنا به قضیهٔ ۲ـ۳، $\gcd(a,b)$ را می‌توان به‌صورت $ax+by$ بیان کرد، در اثبات قضیه اشاره‌ای به نحوهٔ تعیین عددهای صحیح x و y نشده است. برای این منظور، به الگوریتم اقلیدسی متوسل می‌شویم. با شروع از معادلهٔ ماقبل آخری که از الگوریتم به‌دست می‌آید، می‌نویسیم

$$r_n = r_{n-2} - q_n r_{n-1}$$

$r_{n-۱}$ را از معادلهٔ قبلی موجود در الگوریتم حساب می‌کنیم و حاصل را در برابری بالا قرار می‌دهیم

$$\begin{aligned} r_n &= r_{n-۲} - q_n(r_{n-۳} - q_{n-۱}r_{n-۲}) \\ &= (۱ + q_nq_{n-۱})r_{n-۲} + (-q_n)r_{n-۳} \end{aligned}$$

این رابطه، r_n را به‌صورت ترکیبی خطی از $r_{n-۲}$ و $r_{n-۳}$ نشان می‌دهد. با ادامهٔ عقب‌گرد در دستگاه معادله‌ها، متوالیاً باقیمانده‌های $r_{n-۱}$، $r_{n-۲}$، ...، $r_۲$، $r_۱$ را تا مرحله‌ای که $r_n = \gcd(a, b)$ به‌صورت ترکیبی خطی از a و b به‌دست آید، حذف می‌کنیم.

مثال ۲ـ۳

با محاسبهٔ، مثلاً، $\gcd(۱۲۳۷۸,\ ۳۰۵۴)$، نحوهٔ اجرای الگوریتم اقلیدسی را در یک مورد مشخص نشان می‌دهیم. با کاربرد مناسب الگوریتم اقلیدسی، برابریهای

$$\begin{aligned} ۱۲۳۷۸ &= ۳۰۵۴ \times ۴ + ۱۶۲ \\ ۳۰۵۴ &= ۱۶۲ \times ۱۸ + ۱۳۸ \\ ۱۶۲ &= ۱۳۸ \times ۱ + ۲۴ \\ ۱۳۸ &= ۲۴ \times ۵ + ۱۸ \\ ۲۴ &= ۱۸ \times ۱ + ۶ \\ ۱۸ &= ۶ \times ۳ + ۰ \end{aligned}$$

به‌دست می‌آید. طبق بحثی که کردیم، آخرین باقیماندهٔ ناصفر فوق، یعنی عدد صحیح ۶، بزرگترین مقسوم‌علیه مشترک ۱۲۳۷۸ و ۳۰۵۴ است:

$$۶ = \gcd(۱۲۳۷۸, ۳۰۵۴)$$

برای نمایش ۶ به‌صورت ترکیبی خطی از عددهای صحیح ۱۲۳۷۸ و ۳۰۵۴، از برابری ماقبل آخر در دستگاه برابریهای فوق آغاز می‌کنیم و متوالیاً باقیمانده‌های ۱۸، ۲۴، ۱۳۸، و ۱۶۲ را حذف می‌کنیم:

$$\begin{aligned} ۶ &= ۲۴ - ۱۸ \\ &= ۲۴ - (۱۳۸ - ۵ \times ۲۴) \\ &= ۶ \times ۲۴ - ۱۳۸ \end{aligned}$$

$$
\begin{aligned}
&= ۶(۱۶۲ - ۱۳۸) - ۱۳۸ \\
&= ۶ \times ۱۶۲ - ۷ \times ۱۳۸ \\
&= ۶ \times ۱۶۲ - ۷(۳۰۵۴ - ۱۸ \times ۱۶۲) \\
&= ۱۳۲ \times ۱۶۲ - ۷ \times ۳۰۵۴ \\
&= ۱۳۲(۱۲۳۷۸ - ۴ \times ۳۰۵۴) - ۷ \times ۳۰۵۴ \\
&= ۱۳۲ \times ۱۲۳۷۸ + (-۵۳۵)۳۰۵۴
\end{aligned}
$$

بنابراین، داریم

$$۶ = \gcd(۱۲۳۷۸,\ ۳۰۵۴) = ۱۲۳۷۸x + ۳۰۵۴y$$

که $x = ۱۳۲$ و $y = -۵۳۵$. باید توجه داشت که تنها راه بیان ۶ به‌صورت ترکیبی خطی از ۱۲۳۷۸ و ۳۰۵۴ راه فوق نیست؛ مثلاً، با اضافه و کم کردن ۱۲۳۷۸×۳۰۵۴ به‌دست می‌آوریم

$$
\begin{aligned}
۶ &= (۱۳۲ + ۳۰۵۴)۱۲۳۷۸ + (-۵۳۵ - ۱۲۳۷۸)۳۰۵۴ \\
&= ۱۲۳۷۸ \times ۳۱۸۶ + (-۱۲۹۱۳)۳۰۵۴
\end{aligned}
$$
■

لامه[1] ریاضیدان فرانسوی (۱۷۹۵ـ۱۸۷۰) ثابت کرد که تعداد مرحله‌های لازم در الگوریتم اقلیدسی حداکثر پنج برابر تعداد رقمهای عدد صحیح کوچکتر است. در مثال ۲ـ۲، عدد صحیح کوچکتر (یعنی ۳۰۵۴) چهاررقمی است، بنابراین، تعداد کل تقسیمها نمی‌تواند بیش از بیست باشد، و در عمل فقط شش تقسیم لازم آمد. نکتهٔ قابل توجه دیگر این است که به‌ازای هر $n > ۰$، عددهای صحیح a_n و b_n را می‌توان طوری تعیین کرد که برای محاسبهٔ $\gcd(a_n, b_n)$ با الگوریتم اقلیدسی دقیقاً به n تقسیم نیاز باشد. این حکم را در فصل ۱۳ ثابت خواهیم کرد.

بیان نکته‌ای دیگر ضروری است: تعداد مرحله‌ها در الگوریتم تقسیم را معمولاً می‌توان با انتخاب باقیمانده‌های $r_{k+۱}$ به‌طوری که $|r_{k+۱}| < |r_k|/۲$، تقلیل داد؛ یعنی، با کارکردن با باقیمانده‌هایی که کمترین قدرمطلق را دارند. مثال ۲ـ۳ را با رعایت این نکته دوباره حل می‌کنیم:

$$
\begin{aligned}
۱۲۳۷۸ &= ۳۰۵۴ \times ۴ + ۱۶۲ \\
۳۰۵۴ &= ۱۶۲ \times ۱۹ - ۲۴ \\
۱۶۲ &= ۷ \times ۲۴ - ۶ \\
۲۴ &= (-۶)(-۴) + ۰
\end{aligned}
$$

1. Lamé

به طوری که از مجموعهٔ برابریهای فوق معلوم می‌شود، این روش ممکن است به‌جای بزرگترین مقسوم‌علیه مشترک دو عدد صحیح، قرینهٔ آن را به‌دست دهد (آخرین باقیماندهٔ ناصفر ۶− است).

قضیهٔ زیر نتیجهٔ مهمی از الگوریتم اقلیدسی است.

قضیهٔ ۲ـ۷ اگر $k > 0$، آنگاه $\gcd(ka, kb) = k\gcd(a, b)$.

اثبات. اگر هریک از روابط موجود در الگوریتم اقلیدسی به‌ازای a و b (اوایل بخش ۲ـ۳ را ببینید) را در k ضرب کنیم، به‌دست می‌آوریم

$$
\begin{aligned}
ak &= q_1(bk) + r_1k, & 0 &< r_1k < bk \\
bk &= q_2(r_1k) + r_2k, & 0 &< r_2k < r_1k \\
&\vdots \\
r_{n-2}k &= q_n(r_{n-1}k) + r_nk, & 0 &< r_nk < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_nk) + 0
\end{aligned}
\qquad \square
$$

ولی این به‌وضوح همان الگوریتم اقلیدسی است که در مورد عددهای صحیح ak و bk به‌کار می‌رود، و بنابراین آخرین باقیماندهٔ ناصفر، یعنی r_nk، بزرگترین مقسوم‌علیه مشترک ak و bk است؛ یعنی، طبق ادعای قضیه داریم

$$\gcd(ka, kb) = r_nk = k\gcd(a, b)$$

فرع. به‌ازای هر عدد صحیح $k \neq 0$، $\gcd(ka, kb) = |k|\gcd(a, b)$.

اثبات. کافی است حالت $k < 0$ را درنظر گرفت. در این صورت $-k = |k| > 0$، و بنابه قضیهٔ ۲ـ۷

$$
\begin{aligned}
\gcd(ak, bk) &= \gcd(-ak, -bk) \\
&= \gcd(a|k|, b|k|) = |k|\gcd(a, b)
\end{aligned}
\qquad \square
$$

اثبات کوتاه دیگری از قضیهٔ ۲ـ۷ به شرح زیر است: $\gcd(ak, bk)$ کوچکترین عدد صحیح مثبت به‌صورت $(ak)x + (bk)y$ است، که این خود، k برابر کوچکترین عدد صحیح مثبت به‌صورت $ax + by$ است؛ مقدار اخیر برابر با $k\gcd(a, b)$ است.

به مثالی از قضیهٔ ۲ـ۷ توجه کنید:

$$\gcd(۱۲, ۳۰) = ۳\gcd(۴, ۱۰) = ۳ \times ۲\gcd(۲, ۵) = ۶ \times ۱ = ۶$$

مفهومی متناظر با مفهوم بزرگترین مقسوم‌علیه دوعدد صحیح وجود دارد که کوچکترین مضرب مشترک آنهاست؛ ولی در این کتاب موارد زیادی برای استفاده از آن پیش نخواهد آمد. عدد صحیح c مضرب مشترک دوعدد صحیح ناصفر a و b نامیده می‌شود اگر $a|c$ و $b|c$. به وضوح ۰ مضرب مشترکی از a و b است. برای ملاحظهٔ وجود مضربهای مشترک نابدیهی، توجه کنید که هر دوحاصلضرب ab و $-(ab)$ مضرب مشترک a و b هستند، و یکی از اینها مثبت است. بنا به اصل خوشترتیبی، مجموعهٔ مضربهای مشترک مثبت a و b باید شامل کوچکترین عضو باشد؛ این عدد را کوچکترین مضرب مشترک a و b می‌نامیم.

اکنون تعریف رسمی آن را می‌آوریم.

تعریف ۲ـ۴ کوچکترین مضرب مشترک دوعدد صحیح ناصفر a و b، که با $\operatorname{lcm}(a, b)$ نشان داده می‌شود،[1] عدد صحیح مثبت m است به‌طوری که

(۱) $a|m$ و $b|m$،

(۲) اگر $c > ۰$، و اگر $a|c$ و $b|c$، آنگاه $m \le c$.

به عنوان مثال، مضربهای مشترک مثبت عددهای صحیح ۱۲− و ۳۰ عبارت‌اند از ۶۰، ۱۲۰، ۱۸۰، ...؛ پس، $\operatorname{lcm}(-۱۲, ۳۰) = ۶۰$.

نکتهٔ زیر با توجه به بحث بالا بدیهی است: به‌ازای هر دوعدد صحیح ناصفر a و b، $\operatorname{lcm}(a, b)$ همیشه وجود دارد و $\operatorname{lcm}(a, b) \le |ab|$.

چیزی که نیازمند آن هستیم رابطه‌ای میان مفهومهای بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک است. این نیاز را قضیهٔ زیر رفع می‌کند.

قضیهٔ ۲ـ۸ به‌ازای عددهای صحیح مثبت a و b

$$\gcd(a, b)\operatorname{lcm}(a, b) = ab$$

اثبات. برای شروع، قرار می‌دهیم $d = \gcd(a, b)$ و می‌نویسیم $a = dr$، $b = ds$ که r و s عددهایی صحیح‌اند. اگر $m = ab/d$، آنگاه $m = as = rb$، یعنی، m مضرب مشترک (مثبتی) از a و b است.

---

۱. lcm از حروف اولِ عبارت انگلیسی least common multiple (کوچکترین مضرب مشترک) تشکیل شده و ما برای سهولت کاربرد در فرمولها، همین صورت اختصاری انگلیسی را در ترجمه حفظ کرده‌ایم.ـ م.

اکنون فرض کنید c مضرب مشترک مثبتی از a و b است؛ مثلاً $c = au = bv$. به‌طوری که می‌دانیم، عددهای صحیح x و yای وجود دارند که $d = ax + by$. بنابراین

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

این رابطه نشان می‌دهد که $m|c$، و بنابراین می‌توان نتیجه گرفت $m \leq c$. پس، بنابه تعریف ۲ـ۴، $m = \operatorname{lcm}(a, b)$؛ یعنی

$$\operatorname{lcm}(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)}$$

یا

$$\gcd(a, b)\operatorname{lcm}(a, b) = ab$$

و این همان است که می‌خواستیم ثابت کنیم. □

قضیهٔ ۲ـ۸ دارای نتیجه‌ای است که می‌ارزد جداگانه عنوان شود.

فرع. به‌ازای عددهای صحیح مثبت مفروض a و b، $\operatorname{lcm}(a, b) = ab$ اگر و تنها اگر $\gcd(a, b) = ۱$.

شاید عمده‌ترین فایدهٔ قضیهٔ ۲ـ۸ محاسبه‌پذیرکردن کوچکترین مضرب مشترک دوعدد صحیح به کمک بزرگترین مقسوم‌علیه مشترک آنهاست ــ که می‌توان آن را با استفاده از الگوریتم اقلیدسی حساب کرد. به عنوان مثال، دیدیم که $\gcd(۳۰۵۴,\ ۱۲۳۷۸) = ۶$؛ بنابراین

$$\operatorname{lcm}(۳۰۵۴,\ ۱۲۳۷۸) = \frac{۳۰۵۴ \times ۱۲۳۷۸}{۶} = ۶۳۰۰۴۰۲$$

پیش از آنکه به مطالب دیگر بپردازیم، خاطرنشان می‌کنیم که مفهوم بزرگترین مقسوم‌علیه مشترک را می‌توان به روشی بدیهی به بیش از دوعدد صحیح تعمیم داد. در حالت سه‌عدد صحیح a، b، c، که دست‌کم یکی از آنها مخالف صفر است، $\gcd(a,\ b,\ c)$ بزرگترین عدد صحیح مثبت dای تعریف می‌شود که دارای ویژگیهای زیر باشد

(۱) d مقسوم‌علیه هر یک از a، b، c باشد،

(۲) اگر e عددهای صحیح a، b، c را بشمارد، آنگاه $e \leq d$.

دو مثال در این مورد می‌آوریم:

$$\gcd(۳۹,\ ۴۲,\ ۵۴) = ۳ \quad \text{و} \quad \gcd(۴۹,\ ۲۱۰,\ ۳۵۰) = ۷$$

باید توجه داشت که ممکن است سه‌عدد صحیح به عنوان یک سه‌تایی متباین باشند (یعنی، $\gcd(a, b, c) = ۱$)، ولی دوبه‌دو متباین نباشند؛ این نکته با توجه به عددهای صحیح ۶، ۱۰، و ۱۵ آشکار می‌شود.

تمرینهای ۲ـ۳

۱. مطلوب است $\gcd(۱۴۳, ۲۲۷)$، $\gcd(۳۰۶, ۶۵۷)$ و $\gcd(۲۷۲, ۱۴۷۹)$.

۲. با استفاده از الگوریتم اقلیدسی، عددهای صحیح x و yای را به‌دست آورید که به‌ازای آنها

(الف) $\gcd(۵۶, ۷۲) = ۵۶x + ۷۲y$

(ب) $\gcd(۲۴, ۱۳۸) = ۲۴x + ۱۳۸y$

(پ) $\gcd(۱۱۹, ۲۷۲) = ۱۱۹x + ۲۷۲y$

(ت) $\gcd(۱۷۶۹, ۲۳۷۸) = ۱۷۶۹x + ۲۳۷۸y$

۳. ثابت کنید که اگر d مقسوم‌علیه مشترک a و b باشد، آنگاه $d = \gcd(a, b)$ اگر و تنها اگر $\gcd(a/d, b/d) = ۱$. [راهنمایی: از قضیهٔ ۲ـ۷ استفاده کنید.]

۴. به فرض $\gcd(a, b) = ۱$، ثابت کنید:

(الف) $\gcd(a+b, a-b) = ۱$ یا ۲. [راهنمایی: قرار دهید $d = \gcd(a+b, a-b)$ و نشان دهید که $d|۲a$، $d|۲b$؛ بنابراین، $d \leq \gcd(۲a, ۲b) = ۲\gcd(a, b)$.]

(ب) $\gcd(۲a+b, a+۲b) = ۱$ یا ۳.

(پ) $\gcd(a+b, a^۲+b^۲) = ۱$ یا ۲. [راهنمایی: $a^۲+b^۲ = (a+b)(a-b)+۲b^۲$.]

(ت) $\gcd(a+b, a^۲-ab+b^۲) = ۱$ یا ۳. [راهنمایی: $a^۲-ab+b^۲ = (a+b)^۲-۳ab$.]

۵. به‌ازای عددهای صحیح مثبت a، b و $n \geq ۱$، نشان دهید که

(الف) اگر $\gcd(a, b) = ۱$، آنگاه $\gcd(a^n, b^n) = ۱$. [راهنمایی: تمرین ۲۰ (الف)، بخش ۲ـ۲ را ببینید.]

(ب) از رابطهٔ $a^n|b^n$ نتیجه می‌شود که $a|b$. [راهنمایی: قرار دهید $d = \gcd(a, b)$ و بنویسید $a = rd$، $b = sd$، که در آنها $\gcd(r, s) = ۱$. بنا به قسمت (الف)، $\gcd(r^n, s^n) = ۱$. نشان دهید $r = ۱$، پس $a = d$.]

۶. ثابت کنید که اگر $\gcd(a, b) = ۱$، آنگاه $(a+b, ab) = ۱$.

۷. ثابت کنید که در مورد عددهای صحیح ناصفر a و b، شرطهای زیر هم‌ارزند:

(الف) $a|b$، (ب) $\gcd(a, b) = |a|$، (پ) $\operatorname{lcm}(a, b) = |b|$.

۸. مطلوب است $\operatorname{lcm}(۱۴۳, ۲۲۷)$، $\operatorname{lcm}(۳۰۶, ۶۵۷)$ و $\operatorname{lcm}(۲۷۲, ۱۴۷۹)$.

۹. ثابت کنید که بزرگترین مقسوم‌علیه مشترک دوعدد صحیح مثبت همیشه کوچکترین مضرب مشترک آنها را می‌شمارد.

۱۰. به‌ازای عددهای صحیح ناصفر a و b، حکمهای زیر را دربارهٔ $\operatorname{lcm}(a, b)$ ثابت کنید

(الف) $\gcd(a, b) = \operatorname{lcm}(a, b)$ اگر و تنها اگر $a = b$.

(ب) اگر $k > ۰$، آنگاه $\operatorname{lcm}(ka, kb) = k \operatorname{lcm}(a, b)$.

(پ) اگر m مضرب مشترک a و b باشد، آنگاه $\operatorname{lcm}(a, b) | m$. [راهنمایی: قرار دهید $t = \operatorname{lcm}(a, b)$ و با استفاده از الگوریتم اقلیدسی بنویسید $m = qt + r$، که $۰ \leq r < t$. نشان دهید که r مضرب، a و b است.]

۱۱. فرض کنید a، b، c عددهایی صحیح‌اند به طوری که هیچ دو تا از آنها صفر نیستند، و $d = \gcd(a, b, c)$. نشان دهید که

$$\begin{aligned} d &= \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) \\ &= \gcd(\gcd(a, c), b) \end{aligned}$$

۱۲. عددهای صحیح x، y و zای را پیدا کنید که به‌ازای آنها

$$\gcd(۱۹۸,\ ۲۸۸,\ ۵۱۲) = ۱۹۸x + ۲۸۸y + ۵۱۲z$$

[راهنمایی: قرار دهید $d = \gcd(۱۹۸,\ ۲۸۸)$. چون $\gcd(۱۹۸, ۲۸۸, ۵۱۲) = \gcd(d,\ ۵۱۲)$، نخست عددهای صحیح u و vای را پیدا کنید که به‌ازای آنها $\gcd(d,\ ۵۱۲) = du + ۵۱۲v$.]

۲ـ۴ معادلهٔ دیوفانتی $ax + by = c$

اکنون موضوع صحبت را قدری عوض می‌کنیم و به مطالعهٔ معادله‌های دیوفانتی [دیوفانتوسی] می‌پردازیم. این نامگذاری به افتخار دیوفانتوس، ریاضیدانی که نخستین بار به بررسی چنین معادله‌هایی پرداخت، صورت گرفته است. از زندگی شخصی او تقریباً اطلاعی دردست نیست جز اینکه در حدود ۲۵۰ سال پس از میلاد مسیح در اسکندریه می‌زیسته است. تنها گواه مؤثقی که از زمان فعالیت او دردست است،تقدیم شدن کتابی دربارهٔ شیوهٔ محاسبهٔ مصری از طرف اسقف لاتاکیا [لاذقیه] (که در ۲۷۰ میلادی اسقف شد) به دوستش دیوفانتوس است. گرچه آثار دیوفانتوس به یونانی نوشته شده و حاکی از نبوغ یونانی در تجرید ریاضی است، ولی او، به احتمال قوی بابلی‌ای بود که تحت تأثیر فرهنگ هلنی [=یونایی مآب] پرورش یافته بود. آنچه از ویژگیهای زندگی شخصی او می‌دانیم از صورت مسألهٔ سرگرم کننده‌ای (ظاهراً متعلق به قرن چهارم میلادی)

به‌دست آمده است. دورهٔ طفولیت او ۱/۶ عمرش طول کشید. ریشش پس از ۱/۱۲ دیگر از عمرش رویید؛ او پس از ۱/۷ دیگر از عمرش ازدواج کرد، و پسرش ۵ سال بعد متولد شد، پسر به اندازهٔ نصف پدر عمر کرد و پدر چهارسال بعد از او درگذشت. اگر دیوفانتوس در x سالگی فوت کرده باشد، این اطلاعات منجر به معادلهٔ

$$\frac{۱}{۶}x + \frac{۱}{۱۲}x + \frac{۱}{۷}x + ۵ + \frac{۱}{۲}x + ۴ = x$$

می‌شود که جواب آن $x = ۸۴$ است. بنابراین او بایستی به ۸۴ سالگی رسیده باشد، ولی اینکه در چه سالی یا حتی در چه قرنی درگذشته است، معلوم نیست.

اثر مهمی که شهرت دیوفانتوس ناشی از آن است آریثمیتکا [حساب] اوست، که می‌توان آن را قدیمیترین رساله در جبر به شمار آورد. فقط ۶ مقاله از سیزده مقالهٔ متن اصلی این کتاب به‌جای مانده است. در حساب اوست که برای نخستین بار استفادهٔ اصولی از نمادهای ریاضی را مشاهده می‌کنیم، گرچه نمادهای به‌کار رفته در این کتاب اختصاراتی برای واژه‌ها هستند نه نمادهای جبری به معنی امروزی. نمادهای خاصی برای نمایش مفهومهایی که زیاد به‌کار می‌روند، مانند کمیت مجهول در یک معادله و توانهای متفاوت مجهول تا توان ششم درکتاب معرفی شده‌اند؛ دیوفانتوس نمادی نیز برای بیان تفریق و نماد دیگری برای برابری داشت.

معمولاً اصطلاح معادلهٔ دیوفانتی به معادله‌ای برحسب یک یا چند مجهول اطلاق می‌شود که جوابهای صحیح آن مدنظر باشد. ساده‌ترین معادلهٔ دیوفانتی، که ما بررسی خواهیم کرد، معادلهٔ دیوفانتی خطی دومجهولی است:

$$ax + by = c$$

که‌درآن a، b، c عددهای صحیح داده شده‌ای هستند و a و b هردو صفر نیستند. هرجواب این معادله زوجی از عددهای صحیح چون $x_۰$ و $y_۰$ است که، در صورت جانشانی در معادله، در آن صدق کنند؛ یعنی، می‌خواهیم که $ax_۰ + by_۰ = c$. با کمال شگفتی، در آثار به‌جامانده از دیوفانتوس خبری از معادلهٔ خطی نیست (نظریهٔ لازم برای حل آن در اصول اقلیدس آمده است)، شاید به این دلیل که این نوع معادله را بدیهی به‌حساب می‌آورده است؛ بیشتر مسأله‌های او معطوف به پیدا کردن مربعها و مکعبهایی با ویژگیهای خاص است.

معادلهٔ خطی دیوفانتی می‌تواند جوابهای متعددی داشته باشد. به عنوان مثال، معادلهٔ $۳x + ۶y = ۱۸$ را درنظر بگیرید. در اینجا داریم

$$۳ \times ۴ + ۶ \times ۱ = ۱۸$$

$$۳(-۶) + ۶ \times ۶ = ۱۸$$
$$۳ \times ۱۰ + ۶(-۲) = ۱۸$$

ولی معادلهٔ $۲x + ۱۰y = ۱۷$ جوابی ندارد، زیرا طرف چپ معادله، مستقل از مقدارهای x و y، عدد صحیح زوجی است، اما طرف راست معادله زوج نیست. با توجه به این، منطقی است که در جستجوی شرط وجود جواب و علاقه‌مند به دانستن این نکته باشیم که، در صورت وجود جواب، تعیین همهٔ جوابها امکان‌پذیر است یا نه.

بیان شرط حلپذیری آسان است: معادلهٔ دیوفانتی $ax + by = c$ جواب دارد اگر و تنها اگر $d|c$، که $d = \gcd(a, b)$. می‌دانیم عددهای صحیح r و sای وجود دارند که به‌ازای آنها $a = dr$ و $b = ds$. اگر $ax + by = c$ جوابی داشته باشد، یعنی به‌ازای $x_\circ$ و $y_\circ$ مناسبی داشته باشیم $ax_\circ + by_\circ = c$، آنگاه

$$c = ax_\circ + by_\circ = drx_\circ + dsy_\circ = d(rx_\circ + sy_\circ)$$

و بنابراین $d|c$. برعکس، فرض کنید $d|c$، مثلاً $c = dt$. بنابه قضیهٔ ۲ـ۳، عددهای صحیح $x_\circ$ و $y_\circ$ای می‌توان یافت که در $d = ax_\circ + by_\circ$ صدق کنند. اگر این رابطه در t ضرب شود، به‌دست می‌آوریم

$$c = dt = (ax_\circ + by_\circ)t = a(tx_\circ) + b(ty_\circ)$$

پس، $x = tx_\circ$ و $y = ty_\circ$ جواب ویژه‌ای از معادلهٔ دیوفانتی $ax + by = c$ است. به این ترتیب، قسمتی از حکم قضیهٔ زیر ثابت می‌شود.

قضیهٔ ۲ـ۹ معادلهٔ دیوفانتی خطی $ax + by = c$ جواب دارد اگر و تنها اگر $d|c$، که درآن $d = \gcd(a, b)$. اگر $x_\circ$، $y_\circ$ جواب ویژه‌ای از این معادله باشد، آنگاه دیگر جوابها به‌ازای متغیر صحیح t از

$$x = x_\circ + \left(\frac{b}{d}\right)t \qquad \text{و} \qquad y = y_\circ - \left(\frac{a}{d}\right)t$$

به‌دست می‌آیند.

اثبات. برای اثبات حکم دوم قضیه، فرض می‌کنیم جواب $x_\circ$، $y_\circ$ای از معادلهٔ داده شده معلوم باشد. اگر x'، y' جواب دیگری باشد، آنگاه

$$ax_\circ + by_\circ = c = ax' + by'$$

که هم‌ارز است با

$$a(x' - x_\circ) = b(y_\circ - y')$$

بنا به فرع قضیهٔ ۲ـ۴، عددهای صحیح متباین r و s وجود دارند به‌طوری که $a = dr$، $b = ds$. با جانشانی این مقدارها در معادلهٔ اخیر و حذف عامل مشترک d، ملاحظه می‌کنیم که

$$r(x' - x_\circ) = s(y_\circ - y')$$

حال، وضعیت از این قرار است: $r|s(y_\circ - y')$، و $\gcd(r, s) = ۱$. بنا به لم اقلیدس، باید $r|(y_\circ - y')$؛ یا، به بیان دیگر، به ازای عدد صحیح tای، $y_\circ - y' = rt$. با جانشانی به‌دست می‌آوریم

$$x' - x_\circ = st$$

از این رابطه، فرمولهای

$$x' = x_\circ + st = x_\circ + \left(\frac{b}{d}\right) t$$
$$y' = y_\circ - rt = y_\circ - \left(\frac{a}{d}\right) t$$

نتیجه می‌شوند. به‌آسانی می‌توان ملاحظه کرد که این مقدارها به‌ازای هر عدد صحیح t در معادلهٔ دیوفانتی صدق می‌کنند، زیرا

$$\begin{aligned} ax' + by' &= a[x_\circ + \left(\frac{b}{d}\right) t] + b[y_\circ - \left(\frac{a}{d}\right) t] \\ &= (ax_\circ + by_\circ) + \left(\frac{ab}{d} - \frac{ab}{d}\right) t \\ &= c + \circ \times t = c \end{aligned}$$

پس معادلهٔ داده شده به‌ازای هر مقدار t یک جواب، و بنابراین کلاً بینهایت جواب دارد. $\square$

مثال ۲ـ۴

معادلهٔ دیوفانتی خطی

$$۱۷۲x + ۲۰y = ۱۰۰۰$$

را در نظر بگیرید. با کاربرد الگوریتم اقلیدسی برای محاسبهٔ $\gcd(۱۷۲, ۲۰)$، ملاحظه می‌کنیم که

$$۱۷۲ = ۸ \times ۲۰ + ۱۲$$
$$۲۰ = ۱ \times ۱۲ + ۸$$
$$۱۲ = ۱ \times ۸ + ۴$$
$$۸ = ۲ \times ۴$$

و بنابراین $۴ = \gcd(۱۷۲, ۲۰)$. چون $۴|۱۰۰۰$، این معادله جوابی دارد. برای بیان ۴ به‌صورت ترکیبی خطی از ۱۷۲ و ۲۰، با استفاده از برابریهای فوق از آخر به اول، به شرح زیر عمل می‌کنیم:

$$\begin{aligned} ۴ &= ۱۲ - ۸ \\ &= ۱۲ - (۲۰ - ۱۲) \\ &= ۲ \times ۱۲ - ۲۰ \\ &= ۲(۱۷۲ - ۸ \times ۲۰) - ۲۰ \\ &= ۲ \times ۱۷۲ + (-۱۷)۲۰ \end{aligned}$$

از ضرب کردن این رابطه در ۲۵۰ نتیجه می‌شود

$$\begin{aligned} ۱۰۰۰ = ۲۵۰ \times ۴ &= ۲۵۰[۲ \times ۱۷۲ + (-۱۷)۲۰] \\ &= ۵۰۰ \times ۱۷۲ + (-۴۲۵۰)۲۰ \end{aligned}$$

و بنابراین $x = ۵۰۰$ و $y = -۴۲۵۰$ جوابی از معادلهٔ دیوفانتی مورد نظر است. جوابهای دیگر عبارت‌اند از

$$\begin{aligned} x &= ۵۰۰ + \left(\frac{۲۰}{۴}\right)t = ۵۰۰ + ۵t \\ y &= -۴۲۵۰ - \left(\frac{۱۷۲}{۴}\right)t = -۴۲۵۰ - ۴۳t \end{aligned}$$

که t عددی صحیح است. ■

با مختصری تلاش بیشتر، جوابهایِ برحسب عددهای صحیح مثبت، در صورت وجود، به‌دست می‌آیند. برای این منظور، t باید طوری انتخاب شود که در هردو نابرابری

$$۵t + ۵۰۰ > ۰ \text{،} \qquad -۴۳t - ۴۲۵۰ > ۰$$

صدق کند، یا، به عبارت دیگر، باید

$$-۹۸\frac{۳۶}{۴۳} > t > -۱۰۰$$

چون t باید عددی صحیح باشد، به ناچار $t = -۹۹$. بنابراین معادلهٔ دیوفانتی ما دارای جواب مثبت منحصر به‌فرد $x = ۵$، $y = ۷$ متناظر با مقدار $t = -۹۹$ است.

بیان صورتی که قضیهٔ ۲ـ۹ به‌ازای ضریبهای صحیح متباین پیدا می‌کند، مفید است.

فرع. اگر $\gcd(a,b) = ۱$ و اگر $x_۰$، $y_۰$ جواب ویژه‌ای از معالهٔ دیوفانتی خطی $ax + by = c$ باشد، آنگاه همهٔ جوابها به‌ازای مقدارهای صحیح t از روابط

$$x = x_۰ + bt, \qquad y = y_۰ - at$$

به‌دست می‌آیند.

به عنوان مثال: $x_۰ = ۸$، $y_۰ = -۱$ جوابی از معادلهٔ $۵x + ۲۲y = ۱۸$ است؛ بنابه فرع بالا، جواب کامل به‌ازای tی دلخواه از روابط $x = ۸ + ۲۲t$، $y = -۱ - ۵t$ به‌دست می‌آید.

معادله‌های دیوفانتی اغلب به هنگام حل برخی از انواع سنتی مسأله‌های حساب، مانند مثال زیر، ظاهر می‌شوند.

مثال ۲ـ۵

فردی دوازده عدد سیب و پرتقال را به‌بهای ۱۳۲ تومان خرید. اگر بهای یک سیب ۳ تومان بیش از بهای یک پرتقال باشد و تعداد سیبهای خریداری شده بیشتر از پرتقالها باشد، از هریک چه تعداد خریداری شده است؟

برای طرح این مسأله به‌صورت معادله‌ای دیوفانتی، فرض کنیم x تعداد سیبها و y تعداد پرتقالهای خریداری شده باشد. همچنین، بهای یک پرتقال (به تومان) را z می‌نامیم. در این صورت با توجه به شرطهای مسأله داریم

$$(z + ۳)x + zy = ۱۳۲$$

یا معادلش

$$۳x + (x + y)z = ۱۳۲$$

چون $x + y = ۱۲$، معادلهٔ فوق به‌صورت سادهٔ زیر در می‌آید

$$۳x + ۱۲z = ۱۳۲$$

که این نیز به‌صورت $x + ۴z = ۴۴$ ساده می‌شود.

اکنون هدف اصلی ما تعیین عددهای صحیح x و yای است که در معادلهٔ دیوفانتی

$$x + ۴z = ۴۴ \qquad (*)$$

صدق می‌کنند. چون $\gcd(۱,۴) = ۱$ مقسوم‌علیهی از ۴۴ است، این معادله جواب دارد. با ضرب کردن رابطهٔ $۱(-۳) + ۴ \times ۱ = ۱$ در ۴۴ به‌دست می‌آوریم

$$۴۴ = ۱(-۱۳۲) + ۴ \times ۴۴$$

که معلوم می‌شود $x_۰ = -۱۳۲$، $z_۰ = ۴۴$ جوابی از معادله است. دیگر جوابهای (*) به‌صورت زیرند

$$x = -۱۳۲ + ۴t$$
$$y = ۴۴ - t$$

که t در آنها عددی صحیح است.

به‌ازای هر مقدار از بینهایت مقدار t جوابی برای مسأله اصلی به‌دست نمی‌آید. بلکه فقط مقدارهایی از t را باید در نظر گرفت که به‌ازای آنها $۱۲ \geq x > ۶$. بنابراین کافی است tهایی را به‌دست آوریم که

$$۱۲ \geq -۱۳۲ + ۴t > ۶$$

ولی از $۱۲ \geq -۱۳۲ + ۴t$ نتیجه می‌شود $۳۶ \geq t$، و از $-۱۳۲ + ۴t > ۶$ به‌دست می‌آید $t > ۳۴\frac{۱}{۲}$. پس، تنها مقدارهای صحیحی از t که در هردو نابرابری صدق می‌کنند، عبارت‌اند از $t = ۳۵$ و $t = ۳۶$. لذا خرید به دو صورت می‌تواند انجام گرفته باشد: یک دوجین سیب از قرار هرعدد ۱۱ تومان (حالت متناظر با $t = ۳۶$) یا ۸ سیب از قرار هرعدد ۱۲ تومان و ۴ پرتقال از قرار عددی ۹ تومان (حالت متناظر با $t = ۳۵$). ■

این‌گونه مسأله‌های «سیالهٔ» خطی پیشینه‌ای بس طولانی دارند، و قدمت آنها در متون ریاضی چینی به سدهٔ نخست میلادی بازمی‌گردد. در آن متون به دلیل فقدان نمادهای جبری، اغلب در هیأت معماها یا عبارتهای استفهامی ظاهر شده‌اند. محتوای رسالهٔ دستاوردهای برجستهٔ ریاضی اثر چانگ چی یو- چین[1] (سدهٔ ششم میلادی) گواه تواناییهای جبری دانشمندان چینی است. این رسالهٔ استادانه حاوی یکی از معروفترین مسأله‌های معادلات سیاله است که به جامعه‌های دیگر نیز انتقال یافته است ــ یعنی «مسألهٔ یکصد ماکیان». صورت مسأله این است:

> اگر بهای هر خروس ۵ سکه، هر مرغ ۳ سکه، و هر سه جوجه یکه سکه باشد، چند خروس، مرغ و جوجه، به تعداد کل ۱۰۰، می‌توان با ۱۰۰ سکه خرید؟

1. Chang Chiu-chien

مسأله را برحسب معادله می‌توان چنین نوشت (اگر x تعداد خروسها، y تعداد مرغها، و z تعداد جوجه‌ها باشد):

$$x + y + z = ۱۰۰ \quad ،۵x + ۳y + \frac{۱}{۳}z = ۱۰۰$$

با حذف یکی از مجهولها، به معادله‌ای دیوفانتی خطی برحسب دومجهول دیگر می‌رسیم. به طور مشخص، چون $z = ۱۰۰ - x - y$، داریم $۵x + ۳y + ۱/۳(۱۰۰ - x - y) = ۱۰۰$، یا

$$۷x + ۴y = ۱۰۰$$

این معادله دارای جواب عمومی $x = ۴t$، $y = ۲۵ - ۷t$ است، و بنابراین $z = ۷۵ + ۳t$، که t عدد صحیح دلخواهی است. خود چانگ چند جواب ارائه کرده است:

$$z = ۷۸ ،y = ۱۸ ،x = ۴$$

$$z = ۸۱ ،y = ۱۱ ،x = ۸$$

$$z = ۸۴ ،y = ۴ ،x = ۱۲$$

با اندکی تلاش می‌توان همهٔ جوابهای برحسب عددهای صحیح مثبت را تعیین کرد. برای این کار، t باید طوری انتخاب شود که در هر سه نابرابری

$$۷۵ + ۳t > ۰ ،۲۵ - ۷t > ۰ ،۴t > ۰$$

صدق کند. نابرابریهای دوم و سوم هم‌ارزند با $-۲۵ < t < ۳\frac{۴}{۷}$. چون t باید مقداری مثبت داشته باشد، نتیجه می‌گیریم $t = ۱, ۲, ۳$، و به‌ازای اینها دقیقاً همان جوابهای چانگ به‌دست می‌آیند.

تمرینهای ۲ـ۴

۱. کدام یک از معادله‌های دیوفانتی زیر قابل حل نیست؟

(الف) $۶x + ۵۱y = ۲۲$

(ب) $۳۳x + ۱۴y = ۱۱۵$

(پ) $۱۴x + ۳۵y = ۹۳$

۲. همهٔ جوابهای صحیح معادله‌های دیوفانتی زیر را تعیین کنید

(الف) $۵۶x + ۷۲y = ۴۰$

(ب) $24x+138y=18$

(پ) $221x+35y=11$

۳. همهٔ جوابهای صحیح مثبت معادله‌های دیوفانتی زیر را تعیین کنید

(الف) $18x+5y=48$

(ب) $54x+21y=906$

(پ) $123x+360y=99$

(ت) $158x-57y=7$

۴. اگر a و b عددهای صحیح مثبت متباینی باشند، ثابت کنید معادلهٔ دیوفانتی $ax-by=c$ دارای بینهایت جواب صحیح مثبت است. [راهنمایی: عددهای صحیح $x_\circ$ و $y_\circ$ای وجود دارند که $ax_\circ+by_\circ=1$. به‌ازای هر عدد صحیح t، که بزرگتر از هردوی $|x_\circ|/b$ و $|y_\circ|/a$ باشد، $x=x_\circ+bt$ و $y=-(y_\circ-at)$ جواب مثبتی از معادلهٔ مفروض است.]

۵. (الف) ثابت کنید معادلهٔ دیوفانتی $ax+by+cz=d$ برحسب عددهای صحیح حلپذیر است اگر و تنها اگر $\gcd(a,b,c)|d$.

(ب) همهٔ جوابهای صحیح $15x+12y+30z=24$ را پیدا کنید. [راهنمایی: قرار دهید $y=3s-5t$ و $z=-s+2t$.]

۶. (الف) شخصی ۴۵۵ تومان پول خرد متشکل از سکه‌های ۱۰ تومانی و ۲۵ تومانی دارد. حداکثر و حداقل مجموع تعداد سکه‌هایی که می‌تواند داشته باشد چقدر است؟ آیا امکان دارد تعداد سکه‌های ۱۰ تومانی با تعداد سکه‌های ۲۵ تومانی برابر باشد؟

(ب) بهای بلیط تئاتر محله برای بزرگسالان ۱۲۶۰ ریال و برای خردسالان ۵۲۵ ریال است. درآمد تئاتر در شب خاصی ۶۳۰۰۰ ریال بود. به فرض اینکه تعداد تماشاگران بزرگسال بیش از تعداد تماشاگران خردسال بوده، تعداد هر دسته از تماشاگران چقدر بوده است؟

(پ) مجموع تعدادی ۶ و ۹ برابر ۱۲۶ است؛ اگر تعداد ۶ها با تعداد ۹ها عوض شود، مجموع آنها ۱۱۴ می‌شود. تعداد اولیهٔ هریک چقدر است؟

۷. کشاورزی یکصد رأس دام به مبلغ ۲۸۰۰۰۰۰ تومان خرید. قیمتها عبارت بودند از: گوساله، رأسی ۸۴۰۰۰ تومان، بره، رأسی ۳۵۰۰۰ تومان، بز، رأسی ۱۷۵۰۰ تومان. اگر کشاورز از هر نوع دام حداقل یک رأس خریده باشد، چند رأس از هر نوع خریده است؟

۸. مسؤول باجهٔ پرداخت در بانکی در آمریکا، در هنگام خواندن مبلغ یک چک و پرداخت آن، دلار را با سنت و سنت را با دلار اشتباه کرد. صاحب چک بی‌خبر از این اشتباه و پس از هزینه کردن ۶۸ سنت، درکمال شگفتی متوجه شد که هنوز دوبرابر مبلغ چک را در اختیار دارد. کمترین

مقداری را که مبلغ چک می‌توانسته باشد تعیین کنید. [راهنمایی: اگر x تعداد دلارها و y تعداد سنت‌های مبلغ چک باشد، آنگاه $(۱۰۰x + y)۲ = ۱۰۰y + x - ۶۸$.]

۹. هریک از مسأله‌های معماوار زیر را حل کنید:

(الف) آلکویین اهل یورک[1]، ۷۷۵ میلادی. ۸۰۰ کیسهٔ هم‌اندازه حاوی غله طوری میان ۱۰۰ نفر توزیع شد که هر مرد ۲۴ کیسه، هر زن ۱۶ کیسه، و هر کودک ۴ کیسه دریافت کردند. تعداد مردها، زنها، و کودکان را تعیین کنید.

(ب) مهاویره‌کاریا[2]، ۸۵۰ میلادی. ۶۳ خوشه موز هریک با تعداد یکسانی موز، و ۷ عدد موزِ تنها موجود بود. موزها به‌طور برابر میان ۲۳ مسافر توزیع شد. هر خوشه چند موز داشت؟ [راهنمایی: معادلهٔ دیوفانتی $۶۳x + ۷ = ۲۳y$ را در نظر بگیرید.]

(پ) ین کونگ[3]، ۱۳۷۲ میلادی. تعداد مجهولی سکه داریم. اگر آنها را در ۷۷ ردیف بچینیم، ۵۰ سکه کم می‌آوریم؛ ولی اگر در ۷۸ ردیف بچینیم، کم و زیاد نمی‌آوریم. تعداد سکه‌ها چقدر است؟ [راهنمایی: اگر تعداد سکه‌ها N باشد، آنگاه به‌ازای عددهای صحیح x و yای، $N = ۷۷x + ۲۷ = ۷۸y$.]

(ت) کریستف رودلف[4]، ۱۵۲۶ میلادی. گروهی ۲۰ نفره از مردان و زنان و کودکان داریم که مجموعاً ۲۰ سکه و به تفکیک هر مرد ۳ سکه، هر زن دوسکه، و هر کودک ۱/۲ سکه هزینه کرده‌اند. تعداد مردها، زنها، و کودکان را تعیین کنید.

(ث) اویلر، ۱۷۷۰ میلادی. ۱۰۰ را به‌صورت مجموع دوعدد بنویسید که یکی از آنها بر ۷ و دیگری بر ۱۱ بخشپذیر باشد.

1. Alcuin of York
2. Mahaviracarya
3. Yen Kung
4. Christoff Rudolff

۳

اعداد اول و توزیع آنها

«اعداد نیرومندند و چون با هنر همراه گردند،
مقاومت ناپذیرند.»

اثوریدس

۳ـ۱ قضیهٔ بنیادی حساب

مفهوم اساسی در همه مطالبی که تا اینجا دربارهٔ آنها بحث کرده‌ایم ــ و در واقع، جزء اساسی هر مبحث نظریهٔ اعداد ــ مفهوم عدد اول است. پیشتر دیدیم که هر عدد صحیح $a > ۱$ بر ± ۱ و $\pm a$ بخشپذیر است، اگر اینها تنها مقسوم‌علیه‌های a باشند، a عددی اول نامیده می‌شود. به بیانی دیگر:

تعریف ۳ـ۱ عدد صحیح $p > ۱$ عدد اول یا فقط اول نامیده می‌شود اگر تنها مقسوم‌علیه‌های مثبت آن ۱ و p باشند. عدد صحیح بزرگتر از ۱ ای که اول نباشد، مرکب نامیده می‌شود.

در میان ده عدد صحیح مثبت نخستین، تنها ۲، ۳، ۵، ۷ عددهای اول‌اند و بقیه یعنی ۴، ۶، ۸، ۹، ۱۰ اعدادی مرکب‌اند. توجه کنید که عدد صحیح ۲ تنها عدد اول زوج است، و عدد صحیح ۱، چون طبق تعریف نه اول است و نه مرکب، نقش خاصی دارد.

دربقیهٔ کتاب، حتی‌المقدور حرفهای p و q فقط برای نشان دادن عددهای اول به‌کار خواهند رفت.

قضیهٔ ۱۴ از مقالهٔ نهم اصول اقلیدس حاوی حکمی است که بعدها به قضیهٔ بنیادی حساب معروف شد، و حاکی است که هر عدد صحیح بزرگتر از ۱ را صرف‌نظر از ترتیب عاملها، می‌توان به یک و تنها یک روش به‌صورت حاصلضربی از عددهای اول نشان داد. صورت قضیه را از متن اصلی نقل می‌کنیم: "اگر عددی، کوچکترین عددی باشد که چند عدد اول آن را می‌شمارند، هیچ عدد اول دیگری جز همانها آن را نمی‌شمارد." چون هر عددی یا اول است یا، بنابه قضیهٔ بنیادی حساب، تجزیه‌پذیر به عاملهای اول یکتاست (و بیش از این هم قابل تجزیه نیست)، عددهای اول نقش "اجزای تشکیل‌دهنده"ای را بازی می‌کنند که از آنها می‌توان همهٔ عددهای صحیح را ساخت. بنابراین، عددهای اول علاقه و کنجکاوی ریاضیدانان را طی قرون و اعصار برانگیخته‌اند، و گرچه چند قضیهٔ قابل توجه دربارهٔ توزیع آنها در دنبالهٔ عددهای صحیح مثبت ثابت شده است، حکمهای اثبات نشده قابل توجه‌ترند. مسأله‌های حل نشدهٔ مربوط به عددهای اول را می‌توان جزو مسأله‌های حل نشدهٔ برجسته در تمام ریاضیات به‌حساب آورد.

برای شروع بحث با مطلبی ساده‌تر، توجه کنید که عدد اول ۳ عدد صحیح ۳۶ را، که می‌تواند به‌صورت هر یک از حاصلضربهای

$$۶ \times ۶ = ۹ \times ۴ = ۱۲ \times ۳ = ۱۸ \times ۲$$

نوشته شود، می‌شمارد. در هر مورد، ۳ حداقل یکی از عاملهای ضرب را می‌شمارد. این مثالی از حالت کلی زیر است:

قضیهٔ ۳ـ۱ اگر p عددی اول باشد و $p|ab$، آنگاه $p|a$ یا $p|b$.

اثبات. اگر $p|a$، اثبات تمام است؛ پس فرض می‌کنیم $p\nmid a$. چون تنها مقسوم‌علیه‌های مثبت p، ۱ و خود pاند، نتیجه می‌شود $\gcd(p,a) = ۱$. (به‌طورکلی، $\gcd(p,a) = p$ یا $\gcd(p,a) = ۱$ برحسب اینکه $p|a$ یا $p \nmid a$.) پس، بنا به لم اقلیدس، داریم $p|b$.

این قضیه به آسانی در مورد حاصلضربهای بیش از دو عامل تعمیم داده می‌شود. □

فرع ۱. اگر p اول باشد و $p|a_۱a_۲\ldots a_n$، آنگاه به‌ازای kای، $۱ \le k \le n$، $p|a_k$.

اثبات. به استقرا روی تعداد عاملها، یعنی n، استدلال می‌کنیم. اگر $n = ۱$، حکم عنوان شده به وضوح برقرار است، و اگر $n = ۲$، حکم بنابه قضیهٔ ۱.۳ ثابت است. به‌عنوان فرض استقرا، تصور کنید $n > ۲$، و هرگاه p حاصلضرب کمتر از n عامل را بشمارد، آنگاه حداقل یکی از عاملها را

می‌شمارد. اکنون، فرض کنید $p|a_1a_2\ldots a_n$. بنابه قضیهٔ ۱.۳، یا $p|a_n$ یا $p|a_1a_2\ldots a_{n-1}$. اگر $p|a_n$، آنگاه اثبات تمام است. اگر $p|a_1a_2\ldots a_{n-1}$، فرض استقرا تضمین می‌کند که به‌ازای kای، $1 \leq k \leq n-1$، $p|a_k$. در هر حال، p یکی از عددهای صحیح a_1، a_2، …، a_n را می‌شمارد. □

فرع ۲. اگر p، q_1، q_2، …، q_n همگی اول باشند و $p|q_1q_2\ldots q_n$، آنگاه به‌ازای kای، $1 \leq k \leq n$، $p = q_k$.

اثبات. بنابه فرع ۱ می‌دانیم که به‌ازای kای، $1 \leq k \leq n$، $p|q_k$. q_k که عددی اول است بر عدد صحیح مثبتی بجز ۱ یا خود q_k بخشپذیر نیست. چون $p > 1$، نتیجه می‌گیریم $p = q_k$. □

با این زمینه‌چینی، اکنون به قضیهٔ بنیادی حساب می‌رسیم که یکی از ارکان اصلی بحث ماست. به‌طوری که پیشتر توضیح داده شد، این قضیه حاکی از آن است که هر عدد صحیح بزرگتر از ۱، به طریقی که اساساً یکتاست به عددهای اول تجزیه می‌شود؛ منظور از "اساساً" این است که $2 \times 3 \times 2$ و $2 \times 2 \times 3$ تجزیه‌های متمایزی از ۱۲ محسوب نمی‌شوند. به بیانی دقیقتر:

قضیهٔ ۳-۲ (قضیهٔ بنیادی حساب). هر عدد صحیح مثبت $n > 1$ را می‌توان به‌صورت حاصلضرب چند عدد اول بیان کرد؛ این تجزیه، صرف‌نظر از ترتیب نوشته‌شدن عاملها، یکتاست.

اثبات. n یا اول است یا مرکب؛ در حالت اول چیزی برای اثبات وجود ندارد. اگر n مرکب باشد، آنگاه عدد صحیح dای هست که $d|n$ و $1 < d < n$. از میان چنین عددهای صحیح d، p_1 را به‌عنوان کوچکترین آنها انتخاب می‌کنیم (بنا به اصل خوشترتیبی این کار عملی است). در این صورت p_1 باید عددی اول باشد، و گرنه باید دارای مقسوم‌علیه qای، $1 < q < p_1$، باشد؛ ولی در این صورت از $q|p_1$ و $p_1|n$ نتیجه می‌شود $q|n$، که با انتخاب p_1 به‌عنوان کوچکترین مقسوم‌علیه مثبت n، که با ۱ و n برابر نباشد، سازگار نیست.

بنابراین می‌توانیم بنویسیم $n = p_1n_1$، که در آن p_1 عددی اول است و $1 < n_1 < n$. اگر n_1 اول باشد، نمایش مطلوب به‌دست آمده است. در غیر این‌صورت، با تکرار استدلال، دومین عدد اول p_2 به‌دست می‌آید به‌طوری که $n_1 = p_2n_2$؛ یعنی

$$n = p_1p_2n_2, \qquad 1 < n_2 < n_1$$

اگر n_2 اول باشد، نیازی به ادامهٔ استدلال نیست. اگر نباشد، به‌ازای عدد اول p_3ای می‌نویسیم $n_2 = p_3n_3$:

$$n = p_1p_2p_3n_3, \qquad 1 < n_3 < n_2$$

دنبالهٔ نزولی

$$n > n_1 > n_2 > \ldots > 1$$

نمی‌تواندتا بینهایت ادامه داشته باشد، بنابراین پس از تعدادی متناهی مرحله، n_{k-1} عدد اولی، مثلاً p_k است. از اینجا تجزیهٔ

$$n = p_1 p_2 \ldots p_k$$

به عوامل اول دست می‌آید.

برای اثبات قسمت دوم قضیه ــ یکتایی تجزیه به عددهای اول ــ فرض می‌کنیم عدد صحیح n را بتوان به دو روش به‌صورت حاصلضرب چند عدد اول نوشت؛ مثلاً

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s, \quad r \leq s$$

که p_iها و q_jها همگی اول هستند، و به‌ترتیب صعودی نوشته شده‌اند، یعنی

$$p_1 \leq p_2 \leq \ldots \leq p_r, \quad q_1 \leq q_2 \leq \ldots \leq q_s$$

چون $p_1 | q_1 q_2 \ldots q_s$، بنا به فرع ۲ی قضیهٔ ۳ـ۱، به‌ازای kای داریم $p_1 = q_k$؛ ولی در این‌صورت $p_1 \geq q_1$. با استدلالی مشابه، $q_1 \geq p_1$، و بنابراین $p_1 = q_1$. با حذف این عامل مشترک نتیجه می‌شود

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$$

با تکرار فرایند فوق نتیجه می‌شود $p_2 = q_2$ و، بنابراین

$$p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s$$

به این روش ادامه دهید. اگر $r < s$، بالاخره به

$$1 = q_{r+1} q_{r+2} \ldots q_s$$

می‌رسیم که بی‌معنی است، زیرا همواره $q_1 > 1$. پس $r = s$ و

$$p_1 = q_1, \quad p_2 = q_2, \ldots, \quad p_r = q_r$$

یعنی تجزیه‌های فوق برابرند. پس اثبات تمام است. □

البته ممکن است برخی از عددهای اول موجود در تجزیهٔ یک عدد صحیح، تکراری باشند، مثلاً $۵ \times ۳ \times ۳ \times ۲ \times ۲ \times ۲ = ۳۶۰$. با گروهبندی عددهای اول یکسان و قراردادن یک عامل به جای هر گروه، می‌توانیم قضیهٔ ۳ـ۲ را به‌صورت زیر بیان کنیم:

فرع. هر عدد صحیح مثبت $n > ۱$ را می‌توان به روشی یکتا به‌صورت متعارف

$$n = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$$

نوشت، که در آن به‌ازای $i = ۱, ۲, \dots, r$ هر p_i عددی اول، و هر k_i عدد صحیح مثبتی است و $p_۱ < p_۲ < \dots < p_r$.

به‌عنوان مثال، صورت متعارف عدد صحیح ۳۶۰ عبارت است از $۳۶۰ = ۲^۳ \times ۳^۲ \times ۵$. و دو مثال دیگر:

$$۱۷۶۴۰ = ۲^۳ \times ۳^۲ \times ۵ \times ۷^۲ \quad \text{و} \quad ۴۷۲۵ = ۳^۳ \times ۵^۲ \times ۷$$

در مورد قضیهٔ ۳ـ۲ باید احتیاط کرد. زیرا دستگاههای اعدادی موجودند که تجزیه به عددهای "اول" در آنها یکتا نیست. شاید بدیهی‌ترین مثال، مجموعهٔ E مرکب از همهٔ عددهای صحیح مثبت زوج باشد. یک عدد صحیح زوج را e ـ اول می‌نامیم اگر حاصلضرب دو عدد زوج دیگر نباشد. بنابراین، ۲، ۶، ۱۰، ۱۴، ... همگی e ـ اول‌اند و هیچ یک از ۴، ۸، ۱۲، ۱۶ ... e ـ اول نیستند. به‌سادگی دیده می‌شود که عدد صحیح ۶۰ را می‌توان به دو روش متفاوت به e ـ اولها تجزیه کرد: یعنی

$$۶۰ = ۲ \times ۳۰ = ۶ \times ۱۰$$

ازجمله دلیلهای این امر عدم برقراری قضیهٔ ۳ـ۱ در مجموعهٔ E است: $۶|۲\times۳۰$، ولی $۲ \nmid ۶$ و $۳۰ \nmid ۶$.

اکنون فرصت مناسبی برای ذکر قضیهٔ معروفی از فیثاغورس است. ریاضیات به‌عنوان علم با فیثاغورس (۵۶۹ـ۵۰۰ پیش از میلاد) آغاز شد و بخش عمدهٔ محتوای اصول اقلیدس از آنِ فیثاغورس و مکتب اوست. فیثاغورسیان این افتخار را دارند که برای نخستین بار عددها را به فرد و زوج، و اول و مرکب طبقه‌بندی کرده‌اند.

قضیهٔ ۳ـ۳ (فیثاغورس). عدد $\sqrt{۲}$ گنگ است.

اثبات. فرض کنید چنین نیست و $\sqrt{۲}$ گویاست؛ مثلاً، $\sqrt{۲} = a/b$ که a و b عددهایی صحیح‌اند و $\gcd(a, b) = ۱$. طرفین را به توان دو می‌رسانیم و به‌دست می‌آوریم $a^۲ = ۲b^۲$

و بنابراین $b|a^{۲}$. اگر $b > ۱$، بنا به قضیهٔ بنیادی حساب عدد اول pای هست که $p|b$. نتیجه می‌شود $p|a^{۲}$ و بنابه قضیهٔ ۳ـ۱، $p|a$، یعنی، $\gcd(a,b) \geq p$. بنابراین به تناقضی می‌رسیم، مگر اینکه $b = ۱$. ولی اگر $b = ۱$، آنگاه $a^{۲} = ۲$، که غیرممکن است (فرض می‌کنیم خواننده با این نکته که حاصلضرب هیچ عدد صحیح در خودش ۲ نیست، موافق است). فرض گویا بودن $\sqrt{۲}$ درست نیست و بنابراین $\sqrt{۲}$ باید گنگ باشد. □

تمرینهای ۳ـ۱

۱. حدس زده شده است که بینهایت عدد اول به‌صورت $n^{۲} - ۲$ وجود دارد. پنج تا از آنها را پیدا کنید.

۲. با مثالی نشان دهید که حدس زیر درست نیست:

هر عدد صحیح مثبت را می‌توان به‌صورت $p + a^{۲}$ نوشت، که در آن p یا عددی اول است یا برابر ۱ است، و $a \geq ۰$.

۳. هر یک از حکمهای زیر را ثابت کنید:

(الف) هر عدد اولی که به‌صورت $۳n + ۱$ باشد به‌صورت $۶m + ۱$ نیز هست.

(ب) هر عدد صحیحی که به‌صورت $۳n + ۲$ باشد دارای عامل اولی به‌همین صورت است.

(پ) تنها عدد اولِ به‌صورت $n^{۳} - ۱$، ۷ است. [راهنمایی: $n^{۳} - ۱$ را به‌صورت $(n-۱)(n^{۲}+n+۱)$ بنویسید.]

(ت) $p = ۵$ تنها عدد اول pای است که به‌ازای آن $۳p + ۱$ مربع کامل است.

(ث) تنها عدد اولِ به‌صورت $n^{۲} - ۴$، ۵ است.

۴. اگر $p \geq ۵$ عدد اولی باشد، نشان دهید $p^{۲} + ۲$ مرکب است. [راهنمایی: p به یکی از صورتهای $۶k + ۱$ یا $۶k + ۵$ است.]

۵. (الف) اگر p عددی اول باشد و $p|a^{n}$، ثابت کنید $p^{n}|a^{n}$.

(ب) اگر p عددی اول باشد و $\gcd(a,b) = p$، مقدارهای ممکن $\gcd(a^{۲},b^{۲})$، $\gcd(a^{۲},b)$، و $\gcd(a^{۳},b^{۲})$ را مشخص کنید.

۶. هر یک از حکمهای زیر را ثابت کنید:

(الف) هر عدد صحیح به‌صورت $n^{۴} + ۴$، $n > ۱$، مرکب است. [راهنمایی: $n^{۴} + ۴$ را به‌صورت حاصلضرب دو عامل درجهٔ ۲ بنویسید.]

(ب) اگر $n > ۴$ مرکب باشد، آنگاه n، عدد $(n-۱)!$ را می‌شمارد.

(پ) هر عدد صحیح به‌صورت $۸^{n}+۱$، که $n \geq ۱$، مرکب است. [راهنمایی: $۲^{n}+۱|۲^{۳n}+۱$.]

(ت) هر عدد صحیح $n > ۱۱$ را می‌توان به‌صورت مجموع دو عدد مرکب نوشت. [راهنمایی: اگر n زوج باشد، مثلاً $n = ۲k$، آنگاه $n - ۶ = ۲(k - ۳)$؛ به‌ازای n فرد، عدد صحیح $n - ۹$ را درنظر بگیرید.]

۷. همهٔ عددهای اولی را که !۵۰ را می‌شمارند، پیدا کنید.

۸. اگر p و q عددهایی اول باشند و $p \geq q \geq ۵$، ثابت کنید که $۲۴|p^۲ - q^۲$.

۹. (الف) یکی از پرسشهایِ بی‌جواب مانده این است که آیا تعداد عددهای اولی که به‌صورت توانی از ۲ به‌علاوهٔ ۱ هستند، مانند $۵ = ۱ + ۲^۲$، نامتناهی است یا نه. دو عدد اول دیگر را که از این نوع باشند پیدا کنید.

(ب) حدس کلیتری حاکی از آن است که تعداد عددهای اول به‌صورت $n^۲ + ۱$ نامتناهی است، به‌عنوان مثال $۲۵۷ = ۱۶^۲ + ۱$. پنج عدد اول دیگر را که از این نوع باشند مثال بزنید.

۱۰. اگر $p \neq ۵$ عدد اول فردی باشد، ثابت کنید که یکی از عددهای $p^۲ - ۱$ یا $p^۲ + ۱$ بر ۱۰ بخشپذیر است. [راهنمایی: p به یکی از صورتهای $۱۰k + ۱$، $۱۰k + ۳$، $۱۰k + ۷$ یا $۱۰k + ۹$ است.]

۱۱. حدس اثبات نشدهٔ دیگری حاکی است که تعداد اعداد اولی که به‌صورت توانی از ۲ منهای ۱ هستند، مانند $۳ = ۲^۲ - ۱$، نامتناهی است.

(الف) چهار عدد اول دیگر را که از این نوع باشند پیدا کنید.

(ب) اگر $p = ۲^k - ۱$ اول باشد، نشان دهید که، بجز در حالت $k = ۲$، k عدد صحیح فردی است. [راهنمایی: به‌ازای هر $n \geq ۱$، $۳|۴^n - ۱$.]

۱۲. عددهای ۱۲۳۴، ۱۰۱۴۰، و ۳۶۰۰۰ را به حاصلضرب عاملهای اول تجزیه کنید.

۱۳. اگر $n > ۱$ عدد صحیحی به‌صورت $۶k + ۳$ نباشد، ثابت کنید که $n^۲ + ۲^n$ مرکب است. [راهنمایی: نشان دهید که $n^۲ + ۲^n$ بر ۲ یا بر ۳ بخشپذیر است.]

۱۴. حدس زده شده است که هر عدد صحیح زوج را می‌توان به بینهایت روش به‌صورت تفاضل دو عدد اول متوالی نوشت. به‌عنوان مثال

$$۶ = ۲۹ - ۲۳ = ۱۳۷ - ۱۳۱ = ۵۹۹ - ۵۹۳ = ۱۰۱۹ - ۱۰۱۳ = \ldots$$

عدد صحیح ۱۰ را به ۱۵ روش به‌صورت تفاضل دو عدد اول متوالی بنویسید.

۱۵. ثابت کنید عدد صحیح مثبت $a > ۱$ مربع کامل است اگر و تنها اگر همهٔ توانهای عاملهای اول در صورت متعارف a زوج باشند.

۱۶. عدد صحیحی خالی از مربع نامیده می‌شود اگر بر مربع هیچ عدد صحیح بزرگتر از ۱ بخشپذیر نباشد. ثابت کنید

(الف) عدد صحیح $n > ۱$ خالی از مربع است اگر و تنها اگر n تجزیه‌پذیر به حاصلضرب عددهای اول متمایزی باشد.

(ب) هر عدد صحیح $n > ۱$ حاصلضرب یک عدد صحیح خالی از مربع و یک مربع کامل است. [راهنمایی: اگر $n = p_۱^{k_۱} p_۲^{k_۲} \dots p_s^{k_s}$ تجزیهٔ متعارف n باشد، بنویسید $k_i = ۲q_i + r_i$، که برحسب زوج یا فرد بودن k_i، $r_i = ۰$ یا $r_i = ۱$.]

۱۷. نشان دهید که هر عدد صحیح n را می‌توان به‌صورت $n = ۲^k m$ نوشت، که $k \geq ۰$ و m عدد صحیح فردی است.

۱۸. براساس شواهد عددی، به‌نظر می‌رسد تعداد عددهای اول pای که به‌ازای آنها $p + ۵۰$ نیز اول است، نامتناهی است. ۱۵ تا از این عددهای اول را بنویسید.

۳ـ۲ غربال اراتستن

چگونه می‌توانیم اول بودن یا مرکب بودن عدد صحیح داده شده‌ای را تعیین کنیم، و در صورت مرکب بودن عدد، چگونه می‌توانیم عملاً مقسوم‌علیهی نابدیهی از آن را به‌دست آوریم؟ بدیهی‌ترین روش عبارت از تقسیم متوالی عدد صحیح مورد بحث بر هر یک از عددهای ماقبل آن است؛ اگر هیچ یک از آنها (بجز ۱) مقسوم علیه عدد موردنظر نباشد، عدد صحیح مزبور اول است. این روش اگر چه توصیفش بسیار ساده است، در عمل آنقدر سودمند نیست. زیرا حتی اگر هراسی از محاسبهٔ طولانی نداشته باشیم، میزان زمان و کار لازم ممکن است مقرون به‌صرفه نباشد.

عددهای مرکب خاصیتی دارند که می‌توان با استفاده از آنها محاسبه‌های لازم را کاهش داد ــ مع‌الوصف فرایند بازهم کسل‌کننده خواهد بود. اگر عدد صحیح $a > ۱$ای مرکب باشد، می‌توان آن‌را به‌صورت $a = bc$، به‌طوری که $۱ < b < a$ و $۱ < c < a$، نوشت. به‌فرض $b \leq c$، نتیجه می‌گیریم $b^۲ \leq bc = a$ و بنابراین $b \leq \sqrt{a}$. چون $b > ۱$، بنا به قضیهٔ ۳ـ۲، b دارای حداقل یک عامل اول p است. پس $p \leq b \leq \sqrt{a}$؛ به‌علاوه، چون $p|b$ و $b|a$، نتیجه می‌شود که $p|a$. جان کلام این است: هر عدد مرکب a همیشه دارای مقسوم‌علیه اول pای صادق در $p \leq \sqrt{a}$ است.

بنابراین در آزمون اول بودن عدد صحیح مفروض $a > ۱$، کافی است a را بر عددهای اول نابیشتر از $\sqrt{a}$ تقسیم کرد (البته به فرض در دسترس بودن فهرست عددهای اول نابیشتر از $\sqrt{a}$). این مطلب با درنظرگرفتن عدد صحیح $a = ۵۰۹$ روشن می‌شود. چون $۲۲ < \sqrt{۵۰۹} < ۲۳$،

کافی است عددهای اول نابیشتر از ۲۲ را به‌عنوان مقسوم‌علیه‌های احتمالی آزمایش کنیم؛ یعنی، عددهای اول ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹ را. با تقسیم متوالی ۵۰۹ بر هر یک از اینها، متوجه می‌شویم که هیچ یک مقسوم‌علیه ۵۰۹ نیست. نتیجه این است که ۵۰۹ عددی اول است.

مثال ۳ـ۱

روش اخیر الذکر، وسیله‌ای عملی برای تعیین صورت متعارف عددهای صحیح است؛ مثلاً $a = ۲۰۹۳$ را درنظر بگیرید. چون $۴۵ < \sqrt{۲۰۹۳} < ۴۶$، کافی است عددهای اول ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۹، ۲۳، ۳۱، ۳۷، ۴۱، ۴۳ را آزمایش کنیم. با آزمایش معلوم می‌شود که نخستین مقسوم‌علیه ۲۰۹۳ در میان اینها ۷ است و $۲۰۹۳ = ۷ \times ۲۹۹$. در مورد عدد صحیح ۲۹۹، هفت عدد اول کوچکتر از ۱۸ (توجه کنید که $۱۷ < \sqrt{۲۹۹} < ۱۸$) عبارت‌اند از ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷. نخستین مقسوم‌علیه اول ۲۹۹ عدد صحیح ۱۳ است و، پس از تقسیم لازم، به‌دست می‌آوریم $۲۹۹ = ۱۳ \times ۲۳$. ولی خود ۲۳ عددی اول است، پس ۲۰۹۳ دارای دقیقاً سه عامل اول ۷، ۱۳، و ۲۳ است:

$$۲۰۹۳ = ۷ \times ۱۳ \times ۲۳ \qquad \blacksquare$$

اراتستن از اهالی کورنه[1] (۲۷۶ـ۱۹۴ پیش از میلاد مسیح)، ریاضیدان یونانی دیگری است که کار او در نظریهٔ اعداد هنوز هم اهمیت دارد. گرچه نسلهای بعدی بیشتر از او به‌عنوان سرپرست کتابخانهٔ اسکندریه، که معروفیتی جهانی داشت، یاد کرده‌اند، اراتستن در همهٔ زمینه‌های علمی، اگر هم سرآمد نبود، استعداد و قریحه‌ای داشت؛ در زمان خود به «بتا» معروف بود، زیرا معروف بود که در هر زمینه‌ای لااقل مقام دوم را دارد. شاید جالبترین دستاورد اراتستن محاسبهٔ دقیق محیط کرهٔ زمین از طریق کاربرد ساده‌ای از هندسهٔ اقلیدسی باشد.

دیدیم که اگر عدد صحیح $a > ۱$ بر هیچ عدد اولی چون $p \leq \sqrt{a}$ بخشپذیر نباشد، آنگاه a لزوماً اول است. اراتستن با استفاده از این نکته روش هوشمندانه‌ای، موسوم به "غربال اراتستن"، برای تعیین همهٔ عددهای اول کوچکتر از عدد صحیح داده شدهٔ n ابداع کرد. براساس این روش، باید همهٔ عددهای صحیح از ۲ تا n را از کوچک به بزرگ نوشت و سپس، به نوبت با خط زدن مضربهای $۲p$، $۳p$، $۴p$، $۵p$، ... از عددهای اول p، $p \leq \sqrt{n}$، همهٔ عددهای مرکب را حذف کرد. عددهای صحیحی که باقی می‌مانند ــ یعنی عددهایی که در "غربال" می‌مانند ــ اول‌اند.

به‌عنوان مثالی از نحوهٔ اجرای این روش، فرض کنید بخواهیم همهٔ عددهای اول نابیشتر از ۱۰۰ را بیابیم. دنبالهٔ عددهای صحیح متوالی ۲، ۳، ...، ۱۰۰ را درنظر بگیرید. با توجه به اینکه ۲ اول

1. Cyrene

است، با خط زدن همهٔ مضربهای ۲، بجز ۲، از فهرست آغاز می‌کنیم. نخستین عدد صحیح باقیمانده ۳ است، که اول است. بجز ۳، همهٔ مضربهای دیگر ۳ را خط می‌زنیم، بنابراین، ۹، ۱۵، ۲۱، . . . حذف می‌شوند (مضربهای زوج ۳ در مرحلهٔ قبل حذف شده‌اند). کوچکترین عدد صحیح بعد از ۳، که هنوز حذف نشده است، ۵ است. ۵ بر ۲ یا ۳ بخشپذیر نیست ــ وگرنه حذف شده بود ــ پس ۵ نیز اول است. همهٔ مضربهای ۵ بجز خود ۵ مرکب‌اند، پس خود ۵ را نگاه می‌داریم و ۱۰، ۱۵، ۲۰، . . . را حذف می‌کنیم (البته، برخی از اینها پیشتر حذف شده‌اند). نخستین عدد صحیح حذف نشده، که ۷ است، اول است، زیرا بر ۲، ۳ و ۵ یعنی تنها عددهای اول کوچکتر از خود بخشپذیر نیست. پس از حذف مضربهای ۷ بجز خود ۷ که بزرگترین عدد اول کوچکتر از ۱۰ $= \sqrt{۱۰۰}$ است، همهٔ عددهای صحیح مرکب در دنبالهٔ ۲، ۳، ۴، . . .، ۱۰۰ از غربال حذف شده‌اند. همهٔ عددهای صحیح باقیمانده، یعنی ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳، ۲۹، ۳۱، ۳۷، ۴۱، ۴۳، ۴۷، ۵۳، ۵۹، ۶۱، ۶۷، ۷۱، ۷۳، ۷۹، ۸۳، ۸۹، ۹۷، همهٔ عددهای اول کوچکتر از ۱۰۰ هستند.

جدول زیر نتیجهٔ نهایی غربال را نشان می‌دهد. در این جدول، مضربهای ۲ با ＼، مضربهای ۳ با ／، مضربهای ۵ با ــــ ، و مضربهای ۷ با ~ حذف شده‌اند.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

پرسشی که در این مقطع، به‌طور طبیعی، به‌ذهن خواننده متبادر می‌شود این است: آیا بزرگترین عدد اول وجود دارد، یا عددهای اول تا بینهایت ادامه دارند؟ پاسخ را می‌توان در اثبات بسیار ساده‌ای از اقلیدس درمقالهٔ نهم اصول او جستجو کرد. استدلال اقلیدس را عموماً الگویی از ظرافت ریاضی به‌حساب می‌آورند. این استدلال چنین است: به‌ازای هر مجموعهٔ متناهی از عددهای اول، همیشه می‌توان عدد اولی غیرمتعلق به مجموعه پیدا کرد؛ پس، تعداد عددهای اول نامتناهی است. جزئیات دقیق استدلال در زیر می‌آید.

قضیهٔ ۳ـ۴ (اقلیدس). تعداد عددهای اول نامتناهی است.

اثبات. اثبات اقلیدس مبتنی‌بر استفاده از تناقض است. فرض کنید $p_۱ = ۲$، $p_۲ = ۳$، $p_۳ = ۵$، $p_۴ = ۷$، ... عددهای اول به‌ترتیب صعودی باشند، و بزرگترین عدد اول وجود داشته باشد که آن‌را p_n می‌نامیم. عدد صحیح مثبت

$$N = p_۱p_۲\dots p_n + ۱$$

را درنظر بگیرید. چون $N > ۱$، از قضیهٔ ۳ـ۲ نتیجه می‌گیریم که N بر عدد اول pای بخشپذیر است. چون $p_۱$،$p_۲$،...،p_n کل عددهای طبیعی‌اند، p بایستی یکی از $p_۱$،$p_۲$،...،p_n باشد. از مقایسهٔ $p|p_۱p_۲\dots p_n$ و $p|N$، نتیجه می‌گیریم که $p|N - p_۱p_۲\dots p_n$، یا $p|۱$. تنها مقسوم‌علیه مثبت عدد صحیح ۱ خود ۱ است و، چون $p > ۱$، به تناقض می‌رسیم. پس هیچ مجموعهٔ متناهی از عددهای اول شامل همهٔ آنها نیست، بنابراین تعداد عددهای اول نامتناهی است. □

به‌ازای هر عدد اول p، $p^\#$ را حاصلضرب همهٔ عددهای اول نابیشتر از p تعریف می‌کنیم. عددهای به‌صورت $p^\# + ۱$ را می‌توان "عددهای اقلیدسی" لقب داد، زیرا در استدلال اقلیدس به‌منظور اثبات نامتناهی بودن تعداد عددهای اول دیده می‌شوند. جالب توجه است که ۵تای نخست این عددهای صحیح، یعنی

$$۲^\# + ۱ = ۲ + ۱ = ۳$$
$$۳^\# + ۱ = ۲ \times ۳ + ۱ = ۷$$
$$۵^\# + ۱ = ۲ \times ۳ \times ۵ + ۱ = ۳۱$$
$$۷^\# + ۱ = ۲ \times ۳ \times ۵ \times ۷ + ۱ = ۲۱۱$$
$$۱۱^\# + ۱ = ۲ \times ۳ \times ۵ \times ۷ \times ۱۱ + ۱ = ۲۳۱۱$$

همگی عددهایی اول هستند. ولی، هیچ یک از عددهای

$$۱۳^\# + ۱ = ۵۹ \times ۵۰۹$$
$$۱۷^\# + ۱ = ۱۹ \times ۹۷ \times ۲۷۷$$
$$۱۹^\# + ۱ = ۳۴۷ \times ۲۷۹۵۳$$

اول نیستند. اینکه تعداد عددهای اولی چون p، که به‌ازای آن $p^{\#} + ۱$ نیز اول است، نامتناهی است یا نه، پرسشی است که پاسخ آن هنوز معلوم نیست. و در ارتباط با آن، پرسشی مطرح می‌شود که آیا تعداد عددهای $p^{\#} + ۱$ که مرکب‌اند نامتناهی است؟

در حال حاضر، پانزده عدد اول به‌صورت $p^{\#} + ۱$ شناخته شده‌اند. این عددها متناظرند با

$$p = ۲, ۳, ۵, ۷, ۱۱, ۳۱, ۳۷۹, ۱۰۱۹, ۱۰۲۱, ۲۶۵۷, ۳۲۲۹, ۴۵۴۷, ۴۷۸۷, ۱۱۵۴۹, ۱۳۶۴۹$$

و ۱۳۶۴۹ بزرگترین اینهاست که در ۱۹۸۷ کشف شده است؛ به‌ازای هر $p \leq ۱۷۱۵۹$ بجز اینها، $p^{\#} + ۱$ مرکب است.

برای ما قضیهٔ اقلیدس مهمتر از آن است که فقط به یک اثبات آن بسنده کنیم. اکنون اثبات دیگری از آن ارائه می‌کنیم. دنبالهٔ نامتناهی عددهای صحیح مثبت زیر

$$\begin{aligned}
n_۱ &= ۲\\
n_۲ &= n_۱ + ۱\\
n_۳ &= n_۱n_۲ + ۱\\
n_۴ &= n_۱n_۲n_۳ + ۱\\
&\vdots\\
n_k &= n_۱n_۲\dots n_{k-۱} + ۱\\
&\vdots
\end{aligned}$$

را درنظر بگیرید. چون $n_k > ۱$، هر یک از این عددهای صحیح بر عددی اول بخشپذیرند. ولی هیچ دو n_kای مقسوم‌علیه اول مشترکی ندارند. برای اثبات این مطلب، قرار می‌دهیم $d = \gcd(n_i, n_k)$، و فرض می‌کنیم $i < k$. چون d مقسوم‌علیه n_i است، باید $n_۱n_۲\dots n_{k-۱}$ را بشمارد. و چون $d|n_k$، از قضیهٔ ۲ـ۲(۷) نتیجه می‌شود که $d|n_k - n_۱n_۲\dots n_{k-۱}$ و بنابراین $d|۱$. پس، $d = ۱$ و در نتیجه عددهای صحیح n_k $(k = ۱, ۲, \dots)$ دو به دو متباین‌اند. پس به‌همان تعداد عددهای صحیح n_k، عدد اول وجود دارد، یعنی، تعداد عددهای اول نامتناهی است.

فرض کنید p_n، nامین عدد اول در دنبالهٔ طبیعی عددهای اول باشد. بنا به اثبات اقلیدس، تقریبی از مقدار p_n عبارت است از

$$p_{n+۱} \leq p_۱p_۲\dots p_n + ۱ < p_n^n + ۱$$

به‌عنوان مثال، اگر $n = ۳$، بنا به نابرابری فوق داریم

$$۷ = p_۴ < p_۳^۳ + ۱ = ۵^۳ + ۱ = ۱۲۶$$

به‌طوری که دیده می‌شود، این تقریب خیلی نامعقول است. قضیه زیر تقریب بهتری از اندازهٔ p_n ارائه می‌کند.

قضیهٔ ۳ـ۵ اگر p_n، nامین عدد اول باشد، آنگاه $p_n \leq ۲^{۲^{n-۱}}$.

اثبات. به استقرای قوی روی n عمل می‌کنیم. نابرابری عنوان شده به‌ازای $n = ۱$ به‌وضوح برقرار است. به‌عنوان فرض استقرا، فرض می‌کنیم $n > ۱$ و حکم به‌ازای هر عدد صحیح کوچکتر از n برقرار است. در این صورت

$$\begin{aligned} p_{n+۱} &\leq p_۱ p_۲ \ldots p_n + ۱ \\ &\leq ۲ \times ۲^۲ \times \ldots \times ۲^{۲^{n-۱}} + ۱ = ۲^{۱+۲+۲^۲+\ldots+۲^{n-۱}} + ۱ \end{aligned}$$

پس با استفاده از اتحاد $۱ + ۲ + ۲^۲ + \ldots + ۲^{n-۱} = ۲^n - ۱$ داریم

$$p_{n+۱} \leq ۲^{۲^n - ۱} + ۱$$

ولی به‌ازای هر n، $۱ \leq ۲^{۲^n - ۱}$. پس

$$\begin{aligned} p_{n+۱} &\leq ۲^{۲^n-۱} + ۲^{۲^n-۱} \\ &= ۲ \times ۲^{۲^n-۱} = ۲^{۲^n} \end{aligned}$$

مرحلهٔ استقرا، و کل استدلال به انجام رسیده است. □

قضیهٔ ۳ـ۵ نتیجهٔ جالبی دارد.

فرع. به‌ازای هر $n \geq ۱$ حداقل $n + ۱$ عدد اول کوچکتر از $۲^{۲^n}$ وجود دارد.

اثبات. بنا به قضیه، می‌دانیم که $p_۱$، $p_۲$، ...، $p_{n+۱}$ همگی کوچکتر از $۲^{۲^n}$اند. □

عددهای اول خاصی همواره مورد توجه بوده‌اند. در میان اینها، عددهای اولِ مرکب از ارقام یک، به لحاظ سادگی ظاهر، بیشتر جلب توجه می‌کنند. عدد مرکب از ارقام یک، عدد صحیحی است که (در دستگاه دهدهی) به‌صورت دنباله‌ای از ۱ ها نوشته می‌شود، مانند ۱۱، ۱۱۱ یا ۱۱۱۱.

هر چنین عدد صحیحی بایستی به‌صورت $(۱۰^n - ۱)/۹$ باشد. چنین عددی را اگر متشکل از n رقم ۱ متوالی باشد با R_n نشان می‌دهیم[۱]. از ویژگیهای عجیب این عددها این است که عددهای اول در میان آنها نادرند. تاکنون، فقط

$$R_۲ ، R_{۱۹} ، R_{۲۳} ، R_{۳۱۷} \text{ و } R_{۱۰۳۱}$$

به‌عنوان عدد اول شناخته شده‌اند (آخری در سال ۱۹۸۵). معلوم شده است که به‌ازای $n \leq ۱۰۰۰۰$، پنج عدد فوق تنها عددهای اول مرکب از ارقام یک هستند. حدسی نیز راجع به وجود عددهای اول دیگری که از این نوع باشند، زده نشده است. برای اینکه عدد R_nای اول باشد، لازم است که اندیس n اول باشد. ولی این شرط کافی نیست زیرا

$$R_۵ = ۱۱۱۱۱ = ۴۱ \times ۲۷۱ ، R_۷ = ۱۱۱۱۱۱۱ = ۲۳۹ \times ۴۶۴۹$$

تمرینهای ۳ـ۲

۱. اول بودن عدد صحیح ۷۰۱ را با آزمایش همهٔ عددهای اول $p \leq \sqrt{۷۰۱}$ به‌عنوان مقسوم‌علیه‌های احتمالی بررسی کنید. همین کار را در مورد عدد صحیح ۱۰۰۹ انجام دهید.

۲. با استفاده از غربال اراتستن، همهٔ عددهای اول میان ۱۰۰ و ۲۰۰ را به‌دست آورید.

۳. به فرض $p \nmid n$ به‌ازای هر عدد اول $p \leq \sqrt[۳]{n}$، نشان دهید n یا عددی اول و یا حاصلضرب دو عدد اول است. [راهنمایی: فرض کنید برخلاف این حکم، n دارای حداقل سه عامل اول است.]

۴. حکمهای زیر را ثابت کنید

(الف) به‌ازای هر عدد اول p، عدد $\sqrt{p}$ گنگ است.

(ب) اگر $a > ۰$ و $\sqrt[n]{a}$ گویا باشد، آنگاه $\sqrt[n]{a}$ باید عددی صحیح باشد.

(پ) به‌ازای $n \geq ۲$، $\sqrt[n]{n}$ گنگ است. [راهنمایی: از نابرابری $۲^n > n$ استفاده کنید.]

۵. نشان دهید که هر عدد مرکب سه‌رقمی باید دارای عامل اولی کوچکتر از ۳۱ یا برابر آن باشد.

۶. اثبات زیر از نامتناهی بودن عددهای اول را کامل کنید: فرض کنید فقط تعدادی متناهی عدد اول وجود دارد، مثلاً $p_۱، p_۲، \ldots، p_n$. و نیز فرض کنید A حاصلضرب rتای دلخواه از این عددهای اول باشد و قرار دهید $B = p_۱ p_۲ \ldots p_n / A$. در این صورت هر p_kای فقط یکی از A و B را می‌شمارد. چون $A + B > ۱$، $A + B$ دارای مقسوم‌علیه اولی بجز p_kهاست، و این تناقض است.

---

۱. R حرف اول کلمهٔ Repunit (یعنی مرکب از ارقام مکرر یک) است.

۷. اثبات اقلیدس در مورد نامتناهی بودن تعداد عددهای اول را برمبنای فرض وجود بزرگترین عدد اول p و استفاده از عدد صحیح $N = p! + ۱$ طوری تنظیم کنید که به تناقض برسید.

۸. برای اثبات دیگری از نامتناهی بودن تعداد عددهای اول فرض کنید فقط تعداد متناهی عدد اول، مثلاً، $p_۱$، ...، p_n، وجود دارند و با استفاده از عدد صحیح

$$N = p_۲p_۳\dots p_n + p_۱p_۳\dots p_n + \dots + p_۱p_۲\dots p_{n-۱}$$

به تناقض برسید.

۹. (الف) ثابت کنید که اگر $n > ۲$، عدد اول pای وجود دارد که $n < p < n!$. [راهنمایی: اگر $n! - ۱$ اول نباشد، آنگاه دارای مقسوم‌علیه اول pای است؛ و از $p \leq n$ نتیجه می‌شود $p|n!$، که به تناقض می‌انجامد.]

(ب) اگر $n > ۱$، نشان دهید که هر مقسوم‌علیه اول $n! + ۱$ عدد صحیح فردی بزرگتر از n است.

۱۰. فرض کنید q_n کوچکترین عدد اول بزرگتر از $P_n = p_۱p_۲\dots p_n + ۱$ است. حدس زده شده است که تفاضل $q_n - (p_۱p_۲\dots p_n)$ همیشه عددی اول است. درستی این حدس را به‌ازای پنج مقدار نخست n نشان دهید.

۱۱. اگر p_n، nامین عدد اول باشد، قرار دهید $d_n = p_{n+۱} - p_n$. اینکه آیا تعداد جوابهای معادلهٔ $d_n = d_{n+۱}$ نامتناهی است، پرسشی است که هنوز پاسخی نیافته است؛ پنج جواب این معادله را به‌دست آورید.

۱۲. به فرض اینکه p_n، nامین عدد اول باشد، هر یک از حکمهای زیر را ثابت کنید:

(الف) اگر $n \geq ۵$، آنگاه $p_n > ۲n - ۱$.

(ب) هیچ یک از عددهای صحیح $P_n = p_۱p_۲\dots p_n + ۱$ مربع کامل نیست. [راهنمایی: هر یک از P_nها به‌صورت $۴k + ۳$ است.]

(پ) مجموع

$$\frac{۱}{p_۱} + \frac{۱}{p_۲} + \dots + \frac{۱}{p_n}$$

هرگز عدد صحیح نیست.

۱۳. (الف) در مورد عددهای R_n که مرکب از n رقم یک‌اند، ثابت کنید که اگر $k|n$، آنگاه $R_k|R_n$. [راهنمایی: اگر $n = kr$، اتحاد

$$x^n - ۱ = (x^k - ۱)(x^{(r-۱)k} + x^{(r-۲)k} + \dots + x^k + ۱)$$

را درنظر بگیرید.]

(ب) با استفاده از قسمت (الف) عاملهای اول $R_{۱۰}$ را که مرکب از ۱۰ رقم یک است به‌دست آورید.

۳ـ۳ حدس گولدباخ

گرچه بینهایت عدد اول وجود دارد، توزیع آنها در میان عددهای صحیح مثبت فوق‌العاده پیچیده است. در بررسی توزیع این اعداد به کرات به نشانه‌ها یا شاید بشود گفت اشباحی از یک الگو برمی‌خوریم ولی الگویی واقعی که توصیف دقیق آن میسر باشد هنوز پیدا نشده است. تفاضل میان عددهای اول متوالی ممکن است کوچک باشد، مثلاً میان زوجهای ۱۱ و ۱۳، ۱۷ و ۱۹، یا ۱۰۰۰۰۰۰۰۰۰۰۶۱ و ۱۰۰۰۰۰۰۰۰۰۰۶۳. در عین حال بازه‌های به‌اندازهٔ دلخواه طویل در دنبالهٔ عددهای صحیح موجودند که کاملاً عاری از هر عدد اولی هستند.

پاسخ این پرسش دانسته نیست که آیا تعداد زوجهای عددهای اول دوقلو، یعنی زوجهای متشکل از عددهای فرد p و $p+۲$ که هر دو اول باشند، نامتناهی است یا نه. شواهد عددی دلالت به مثبت بودن پاسخ می‌کنند. با استفاده از کامپیوتر تعداد ۱۵۲۸۹۲ جفت عدد اول دوقلو کوچکتر از ۳۰۰۰۰۰۰۰ و بیست جفت بین $۱۰^{۱۲}$ و $۱۰^{۱۲} + ۱۰۰۰۰$ پیدا شده است که نشان می‌دهد تعداد این جفتها با بزرگ شدن عددهای صحیح مثبت، کمتر می‌شود. مثالهایی از دوقلوهای بسیار بزرگ شناخته شده‌اند. بزرگترینشان تا امروز

$$۱۰۷۵۷۰۴۶۳ \times ۱۰^{۲۲۵۰} \pm ۱$$

اند، که هر یک دارای ۲۲۵۹ رقم دهدهی‌اند، و در ۱۹۸۵ کشف شدند.

عددهای اول متوالی نه تنها ممکن است به یکدیگر خیلی نزدیک باشند، بلکه ممکن است از هم خیلی دور نیز باشند؛ یعنی فاصله‌هایِ به‌دلخواه بزرگ نیز ممکن است میان عددهای اول متوالی وجود داشته باشد. دقیقتر بگوییم: به‌ازای هر عدد صحیح مثبت n، n عدد صحیح متوالی که همگی مرکب باشند، وجود دارد. برای اثبات این، کافی است عددهای صحیح

$$(n+۱)! + ۲, (n+۱)! + ۳, \ldots, (n+۱)! + (n+۱)$$

را، که در آنها $(n+۱)! = (n+۱)n \times \ldots \times ۳ \times ۲ \times ۱$، درنظر بگیریم. این عددها تعدادشان n است و متوالی‌اند. آنچه مهم است، مرکب بودن هر یک از آنهاست؛ $(n+۱)! + ۲$ بر ۲ بخشپذیر است، $(n+۱)! + ۳$ بر ۳ بخشپذیر است، و الی آخر.

به‌عنوان نمونه، اگر دنباله‌ای از چهار عدد صحیح متوالی مرکب را بخواهیم، آنگاه با استدلال فوق، عددهای ۱۲۲، ۱۲۳، ۱۲۴، و ۱۲۵ به‌دست می‌آیند

$$۵! + ۲ = ۱۲۲ = ۲ \times ۶۱$$
$$۵! + ۳ = ۱۲۳ = ۳ \times ۴۱$$
$$۵! + ۴ = ۱۲۴ = ۴ \times ۳۱$$
$$۵! + ۵ = ۱۲۵ = ۵ \times ۲۵$$

البته، می‌توان مجموعه‌های دیگری متشکل از چهار عدد مرکب متوالی به‌دست آورد. مثلاً، ۲۴، ۲۵، ۲۶، ۲۷ یا ۳۲، ۳۳، ۳۴، ۳۵.

همان‌طورکه این مثال نشان می‌دهد،روش ما برای تعیین فاصله‌های بین عددهای اول متوالی، تقریب بسیار خامی از محل ظهور آنها در میان عددهای صحیح به‌دست می‌دهد. اخیراً فاصلهٔ بزرگی به طول ۶۵۴ (یعنی، $p_{n+۱} - p_n = ۶۵۴$) که در آن هیچ عدد اولی وجود ندارد، بعد از عدد اول ۱۱۰۰۰۰۰۱۴۴۶۶۱۳۳۵۳ کشف شد؛ پیش از این عدد، فقط فاصله‌های کوچکتر قرار دارند. به‌طور نظری، فاصله‌ای به‌طول حداقل ۶۵۴ را می‌توان بعد از عدد صحیح $۶۵۴! + ۱$ به‌دست آورد، ولی چون $۶۵۴! \sim (۱٫۴۷)۱۰^{۱۵۵۹}$، این نکته ارزش عملی چندانی ندارد.

بنابراین، به مسألهٔ حل نشدهٔ دیگری مربوط به عددهای اول، یعنی، حدس گولدباخ، می‌رسیم. کریستیان گولدباخ در نامه‌ای به اویلر (در ۱۷۴۲ میلادی) این حدس را مطرح کرد که هر عدد صحیح زوج مجموع دو عدد است که یا اول، یا ۱اند. صورت نسبتاً کلیتر حدس این است که هر عدد صحیح زوج بزرگتر از ۴ را می‌توان به‌صورت مجموع دو عدد اول فرد نوشت. به‌آسانی می‌توان صحت حدس فوق را در مورد چند عدد زوج نخست تحقیق کرد:

$$۲ = ۱ + ۱$$
$$۴ = ۲ + ۲ = ۱ + ۳$$
$$۶ = ۳ + ۳ = ۱ + ۵$$
$$۸ = ۳ + ۵ = ۱ + ۷$$
$$۱۰ = ۳ + ۷ = ۵ + ۵$$
$$۱۲ = ۵ + ۷ = ۱ + ۱۱$$
$$۱۴ = ۳ + ۱۱ = ۷ + ۷ = ۱ + ۱۳$$

$$۱۶ = ۳ + ۱۳ = ۵ + ۱۱$$
$$۱۸ = ۵ + ۱۳ = ۷ + ۱۱ = ۱ + ۱۷$$
$$۲۰ = ۳ + ۱۷ = ۷ + ۱۳ = ۱ + ۱۹$$
$$۲۲ = ۳ + ۱۹ = ۵ + ۱۷ = ۱۱ + ۱۱$$
$$۲۴ = ۵ + ۱۹ = ۷ + ۱۷ = ۱۱ + ۱۳ = ۱ + ۲۳$$
$$۲۶ = ۳ + ۲۳ = ۷ + ۱۹ = ۱۳ + ۱۳$$
$$۲۸ = ۵ + ۲۳ = ۱۱ + ۱۷$$
$$۳۰ = ۷ + ۲۳ = ۱۱ + ۱۹ = ۱۳ + ۱۷ = ۱ + ۲۹$$

به‌نظر می‌رسد که اویلر هرگز برای حل مسأله اقدام نکرده است، ولی در نامه‌ای که بعداً به گولدباخ نوشت، متقابلاً حدسی از خود ارائه کرد: هر عدد صحیح زوج ناکمتر از ۶ به‌صورت $۴n + ۲$، مجموع دو عدد است که هر یک یا عددی اول به‌صورت $۴n + ۱$ و یا ۱ است.

اطلاعات عددی بسیار زیادی در تأیید حدس گولدباخ به‌دست آمده است. با محاسبهٔ مستقیم، درستی آن به‌ازای هر عدد صحیح زوج کوچکتر از $۱۰^۸$ به تأیید رسیده است. معلوم شده است که بیشتر عددهای زوج $۲m$، $۱۰^۸ > ۲m > ۰$، مجموع یک عدد اول «کوچک» (یعنی، یکی از ۱۵۰ عدد اول نخست) و عدد اولی نسبتاً نزدیک به $۲m$ هستند. گرچه این مشاهده این گمان را که حدس گولدباخ درست است تقویت می‌کند، با اثبات ریاضی آن فاصلهٔ زیادی دارد، و همهٔ تلاشها برای اثبات آن با شکست کامل مواجه شده است. گادفری هرلد هاردی[1]، که از معروفترین متخصصان نظریهٔ اعداد این سده است، در سخنرانی خود در انجمن ریاضی کپنهاک در سال ۱۹۲۱ اظهار کرد که حدس گولدباخ "به اندازهٔ هر مسالهٔ حل نشدهٔ دیگر ریاضی" مشکل به‌نظر می‌رسد.

اضافه می‌کنیم که اگر حدس گولدباخ درست باشد، هر عدد فرد بزرگتر از ۷ باید مجموع سه عدد اول باشد؛ زیرا اگر n عدد صحیح فردی بزرگتر از ۷ باشد، آنگاه $n - ۳$ عدد زوجی بزرگتر از ۴ است؛ حال اگر $n - ۳$ قابل بیان به‌صورت مجموع دو عدد فرد اول باشد، آنگاه n مجموع سه عدد اول است.

نخستین پیشرفت واقعی در زمینهٔ این حدس در طی تقریباً ۲۰۰ سال، در سال ۱۹۲۲ با مساعی هاردی و لیتل‌وود[2] حاصل شد. آنها برمبنای فرض اثبات نشده‌ای، معروف به تعمیم فرض ریمان، نشان دادند که هر عدد فرد به‌اندازهٔ کافی بزرگ مجموع سه عدد اول فرد است. در سال

1. G. H. Hardy 2. Littlewood

۱۹۳۷، وینوگرادوف[1]، ریاضیدان روس، توانست با کنار گذاشتن تعمیم فرض ریمان، اثباتی نامشروط برای این حکم ارائه دهد، یعنی، ثابت کرد n_0ای وجود دارد که عملاً قابل محاسبه است و هر عدد صحیح فردِ بزرگتر از آن را می‌توان به‌صورت مجموع سه عدد اول فرد نوشت.

$$n = p_1 + p_2 + p_3 \qquad (n \text{ فرد، } n \text{ به اندازهٔ کافی بزرگ})$$

وینوگرادوف نتوانست میزان بزرگی n_0 را تعیین کند، ولی بوروتسکین[2] (در سال ۱۹۵۶) ثابت کرد که $n_0 < 3^{3^{15}}$. از اینجا بیدرنگ نتیجه می‌شود که هر عدد زوج از مرحله‌ای به بعد مجموع دو یا چهار عدد اول است. بنابراین، کافی است مسأله را به‌ازای هر عدد فرد n در محدودهٔ $9 \leq n \leq n_0$، بررسی کرد، ولی این بررسی به‌ازای عدد صحیح داده شده‌ای، به‌صورت محاسبهٔ کسالت‌آوری در می‌آید (متأسفانه، n_0 به‌اندازه‌ای بزرگ است که این کار فراتر از توان پیشرفته‌ترین کامپیوترهاست).

مسألهٔ دیگری که ارتباط نزدیکی به حدس گولدباخ دارد این است که آیا هر عدد زوج مجموع دو عدد "تقریباً اول" است، یعنی مجموع دو عدد صحیحی که هیچ یک بیش از تعداد معینی عامل اول ندارد، یا خیر. هر چه تعداد عاملهای اول کمتر باشد، نتیجه بهتر است. نخستین قضیه از این نوع را برون[3] (در سال ۱۹۲۰) ثابت کرد. او نشان داد که هر عدد زوج به‌اندازهٔ کافی بزرگ را می‌توان به‌صورت مجموع دو عدد، هر یک با حداکثر ۹ عامل اول، نوشت. بعداً، بوکستاب[4] (۱۹۴۰) با تقلیل تعداد عاملهای اول به ۴ نتیجهٔ فوق را قویتر کرد.

در سال ۱۹۴۸ رنی[5] ریاضیدان مجارستانی، ثابت کرد که هر عدد صحیح زوجِ به اندازهٔ کافی بزرگ n، مجموع یک عدد اول و یک عدد "تقریباً اول" است:

$$n = p + p_1 p_2 \dots p_r \qquad (n \text{ زوج، } n \text{ به‌اندازه کافی بزرگ})$$

در اثبات رنی، r خیلی بزرگ است. اگر بتوان نشان داد که $r = 1$، می‌توان حدس گولدباخ را به‌ازای هر n بزرگ نتیجه گرفت. بعداً وانگ[6] (در سال ۱۹۵۹) r را به $r \leq 4$ و وینوگرادوف[7] (در سال ۱۹۶۵) r را به $r \leq 3$ تقلیل داد. نزدیکترین نتیجه به اثبات این حدس که با این روش به‌دست آمده نتیجهٔ (۱۹۶۶) چن‌جینگ ـ رون[8] است که می‌گوید $r \leq 2$. به گفتهٔ دیگر، از جایی به بعد، هر عدد صحیح زوج مجموع یک عدد اول و حاصلضرب حداکثر دو عدد اول است. اثبات

1. I. M. Vinogradov 2. Borozdkin 3. Brun

4. Buchstab 5. Renyi 6. Wang 7. A. I. Vinogradov

8. Chen Jing-Run

اولیهٔ چن بسیار طولانی بود، ولی او در ۱۹۷۳ استدلال خود را بهتر کرد و طولش را به ۲۰ صفحه کاهش داد.

به‌دلیل وجود شواهد قوی به‌سود حدس معروف گولدباخ، به‌راحتی قانع می‌شویم که این حدس درست است. با این حال ممکن است نادرست باشد. وینوگرادوف نشان داد که اگر $A(x)$ تعداد عددهای صحیح زوج $n \leq x$ای باشد که به‌صورت مجموع دو عدد اول نیستند، آنگاه

$$\lim_{x \to \infty} \frac{A(x)}{x} = ۰$$

به استناد این می‌توانیم بگوییم که "تقریباً همهٔ" عددهای صحیح زوج در حدس گولدباخ صدق می‌کنند. ادموند لانداو[1] چه خوب گفته است که: "حدس گولدباخ به‌ازای حداکثر ۰٪ همهٔ عددهای صحیح زوج نادرست است"؛ البته، این «حداکثر» ۰٪، احتمال وجود بینهایت استثنا را نفی نمی‌کند.

قدری از بحث اصلی دور افتادیم. توجه کنید که بنا به الگوریتم تقسیم، هر عدد صحیح مثبت را می‌توان به‌طور یکتا به یکی از صورتهای

$$۴n،\ ۴n + ۱،\ ۴n + ۲،\ ۴n + ۳$$

به‌ازای یک $n \geq ۰$ مناسب، نوشت. عددهای صحیح $۴n$ و $۴n + ۲ = ۲(۲n + ۱)$ هر دو به وضوح زوج‌اند. پس، عددهای صحیح فرد در قالب دو تصاعد ظاهر می‌شوند: یکی متشکل از عددهای صحیح به‌صورت $۴n + ۱$

$$۱،\ ۵،\ ۹،\ ۱۳،\ ۱۷،\ ۲۱،\ \ldots$$

و دیگری متشکل از عددهای صحیح به‌صورت $۴n + ۳$

$$۳،\ ۷،\ ۱۱،\ ۱۵،\ ۱۹،\ ۲۳،\ \ldots$$

هر یک از این دو تصاعد به‌وضوح شامل تعدادی عدد اول است، اما این پرسش مطرح می‌شود که آیا تعداد عددهای اول در هر یک از آنها نامتناهی است؟ این پرسش فرصت مناسبی برای کاربرد دوبارهٔ روش اقلیدس در اثبات وجود تعدادی نامتناهی عدد اول فراهم می‌کند. با تغییری جزئی در استدلال اقلیدس آشکار می‌شود که تعداد عددهای اولِ به‌صورت $۴n + ۳$ نامتناهی است. برای اثبات از لم سادهٔ زیر استفاده می‌کنیم.

1. Edmund Landau

لم. حاصلضرب دو عدد یا چند صحیح که به‌صورت $۴n + ۱$ باشند، به همین صورت است.

اثبات. کافی است حاصلضربِ فقط دو عدد صحیح را در نظر بگیرید. فرض کنید $k = ۴n + ۱$ و $k' = ۴m + ۱$. با ضرب این دو در یکدیگر، به‌دست می‌آوریم

$$\begin{aligned} kk' &= (۴n + ۱)(۴m + ۱) \\ &= ۱۶nm + ۴n + ۴m + ۱ = ۴(۴nm + n + m) + ۱ \end{aligned}$$

که صورت مطلوب است. □

این لم راه را برای اثبات قضیهٔ زیر هموار می‌کند.

قضیهٔ ۳ـ۶ تعداد عددهای اولِ به‌صورت $۴n + ۳$، نامتناهی است.

اثبات. به امید رسیدن به تناقض، فرض می‌کنیم که فقط تعدادی متناهی عدد اول به‌صورت $۴n + ۳$ وجود دارد؛ اینها را $q_۱، q_۲، \ldots، q_s$ می‌نامیم. عدد صحیح مثبت

$$N = ۴q_۱q_۲ \ldots q_s - ۱ = ۴(q_۱q_۲ \ldots q_s - ۱) + ۳$$

را درنظر می‌گیریم و فرض می‌کنیم $N = r_۱r_۲ \ldots r_t$ تجزیهٔ آن به حاصلضرب عاملهای اول باشد. چون N عدد صحیح فردی است، به‌ازای هر k داریم $r_k \neq ۲$، بنابراین هر r_k به‌صورت $۴n + ۱$ یا $۴n + ۳$ است. بنا به لم، حاصلضرب هر تعداد از عددهای اولِ به‌صورت $۴n + ۱$ باز عدد صحیحی از همین نوع است. برای اینکه N به‌صورت $۴n + ۳$ باشد، که به‌وضوح هست، N باید دارای حداقل یک عامل اول به‌صورت $۴n + ۳$ باشد. ولی r_i هیچ یک از $q_۱، q_۲، \ldots، q_s$ نیست، زیرا اگر چنین باشد، به تناقض $r_i | ۱$ می‌رسیم. تنها نتیجه‌گیری ممکن این است که بینهایت عدد اول به‌صورت $۴n + ۳$ وجود دارد. □

اکنون که می‌دانیم تعداد عددهای اولِ به‌صورت $۴n + ۳$ نامتناهی است، منطقی است سؤال شود: آیا تعداد عددهای اولِ به‌صورت $۴n + ۱$ نیز متناهی است؟ پاسخ مثبت است ولی اثبات آن نیاز به مقدماتی دارد که تا عرضهٔ آنها باید صبر کرد. هر دوی این نتیجه‌ها حالتهای خاصی از یک قضیهٔ جالب توجه دیریکله دربارهٔ عددهای اول در تصاعدهای حسابی هستند، که در سال ۱۸۳۷ ثابت شد. اثبات آن بسیار مشکلتر از آن است که در اینجا آورده شود، بنابراین فقط به بیان صورت آن اکتفا می‌کنیم.

قضیهٔ ۳ـ۷ (دیریکله). اگر a و b عددهای صحیح مثبت متباینی باشند، آنگاه تصاعد حسابی

$$a, a+b, a+\text{۲}b, a+\text{۳}b, \ldots$$

شامل بینهایت عدد اول است. □

به‌عنوان نمونه، قضیهٔ دیریکله می‌گوید که تعداد عددهای اولی که به ۹۹۹ ختم می‌شوند، مانند ۱۹۹۹، ۱۰۰۹۹۹، ۱۰۰۰۰۹۹۹، ...، نامتناهی است زیرا، اینها در تصاعد حسابی معین شده به‌وسیله $\text{۱۰۰۰}n + \text{۹۹۹}$، که در آن $\gcd(\text{۱۰۰۰}, \text{۹۹۹}) = \text{۱}$، ظاهر می‌شوند.

تصاعدی حسابی به‌صورت a، $a+b$، $a+\text{۲}b$، ... وجود ندارد که فقط متشکل از عددهای اول باشد. برای اثبات، فرض کنید $a + nb = p$، که p عددی اول است. اگر به‌ازای $k = \text{۱}, \text{۲}, \text{۳}, \ldots$، قرار دهیم $n_k = n + kp$، آنگاه n_kامین جملهٔ تصاعد عبارت است از

$$a + n_k b = a + (n + kp)b = (a + nb) + kpb = p + kpb$$

چون هر جملهٔ سمت راستی بر p بخشپذیر است، $a + n_k b$ نیز بر p بخشپذیر است. به گفتهٔ دیگر، تصاعد باید شامل بینهایت عدد مرکب باشد.

یکی از مسأله‌های قدیمی، ولی هنوز حل نشده، این است که آیا تصاعدی حسابی به‌طول دلخواه ولی متناهی وجود دارد که فقط متشکل از عددهای اول (نه لزوماً متوالی) باشد. طویلترین تصاعد حسابی از این نوع که تاکنون شناخته شده، فقط از ۱۹ عدد اول تشکیل شده است:

$$\text{۸۲۹۷۶۴۴۳۸۷} + \text{۴۱۸۰۵۶۶۳۹۰}n, \qquad (\text{۰} \le n \le \text{۱۸})$$

تجزیهٔ قدر نسبت [تفاضل مشترک] جمله‌های این تصاعد به عاملهای اول عبارت است از

$$\text{۲} \times \text{۳} \times \text{۵} \times \text{۷} \times \text{۱۱} \times \text{۱۳} \times \text{۱۷} \times \text{۱۹} \times \text{۴۳۱}$$

که بر ۵۱۰۵۱۰، حاصلضرب عددهای اول کمتر از ۱۹، بخشپذیر است. این مثالی است از قضیهٔ زیر:

قضیهٔ ۳ـ۸ اگر $n > \text{۲}$ جملهٔ تصاعد حسابی

$$p, p+d, p+\text{۲}d, \ldots, p+(n-\text{۱})d$$

عددهایی اول باشند، آنگاه قدر نسبت [تفاضل مشترک جمله‌های] تصاعد، یعنی d، بر هر عدد اول $q < n$ بخشپذیر است.

اثبات. فرض کنید $q < n$ عددی اول باشد و برخلاف حکم، $q \nmid d$. ادعا می‌کنیم که باقیمانده‌های تقسیم q جملهٔ نخست

$$p, p+d, p+۲d, \ldots, p+(q-۱)d \qquad (۱)$$

بر q متمایزند. اگر چنین نباشد، عددهای صحیح j و k، $۰ \leq j \leq k \leq q-۱$، وجود دارند به‌طوری‌که باقیمانده‌های تقسیم $p+jd$ و $p+kd$ بر q برابرند. پس q تفاضل آنها یعنی $(k-j)d$ را می‌شمارد. ولی $\gcd(q,d) = ۱$، و بنابراین از لم اقلیدس نتیجه می‌شود $q|k-j$، که چون $k-j \leq q-۱$، قابل قبول نیست.

چون q باقیماندهٔ متمایز تولید شده از (۱) جزء q عدد صحیح $۰، ۱، \ldots، q-۱$ هستند، یکی از این باقیمانده‌ها باید صفر باشد. یعنی tای، $۰ \leq t \leq q-۱$، هست به‌طوری که $q|p+td$. بنابراین، چون $q < n \leq p \leq p+td$، نتیجه می‌گیریم که $p+td$ مرکب است. (اگر $p < n$، $p+pd = p(۱+d)$ یکی از جمله‌های تصاعد است.) با این تناقض، اثبات اینکه $q|d$،کامل می‌شود. □

حدس زده شده است که تصاعدهای حسابی متناهی با طول دلخواه، متشکل از عددهای اول متوالی وجود دارند. دو مثال از این‌گونه تصاعدها، که متشکل از، به‌ترتیب،سه و چهار عدد اول‌اند، عبارت‌اند از ۴۱، ۴۷، ۵۳ و ۲۵۱، ۲۵۷، ۲۶۳، ۲۶۹. چندی پیش، با استفاده از کامپیوتر تصاعدهایی متشکل از پنج و شش عدد اول متوالی به‌دست آمد که قدر نسبتهای آنها ۳۰ است؛ این تصاعدها، به‌ترتیب با عددهای اول

۹۸۴۳۰۱۹ و ۱۲۱۱۷۴۸۱۱

آغاز می‌شوند. امکان کشف تصاعدی حسابی متشکل از هفت عدد متوالی، لااقل فعلاً، وجود ندارد. اگر محدودیت متوالی بودن عددهای اول حذف شود، آنگاه می‌توان بینهایت مجموعهٔ متشکل از هفت عدد اول به‌صورت تصاعدی حسابی، به‌دست آورد؛ مثالی از این نوع عبارت است از ۷، ۱۵۷، ۳۰۷، ۴۵۷، ۶۰۷، ۷۵۷، ۹۰۷.

برای حسن‌ختام، مسألهٔ معروف دیگری را مطرح می‌کنیم که تاکنون مصممانه‌ترین تلاشها برای حل آن ناکام مانده است. ریاضیدانها در طی سده‌های متمادی به دنبال فرمول ساده‌ای بوده‌اند که همهٔ عددهای اول را تولید کند، یا در صورت عدم امکان، فرمولی که حداقل فقط مولد عددهای اول باشد. در نگاه نخست، این هدف قابل دسترسی به‌نظر می‌رسد: تابع $f(n)$ای پیدا کنید که دامنه‌اش،

مثلاً، عددهای صحیح نامنفی و برد آن زیر مجموعه‌ای نامتناهی از مجموعهٔ همهٔ عددهای اول باشد. در سده‌های میانه، خیلیها معتقد بودند که چند جمله‌ای درجه دوم

$$f(n) = n^۲ + n + ۴۱$$

فقط مقدارهای اول را می‌پذیرد. طبق جدول زیر، این ادعا به‌ازای $n = ۰, ۱, \ldots, ۳۹$ درست است.

n	$f(n)$	n	$f(n)$	n	$f(n)$
۰	۴۱	۱۴	۲۵۱	۲۸	۸۵۳
۱	۴۳	۱۵	۲۸۱	۲۹	۹۱۱
۲	۴۷	۱۶	۳۱۳	۳۰	۹۷۱
۳	۵۳	۱۷	۳۴۷	۳۱	۱۰۳۳
۴	۶۱	۱۸	۳۸۳	۳۲	۱۰۹۷
۵	۷۱	۱۹	۴۲۱	۳۳	۱۱۶۳
۶	۸۳	۲۰	۴۶۱	۳۴	۱۲۳۱
۷	۹۷	۲۱	۵۰۳	۳۵	۱۳۰۱
۸	۱۱۳	۲۲	۵۴۷	۳۶	۱۳۷۳
۹	۱۳۱	۲۳	۵۹۳	۳۷	۱۴۴۷
۱۰	۱۵۱	۲۴	۶۴۱	۳۸	۱۵۲۳
۱۱	۱۷۳	۲۵	۶۹۱	۳۹	۱۶۰۱
۱۲	۱۹۷	۲۶	۷۴۳		
۱۳	۲۲۳	۲۷	۷۹۷		

ولی، این حدس هیجان‌انگیز در حالتهای $n = ۴۰$ و $n = ۴۱$، که در آن حالات عامل ۴۱ای وجود دارد، درست نیست:

$$f(۴۰) = ۴۰ \times ۴۱ + ۴۱ = ۴۱^۲$$

و

$$f(۴۱) = ۴۱ \times ۴۲ + ۴۱ = ۴۱ \times ۴۳$$

مقدار بعدی $f(۴۲) = ۱۷۴۷$ باز عددی اول است. فعلاً معلوم نیست که تعداد مقدارهای اول $f(n) = n^۲ + n + ۴۱$ به‌ازای nهای صحیح متناهی است یا نه.

تصادفی نیست که تابع فوق عددهای غیر اول را نیز تولید می‌کند زیرا به آسانی می‌توان ثابت کرد چند جمله‌ای غیر ثابتی با ضریبهای صحیح وجود ندارد که فقط مقدارهای اول را به‌ازای nهای صحیح بپذیرد. فرض می‌کنیم چنان چند جمله‌ایی وجود دارد و طوری استدلال می‌کنیم که به تناقض برسیم. گیریم

$$f(n) = a_k n^k + a_{k-۱} n^{k-۱} + \ldots + a_۲ n^۲ + a_۱ n + a_۰$$

که در آن همهٔ ضریبهای $a_۰$، $a_۱$، $\ldots$ ، a_k عددهای صحیح‌اند و $a_k \neq ۰$. به‌ازای مقدار مشخص nای، مثلاً $n = n_۰$، $p = f(n_۰)$ عددی اول است. اکنون، به‌ازای عدد صحیح دلخواه t، عبارت $f(n_۰ + tp)$ را درنظر می‌گیریم

$$\begin{aligned} f(n_۰ + tp) &= a_k(n_۰ + tp)^k + \ldots + a_۱(n_۰ + tp) + a_۰ \\ &= (a_k n_۰^k + \ldots + a_۱ n_۰ + a_۰) + pQ(t) \\ &= f(n_۰) + pQ(t) \\ &= p + pQ(t) = p(۱ + Q(t)) \end{aligned}$$

که در آن $Q(t)$ چند جمله‌ایی برحسب t با ضریبهای صحیح است. استدلال ما نشان می‌دهد که $p|f(n_۰ + tp)$؛ پس، بنا به فرضمان مبنی‌بر اینکه مقدارهای $f(n)$ همیشه اول است، به‌ازای هر مقدار صحیح t داریم $f(n_۰ + tp) = p$. چون چند جمله‌ایی از درجهٔ k نمی‌تواند یک مقدار را بیش از k بار بپذیرد، تناقض مطلوب را به‌دست آورده‌ایم.

در سالهای اخیر شاهد موفقیتهایی در پیدا کردن تابعهایی که مقدارهایشان فقط از عددهای اول باشند بوده‌ایم. میلز[1] ثابت کرد (۱۹۴۷) عدد حقیقی مثبت rای وجود دارد به‌طوری که عبارت $f(n) = [r^{۳^n}]$ به‌ازای $n = ۱, ۲, ۳, \ldots$ اول است (کروشه نشان‌دهندهٔ تابع جزء صحیح است). نیازی به گفتن ندارد که این قضیه یک قضیهٔ وجودی است و اطلاعی دربارهٔ مقدار واقعی r در دست نیست.

تمرینهای ۳ـ۳

۱. نشان دهید که عددهای صحیح ۱۹۴۹ و ۱۹۵۱ عددهای اول دوقلویی هستند.

۲. (الف) نشان دهید که اگر عدد ۱ به حاصلضرب دو عدد اول دوقلو اضافه شود، همیشه مربع کاملی به‌دست می‌آید.

1. W. H. Mills

(ب) اگر $p > ۳$، نشان دهید که مجموع عددهای دوقلوی p و $p + ۲$ بر ۱۲ بخشپذیر است.

۳. همهٔ عددهای اول p و q را که در $p - q = ۳$ صدق کنند، پیدا کنید.

۴. در سال ۱۸۹۶، سیلوستر حدس گولدباخ را به‌صورت دیگری چنین عنوان کرد: هر عدد صحیح زوج بزرگتر از ۴ به‌صورت $۲n$ مجموع عدد اولی بزرگتر از $n/۲$ و عدد اولی کوچکتر از $۳n/۲$ است. درستی این صورت از حدس گولدباخ را به‌ازای همهٔ عددهای زوج میان ۶ و ۷۶ نشان دهید.

۵. در سال ۱۷۵۲، گولدباخ حدس زیر را به اویلر ارائه کرد: هر عدد صحیح فرد را می‌توان به‌صورت $p + ۲a^۲$ نوشت، که p یا عددی اول یا ۱ است و $a \geq ۰$. نشان دهید که عدد صحیح ۵۷۷۷ این حدس را نقض می‌کند.

۶. ثابت کنید که حدس گولدباخ: "هر عدد صحیح زوج بزرگتر از ۲ مجموع دو عدد اول است" هم‌ارز است با عبارت "هر عدد صحیح بزرگتر از ۵ مجموع سه عدد اول است" [راهنمایی: اگر $۲n - ۲ = p_۱ + p_۲$، آنگاه $۲n = p_۱ + p_۲ + ۲$ و $۲n + ۱ = p_۱ + p_۲ + ۳$.]

۷. طبق حدسی از لاگرانژ (۱۷۷۵) هر عدد صحیح فرد بزرگتر از ۵ را می‌توان به‌صورت $p_۱ + ۲p_۲$، که هر دوی $p_۱$ و $p_۲$ عددهای اولی هستند، نوشت. درستی این حدس را به‌ازای هر عدد صحیح فرد بزرگتر از ۵ و نابیشتر از ۷۵ ثابت کنید.

۸. می‌توان نشان داد که به‌ازای هرعدد صحیح مثبت n، عدد صحیح مثبت زوج aای که به n روش متفاوت به‌صورت مجموع دو عدد اول فرد قابل نمایش باشد، وجود دارد. نشان دهید که عددهای صحیح ۶۰، ۷۸، و ۸۴ را می‌توان، به‌ترتیب، به شش، هفت، و هشت روش به‌صورت مجموع دو عدد اول نوشت.

۹. (الف) نشان دهید که به‌ازای $n > ۳$، همهٔ عددهای صحیح n، $n + ۲$ و $n + ۴$ اول نیستند.

(ب) سه عدد صحیح p، $p + ۲$، $p + ۶$ یک سه‌تایی اول نامیده می‌شوند اگر هر سه اول باشند. پنج مجموعه متشکل از سه‌تاییهای اول پیدا کنید.

۱۰. نشان دهید که اگر $n > ۱$، دنبالهٔ

$$(n + ۱)! - ۲, \quad (n + ۱)! - ۳, \ldots, \quad (n + ۱)! - (n + ۱)$$

مولد n عدد صحیح مرکب متوالی است.

۱۱. کوچکترین عدد صحیح مثبت nای را پیدا کنید که به‌ازای آن مقدار تابع $f(n) = n^۲ + n + ۱۷$ مرکب باشد. همین کار را در مورد تابعهای $g(n) = n^۲ + ۲۱n + ۱$ و $h(n) = ۳n^۲ + ۳n + ۲۳$ انجام دهید.

۱۲. گرچه حکم زیر را بِرتران حدس زد، ولی نخستین بار چبیشف آن‌را در ۱۸۵۰ ثابت کرد: به‌ازای هر عدد صحیح مثبت $n > ۱$، دست‌کم یک عدد اول p وجود دارد که $n < p < ۲n$. اگر p_n، nامین عدد اول باشد، با استفاده از حدس بِرتران نشان دهید که $p_n < ۲^n$.

۱۳. با استفاده از روش اثبات قضیهٔ ۳ـ۶ نشان دهید که تعداد عددهای اول به‌صورت $۶n + ۵$، نامتناهی است.

۱۴. مقسوم‌علیه اولی از عدد صحیح $N = ۴(۳ \times ۷ \times ۱۱) - ۱$ را که به‌صورت $۴n + ۳$ باشد، به‌دست آورید. همین‌کار را در مورد $N = ۴(۳ \times ۷ \times ۱۱ \times ۱۵) - ۱$ انجام دهید.

۱۵. پرسش بدون پاسخ دیگر این است که آیا تعداد مجموعه‌های متشکل از پنج عدد صحیح فرد متوالی که چهار عضوشان اول باشند نامتناهی است یا نه. پنج تا از این مجموعه‌ها را پیدا کنید.

۱۶. فرض کنید دنبالهٔ متشکل از ۱ و عددهای اول به‌صورت $p_۰ = ۱$، $p_۱ = ۲$، $p_۲ = ۳$، $p_۳ = ۵$، ... نشان داده شود. می‌دانیم که به‌ازای هر $n \geq ۱$، ضریبهای $\epsilon_k = \pm ۱$ را می‌توان طوری انتخاب کرد که

$$p_{۲n} = p_{۲n-۱} + \sum_{k=۰}^{۲n-۲} \epsilon_k p_k \text{ ، } p_{۲n+۱} = ۲p_{۲n} + \sum_{k=۰}^{۲n-۱} \epsilon_k p_k$$

به‌عنوان مثال

$$۱۳ = ۱ + ۲ - ۳ - ۵ + ۷ + ۱۱$$

و

$$۱۷ = ۱ + ۲ - ۳ - ۵ + ۷ - ۱۱ + ۲ \times ۱۳$$

نمایشهای مشابه را برای عددهای اول ۲۳، ۲۹، ۳۱، و ۳۷ تعیین کنید.

۱۷. در سال ۱۸۴۸ دپولینیاک[1] ادعا کرد که هر عدد صحیح فرد مجموع عددی اول و توانی از ۲ است. مثلاً $۵۵ = ۴۷ + ۲^۳ = ۲۳ + ۲^۵$. نشان دهید که عددهای صحیح ۵۰۹ و ۸۷۷ این ادعا را نقض می‌کنند.

۱۸. (الف) اگر p عددی اول باشد و $p \nmid b$، ثابت کنید که هر جملهٔ pام تصاعد حسابی

$$a, a + b, a + ۲b, a + ۳b, \ldots$$

بر p بخشپذیر است. [راهنمایی: چون $\gcd(p, b) = ۱$، عددهای صحیح r و sای موجودند به‌طوری که $pr + bs = ۱$. قرار دهید $n_k = kp - as$، $k = ۱, ۲, \ldots$، و نشان دهید $p | (a + n_k b)$.]

---
1. de Polignac

(ب) از قسمت (الف) نتیجه بگیرید که اگر b عدد صحیح فردی باشد، آنگاه هر جملهٔ دیگر این تصاعد، عددی زوج است.

۱۹. در سال ۱۹۵۰، ثابت شد که هر عدد صحیح $n > ۹$ را می‌توان به‌صورت مجموع عددهای اول فرد متمایز نوشت. عددهای صحیح ۲۵، ۶۹، ۸۱، و ۱۲۵ را به این‌صورت بنویسید.

۲۰. اگر هر دوی p و $p^۲ + ۸$ عددهایی اول باشند، ثابت کنید که $p^۳ + ۴$ نیز اول است.

۲۱. (الف) نشان دهید که به‌ازای هر عدد صحیح مثبت k، تصاعد حسابی

$$a + b, a + ۲b, a + ۳b, \ldots$$

که $\gcd(a, b) = ۱$، حاوی k جملهٔ مرکب متوالی است. [راهنمایی: قرار دهید $n = (a + b)(a + ۲b) \ldots (a + kb)$ و k جملهٔ

$$a + (n + ۱)b ،a + (n + ۲)b ،\ldots ,\ a + (n + k)b$$

را درنظر بگیرید.]

(ب) پنج جملهٔ مرکب متوالی در تصاعد حسابی

$$۶, ۱۱, ۱۶, ۲۱, ۲۶, ۳۱, ۳۶, \ldots$$

پیدا کنید.

۲۲. نشان دهید ۱۳ بزرگترین عدد اولی است که می‌تواند دو عدد صحیح متوالی به‌صورت $n^۲ + ۳$ را بشمارد.

۲۳. (الف) میانگین حسابی عددهای اول دوقلوی ۵ و ۷ عدد مثلثی ۶ است. آیا عددهای اول دوقلوی دیگری با میانگین مثلثی وجود دارند؟

(ب) میانگین حسابی عددهای اول دوقلوی ۳ و ۵ عدد مربع کامل ۴ است. آیا عددهای اول دوقلوی دیگری با میانگین مربع وجود دارند؟

۲۴. همهٔ عددهای اول دوقلوی p و $q = p + ۲$ای را تعیین کنید که به‌ازای آنها $pq - ۲$ نیز اول باشد.

۲۵. فرض کنید p_n، nامین عدد اول باشد. اگر $n > ۳$، نشان دهید که

$$p_n < p_۱ + p_۲ + \ldots + p_{n-۱}$$

[راهنمایی: از حدس برتران و استقرا استفاده کنید.]

۲۶. نشان دهید

(الف) تعداد عددهای اولی که به ۳۳ ختم می‌شوند، مانند ۳۳، ۲۳۳، ۴۳۳، ۷۳۳، ۱۰۳۳، . . .، نامتناهی است. [راهنمایی: از قضیهٔ دیریکله استفاده کنید.]

(ب) تعداد عددهای اولی که به زوج دوقلویی از عددهای اول متعلق نیستند، نامتناهی است. [راهنمایی: تصاعد حسابی $۲۱k + ۵$، $k = ۱, ۲, \ldots$ را درنظر بگیرید.]

(پ) به‌ازای هر n دلخواه، عدد اولی وجود دارد که به n رقم ۱ ختم می‌شود. [راهنمایی: برای به‌دست آوردن عدد اولی که n رقم سمت راست آن ۱ باشد تصاعد حسابی $۱۰^n k + R_n$، $k = ۱, ۲, \ldots$، را درنظر بگیرید.]

۲۷. ثابت کنید که به‌ازای هر $n \geq ۲$، عدد اول pای با $p < n < ۲p$ وجود دارد. [راهنمایی: اگر $n = ۲k + ۱$، آنگاه بنا به حدس برتران عدد اول pای وجود دارد که $k < p < ۲k$.]

۲۸. (الف) اگر $n > ۱$، نشان دهید که $n!$ هرگز مربع کاملی نیست.

(ب) مقدارهایی از $n \geq ۱$ را به‌دست آورید که به‌ازای آنها

$$n! + (n + ۱)!(n + ۲)!$$

مربع کامل باشد. [راهنمایی: توجه کنید که $n! + (n + ۱)! + (n + ۲)! = n!(n + ۲)^۲$.]

۴

نظریهٔ همنهشتیها

«زمانی گاوس گفت ریاضیات ملکهٔ علوم و نظریهٔ اعداد ملکهٔ ریاضیات است؛ اگر این سخن درست باشد، می‌توانیم اضافه کنیم که رسالهٔ تحقیقات حسابی گاوس منشور نظریهٔ اعداد است.»

کانتور

۴ـ۱ کارل فریدریش گاوس

رویکرد دیگری به موضوع تقسیم‌پذیری [بخش‌پذیری] از طریق حساب مانده‌ها یا نظریهٔ همنهشتیهاست که اکنون همه آن را می‌شناسند. مفهوم و نمادی که آن مفهوم را به صورت چنان ابزار توانایی در می‌آورد، نخستین بار به وسیلهٔ ریاضیدان آلمانی، کارل فریدریش گاوس (۱۷۷۷ـ۱۸۵۵)، در کتاب تحقیقات حسابی‌اش، معرفی شد؛ این اثر عظیم، که در ۱۸۰۱ میلادی در ۲۴ سالگی گاوس منتشر شد، نظریهٔ جدید اعداد را پایه‌ریزی کرد. معروف است که بخش اعظم کتاب تحقیقات حسابی در سال قبل از انتشار به صورت رساله‌ای به آکادمی فرانسه تقدیم شده و به چنان شیوهٔ زننده‌ای

مردود شناخته شده بود که، حتی در صورت صائب بودن نظر داوران مبنی بر بی‌ارزشی آن، قابل توجیه نمی‌توانسته باشد (به منظور تعیین صحت و سقم این داستان ناخوشایند، مسؤولان آکادمی در سال ۱۹۳۵ جستجوی گسترده‌ای در بایگانی خود به‌عمل آوردند، و نتیجه گرفتند که، تحقیقات حسابی هرگز تسلیم آکادمی نشده، یا حداقل مردود نشده است). کرونکر می‌گوید «تصور اینکه مردی به آن کم‌سن‌وسالی به تنهایی بتواند چنان گنجینهٔ پرباری از نتیجه‌ها عرضه کند، و بالاتر از آن، چنان بررسی عمیق و منسجمی از یک مبحث کاملاً جدید به عمل آورد، واقعاً دشوار است».

گاوس در خردسالی جزو کودکان نابغه‌ای بود که استعداد ریاضی ذاتی آنها خیلی زود آشکار می‌شود. برطبق روایتی مؤثق، در سه‌سالگی اشتباهی را در محاسبهٔ صورت پرداختهای پدرش تصحیح کرد. استعداد ریاضیش به اندازه‌ای معلمان مدرسه‌اش را مرعوب کرد که وقتی گاوس ۱۰ سال داشت، اعتراف کردند که، هر چه می‌دانسته‌اند به این طفل آموخته‌اند. معروف است که، گاوس در نخستین کلاس حساب خود، با حل فوری مسأله‌ای که «وقت‌گیر» محسوب می‌شد، معلمش را متعجب ساخت: مجموع همهٔ عددهای از ۱ تا ۱۰۰ را پیدا کنید. بعداً گاوس جوان اعتراف کرد که پی‌برده بود

$$۱ + ۱۰۰ = ۱۰۱,\ ۲ + ۹۹ = ۱۰۱,\ ۳ + ۹۸ = ۱۰۱, \ldots,\ ۵۰ + ۵۱ = ۱۰۱$$

چون ۵۰ زوج از عددها که مجموع هر زوج ۱۰۱ است، وجود دارد، مجموع همهٔ این عددها باید $۵۰ \times ۱۰۱ = ۵۰۵۰$ باشد. به این ترتیب روش دیگری برای اثبات فرمول

$$۱ + ۲ + ۳ + \ldots + n = \frac{n(n+۱)}{۲}$$

به منظور جمع n عدد صحیح مثبت نخست به‌دست می‌آید. کافی است عددهای صحیح متوالی از ۱ تا n را در دوسطر به صورت زیر نوشت:

$$\begin{array}{cccccc} ۱ & ۲ & ۳ & \ldots & n-۱ & n \\ n & n-۱ & n-۲ & \ldots & ۲ & ۱ \end{array}$$

با جمع کردن درایه‌های ستونهای عمودی، n جملهٔ برابر با $n + ۱$ به‌دست می‌آید؛ اگر این جمله‌ها با هم جمع شوند، مقدار $n(n + ۱)$ را به‌دست می‌آوریم. چون همین مجموع را می‌توان از جمع درایه‌های دوسطر نیز به‌دست آورد، به فرمول $۲(۱ + ۲ + ۳ + \ldots + n) = n(n + ۱)$ می‌رسیم.

گاوس به یک رشته موفقیتهای شایانِ پی‌درپی نائل شد. مدتها بود که مسأله ترسیم چند ضلعیهای منتظم فقط با استفاده از «ابزارهای اقلیدسی»، یعنی، فقط با خطکش و پرگار، به بوتهٔ فراموشی سپرده شده بود، زیرا عقیده بر این بود که پیشینیان همهٔ ترسیمهای ممکن را آزموده‌اند. در ۱۷۹۶، گاوس نشان داد که هفده ضلعی منتظم را می‌توان به روش فوق رسم کرد، و این نخستین گام به جلو در این

زمینه از زمان اقلیدس به بعد بود. رسالهٔ دکتری گاوس در سال ۱۷۹۹ شامل اثبات دقیقی از قضیهٔ بنیادی جبر بود که نخست ژیرار[1] در ۱۶۲۹ آن‌را مطرح کرده و سپس دالامبر (۱۷۴۶)، و بالاخره اویلر (۱۷۴۹) آن را به‌طور ناقص ثابت کرده بودند. این قضیه (که می‌گوید هر معادلهٔ جبری درجهٔ n دقیقاً n ریشهٔ مختلط دارد) همیشه مورد علاقهٔ گاوس بود و او آن را، کلاً، به چهار روش متفاوت ثابت کرد. چاپ کتاب تحقیقات حسابی در سال ۱۸۰۱، گاوس را بیدرنگ در صف اول ریاضیدانان قرار داد.

شگفت‌انگیزترین دستاورد گاوس بیشتر به نجوم نظری مربوط می‌شد تا به ریاضیات. در نخستین شب سدهٔ نوزدهم، یکم ژانویهٔ ۱۸۰۱، پیاتسی منجم ایتالیایی نخستین نمونه از سیارکها را که بعداً سرس[2] نامیده شد، کشف کرد. ولی همین که این شئ جدید الاکتشاف، که فقط با تلسکوپ قابل رؤیت بود، در مسیر خود از خورشید عبور کرد، هیچ منجمی، حتی خود پیاتسی، دوباره قادر به تعیین مکان آن نشد. پیاتسی ۴۱ روز به رصد کردن ادامه داد، که در خلال آن مدار سیارک فقط یک کمان ۹ درجه را طی کرد. گاوس توانست با استفاده از اطلاعات بسیار کم موجود مدار سرس را با چنان دقت شگفت‌آوری محاسبه کند که در پایان سال سیارک گریزپا دوباره و تقریباً به‌طور دقیق در مکانهایی که او پیش‌بینی کرده بود، دیده شد. این موفقیت موجب شهرت جهانی گاوس و انتصاب او به مدیریت رصدخانهٔ گوتینگن گردید.

تا اواسط سدهٔ نوزدهم، ریاضیات در سیر رشد خود به صورت نظامی بسیار گسترده متشکل از زمینه‌های بسیار متعدد درآمده بود و فقط متخصصان راه خود را باز می‌شناختند. گاوس آخرین ریاضیدان جامع‌الاطراف بود، و گزافه نیست اگر گفته شود که وی تقریباً با هر مبحث ریاضی تا اندازه‌ای الفت داشت. معاصران گاوس وی را سلطان ریاضیات و همتراز ارشمیدس و آیزک نیوتون به‌شمار می‌آوردند. این امر از واقعهٔ کوچکی معلوم می‌شود: وقتی نظر لاپلاس را در مورد بزرگترین ریاضیدان آلمانی پرسیدند، پاسخ داد «پفاف[3]». وقتی سؤال کننده گفت که او فکر می‌کرده گاوس بزرگترین است، لاپلاس جواب داد «پفاف تا امروز بزرگترین ریاضیدان در آلمان است، ولی گاوس بزرگترین ریاضیدان در کل اروپاست.»

گرچه گاوس در همهٔ شاخه‌های ریاضیات فعال بود، به نظریهٔ اعداد علاقهٔ خاصی داشت و ارج بسیار می‌نهاد. وی اصرار داشت که، «ریاضیات ملکهٔ علوم است، و نظریهٔ اعداد ملکهٔ ریاضیات.»

۲ـ۴ ویژگیهای اساسی همنهشتی

گاوس در فصل اول کتاب تحقیقات حسابی مفهوم همنهشتی و نماد آن را که باعث می‌شود این مفهوم ابزار نیرومندی باشد، معرفی می‌کند (او توضیح می‌دهد که دلیل انتخاب نماد $\equiv$ تشابه زیاد

1. Girard   2. Ceres   3. Pfaff

مفهوم همنهشتی با برابری جبری است). به گفته گاوس، «اگر عدد nای [چون پیمانه‌ای باشد که] تفاضل میان دوعدد a و b را اندازه‌گیری کند، آنگاه a و b نسبت به n همنهشت نامیده می‌شوند؛ وگرنه، ناهمنهشت.» این مطلب را در قالب تعریف بیان می‌کنیم.

تعریف ۴ـ۱ فرض می‌کنیم n عدد صحیح مثبت ثابتی باشد. دوعدد صحیح a و b همنهشت به پیمانهٔ n نامیده می‌شوند، و این رابطهٔ آنها به صورت

$$a \equiv b(n \text{ به پیمانهٔ })$$

نشان داده می‌شود اگر n تفاضل $a-b$ را بشمارد؛ یعنی، اگر به‌ازای عدد صحیح kای، $a-b=kn$.

برای روشن شدن این تعریف، مثلاً فرض می‌کنیم $n=7$. به‌سادگی دیده می‌شود که $(\text{به پیمانهٔ } 7)\ 24 \equiv 3$ ، $(\text{به پیمانهٔ } 7)\ 11 \equiv -31$ ، $(\text{به پیمانهٔ } 7)\ -64 \equiv -15$ ، زیرا $24-3=(-3)7$ ، $-31-11=(-6)7$ ، و $-15-(-64)=7\times 7$. اگر $n \nmid (a-b)$، می‌گوییم که a همنهشت با b به پیمانهٔ n نیست و در این حالت می‌نویسیم $a \not\equiv b(n \text{ به پیمانهٔ })$ به عنوان مثال: $(\text{به پیمانهٔ } 7)\ 25 \not\equiv 12$ ، زیرا $25-12=13$ بر ۷ بخشپذیر نیست.

باید توجه کرد که هر دوعدد صحیحی همنهشت به پیمانهٔ ۱ اند، در صورتی که دوعدد صحیح وقتی همنهشت به پیمانهٔ ۲ اند که هردو زوج یا هردو فرد باشند. چون همنهشتی به پیمانهٔ ۱ جالب توجه نیست، معمولاً فرض می‌شود $n>1$.

فرض می‌کنیم a عددی صحیح و q و r، به ترتیب، خارج قسمت و باقیماندهٔ تقسیم a بر n باشند. یعنی

$$a=qn+r, \qquad 0 \le r < n$$

در این صورت، بنا به تعریف همنهشتی، $a \equiv r(n \text{ به پیمانهٔ })$. چون برای r، n انتخاب وجود دارد، نتیجه می‌گیریم که هرعدد صحیح دقیقاً با یکی از مقدارهای ۰، ۱، ۲، …، $n-1$، همنهشت به پیمانهٔ n است؛ به ویژه، $a \equiv 0\ (n \text{ به پیمانهٔ })$ اگر و تنها اگر $n|a$. مجموعهٔ n عدد صحیح ۰، ۱، ۲، …، $n-1$ مجموعهٔ کوچکترین مانده‌های مثبت به پیمانهٔ n نامیده می‌شود.

به‌طور کلی، گوییم مجموعهٔ n عدد صحیح a_1، a_2، …، a_n تشکیل مجموعهٔ کاملی از مانده‌ها (یا دستگاه کاملی از مانده‌ها) به پیمانهٔ n می‌دهد اگر هر عدد صحیح دقیقاً با یکی از a_kها همنهشت به پیمانهٔ n باشد؛ به بیان دیگر، a_1، a_2، …، a_n همنهشت به پیمانهٔ n با ۰، ۱، ۲، …، $n-1$، به‌ترتیبی، باشند. به عنوان مثال

$$-12,\ -4,\ 11,\ 13,\ 22,\ 82,\ 91$$

تشکیل مجموعهٔ کاملی از مانده‌ها به پیمانهٔ ۷ می‌دهند؛ در اینجا همنهشتیهای زیر را به پیمانهٔ ۷ داریم

$$-۱۲ \equiv ۲،\ -۴ \equiv ۳،\ ۱۱ \equiv ۴،\ ۱۳ \equiv ۶،\ ۲۲ \equiv ۱،\ ۸۲ \equiv ۵،\ ۹۱ \equiv ۰$$

نکته‌ای نسبتاً مهم این است که هر n عدد صحیح تشکیل مجموعهٔ کاملی از مانده‌ها به پیمانهٔ n می‌دهند اگر و تنها اگر هیچ دوتا از این عددهای صحیح همنهشت به پیمانهٔ n نباشند. این نکته را در آینده به کار خواهیم برد.

نخستین قضیهٔ این فصل محک سودمندی برای همنهشتی به پیمانهٔ n برحسب باقیمانده‌های تقسیم بر n ارائه می‌دهد.

قضیهٔ ۴ـ۱ به‌ازای عددهای صحیح دلخواه a و b، $a \equiv b$ (به پیمانهٔ n) اگر و تنها اگر باقیمانده‌های ناصفرِ تقسیم a و b بر n برابر باشند.

اثبات. نخست، فرض می‌کنیم $a \equiv b$ (به پیمانهٔ n) ، بنابراین به‌ازای عدد صحیح kای $a = b + kn$. اگر b را بر n تقسیم کنیم، باقیماندهٔ rای خواهد داشت؛ یعنی $b = qn + r$، که $۰ \leq r < n$. بنابراین

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

که نشان می‌دهد باقیمانده‌های تقسیم a و b بر n برابرند.

از سوی دیگر، فرض می‌کنیم $a = q_۱n + r$ و $b = q_۲n + r$، یعنی باقیماندهٔ هر دو r است که $۰ \leq r < n$. در این صورت

$$a - b = (q_۱\, n + r) - (q_۲\, n + r) = (q_۱ - q_۲)n$$

بنابراین $n | a - b$. به زبان همنهشتی، نتیجه می‌شود که $a \equiv b$ (به پیمانهٔ n) □

مثال ۴ـ۱

چون می‌توان عددهای صحیح ۵۶− و ۱۱− را به‌صورت

$$-۵۶ = (-۷)۹ + ۷ ،\qquad -۱۱ = (-۲)۹ + ۷$$

با باقیماندهٔ یکسان ۷ بیان کرد، بنا به قضیهٔ ۴ـ۱، $-۵۶ \equiv -۱۱$ (به پیمانهٔ ۹) . از سوی دیگر، همنهشتی $-۳۱ \equiv ۱۱$ (به پیمانهٔ ۷) به این معنی است که باقیمانده‌های تقسیم ۳۱− و ۱۱ بر

۷ برابرند؛ این موضوع با توجه به رابطه‌های

$$-۳۱ = (-۵)۷ + ۴ \quad ، \quad ۱۱ = ۱ \times ۷ + ۴$$

روشن است. ■

همنهشتی را می‌توان صورتی تعمیم یافته از برابری به حساب آورد، به این معنی که ویژگیهایش از لحاظ جمع و ضرب یادآورِ برابری معمولی است. برخی از ویژگیهای ابتدایی برابری که در مورد همنهشتی نیز صادق‌اند، در قضیهٔ زیر ملاحظه می‌شوند.

قضیهٔ ۴ـ۲ فرض می‌کنیم $n > ۰$ ثابت و a، b، c، d عددهای صحیح دلخواهی باشند. در این صورت ویژگیهای زیر برقرارند

(۱) $a \equiv a$ (به پیمانهٔ n) .

(۲) اگر $a \equiv b$ (به پیمانهٔ n) ، آنگاه $b \equiv a$ (به پیمانهٔ n) .

(۳) اگر $a \equiv b$ (به پیمانهٔ n) و $b \equiv c$ (به پیمانهٔ n) ، آنگاه $a \equiv c$ (به پیمانهٔ n) .

(۴) اگر $a \equiv b$ (به پیمانهٔ n) و $c \equiv d$ (به پیمانهٔ n) ، آنگاه $a + c \equiv b + d$ (به پیمانهٔ n) و $ac \equiv bd$ (به پیمانهٔ n) .

(۵) اگر $a \equiv b$ (به پیمانهٔ n) ، آنگاه $a+c\equiv b+c$ (به پیمانهٔ n) و $ac \equiv bc$ (به پیمانهٔ n) .

(۶) اگر $a\equiv b$ (به پیمانهٔ n) ، آنگاه به ازای هر عدد صحیح مثبت k، $a^k \equiv b^k$ (به پیمانهٔ n) .

اثبات. به ازای هر عدد صحیح a داریم $a - a = ۰ \times n$، بنابراین $a \equiv a$ (به پیمانهٔ n). حال اگر $a \equiv b$ (به پیمانهٔ n)، آنگاه به‌ازای عدد صحیح kای، $a - b = kn$. پس، $b - a = -(kn) = (-k)n$، و چون $-k$ عدد صحیحی است، از اینجا (۲) نتیجه می‌شود.

اثبات ویژگی (۳) اندکی مشکلتر است: فرض می‌کنیم $a \equiv b$ (به پیمانهٔ n) و $b \equiv c$ (به پیمانهٔ n) . در این صورت عددهای صحیح k و hای وجود دارند که $a - b = hn$ و $b - c = kn$. نتیجه می‌شود که

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

بنابراین $a \equiv c$ (به پیمانهٔ n) .

به همین روش، اگر $a \equiv b$ (به پیمانهٔ n) و $c \equiv d$ (به پیمانهٔ n) ، آنگاه می‌دانیم که به‌ازای عددهای صحیح $k_۱$ و $k_۲$ای، $a - b = k_۱n$ و $c - d = k_۲n$. با جمع کردن این معادله‌ها

به‌دست می‌آوریم

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= k_۱n+k_۲n=(k_۱+k_۲)n\end{aligned}$$

یا، به صورت عبارتی همنهشتی، (به پیمانهٔ $a+c\equiv b+d(n$. در مورد دومین ویژگی مذکور در (۴)، ملاحظه می‌کنیم که

$$ac=(b+k_۱n)(d+k_۲n)=bd+(bk_۲+dk_۱+k_۱k_۲n)n$$

چون $bk_۲+dk_۱+k_۱k_۲n$ عددی صحیح است، نتیجه می‌شود که $ac-bd$ بر n بخشپذیر است، بنابراین (به پیمانهٔ $ac\equiv bd(n$.

اثبات ویژگی (۵) با توجه به اینکه (به پیمانهٔ $c\equiv c(n$،از اثبات (۴) نتیجه می‌شود. و بالاخره، (۶) را با استدلالی استقرایی نتیجه می‌گیریم. این حکم به‌ازای $k=۱$ به‌وضوح برقرار است، و فرض می‌کنیم به‌ازای kی ثابتی برقرار باشد. بنا به (۴)، می‌دانیم که از (به پیمانهٔ $a\equiv b(n$ و (به پیمانهٔ $a^k\equiv b^k(n$ نتیجه می‌شود (به پیمانهٔ $aa^k\equiv bb^k(n$، یا (به پیمانهٔ $a^{k+۱}\equiv b^{k+۱}(n$. و این حکم موردنظر به ازای $k+۱$ است، بنابراین مرحلهٔ استقرا به انجام رسیده است. □

پیش از ادامهٔ بحث با ذکر مثالی نشان می‌دهیم که همنهشتیها چه کمک زیادی به انجام دادن گونه‌هایی از محاسبه‌ها می‌کنند.

مثال ۴ـ۲

نشان می‌دهیم که ۴۱، $۲^{۲۰}-۱$ را می‌شمارد. کار را با ملاحظهٔ همنهشتی (به پیمانهٔ $۲^۵\equiv -۹(۴۱$ آغاز می‌کنیم، که از اینجا بنابه قضیهٔ ۴ـ۲ (۶) داریم (به پیمانهٔ $(۲^۵)^۴\equiv(-۹)^۴(۴۱$ ؛ به بیان دیگر، (به پیمانهٔ $۲^{۲۰}\equiv ۸۱\times ۸۱(۴۱$. ولی (به پیمانهٔ $۸۱\equiv -۱(۴۱$ و بنابراین (به پیمانهٔ $۸۱\times ۸۱\equiv ۱(۴۱$. و بالاخره، با استفاده از بخشهای (۲) و (۵) از قضیهٔ ۴ـ۲

$$۲^{۲۰}-۱\equiv ۸۱\times ۸۱-۱\equiv ۱-۱\equiv ۰(۴۱ \text{ به پیمانهٔ})$$

پس، همان طور که می‌خواستیم، $۴۱|۲^{۲۰}-۱$. ■

مثال ۴ـ۳

برای اینکه مثال دیگری در همین زمینه بیاوریم، فرض می‌کنیم از ما خواسته باشند باقیماندهٔ تقسیم مجموع

$$۱! + ۲! + ۳! + ۴! + \ldots + ۹۹! + ۱۰۰!$$

بر ۱۲ را به‌دست آوریم. حل مسأله بدون بهره‌گیری از همنهشتی مستلزم محاسبه‌ای طاقت‌فرساست. سرآغاز کار ما توجه به همنهشتی $۴! \equiv ۲۴ \equiv ۰$ (به پیمانهٔ ۱۲) است؛ بنابراین، به‌ازای $k \geq ۴$

$$k! \equiv ۴! \times ۵ \times ۶ \ldots k \equiv ۰ \times ۵ \times ۶ \ldots k \equiv ۰ (\text{به پیمانهٔ ۱۲})$$

بنابراین

$$\begin{aligned} &۱! + ۲! + ۳! + ۴! + \ldots + ۱۰۰! \\ &\qquad \equiv ۱! + ۲! + ۳! + ۰ + \ldots + ۰ \equiv ۹ (\text{به پیمانهٔ ۱۲}) \end{aligned}$$

پس، باقیماندهٔ تقسیم مجموع بر ۱۲ برابر ۹ است. ■

در قضیهٔ اخیر ملاحظه شد که اگر $a \equiv b$ (به پیمانهٔ n)، آنگاه به‌ازای هر عدد صحیح c، $ca \equiv cb$ (به پیمانهٔ n). ولی عکس این موضوع صادق نیست. به عنوان مثال، توجه کنید که گرچه $۲ \times ۴ \equiv ۲ \times ۱$ (به پیمانهٔ ۶)، ولی $۴ \not\equiv ۱$ (به پیمانهٔ ۶). به طور خلاصه، در حساب همنهشتیها همیشه نمی‌توان عامل مشترکی را آزادانه حذف کرد.

ولی با پیش‌شرطهای مناسبی، حذف مجاز است؛ یک گام مهم در این جهت، در قضیهٔ زیر شرح داده شده است.

قضیهٔ ۴ـ۳ اگر $ca \equiv cb$ (به پیمانهٔ n) و $d = \gcd(c, n)$ آنگاه $a \equiv b$ (به پیمانهٔ $\frac{n}{d}$).

اثبات. بنا به فرض، می‌توانیم به‌ازای عدد صحیح kای بنویسیم

$$c(a - b) = ca - cb = kn$$

چون $d = \gcd(c, n)$، عددهای صحیح متباین r و sای وجود دارند به طوری که $c = dr$ و $n = ds$. اگر این مقدارها در معادلهٔ فوق قرار داده شوند و عامل مشترک d حذف شود، نتیجه می‌گیریم

$$r(a - b) = ks$$

پس، $s|r(a - b)$ و $\gcd(r, s) = ۱$. بنا به لم اقلیدس $s|a - b$، یا $a \equiv b$ (به پیمانهٔ s)؛ به بیان دیگر، $a \equiv b$ (به پیمانهٔ $\frac{n}{d}$). □

قویترین حالت قضیهٔ ۴ـ۳ وقتی است که شرط $\gcd(c, n) = ۱$ اضافه شود، زیرا در این صورت می‌توان عمل حذف را بدون تغییری در پیمانه انجام داد.

فرع ۱. اگر $ca \equiv cb$ (به پیمانهٔ n) و $\gcd(c, n) = ۱$، آنگاه $a \equiv b$ (به پیمانهٔ n).

با اغتنام فرصت حالت خاصی از فرع ۱ را که مکرراً به کار خواهیم برد، ذکر می‌کنیم.

فرع ۲. اگر p عددی اول، $p \nmid c$، و $ca \equiv cb$ (به پیمانهٔ p)، آنگاه $a \equiv b$ (به پیمانهٔ p).

اثبات. شرطهای اول بودن p و $p \nmid c$ دلالت می‌کنند که $\gcd(c, p) = ۱$. □

مثال ۴ـ۴

همنهشتی $۳۳ \equiv ۱۵$ (به پیمانهٔ ۹) یا به عبارت دیگر $۳ \times ۱۱ \equiv ۳ \times ۵$ (به پیمانهٔ ۹) را در نظر می‌گیریم. چون $\gcd(۳, ۹) = ۳$، بنا به قضیهٔ ۴ـ۳، $۱۱ \equiv ۵$ (به پیمانهٔ ۳). مثال دیگر، همنهشتی $-۳۵ \equiv ۴۵$ (به پیمانهٔ ۸) است که صورت دیگر آن $۵ \times (-۷) \equiv ۵ \times ۹$ (به پیمانهٔ ۸) است. چون ۵ و ۸ متباین‌اند، می‌توانیم با حذف ۵ به همنهشتی هم‌ارز $-۷ \equiv ۹$ (به پیمانهٔ ۸) برسیم. ■

باید توجه کرد که در قضیهٔ ۴ـ۳، قید $c \not\equiv ۰$ (به پیمانهٔ n) ضروری نیست. در واقع، اگر $c \equiv ۰$ (به پیمانهٔ n)، آنگاه $\gcd(c, n) = n$ و حکم قضیه به صورت $a \equiv b$ (به پیمانهٔ ۱) درمی‌آید که پیشتر دیده‌ایم به‌ازای هر دوعدد صحیح a و b برقرار است.

حالت شگفت‌انگیز دیگری هم ممکن است در همنهشتیها پیش آید: ممکن است حاصلضرب دو عددِ صحیحِ ناهمنهشت با صفر، همنهشت با صفر باشد. به عنوان مثال، گرچه $۴ \times ۳ \equiv ۰$ (به پیمانهٔ ۱۲)، ولی $۳ \not\equiv ۰$ (به پیمانهٔ ۱۲) و $۴ \not\equiv ۰$ (به پیمانهٔ ۱۲). به سادگی می‌توان نشان داد که اگر $ab \equiv ۰$ (به پیمانهٔ n) و $\gcd(a, n) = ۱$، آنگاه $b \equiv ۰$ (به پیمانهٔ n)؛ زیرا طبق فرع ۱ در فوق مجازیم عامل a را از دوطرف همنهشتی $ab \equiv a \times ۰$ (به پیمانهٔ n) حذف کنیم. در حالت خاص، اگر p عددی اول باشد و $ab \equiv ۰$ (به پیمانهٔ p)، آنگاه یا $a \equiv ۰$ (به پیمانهٔ p) و یا $b \equiv ۰$ (به پیمانهٔ p).

تمرینهای ۴ـ۲

۱. هریک از حکمهای زیر را ثابت کنید:

(الف) اگر $a \equiv b$ (به پیمانهٔ n) و $m|n$، آنگاه $a \equiv b$ (به پیمانهٔ m).

(ب) اگر (به پیمانهٔ n) $a \equiv b$ و $c > \circ$، آنگاه (به پیمانهٔ cn) $ca \equiv cb$.

(پ) اگر (به پیمانهٔ n) $a \equiv b$ و عددهای صحیح a، b، n همه بر $d > \circ$ بخشپذیر باشند، آنگاه (به پیمانهٔ n/d) $a/d \equiv b/d$.

۲. با ارائهٔ مثالی نشان دهید که از (به پیمانهٔ n) $a^۲ \equiv b^۲$ لزوماً (به پیمانهٔ n) $a \equiv b$ نتیجه نمی‌شود.

۳. اگر (به پیمانهٔ n) $a \equiv b$، ثابت کنید که $\gcd(a, n) = \gcd(b, n)$.

۴. (الف) باقیمانده‌های تقسیم $۲^{۵۰}$ و $۴۱^{۶۵}$ بر ۷ را پیدا کنید.

(ب) باقیماندهٔ تقسیم مجموع

$$۱^۵ + ۲^۵ + ۳^۵ + \ldots + ۹۹^۵ + ۱۰۰^۵$$

بر ۴ چیست؟

۵. ثابت کنید که عدد صحیح $۵۳^{۱۰۳} + ۱۰۳^{۵۳}$ بر ۳۹ و $۱۱۱^{۳۳۳} + ۳۳۳^{۱۱۱}$ بر ۷ بخشپذیر است.

۶. اگر $n \geq ۱$، هر یک از حکمهای بخشپذیری زیر را با استفاده از نظریهٔ همنهشتی ثابت کنید:

(الف) $۷ | ۵^{۲n} + ۳ \times ۲^{۵n-۲}$

(ب) $۱۳ | ۳^{n+۲} + ۴^{۲n+۱}$

(پ) $۲۷ | ۲^{۵n+۱} + ۵^{n+۲}$

(ت) $۴۳ | ۶^{n+۲} + ۷^{۲n+۱}$

۷. اگر $n \geq ۱$، نشان دهید که

$$(-۱۳)^{n+۱} \equiv (-۱۳)^n + (-۱۳)^{n-۱} \quad (\text{به پیمانهٔ } ۱۸۱)$$

[راهنمایی: توجه کنید که (به پیمانهٔ ۱۸۱) $(-۱۳)^۲ \equiv -۱۳ + ۱$؛ از استقرا بر n استفاده کنید.]

۸. حکمهای زیر را ثابت کنید:

(الف) اگر a عدد صحیح فردی باشد، آنگاه (به پیمانهٔ ۸) $a^۲ \equiv ۱$.

(ب) به ازای هر عدد صحیح a، (به پیمانهٔ ۷) ۶ یا ۱ یا $a^۳ \equiv \circ$.

(پ) به ازای هر عدد صحیح a، (به پیمانهٔ ۵) ۱ یا $a^۴ \equiv \circ$.

(ت) اگر عدد صحیح a بر ۲ یا ۳ بخشپذیر نباشد، آنگاه (به پیمانهٔ ۲۴) $a^۲ \equiv ۱$.

۹. اگر p عددی اول باشد و $n < p < ۲n$، نشان دهید که

$$\binom{۲n}{n} \equiv \circ \quad (\text{به پیمانهٔ } p)$$

۱۰. اگر a_1، a_2، ...، a_n مجموعهٔ کاملی از ماندهها به پیمانهٔ n باشد و $\gcd(a, n) = 1$، ثابت کنید که aa_1، aa_2، ...، aa_n نیز مجموعهٔ کاملی از ماندهها به پیمانهٔ n است. [راهنمایی: کافی است نشان دهید که عددهای مزبور ناهمنهشت به پیمانهٔ nاند.]

۱۱. نشان دهید که $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ مجموعهٔ کاملی از ماندهها به پیمانهٔ ۱۱ تشکیل می‌دهند، ولی 0، 1^2، 2^2، 3^2، ...، 10^2، چنین مجموعه‌ای تشکیل نمی‌دهند.

۱۲. حکمهای زیر را ثابت کنید:

(الف) اگر $\gcd(a, n) = 1$، آنگاه به ازای هر c عددهای صحیح

$$c, c+a, c+2a, c+3a, \ldots, c+(n-1)a$$

مجموعهٔ کاملی از ماندهها به پیمانهٔ n تشکیل می‌دهند.

(ب) هر n عدد صحیح متوالی مجموعهٔ کاملی از ماندهها به پیمانهٔ n تشکیل می‌دهند. [راهنمایی: از قسمت (الف) استفاده کنید.]

(پ) حاصلضرب هر n عدد صحیح متوالی بر n بخشپذیر است.

۱۳. نشان دهید که اگر $a \equiv b$ (به پیمانهٔ n_1)، $a \equiv b$ (به پیمانهٔ n_2) و $n = \operatorname{lcm}(n_1, n_2)$، آنگاه $a \equiv b$ (به پیمانهٔ n). بنابراین، اگر n_1 و n_2 متباین باشند، $a \equiv b$ (به پیمانهٔ $n_1 n_2$).

۱۴. با آوردن مثالی نشان دهید که از $a^k \equiv b^k$ (به پیمانهٔ n) و $k \equiv j$ (به پیمانهٔ n) لزوماً $a^j \equiv b^j$ (به پیمانهٔ n) نتیجه نمی‌شود.

۱۵. ثابت کنید که اگر a عدد صحیح فردی باشد، آنگاه به‌ازای هر $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

[راهنمایی: به استقرا بر n عمل کنید.]

۱۶. با استفاده از نظریهٔ همنهشتی نشان دهید که

$$89 \mid 2^{44} - 1 \quad \text{و} \quad 97 \mid 2^{48} - 1$$

۱۷. ثابت کنید که اگر $ab \equiv cd$ (به پیمانهٔ n)، $b \equiv d$ (به پیمانهٔ n) و $\gcd(b, n) = 1$ آنگاه $a \equiv c$ (به پیمانهٔ n).

۱۸. اگر $a \equiv b$ (به پیمانهٔ n_1)، $a \equiv c$ (به پیمانهٔ n_2) و $n = \gcd(n_1, n_2)$، ثابت کنید که $b \equiv c$ (به پیمانهٔ n).

۴ـ۳ آزمونهای ویژهٔ تقسیمپذیری [بخشپذیری]

یکی از کاربردهای جالبتر نظریهٔ همنهشتی، پیدا کردن معیارهای ویژه‌ای برای بخشپذیری عدد صحیح داده شده‌ای بر عدد صحیح دیگر است. این آزمونهای بخشپذیری در اساس به دستگاه نمادهای به کار رفته برای دادن «نام» به عددهای صحیح و، به ویژه، به این نکته که عدد ۱۰ به عنوان پایهٔ دستگاه عددی ما انتخاب شده است، بستگی دارد. بنابراین، بحث را با نشان دادن این موضوع آغاز می‌کنیم که به ازای عدد صحیح داده شدهٔ b، $b > 1$، هرعدد صحیح مثبت N را می‌توان به‌طور یکتا برحسب توانهای b به صورت

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b + a_0$$

نوشت که درآن ضریبهای a_k می‌توانند b مقدار مختلف $0, 1, 2, \ldots, b-1$ را اختیار کنند. بنا به الگوریتم تقسیم، عددهای صحیح q_1 و a_0 وجود دارند به طوری که

$$N = q_1 + a_0, \qquad 0 \leq a_0 < b$$

اگر $q_1 \geq b$، می‌توانیم یک بار دیگر تقسیم کنیم؛ به‌دست می‌آوریم

$$q_1 = q_2 b + a_1, \qquad 0 \leq a_1 < b$$

اکنون q_1 را در معادلهٔ قبلی جایگزین می‌کنیم. در این صورت

$$N = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0$$

اگر $q_2 \geq b$، به همین روش ادامه می‌دهیم. با طی کردن مرحله‌ای دیگر: $q_2 = q_3 b + a_2$، که $0 \leq a_2 < b$، پس

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

چون $N > q_1 > q_2 > \ldots \geq 0$ دنباله‌ای اکیداً نزولی از عددهای صحیح است، این فرایند بالاخره در مرحله‌ای به پایان می‌رسد، مثلاً در $(m-1)$ امین مرحله، که

$$q_{m-1} = q_m b + a_{m-1}, \qquad 0 \leq a_{m-1} < b$$

و $0 \leq q_m < b$. با قرار دادن $a_m = q_m$ به نمایش

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b + a_0$$

می‌رسیم که مطلوب ما بود.

برای اثبات یکتایی، فرض می‌کنیم N دونمایش متمایز داشته باشد؛ یعنی

$$N = a_m b^m + \ldots + a_1 b + a_0 = c_m\, b^m + \ldots + c_1 b + c_0$$

به طوری که به ازای هر i، $0 \leq a_i < b$ و به ازای هر j، $0 \leq c_j < b$ (با افزودن جمله‌هایی با ضرایب $a_i = 0$ یا $c_j = 0$ در صورت لزوم، می‌توانیم توان m را یکی بگیریم). با تفریق نمایش دوم از اولی نتیجه می‌گیریم

$$0 = d_m b^m + \ldots + d_1\, b + d_0$$

که در آن به ازای هر i، $0 \leq i \leq m$، $d_i = a_i - c_i$. چون این دونمایشِ N را متفاوت فرض کردیم، به‌ازای iای باید داشته باشیم $d_i \neq 0$. کوچکترین اندیس iای را که به ازای آن $d_k \neq 0$، k می‌نامیم. پس

$$0 = d_m b^m + \ldots + d_{k+1}\, b^{k+1} + d_k b^k$$

و بنابراین، بعد از تقسیم بر b^k داریم

$$d_k = -b(d_m b^{m-k-1} + \ldots + d_{k+1})$$

یعنی، $b|d_k$. ولی، از نابرابریهای $0 \leq a_k < b$ و $0 \leq c_k < b$ نتیجه می‌شود $-b < a_k - c_k < b$، یا $|d_k| < b$. تنها راه سازگاری شرطهای $b|d_k$ و $|d_k| < b$ این است که $d_k = 0$، که غیرممکن است. از این تناقض نتیجه می‌گیریم که نمایش N یکتاست.

نکتهٔ اساسی در بحث فوق این است که عدد صحیح N کاملاً با دنبالهٔ a_m، a_{m-1}، ...، a_1، a_0 از ضریبها معین می‌شود و بنابراین توانهای b و علامتهای جمع زائد هستند. پس به‌جای عدد

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b + a_0$$

می‌توان نماد ساده‌تر

$$N = (a_m\, a_{m-1} \ldots a_2\, a_1\, a_0)_b$$

را در نظر گرفت (سمت راست را نباید حاصلضرب به‌حساب آورد، بلکه فقط صورتی اختصاری از N است). این نمایشِ N را نمایش N در پایهٔ b می‌نامند.

هرچه مقدار b کوچکتر باشد، نمایش عدد طویلتر است. ولی این حسن را دارد که ضریبهای لازم کمترند. ساده‌ترین حالت وقتی است که $b = 2$، و دستگاه شمارش حاصل را دستگاه عددهای

دودویی می‌نامند. این نکته که ضریبها در نمایش عددها در دستگاه دودویی فقط می‌توانند ۰ یا ۱ باشند به این معنی است که هر عدد صحیح مثبت فقط به یک روش به صورت مجموعی از توانهای متمایز ۲ قابل نمایش است. به عنوان مثال، عدد ۱۰۵ را می‌توان به صورت

$$\begin{aligned} ۱۰۵ &= ۱ \times ۲^{۶} + ۱ \times ۲^{۵} + ۰ \times ۲^{۴} + ۱ \times ۲^{۳} + ۰ \times ۲^{۲} + ۰ \times ۲ + ۱ \\ &= ۲^{۶} + ۲^{۵} + ۲^{۳} + ۱ \end{aligned}$$

یا، به صورت خلاصه شدهٔ

$$۱۰۵ = (۱۱۰۱۰۰۱)_{۲}$$

نوشت. برعکس

$$(۱۰۰۱۱۱۱)_{۲} = ۱ \times ۲^{۶} + ۰ \times ۲^{۵} + ۰ \times ۲^{۴} + ۱ \times ۲^{۳} + ۱ \times ۲^{۲} + ۱ \times ۲ + ۱ = ۷۹$$

دستگاه دودویی برای استفاده در کامپیوتر و ماشین‌حساب، مناسبترین دستگاه عددی است، زیرا عددهای دودویی با رشته‌هایی متشکل از ۰ و ۱ نمایش داده می‌شوند؛ ۰ و ۱ را در دستگاه کامپیوتر می‌توان با روشن و خاموش کردن کلیدی (یا ابزار الکترونیکی مشابهی) نشان داد.

معمولاً عددها را در دستگاه دهدهی، یعنی $b = ۱۰$، باحذف اندیس ۱۰ که مشخص کنندهٔ پایه است، می‌نویسیم. به عنوان مثال، نماد ۱۴۹۲ نشان دهندهٔ عبارت

$$۱ \times ۱۰^{۳} + ۴ \times ۱۰^{۲} + ۹ \times ۱۰ + ۲$$

است. عددهای صحیح ۱، ۴، ۹ و ۲ رقمهای عدد داده شده نامیده می‌شوند که ۱ رقم هزارگان، ۴ رقم صدگان، ۹ رقم دهگان، و ۲ رقم یکان است. به زبان فنی، نمایش عددهای صحیح مثبت به صورت مجموعهایی از توانهای ۱۰، با ضریبهایی حداکثر ۹، نمایش دهدهی آنها نامیده می‌شود.

اکنون می‌خواهیم محکهایی برای تعیین بخشپذیری عدد صحیح بر ۹ یا ۱۱، بدون انجام عمل تقسیم، به‌دست آوریم. به این منظور، به حکمی نیازمندیم که مربوط است به کاربرد همنهشتیها در مورد چند جمله‌ایهایِ با ضریبهای صحیح.

قضیهٔ ۴ـ۴ فرض کنید $P(x) = \sum_{k=0}^{m} c_k x^k$ تابعی چند جمله‌ای از x با ضریبهای صحیح c_k باشد. اگر $a \equiv b \ (n \text{ به پیمانهٔ})$، آنگاه $P(a) \equiv P(b) \ (n \text{ به پیمانهٔ})$.

اثبات. چون $a \equiv b \ (n \text{ به پیمانهٔ})$، بنا به بخش (۶) از قضیهٔ ۴ـ۲ داریم $a^k \equiv b^k \ (n \text{ به پیمانهٔ})$، $0 \le k \le m$. بنابراین به ازای هر چنین kای خواهیم داشت

$$c_k a^k \equiv c_k b^k \ (n \text{ به پیمانهٔ})$$

با جمع این $m+1$ همنهشتی، نتیجه می‌گیریم که

$$\sum_{k=0}^{m} c_k\, a^k \equiv \sum_{k=0}^{m} c_k\, b^k \ (\text{به پیمانهٔ } n)$$

و یا، با استفاده از نمادی متفاوت، خواهیم داشت $P(a) \equiv P(b)\ (\text{به پیمانهٔ } n)$. □

اگر $P(x)$ یک چندجمله‌ای با ضریبهای صحیح باشد، گوییم a جوابی از همنهشتی $P(x) \equiv 0\ (\text{به پیمانهٔ } n)$ است اگر $P(a) \equiv 0\ (\text{به پیمانهٔ } n)$.

فرع. اگر a جوابی از معادلهٔ $P(x) \equiv 0\ (\text{به پیمانهٔ } n)$ باشد و $a \equiv b\ (\text{به پیمانهٔ } n)$، آنگاه b نیز جوابی از آن است.

اثبات. بنا به قضیهٔ اخیر، می‌دانیم $P(a) \equiv P(b)\ (\text{به پیمانهٔ } n)$. پس، اگر a جوابی از معادلهٔ $P(x) \equiv 0\ (\text{به پیمانهٔ } n)$ باشد، آنگاه $P(b) \equiv P(a) \equiv 0\ (\text{به پیمانهٔ } n)$، یعنی b نیز جواب است. □

یک محک بخشپذیری که در ذهن داریم عبارت است از: عدد صحیح مثبت بر ۹ بخشپذیر است اگر و تنها اگر مجموع ارقام نمایش دهدهی‌اش بر ۹ بخشپذیر باشد.

قضیهٔ ۴ـ۵ فرض می‌کنیم $N = a_m \times 10^m + a_{m-1} \times 10^{m-1} + \ldots + a_1 \times 10 + a_0$ بسط دهدهی عدد صحیح مثبت N، $0 \le a_k < 10$، باشد و $S = a_0 + a_1 + \ldots + a_m$. در این صورت $9|N$ اگر و تنها اگر $9|S$.

اثبات. چندجمله‌ای $P(x) = \sum_{k=0}^{m} a_k\, x^k$ را که دارای ضرایب صحیح است در نظر می‌گیریم. نکتهٔ اصلی در این اثبات این است که $10 \equiv 1\ (\text{به پیمانهٔ } 9)$، و از اینجا بنا به قضیهٔ ۴ـ۴، $P(10) \equiv P(1)\ (\text{به پیمانهٔ } 9)$. ولی $P(10) = N$ و $P(1) = a_0 + a_1 + \ldots + a_m = S$، پس $N \equiv S\ (\text{به پیمانهٔ } 9)$. نتیجه می‌شود $N \equiv 0\ (\text{به پیمانهٔ } 9)$ اگر و تنها اگر $S \equiv 0\ (\text{به پیمانهٔ } 9)$، و این همان حکمی است که می‌خواستیم ثابت کنیم. □

قضیهٔ ۴ـ۴ مبنایِ آزمون معروفی برای بخشپذیری بر ۱۱ نیز هست؛ یعنی این محک که عدد صحیح بر ۱۱ بخشپذیر است اگر و تنها اگر مجموع متناوب رقمهایش بر ۱۱ بخشپذیر باشد. به بیان دقیقتر داریم:

قضیهٔ ۴ـ۶ فرض می‌کنیم $N = a_m ۱۰^m + a_{m-۱} ۱۰^{m-۱} + \ldots + a_۱ ۱۰ + a_۰$ نمایش دهدهی عدد صحیح مثبت N، $۰ \le a_k < ۱۰$، باشد و $T = a_۰ - a_۱ + a_۲ - \ldots + (-۱)^m a_m$. در این صورت، $۱۱ | N$ اگر و تنها اگر $۱۱ | T$.

اثبات. مانند اثبات قضیهٔ ۴ـ۵، قرار می‌دهیم $P(x) = \sum_{k=۰}^{m} a_k x^k$. چون $۱۰ \equiv -۱$ (به پیمانهٔ ۱۱)، به‌دست می‌آوریم $P(۱۰) \equiv P(-۱)$ (به پیمانهٔ ۱۱). ولی $N = P(۱۰)$، در صورتی که $P(-۱) = a_۰ - a_۱ + a_۲ - \ldots + (-۱)^m a_m = T$، بنابراین $N \equiv T$ (به پیمانهٔ ۱۱). نتیجه این است که یا هردوی N و T بر ۱۱ بخشپذیرند یا هیچ یک بر ۱۱ بخشپذیر نیست. □

مثال ۴ـ۵

برای ملاحظهٔ مثالی از دو قضیهٔ اخیر، عدد $N = ۱۵۷۱۷۲۴$ را در نظر می‌گیریم. چون مجموع

$$۱ + ۵ + ۷ + ۱ + ۷ + ۲ + ۴ = ۲۷$$

بر ۹ بخشپذیر است، قضیهٔ ۴ـ۵ تضمین می‌کند که N بر ۹ بخشپذیر است. این عدد بر ۱۱ نیز بخشپذیر است زیرا مجموع متناوب

$$۴ - ۲ + ۷ - ۱ + ۷ - ۵ + ۱ = ۱۱$$

بر ۱۱ بخشپذیر است. ■

تمرینهای ۴ـ۳

۱. حکمهای زیر را ثابت کنید:

(الف) به ازای هر عدد صحیح a، رقم یکان $a^۲$ یکی از عددهای ۰، ۱، ۴، ۵، ۶ و ۹ است.

(ب) هر یک از عددهای صحیح ۰، ۱، ۲، ۳، ۴، ۵، ۶، ۷، ۸، ۹ می‌تواند رقم یکان $a^۳$ باشد.

(پ) به ازای هرعدد صحیح a، رقم یکان $a^۴$ یکی از عددهای ۰، ۱، ۵، یا ۶ است.

(ت) رقم یکان هر عدد مثلثی یکی از عددهای ۰، ۱، ۳، ۵، ۶، یا ۸ است.

۲. دورقم آخر عدد $۹^{۹^{۹}}$ را پیدا کنید. [راهنمایی: $۹^{۹} \equiv ۹$ (به پیمانهٔ ۱۰)، پس $۹^{۹^{۹}} = ۹^{۹+۱۰k}$؛ اکنون از همنهشتی $۹^{۱۰} \equiv ۱$ (به پیمانهٔ ۱۰۰) استفاده کنید.]

۳. بدون عمل تقسیم، تعیین کنید که عددهای صحیح ۱۷۶۵۲۱۲۲۱ و ۱۴۹۲۳۵۶۷۸ بر ۹ یا ۱۱ بخشپذیرند یا نه.

۴. (الف) حکم زیر را که تعمیم قضیهٔ ۴ـ۵ است ثابت کنید: اگر نمایش عدد صحیح N در پایهٔ b به صورت

$$N = a_m b^m + \dots + a_۲ b^۲ + a_۱ b + a_۰ ,\quad ۰ \le a_k \le b - ۱$$

باشد، آنگاه $b-۱|N$ اگر و تنها اگر $b - ۱|(a_m + \dots + a_۲ + a_۱ + a_۰)$.

(ب) محکهایی برای بخشپذیری N در پایهٔ ۹ بر ۳ و ۸، برحسب رقمهای N در آن پایه، ارائه کنید.

(پ) آیا عدد صحیح $(۴۴۷۸۳۶)_۹$ بر ۳ و ۸ بخشپذیر است؟

۵. با استفاده از همنهشتیهای به پیمانه‌های ۹، ۱۱، رقمهای مجهول در برابریهای زیر را به‌دست آورید

(الف) $۵۱۸۴۰ \times ۲۷۳۵۸۱ = ۱۴۱۸۲۴۳x۰۴۰$

(ب) $۲x۹۹۵۶۱ = [۳(۵۲۳ + x)]^۲$

(پ) $۲۷۸۴x = x \times ۵۵۶۹$

(ت) $۵۱۲ \times ۱x۵۳۱۲۵ = ۱۰۰۰۰۰۰۰۰۰$

۶. محکهای بخشپذیری زیر را ثابت کنید:

(الف) عدد صحیح بر ۲ بخشپذیر است اگر و تنها اگر رقم یکان آن ۰، ۲، ۴، ۶ یا ۸ باشد.

(ب) عدد صحیح بر ۳ بخشپذیر است اگر و تنها اگر مجموع رقمهای آن بر ۳ بخشپذیر باشد.

(پ) عدد صحیح بر ۴ بخشپذیر است اگر و تنها اگر عدد متشکل از رقمهای دهگان و یکان آن بر ۴ بخشپذیر باشد. [راهنمایی: به ازای $k \ge ۲$، (به پیمانهٔ ۴) $۱۰^k \equiv ۰$.]

(ت) عدد صحیح بر ۵ بخشپذیر است اگر و تنها اگر رقم یکان آن ۰ یا ۵ باشد.

۷. نشان دهید که به ازای هر عدد صحیح a، $a^۲ - a + ۷$ به یکی از رقمهای ۳، ۷، یا ۹ ختم می‌شود.

۸. باقیماندهٔ تقسیم $۴۴۴۴^{۴۴۴۴}$ بر ۹ را پیدا کنید [راهنمایی: توجه کنید که (به پیمانهٔ ۹) $۲^۳ \equiv -۱$.]

۹. ثابت کنید هیچ عدد صحیحی که مجموع رقمهایش ۱۵ باشد، مربع یا مکعب نیست. [راهنمایی: به ازای هر a، (به پیمانهٔ ۹) ۸ یا $a^۳ \equiv ۰, ۱$.]

۱۰. به فرض بخشپذیری $۲۷۳x۴۹y۵$ بر ۴۹۵، رقمهای x و y را به‌دست آورید.

۱۱. سه رقم آخر عدد $۷^{۹۹۹}$ را تعیین کنید.

[راهنمایی: (به پیمانهٔ ۱۰۰۰) $۷^{۴n} \equiv (۱ + ۴۰۰)^n \equiv ۱ + ۴۰۰n$.]

۱۲. اگر t_n نشان دهندهٔ n امین عدد مثلثی باشد، نشان دهید که (به پیمانهٔ k) $t_{n+۲k} \equiv t_n$؛ و از اینجا t_n و $t_{n+۲۰}$ باید رقم آخر یکسانی داشته باشند.

۱۳. ثابت کنید که به ازای هر $n > ۱$، عدد اولی با دست‌کم n رقم صفر وجود دارد. [راهنمایی: تصاعد حسابی $۱۰^{n+۱}k + ۱$ به ازای $k = ۱, ۲, \ldots$ را درنظر بگیرید.]

۱۴. مقدارهایی از $n \geq ۱$ را پیدا کنید که به ازای آنها $۱! + ۲! + ۳! + \ldots + n!$ مربع کامل باشد. [راهنمایی: تمرین ۱ (الف).]

۱۵. نشان دهید ۲^n عدد صحیح N را می‌شمارد اگر و تنها اگر ۲^n عدد حاصل از n رقم آخر N را بشمارد. [راهنمایی: به ازای $k \geq n$، (به پیمانهٔ ۲^n) $۱۰^k = ۲^k \times ۵^k \equiv ۰$.]

۱۶. فرض می‌کنیم $N = a_m ۱۰^m + \ldots + a_۲ ۱۰^۲ + a_۱ ۱۰ + a_۰$، $۰ \leq a_k \leq ۹$، بسط دهدهی عدد صحیح مثبت N باشد.

(الف) ثابت کنید هر سه‌عدد ۷، ۱۱، و ۱۳ عدد N را می‌شمارند اگر و تنها اگر ۷، ۱۱، و ۱۳ عدد صحیح

$$M = (۱۰۰a_۲ + ۱۰a_۱ + a_۰) - (۱۰۰a_۵ + ۱۰a_۴ + a_۳)$$
$$+ (۱۰۰a_۸ + ۱۰a_۷ + a_۶) - \ldots$$

را بشمارند. [راهنمایی: اگر n زوج باشد، آنگاه به پیمانهٔ ۱۰۰۱ داریم $۱۰^{۳n} \equiv ۱$، $۱۰^{۳n+۱} \equiv ۱۰$، $۱۰^{۳n+۲} \equiv ۱۰۰$؛ اگر n فرد باشد، آنگاه به پیمانهٔ ۱۰۰۱ داریم $۱۰^{۳n} \equiv -۱$، $۱۰^{۳n+۱} \equiv -۱۰$، $۱۰^{۳n+۲} \equiv -۱۰۰$.]

(ب) ثابت کنید ۶، عدد N را می‌شمارد اگر و تنها اگر ۶ عدد صحیح $M = a_۰ + ۴a_۱ + ۴a_۲ + \ldots + ۴a_m$ را بشمارد.

۱۷. بدون انجام عمل تقسیم تعیین کنید که عدد صحیح ۱۰۱۰۹۰۸۸۹۹ برکدام یک از عددهای ۷، ۱۱، و ۱۳ بخشپذیر است.

۱۸. (الف) فرض می‌کنیم M، عدد صحیح حاصل از مقلوب کردن رقمهای عدد صحیح داده شدهٔ N باشد (به عنوان مثال، اگر $N = ۶۹۲۳$، آنگاه $M = ۳۲۹۶$). تحقیق کنید که $N - M$ بر ۹ بخشپذیر است.

(ب) مقلوب مستوی عددی است که با مقلوب خود برابر باشد (به عنوان مثال، ۳۷۳ و ۵۲۱۱۲۵ مقلوب مستوی‌اند.) ثابت کنید که هر عدد مقلوب مستوی که تعداد رقمهایش زوج باشد بر ۱۱ بخشپذیر است.

۱۹. اگر عدد R_n مرکب از n رقم یک باشد، نشان دهید

(الف) $۹|R_n$ اگر و تنهااگر $۹|n$.

(ب) $۱۱|R_n$ اگر و تنها اگر n زوج باشد.

۲۰. عدد $R_۶ = ۱۱۱۱۱۱$ را به حاصلضرب عددهای اول تجزیه کنید. [راهنمایی: تمرین ۱۶.]

۲۱. توضیح دهید چرا برابریهایِ شگفت‌انگیز زیر برقرارند:

$$۱\times ۹+۲=۱۱$$
$$۱۲\times ۹+۳=۱۱۱$$
$$۱۲۳\times ۹+۴=۱۱۱۱$$
$$۱۲۳۴\times ۹+۵=۱۱۱۱۱$$
$$۱۲۳۴۵\times ۹+۶=۱۱۱۱۱۱$$
$$۱۲۳۴۵۶\times ۹+۷=۱۱۱۱۱۱۱$$
$$۱۲۳۴۵۶۷\times ۹+۸=۱۱۱۱۱۱۱۱$$
$$۱۲۳۴۵۶۷۸\times ۹+۹=۱۱۱۱۱۱۱۱۱$$
$$۱۲۳۴۵۶۷۸۹\times ۹+۱۰=۱۱۱۱۱۱۱۱۱۱$$

[راهنمایی: تساوی $(۱۰^{n-۱}+۲\times۱۰^{n-۲}+۳\times۱۰^{n-۳}+\dots+n)(۱۰-۱)+(n+۱)=(۱۰^{n+۱}-۱)/۹$ را نشان دهید.]

۲۲. صورت حسابی قدیمی و تا اندازه‌ای ناخوانا نشان می‌دهد که ۷۲ کیلو گوشت گوساله به $x۶۷۹y$ تومان خریداری شده است. رقمهای مجهول را پیدا کنید.

۲۳. اگر ۷۹۲ عدد صحیح $۱۳xy۴۵z$ را بشمارد، رقمهای x، y، z را حساب کنید. [راهنمایی: بنا به تمرین ۱۵، $۸|۴۵z$.]

۴ـ۴ همنهشتیهای خطی

اکنون موقعیت مناسبی برای بررسی نظریهٔ همنهشتیهای خطی است: معادلهٔ به صورت $ax \equiv b$ (به پیمانهٔ n) همنهشتی خطی نامیده می‌شود، و منظور از جواب چنین معادله‌ای عدد صحیح $x_۰$ای است که $ax_۰ \equiv b$ (به پیمانهٔ n). بنا به تعریف، $ax_۰ \equiv b$ (به پیمانهٔ n) اگر و تنها اگر $n|ax_۰ - b$ یا، معادل آن، به‌ازای عدد صحیح $y_۰$ای، $ax_۰ - b = ny_۰$. بنابراین، مسألهٔ تعیین همهٔ عددهای صحیحِ صادق در همنهشتی خطی $ax \equiv b$ (به پیمانهٔ n) با مسألهٔ تعیین

همهٔ جوابهای معادلهٔ دیوفانتی خطی $ax - ny = b$ یکسان است. بنابراین، می‌توان از قضیه‌ها و نتیجه‌های فصل ۲ استفاده کرد.

جوابهایی از معادلهٔ $ax \equiv b$ (به پیمانهٔ n) را که همنهشت به پیمانهٔ nاند، هرچند به معنی معمول برابر نباشند، یکی می‌گیریم. به عنوان مثال، هردوی $x = ۳$ و $x = -۹$ در همنهشتی $۳x \equiv ۹$ (به پیمانهٔ ۱۲) صدق می‌کنند؛ چون $-۹ \equiv ۳$ (به پیمانهٔ ۱۲)، این دوعدد جوابهای متفاوتی محسوب نمی‌شوند. به طور خلاصه، وقتی صحبت از تعداد جوابهای $ax \equiv b$ (به پیمانهٔ n) است، منظور تعداد عددهای صحیح ناهمنهشتی است که در این همنهشتی صدق می‌کنند.

با توجه به این نکته‌ها، قضیهٔ اصلی این بخش را می‌توان به آسانی بیان کرد.

قضیهٔ ۴ـ۷ همنهشتی خطی $ax \equiv b$ (به پیمانهٔ n) دارای جواب است اگر و تنها اگر $d|b$، که $d = \gcd(a, n)$. اگر $d|b$، معادله دارای d جواب دوبه‌دو ناهمنهشت به پیمانهٔ n است.

اثبات. پیشتر دیده‌ایم که همنهشتی داده شده با معادلهٔ دیوفانتی خطی $ax - ny = b$ هم‌ارز است. بنا به قضیهٔ ۲ـ۹ می‌دانیم که، معادلهٔ اخیر حلپذیر است اگر و تنها اگر $d|b$؛ به علاوه، اگر حلپذیر باشد و $x_{\circ}$، $y_{\circ}$ جواب ویژه‌ای از آن باشد، آنگاه هر جواب دیگر، به ازای مقداری از t، به صورت

$$x = x_{\circ} + \frac{n}{d}t \quad , \quad y = y_{\circ} + \frac{a}{d}t$$

است.

از میان عددهای صحیح مختلفی که در فرمول اولی صدق می‌کنند، عددهایی را در نظر می‌گیریم که به‌ازای مقدارهای متوالی $t = ۰, ۱, ۲, \ldots, d - ۱$ به‌دست می‌آیند

$$x_{\circ}, x_{\circ} + \frac{n}{d}, x_{\circ} + \frac{۲n}{d}, \ldots, x_{\circ} + \frac{(d-۱)n}{d}$$

ادعا می‌کنیم این عددهای صحیح ناهمنهشت به پیمانهٔ nاند و هر عدد صحیح x دیگری که در فرمول صدق کند با یکی از آنها همنهشت است. اگر به ازای $۰ \leq t_۱ < t_۲ \leq d - ۱$ داشته باشیم

$$x_{\circ} + \frac{n}{d}t_۱ \equiv x_{\circ} + \frac{n}{d}t_۲ (\text{به پیمانهٔ } n)$$

آنگاه لازم می‌آید

$$\frac{n}{d}t_۱ \equiv \frac{n}{d}t_۲ (\text{به پیمانهٔ } n)$$

داریم $\gcd(n/d, n) = n/d$ و بنابراین، بنا به قضیهٔ ۴ـ۳، می‌توان با حذف عامل n/d به همنهشتی

$$t_۱ \equiv t_۲ (\text{به پیمانهٔ } d)$$

رسید که به معنی $d|t_2 - t_1$ است. ولی این امر، با توجه به نابرابریهای $0 < t_2 - t_1 < d$، غیرممکن است.

می‌ماند اینکه نشان دهیم هر جواب دیگر $x_0 + (n/d)\,t$ با یکی از d عدد صحیح مذکور در فوق همنهشت به پیمانهٔ n است. بنا به الگوریتم تقسیم، $t = qd + r$، $0 \leq r \leq d - 1$. پس

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n} \end{aligned}$$

که $x_0 + (n/d)\,r$ یکی از d جواب انتخابی ماست. به این ترتیب، اثبات به پایان می‌رسد. □

استدلالی که در قضیهٔ ۴ـ۷ ارائه کردیم نشان دهندهٔ نکته‌ای است که ارزش دارد به طور صریح عنوان شود: اگر x_0 جوابی از $ax \equiv b \pmod{n}$ باشد، آنگاه $d = \gcd(a, n)$ جواب ناهمنهشت به پیمانهٔ n عبارت‌اند از

$$x_0, x_0 + \frac{n}{d},\ x_0 + 2\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)$$

برای استفادهٔ خواننده، صورتی از قضیهٔ ۴ـ۷ را در حالت خاصی که a و b متباین فرض می‌شوند، ذکر می‌کنیم.

فرع. اگر $\gcd\,(a, n) = 1$، آنگاه همنهشتی خطی $ax \equiv b \pmod{n}$ دارای جواب یکتایی به پیمانهٔ n است.

این بحث را فعلاً کنار می‌گذاریم تا نظری به دو مثال مشخص بیندازیم.

مثال ۴ـ۶

معادلهٔ همنهشتی خطی $18x \equiv 30 \pmod{42}$ را در نظر می‌گیریم. چون $\gcd(18, 42) = 6$ و ۶ مطمئناً ۳۰ را می‌شمارد، قضیهٔ ۴ـ۷ وجود دقیقاً شش جواب را تضمین می‌کند، که ناهمنهشت به پیمانهٔ ۴۲اند. با جستجو، معلوم می‌شود که $x = 4$ یکی از جوابهاست. طبق تحلیل بالا، جوابهای ششگانه عبارت‌اند از

$$x \equiv 4 + \left(\frac{42}{6}\right)t \equiv 4 + 7t \pmod{42}, \qquad t = 0, 1, \ldots, 5$$

یا

$$x \equiv ۴, ۱۱, ۱۸, ۲۵, ۳۲, ۳۹ (\text{به پیمانهٔ } ۴۲) \quad \blacksquare$$

مثال ۴ـ۷

همنهشتی خطی $۹x \equiv ۲۱$ (به پیمانهٔ ۳۰) را درنظر می‌گیریم. در آغاز، چون $\gcd(۹, ۳۰) = ۳$ و $۳|۲۱$، می‌دانیم که باید سه جواب ناهمنهشت موجود باشد.

یکی از روشهای تعیین این جوابها، تقسیم همنهشتی داده شده بر ۳، یعنی در نظر گرفتن همنهشتی هم‌ارز $۳x \equiv ۷$ (به پیمانهٔ ۱۰) به‌جای آن است. متباین بودن ۳ و ۱۰ نشان می‌دهد که همنهشتی اخیر، جواب یکتایی به پیمانهٔ ۱۰ دارد. می‌توانیم عددهای ۰،۱،۲،...،۹ را به نوبت آزمایش کنیم تا جواب معادله به‌دست آید، ولی این روش، کارامدترین روش نیست. شیوهٔ بهتر این است: با ضرب طرفین همنهشتی $۳x \equiv ۷$ (به پیمانهٔ ۱۰) در ۷ به‌دست می‌آوریم

$$۲۱x \equiv ۴۹ (\text{به پیمانهٔ } ۱۰)$$

که به $x \equiv ۹$ (به پیمانهٔ ۱۰) تحویل می‌شود (این ساده‌سازی، تصادفی نیست زیرا مضربهای ۰×۳، ۱×۳، ۲×۳، ...، ۹×۳ مجموعهٔ کاملی از مانده‌ها به پیمانهٔ ۱۰ تشکیل می‌دهند؛ پس یکی از آنها لزوماً همنهشت با ۱ به پیمانهٔ ۱۰ است). ولی همنهشتی اصلی به پیمانهٔ ۳۰ است، و جوابهای ناهمنهشت آن جزء عددهای صحیح ۰، ۱، ۲، ...، ۲۹اند. با قراردادن $t = ۰, ۱, ۲$ در فرمول

$$x = ۹ + ۱۰t$$

به‌دست می‌آوریم ۹، ۱۹، ۲۹. بنابراین

$$x \equiv ۹ (\text{به پیمانهٔ } ۳۰)،\quad x \equiv ۱۹ (\text{به پیمانهٔ } ۳۰)،\quad x \equiv ۲۹ (\text{به پیمانهٔ } ۳۰)$$

سه‌جواب مطلوب همنهشتی $۹x \equiv ۲۱$ (به پیمانهٔ ۳۰) هستند.

روش متفاوتی برای حل این مسأله، استفاده از روش پیشنهادی در اثبات قضیهٔ ۴ـ۷ است. چون همنهشتی $۹x \equiv ۲۱$ (به پیمانهٔ ۳۰) هم‌ارز با معادلهٔ دیوفانتی خطی

$$۹x - ۳۰y = ۲۱$$

است، با نمایش $\gcd(۹, ۳۰) = ۳$ به‌صورت ترکیبی خطی از ۹ و ۳۰ آغاز می‌کنیم. با جستجو یا با استفاده از الگوریتم اقلیدسی، معلوم می‌شود که $۳ = ۹(-۳) + ۳۰ \times ۱$. پس

$$۲۱ = ۷ \times ۳ = ۹(-۲۱) - ۳۰(-۷)$$

بنابراین، $x = -۲۱$، $y = -۷$ در معادلهٔ دیوفانتی صدق می‌کنند و، در نتیجه، همهٔ جوابهای همنهشتی مورد بحث از فرمول

$$x = -۲۱ + \frac{۳۰}{۳}t = -۲۱ + ۱۰t$$

به‌دست می‌آیند. عددهای صحیح $x = -۲۱ + ۱۰t$، که در آن $t = ۰, ۱, ۲$ ، ناهمنهشت به پیمانهٔ ۳۰اند (ولی همگی همنهشت به پیمانهٔ ۱۰اند)؛ پس به جوابهای ناهمنهشت

$$x \equiv -۲۱ (\text{به پیمانهٔ } ۳۰)،\quad x \equiv -۱۱ (\text{به پیمانهٔ } ۳۰)،\quad x \equiv -۱ (\text{به پیمانهٔ } ۳۰)$$

یا، درصورت ترجیح دادن عددهای مثبت، به $x \equiv ۹, ۱۹, ۲۹$ (به پیمانهٔ ۳۰) می‌رسیم. ■

اکنون که تک همنهشتی خطی را بررسی کرده‌ایم، طبیعی است به بررسی مسألهٔ حل دستگاهی از همنهشتیهای خطی چون

$$a_1 x \equiv b_1 (\text{به پیمانهٔ } m_1)،\quad a_2 x \equiv b_2 (\text{به پیمانهٔ } m_2)،\quad \ldots،\quad a_r x \equiv b_r (\text{به پیمانهٔ } m_r)$$

بپردازیم. فرض می‌کنیم که پیمانه‌های m_k دوبه‌دو متباین‌اند. واضح است که دستگاه جوابی نخواهد داشت مگر اینکه هر یک از همنهشتیها جواب داشته باشد یعنی، به ازای هر k داشته باشیم $d_k | b_k$، که در آن $d_k = \gcd(a_k, m_k)$. هرگاه این شرطها برقرار باشند، می‌توان با حذف عامل d_k در همنهشتی kام، دستگاهی جدید (که مجموعهٔ جوابهایش با مجموعهٔ جوابهای دستگاه اولیه یکسان است) به‌دست آورد:

$$a'_1 x \equiv b'_1 (\text{به پیمانهٔ } n_1)،\quad a'_2 x \equiv b'_2 (\text{به پیمانهٔ } n_2)،\quad \ldots،\quad a'_r x \equiv b'_r (\text{به پیمانهٔ } n_r)$$

که درآن $n_k = m_k / d_k$ و به‌ازای $i \neq j$، $\gcd(n_i, n_j) = ۱$؛ همچنین $\gcd(a'_i, n_i) = ۱$. جوابهای این همنهشتیها به صورت

$$x \equiv c_1 (\text{به پیمانهٔ } n_1)،\quad x \equiv c_2 (\text{به پیمانهٔ } n_2)،\quad \ldots،\quad x \equiv c_r (\text{به پیمانهٔ } n_r)$$

در می‌آیند. بنابراین، مسأله مورد بحث تبدیل می‌شود به پیدا کردن جواب مشترک دستگاهی از همنهشتیها که از این نوعِ ساده‌ترند.

نوعی مسأله که به وسیلهٔ دستگاهی از همنهشتیها قابل حل است،سابقه‌ای طولانی دارد و از جمله در نوشته‌های چینی مربوط به نخستین سدهٔ میلادی دیده می‌شود. سون ـ تسو[1] می‌گوید: عددی پیدا

1. Sun-Tsu

کنید که باقیمانده‌های تقسیمش بر ۳، ۵، ۷، به ترتیب، ۲، ۳، ۲ باشد. (چنین معماهای ریاضی ابداً محدود به محیط فرهنگی خاصی نیست؛ در واقع، همین مسأله در مقدمات حساب نیکوماخوس، ریاضیدان یونانیِ حوالی ۱۰۰ میلادی، نیز دیده می‌شود.) به دلیل کارهای پیشگامانهٔ چینیها در این زمینه است که قاعدهٔ تعیین جواب دستگاههای مزبور معمولاً قضیهٔ باقیماندهٔ چینی نامیده می‌شود.

قضیهٔ ۴ـ۸ (قضیهٔ باقیماندهٔ چینی). فرض می‌کنیم n_1، n_2، ...، n_r عددهای صحیح مثبتِ دوبه‌دو متباینی هستند یعنی به‌ازای $i \neq j$، $\gcd(n_i, n_j) = 1$. در این صورت دستگاه همنهشتیهای خطی

$$x \equiv a_1 (\text{به پیمانهٔ } n_1)$$
$$x \equiv a_2 (\text{به پیمانهٔ } n_2)$$
$$\vdots$$
$$x \equiv a_r (\text{به پیمانهٔ } n_r)$$

جوابی دارد که به پیمانهٔ عدد صحیح $n_1 n_2 \ldots n_r$ یکتاست.

اثبات. با تشکیل حاصلضرب $n = n_1 n_2 \ldots n_r$ آغاز می‌کنیم. به‌ازای هر $k = 1, 2, \ldots, r$، قرار می‌دهیم

$$N_k = \frac{n}{n_k} = n_1 \ldots n_{k-1} n_{k+1} \ldots n_r$$

به بیان دیگر، N_k حاصلضرب همهٔ عددهای صحیح n_i به استثنای n_k است. بنا به فرض، n_iها دوبه‌دو متباین‌اند، پس $\gcd(N_k, n_k) = 1$. بنابراین، می‌توان طبق نظریهٔ تک‌همنهشتی خطی، همنهشتی $N_k x \equiv 1$ (به پیمانهٔ n_k) را حل کرد؛ جواب یکتای این همنهشتی را x_k می‌نامیم. ثابت می‌کنیم عدد صحیح

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$$

جوابی از دستگاهِ مفروض است.

نخست باید توجه کرد که اگر $i \neq k$، آنگاه $N_i \equiv 0$ (به پیمانهٔ n_k)، زیرا در این صورت $n_k | N_i$. نتیجه این است که

$$\overline{x} = a_1 N_1 x_1 + \ldots + a_r N_r x_r \equiv a_k N_k x_k (\text{به پیمانهٔ } n_k)$$

ولی عدد صحیح x_k طوری انتخاب شد که در همنهشتی (به پیمانهٔ n_k) $N_k x \equiv ۱$ صدق کند؛ بنابراین

$$\overline{x} \equiv a_k \times ۱ \equiv a_k (n_k \text{به پیمانهٔ})$$

این نشان می‌دهد که برای دستگاه همنهشتیهای داده شده جوابی وجود دارد.

برای اثبات یکتایی فرض می‌کنیم x' عدد صحیح دیگری است که در این همنهشتیها صدق می‌کند. در این صورت

$$\overline{x} \equiv a_k \equiv x' (n_k \text{به پیمانهٔ})، \qquad k = ۱, ۲, \ldots, r$$

و بنابراین به ازای هر مقدار k، $n_k | x - x'$. چون $\gcd(n_i, n_j) = ۱$، بنا به فرع ۲ی قضیهٔ ۲ـ۴، $n_۱ n_۲ \ldots n_r | x - x'$؛ پس (به پیمانهٔ n) $x \equiv x'$. به این ترتیب، اثبات قضیهٔ باقیماندهٔ چینی به‌انجام می‌رسد. □

مثال ۴ـ۸

مسأله‌ای که سون ـ تسو طرح کرده است متناظر با دستگاه متشکل از سه‌همنهشتی

$$x \equiv ۲ (\text{به پیمانهٔ}\ ۳)$$
$$x \equiv ۳ (\text{به پیمانهٔ}\ ۵)$$
$$x \equiv ۲ (\text{به پیمانهٔ}\ ۷)$$

است. با استفاده از شیوهٔ نمادگذاری در قضیهٔ ۴ـ۸، داریم $n = ۳ \times ۵ \times ۷ = ۱۰۵$ و

$$N_۱ = n/۳ = ۳۵ ،N_۲ = n/۵ = ۲۱ ،N_۳ = n/۷ = ۱۵$$

چون همنهشتیهای خطی

$$۳۵x \equiv ۱ (\text{به پیمانهٔ}\ ۳)،\ ۲۱x \equiv ۱ (\text{به پیمانهٔ}\ ۵)،\ ۱۵x \equiv ۱ (\text{به پیمانهٔ}\ ۷)$$

به ترتیب دارای جوابهای ۲، ۱، ۱ هستند، پس

$$\overline{x} = ۲ \times ۳۵ \times ۲ + ۳ \times ۲۱ \times ۱ + ۲ \times ۱۵ \times ۱ = ۲۳۳$$

جوابی به پیمانهٔ ۱۰۵ از دستگاه است و جواب یکتای (به پیمانهٔ ۱۰۵) $\overline{x} = ۲۳۳ \equiv ۲۳$ را به‌دست می‌آوریم. ■

مثال ۴ـ۹

مثال دوم ما حل همنهشتی خطی

$$۱۷x \equiv ۹ (\text{به پیمانهٔ } ۲۷۶)$$

است. چون $۲۳ \times ۴ \times ۳ = ۲۷۶$، حل همنهشتی فوق معادل با تعیین جوابی برای دستگاه همنهشتیهای زیر است

$$\begin{array}{lll} ۱۷x \equiv ۹ (\text{به پیمانهٔ } ۳) & \text{یا} & x \equiv ۰ (\text{به پیمانهٔ } ۳) \\ ۱۷x \equiv ۹ (\text{به پیمانهٔ } ۴) & & x \equiv ۱ (\text{به پیمانهٔ } ۴) \\ ۱۷x \equiv ۹ (\text{به پیمانهٔ } ۲۳) & & ۱۷x \equiv ۹ (\text{به پیمانهٔ } ۲۳) \end{array}$$

توجه کنید که اگر (به پیمانهٔ ۳) $x \equiv ۰$، آنگاه به‌ازای عدد صحیح kای، $x = ۳k$. این را در دومین همنهشتی دستگاه قرار می‌دهیم و به‌دست می‌آوریم

$$۳k \equiv ۱ (\text{به پیمانهٔ } ۴)$$

با ضرب طرفین این همنهشتی در ۳ نتیجه می‌شود

$$k \equiv ۹k \equiv ۳ (\text{به پیمانهٔ } ۴)$$

بنابراین $k = ۳ + ۴j$، که j عدد صحیحی است. پس

$$x = ۳(۳ + ۴j) = ۹ + ۱۲j$$

برای اینکه x در آخرین همنهشتی صدق کند، باید داشته باشیم

$$۱۷(۹ + ۱۲j) \equiv ۹ (\text{به پیمانهٔ } ۲۳)$$

یا (به پیمانهٔ ۲۳) $۲۰۴j \equiv -۱۴۴$، که به (به پیمانهٔ ۲۳) $۳j \equiv ۶$ یعنی به (به پیمانهٔ ۲۳) $j \equiv ۲$ تحویل می‌شود؛ از اینجا نتیجه می‌گیریم که به ازای عدد صحیح tای، $j = ۲ + ۲۳t$، و بنابراین

$$x = ۹ + ۱۲(۲ + ۲۳t) = ۳۳ + ۲۷۶t$$

نتیجه اینکه، (به پیمانهٔ ۲۷۶) ۳۳ $\equiv x$ جواب دستگاه همنهشتیها و نیز جواب (به پیمانهٔ ۲۷۶) ۹ $\equiv$ ۱۷x است. ■

تمرینهای ۴ـ۴

۱. همنهشتیهای خطی زیر را حل کنید:

(الف) (به پیمانهٔ ۲۹) ۱۵ $\equiv$ ۲۵x

(ب) (به پیمانهٔ ۲۶) ۲ $\equiv$ ۵x

(پ) (به پیمانهٔ ۲۱) ۱۵ $\equiv$ ۶x

(ت) (به پیمانهٔ ۱۰۲) ۸ $\equiv$ ۳۶x

(ث) (به پیمانهٔ ۹۸) ۶۰ $\equiv$ ۳۴x

(ج) (به پیمانهٔ ۳۰۱) ۱۳۳ $\equiv$ ۱۴۰x [راهنمایی: ۷ = gcd(۱۴۰, ۳۰۱).]

۲. با استفاده از همنهشتیها، معادله‌های دیوفانتی زیر را حل کنید:

(الف) ۹ = ۴x+۵۱y [راهنمایی: از (به پیمانهٔ ۵۱) ۹ $\equiv$ ۴x نتیجه می‌شود ۱۵+۵۱t = x، درحالی که از (به پیمانهٔ ۴) ۹ $\equiv$ ۵۱y نتیجه می‌شود ۳+۴s = y. رابطهٔ میان s و t را به‌دست آورید.]

(ب) ۳۳۱ = ۱۲x + ۲۵y

(پ) ۱۷ = ۵x − ۵۳y

۳. همهٔ جوابهای همنهشتی خطی (به پیمانهٔ ۱۳) ۱۱ $\equiv$ ۳x − ۷y را به‌دست آورید.

۴. هریک از دستگاههای همنهشتی زیر را حل کنید:

(الف) (به پیمانهٔ ۳) ۱ $\equiv x$، (به پیمانهٔ ۵) ۲ $\equiv x$، (به پیمانهٔ ۷) ۳ $\equiv x$.

(ب) (به پیمانهٔ ۱۱) ۵ $\equiv x$، (به پیمانهٔ ۲۹) ۱۴ $\equiv x$، (به پیمانهٔ ۳۱) ۱۵ $\equiv x$.

(پ) (به پیمانهٔ ۶) ۵ $\equiv x$، (به پیمانهٔ ۱۱) ۴ $\equiv x$، (به پیمانهٔ ۱۷) ۳ $\equiv x$.

(ت) (به پیمانهٔ ۵) ۱ $\equiv$ ۲x، (به پیمانهٔ ۶) ۹ $\equiv$ ۳x، (به پیمانهٔ ۷) ۱ $\equiv$ ۴x، (به پیمانهٔ ۱۱) ۹ $\equiv$ ۵x.

۵. همنهشتی خطی (به پیمانهٔ ۷ × ۵ × ۳ × ۲) ۳ $\equiv$ ۱۷x را با حل دستگاه

(به پیمانهٔ ۲) ۳ $\equiv$ ۱۷x، (به پیمانهٔ ۳) ۳ $\equiv$ ۱۷x، (به پیمانهٔ ۵) ۳ $\equiv$ ۱۷x، (به پیمانهٔ ۷) ۳ $\equiv$ ۱۷x

حل کنید.

۶. کوچکترین عدد صحیح ۲ < a را طوری پیدا کنید که

$$۲|a،\ ۳|a+۱،\ ۴|a+۲،\ ۵|a+۳،\ ۶|a+۴$$

۷. (الف) سه عدد صحیح متوالی پیدا کنید که هریک دارای عاملی به صورت مربع کامل باشد. [راهنمایی: عدد صحیح a را طوری پیدا کنید که $۲^۲|a$، $۳^۲|a+۱$، $۵^۲|a+۲$.]

(ب) سه‌عدد صحیح متوالی پیدا کنید که نخستین آنها بر مربع یک عدد، دومی بر مکعب یک عدد و سومی بر توان چهارم یک عدد بخشپذیر باشد.

۸. (برهمگوپته[1]، سدهٔ هفتم میلادی) هرگاه از سبد تخم‌مرغی هربار ۲تا یا هربار ۳تا یا هربار ۴تا یا هربار ۵تا یا هربار ۶تا تخم‌مرغ برداشته شود، بالاخره، به ترتیب، ۱، ۲، ۳، ۴، ۵ تخم‌مرغ باقی می‌ماند. اگر هربار ۷ تا تخم‌مرغ برداشته شود، چیزی باقی نمی‌ماند. در آغاز تعداد تخم‌مرغهای سبد حداقل چقدر است؟

۹. اغلب مسألهٔ سبد تخم‌مرغ به صورت زیر عنوان می‌شود: اگر هربار ۲تا یا هربار ۳تا یا هربار ۴تا یا هربار ۵تا یا هربار ۶تا تخم‌مرغ از سبد برداشته شود، ۱ تخم‌مرغ باقی می‌ماند؛ ولی اگر هربار ۷ تا برداشته شود، تخم‌مرغی باقی نمی‌ماند. در آغاز تعداد تخم‌مرغهای سبد حداقل چقدر است؟

۱۰. (مسألهٔ چینی باستان.) ۱۷ نفر دزد، به کمک هم کیسه‌ای پراز سکه‌های طلا دزدیدند. وقتی سکه‌ها را به طور برابر تقسیم کردند، سه‌سکه باقی ماند. در مشاجره‌ای که برسر تصاحب سکه‌های اضافی رخ داد، یکی از دزدان کشته شد. دوباره سکه‌ها را به‌طور برابر تقسیم کردند، این بار ۱۰ سکه باقی ماند. در مشاجرهٔ دوباره‌ای که راه افتاد، دزد دیگری کشته شد. به این ترتیب تقسیم برابر کل سکه‌ها میان بازماندگان ممکن شد. تعداد سکه‌های دزدیده شده حداقل چقدر بوده است؟

۱۱. ثابت کنید همنهشتیهای

$$x \equiv a \pmod{n} \quad \text{و} \quad x \equiv b \pmod{m}$$

دارای جواب مشترک هستند اگر و تنها اگر $\gcd(n,m)|a-b$؛ نشان دهید که جواب مشترک، در صورت وجود، به پیمانهٔ $\operatorname{lcm}(n,m)$ یکتاست.

۱۲. با استفاده از تمرین ۱۱ نشان دهید که دستگاه

$$x \equiv ۵ \pmod{۶} \quad \text{و} \quad x \equiv ۷ \pmod{۱۵}$$

جواب ندارد.

۱۳. اگر $x \equiv a \pmod{n}$، ثابت کنید یا $x \equiv a \pmod{۲n}$ یا $x \equiv a+n \pmod{۲n}$.

۱۴. باقیمانده‌های تقسیم عدد صحیحی بین ۱ و ۱۲۰۰ بر ۹، ۱۱، ۱۳، به ترتیب، ۱، ۲، ۶ است. این عدد صحیح چیست؟

1. Brahmagupta

۱۵. (الف) عدد صحیحی پیدا کنید که باقیمانده‌های تقسیمش بر ۲، ۳، ۶، ۱۲، به ترتیب، ۱، ۲، ۵، ۵ باشد. (یی‌خینگ[1]، متوفا در ۷۱۷.)

(ب) عدد صحیحی پیدا کنید که باقیمانده‌های تقسیمش بر ۳، ۴، ۵، ۶، به‌ترتیب، ۲، ۳، ۴، ۵ باشد. (بهاسکره[2] متولد ۱۱۱۴.)

(پ) عدد صحیحی پیدا کنید که باقیمانده‌های تقسیمش بر ۱۰، ۱۳، ۱۷، به‌ترتیب، ۳، ۱۱، ۱۵ باشد. (رگیومونتانوس[3]، ۱۴۳۶ـ۱۴۷۳.)

۱۶. فرض می‌کنیم t_n، nامین عدد مثلثی باشد. به ازای چه مقدارهای n، عدد t_n عدد $t_1^2 + t_2^2 + \ldots + t_n^2$ را می‌شمارد؟ [راهنمایی: چون

$$t_1^2 + t_2^2 + \ldots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$$

کافی است nهایی پیدا کنیم که به‌ازای آنها

$$3n^3 + 12n^2 + 13n + 2 \equiv 0 \quad (\text{به پیمانهٔ } 2 \times 3 \times 5)\text{.]}$$

۱۷. جوابهای دستگاه همنهشتیهای

$$3x + 4y \equiv 5 \; (\text{به پیمانهٔ } 13)$$
$$2x + 5y \equiv 7 \; (\text{به پیمانهٔ } 13)$$

را به‌دست آورید.

۱۸. دوجواب ناهمنهشت به پیمانهٔ ۲۱۰ دستگاه

$$2x \equiv 3 \; (\text{به پیمانهٔ } 5)$$
$$4x \equiv 2 \; (\text{به پیمانهٔ } 6)$$
$$3x \equiv 2 \; (\text{به پیمانهٔ } 7)$$

را به‌دست آورید.

---

1. Yih-hing 2. Bhaskara 3. Regiomontanus

۵

قضیهٔ فرما

«و شاید آیندگان از اینکه نشان داده‌ام قدیمیها همه‌چیز را نمی‌دانستند، سپاسگزار من باشند.»

پییر فرما

۵ـ۱ پییر دُ فرما

دانش به‌دست‌آمده در جهان باستان در دوران رخوت فکری در سده‌های میانه تا حد زیادی به فراموشی سپرده شد، و فقط بعد از سدهٔ دوازدهم بود که اروپای غربی دوباره متوجه ریاضیات گردید. ترجمهٔ آثار از یونانی و به‌ویژه از عربی به لاتینی، مایه تجدید حیات علمی به سبک گذشته شد. نخستین ترجمهٔ لاتینی نسخه‌های عربی رسالهٔ مهم اقلیدس یعنی اصول در ۱۱۲۰ عرضه شد. این ترجمه، روایت قابل‌اعتمادی از اصول نبود زیرا اصل اثر با ترجمه‌های غیردقیق متوالی از یونانی به عربی، سپس به کاستیلی، و بالاخره به لاتینی، درآمده و اشتباهات نسخه‌برداران ناوارد به محتوای کتاب نیز در مراحل مختلف به آن لطمه واردکرده بود. مع‌الوصف همین ترجمهٔ لاتینی، با همهٔ لغزشهایی که در آن راه یافته بود، تا سال ۱۵۰۵ که به اصل یونانی کتاب دست یافتند، مرجع اصلی همهٔ چاپهای شناخته‌شده در اروپا بود.

با تصرف قسطنطنیه به‌دست ترکان عثمانی در ۱۴۵۳، علمای بیزانسی که [قرنها] حافظان اصلی ریاضیات در آنجا بودند، شاهکارهای دانش یونان باستان را به باختر آوردند. نوشته‌اند که نسخه‌ای از باقیماندهٔ حساب دیوفانتوس در ۱۴۶۲ توسط یوهانس مولر[1] (که بیشتر به رگیومونتانوس معروف است و نام اخیر از صورت لاتینی نام زادگاهش کونیگسبرگ آمده است) در کتابخانهٔ واتیکان پیدا شده است. احتمالاً این نسخه را پناهندگان بیزانسی به رم آورده بودند. رگیومونتانوس ملاحظه کرد که «در این مقاله‌ها [ابواب کتاب] جوهر اصلی کل حساب مستتر است»، و کوشید دیگران را به ترجمهٔ آن علاقه‌مند کند. علی‌رغم این کوشش، کتاب تا انتشار نخستین ترجمه و نسخهٔ چاپی آن در ۱۵۷۲ توسط پرفسور آلمانی ویلهم هولتسمان[2]، که آثارش را به اسم مستعار کسیلاندر[3] (صورت یونانی هولتسمان) می‌نوشت، عملاً دور از دسترس باقی ماند. کتاب حساب وقتی کاملاً در دسترس ریاضیدانان اروپایی قرار گرفت که کلود باشه[4] ــ با اقتباس آزاد از کسیلاندر ــ متن اصلی یونانی را به همراه ترجمه‌ای لاتینی مشتمل بر یادداشتها و اظهارنظرهایی چاپ کرد (۱۶۲۱). احتمالاً همین چاپ از کتاب بود که توجه فرما را برای نخستین بار به مسائل نظریهٔ اعداد جلب کرد.

در تاریخ ریاضیات، کمتر دوره‌ای به اندازهٔ سدهٔ هفدهم بارآور بوده است؛ تعداد مردان برجسته‌ای که فقط اروپای شمالی در این دوره پروراند، کمتر از دورهٔ هزارسالهٔ پیش از آن نبود. در عصر مشاهیری چون دزارگ، دکارت، پاسکال، والیس، برنولی، لایب‌نیتس، و نیوتن، یک کارمند دولت فرانسه به‌نام پیر دُ فرما (۱۶۰۱ـ۱۶۶۵) شهرتی همتراز این علمای برجسته پیدا کرد. فرما، «شهریار آماتورها»، آخرین ریاضیدان بزرگی بود که ریاضیات را به‌عنوان یک مشغلهٔ فرعی در جوار حرفهٔ غیرعلمی خود دنبال می‌کرد. این حقوقدان و قاضی وابسته به مجلس ایالتی در تولوز، از مشاجرات روزمره به دنیای انتزاعی ریاضی پناه می‌برد. فرما ظاهراً آموزش خاصی در ریاضیات ندیده بود و تا پایان ۳۰ سالگی علاقه‌ای به مطالعهٔ ریاضی بروز نداد؛ از نظر او، ریاضیات فقط یک سرگرمی بود که اوقات فراغتش را پر می‌کرد. مع‌الوصف، هیچ‌یک از معاصرینِ حرفه‌ای او اکتشافاتی عظیمتر یا سهم مؤثرتری در پیشبرد ریاضیات نداشت: او به‌عنوان یکی از مبدعان هندسهٔ تحلیلی (این نام در اوایل قرن نوزدهم به این مبحث داده شد)، مبانی فنی حساب دیفرانسیل و انتگرال را پی‌ریزی کرد، و همراه با پاسکال، قواعد مفهومی نظریهٔ احتمال را تنظیم کرد. بی‌تردید عشق واقعی فرما در ریاضیات، نظریهٔ اعداد بود و آن را از زندان خرافات و راز و رمز، که مدتی طولانی در آن محبوس بود، نجات داد. کارهای او در این زمینه، کارهای دیگران را تحت‌الشعاع قرار داد، شاید بهتر باشد گفته شود که تجدید علاقه به وجه نظری نظریهٔ اعداد با کارهای فرما آغاز شد.

فرما لذت حاصل از تحقیقات ریاضی را به هرگونه شهرتی که ممکن بود از این رهگذر عاید

1. Johannes Müller 2. Holzmann 3. Xylander 4. Bachet

او شود، ترجیح می‌داد؛ درواقع، در سراسر زندگیش فقط یک نوشتهٔ مهم، آن هم ۵ سال پیش از وفاتش با امضای اختصاری گمراه‌کنندهٔ M.P.E.A.S. منتشر کرد. وی با خودداری سرسختانه از اینکه آثارش را به‌صورت نهایی درآورد، کوششهای متعددی را که دیگران برای چاپ نتایجش به‌نام او به‌عمل آوردند، عقیم ساخت. ولی مکاتبات فراوانش با ریاضیدانان معاصر، بی‌علاقگی او به انتشار مطلب را تا اندازه‌ای جبران کرده است. بخش اعظم اطلاعات مختصری که دربارهٔ کارهایش داریم، از نامه‌هایش به دوستانی که با آنها تبادل فکری داشت، یا موفقیتهایش را که به آنها گزارش می‌کرد، به‌دست آمده است. این دوستان با دست‌به‌دست‌گرداندن این نامه‌ها یا ارسال رونوشتهایی از آنها به سراسر قارهٔ اروپا، کوشش فراوانی برای شناسانیدن استعدادهای فرما به‌عمل آوردند.

چون انجام وظایف حرفه‌ای هر روز بیش از پیش وقت او را می‌گرفت، فرما ناچار می‌شد نتیجه‌های کار خود را در حاشیهٔ هرکتابی که اتفاقاً مورداستفاده‌اش بود، بنویسد. بسیاری از قضیه‌های معروفش در نظریهٔ اعداد در حاشیهٔ نسخهٔ شخصی فرما از کتاب دیوفانتوس چاپ باشه دیده می‌شوند. این قضیه‌ها را پسرش ساموئل پنج سال بعد از وفات او کشف کرد؛ وی چاپ جدیدی از حساب عرضه کرد که حواشی معروف پدرش را نیز به‌همراه داشت. چون در حاشیهٔ کتابها جای زیادی وجود ندارد، فرما عادت داشت نتیجه‌هایش را بدون ذکر اثبات یادداشت کند. ریاضیدانان پس از او بارها آرزو کرده‌اند که کاش حواشی کتاب حساب وسیعتر می‌بود یا اینکه فرما کمتر عادت به پنهان‌کردن روشهایش می‌داشت.

۲ـ۵ روش تجزیهٔ فرما

فرما در گوشه‌ای از نامه‌ای در ۱۶۴۳، که به احتمال قوی، خطاب به پدر روحانی مارین مرسن[1] بوده است روش ابداعی خود برای تجزیهٔ عددهای بزرگ را شرح داد. این نخستین پیشرفت واقعی نسبت به روش قدیمی پیداکردن عاملی از n با تقسیم n بر همهٔ عددهای اول تا بیشتر از $\sqrt{n}$ بود. نکتهٔ اصلی در روش فرما این است که جستجوی عاملهای عددصحیح فرد n (چون توانهای ۲ به‌آسانی قابل‌تشخیص‌اند و می‌توان آنها را در آغاز حذف کرد، فرض فردبودن n خللی به کلیت مطلب وارد نمی‌کند) معادل است با به‌دست آوردن جوابهای صحیح x و y معادلهٔ

$$n = x^2 - y^2$$

اگر n تفاضل دو مربع باشد، واضح است که آن را می‌توان به‌صورت

$$n = x^2 - y^2 = (x+y)(x-y)$$

1. Marin Mersenne

تجزیه کرد. برعکس، اگر n به‌صورت $n = ab$، $a \geq b \geq ۱$، قابل‌تجزیه باشد، می‌توانیم بنویسیم

$$n = \left(\frac{a+b}{۲}\right)^۲ - \left(\frac{a-b}{۲}\right)^۲$$

به‌علاوه، چون n عددصحیح فردی فرض می‌شود، خود a و b فردند؛ پس $(a+b)/۲$ و $(a-b)/۲$ عددهای صحیح نامنفیی هستند.

جستجو برای تعیین x و yای صادق در معادلهٔ $n = x^۲ - y^۲$، یا هم‌ارز با آن، معادلهٔ

$$x^۲ - n = y^۲$$

نخست با تعیین کوچکترین عددصحیح k، به‌طوری‌که $k^۲ \geq n$، آغاز می‌شود. اکنون متوالیاً عددهای

$$k^۲ - n ،(k+۱)^۲ - n ،(k+۲)^۲ - n ،(k+۳)^۲ - n ، \ldots$$

را بررسی می‌کنیم تا مقداری برای $m \geq \sqrt{n}$ بیابیم که $m^۲ - n$ به‌ازای آن مربع کامل باشد. این فرایند نمی‌تواند تا بینهایت ادامه یابد، زیرا بالاخره به

$$\left(\frac{n+۱}{۲}\right)^۲ - n = \left(\frac{n-۱}{۲}\right)^۲$$

می‌رسیم که نمایشی از nای متناظر با تجزیهٔ بدیهی $n = n \times ۱$ است. اگر به‌ازای هیچ عددصحیح mای با ضابطه $\sqrt{n} \leq m < (n+۱)/۲$، تفاضل $m^۲ - n$ مربع کامل نشود، آنگاه n عاملی جز n و ۱ ندارد، و در چنین حالتی n اول است.

فرما فرایند اخیرالذکر را برای تجزیهٔ

$$۲۰۲۷۶۵۱۲۸۱ = ۴۴۰۲۱ \times ۴۶۰۶۱$$

با طی فقط ۱۱ مرحله به‌کار برد. حال آنکه در روش قبلی، ۴۸۵۰ تقسیم بر عددهای اول فرد تا ۴۴۰۲۱ لازم است. شاید این مثال مناسب عمداً طرح شد تا امتیاز عمدهٔ این روش نشان داده شود: درکاربرد این روش نیازی به اطلاع از همهٔ عددهای اول کوچکتر از $\sqrt{n}$ برای به‌دست‌آوردن عاملی از n نیست.

مثال ۵ـ۱

برای توضیح کاربرد روش فرما عددصحیح $n = ۱۱۹۱۴۳$ را تجزیه می‌کنیم. با استفاده از جدولی از مربعهای اعداد، ملاحظه می‌کنیم که $۳۴۵^۲ < ۱۱۹۱۴۳ < ۳۴۶^۲$؛ بنابراین کافی است مقدارهای

$k^۲ - ۱۱۹۱۴۳$ را به‌ازای k های واقع در محدودهٔ $۳۴۶ \leq k < (۱۱۹۱۴۳+۱)/۲ = ۵۹۵۷۲$ درنظر بگیریم. محاسبات به‌صورت زیر آغاز می‌شود:

$$
\begin{aligned}
۳۴۶^۲ - ۱۱۹۱۴۳ &= ۱۱۹۷۱۶ - ۱۱۹۱۴۳ = ۵۷۳\\
۳۴۷^۲ - ۱۱۹۱۴۳ &= ۱۲۰۴۰۹ - ۱۱۹۱۴۳ = ۱۲۶۶\\
۳۴۸^۲ - ۱۱۹۱۴۳ &= ۱۲۱۱۰۴ - ۱۱۹۱۴۳ = ۱۹۶۱\\
۳۴۹^۲ - ۱۱۹۱۴۳ &= ۱۲۱۸۰۱ - ۱۱۹۱۴۳ = ۲۶۵۸\\
۳۵۰^۲ - ۱۱۹۱۴۳ &= ۱۲۲۵۰۰ - ۱۱۹۱۴۳ = ۳۳۵۷\\
۳۵۱^۲ - ۱۱۹۱۴۳ &= ۱۲۳۲۰۱ - ۱۱۹۱۴۳ = ۴۰۵۸\\
۳۵۲^۲ - ۱۱۹۱۴۳ &= ۱۲۳۹۰۴ - ۱۱۹۱۴۳ = ۴۷۶۱ = ۶۹^۲
\end{aligned}
$$

بنابه سطر آخر

$$۱۱۹۱۴۳ = ۳۵۲^۲ - ۶۹^۲ = (۳۵۲ + ۶۹)(۳۵۲ - ۶۹) = ۴۲۱ \times ۲۸۳$$

که هریک از عاملها عددی اول است. فقط با هفت آزمایش، عدد ۱۱۹۱۴۳ را به حاصلضربی از عددهای اول تجزیه کردیم. البته، همیشه این‌قدر بخت با ما یار نیست؛ ممکن است بیش از اینها طول بکشد تا تفاضلی که مربع باشد، به‌دست آید.

روش فرما به‌ویژه وقتی که n دارای دو عامل تقریباً برابر باشد، بسیار کارآمد است، زیرا در این حالت مربع مناسب به‌سرعت به‌دست می‌آید. به‌عنوان مثال، فرض می‌کنیم قرار باشد $n = ۲۳۴۴۹$ تجزیه شود. کوچکترین مربع بیشتر از n عدد $۱۵۴^۲$ است، بنابراین دنبالهٔ $k^۲ - n$ با

$$۱۵۴^۲ - ۲۳۴۴۹ = ۲۳۷۱۶ - ۲۳۴۴۹ = ۲۶۷$$

آغاز می‌شود. ولی

$$۱۵۵^۲ - ۲۳۴۴۹ = ۲۴۰۲۵ - ۲۳۴۴۹ = ۵۷۶ = ۲۴^۲$$

پس، عاملهای ۲۳۴۴۹ عبارت‌اند از

$$۲۳۴۴۹ = (۱۵۵ + ۲۴)(۱۵۵ - ۲۴) = ۱۷۹ \times ۱۳۱$$

به هنگام بررسی تفاضلهای $k^۲ - n$ به‌عنوان مربعهای احتمالی، بسیاری مقدارها را می‌توان بیدرنگ با توجه به رقمهای یکان حذف کرد. مثلاً، می‌دانیم، که رقم یکان هر مربعی باید یکی از

رقمهای ۰، ۱، ۴، ۵، ۶، ۹ باشد (تمرین ۱ (الف)، بخش ۴ـ۳). بنابراین، می‌توانیم همهٔ مقدارها در مثال فوق، بجز ۱۲۶۶، ۱۹۶۱، و ۴۷۶۱ را حذف کنیم. به‌علاوه با محاسبهٔ مربعهای عددهای از ۰ تا ۹۹ به پیمانهٔ ۱۰۰، ملاحظه می‌شود که، دو رقم آخر هریک از این مربعها باید یکی از بیست‌ودو عدد دورقمی زیر باشد:

۰۰	۲۱	۴۱	۶۴	۸۹
۰۱	۲۴	۴۴	۶۹	۹۶
۰۴	۲۵	۴۹	۷۶	
۰۹	۲۹	۵۶	۸۱	
۱۶	۳۶	۶۱	۸۴	

بنابراین می‌توان از بررسی عددصحیح ۱۲۶۶ صرف‌نظر کرد. چون ۶۱ جزو دو عددهای دورقمی مجاز است، کافی است فقط عددهای ۱۹۶۱ و ۴۷۶۱ را بررسی کرد؛ اولی مربع نیست، ولی $۴۷۶۱ = ۶۹^۲$. ■

تمرینهای ۵ـ۲

۱. عددهای زیر را به روش فرما تجزیه کنید

(الف) ۲۲۷۹

(ب) ۱۰۵۴۱

(پ) ۳۴۰۶۶۳ [راهنمایی: $۵۸۴^۲$ نخستین عدد مربع بزرگتر از ۳۴۰۶۶۳ است.]

۲. ثابت کنید دو رقم سمت راست هر عدد مربع باید به یکی از صورتهای زیر باشد: ۰۰، ۰۱، ۰۴، ۰۹، ۱۶، ۲۱، ۲۴، ۲۵، ۲۹، ۳۶، ۴۱، ۴۴، ۴۹، ۵۶، ۶۱، ۶۴، ۶۹، ۷۶، ۸۱، ۸۴، ۸۹، ۹۶ [راهنمایی: چون (به پیمانهٔ ۱۰۰) $x^۲ \equiv (۵۰ + x)^۲$ و (به پیمانهٔ ۱۰۰) $x^۲ \equiv (۵۰ - x)^۲$، کافی است دو رقم سمت راست $x^۲$ را به‌ازای ۲۶ مقدار $x = ۰, ۱, ۲, \ldots, ۲۵$ بررسی کنید.]

۳. عدد $۲^{۱۱} - ۱$ را به روش تجزیهٔ فرما تجزیه کنید.

۴. در ۱۶۴۷، مِرسن ملاحظه کرد که اگر بتوان عددی را به دو روش متمایز به‌صورت مجموعی از دو مربع متباین نوشت، عدد مزبور مرکب است و می‌توان آن را به‌صورت ذیل تجزیه کرد: اگر $n = a^۲ + b^۲ = c^۲ + d^۲$، آنگاه

$$n = (ac + bd)(ac - bd)/(a + d)(a - d)$$

با استفاده از این نتیجه عددهای

$$۴۹۳ = ۱۸^۲ + ۱۳^۲ = ۲۲^۲ + ۳^۲$$

$$۳۸۰۲۵ = ۱۶۸^۲ + ۹۹^۲ = ۱۵۶^۲ + ۱۱۷^۲$$

را تجزیه کنید.

۳ـ۵ قضیهٔ کوچک

مهمترین مخاطب فرما در نامه‌نگاریهایش در زمینهٔ نظریهٔ اعداد، کارمندی از ضرابخانهٔ فرانسه به‌نام برنار فرنیکل دو بسی[1] (۱۶۰۵ـ۱۶۷۵) بود که به‌خاطر استعدادش در بازی با عددهای بزرگ معروف بود. (توانایی فرنیکل در محاسبات عددی با توجه به ماجرای زیر معلوم می‌شود: فرما مسأله‌ای طرح کرده و در آن خواستار تعیین مکعبهایی شده بود که حاصل جمع آنها با مقسوم‌علیه‌های سره‌شان به‌صورت مربع کامل است، مانند $۷^۳ + (۱ + ۷ + ۷^۲) = ۲۰^۲$؛ فرنیکل به‌محض اینکه از این مسأله آگاه شد، ۴ مثال متفاوت ارائه کرد و فردای آن روز نیز شش مثال دیگر عرضه کرد.) گرچه فرنیکل به‌عنوان ریاضیدان ابداً همتراز با فرما نبود، تنها ریاضیدان معاصر او بود که می‌توانست فرما را در نظریهٔ اعداد به مبارزه بطلبد، و همین مبارزه‌طلبیها موجب فاش شدن برخی از دستاوردهای بسیار محرمانهٔ فرما شد. یکی از برجسته‌ترین آنها، این قضیه است: اگر p عددی اول و a عددی صحیح و بخش‌ناپذیر بر p باشد، آنگاه p عدد $a^{p-۱} - ۱$ را می‌شمارد. در ۱۸ اکتبر ۱۶۴۰، فرما این نتیجه را طی نامه‌ای به فرنیکل اطلاع داد. در این نامه یادآوری کرده بود که: «اگر اثبات بیش از حد طولانی نمی‌بود، آن را برای شما می‌نوشتم». این قضیه از آن زمان، برای متمایزشدن از قضیهٔ «مهم» یا «آخر» فرما، که موضوع اصلی فصل ۱۱ است، به «قضیهٔ کوچک» فرما معروف شده است. تقریباً صد سال سپری شد تا اویلر نخستین اثبات قضیهٔ کوچک را در ۱۷۳۶ منتشر کرد. ولی به‌نظر می‌رسد که از این افتخار سهمی به لایب‌نیتس نرسیده است زیرا او نیز، اندکی پیش از ۱۶۸۳، اثبات مشابهی از خود در دستنوشته‌ای منتشر نشده بر جای گذاشت.

اکنون به اثباتی از قضیهٔ فرما می‌پردازیم.

قضیهٔ ۵ـ۱ (قضیهٔ کوچک فرما). اگر p عددی اول باشد و $p \nmid a$، آنگاه $a^{p-۱} \equiv ۱ \pmod{p}$ (به پیمانهٔ p).

اثبات. با درنظرگرفتن $p - ۱$ مضرب مثبت نخست a آغاز می‌کنیم، یعنی عددهای صحیح a، $۲a$، $۳a$، …، $(p - ۱)a$. هیچ‌یک از این عددها با دیگری یا با صفر به پیمانهٔ p همنهشت

1. Bernhard Frénicle de Bessy

نیست. درواقع، اگر

$$(\text{به پیمانهٔ } p)\ ra \equiv sa \text{،} \qquad ۱ \leq r < s \leq p - ۱$$

آنگاه می‌توان با حذف a به $r \equiv s (p$ به پیمانهٔ$)$ رسید، که غیرممکن است. بنابراین، مجموعهٔ فوق از عددهای صحیح باید، با ترتیبی، با ۱، ۲، ۳، ...، $(p - ۱)$ همنهشت به پیمانهٔ p باشند. با ضرب همهٔ این همنشتیها درهم، ملاحظه می‌کنیم که

$$a \times ۲a \times ۳a \times \ldots \times (p - ۱)a \equiv ۱ \times ۲ \times ۳ \times \ldots \times (p - ۱)(p \text{ به پیمانهٔ})$$

یا

$$a^{p-۱}(p - ۱)! \equiv (p - ۱)!\ (p \text{ به پیمانهٔ})$$

با حذف $(p - ۱)!$ از هر دو طرف (این کار مجاز است زیرا $p \nmid (p - ۱)!$)، به $a^{p-۱} \equiv ۱\ (p$ به پیمانهٔ$)$ می‌رسیم، که همان قضیهٔ کوچک فرماست. □

این نتیجه را می‌توان به‌صورتی نسبتاً کلیتر، مستقل از شرط $p \nmid a$، بیان کرد.

فرع. اگر p عددی اول باشد، آنگاه به‌ازای هر عددصحیح a، $a^p \equiv a\ (p$ به پیمانهٔ$)$.

اثبات. وقتی $p|a$، حکم به‌وضوح برقرار است زیرا در این حالت، $a^p \equiv ۰ \equiv a\ (p$ به پیمانهٔ$)$. اگر $p \nmid a$، آنگاه طبق قضیهٔ فرما، $a^{p-۱} \equiv ۱\ (p$ به پیمانهٔ$)$. با ضرب این همنهشتی در a، نتیجهٔ $a^p \equiv a\ (p$ به پیمانهٔ$)$ حاصل می‌شود. □

اثبات دیگری برای گزارهٔ $a^p \equiv a\ (p$ به پیمانهٔ$)$ وجود دارد که مستلزم استقرا بر a است. اگر $a = ۱$، داریم $۱^p \equiv ۱\ (p$ به پیمانهٔ$)$ که به‌وضوح درست است؛ اگر هم $a = ۰$، حکم برقرار است. فرض می‌کنیم حکم به‌ازای a برقرار باشد و برقراری آن را به‌ازای $a + ۱$ نشان می‌دهیم. طبق قضیهٔ دوجمله‌ای

$$(a + ۱)^p = a^p + \binom{p}{۱} a^{p-۱} + \ldots + \binom{p}{k} a^{p-k} + \ldots + \binom{p}{p - ۱} a + ۱$$

که در آن

$$\binom{p}{k} = \frac{p!}{k!(p - k)!} = \frac{p(p - ۱) \ldots (p - k + ۱)}{۱ \times ۲ \times \ldots \times k}$$

استدلال ما مبتنی بر این حقیقت است که به‌ازای $1 \le k \le p - 1$، داریم $\binom{p}{k} \equiv 0$ (به پیمانهٔ p). برای اثبات این نکته، توجه کنید که

$$k!\binom{p}{k} = p(p-1)\dots(p-k+1) \equiv 0 \ (\text{به پیمانهٔ } p)$$

که بنابه آن، $p|k!$ یا $p|\binom{p}{k}$. ولی از $p|k!$ نتیجه می‌شود که به‌ازای j ای که $1 \le j \le k \le p-1$، داریم $p|j$، که غیرممکن است. پس، $p|\binom{p}{k}$ یا، به‌عبارت دیگر

$$\binom{p}{k} \equiv 0 \ (\text{به پیمانهٔ } p)$$

نکته‌ای که می‌خواهیم نتیجه بگیریم این است که

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \ (\text{به پیمانهٔ } p)$$

که آخرین همنهشتی سمت راست با استفاده از فرض استقرا به‌دست می‌آید. بنابراین، همنهشتی مطلوب به‌ازای $a+1$ و، درنتیجه، به‌ازای هر $a \ge 0$ ای برقرار است. اگر a عددی صحیح و منفی باشد، باز حکم برقرار است: چون به‌ازای r ای، $0 \le r \le p - 1$، داریم $a \equiv r$ (به پیمانهٔ p)، پس $a^p \equiv r^p \equiv r \equiv a$ (به پیمانهٔ p).

قضیهٔ فرما کاربردهای بسیاری دارد و در بخش بزرگی از کارهایی که در نظریهٔ اعداد انجام می‌شود دارای نقش حیاتی است. این قضیه ابزار کارایی برای کوتاهترکردن برخی از محاسبات است. اگر، به‌عنوان نمونه، خواسته شود که ثابت کنیم $5^{38} \equiv 4$ (به پیمانهٔ ۱۱)، از همنهشتی $5^{10} \equiv 1$ (به پیمانهٔ ۱۱) برای شروع کار استفاده می‌کنیم. بنابراین

$$\begin{aligned} 5^{38} &= 5^{10 \times 3 + 8} = (5^{10})^3 (5^2)^4 \\ &\equiv 1^3 \times 3^4 = 81 \equiv 4 \ (\text{به پیمانهٔ } 11) \end{aligned}$$

کاربرد دیگر قضیهٔ فرما در آزمون اول بودن عددصحیح داده‌شدهٔ n ای است، زیرا اگر بشود نشان داد که به‌ازای a ای، همنهشتی

$$a^n \equiv a \ (\text{به پیمانهٔ } n)$$

برقرار نیست، آنگاه n لزوماً مرکب است. به‌عنوان مثالی از کاربرد این روش، $n = ۱۱۷$ را درنظر می‌گیریم. با انتخاب مقدار صحیح کوچکی برای a، مثلاً $a = ۲$، می‌توان از طول محاسبه کاست. چون می‌توانیم بنویسیم

$$۲^{۱۱۷} = ۲^{۷\times۱۶+۵} = (۲^۷)^{۱۶} \times ۲^۵$$

و $۲^۷ = ۱۲۸ \equiv ۱۱$ (به پیمانهٔ ۱۱۷)، پس داریم

$$۲^{۱۱۷} \equiv ۱۱^{۱۶} \times ۲^۵ \equiv (۱۲۱)^۸ \times ۲^۵ \equiv ۴^۸ \times ۲^۵ = ۲^{۲۱} \ (\text{به پیمانهٔ } ۱۱۷)$$

ولی $(۲^۷)^۳ = ۲^{۲۱}$، که منجر می‌شود به

$$۲^{۲۱} \equiv ۱۱^۳ \equiv ۱۲۱ \times ۱۱ \equiv ۴ \times ۱۱ \equiv ۴۴ \ (\text{به پیمانهٔ } ۱۱۷)$$

با ترکیب این همنهشتیها بالاخره به‌دست می‌آوریم

$$۲^{۱۱۷} \equiv ۴۴ \not\equiv ۲ \ (\text{به پیمانهٔ } ۱۱۷)$$

بنابراین ۱۱۷ باید مرکب باشد؛ درواقع، $۱۱۷ = ۱۳ \times ۹$.

بد نیست با آوردن مثالی نشان دهیم که عکس قضیهٔ فرما برقرار نیست، به‌عبارت دیگر، نشان دهیم که اگر به‌ازای عددصحیح a ای، $a^{n-۱} \equiv ۱$ (به پیمانهٔ n)، آنگاه n لزوماً اول نیست. ابتدا به یک لم تکنیکی نیازمندیم:

لم. اگر p و q عددهای اول متمایزی باشند به‌طوری که $a^p \equiv a$ (به پیمانهٔ q) و $a^q \equiv a$ (به پیمانهٔ p)، آنگاه $a^{pq} \equiv a$ (به پیمانهٔ pq).

اثبات. بنابه فرع اخیر، می‌دانیم $(a^q)^p \equiv a^q$ (به پیمانهٔ p)، و بنابه فرض، $a^q \equiv a$ (به پیمانهٔ p). با ترکیب این همنهشتیها به‌دست می‌آوریم $a^{pq} \equiv a$ (به پیمانهٔ p) یا، به بیان دیگر، $p|a^{pq} - a$. به روشی کاملاً مشابه نشان داده می‌شود که $q|a^{pq} - a$. پس، بنابه فرع قضیهٔ ۲ـ۴، $pq|a^{pq} - a$، که می‌توان آن را به‌صورت $a^{pq} \equiv a$ (به پیمانهٔ pq) نوشت. □

اکنون نشان می‌دهیم $۲^{۳۴۰} \equiv ۱$ (به پیمانهٔ ۳۴۱) که در آن $۳۴۱ = ۱۱ \times ۳۱$. برای حرکت در این جهت توجه می‌کنیم که $۲^{۱۰} = ۱۰۲۴ = ۳۱ \times ۳۳ + ۱$. پس

$$۲^{۱۱} = ۲ \times ۲^{۱۰} \equiv ۲ \times ۱ \equiv ۲ \ (\text{به پیمانهٔ } ۳۱)$$

و

$$۲^{۳۱} = ۲(۲^{۱۰})^{۳} \equiv ۲ \times ۱^{۳} \equiv ۲ \text{ (به پیمانهٔ ۱۱)}$$

با استفاده از لم، داریم

$$۲^{۱۱ \times ۳۱} \equiv ۲ \text{ (به پیمانهٔ ۳۱} \times ۱۱)$$

یا $۲^{۳۴۱} \equiv ۲$ (به پیمانهٔ ۳۴۱). با حذف عامل ۲ به

$$۲^{۳۴۰} \equiv ۱ \text{ (به پیمانهٔ ۳۴۱)}$$

می‌رسیم که نشان می‌دهد عکس قضیهٔ فرما برقرار نیست.

علاقهٔ تاریخی به عددهای به‌صورت $۲^n - ۲$ از ادعای ریاضیدانان چینی ۲۵ سده پیش مبنی بر اینکه n اول است اگر و تنها اگر $n | ۲^n - ۲$، نشأت گرفته است (درواقع این محک به‌ازای هر عددصحیح $n \leq ۳۴۰$، قابل‌اعتماد است). نیازی به گفتن نیست که مثال فوق که در آن $۳۴۱ | ۲^{۳۴۱} - ۲$ و $۳۴۱ = ۱۱ \times ۳۱$، این ادعا را رد می‌کند؛ این مثال در سال ۱۸۱۹ کشف شد. حالتی که در آن $n | ۲^n - ۲$، آنقدر پیش می‌آید که شایسته است نام خاصی داشته باشد: عددصحیح مرکب n اوّلنما نامیده می‌شود اگر $n | ۲^n - ۲$. می‌توان نشان داد که بینهایت عدد اوّلنما وجود دارد و چهار تا از آنها که از بقیه کوچکترند عبارت‌اند از: ۳۴۱، ۵۶۱، ۶۴۵، و ۱۱۰۵.

به کمک قضیهٔ زیر می‌توانیم دنباله‌ای صعودی از اوّلنماها بسازیم.

قضیهٔ ۵ـ۲ اگر عدد n اوّلنمای فردی باشد، آنگاه $M_n = ۲^n - ۱$ اوّلنمای بزرگتری است.

اثبات. چون n عدد مرکبی است، می‌توانیم بنویسیم $n = rs$، که $۱ < r \leq s < n$. پس، بنابه تمرین ۲۱ در بخش ۲ـ۲، $۲^r - ۱ | ۲^n - ۱$، یا به‌عبارت دیگر $۲^r - ۱ | M_n$، که نشان می‌دهد M_n عددی مرکب است. بنابه فرض، $۲^n \equiv ۲$ (به پیمانهٔ n)، و بنابراین به‌ازای عددصحیح k ای، $kn = ۲^n - ۲$. نتیجه می‌شود که

$$۲^{M_n - ۱} = ۲^{۲^n - ۲} = ۲^{kn}$$

از اینجا داریم

$$\begin{aligned} ۲^{M_n-۱} - ۱ &= ۲^{kn} - ۱ \\ &= (۲^n - ۱)(۲^{n(k-۱)} + ۲^{n(k-۲)} + \ldots + ۲^n + ۱) \\ &= M_n(۲^{n(k-۱)} + ۲^{n(k-۲)} + \ldots + ۲^n + ۱) \\ &\equiv ۰ \ (\text{به پیمانهٔ } M_n) \end{aligned}$$

پس، $۲^{M_n} - ۲ \equiv ۰ \ (\text{به پیمانهٔ } M_n)$، و بنابراین M_n اوّلنماست. □

حکمی مشابه قضیهٔ دیریکله (در ۱۹۶۳) ثابت شده است مبنی بر اینکه هر تصاعد حسابی $an + b$، $n = ۱, ۲, \ldots$، به‌شرط $\gcd(a, b) = ۱$ حاوی بینهایت اوّلنماست. مع‌الوصف، این «اولهای جعلی» بسیار نادرتر از اولهای واقعی‌اند؛ به‌عنوان مثال، در مقایسه با ۷۸۴۹۲ عدد اول کوچکتر از یک میلیون، فقط ۲۴۵ اولنمای کوچکتر از یک میلیون وجود دارد. نخستین مثال از اولنمای زوج، یعنی عدد

$$۱۶۱۰۳۸ = ۲ \times ۷۳ \times ۱۱۰۳$$

در ۱۹۵۰ کشف شد.

عددهای مرکب nای وجود دارند با این خاصیت که به‌ازای هر عددصحیح a، $a^n \equiv a \ (\text{به پیمانهٔ } n)$. کوچکترین عدد در میان این n ها ۵۶۱ است. این عددهای استثنایی اولنماهای مطلق یا، به افتخار کارمایکل[1] ریاضیدانی که برای نخستین بار (در ۱۹۰۹) متوجه وجود چنین عددهایی شد، عددهای کارمایکل نامیده می‌شوند. برای ملاحظه اینکه $۵۶۱ = ۳ \times ۱۱ \times ۱۷$ اولنمایی مطلق است، توجه می‌کنیم که از $\gcd(a, ۵۶۱) = ۱$ نتیجه می‌شود

$$\gcd(a, ۳) = \gcd(a, ۱۱) = \gcd(a, ۱۷) = ۱$$

پس، بنابه قضیهٔ فرما، همنهشتیهای

$$a^{۲} \equiv ۱ \ (\text{به پیمانهٔ } ۳), a^{۱۰} \equiv ۱ \ (\text{به پیمانهٔ } ۱۱), a^{۱۶} \equiv ۱ \ (\text{به پیمانهٔ } ۱۷)$$

و، به‌ترتیب، همنهشتیهای

$$a^{۵۶۰} \equiv (a^{۲})^{۲۸۰} \equiv ۱ \ (\text{به پیمانهٔ } ۳)$$

1. R. C. Carmichael

$$a^{۵۶۰} \equiv (a^{۱۰})^{۵۶} \equiv ۱ \quad (\text{به پیمانهٔ } ۱۱)$$
$$a^{۵۶۰} \equiv (a^{۱۶})^{۳۵} \equiv ۱ \quad (\text{به پیمانهٔ } ۱۷)$$

به‌دست می‌آیند. اینها منجر به همنهشتی $a^{۵۶۰} \equiv ۱$ (به پیمانهٔ ۵۶۱)، که در آن $\gcd(a, ۵۶۱) = ۱$، می‌شوند. ولی در این صورت به‌ازای هر a، $a^{۵۶۱} \equiv a$ (به پیمانهٔ ۵۶۱)، و این نشان می‌دهد که ۵۶۱ اوّلنمایی مطلق است.

اکنون قضیه‌ای ارائه می‌کنیم که از آن می‌توان برای تولید اوّلنماهای مطلق استفاده کرد.

قضیهٔ ۵ـ۳ فرض می‌کنیم n یک عددصحیح مرکب خالی از مربع، مثلاً $n = p_۱p_۲\ldots p_r$، که p_i ها عددهای اول متمایزی هستند، باشد. اگر به‌ازای هر $i = ۱, ۲, \ldots, r$، $p_i - ۱ | n - ۱$، آنگاه n اولنمای مطلقی است.

اثبات. فرض می‌کنیم a عددی صحیح است به‌طوری که $\gcd(a, n) = ۱$ و به‌ازای هر i، $\gcd(a, p_i) = ۱$. در این صورت، بنابه قضیهٔ فرما، $p_i | a^{p_i - ۱} - ۱$. چون $p_i - ۱ | n - ۱$، داریم $p_i | a^{n-۱} - ۱$، و بنابراین به‌ازای هر a و $i = ۱, ۲, \ldots, r$، $p_i | a^n - a$. و بالاخره به‌عنوان نتیجه‌ای از فرع قضیهٔ ۲ـ۴ داریم $n | a^n - a$، که نشان می‌دهد n اوّلنمای مطلقی است. □

مثالهایی از عددهای صحیح صادق در شرطهای قضیهٔ ۵ـ۳ عبارت‌اند از

$$۱۷۲۹ = ۷ \times ۱۳ \times ۱۹،\ ۶۶۰۱ = ۷ \times ۲۳ \times ۴۱،\ \text{و}\ ۱۰۵۸۵ = ۵ \times ۲۹ \times ۷۳$$

اعتقاد عمومی این است که بینهایت اولنمای مطلق وجود دارد، ولی این حدس هنوز ثابت نشده است، و فقط ۴۳ اولنمای مطلق کوچکتر از یک میلیون وجود دارد.

تمرینهای ۵ـ۳

۱. نشان دهید که به‌ازای $k = ۱, ۲, ۳$، $۱۸^{۶} \equiv ۱$ (به پیمانهٔ ۷^k).

۲. (الف) اگر $\gcd(a, ۳۵) = ۱$، نشان دهید $a^{۱۲} \equiv ۱$ (به پیمانهٔ ۳۵). [راهنمایی. بنابه قضیهٔ فرما، $a^{۶} \equiv ۱$ (به پیمانهٔ ۷) و $a^{۴} \equiv ۱$ (به پیمانهٔ ۵).]

(ب) اگر $\gcd(a, ۴۲) = ۱$، نشان دهید که $۱۶۸ = ۳ \times ۷ \times ۸$، $a^{۶} - ۱$ را می‌شمارد.

(پ) اگر $\gcd(a, ۱۳۳) = \gcd(b, ۱۳۳) = ۱$، نشان دهید $۱۳۳ | a^{۱۸} - b^{۱۸}$.

۳. ثابت کنید بینهایت عدد مرکب n وجود دارد که به‌ازای آنها $a^{n-۱} \equiv a$ (به پیمانهٔ n). [راهنمایی: n را برابر $۲p$ بگیرید، که p عدد اول فردی است.]

۴. هریک از همنهشتیهای زیر را ثابت کنید:

(الف) به‌ازای هر a، (به پیمانهٔ ۱۵) $a^{۲۱} \equiv a$. [راهنمایی: بنا به قضیهٔ فرما، (به پیمانهٔ ۵) $a^{۵} \equiv a$.]

(ب) به‌ازای هر a، (به پیمانهٔ ۴۲) $a^{۷} \equiv a$.

(پ) به‌ازای هر a، (به پیمانهٔ $۳ \times ۷ \times ۱۳$) $a^{۱۳} \equiv a$.

(ت) به‌ازای هر a، (به پیمانهٔ ۳۰) $a^{۹} \equiv a$.

۵. اگر $\gcd(a, ۳۰) = ۱$، نشان دهید عدد ۶۰ عدد $a^{۴} + ۵۹$ را می‌شمارد.

۶. (الف) با استفاده از قضیهٔ فرما رقم یکان $۳^{۱۰۰۰}$ را به‌دست آورید.

(ب) نشان دهید که به‌ازای هر عدد صحیح a، رقمهای یکان a و $a^{۵}$ یکسان است.

۷. اگر $۷ \nmid a$، ثابت کنید یا $a^{۳} + ۱$ یا $a^{۳} - ۱$ بر ۷ بخشپذیر است. [راهنمایی: قضیهٔ فرما را به‌کار ببرید.]

۸. سه بارِ آخر ظهور ستارهٔ دنباله‌دار هالی در سالهای ۱۸۳۵، ۱۹۱۰، و ۱۹۸۶ بوده است. ظهور آتی آن در ۲۰۶۱ خواهد بود. ثابت کنید

$$۱۸۳۵^{۱۹۱۰} + ۱۹۸۶^{۲۰۶۱} \equiv ۰ \text{ (به پیمانهٔ ۷)}$$

۹. (الف) فرض کنید p عددی اول باشد و $\gcd(a, p) = ۱$. با استفاده از قضیهٔ فرما نشان دهید (به پیمانهٔ p) $x \equiv a^{p-۲}b$ جوابی از همنهشتی خطی (به پیمانهٔ p) $ax \equiv b$ است.

(ب) با کاربرد بخش (الف)، همنهشتیهای خطی (به پیمانهٔ ۳۱) $۲x \equiv ۱$، (به پیمانهٔ ۱۱) $۶x \equiv ۵$، و (به پیمانهٔ ۲۹) $۳x \equiv ۱۷$ را حل کنید.

۱۰. به فرض اینکه a و b عددهایی صحیح و تقسیم‌ناپذیر بر عدد اول p باشند، ثابت کنید:

(الف) اگر (به پیمانهٔ p) $a^{p} \equiv b^{p}$، آنگاه (به پیمانهٔ p) $a \equiv b$.

(ب) اگر (به پیمانهٔ p) $a^{p} \equiv b^{p}$، آنگاه (به پیمانهٔ $p^{۲}$) $a^{p} \equiv b^{p}$. [راهنمایی: بنابه (الف)، به‌ازای k ای، $a = b + pk$؛ بنابراین $a^{p} - b^{p} = (b + pk)^{p} - b^{p}$ ؛ اکنون نشان دهید $p^{۲}$ عبارت اخیر را می‌شمارد.]

۱۱. با کاربرد قضیهٔ فرما ثابت کنید که اگر p عدد فرد اولی باشد، آنگاه

(الف) (به پیمانهٔ p) $۱^{p-۱} + ۲^{p-۱} + ۳^{p-۱} + \ldots + (p-۱)^{p-۱} \equiv -۱$

(ب) (به پیمانهٔ p) $۱^{p} + ۲^{p} + ۳^{p} + \ldots + (p-۱)^{p} \equiv ۰$ [راهنمایی: از اتحاد $۱ + ۲ + ۳ + \ldots + (p-۱) = p(p-۱)/۲$ استفاده کنید.]

۱۲. ثابت کنید که اگر p یک عدد اول فرد و k عددی صحیح صادق در $۱ \leq k \leq p-۱$ باشد، آنگاه ضریب دوجمله‌ای $\binom{p-۱}{k}$ همنهشت با $(-۱)^k$ به پیمانهٔ p است.

۱۳. فرض کنید p و q عددهای اول فرد متمایزی باشند و $p-۱|q-۱$. اگر $\gcd(a,pq)=۱$، نشان دهید که $a^{q-۱} \equiv ۱$ (به پیمانهٔ pq).

۱۴. اگر p و q عددهای اول متمایزی باشند، ثابت کنید

$$p^{q-۱}+q^{p-۱} \equiv ۱ \ (\text{به پیمانهٔ } pq)$$

۱۵. حکمهای زیر را ثابت کنید:

(الف) اگر p عددی اول و عدد $M_p = ۲^p - ۱$ مرکب باشد، آنگاه M_p اوّلنماست.

(ب) هر عدد مرکب $F_n = ۲^{۲^n}+۱$ $(n=۰,۱,۲,\ldots)$ اوّلنماست. [راهنمایی: بنابه تمرین ۲۱، بخش ۲ـ۲، از $۲^{n+۱}|۲^{۲^n}$ نتیجه می‌شود $۲^{۲^{n+۱}}-۱|۲^{۲^n}-۱$، ولی $F_n|۲^{۲^{n+۱}}-۱$.]

۱۶. نشان دهید عددهای صحیح زیر اولنمای مطلق‌اند:

(الف) $۱۱۰۵ = ۵ \times ۱۳ \times ۱۷$

(ب) $۲۸۲۱ = ۷ \times ۱۳ \times ۳۱$

(پ) $۲۴۶۵ = ۵ \times ۱۷ \times ۲۹$

۱۷. بانشان‌دادن اینکه $۱۱^{۳۴۱} \not\equiv ۱۱$ (به پیمانهٔ ۳۴۱)، نتیجه بگیرید که اولنمای ۳۴۱ مطلق نیست [راهنمایی: $۳۱ \nmid ۱۱^{۳۴}-۱۱$].

۱۸. (الف) اگر p یک عدد اول فرد باشد و $n=۲p$، ثابت کنید به‌ازای هر عددصحیح a، $a^{n-۱} \equiv a$ (به پیمانهٔ n).

(ب) نشان دهید که به‌ازای $n = ۱۹۵ = ۳ \times ۵ \times ۱۳$ و هر عدد صحیح a، $a^{n-۲} \equiv a$ (به پیمانهٔ n).

۱۹. ثابت کنید که هر عددصحیح به‌صورت

$$n = (۶k+۱)(۱۲k+۱)(۱۸k+۱)$$

به شرط اول بودن هر سه عامل، اوّلنمایی مطلق است، پس، $۱۷۲۹ = ۷ \times ۱۳ \times ۱۹$ اولنمایی مطلق است.

۲۰. نشان دهید $۵۶۱|۲^{۵۶۱}-۲$ و $۵۶۱|۳^{۵۶۱}-۳$. اینکه آیا بینهایت عدد مرکب n با ویژگیهای $n|۲^n-۲$ و $n|۳^n-۳$ وجود دارد یا نه، پرسش پاسخ‌نیافته‌ای است.

۴ـ۵ قضیهٔ ویلسن

اکنون به نقطهٔ عطف دیگری در سیر پیشرفت نظریهٔ اعداد می‌پردازیم. ادوارد وارینگ[1] ریاضیدان انگلیسی (۱۷۴۱ـ۱۷۹۳) در سال ۱۷۷۰ در تأملات جبری[2] اش تعدادی قضیهٔ جدید ارائه کرد. مهمترین آنها ویژگی جالبی از عددهای اول است که آن را یکی از دانشجویان سابقش، جان ویلسن نامی، با وی در میان گذاشته شده بود. ویژگی مزبور این است: اگر p عدد اولی باشد، $(p-۱)!+۱$ را می‌شمارد. ظاهراً ویلسن این ویژگی را براساس محاسباتی عددی حدس زده بود؛ ولی به هر حال، نه وارینگ و نه ویلسن، هیچ‌یک نمی‌دانست آن را چگونه ثابت کند. وارینگ با اعتراف به ناتوانیش در ارائهٔ اثبات، خاطرنشان کرد: «اثبات قضیه‌هایی از این نوع به‌دلیل فقدان نمادی برای نمایش عددهای اول مشکل است.» (گاوس به‌محض اطلاع از این نظر، اظهار نمود «مفهوم، نه نماد»، و منظورش این بود که در این‌گونه مسأله‌ها مفهوم است که واقعاً اهمیت دارد، نه نماد.) اندکی بعد (در ۱۷۷۱)، برخلاف پیش‌بینی ناامیدکنندهٔ وارینگ، لاگرانژ ویژگی فوق را که اکنون به «قضیهٔ ویلسن» معروف است ثابت کرد و نشان داد که عکس آن نیز برقرار است. شاید منصفانه‌تر می‌بود که این قضیه به‌نام لایب‌نیتس نامگذاری می‌شد زیرا براساس شواهدی، وی حداقل یک سده پیشتر به این نتیجه واقف بود، ولی چیزی دربارهٔ آن منتشر نکرد.

اکنون اثباتی از قضیهٔ ویلسن می‌آوریم.

قضیهٔ ۴ـ۵ (ویلسن). اگر p اول باشد، آنگاه

$$(p-۱)! \equiv -۱ \qquad (\text{به پیمانهٔ } p)$$

اثبات. با کنارگذاشتن حالتهای بدیهی $p=۲$ و $p=۳$، فرض می‌کنیم $p>۳$. همچنین فرض می‌کنیم a یکی از $p-۱$ عددصحیح مثبت

$$۱, ۲, ۳, \ldots, p-۱$$

باشد و همنهشتی خطی $ax \equiv ۱$ (به پیمانهٔ p) را درنظر می‌گیریم. پس $\gcd(a,p)=۱$. بنابه قضیهٔ ۴ـ۷، این همنهشتی جواب یکتایی به پیمانهٔ p دارد؛ پس عدد صحیح یکتایی چون a' با ضابطهٔ $۱ \leq a' \leq p-۱$ وجود دارد که در $aa' \equiv ۱$ (به پیمانهٔ p) صدق می‌کند.

چون p عددی اول است، $a=a'$ اگر و تنها اگر $a=۱$ یا $a=p-۱$. درواقع، همنهشتی $a^۲ \equiv ۱$ (به پیمانهٔ p) هم‌ارز با $(a-۱)(a+۱) \equiv ۰$ (به پیمانهٔ p) است. بنابراین، یا

1. Edward Waring
2. Meditationes Algebraticae

(به پیمانهٔ p) $a - ۱ \equiv ۰$، که در این صورت $a = ۱$، یا (به پیمانهٔ p) $a + ۱ \equiv ۰$، که بنابراین $a = p - ۱$.

اگر عددهای ۱ و $p - ۱$ را حذف کنیم، می‌توانیم بقیهٔ عددهای صحیح ۲، ۳، . . .، $p - ۲$ را به‌صورت دوتاییهای a' و a طوری دسته‌بندی کنیم که $a \neq a'$ و (به پیمانهٔ p) $aa' \equiv ۱$. با ضرب این $(p - ۳)/۲$ همنهشتی درهم و مرتب کردن عاملها به‌صورت طبیعی، به‌دست می‌آوریم

$$۲ \times ۳ \times \ldots \times (p - ۲) \equiv ۱ \ (\text{به پیمانهٔ } p)$$

یا

$$(p - ۲)! \equiv ۱ \ (\text{به پیمانهٔ } p)$$

اکنون با ضرب در $p - ۱$، همنهشتی

$$(p - ۱)! \equiv p - ۱ \equiv -۱ \ (\text{به پیمانهٔ } p)$$

را به‌دست می‌آوریم که می‌خواستیم آن را ثابت کنیم. □

مثالی عددی برای روشن شدن اثبات قضیهٔ ویلسن می‌تواند مفید باشد. به‌طور مشخص، فرض می‌کنیم $p = ۱۳$. می‌توان عددهای صحیح ۲، ۳، . . .، ۱۱ را به $(p - ۳)/۲ = ۵$ دستهٔ دوتایی طوری دسته‌بندی کرد که حاصلضرب عناصر هریک از دوتاییها همنهشت با ۱ به پیمانهٔ ۱۳ باشد. اگر این همنهشتیها را به‌طور صریح بنویسیم:

$$۲ \times ۷ \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$
$$۳ \times ۹ \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$
$$۴ \times ۱۰ \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$
$$۵ \times ۸ \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$
$$۶ \times ۱۱ \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$

از ضرب همنهشتیهای فوق به‌دست می‌آوریم

$$۱۱! = (۲ \times ۷)(۳ \times ۹)(۴ \times ۱۰)(۵ \times ۸)(۶ \times ۱۱) \equiv ۱ \ (\text{به پیمانهٔ } ۱۳)$$

و بنابراین

$$۱۲! \equiv ۱۲ \equiv -۱ \ (\text{به پیمانهٔ } ۱۳)$$

پس، به‌ازای $p = ۱۳$، (به پیمانهٔ p) $(p-۱)! \equiv -۱$.

عکس قضیهٔ ویلسن نیز برقرار است: اگر (به پیمانهٔ n) $(n-۱)! \equiv -۱$، آنگاه n باید اول باشد؛ زیرا اگر n اول نباشد، دارای مقسوم‌علیه d ای، $۱ < d < n$، است. به‌علاوه، چون $d \leq n-۱$، d به‌عنوان یکی از عاملها در $(n-۱)!$ حضور دارد، و درنتیجه $d|(n-۱)!$. ولی، فرض کرده‌ایم $n|(n-۱)!+۱$، و بنابراین $d|(n-۱)!+۱$؛ درنتیجه $d|۱$، که بی‌معنی است.

قضیهٔ ویلسن و عکس آن همراه باهم، شرطی لازم و کافی برای تعیین اول بودن به‌دست می‌دهند به این صورت که عددصحیح $n > ۱$ اول است اگر و تنها اگر (به پیمانهٔ n) $(n-۱)! \equiv -۱$. متأسفانه، اهمیت نظری این قضیه بیش از اهمیت عملی آن است زیرا با بزرگ‌شدن n، $(n-۱)!$ به‌سرعت بزرگ می‌شود به‌حدی که محاسبات مربوط عملی نیست.

این فصل را با کاربردی از قضیهٔ ویلسن در مطالعهٔ همنهشتیهای درجهٔ دوم پایان می‌دهیم. [یادآوری می‌کنیم که منظور از همنهشتی درجهٔ دوم یک همنهشتی به‌صورت (به پیمانهٔ n) $ax^۲+bx+c \equiv ۰$، با ضابطهٔ (به پیمانهٔ n) $a \not\equiv ۰$، است.]

قضیهٔ ۵ـ۵ همنهشتی درجهٔ دوم (به پیمانهٔ p) $x^۲+۱ \equiv ۰$، به‌ازای عدد اول فرد p دارای جواب است اگر و تنها اگر (به پیمانهٔ ۴) $p \equiv ۱$.

اثبات. فرض می‌کنیم a جوابی از (به پیمانهٔ p) $x^۲+۱ \equiv ۰$ باشد، یعنی (به پیمانهٔ p) $a^۲ \equiv -۱$. چون $p \nmid a$، بنابه قضیهٔ فرما داریم

$$۱ \equiv a^{p-۱} \equiv (a^۲)^{(p-۱)/۲} \equiv (-۱)^{(p-۱)/۲} \quad (\text{به پیمانهٔ } p)$$

ممکن نیست به‌ازای عددصحیحی چون k داشته باشیم $p = ۴k+۳$ زیرا در این صورت،

$$(-۱)^{(p-۱)/۲} = (-۱)^{۲k+۱} = -۱$$

پس (به پیمانهٔ p) $۱ \equiv -۱$؛ و خلاصه اینکه $p|۲$، که به‌وضوح قابل‌قبول نیست. پس، p باید به‌صورت $۴k+۱$ باشد.

اکنون عکس قضیه را ثابت می‌کنیم. در حاصلضرب

$$(p-۱)! = ۱ \times ۲ \times \ldots \times \frac{p-۱}{۲} \times \frac{p+۱}{۲} \times \ldots \times (p-۲)(p-۱)$$

همنهشتیهای

$$p-۱ \equiv -۱ \quad (\text{به پیمانهٔ } p)$$
$$p-۲ \equiv -۲ \quad (\text{به پیمانهٔ } p)$$
$$\vdots$$
$$\frac{p+۱}{۲} \equiv -\frac{p-۱}{۲} \quad (\text{به پیمانهٔ } p)$$

را داریم. با تغییر ترتیب عاملها به‌دست می‌آوریم

$$(p-۱)! \equiv ۱ \times (-۱) \times ۲(-۲) \times \ldots \times \frac{p-۱}{۲} \times \left(-\frac{p-۱}{۲}\right) \quad (\text{به پیمانهٔ } p)$$
$$\equiv (-۱)^{(p-۱)/۲}\left(۱ \times ۲ \times \ldots \times \frac{p-۱}{۲}\right)^۲ \quad (\text{به پیمانهٔ } p)$$

زیرا $(p-۱)/۲$ علامت منها وجود دارد. اینجاست که می‌توان قضیهٔ ویلسن را وارد کارکرد زیرا، چون $(p-۱)! \equiv -۱$ (به پیمانهٔ p)، داریم

$$-۱ \equiv (-۱)^{(p-۱)/۲}\left[\left(\frac{p-۱}{۲}\right)!\right]^۲ \quad (\text{به پیمانهٔ } p)$$

اگر فرض کنیم p به‌صورت $۴k+۱$ است، آنگاه $(-۱)^{(p-۱)/۲} = ۱$، و بنابراین

$$-۱ \equiv \left[\left(\frac{p-۱}{۲}\right)!\right]^۲ \quad (\text{به پیمانهٔ } p)$$

نتیجه اینکه $[(p-۱)/۲]!$ در همنهشتی درجه دوم $x^۲+۱ \equiv ۰$ (به پیمانهٔ p) صدق می‌کند. □

حال به مثالی عددی توجه کنید: حالت $p=۱۳$ را درنظر می‌گیریم که عدد اولی به‌صورت $۴k+۱$ است. داریم $(p-۱)/۲ = ۶$ و به‌آسانی می‌توان ملاحظه کرد که

$$۶! = ۷۲۰ \equiv ۵ \quad (\text{به پیمانهٔ } ۱۳)$$

و

$$۵^۲+۱ = ۲۶ \equiv ۰ \quad (\text{به پیمانهٔ } ۱۳)$$

بنابراین، به‌ازای $p=۱۳$، همنهشتی $[(\frac{۱}{۲}(p-۱))!]^۲+۱ \equiv ۰$ (به پیمانهٔ p) برقرار است.

قضیهٔ ویلسن نشان می‌دهد که بینهایت عدد مرکب به‌صورت $n! + ۱$ وجود دارد. از سوی دیگر، متناهی یا نامتناهی بودن تعداد عددهای اول به‌صورت $n! + ۱$ پرسشی است که هنوز پاسخی نیافته است. تنها مقدارهایی از n در محدودهٔ $۱ \leq n \leq ۱۰۰$، که به‌ازای آنها اول بودن $n! + ۱$ به اثبات رسیده است، عبارت‌اند از $n = ۱, ۲, ۳, ۱۱, ۲۷, ۳۷, ۴۱, ۷۳, ۷۷$. فعلاً بزرگترین عدد اول شناخته‌شده به‌صورت $n! + ۱$، عدد $۱۴۷۷! + ۱$ است که در ۱۹۸۴ کشف شد.

تمرینهای ۵ـ۴

۱. (الف) باقیماندهٔ تقسیم $۱۵!$ بر ۱۷ را تعیین کنید.

(ب) باقیماندهٔ تقسیم $۲(۲۶)!$ بر ۲۹ را تعیین کنید. [راهنمایی. بنابه قضیهٔ ویلسن، به‌ازای هر عدد اول فرد $p > ۳$، $۲(p-۳)! \equiv -۱$ (به پیمانهٔ p)].

۲. با بررسی اینکه $۱۶! \equiv -۱$ (به پیمانهٔ ۱۷) یا نه، تعیین کنید که ۱۷ اول است یا نه.

۳. عددهای صحیح ۲، ۳، ۴، ...، ۲۱ را طوری به‌صورت زوجهای a و b دسته‌بندی کنید که $ab \equiv ۱$ (به پیمانهٔ ۲۳).

۴. نشان دهید $۱۸! \equiv -۱$ (به پیمانهٔ ۴۳۷).

۵. (الف) ثابت کنید عددصحیح $n > ۱$ اول است اگر و تنها اگر $(n-۲)! \equiv ۱$ (به پیمانهٔ n).

(ب) اگر $n \neq ۴$ عددصحیح مرکبی باشد، نشان دهید $(n-۱)! \equiv ۰$ (به پیمانهٔ n).

۶. ثابت کنید که به‌ازای عدد اول ثابت دادهٔشدهٔ p، همنهشتی زیر برقرار است

$$(p-۱)! \equiv p-۱(۱+۲+۳+\ldots+(p-۱) \text{ (به پیمانهٔ }$$

۷. اگر p اول باشد، ثابت کنید به‌ازای هر عددصحیح a

$$p \mid a^p + (p-۱)!a \qquad \text{و} \qquad p \mid (p-۱)!a^p + a$$

[راهنمایی: بنابه قضیهٔ ویلسن، $a^p + (p-۱)!a \equiv a^p - a$ (به پیمانهٔ p).]

۸. دو عدد اول فرد $p \geq ۱۳$ پیدا کنید که به‌ازای هر یک، همنهشتی $(p-۱)! \equiv -۱$ (به پیمانهٔ $p^۲$) برقرار باشد.

۹. با استفاده از قضیهٔ ویلسن، ثابت کنید به‌ازای هر عدد اول فرد p

$$۱^۲ \times ۳^۲ \times ۵^۲ \times \ldots \times (p-۲)^۲ \equiv (-۱)^{(p+۱)/۲} \text{ (به پیمانهٔ } p)$$

[راهنمایی: چون $k \equiv -(p-k)$ (به پیمانهٔ p)، نتیجه می‌شود

$$۲ \times ۴ \times ۶ \times \ldots \times (p-۱) \equiv (-۱)^{(p-۱)/۲} ۱ \times ۳ \times ۵ \times \ldots \times (p-۲) \text{ (به پیمانهٔ } p)]$$

۱۰. (الف) به‌ازای p ی اولی به‌صورت ۳ + $۴k$، ثابت کنید که

$$\left(\frac{p-۱}{۲}\right)! \equiv ۱ \ (\text{به پیمانهٔ } p) \quad \text{یا} \quad \left(\frac{p-۱}{۲}\right)! \equiv -۱ \ (\text{به پیمانهٔ } p)$$

و بنابراین $[(p-۱)/۲]!$ در همنهشتی درجه دوم (به پیمانهٔ p) $x^۲ \equiv ۱$ صدق می‌کند.

(ب) با استفاده از قسمت (الف) نشان دهید که اگر $p = ۴k + ۳$ اول باشد، آنگاه حاصلضرب همهٔ عددهای صحیح زوج کوچکتر از p با ۱ یا ۱− همنهشت به پیمانهٔ p است. [راهنمایی: از قضیهٔ فرما نتیجه می‌شود (به پیمانهٔ p) $۲^{(p-۱)/۲} \equiv \pm ۱$.]

۱۱. با کاربرد قضیهٔ ۵ـ۵ دو جواب برای همنهشتیهای درجه دوم (به پیمانهٔ ۲۹) $x^۲ \equiv -۱$ و (به پیمانهٔ ۳۷) $x^۲ \equiv -۱$ به‌دست آورید.

۱۲. نشان دهید که اگر $p = ۴k + ۳$ اول باشد و (به پیمانهٔ p) $a^۲ + b^۲ \equiv ۰$، آنگاه (به پیمانهٔ p) $a \equiv b \equiv ۰$. [راهنمایی: اگر (به پیمانهٔ p) $a \not\equiv ۰$، آنگاه عدد صحیح c ای وجود دارد که (به پیمانهٔ p) $ac \equiv ۱$؛ از این موضوع برای بررسی قضیهٔ ۵ـ۵ استفاده کنید.]

۱۳. ثابت کنید مقسوم‌علیه‌های اول فرد عدد صحیح $n^۲ + ۱$ به‌صورت $۴k + ۱$ هستند. [راهنمایی: قضیهٔ ۵ـ۵].

۱۴. نشان دهید که $۴(۲۹!) + ۵!$ بر ۳۱ بخشپذیر است.

۱۵. نشان دهید که به ازای عدد اول p و $۰ \leq k \leq p-۱$،

$$k!(p-k-۱)! \equiv (-۱)^{k+۱} \ (\text{به پیمانهٔ } p)$$

۱۶. اگر p و q عددهای اول متمایزی باشند، ثابت کنید به‌ازای هر عددصحیح a، $pq | a^{pq} - a^p - a^q + a$.

۱۷. ثابت کنید که اگر p و $p + ۲$ دو عدد اول دوقلو باشند، آنگاه

$$۴((p-۱)! + ۱) + p \equiv ۰ \ (\text{به پیمانهٔ } p(p+۲))$$

۶

تابعهای حسابی

«ریاضیدانان شبیه فرانسویها هستند: هرچه به آنها بگویید، به زبان خود ترجمه می‌کنند و بیدرنگ آن را به صورتی کاملاً متفاوت در می‌آورند.»

گوته

۶ـ۱ تابعهای τ و σ

برخی از تابعها دربررسی مقسوم‌علیه‌های عدد صحیح اهمیت ویژه‌ای دارند. هر تابعی که دامنهٔ تعریف آن مجموعهٔ عددهای صحیح مثبت باشد تابعی حسابی یا نظریهٔ اعدادی نامیده می‌شود. گرچه مقدار تابع حسابی لزوماً عددی صحیح مثبت، یا حتی صحیح نیست، بیشتر تابعهای حسابی مورد بحث ما تابعهایی با مقدارهای صحیح‌اند. از جملهٔ طبیعیترین و آسانترین آنها از نظر کاربرد، تابعهای τ و σ هستند.

تعریف ۶ـ۱ به ازای هر عدد صحیح مثبت n، $\tau(n)$ نشان‌دهندهٔ تعداد مقسوم‌علیه‌های n، و $\sigma(n)$ نشان‌دهندهٔ مجموع این مقسوم علیه‌هاست.

به عنوان مثالی از این مفهومها، $n = ۱۲$ را درنظر می‌گیریم. چون ۱۲ دارای مقسوم‌علیه‌های مثبت ۱، ۲، ۳، ۴، ۶، و ۱۲ است، ملاحظه می‌کنیم که $\tau(۱۲) = ۶$ و

$$\sigma(۱۲) = ۱ + ۲ + ۳ + ۴ + ۶ + ۱۲ = ۲۸$$

به ازای چند عدد صحیح مثبت نخست داریم

$$\tau(۱) = ۱,\ \tau(۲) = ۲,\ \tau(۳) = ۲,\ \tau(۴) = ۳,\ \tau(۵) = ۲,\ \tau(۶) = ۴, \ldots$$

و

$$\sigma(۱) = ۱,\ \sigma(۲) = ۳,\ \sigma(۳) = ۴,\ \sigma(۴) = ۷,\ \sigma(۵) = ۶,\ \sigma(۶) = ۱۲, \ldots$$

به‌آسانی می‌توان نشان داد که $\tau(n) = ۲$ اگر و تنها اگر n عددی اولی باشد؛ همچنین، $\sigma(n) = n + ۱$ اگر و تنها اگر n اول باشد.

پیش از بررسی مفصلتر تابعهای τ و σ، نمادی را معرفی می‌کنیم که به روشن شدن موضوع در بعضی موارد کمک خواهد کرد. معمولاً نماد

$$\sum_{d|n} f(d)$$

به معنی «مجموع مقدارهای $f(d)$ به‌ازای همهٔ مقسوم‌علیه‌های مثبت d ی عدد صحیح مثبت n» به کار می‌رود. به عنوان مثال داریم

$$\sum_{d|۲۰} f(d) = f(۱) + f(۲) + f(۴) + f(۵) + f(۱۰) + f(۲۰)$$

با این قرارداد، τ و σ را می‌توان به صورت

$$\tau(n) = \sum_{d|n} ۱، \qquad \sigma(n) = \sum_{d|n} d$$

تعریف کرد. نماد $\sum_{d|n} ۱$ به این معنی است که باید ۱هایی به تعداد مقسوم‌علیه‌های مثبت n را باهم جمع کنیم؛ مثال: عدد صحیح ۱۰ دارای چهار مقسوم‌علیه مثبت ۱، ۲، ۵، ۱۰ است، بنابراین

$$\tau(۱۰) = \sum_{d|۱۰} ۱ = ۱ + ۱ + ۱ + ۱ = ۴$$

و

$$\sigma(۱۰) = \sum_{d|۱۰} d = ۱ + ۲ + ۵ + ۱۰ = ۱۸$$

با استفاده از نخستین قضیهٔ این فصل، تعیین مقسوم‌علیه‌های مثبت عدد صحیح مثبت n به شرط معلوم بودن تجزیه‌اش به عاملهای اول، تسهیل می‌شود.

قضیهٔ ۶ـ۱ اگر $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ تجزیهٔ $n > 1$ به عاملهای اول باشد، آنگاه مقسوم‌علیه‌های مثبت n دقیقاً عددهای صحیح dای هستند که به صورت

$$d = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$$

$0 \le a_i \le k_i$، $(i = 1, 2, \dots, r)$ هستند.

اثبات. توجه کنید که مقسوم‌علیه $d = 1$ متناظر با $a_1 = a_2 = \dots = a_r = 0$ و خود n متناظر با $a_1 = k_1$، $a_2 = k_2$، ...، $a_r = k_r$ است. فرض می‌کنیم d عدد n را به‌طور نابدیهی می‌شمارد؛ مثلاً $n = dd'$، که $d > 1$، $d' > 1$. هریک از d و d' را به صورت حاصلضرب چند عدد اول (نه لزوماً متمایز) می‌نویسیم

$$d = q_1q_2\dots q_s, \qquad d' = t_1t_2\dots t_u$$

که در آن q_iها و t_jها اول‌اند. در این صورت

$$p_1^{k_1}p_2^{k_2}\dots p_r^{k_r} = q_1\dots q_s t_1\dots t_u$$

دو تجزیهٔ عدد صحیح مثبت n به عاملهای اول‌اند. بنا به یکتایی تجزیه به عاملهای اول، هر q_iی اول باید یکی از p_jها باشد. اگر هر دسته از عاملهای اولِ برابر را درهم ضرب و به صورت یک جمله بنویسیم، به‌دست می‌آوریم

$$d = q_1q_2\dots q_s = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$$

که برخی از a_iها ممکن است صفر باشند.

به‌عکس، هر عدد $d = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$، $(0 \le a_i \le k_i)$، مقسوم‌علیهی از n است، زیرا می‌توانیم بنویسیم

$$\begin{aligned} n &= p_1^{k_1}p_2^{k_2}\dots p_r^{k_r} \\ &= (p_1^{a_1}p_2^{a_2}\dots p_r^{a_r})(p_1^{k_1-a_1}p_2^{k_2-a_2}\dots p_r^{k_r-a_r}) \\ &= dd' \end{aligned}$$

که درآن $d' = p_1^{k_1-a_1}p_2^{k_2-a_2}\dots p_r^{k_r-a_r}$ و به ازای هر i، $k_i - a_i \geq 0$. پس $d' > 0$ و $d|n$. □

اکنون این قضیه را به کار می‌بریم.

قضیهٔ ۶ـ۲ اگر $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ تجزیهٔ $n > 1$ به عاملهای اول باشد، آنگاه

(الف) $\tau(n) = (k_1+1)(k_2+1)\dots(k_r+1)$، و

(ب) $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \times \frac{p_2^{k_2+1}-1}{p_2-1} \times \dots \times \frac{p_r^{k_r+1}-1}{p_r-1}$.

اثبات. بنا به قضیهٔ ۶ـ۱، مقسوم‌علیه‌های مثبت n دقیقاً عددهای صحیحی چون

$$d = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$$

هستند که $0 \leq a_i \leq k_i$. تعداد k_1+1 انتخاب برای توان a_1 وجود دارد؛ k_2+1 انتخاب برای a_2، ...، k_r+1 انتخاب برای a_r؛ پس، n دقیقاً

$$(k_1+1)(k_2+1)\dots(k_r+1)$$

مقسوم‌علیه دارد.

برای محاسبهٔ $\sigma(n)$، حاصلضرب

$$(1+p_1+p_1^2+\dots+p_1^{k_1})(1+p_2+p_2^2+\dots+p_2^{k_2})\dots(1+p_r+p_r^2+\dots+p_r^{k_r})$$

را در نظر می‌گیریم. هر مقسوم‌علیه مثبت n دقیقاً یک‌بار به صورت جمله‌ای از بسط این حاصلضرب ظاهر می‌شود، در نتیجه

$$\sigma(n) = (1+p_1+p_1^2+\dots+p_1^{k_1})\dots(1+p_r+p_r^2+\dots+p_r^{k_r})$$

با به‌کاربردن فرمول مجموع سری هندسی متناهی در مورد iامین عامل سمت راست، به‌دست می‌آوریم

$$1+p_1+p_i^2+\dots+p_i^{k_i} = \frac{p_i^{k_i+1}-1}{p_i-1}$$

نتیجه می‌شود که

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \times \frac{p_2^{k_2+1}-1}{p_2-1} \times \dots \times \frac{p_r^{k_r+1}-1}{p_r-1}$$

متناظر با نماد $\sum$ برای مجموعها، می‌توان با استفاده از حرف بزرگ «پی» در الفبای یونانی نمادی برای حاصلضربها تعریف کرد. محدودیتی که عددهای مورد عمل را مشخص می‌کند، معمولاً زیر علامت Π ذکر می‌شود. به عنوان مثال

$$\prod_{۱\leq d\leq ۵} f(d) = f(۱)f(۲)f(۳)f(۴)f(۵)$$

$$\prod_{d|۹} f(d) = f(۱)f(۳)f(۹)$$

$$\prod_{\substack{p|۳۰ \\ \text{عددی اول است } p}} f(d) = f(۲)f(۳)f(۵)$$

با این قرارداد، حکم قضیهٔ ۶ـ۲ به صورت فشردهٔ زیر در می‌آید: اگر $n = p_۱^{k_۱}p_۲^{k_۲}\dots p_r^{k_r}$ تجزیهٔ $n > ۱$ به عاملهای اول باشد، آنگاه

$$\tau(n) = \prod_{۱\leq i\leq r}(k_i + ۱)$$

و

$$\sigma(n) = \prod_{۱\leq i\leq r}\frac{p_i^{k_i+۱} - ۱}{p_i - ۱}$$

مثال ۶ـ۱

عدد $۱۸۰ = ۲^۲ \times ۳^۲ \times ۵$ دارای

$$\tau(۱۸۰) = (۲+۱)(۲+۱)(۱+۱) = ۱۸$$

مقسوم‌علیه مثبت است. اینها عددهای صحیحی به صورت

$$۲^{a_۱} \times ۳^{a_۲} \times ۵^{a_۳}$$

هستند به‌طوری که $a_۱ = ۰, ۱, ۲$؛ $a_۲ = ۰, ۱, ۲$؛ $a_۳ = ۰, ۱$. به‌طور مشخص داریم

$$۱, ۲, ۳, ۴, ۵, ۶, ۹, ۱۰, ۱۲, ۱۵, ۱۸, ۲۰, ۳۰, ۳۶, ۴۵, ۶۰, ۹۰, ۱۸۰$$

مجموع این عددهای صحیح برابر است با

$$\sigma(۱۸۰) = \frac{۲^۳ - ۱}{۲ - ۱} \times \frac{۳^۳ - ۱}{۳ - ۱} \times \frac{۵^۲ - ۱}{۵ - ۱} = \frac{۷}{۱} \times \frac{۲۶}{۲} \times \frac{۲۴}{۴} = ۷ \times ۱۳ \times ۶ = ۵۴۶ \quad ■$$

یکی از ویژگیهای جالبتر تابع مقسوم‌علیه τ این است که حاصلضرب مقسوم‌علیه‌های مثبت عدد صحیح $n > 1$ برابر با $n^{\tau(n)/2}$ است. اثبات این حکم دشوار نیست: فرض می‌کنیم d مقسوم‌علیه مثبت دلخواهی از n باشد، بنابراین به‌ازای d'ای، $n = dd'$. اگر d همهٔ $\tau(n)$ مقسوم‌علیه مثبت n را اختیار کند، $\tau(n)$ معادله از این‌دست به‌دست می‌آید. با ضرب این معادله‌ها در یکدیگر، به‌دست می‌آوریم

$$n^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d'$$

ولی، اگر d همهٔ مقسوم‌علیه‌های n را اختیار کند، d' نیز چنین می‌کند؛ پس $\Pi_{d|n} d = \Pi_{d'|n} d'$. در نتیجه

$$n^{\tau(n)} = \left(\prod_{d|n} d\right)^2$$

یا معادلش

$$n^{\tau(n)/2} = \prod_{d|n} d$$

خواننده ممکن است (یا، در واقع، باید) در مورد درستی این رابطه شک کند، زیرا ابداً واضح نیست که طرف چپ همیشه عدد صحیحی است. اگر $\tau(n)$ زوج باشد، قطعاً مشکلی در کار نیست. اگر $\tau(n)$ فرد باشد، n مربعی کامل خواهد بود (تمرین ۷)، مثلاً $n = m^2$؛ بنابراین $n^{\tau(n)/2} = m^{\tau(n)}$، و این به همهٔ تردیدها پایان می‌دهد.

به عنوان مثالی عددی، حاصلضرب پنج مقسوم‌علیه ۱۶ (یعنی، ۱، ۲، ۴، ۸، ۱۶) را در نظر می‌گیریم که عبارت است از

$$\prod_{d|16} d = 16^{\tau(16)/2} = 16^{5/2} = 4^5 = 1024$$

تابعهای ضربی در مطالعهٔ تجزیهٔ عدد صحیح به عاملهای اول به‌طور طبیعی مطرح می‌شوند. پیش از ارائه تعریف، ملاحظه می‌کنیم که

$$\tau(2 \times 10) = \tau(20) = 6 \neq 2 \times 4 = \tau(2) \times \tau(10)$$

و نیز

$$\sigma(2 \times 10) = \sigma(20) = 42 \neq 3 \times 18 = \sigma(2) \times \sigma(10)$$

این محاسبات این نکتهٔ ناخوشایند را نشان می‌دهند که برابریهای

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

در حالت کلی برقرار نیستند. ولی، اگر m و n متباین باشند، آنگاه برابری همیشه برقرار است. این ویژگی الهامبخش تعریف زیر است.

تعریف ۶ـ۲ تابع حسابی f ضربی نامیده می‌شود اگر به‌ازای هر دو عدد صحیح مثبت متباین m و n داشته باشیم

$$f(mn) = f(m)f(n)$$

به عنوان مثالهایی ساده از تابعهای ضربی، کافی است تابعهای به صورت $f(n) = ۱$ و $g(n) = n$ به‌ازای هر $n \geq ۱$ را در نظر گرفت. به استقرا نتیجه می‌شود که اگر f ضربی و $n_۱$، $n_۲$، ...، n_r عددهای صحیح مثبت دوبه‌دو متباینی باشند، آنگاه

$$f(n_۱ n_۲ \dots n_r) = f(n_۱)f(n_۲)\dots f(n_r)$$

تابعهای ضربی امتیاز مهمی دارند: اگر مقدارهایشان به‌ازای توانهای عددهای اول معلوم باشد، کاملاً مشخص می‌شوند. در واقع، اگر $n > ۱$ عدد صحیح مثبتی باشد، آنگاه می‌توانیم بنویسیم $n = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$؛ چون $p_i^{k_i}$ها دوبه‌دو متباین‌اند، ویژگی ضربی تضمین می‌کند که

$$f(n) = f(p_۱^{k_۱})f(p_۲^{k_۲})\dots f(p_r^{k_r})$$

اگر f تابعی ضربی باشد که متحد با صفر نیست، آنگاه عدد صحیح nای وجود دارد به‌طوری که $f(n) \neq ۰$. ولی

$$f(n) = f(n \cdot ۱) = f(n)f(۱)$$

چون $f(n)$ ناصفر است، با حذف آن از دوطرف معادله به‌دست می‌آید $f(۱) = ۱$. نکته‌ای که مایلیم مورد توجه قرار دهیم این است که به‌ازای هر تابع ضربی ناصفر، $f(۱) = ۱$.

اکنون ثابت می‌کنیم σ و τ دارای ویژگی ضربی‌اند.

قضیهٔ ۶ـ۳ هر دو تابع σ و τ ضربی‌اند.

اثبات. فرض می‌کنیم m و n عددهای صحیح متباینی هستند. چون حکم به وضوح در حالت $m = ۱$ یا $n = ۱$ برقرار است، فرض می‌کنیم $m > ۱$ و $n > ۱$. اگر

$$m = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r} \qquad \text{و} \qquad n = q_۱^{j_۱} q_۲^{j_۲} \dots q_s^{j_s}$$

تجزیهٔ m و n به عاملهای اول باشند؛ چون $\gcd(m, n) = ۱$، هیچ p_iای نمی‌تواند در میان q_jها باشد. نتیجه می‌شود که تجزیهٔ mn به عاملهای اول عبارت است از

$$mn = p_۱^{k_۱} \dots p_r^{k_r} q_۱^{j_۱} \dots q_s^{j_s}$$

با استفاده از قضیهٔ ۶ـ۲ به‌دست می‌آوریم

$$\begin{aligned} \tau(mn) &= [(k_۱ + ۱) \dots (k_r + ۱)][(j_۱ + ۱) \dots (j_s + ۱)] \\ &= \tau(m)\tau(n) \end{aligned}$$

به روشی مشابه و با استفاده از قضیهٔ ۶ـ۲ داریم

$$\begin{aligned} \sigma(mn) &= \left[\frac{p_۱^{k_۱+۱} - ۱}{p_۱ - ۱} \times \dots \times \frac{p_r^{k_r+۱} - ۱}{p_r - ۱}\right] \left[\frac{q_۱^{j_۱+۱} - ۱}{q_۱ - ۱} \times \dots \times \frac{q_s^{j_s+۱} - ۱}{q_s - ۱}\right] \\ &= \sigma(m)\sigma(n) \end{aligned}$$

بنابراین، τ و σ تابعهایی ضربی‌اند. □

برنامهٔ خود را با اثبات حکمی کلی دربارهٔ تابعهای ضربی ادامه می‌دهیم. ولی برای این کار به لم زیر نیازمندیم.

لم. اگر $\gcd(m, n) = ۱$، آنگاه مجموعهٔ مقسوم‌علیه‌های مثبت mn متشکل از همهٔ حاصلضربهای $d_۱d_۲$ای است که $d_۱|n$، $d_۲|n$ و $\gcd(d_۱, d_۲) = ۱$؛ به علاوه، همهٔ این حاصلضربها متمایزند.

اثبات. اگر $m = ۱$ یا $n = ۱$، حکم بدیهی است. پس، فرض می‌کنیم $n > ۱$ و $m > ۱$. گیریم $m = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$ و $n = q_۱^{j_۱} q_۲^{j_۲} \dots q_s^{j_s}$، به ترتیب، تجزیهٔ m و n به عاملهای اول باشند. چون عددهای اول $p_۱$، ...، p_r، $q_۱$، ...، q_s متمایزند، تجزیهٔ mn به عاملهای اول عبارت است از

$$mn = p_۱^{k_۱} \dots p_r^{k_r} q_۱^{j_۱} \dots q_s^{j_s}$$

پس، هر مقسوم‌علیه مثبت mn مثل d به‌طور یکتا قابل نمایش به صورت

$$d = p_۱^{a_۱} \dots p_r^{a_r} q_۱^{b_۱} \dots q_s^{b_s}, \quad ۰ \leq a_i \leq k_i ، ۰ \leq b_i \leq j_i$$

است. این نشان می‌دهد که می‌توانیم d را به صورت $d = d_۱ d_۲$ بنویسیم، که $d_۱ = p_۱^{a_۱} \dots p_r^{a_r}$ عدد m را و $d_۲ = q_۱^{b_۱} \dots q_s^{b_s}$ عدد n را می‌شمارد. چون هیچ p_iای برابر هیچ q_jای نیست، مطمئناً داریم $\gcd(d_۱, d_۲) = ۱$. □

نکته‌ای اساسی در بیشتر مطالب بعدی، قضیهٔ زیر است.

قضیهٔ ۶ـ۴ اگر f تابعی ضربی و F تابعی با ضابطهٔ

$$F(n) = \sum_{d|n} f(d)$$

باشد، آنگاه F نیز ضربی است.

اثبات. فرض می‌کنیم m و n عددهایی صحیح مثبت، و متباین باشند. در این صورت

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_۱|m \\ d_۲|n}} f(d_۱ d_۲)$$

زیرا هر مقسوم‌علیه d از mn را می‌توان به روشی یکتا به صورت حاصلضرب مقسوم‌علیه $d_۱$ای از m و مقسوم‌علیه $d_۲$ای از n، که در آن $\gcd(d_۱, d_۲) = ۱$، نوشت. بنابه تعریف تابع ضربی

$$f(d_۱ d_۲) = f(d_۱) f(d_۲)$$

نتیجه می‌شود که

$$\begin{aligned} F(mn) &= \sum_{\substack{d_۱|m \\ d_۲|n}} f(d_۱) f(d_۲) = \left(\sum_{d_۱|m} f(d_۱)\right)\left(\sum_{d_۲|n} f(d_۲)\right) \\ &= F(m) F(n) \end{aligned}$$ □

بیفایده نیست که اثبات قضیهٔ ۶ـ۴ را برای یک مثال مشخص مرور کنیم. به ازای $m = ۸$ و $n = ۳$ داریم

$$F(۸ \times ۳) = \sum_{d|۲۴} f(d)$$

$$= f(۱) + f(۲) + f(۳) + f(۴) + f(۶) + f(۸) + f(۱۲) + f(۲۴)$$
$$= f(۱ \times ۱) + f(۲ \times ۱) + f(۱ \times ۳) + f(۴ \times ۱) + f(۲ \times ۳)$$
$$+ f(۸ \times ۱) + f(۴ \times ۳) f(۸ \times ۳)$$

$$= f(۱)f(۱) + f(۲)f(۱) + f(۱)f(۳) + f(۴)f(۱) + f(۲)f(۳)$$
$$+ f(۸)f(۱) + f(۴)f(۳) + f(۸)f(۳)$$

$$= [f(۱) + f(۲) + f(۴) + f(۸)][f(۱) + f(۳)]$$
$$= \sum_{d|۸} f(d) \times \sum_{d|۳} f(d) = F(۸)F(۳)$$

قضیهٔ ۶ـ۴ راه ظاهراً کوتاهی برای اثبات ضربی بودن τ و σ در پیش‌پای ما می‌گذارد.

فرع. تابعهای τ و σ ضربی‌اند.

اثبات. پیشتر دیدیم که تابع ثابت $f(n) = ۱$ و تابع همانی $f(n) = n$ ضربی‌اند. چون τ و σ را می‌توان به صورت

$$\sigma(n) = \sum_{d|n} d \quad \text{و} \quad \tau(n) = \sum_{d|n} ۱$$

نمایش داد، حکم بیدرنگ از قضیهٔ ۶ـ۴ نتیجه می‌شود.

تمرینهای ۶ـ۱

۱. فرض می‌کنیم m و n عددهایی صحیح مثبت و $p_۱$، $p_۲$، ...، p_r عددهای اول متمایزی باشند که حداقل یکی از m یا n را می‌شمارند. در این صورت m و n را می‌توان به صورت

$$m = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}، \quad k_i \geq ۰، \text{ به‌ازای } ۱ \leq i \leq r$$
$$n = p_۱^{j_۱} p_۲^{j_۲} \dots p_r^{j_r}، \quad j_i \geq ۰، \text{ به‌ازای } ۱ \leq i \leq r$$

نوشت. ثابت کنید اگر $u_i = \min\{k_i, j_i\}$، یعنی u_i کوچکترین عدد از میان دوعدد k_i و j_i باشد، و $v_i = \max\{k_i, j_i\}$ یعنی v_i بزرگترین عدد در میان دوعدد k_i و j_i باشد، آنگاه $\gcd(m,n) = p_۱^{u_۱} p_۲^{u_۲} \dots p_r^{u_r}$، $\operatorname{lcm}(m,n) = p_۱^{v_۱} p_۲^{v_۲} \dots p_r^{v_r}$.

۲. با استفاده از نتیجهٔ تمرین ۱، $\gcd(۱۲۳۷۸, ۳۰۵۴)$ و $\text{lcm}(۱۲۳۷۸, ۳۰۵۴)$ را حساب کنید.

۳. از تمرین ۱ نتیجه بگیرید که به‌ازای عددهای صحیح مثبت m و n داریم

$$\gcd(m,n)\,\text{lcm}(m,n) = mn$$

۴. با استفاده از نمادهای تمرین ۱ نشان دهید $\gcd(m,n) = ۱$ اگر و تنها اگر به ازای $i = ۱, ۲, \ldots, r$، $k_i j_i = ۰$.

۵. (الف) نشان دهید که به ازای $n = ۳۶۵۵$ و $n = ۴۵۰۳$ داریم

$$\tau(n) = \tau(n+۱) = \tau(n+۲) = \tau(n+۳)$$

(ب) اگر $n = ۱۴۲۰۶$ و $n = ۹۵۷$، نشان دهید $\sigma(n) = \sigma(n+۱)$.

۶. نشان دهید که به ازای هر عدد صحیح $n \geq ۱$، $\tau(n) \leq ۲\sqrt{n}$. [راهنمایی: اگر $d|n$، آنگاه یکی از d یا n/d نابیشتر از $\sqrt{n}$ است.]

۷. ثابت کنید:

(الف) $\tau(n)$ عدد صحیح فردی است اگر و تنها اگر n مربع کاملی باشد؛

(ب) $\sigma(n)$ عدد صحیح فردی است اگر و تنها اگر n مربعی کامل یا دوبرابر مربعی کامل باشد. [راهنمایی: اگر p عدد اول فردی باشد، آنگاه $۱ + p + p^۲ + \ldots + p^k$ فقط وقتی فرد است که k زوج باشد.]

۸. نشان دهید که به ازای هر عدد صحیح مثبت n، $\sum_{d|n} ۱/d = \sigma(n)/n$.

۹. اگر n عددی صحیح و خالی از مربع و r تعداد مقسوم‌علیه‌های اول n باشد، ثابت کنید $\tau(n) = ۲^r$.

۱۰. حکمهای زیر را ثابت کنید:

(الف) اگر $n = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$ تجزیهٔ $n > ۱$ به عاملهای اول باشد، آنگاه

$$۱ > \frac{n}{\sigma(n)} > \left(۱ - \frac{۱}{p_۱}\right)\left(۱ - \frac{۱}{p_۲}\right)\ldots\left(۱ - \frac{۱}{p_r}\right)$$

(ب) به ازای هز عدد صحیح n

$$\frac{\sigma(n!)}{n!} \geq ۱ + \frac{۱}{۲} + \frac{۱}{۳} + \ldots + \frac{۱}{n}$$

[راهنمایی: تمرین ۸ را ببینید.]

(پ) اگر $n > 1$ عدد مرکبی باشد، آنگاه $\sigma(n) > n + \sqrt{n}$. [راهنمایی: فرض کنید $d|n$ به طوری که $1 < d < n$، بنابراین $1 < (n/d) < n$. اگر $d \leq \sqrt{n}$، آنگاه $(n/d) \geq \sqrt{n}$.]

۱۱. نشان دهید که به ازای هر عدد صحیح مثبت $k > 1$ بینهایت عدد صحیح n با ضابطهٔ $\tau(n) = k$ و فقط تعدادی متناهی عدد n با ضابطهٔ $\sigma(n) = k$ وجود دارد. [راهنمایی: از تمرین ۱۰ (الف) استفاده کنید.]

۱۲. (الف) صورت کلی همهٔ عددهای صحیح مثبت n را، به‌طوری که، $\tau(n) = 10$، پیدا کنید. کوچکترین عدد صحیح مثبتی که به ازای آن حکم برقرار است، کدام است؟

(ب) نشان دهید که هیچ عدد صحیح مثبت nای در $\sigma(n) = 10$ صدق نمی‌کند. [راهنمایی: توجه کنید که اگر $n > 1$، آنگاه $\sigma(n) > n$.]

۱۳. ثابت کنید به‌ازای بینهایت زوج از عددهای صحیح m و n داریم $\sigma(m^2) = \sigma(n^2)$. [راهنمایی: k را طوری انتخاب کنید که $\gcd(k, 10) = 1$ و عددهای صحیح $m = 5k$ و $n = 4k$ را در نظر بگیرید.]

۱۴. هریک از حکمهای زیر را به ازای $k \geq 2$ ثابت کنید:

(الف) $n = 2^{k-1}$ در معادلهٔ $\sigma(n) = 2n - 1$ صدق می‌کند؛

(ب) اگر $2^k - 1$ اول باشد، آنگاه $n = 2^{k-1}(2^k - 1)$ در معادلهٔ $\sigma(n) = 2n$ صدق می‌کند؛

(پ) اگر $2^k - 3$ اول باشد، آنگاه $n = 2^{k-1}(2^k - 3)$ در معادلهٔ $\sigma(n) = 2n + 2$ صدق می‌کند.

معلوم نیست عددهای صحیح مثبت nای با ضابطهٔ $\sigma(n) = 2n + 1$ وجود دارند یا نه.

۱۵. اگر n و $n + 2$ یک جفت عدد اول دوقلو باشند، نشان دهید که $\sigma(n + 2) = \sigma(n) + 2$؛ این برابری به ازای $n = 434$ و $n = 8575$ نیز برقرار است.

۱۶. (الف) ثابت کنید که به ازای هر عدد صحیح $n > 1$، عددهای صحیح n_1 و n_2ای وجود دارند که $\tau(n_1) + \tau(n_2) = n$.

(ب) ثابت کنید از حدس گولدباخ نتیجه می‌شود که به ازای هر عدد صحیح زوج $2n$، عددهای صحیح n_1 و n_2ای وجود دارند به طوری که $\sigma(n_1) + \sigma(n_2) = 2n$.

۱۷. نشان دهید که به ازای هر عدد صحیح ثابت k تابع f با ضابطهٔ $f(n) = n^k$ ضربی است.

۱۸. اگر f و g تابعهای ضربی باشند و به ازای هرعدد اول p و هر عدد صحیح $k \geq 1$ داشته باشیم $f(p^k) = g(p^k)$، ثابت کنید $f = g$.

۱۹. اگر f و g تابعهایی ضربی باشند، ثابت کنید حاصلضرب fg و خارج‌قسمت f/g (هرگاه تابع اخیر تعریف شده باشد) نیز تابعهایی ضربی‌اند.

۲۰. تابع ρ را با تعریف $\rho(1) = 1$ و $\rho(n) = 2^r$، اگر تجزیهٔ $n > 1$ به عاملهای اول به صورت $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ باشد، در نظر می‌گیریم. به عنوان مثال، $\rho(8) = 2$ و $\rho(10) = \rho(36) = 2^2$.

(الف) نتیجه بگیرید که ρ تابعی ضربی است.

(ب) فرمولی برای $F(n) = \sum_{d|n} \rho(d)$ برحسب تجزیهٔ n به عاملهای اول به‌دست آورید.

۲۱. ثابت کنید به ازای هر عدد صحیح مثبت n، $\sum_{d|n} \tau(d)^3 = (\sum_{d|n} \tau(d))^2$. [راهنمایی: هردو طرف معادلهٔ مورد بحث تابعهایی ضربی از n هستند، بنابراین کافی است حالت $n = p^k$، p عددی اول، را در نظر بگیرید.]

۲۲. فرض می‌کنیم به ازای $n > 0$، $\sigma_s(n)$ نشان دهندهٔ مجموع توانهای sام مقسوم‌علیه‌های مثبت n باشد؛ یعنی

$$\sigma_s(n) = \sum_{d|n} d^s$$

نشان دهید که

(الف) $\sigma_0 = \tau$ و $\sigma_1 = \sigma$.

(ب) σ_s تابعی ضربی است. [راهنمایی: تابع f با تعریف $f(n) = n^s$ ضربی است.]

(پ) اگر $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ تجزیهٔ n به عاملهای اول باشد، آنگاه

$$\sigma_s(n) = \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1}\right) \times \left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1}\right) \times \dots \times \left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1}\right)$$

۲۳. نشان دهید که به ازای هر عدد صحیح مثبت n داریم

(الف) $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d)$، و

(ب) $\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\tau(d)$. [راهنمایی: چون تابعهای $F(n) = \sum_{d|n} \sigma(d)$ و $G(n) = \sum_{d|n} (n/d)\, \tau(d)$ ضربی‌اند، کافی است ثابت کنیم به‌ازای هر عدد اول p، $F(p^k) = G(p^k)$.]

۶ـ۲ فرمول وارونسازی موبیوس

در اینجا تابع دیگری موسوم به تابع μی موبیوس را مطرح می‌کنیم که به طور طبیعی روی عددهای صحیح مثبت تعریف می‌شود.

تعریف ۶ـ۳ به ازای اعداد صحیح مثبت n، تابع μ را با ضابطه

$$\mu(n) = \begin{cases} ۱ & n = ۱ \text{ اگر } \\ ۰ & p^۲|n \text{ اگر به ازای عدد اول } p \text{ای، } \\ (-۱)^r & n = p_۱p_۲\ldots p_r \text{ اگر } \text{، به‌طوری که } p_i\text{ها متمایز باشند} \end{cases}$$

تعریف می‌کنیم.

به عبارت دیگر، تعریف ۶ـ۳ می‌گوید که اگر n خالی از مربع نباشد، $\mu(n) = ۰$، و اگر n خالی از مربع با r مقسوم‌علیه اول متمایز باشد، آنگاه $\mu(n) = (-۱)^r$. به عنوان مثال، $\mu(۳۰) = \mu(۲ \times ۳ \times ۵) = (-۱)^۳ = -۱$. چند مقدار نخست μ عبارت‌اند از

$$\mu(۱) = ۱, \mu(۲) = -۱, \mu(۳) = -۱, \mu(۴) = ۰,\ \mu(۵) = -۱, \mu(۶) = ۱, \ldots$$

اگر p عددی اول باشد، بدیهی است که $\mu(p) = -۱$؛ همچنین، به‌ازای $k \geq ۲$، $\mu(p^k) = ۰$.

شاید خواننده حدس زده باشد که تابع μی موبیوس ضربی است. این همان چیزی است که قضیهٔ زیر می‌گوید.

قضیهٔ ۶ـ۵ تابع μ تابعی ضربی است.

اثبات. می‌خواهیم نشان دهیم که اگر m و n متباین باشند، $\mu(mn) = \mu(m)\mu(n)$. اگر به ازای عدد اول pای، $p^۲|m$ یا $p^۲|n$، آنگاه $p^۲|mn$؛ پس، $\mu(mn) = ۰ = \mu(m)\mu(n)$، و فرمول به وضوح برقرار است. بنابراین فرض می‌کنیم هم m و هم n عددهای صحیح خالی از مربعی هستند. مثلاً $m = p_۱p_۲\ldots p_r$، $n = q_۱q_۲\ldots q_s$، که در آن عددهای اول p_i و q_j همگی متمایزند. در این صورت

$$\begin{aligned}\mu(mn) &= \mu(p_۱\ldots p_rq_۱\ldots q_s) = (-۱)^{r+s} \\ &= (-۱)^r(-۱)^s = \mu(m)\mu(n)\end{aligned}$$

و اثبات به انجام می‌رسد. □

ببینیم چه اتفاقی می‌افتد اگر $\mu(d)$ به ازای همهٔ مقسوم‌علیه‌های مثبت dی عدد صحیح nای محاسبه شود و نتیجه‌ها با هم جمع شوند. در حالت $n = ۱$، پاسخ آسان است زیرا

$$\sum_{d|۱} \mu(d) = \mu(۱) = ۱$$

فرض می‌کنیم $n > ۱$ و قرار می‌دهیم

$$F(n) = \sum_{d|n} \mu(d)$$

برای تدارک مقدمات، نخست $F(n)$ را به‌ازای توان عددی اول، مثلاً $n = p^k$، حساب می‌کنیم. چون تنها مقسوم‌علیه‌های مثبت p^k، $k + ۱$ عدد صحیح ۱، p، $p^۲$، ...، p^k هستند، داریم

$$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(۱) + \mu(p) + \mu(p^۲) + \ldots + \mu(p^k)$$
$$= \mu(۱) + \mu(p) = ۱ + (-۱) = ۰$$

از آنجا که می‌دانیم μ تابعی ضربی است، توسل به قضیهٔ ۶ـ۴ مجاز است؛ این قضیه تضمین می‌کند که F نیز ضربی است. بنابراین، اگر $n = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$ تجزیهٔ متعارف n باشد، آنگاه $F(n)$ حاصلضرب مقدارهای F به‌ازای توانهای عددهای اول موجود در این تجزیه است:

$$F(n) = F(p_۱^{k_۱}) F(p_۲^{k_۲}) \ldots F(p_r^{k_r}) = ۰$$

این نتیجه را به صورت قضیهٔ زیر بیان می‌کنیم.

قضیهٔ ۶ـ۶ به ازای هر عدد صحیح مثبت $n \geq ۱$ داریم

$$\sum_{d|n} \mu(d) = \begin{cases} ۱ & n = ۱ \\ ۰ & n > ۱ \end{cases}$$

که در آن d همهٔ مقسوم‌علیه‌های مثبت n را اختیار می‌کند.

به عنوان مثالی از این قضیه، $n = ۱۰$ را در نظر می‌گیریم. مقسوم‌علیه‌های ۱۰ عبارت‌اند از ۱، ۲، ۵، ۱۰ و مجموع مطلوب برابر است با

$$\sum_{d|۱۰} \mu(d) = \mu(۱) + \mu(۲) + \mu(۵) + \mu(۱۰)$$
$$= ۱ + (-۱) + (-۱) + ۱ = ۰$$

اهمیت زیاد تابع موبیوس از قضیهٔ زیر معلوم می‌شود.

قضیهٔ ۶ـ۷ (فرمول وارونسازی موبیوس) فرض می‌کنیم F و f دو تابع حسابی باشند که با فرمول

$$F(n) = \sum_{d|n} f(d)$$

به هم مربوط می‌شوند. در این صورت

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

اثبات. همین که d با $d' = n/d$ تعویض شود، ملاحظه می‌شود که دومجموع مذکور در حکم قضیه برابرند؛ اگر d همهٔ مقسوم‌علیه‌های مثبت n را اختیار کند، d' نیز چنین می‌کند.

با انجام محاسبات لازم به‌دست می‌آوریم

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} f(c)\right) = \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c)\right) \quad (۱)$$

به آسانی ملاحظه می‌شود که $d|n$ و $c|(n/d)$ اگر و تنها اگر $c|n$ و $d|(n/c)$. بنابراین، آخرین عبارت در (۱) به صورت

$$\begin{aligned} \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c)\right) &= \sum_{c|n} \left(\sum_{d|\frac{n}{c}} f(c) \mu(d)\right) \quad (۲) \\ &= \sum_{c|n} \left(f(c) \sum_{c|\frac{n}{c}} \mu(d)\right) \end{aligned}$$

در می‌آید. بنا به قضیهٔ ۶ـ۶، مجموع $\sum_{d|n/c} \mu(d)$ صفر است مگر وقتی که $(n/c) = ۱$ (یعنی، وقتی $n = c$)، که در این حالت برابر ۱ است؛ بنابراین، سمت راست (۲) به‌صورت زیر ساده می‌شود

$$\sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d)\right) = \sum_{c=n} f(c) \times ۱ = f(n)$$

و نتیجهٔ مطلوب به‌دست آمده است. □

با استفادهٔ مجدد از $n = ۱۰$ نشان می‌دهیم که مجموع مضاعف در (۲) چگونه به‌دست می‌آید. در این مثال داریم

$$\begin{aligned}\sum_{d|۱۰}\left(\sum_{c|\frac{۱۰}{d}}\mu(d)f(c)\right) =&\mu(۱)[f(۱)+f(۲)+f(۵)+f(۱۰)]\\ &+\mu(۲)[f(۱)+f(۵)]+\mu(۵)[f(۱)+f(۲)]\\ &+\mu(۱۰)f(۱)\\ =&f(۱)[\mu(۱)+\mu(۲)+\mu(۵)+\mu(۱۰)]\\ &+f(۲)[\mu(۱)+\mu(۵)]+f(۵)[\mu(۱)+\mu(۲)]\\ &+f(۱۰)\mu(۱)\\ =&\sum_{c|۱۰}\left(\sum_{d|(۱۰/c)} f(c)\mu(d)\right)\end{aligned}$$

برای ملاحظهٔ اینکه قاعدهٔ وارونسازی موبیوس چگونه در حالت خاص به‌کار می‌رود، خاطرنشان می‌کنیم که هردو تابع τ و σ را می‌توان به صورت «تابعهای مجموع»

$$\sigma(n)=\sum_{d|n} d \quad \text{و} \quad \tau(n)=\sum_{d|n} ۱$$

تعریف کرد. قضیهٔ ۶ـ۷ می‌گوید که این فرمولها را می‌توان معکوس کرد و در این صورت

$$n=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sigma(d) \quad \text{و} \quad ۱=\sum_{d|n}\mu\left(\frac{n}{d}\right)\tau(d)$$

که به ازای هر $n \geq ۱$ برقرار هستند.

قضیهٔ ۶ـ۴ تضمین می‌کند که اگر f تابعی ضربی باشد، آنگاه $F(n) = \sum_{d|n} f(d)$ نیز ضربی است. برعکس، ممکن است این پرسش مطرح شود که آیا طبیعت ضربی F نیز به f تحمیل می‌شود؟ با کمال شگفتی پاسخ مثبت است.

قضیهٔ ۶ـ۸ اگر F تابعی ضربی باشد و

$$F(n)=\sum_{d|n} f(d)$$

آنگاه f نیز ضربی است.

اثبات. فرض می‌کنیم m و n عددهای صحیح مثبت متباینی باشند. خاطرنشان می‌کنیم که هر مقسوم‌علیه dی mn را می‌توان به طور یکتا به صورت $d = d_1 d_2$ ، که $d_1|m$، $d_2|n$، و $\gcd(d_1, d_2) = 1$، نوشت. بنابراین، با استفاده از فرمول وارونسازی داریم

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) = f(m) f(n) \end{aligned}$$

که حکم قضیه است. نیازی به گفتن نیست که، ضربی بودن μ و F در محاسبهٔ فوق ضرورت دارد. □

به ازای $n \geq 1$ تعریف می‌کنیم

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

بنابراین $M(n)$ برابر است با تفاضل تعداد عددهای صحیح مثبت خالی از مربع $k \leq n$ با تعداد زوجی عامل اول و تعداد عددهای صحیح خالی از مربع $k \leq n$ با تعداد فردی عامل اول. به عنوان مثال، $M(9) = 2 - 4 = -2$. در سال ۱۸۹۷، فرانتس مرتنس[1] (۱۸۴۰ـ۱۹۲۷) مقاله‌ای مشتمل بر جدولی پنجاه صفحه‌ای از مقدارهای $M(n)$، $n = 1, 2, \ldots, 10000$ چاپ کرد. وی به استناد جدول مزبور نتیجه گرفت که به «احتمال بسیار زیاد»، به ازای $n > 1$

$$|M(n)| < \sqrt{n}$$

(در مثال فوق، $|M(9)| = 2 < \sqrt{9}$.) این نتیجه‌گیری بعداً به حدس مرتنس معروف شد. با تحقیقی کامپیوتری در ۱۹۶۳ صحت این حدس به‌ازای هر n تا ۱۰ میلیارد تأیید شد. ولی در ۱۹۸۴، اندرو اُدلیزکو[2] و هرمانت ریل[3] نشان دادند که حدس درست نیست. اثبات آنها، که با

1. Franz Mertens 2. Andrew Odlyzko 3. Hermante Riele

استفاده از کامپیوتر صورت گرفت، اثباتی غیرمستقیم است و هیچ عدد n مشخصی که به‌ازای آن $|M(n)| \geq \sqrt{n}$، ارائه نمی‌کند؛ فقط نشان می‌دهد که چنان nای باید موجود باشد. بعداً نشان داده شد که مثال ناقضی برای حدس مرتنس دست‌کم به‌ازای یک $n \leq (۳٫۲۱) \times ۱۰^{۶۴}$ موجود است.

تمرینهای ۶ـ۲

۱. (الف) نشان دهید به‌ازای هر عدد صحیح مثبت n داریم

$$\mu(n)\mu(n+۱)\mu(n+۲)\mu(n+۳) = ۰$$

(ب) نشان دهید به ازای هر عدد صحیح $n \geq ۳$، $\sum_{k=۱}^{n} \mu(k!) = ۱$.

۲. تابع من‌گولت[1] Λ با ضابطهٔ

$$\Lambda(n) = \begin{cases} \log p & \text{اگر } n = p^k \text{، که } p \text{ عددی اول است و } k \geq ۱ \\ ۰ & \text{در غیر این صورت} \end{cases}$$

تعریف می‌شود. ثابت کنید

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d = -\sum_{d|n} \mu(d) \log d$$

[راهنمایی: نخست نشان دهید $\sum_{d|n} \Lambda(d) = \log n$ و سپس فرمول وارونسازی موبیوس را به‌کار ببرید.]

۳. فرض می‌کنیم $n = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$ تجزیهٔ عدد صحیح $n > ۱$ به عاملهای اول باشد. اگر f تابعی ضربی باشد، ثابت کنید

$$\sum_{d|n} \mu(d) f(d) = (۱ - f(p_۱))(۱ - f(p_۲)) \ldots (۱ - f(p_r))$$

[راهنمایی: بنا به قضیهٔ ۶ـ۴، تابع F با تعریف $F(n) = \sum_{d|n} \mu(d) f(d)$ ضربی است؛ پس $F(n)$ حاصلضرب مقدارهای $F(p_i^{k_i})$ است.]

۴. اگر عدد صحیح $n > ۱$ دارای تجزیهٔ $n = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$ به عاملهای اول باشد، با استفاده از تمرین ۳، حکمهای زیر را ثابت کنید:

(الف) $\sum_{d|n} \mu(d) \tau(d) = (-۱)^r$

1. Mangoldt

(ب) $\sum_{d|n} \mu(d)\sigma(d) = (-۱)^r p_۱ p_۲ \dots p_r$

(پ) $\sum_{d|n} \mu(d)/d = (۱ - ۱/p_۱)(۱ - ۱/p_۲)\dots(۱ - ۱/p_r)$

(ت) $\sum_{d|n} d\mu(d) = (۱ - p_۱)(۱ - p_۲)\dots(۱ - p_r)$

۵. فرض می‌کنیم $S(n)$ نشان دهندهٔ تعداد مقسوم‌علیه‌های خالی از مربع n باشد. اگر r تعداد مقسوم‌علیه‌های اول متمایز n باشد، نشان دهید

$$S(n) = \sum_{d|n} |\mu(d)| = ۲^r$$

[راهنمایی: S تابعی ضربی است.]

۶. فرمولهایی برای $\sum_{d|n} \mu^۲(d)/\tau(d)$ و $\sum_{d|n} \mu^۲(d)/\sigma(d)$ برحسب تجزیهٔ n به عاملهای اول به‌دست آورید.

۷. تابع لیوویل λ با ضابطهٔ $\lambda(۱) = ۱$ و $\lambda(n) = (-۱)^{k_۱+k_۲+\dots k_r}$ به‌ازای $n > ۱$، که تجزیهٔ آن به عاملهای اول به صورت $n = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$ است، تعریف می‌شود. به عنوان مثال، $\lambda(۳۶۰) = \lambda(۲^۳ \times ۳^۲ \times ۵) = (-۱)^{۳+۲+۱} = (-۱)^۶ = ۱$.

(الف) ثابت کنید λ تابعی ضربی است؛

(ب) نشان دهید به ازای هر عدد صحیح مثبت n داریم

$$\sum_{d|n} \lambda(d) = \begin{cases} ۱ & \text{اگر به ازای عدد صحیح } m\text{ای، } n = m^۲ \\ ۰ & \text{در غیر این صورت} \end{cases}$$

۸. اگر $n = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$ تجزیهٔ عدد صحیح $n > ۱$ به عاملهای اول باشد، نشان دهید $\sum_{d|n} \mu(d)\lambda(d) = ۲^r$.

۶ـ۳ تابع بزرگترین عدد صحیح [جزء صحیح]

تابع بزرگترین عدد صحیح یا «جزء صحیح» یا «کروشه» تابعی بسیار مناسب در بررسی مسأله‌های تقسیم‌پذیری [بخشپذیری] است. این تابع گرچه به معنی دقیق کلمه، نظریهٔ اعدادی نیست، بررسی آن در این فصل مناسبت دارد.

تعریف ۶ـ۴ به ازای هر عدد حقیقی دلخواه x، بزرگترین عدد صحیح نابیشتر از x را با $[x]$ نشان می‌دهیم؛ یعنی $[x]$ تنها عدد صحیحی است که $x - ۱ < [x] \leq x$. به عنوان مثال

$$\left[-\frac{۳}{۲}\right] = -۲,\ [\sqrt{۲}] = ۱,\ \left[\frac{۱}{۳}\right] = ۰,\ [\pi] = ۳,\ [-\pi] = -۴$$

نکته‌ای مهم که در اینجا باید به آن اشاره کرد این است که برابری $x = [x]$ برقرار است اگر و تنها اگر x عددی صحیح باشد. همچنین بنا به تعریف ۶ـ۴ واضح است که هر عدد حقیقی x را می‌توان به ازای عدد حقیقی θی مناسبی، $۰ \leq \theta < ۱$، به صورت

$$x = [x] + \theta$$

نوشت.

اکنون آماده می‌شویم مسألهٔ تعداد دفعات ظهور عدد اول pی خاصی در تجزیهٔ $n!$ را بررسی کنیم. به عنوان مثال، اگر $p = ۳$ و $n = ۹$، آنگاه

$$\begin{aligned} ۹! &= ۱ \times ۲ \times ۳ \times ۴ \times ۵ \times ۶ \times ۷ \times ۸ \times ۹ \\ &= ۲^۷ \times ۳^۴ \times ۵ \times ۷ \end{aligned}$$

بنابراین توان دقیقی از ۳ که $۹!$ را می‌شمارد، ۴ است. در دست داشتن فرمولی که پاسخ این مسأله را، بدون نوشتن $n!$ به صورت متعارف، به‌دست دهد، مطلوب است.

قضیهٔ ۶ـ۹ اگر n عددی صحیح مثبت و p عددی اول باشد، آنگاه نمای بزرگترین توانی از p که $n!$ را می‌شمارد برابر است با

$$\sum_{k=۱}^{\infty} [n/p^k]$$

(این سری نامتناهی نیست، زیرا به‌ازای $p^k > n$، $[n/p^k] = ۰$.)

اثبات. در میان n عدد صحیح مثبت نخست، عددهای تقسیمپذیر بر p عبارت‌اند از p، $۲p$، $\ldots$، tp، که در آن t بزرگترین عدد صحیحی است که $tp \leq n$؛ به بیان دیگر، t بزرگترین عدد صحیح نابیشتر از n/p است (یعنی، $t = [n/p]$). بنابراین، دقیقاً $[n/p]$ مضرب p در حاصلضربی که توسط $n!$ تعریف می‌شود، وجود دارد یعنی

$$p, ۲p, \ldots, \left[\frac{n}{p}\right] p \qquad (۱)$$

نمای p در تجزیهٔ $n!$ به عاملهای اول، با جمع کردن تعداد عددهای صحیح در (۱) با تعداد عددهای صحیح بخشپذیر بر $p^۲$ در میان ۱، ۲، $\ldots$، n، و سپس تعداد عددهای بخشپذیر بر $p^۳$، و الی آخر به‌دست می‌آید. اگر مانند پاراگراف نخست استدلال کنیم، عددهای صحیح میان ۱ و n که بر $p^۲$ بخشپذیرند، عبارت‌اند از

$$p^۲, ۲p^۲, \ldots, \left[\frac{n}{p^۲}\right] p^۲ \qquad (۲)$$

که تعداد آنها $[n/p^۲]$ است. از میان اینها، $[n/p^۳]$ تایشان باز بر p بخشپذیرند:

$$p^۳, ۲p^۳, \dots, \left[\frac{n}{p^۳}\right] p^۳ \qquad (۳)$$

با تکرار این فرایند به دفعات متناهی، نتیجه می‌گیریم کل تعداد دفعاتی که p عدد $n!$ را می‌شمارد، عبارت است از

$$\sum_{k=۱}^{\infty} \left[\frac{n}{p^k}\right] \qquad \square$$

این نتیجه را می‌توان به صورت معادلهٔ زیر، که معمولاً تحت عنوان فرمول لژاندر ارائه می‌شود، نوشت

$$n! = \prod_{p \leq n} p^{\sum_{k=۱}^{\infty} \left[\frac{n}{p^k}\right]}$$

مثال ۶ـ۲

می‌خواهیم تعداد صفرهایی را که نمایش دهدهی !۵۰ به آنها ختم می‌شود، تعیین کنیم. برای تعیین تعداد دفعه‌های ظهور ۱۰ در حاصلضرب !۵۰، کافی است نماهای ۲ و ۵ را در تجزیهٔ !۵۰ به عاملهای اول پیدا کنیم، و سپس کوچکترین آنها را انتخاب کنیم.

با محاسبه‌ای مستقیم ملاحظه می‌کنیم که

$$\left[\frac{۵۰}{۲}\right] + \left[\frac{۵۰}{۲^۲}\right] + \left[\frac{۵۰}{۲^۳}\right] + \left[\frac{۵۰}{۲^۴}\right] + \left[\frac{۵۰}{۲^۵}\right]$$
$$= ۲۵ + ۱۲ + ۶ + ۳ + ۱ = ۴۷$$

بنا به قضیهٔ ۶ـ۹، $۲^{۴۷}$ عدد !۵۰ را می‌شمارد، ولی $۲^{۴۸}$ نمی‌شمارد. به طور مشابه

$$\left[\frac{۵۰}{۵}\right] + \left[\frac{۵۰}{۵^۲}\right] = ۱۰ + ۲ = ۱۲$$

و بنابراین، نمای بزرگترین توانی از ۵ که !۵ را می‌شمارد ۱۲ است. یعنی !۵۰ به ۱۲ صفر ختم می‌شود. ■

اثبات قضیهٔ زیر با استفادهٔ از قضیهٔ ۶ـ۹ امکانپذیر است.

قضیهٔ ۶ـ۱۰ اگر n و r عددهای صحیح مثبتی باشند و $۱ \leq r \leq n$، آنگاه ضریب دوجمله‌ای

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

نیز عددی صحیح است.

اثبات. استدلال بر پایهٔ این نکته است که به‌ازای هر دو عدد حقیقی دلخواه a و b، $[a+b] \geq [a]+[b]$. پس به ازای هر عامل اول p از $r!(n-r)!$،

$$[n/p^k] \geq [r/p^k] + [(n-r)/p^k]، \qquad k = ۱, ۲, \ldots$$

با جمع کردن این نابرابریها با یکدیگر، به‌دست می‌آوریم

$$\sum_{k\geq ۱} \left[\frac{n}{p^k}\right] \geq \sum_{k\geq ۱} \left[\frac{r}{p^k}\right] + \sum_{k\geq ۱} \left[\frac{(n-r)}{p^k}\right] \qquad (۱)$$

سمت چپ (۱) نشان دهندهٔ نمای بزرگترین توانی از عدد اول p است که $n!$ را می‌شمارد، در حالی که، سمت راست آن برابر با نمای بزرگترین توان p است که در $r!(n-r)!$ وجود دارد. پس p در صورت $n!/r!(n-r)!$ حداقل به همان تعداد دفعات ظاهر می‌شود که در مخرج. چون این موضوع به‌ازای هر مقسوم‌علیه اول مخرج صادق است، $r!(n-r)!$ باید $n!$ را بشمارد، یعنی $n!/r!(n-r)!$ عددی صحیح است. □

فرع. به ازای هر عدد صحیح مثبت r، حاصلضرب هر r عدد صحیح مثبت متوالی بر $r!$ بخشپذیر است.

اثبات. حاصلضرب r عدد صحیح مثبت متوالی ختم شده به n عبارت است از

$$n(n-۱)(n-۲)\ldots(n-r+۱)$$

داریم

$$n(n-۱)\ldots(n-r+۱) = \left(\frac{n!}{r!(n-r)!}\right) r!$$

چون $(n!/r!(n-r)!)$ عددی صحیح است، نتیجه می‌شود $r!$ حاصلضرب $n(n-r)\ldots(n-r+۱)$ را می‌شمارد. □

اکنون که تابع بزرگترین عدد صحیح را معرفی کرده‌ایم، می‌خواهیم ببینیم چه نقشی در مطالعهٔ تابعهای حسابی [نظریهٔ اعدادی] ایفا می‌کند.

قضیهٔ ۶ـ۱۱ فرض می‌کنیم f و F تابعهایی حسابی باشند به طوری که

$$F(n) = \sum_{d|n} f(d)$$

در این صورت، به ازای هر عدد صحیح مثبت N داریم

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

اثبات. در آغاز ملاحظه کنید که

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d) \qquad (1)$$

استراتژی ما دسته‌بندی جمله‌های با مقدارهای $f(d)$ی یکسان دراین مجموع مضاعف است. به‌ازای عدد صحیح مثبت مفروض $k \leq N$، جملهٔ $f(k)$ در $\sum_{d|n} f(d)$ ظاهر می‌شود اگر و تنها اگر k مقسوم‌علیهی از n باشد. (چون هر عدد صحیحی مقسوم‌علیه خودش نیز هست، سمت راست (۱) حداقل یک بار حاوی $f(k)$ است.) حال برای محاسبهٔ تعداد مجموعهای $\sum_{d|n} f(d)$ای که شامل جملهٔ $f(k)$ هستند، کافی است تعداد مضربهای k در میان ۱, ۲, ... ,N را به‌دست آوریم. $[N/k]$ تا از این مضربها وجود دارد:

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k$$

پس، به‌ازای هر k با ضابطهٔ $1 \leq k \leq N$، $[N/k]$ عدد صحیح مثبت متفاوت n، $n \leq N$، وجود دارد به طوری که $f(k)$ جمله‌ای از $\sum_{d|n} f(d)$ است. پس، مجموع مضاعف (۱) را می‌توانیم به صورت

$$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

بازنویسی کنیم و بنابراین، اثبات تمام است. □

نتیجهٔ زیر کاربردی مستقیم از قضیهٔ ۶ـ۱۱ است.

فرع ۱. اگر N عدد صحیح مثبتی باشد، آنگاه

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

اثبات. با ملاحظهٔ اینکه $\tau(n) = \sum_{d|n} 1$، τ را جایگزین F می‌کنیم و f را تابع ثابتی تعریف می‌کنیم که به‌ازای هر n، $f(n) = 1$. □

به همین ترتیب، از رابطهٔ $\sigma(n) = \sum_{d|n} d$ نتیجه می‌شود:

فرع ۲. اگر N عدد صحیح مثبتی باشد، آنگاه

$$\sum_{n=۱}^{N} \sigma(n) = \sum_{n=۱}^{N} n \left[\frac{N}{n}\right]$$

شاید مثال زیر به روشن شدن دو فرع اخیر کمک کند.

مثال ۶ـ۳

$N = ۶$ را در نظر می‌گیریم. با توجه به محاسبات ابتدای بخش ۶ـ۱:

$$\sum_{n=۱}^{۶} \tau(n) = ۱۴$$

داریم

$$\sum_{n=۱}^{۶} \left[\frac{۶}{n}\right] = [۶] + [۳] + [۲] + \left[\frac{۳}{۲}\right] + \left[\frac{۶}{۵}\right] + [۱]$$
$$= ۶ + ۳ + ۲ + ۱ + ۱ + ۱ = ۱۴$$

که با فرع ۱ سازگار است. در حالت فعلی، همچنین داریم

$$\sum_{n=۱}^{۶} \sigma(n) = ۳۳$$

و با محاسبه‌ای ساده به‌دست می‌آید

$$\sum_{n=۱}^{۶} n \left[\frac{۶}{n}\right] = ۱[۶] + ۲[۳] + ۳[۲] + ۴[۳/۲] + ۵[۶/۵] + ۶[۱]$$
$$= ۱ \times ۶ + ۲ \times ۳ + ۳ \times ۲ + ۴ \times ۱ + ۵ \times ۱ + ۶ \times ۱ = ۳۳$$ ■

تمرینهای ۶ـ۳

۱. نشان دهید که به‌ازای عددهای صحیح $a, b > ۰$، عدد صحیح یکتای r، $۰ \le r < b$، وجود دارد به طوری که $a = [a/b]\, b + r$.

۲. فرض می‌کنیم x و y عددهایی حقیقی‌اند. ثابت کنید تابع بزرگترین عدد صحیح در ویژگیهای زیر صدق می‌کند:

(الف) به ازای هر عدد صحیح n، $[x + n] = [x] + n$.

(ب) برحسب اینکه x عددی صحیح باشد یا نباشد، ۱− یا ۰ $= [-x] + [x]$. [راهنمایی: بنویسید $x = [x] + \theta$، $\circ \leq \theta < ۱$، و بنابراین $-x = -[x] - ۱ + (۱ - \theta)$.]

(پ) $[x] + [y] \leq [x + y]$ و، هرگاه x و y مثبت باشند، $[x][y] \leq [xy]$.

(ت) به‌ازای هر عدد صحیح مثبت n، $[[x]/n] = [x/n]$. [راهنمایی: فرض کنید $x/n = [x/n] + \theta$، $\circ \leq \theta < ۱$؛ در این صورت $[x] = n\,[x/n] + [n\theta]$.]

(ث) به ازای عددهای صحیح n، m و k، $[nm/k] \geq n\,[m/k]$.

(ج) $[۲x] + [۲y] \geq [x] + [y] + [x + y]$. [راهنمایی: قرار دهید $x = [x] + \theta$ و $y = [y] + \theta'$، $\circ \leq \theta,\ \theta' < ۱$. حالتهایی را در نظر بگیرید که در آنها، به ترتیب، هیچ‌کدام، یکی، یا هردوی θ و θ' ناکمتر از $\frac{۱}{۲}$ باشند.]

۳. بزرگترین توانی از ۵ و بزرگترین توانی از ۷ را پیدا کنید که، به ترتیب، !۱۰۰۰ و !۲۰۰۰ را بشمارند.

۴. نشان دهید که به ازای هر عدد صحیح $n \geq \circ$، $n = [n/۲] - [-n/۲]$.

۵. (الف) نشان دهید که !۱۰۰۰ به ۲۴۹ صفر ختم می‌شود.

(ب) به ازای چه مقدارهای n عدد $n!$ به ۳۷ صفر ختم می‌شود؟

۶. اگر $n \geq ۱$ و p عددی اول باشد، ثابت کنید

(الف) $(۲n)!/(n!)^۲$ عدد صحیح زوجی است. [راهنمایی: از استقرا بر n استفاده کنید.]

(ب) نمای بزرگترین توان p که $(۲n)!/(n!)^۲$ را می‌شمارد عبارت است از

$$\sum_{k=۱}^{\infty}\left(\left[\frac{۲n}{p^k}\right] - ۲\left[\frac{n}{p^k}\right]\right)$$

(پ) نمای هر عدد اول p، $n < p < ۲n$، در تجزیهٔ $(۲n)!/(n!)^۲$ به عاملهای اول، ۱ است.

۷. فرض می‌کنیم عدد صحیح مثبت n برحسب توانهای عدد اول p نوشته شده باشد، یعنی $n = a_k p^k + \ldots a_۲ p^۲ + a_۱ p + a_\circ$، $\circ \leq a_i < p$. نشان دهید که نمای بزرگترین توانی از p که در تجزیهٔ $n!$ به عاملهای اول ظاهر می‌شود عبارت است از

$$\frac{n - (a_k + \ldots + a_۲ + a_۱ + a_\circ)}{p - ۱}$$

۸. (الف) با استفاده از تمرین ۷ نشان دهید که نمای بزرگترین توان p که $(p^k - ۱)!$ را می‌شمارد، $[p^k - (p - ۱)k - ۱]/(p - ۱)$ است. [راهنمایی: از اتحاد

$$p^k - ۱ = (p - ۱)(p^{k-۱} + \ldots + p^۲ + p + ۱)$$

استفاده کنید.]

(ب) بزرگترین توانهای ۳ و ۷ را که، به ترتیب، !۸۰ و !۲۴۰۰ را می‌شمارند، به‌دست آورید. [راهنمایی: ۱ − ۷^۴ = ۲۴۰۰.]

۹. عدد صحیح $n \geq ۱$ را طوری پیدا کنید که نمای بزرگترین توان ۵ موجود در $n!$ برابر ۱۰۰ باشد. [راهنمایی: چون مجموع ضریبهای توانهای ۵ مورد نیاز برای نمایش n در پایهٔ ۵ حداقل ۱ است، با بررسی معادلهٔ $(n-۱)/۴ = ۱۰۰$ آغاز کنید.]

۱۰. نشان دهید که به‌ازای عدد صحیح مثبت N داریم

(الف) $\sum_{n=۱}^{N} \mu(n)\,[N/n] = ۱$

(ب) $|\sum_{n=۱}^{N} \mu(n)/n| \leq ۱$

۱۱. درستی گزاره‌های تمرین ۱۰ را به ازای $N = ۶$ نشان دهید.

۱۲. نشان دهید که فرمول

$$\sum_{n=۱}^{N} \lambda(n) \left[\frac{N}{n}\right] = [\sqrt{N}]$$

به ازای هر عدد صحیح مثبت N برقرار است. [راهنمایی: با توجه به اینکه $[\sqrt{n}]$ مربع کامل نابیشتر از n وجود دارد، قضیهٔ ۶ـ۱۱ را در مورد تابع ضربی $F(n) = \sum_{d|n} \lambda(d)$ به‌کار ببرید.]

۱۳. ثابت کنید که به ازای عدد صحیح مثبت N داریم

(الف) $N = \sum_{n=۱}^{۲N} \tau(n) - \sum_{n=۱}^{N} [۲N/n]$

(ب) $\tau(N) = \sum_{n=۱}^{N} ([N/n] - [N-۱/n])$.

۷

تعمیم قضیهٔ فرما به‌وسیله اویلر

«اویلر خیلی راحت محاسبه می‌کرد، به همان راحتی که انسان نفس می‌کشد یا عقاب خود را در آسمان نگه می‌دارد.»

آراگو

۷ـ۱ لئونهارت اویلر

اهمیت کار فرما، بیش از آنکه به سهم او در ریاضیات زمان خودش بستگی داشته باشد، ناشی از تأثیر حیات‌بخش آن در کارهای ریاضیدانان نسلهای بعد است. شاید بزرگترین نقطهٔ ضعف کارنامهٔ فرما ناتوانی او در علاقه‌مند کردن دیگران به نظریهٔ اعداد جدید خودش بوده باشد. می‌بایست سده‌ای بگذرد تا ریاضیدان درجهٔ اولی چون لئونهارت اویلر (۱۷۰۷ـ۱۷۸۳)، بتواند کار او را بفهمد یا اهمیت آن را تصدیق کند. بسیاری از قضیه‌های بدون اثباتی که فرما مطرح کرد، مقهور تبحر اویلر گردید، و احتمالاً، استدلالهای ارائه‌شده توسط اویلر در اساس با اثباتهای ادعایی فرما تفاوتی نداشته است.

اویلر، مهمترین ریاضیدان سدهٔ هجدهم، پسر کشیش پروتستانی بود که در حومهٔ شهر بازل

در سوئیس زندگی می‌کرد. پدرش مشتاقانه مایل بود او حرفهٔ کشیشی را انتخاب کند و لئونهارت را در ۱۳ سالگی برای آموختن علوم الهی به دانشگاه بازل فرستاد. در آنجا بود که اویلر با یوهان برنولی ــ یکی از ریاضیدانان پیشرو آن زمان در اروپا ــ آشنا شد و با دو پسر برنولی، نیکولاوس و دانیل دوست شد. پس از اندک زمانی، مطالعهٔ الهیات را که به وی تحمیل شده بود رها کرد تا بتواند خود را کاملاً وقف ریاضیات کند. در ۱۷۲۳ درجهٔ کارشناسی ارشد خود را دریافت کرد و در سال ۱۷۲۷، که فقط ۱۹ سال داشت، رساله‌اش در باب بهترین روش نصب دکلهای کشتی، برندهٔ جایزه‌ای از آکادمی علوم پاریس شد.

برخلاف سدهٔ هفدهم که دوران ریاضیدانان آماتور بزرگ بود، سدهٔ هجدهم، تقریباً به‌طور کامل، دوران حرفه‌ایها ــ استادان دانشگاهها و عضوهای آکادمیهای علمی ــ بود. بسیاری از پادشاهان آن عصر از اینکه مشوق علم به‌حساب آیند، به خود می‌بالیدند، و آکادمیها، مانند جواهرات معنوی سلطنتی در دربارها می‌درخشیدند. گرچه احتمالاً انگیزهٔ این فرمانروایان کاملاً بشردوستانه نبوده است، باید گفت که انجمنهای علمی مرکزهای مهمی برای ارتقای علم بودند. آنها به دانشمندان برجسته حقوق می‌پرداختند، مجله‌های تحقیقاتی منظم انتشار می‌دادند، و جایزه‌های نقدی به یافته‌های علمی اعطا می‌کردند. اویلر در زمانهای متفاوتی عضو دو آکادمی جدیدالتأسیس بود، آکادمی سلطنتی در سن‌پترزبورگ (از ۱۷۲۷ تا ۱۷۴۱، و دوباره، از ۱۷۶۶ تا ۱۷۸۳) و آکادمی سلطنتی در برلین (از ۱۷۴۱ تا ۱۷۶۶). در ۱۷۲۵، پتر کبیر آکادمی سن‌پترزبورگ را تأسیس کرده و عده‌ای از ریاضیدانان پیشگام مانند نیکولاوس و دانیل برنولی به دعوت او به روسیه رفته بودند. به توصیهٔ آنها منصبی برای اویلر درنظرگرفته شد. او چندی قبل از آن به‌دلیل جوانی از کرسی استادی فیزیک در دانشگاه بازل محروم شده بود و بنابراین مشتاقانه دعوت آکادمی را پذیرفت. در پترزبورگ پس از مدت کوتاهی با کریستیان گولدباخ (صاحب حدس معروف)، دانشمند جامع‌الاطراف، که بعداً از استادی ریاضیات به وزارت امور خارجهٔ روسیه رسید، آشنا شد. با توجه به علایق گولدباخ، احتمالاً او نخستین فردی بوده است که نظر اویلر را به‌کارهای فرما در نظریهٔ اعداد جلب کرده است.

اویلر بالاخره از خفقان سیاسی حاکم بر روسیهٔ آن زمان به‌جان آمد و دعوت فردریک کبیر را برای عضویت در آکادمی برلین پذیرفت. نقل شده است که در یک میهمانی در بار پروس، مورد تفقد ملکهٔ مادر قرارگرفت و هنگامی‌که ملکه از او پرسید که چرا باید دانشمند عالیقدری چون وی این اندازه کمرو و کم‌حرف باشد، پاسخ داد: «خانم، من از کشوری آمده‌ام که در آنجا اگر کسی حرف بزند، سرش بالای دار می‌رود». ولی برخلاف رفتارگرم روسها با وی که او را مجذوب ساخته بود، فردریک و دربار او رفتار سردی با اویلر داشتند که موجب آزردگیش شد، و بنابراین، در ۱۷۶۶ برای گذرانیدن بقیهٔ ایام زندگی خود به پترزبورگ بازگشت. متأسفانه دو سه سال از بازگشت اویلر نگذشته بود که کاملاً نابینا شد.

مع‌الوصف، اویلر اجازه نداد که نابیناییش وقفه‌ای در فعالیتهای علمی او ایجاد کند؛ به یاری حافظهٔ شگفت‌انگیزش، انتشارات وی به اندازه‌ای زیاد شد که عملاً تدوین و تنظیم‌آنها فوق‌العاده دشوارگشت. بدون تردید، اویلر کثیرالآثارترین ریاضیدان در سراسر تاریخ ریاضیات است. در دوران زندگیش بیش از ۷۰۰ کتاب و مقاله نوشت یا تقریر کرد، و به اندازه‌ای مطلب چاپ‌نشده از خود باقی گذاشت که انتشار دستنوشته‌هایش توسط آکادمی سن‌پترزبورگ ۴۷ سال پس از وفات وی ادامه یافت. در ۱۹۱۱، انتشار مجموعه آثار اویلر توسط انجمن علوم طبیعی سوئیس آغاز شد و تخمین زده می‌شود که برای به‌انجام‌رساندن این برنامهٔ تاریخی به بیش از ۷۵ جلد بزرگ نیاز خواهد بود. بهترین گواه کیفیت این آثار آن است که دوازده بار برندهٔ جایزهٔ دو سالانه و پرطرفدار آکادمی فرانسه در پاریس شدند.

اویلر در طی اقامتش در برلین، مقاله پشت مقاله می‌نوشت و هر مقاله‌ای راکه به پایان می‌رسید روی انبوه دستنوشته‌های قبلی قرار می‌داد. هرگاه مجلهٔ آکادمی دچار کمبود مطلب می‌شد، از چند مقالهٔ اویلر که در بالای تل دستنوشته‌ها بودند استفاده می‌کرد. اما چون ارتفاع این تل سریعتر از نیازهای مجله رشد می‌کرد، مقاله‌های قسمت تحتانی تل تا مدتهای مدید در جای خود ماندند. به این دلیل است که مقاله‌های متعددی از اویلر وقتی منتشر شدند که مقاله‌های حاوی تعمیمها و بسطهای نتیجه‌های مذکور در آنها پیشتر به‌نام وی چاپ شده بودند. اضافه می‌کنیم که عادت اویلر به مطلع کردن عموم از نتایج کار خود کاملاً با سنت پنهانکاری زمان فرما متفاوت بود.

۷ـ۲ تابع فیِ اویلر

این فصل به قسمتی از نظریه می‌پردازد که از قضیه‌ای معروف به تعمیم قضیهٔ فرما توسط اویلر، نشأت گرفته است. به‌طور خلاصه، اویلر قضیهٔ فرما را که ناظر به همنهشتیهایِ به پیمانه‌های اول است، به همنهشتیهایِ به پیمانه‌های دلخواه تعمیم داد. در حین این کار، تابع حسابی مهمی به شرح زیر معرفی کرد.

تعریف ۷ـ۱ به‌ازای $n \geq ۱$، $\phi(n)$ نشان‌دهندهٔ تعداد عددهای صحیح مثبت متباین با n و نابیشتر از n است.

به‌عنوان مثالی از این تعریف، ملاحظه می‌کنیم که $\phi(۳۰) = ۸$؛ زیرا در میان عددهای صحیح مثبت نابیشتر از ۳۰، دقیقاً هشت عدد متباین با ۳۰ وجود دارد؛ این عددها مشخصاً عبارت‌اند از

$$۱, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹$$

به همین نحو خواننده می‌تواند تحقیق کند که به‌ازای چند عدد صحیح مثبت نخست داریم

$$\phi(۱) = ۱, \phi(۲) = ۱, \phi(۳) = ۲, \phi(۴) = ۲, \ \phi(۵) = ۴, \phi(۶) = ۲, \phi(۷) = ۶, \ldots$$

توجه می‌کنیم که $\phi(۱) = ۱$، زیرا $\gcd(۱, ۱) = ۱$. در حالی که اگر $n > ۱$، آنگاه $\gcd(n, n) = n \neq ۱$، بنابراین $\phi(n)$ را می‌توان به‌عنوان تعداد عددهای صحیح مثبت کوچکتر از n و متباین با n درنظر گرفت. تابع ϕ معمولاً به‌نام ابداع‌کننده‌اش تابع فیِ اویلر (و گاهی نیز نشانگر) نامیده می‌شود؛ ولی نماد تابعی $\phi(n)$ از آنِ گاوس است.

اگر n عدد اولی باشد، آنگاه هر عدد صحیح کمتر از n با آن متباین است؛ بنابراین $\phi(n) = n - ۱$. از سوی دیگر، اگر $n > ۱$ مرکب باشد، آنگاه n دارای مقسوم‌علیه d ای است که $۱ < d < n$. نتیجه می‌شود در میان عددهای ۱، ۲، ۳، ...، n، حداقل دو عدد صحیح وجود دارند که با n متباین نیستند، یعنی d و خود n. درنتیجه، $\phi(n) \leq n - ۲$. بنابراین ثابت می‌شود که به‌ازای $n > ۱$

$\phi(n) = n - ۱$ اگر و تنها اگر n اول باشد.

نخستین کاری که در دستور بحث ماست به‌دست‌آوردن فرمولی است که به ما امکان دهد مقدار $\phi(n)$ را مستقیماً با استفاده از تجزیهٔ n به توانهای عاملهای اول به‌دست آوریم. گام بزرگی در این راستا، مبتنی بر قضیهٔ زیر است

قضیهٔ ۷ـ۱ اگر p عددی اول باشد و $k > ۰$، آنگاه

$$\phi(p^k) = p^k - p^{k-۱} = p^k \left(۱ - \frac{۱}{p}\right)$$

اثبات. واضح است که $\gcd(n, p^k) = ۱$ اگر و تنها اگر $p \nmid n$. میان ۱ و p^k، $p^{k-۱}$ عدد صحیح بخشپذیر بر p وجود دارد، یعنی

$$p, ۲p, ۳p, \ldots, (p^{k-۱})p$$

بنابراین، مجموعهٔ $\{۱, ۲, \ldots, p^k\}$ شامل دقیقاً $p^k - p^{k-۱}$ عدد صحیح است که با p^k متباین‌اند و بنابراین، طبق تعریف تابع فی، $\phi(p^k) = p^k - p^{k-۱}$. □

به‌عنوان مثال داریم

$$\phi(۹) = \phi(۳^۲) = ۳^۲ - ۳ = ۶$$

شش عدد صحیح مثبت کوچکتر از ۹ و متباین با آن عبارت‌اند از ۱، ۲، ۴، ۵، ۷، ۸. به‌عنوان مثالی دیگر، ۸ عدد صحیح مثبت وجود دارند که کوچکتر از ۱۶ هستند و با آن متباین‌اند، یعنی، ۱، ۳، ۵، ۷، ۹، ۱۱، ۱۳، ۱۵. از قضیهٔ ۷ـ۱ نیز همین تعداد به‌دست می‌آید

$$\phi(۱۶) = \phi(۲^۴) = ۲^۴ - ۲^۳ = ۱۶ - ۸ = ۸$$

اکنون می‌دانیم که چگونه مقدار تابع ϕ را به‌ازای توانهای اول حساب کنیم و هدفمان به‌دست‌آوردن فرمولی برای $\phi(n)$ با استفاده از تجزیهٔ n به حاصلضرب عددهای اول است. حلقهٔ مفقوده در این زنجیره، واضح است: نشان می‌دهیم که ϕ تابعی ضربی است. راه را با ذکر لم آسانی هموار می‌کنیم.

لم. به‌ازای عددهای صحیح a، b و c، $\gcd(a, bc) = ۱$ اگر و تنها اگر $\gcd(a, b) = ۱$ و $\gcd(a, c) = ۱$.

اثبات. نخست فرض می‌کنیم $\gcd(a, bc) = ۱$ و قرار می‌دهیم $d = \gcd(a, b)$. در این صورت $d|a$ و $d|b$، و درنتیجه $d|a$ و $d|bc$. پس $\gcd(a, bc) \geq d$، و بنابراین $d = ۱$. با استدلالی مشابه، $\gcd(a, c) = ۱$.

به‌عکس، فرض می‌کنیم $\gcd(a, c) = \gcd(a, b) = ۱$ و $\gcd(a, bc) = d_۱ > ۱$. در این صورت $d_۱$ باید مقسوم‌علیه اولی مانند p داشته باشد. چون $d_۱|bc$، نتیجه می‌شود که $p|bc$؛ از این‌رو، $p|b$ یا $p|c$. اگر $p|b$، آنگاه (با توجه به اینکه $p|a$) $\gcd(a, b) \geq p$، که تناقضی است. به‌همین ترتیب، شرط $p|c$ نیز منجر به نتیجهٔ نادرست $\gcd(a, c) \geq p$ می‌شود. بنابراین $d_۱ = ۱$ و لم اثبات شده است. □

قضیهٔ ۷ـ۲ تابع ϕ تابعی ضربی است.

اثبات. لازم است نشان دهیم که هرگاه m و n عامل مشترکی نداشته باشند، $\phi(mn) = \phi(m)\phi(n)$. چون $\phi(۱) = ۱$، حکم به‌وضوح به‌ازای $m = ۱$ یا $n = ۱$ برقرار است. بنابراین فرض می‌کنیم $m > ۱$ و $n > ۱$. عددهای صحیح از ۱ تا mn را در m ستون

متشکل از n عدد صحیح، به‌صورت زیر، می‌نویسیم:

$$\begin{array}{ccccccc}
۱ & ۲ & \ldots & r & \ldots & m \\
m+۱ & m+۲ & & m+r & & ۲m \\
۲m+۱ & ۲m+۲ & & ۲m+r & & ۳m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-۱)m+۱ & (n-۱)m+۲ & & (n-۱)m+r & & nm
\end{array}$$

می‌دانیم $\phi(mn)$ برابر با تعداد درایه‌هایی در جدول فوق است که با mn متباین‌اند؛ باتوجه به لم، این برابر با تعداد عددهای صحیحی است که با هردوی m و n متباین‌اند.

پیش از اینکه به جزئیات بپردازیم، مناسب است دربارهٔ شگردی که به‌کار می‌بریم، توضیحی بدهیم: چون $\gcd(r,m) = \gcd(qm+r,m)$، عددهای واقع در ستون rام با m متباین‌اند، اگر و تنها اگر خود r با m متباین باشد. بنابراین، فقط $\phi(m)$ ستون حاوی عددهای متباین با m اند، و هر درایهٔ چنین ستونی با m متباین است. اکنون باید ثابت کنیم که در هریک از این $\phi(m)$ ستون دقیقاً $\phi(n)$ عدد صحیح متباین با n وجود دارد؛ زیرا در این صورت مجموعاً $\phi(m)\phi(n)$ عدد در جدول فوق وجود خواهد داشت که با هردوی m و n متباین‌اند.

درایه‌های ستون rام (که فرض شده است $\gcd(r,m) = ۱$) عبارت‌اند از

$$r, m+r, ۲m+r, \ldots, (n-۱)m+r$$

n عدد صحیح در این دنباله وجود دارند و هیچ دو تا از آنها به پیمانهٔ n همنهشت نیستند. درواقع، اگر مثلاً

$$km + r \equiv jm + r \ (\text{به پیمانهٔ } n)$$

که در آن $۰ \leq k < j < n$، لازم می‌آید $km \equiv jm$ (به پیمانهٔ n). چون $\gcd(m,n) = ۱$، می‌توانیم با حذف m از طرفین این همنهشتی به تناقض $k \equiv j$ (به پیمانهٔ n) برسیم. بنابراین، هریک از درایه‌های ستون rام با یکی از اعداد ۰، ۱، ۲، ...، $n-۱$ به پیمانهٔ n همنهشت‌اند. ولی اگر $s \equiv t$ (به پیمانهٔ n)، آنگاه $\gcd(s,n) = ۱$ اگر و تنها اگر $\gcd(t,n) = ۱$. نتیجه این است که تعداد عددهای صحیح متباین با n واقع در ستون rام برابر با تعداد عضوهای مجموعهٔ $\{۰, ۱, ۲, \ldots, n-۱\}$ یعنی $\phi(n)$ است. بنابراین، کل تعداد درایه‌های متباین با هردوی m و n در جدول مزبور، $\phi(m)\phi(n)$ است. به این ترتیب اثبات قضیه به انجام می‌رسد. □

با این مقدمات، اکنون می‌توانیم قضیهٔ زیر را ثابت کنیم.

قضیهٔ ۷ـ۳ اگر عددصحیح $n > ۱$ دارای تجزیهٔ $n = p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$ به عاملهای اول باشد، آنگاه

$$\begin{aligned}\phi(n) &= (p_۱^{k_۱} - p_۱^{k_۱-۱})(p_۲^{k_۲} - p_۲^{k_۲-۱}) \dots (p_r^{k_r} - p_r^{k_r-۱}) \\ &= n\left(۱ - \frac{۱}{p_۱}\right)\left(۱ - \frac{۱}{p_۲}\right) \dots \left(۱ - \frac{۱}{p_r}\right)\end{aligned}$$

اثبات. به استقرا بر r، یعنی تعداد عاملهای اول متمایز n متوسل می‌شویم. بنابه قضیهٔ ۷ـ۱، حکم به‌ازای $r = ۱$ برقرار است. فرض می‌کنیم حکم به‌ازای $r = i$ برقرار باشد. چون

$$\gcd(p_۱^{k_۱} p_۲^{k_۲} \dots p_i^{k_i}, {p_{i+۱}}^{k_i+۱}) = ۱$$

بنابه تعریف تابع ضربی داریم

$$\begin{aligned}\phi((p_۱^{k_۱} \dots p_i^{k_i}){p_{i+۱}}^{k_{i+۱}}) &= \phi(p_۱^{k_۱} \dots p_i^{k_i})\phi({p_{i+۱}}^{k_i+۱}) \\ &= \phi(p_۱^{k_۱} \dots p_i^{k_i}) \\ &\quad ({p_{i+۱}}^{k_i+۱} - {p_{i+۱}}^{k_{i+۱}-۱})\end{aligned}$$

بنابه فرض استقرا، در مورد عامل نخستِ سمت راست داریم

$$\phi(p_۱^{k_۱} p_۲^{k_۲} \dots p_i^{k_i}) = (p_۱^{k_۱} - p_۱^{k_۱-۱})(p_۲^{k_۲} - p_۲^{k_۱-۱}) \dots (p_i^{k_i} - p_i^{k_i-۱})$$

و با استفاده از این، مرحلهٔ استقرا و نیز اثبات به انجام می‌رسد. □

مثال ۷ـ۱

به‌عنوان نمونه، $\phi(۳۶۰)$ را حساب می‌کنیم. تجزیهٔ ۳۶۰ به توانهای عاملهای اول عبارت است از $۲^۳ \times ۳^۲ \times ۵$، و بنابراین، بنابه قضیهٔ ۷ـ۳ داریم

$$\begin{aligned}\phi(۳۶۰) &= ۳۶۰\left(۱ - \frac{۱}{۲}\right)\left(۱ - \frac{۱}{۳}\right)\left(۱ - \frac{۱}{۵}\right) \\ &= ۳۶۰ \times \frac{۱}{۲} \times \frac{۲}{۳} \times \frac{۴}{۵} = ۹۶\end{aligned}$$ ■

خوانندهٔ تیزبین متوجه شده است که بجز $\phi(۱)$ و $\phi(۲)$، مقدارهای $\phi(n)$ در مثالهای ما همواره زوج بوده‌اند. قضیهٔ زیر نشان می‌دهد که این ویژگی به‌ازای هر $n \geq ۳$ برقرار است.

قضیهٔ ۷ـ۴ به‌ازای $n > ۲$، $\phi(n)$ عدد صحیح زوجی است.

اثبات. نخست، فرض می‌کنیم n توانی از ۲ باشد، مثلاً $n = ۲^k$، $k \geq ۲$. بنابه قضیهٔ ۷ـ۳

$$\phi(n) = \phi(۲^k) = ۲^k \left(۱ - \frac{۱}{۲}\right) = ۲^{k-۱}$$

که عددی زوج است. اگر n توانی از ۲ نباشد، بر عدد اول فرد pای بخشپذیر است؛ بنابراین می‌توانیم n را به‌صورت $n = p^k m$، که در آن $k \geq ۱$ و $\gcd(p^k, m) = ۱$، بنویسیم. با استفاده از طبیعت ضربی تابع ϕ به‌دست می‌آوریم

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-۱}(p-۱)\phi(m)$$

که باز عددی زوج است، زیرا $۲|p-۱$. □

می‌توانیم قضیهٔ اقلیدس دربارهٔ نامتناهی بودن عددهای اول را به روش جدیدی ثابت کنیم: مانند پیش، فرض می‌کنیم فقط تعدادی متناهی عدد اول وجود دارد. این عددها را $p_۱$، ...، p_r می‌نامیم و عدد صحیح $n = p_۱p_۲\dots p_r$ را درنظر می‌گیریم. استدلال می‌کنیم که اگر $۱ < a \leq n$، آنگاه $\gcd(a, n) \neq ۱$؛ زیرا، بنابه قضیهٔ بنیادی حساب، a دارای مقسوم‌علیه اول q ای است. چون $p_۱$، $p_۲$، ...، p_r تنها عددهای اول موجود هستند، q باید یکی از این p_i ها باشد، بنابراین $q|n$؛ به‌عبارت دیگر، $\gcd(a, n) \geq q$. نتیجهٔ همهٔ اینها این است که $\phi(n) = ۱$، که بنابه قضیهٔ ۷ـ۴ به‌وضوح غیرممکن است.

تمرینهای ۷ـ۲

۱. $\phi(۱۰۰۱)$، $\phi(۵۰۴۰)$، و $\phi(۳۶۰۰۰)$ را حساب کنید.

۲. نشان دهید که به‌ازای $n = ۵۱۸۶$، $\phi(n) = \phi(n+۱) = \phi(n+۲)$.

۳. نشان دهید که اگر $k \geq ۰$، عددهای صحیح $m = ۳^k \times ۵۶۸$ و $n = ۳^k \times ۶۳۸$ همزمان در

$$\tau(m) = \tau(n)\text{،}\quad \sigma(m) = \sigma(n)\text{،}\quad \phi(m) = \phi(n)$$

صدق می‌کنند.

۴. درستی هریک از حکمهای زیر را ثابت کنید:

(الف) اگر n عدد صحیح مثبت فردی باشد، آنگاه $\phi(۲n) = \phi(n)$.

(ب) اگر n عدد صحیح مثبت زوجی باشد، آنگاه $\phi(۲n) = ۲\phi(n)$.

(پ) $\phi(۳n) = ۳\phi(n)$ اگر و تنها اگر $۳|n$.

(ت) $\phi(۳n) = ۲\phi(n)$ اگر و تنها اگر $۳ \nmid n$.

(ث) $\phi(n) = n/۲$ اگر و تنها اگر به‌ازای $k \geq ۱$ ای، $n = ۲^k$. [راهنمایی: بنویسید $n = ۲^k N$، که در آن N فرد است، و با استفاده از شرط $\phi(n) = n/۲$ نشان دهید $N = ۱$.]

۵. ثابت کنید که اگر هر دو عدد p و $۲p - ۱$ عدد اول فرد باشند و $n = ۲(۲p - ۱)$، آنگاه $\phi(n) = \phi(n + ۲)$.

۶. نشان دهید بینهایت عدد صحیح مثبت n وجود دارد که به‌ازای هریک از آنها $\phi(n)$ مربع کاملی است. [راهنمایی: عددهای صحیح $n = ۲^{k+۱}$ به‌ازای $k = ۱, ۲, \ldots$ را درنظر بگیرید.]

۷. درستی حکمهای زیر را نشان دهید:

(الف) به‌ازای هر عدد صحیح مثبت n، $(۱/۲)\sqrt{n} \leq \phi(n) \leq n$. [راهنمایی: بنویسید $n = ۲^{k_۰} p_۱^{k_۱} \ldots p_r^{k_r}$، بنابراین $\phi(n) = ۲^{k_۰ - ۱} p_۱^{k_۱ - ۱} \ldots p_r^{k_r - ۱}(p_۱ - ۱) \ldots (p_r - ۱)$. سپس با استفاده از نابرابریهای $\sqrt{p} < p - ۱$ و $k - \frac{۱}{۲} \geq k/۲$، $\phi(n) \geq ۲^{k_۰ - ۱} p_۱^{k_۱/۲} \ldots p_r^{k_r/۲}$ را نتیجه بگیرید.]

(ب) اگر عدد صحیح $n > ۱$ دارای r عامل اول متمایز باشد، آنگاه $\phi(n) \geq n/۲^r$.

(پ) اگر $n > ۱$ عددی مرکب باشد، آنگاه $\phi(n) \leq n - \sqrt{n}$. [راهنمایی: فرض کنید p کوچکترین عامل اول n باشد، بنابراین $p \leq \sqrt{n}$. در این صورت $\phi(n) \leq n(۱ - ۱/p)$.]

۸. ثابت کنید که اگر عدد صحیح n دارای r عامل اول فرد متمایز باشد، آنگاه $۲^r | \phi(n)$.

۹. ثابت کنید که

(الف) اگر n و $n + ۲$ زوجی از عددهای اول دوقلو باشند، آنگاه $\phi(n + ۲) = \phi(n) + ۲$؛ این معادله به‌ازای $n = ۱۲, ۱۴, ۲۰$ نیز برقرار است.

(ب) اگر هر دو عدد p و $۲p + ۱$ عدد اول فرد باشند، آنگاه $n = ۴p$ در معادلهٔ $\phi(n + ۲) = \phi(n) + ۲$ صدق می‌کنند.

۱۰. اگر هر عدد اول که n را می‌شمارد m را نیز بشمارد، ثابت کنید $\phi(nm) = n\phi(m)$؛ به‌ویژه، به‌ازای هر عدد صحیح مثبت n، $\phi(n^۲) = n\phi(n)$.

۱۱. (الف) ثابت کنید که اگر $\phi(n) | n - ۱$، آنگاه n عددی صحیح و خالی از مربع است. [راهنمایی: فرض کنید n به‌صورت $n = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$، $k_۱ \geq ۲$ به عاملهای اول تجزیه شود. در این صورت $p_۱ | \phi(n)$ و بنابراین $p_۱ | n - ۱$، که منجر به تناقض می‌شود.]

(ب) نشان دهید که اگر k و j عددهای صحیح مثبتی باشند و $n = ۲^k$ یا $n = ۲^k ۳^j$، آنگاه $\phi(n) | n$.

۱۲. اگر $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$، نابرابریهای زیر را ثابت کنید:

(الف) $\sigma(n)\phi(n) \geq n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\dots\left(1-\frac{1}{p_r^2}\right)$، و

(ب) $\tau(n)\phi(n) \geq n$. [راهنمایی: نشان دهید که $\tau(n)\phi(n) \geq 2^r \times n(1/2)^r$.]

۱۳. به فرض $d|n$، ثابت کنید $\phi(d)|\phi(n)$. [راهنمایی: تجزیهٔ n و d به عاملهای اول را درنظر بگیرید.]

۱۴. دو تعمیم زیر از قضیهٔ ۷ـ۲ را ثابت کنید

(الف) به‌ازای عددهای صحیح مثبت m و n داریم

$$\phi(m)\phi(n) = \frac{\phi(mn)\phi(d)}{d}$$

که در آن $d = \gcd(m, n)$.

(ب) به‌ازای عددهای صحیح مثبت m و n داریم

$$\phi(m)\phi(n) = \phi(\gcd(m, n))\phi(\operatorname{lcm}(m, n))$$

۱۵. ثابت کنید که

(الف) بینهایت عدد صحیح n وجود دارد به‌طوری که $\phi(n) = n/3$. [راهنمایی: $n = 2^k 3^j$ را به‌ازای عددهای صحیح مثبت k و j درنظر بگیرید.]

(ب) عدد صحیح n ای وجود ندارد که به‌ازای آن $\phi(n) = n/4$.

۱۶. نشان دهید از حدس گولدباخ نتیجه می‌شود که به‌ازای هر عدد صحیح زوج $2n$، عددهای صحیح مثبت n_1 و n_2 وجود دارند به‌طوری که $\phi(n_1) + \phi(n_2) = 2n$.

۱۷. نشان دهید که به‌ازای عدد صحیح مثبت دادهشدهٔ k،

(الف) حداکثر تعدادی متناهی عدد صحیح مثبت n وجود دارد که به‌ازای آنها $\phi(n) = k$؛

(ب) اگر معادلهٔ $\phi(n) = k$ دارای جواب یکتایی، مثلاً $n = n_0$، باشد، آنگاه $4|n_0$. [راهنمایی: تمرین ۴ (الف) و ۴ (ب) را نگاه کنید.]

براساس حدس معروفی از کارمایکل، تعداد جوابهای $\phi(n) = k$ نمی‌تواند برابر ۱ باشد.

۱۸. همهٔ جوابهای $\phi(n) = 16$ و $\phi(n) = 24$ را پیداکنید. [راهنمایی: اگر $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ در $\phi(n) = k$ صدق کند، آنگاه $n = [k/\Pi(p_i - 1)]\Pi p_i$. بنابراین، عددهای صحیح $d_i = p_i - 1$ را می‌توان با توجه به شرطهای زیر تعیین کرد: (۱) $d_i|k$، (۲) $d_i + 1$ عددی اول باشد و (۳) $k/(\Pi d_i)$ دارای عامل اولی که در Πp_i موجود نیست، نباشد.]

۱۹. (الف) ثابت کنید که اگر p عددی اول و $۲p+۱$ مرکب باشد، معادلهٔ $\phi(n)=۲p$ حلپذیر نیست.

(ب) ثابت کنید معادلهٔ $\phi(n)=۱۴$ جواب ندارد، و ۱۴ کوچکترین عدد صحیح زوج (مثبت) با این ویژگی است.

۲۰. اگر p عددی اول باشد و $k\geq ۲$، نشان دهید $\phi(\phi(p^k))=p^{k-۲}\phi((p-۱)^۲)$.

۷ـ۳ قضیهٔ اویلر

به‌طوری که پیشتر گفته شد، نخستین اثبات منتشرشدهٔ قضیهٔ فرما (یعنی این قضیه که اگر $p\nmid a$، آنگاه $a^{p-۱}\equiv ۱$ (به پیمانهٔ p)) در سال ۱۷۳۶ توسط اویلر ارائه شد. وی بعدها در سال ۱۷۶۰ موفق شد قضیهٔ فرما را از حالت عدد اول p به عدد صحیح مثبت دلخواه n تعمیم دهد. این نتیجهٔ مهم حاکی است که: اگر $\gcd(a,n)=۱$، آنگاه $a^{\phi(n)}\equiv ۱$ (به پیمانهٔ n).

به‌عنوان مثال، به‌ازای $n=۳۰$ و $a=۱۱$ داریم

$$۱۱^{\phi(۳۰)}\equiv ۱۱^۸\equiv (۱۱^۲)^۴\equiv (۱۲۱)^۴\equiv ۱^۴\equiv ۱ \quad (\text{به پیمانهٔ } ۳۰)$$

برای اثبات تعمیم اویلر از قضیهٔ فرما، به لمی مقدماتی نیازمندیم.

لم. فرض می‌کنیم $n>۱$ و $\gcd(a,n)=۱$. اگر $a_۱$، $a_۲$، ...، $a_{\phi(n)}$ عددهای صحیح مثبت کوچکتر از n و متباین با آن باشند، آنگاه هریک از

$$aa_۱, aa_۲, \ldots, aa_{\phi(n)}$$

با یکی از عددهای

$$a_۱, a_۲, \ldots, a_{\phi(n)}$$

همنهشت به پیمانهٔ n است.

اثبات. توجه می‌کنیم که هیچ دو تا از عددهای صحیح $aa_۱$، $aa_۲$، ...، $aa_{\phi(n)}$ همنهشت به پیمانهٔ n نیستند زیرا اگر $aa_i\equiv aa_j$ (به پیمانهٔ n)، $۱\leq i<j\leq \phi(n)$، آنگاه با استفاده از قانون حذف به‌دست می‌آوریم $a_i\equiv a_j$ (به پیمانهٔ n)، که تناقض است. به‌علاوه، چون به‌ازای هر i، $\gcd(a_i,n)=۱$ و $\gcd(a,n)=۱$، بنا به لم بعد از قضیهٔ ۷ـ۱، هریک از aa_i ها با n متباین است.

یکی از این عددها، مثلاً aa_i، را درنظر می‌گیریم. عدد صحیح یکتای b ای وجود دارد به‌طوری که $\circ \leq b < n$، و به‌ازای آن، $aa_i \equiv b$ (به پیمانهٔ n). چون

$$\gcd(b,n) = \gcd(aa_i,n) = ۱$$

b باید یکی از عددهای صحیح $a_۱$، $a_۲$، …، $a_{\phi(n)}$ باشد. این نشان می‌دهد که هریک از عددهای $aa_۱$، $aa_۲$، …، $aa_{\phi(n)}$ با یکی از عددهای $a_۱$، $a_۲$، …، $a_{\phi(n)}$ همنهشت به پیمانهٔ n است. □

قضیهٔ ۷ـ۵ (اویلر). اگر n عددی صحیح و مثبت باشد و $\gcd(a,n) = ۱$، آنگاه $a^{\phi(n)} \equiv ۱$ (به پیمانهٔ n).

اثبات. حکم به‌ازای $n = ۱$ به‌وضوح برقرار است. پس فرض می‌کنیم $n > ۱$. عددهای صحیح مثبتِ کوچکتر از n و متباین با آن را $a_۱$، $a_۲$، …، $a_{\phi(n)}$ می‌نامیم. چون $\gcd(a,n) = ۱$، بنابه لم، هریک از عددهای $aa_۱$، $aa_۲$، …، $aa_{\phi(n)}$ با یکی از عددهای $a_۱$، $a_۲$، …، $a_{\phi(n)}$ همنهشت به پیمانهٔ n است. پس

$$aa_۱ \equiv a'_۱ \ (\text{به پیمانهٔ } n)$$
$$aa_۲ \equiv a'_۲ \ (\text{به پیمانهٔ } n)$$
$$\vdots \qquad \vdots$$
$$aa_{\phi(n)} \equiv a'_{\phi(n)} \ (\text{به پیمانهٔ } n)$$

که در آن $a'_۱$، $a'_۲$، …، $a'_{\phi(n)}$ همان عددهای صحیح $a_۱$، $a_۲$، …، $a_{\phi(n)}$، احتمالاً با ترتیبی متفاوت، هستند. با ضرب این $\phi(n)$ همنهشتی درهم، به‌دست می‌آوریم

$$(aa_۱)(aa_۲)\ldots(aa_{\phi(n)}) \equiv a'_۱a'_۲\ldots a'_{\phi(n)} \ (\text{به پیمانهٔ } n)$$
$$\equiv a_۱a_۲\ldots a_{\phi(n)} \ (\text{به پیمانهٔ } n)$$

و بنابراین

$$a^{\phi(n)}(a_۱a_۲\ldots a_{\phi(n)}) \equiv a_۱a_۲\ldots a_{\phi(n)} \ (\text{به پیمانهٔ } n)$$

چون به‌ازای هر i، $\gcd(a_i,n) = ۱$، بنابه لم پیش از قضیهٔ ۷ـ۲، ۱، $\gcd(a_۱a_۲\ldots a_{\phi(n)},n) = ۱$. بنابراین با تقسیم هر دو طرف همنهشتی اخیر بر عامل مشترک $a_۱a_۲\ldots a_{\phi(n)}$، به‌دست می‌آوریم

$$a^{\phi(n)} \equiv ۱ \ (\text{به پیمانهٔ } n)$$

□

این اثبات را می‌توان با مثالی عددی به بهترین نحو توضیح داد. به‌عنوان نمونه، فرض می‌کنیم $n = ۹$. عددهای صحیح مثبت کوچکتر از ۹ و متباین با آن عبارت‌اند از

$$۱, ۲, ۴, ۵, ۷, ۸$$

اینها نقش عددهای صحیح $a_۱$، $a_۲$، ...، $a_{\phi(n)}$ در اثبات قضیهٔ ۷ـ۵ را ایفا می‌کنند. اگر $a = -۴$، آنگاه عددهای صحیح aa_i عبارت‌اند از

$$-۴, -۸, -۱۶, -۲۰, -۲۸, -۳۲$$

که به پیمانهٔ ۹

$$-۴ \equiv ۵, -۸ \equiv ۱, -۱۶ \equiv ۲, -۲۰ \equiv ۷, -۲۸ \equiv ۸, -۳۲ \equiv ۴$$

اگر همنهشتیهای فوق در یکدیگر ضرب شوند، به‌دست می‌آوریم

$$(-۴)(-۸)(-۱۶)(-۲۰)(-۲۸)(-۳۲) \equiv ۵ \times ۱ \times ۲ \times ۷ \times ۸ \times ۴ \ (\text{به پیمانهٔ ۹})$$

یا

$$(۱ \times ۲ \times ۴ \times ۵ \times ۷ \times ۸)(-۴)^۶ \equiv (۱ \times ۲ \times ۴ \times ۵ \times ۷ \times ۸) \ (\text{به پیمانهٔ ۹})$$

با حذف پیاپی شش عدد صحیح ۱، ۲، ۴، ۵، ۷، ۸ به‌دلیل متباین بودن با ۹، نتیجه می‌شود

$$(-۴)^۶ \equiv ۱ \ (\text{به پیمانهٔ ۹})$$

درستی این همنهشتی با محاسبهٔ زیر تأیید می‌شود

$$(-۴)^۶ \equiv ۴^۶ \equiv (۶۴)^۲ \equiv ۱^۲ \equiv ۱ \ (\text{به پیمانهٔ ۹})$$

توجه کنید که قضیهٔ ۷ـ۵ واقعاً قضیهٔ منسوب به فرما را، که پیشتر ثابت کردیم، تعمیم می‌دهد. زیرا اگر p عددی اول باشد، آنگاه $\phi(p) = p - ۱$؛ پس، اگر $\gcd(a, p) = ۱$، به‌دست می‌آوریم

$$a^{p-۱} \equiv a^{\phi(p)} \equiv ۱ \ (\text{به پیمانهٔ } p)$$

و بنابراین:

فرع (فرما). اگر p عددی اول باشد و $p \nmid a$، آنگاه

$$a^{p-1} \equiv 1 \pmod{p}$$

مثال ۷ـ۲

قضیهٔ اویلر در تحویل توانهای بزرگ به پیمانهٔ n سودمند است. به‌عنوان مثال، دو رقم سمت راست نمایش دهدهی 3^{256} را تعیین می‌کنیم. این کار معادل است با تعیین کوچکترین عدد صحیح نامنفی همنهشت با 3^{256} به پیمانهٔ ۱۰۰. چون $\gcd(3, 100) = 1$ و

$$\phi(100) = \phi(2^2 \times 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

بنابه قضیهٔ اویلر داریم

$$3^{40} \equiv 1 \pmod{100}$$

و بنابه الگوریتم تقسیم، $256 = 6 \times 40 + 16$؛ پس

$$3^{256} = 3^{6\times 40+16} = (3^{40})^6 \times 3^{16} \equiv 3^{16} \pmod{100}$$

و مسألهٔ ما به محاسبهٔ دو رقم سمت راست 3^{16} تحویل می‌شود. بدون ذکر دلیلها، محاسبه به شرح زیر است

$$3^{16} \equiv (81)^4 \equiv (-19)^4 = (361)^2 \equiv (61)^2 \equiv 21 \pmod{100} \qquad \blacksquare$$

راه دیگری برای اثبات قضیهٔ اویلر وجود دارد که مستلزم استفاده از قضیهٔ فرماست.

اثبات دوم قضیهٔ اویلر: در آغاز، به استقرا نشان می‌دهیم که اگر $p \nmid a$ (p عددی اول است)، آنگاه به‌ازای هر عدد صحیح مثبت k،

$$a^{\phi(p^k)} \equiv 1 \pmod{p^k} \qquad (1)$$

به‌ازای $k = 1$، حکم به‌صورت قضیهٔ فرما تبدیل می‌شود. با فرض درستی (۱) به‌ازای مقدار ثابتی از k، نشان می‌دهیم که (۱) به‌ازای $k + 1$ نیز درست است.

چون (۱) بنابه فرض برقرار است، به‌ازای عدد صحیح q ای می‌توانیم بنویسیم

$$a^{\phi(p^k)} = 1 + qp^k$$

توجه داریم که

$$\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\phi(p^k)$$

با استفاده از این رابطه‌ها و قضیهٔ دوجمله‌ای، به‌دست می‌آوریم

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} \\ &= (1 + qp^k)^p \\ &= 1 + \binom{p}{1}(qp^k) + \binom{p}{2}(qp^k)^2 + \dots \\ &\quad + \binom{p}{p-1}(qp^k)^{p-1} + (qp^k)^p \\ &\equiv 1 + \binom{p}{1}(qp^k) \ (\text{به پیمانهٔ } p^{k+1}) \end{aligned}$$

ولی $p | \binom{p}{1}$ و بنابراین $p^{k+1} | \binom{p}{1}(qp^k)$. پس، آخرین همنهشتی نوشته‌شده به‌صورت

$$a^{\phi(p^{k+1})} \equiv 1 \ (\text{به پیمانهٔ } p^{k+1})$$

درمی‌آید و اثبات مرحلهٔ استقرا به انجام می‌رسد.

اکنون فرض می‌کنیم $\gcd(a, n) = 1$ و n به‌صورت $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ به عاملهای اول تجزیه شود. با توجه به آنچه که پیشتر ثابت شده است، هریک از همنهشتیهای

$$a^{\phi(p_i^{k_i})} \equiv 1 \ (\text{به پیمانهٔ } p_i^{k_i}), \qquad i = 1, 2, \dots, r \qquad (2)$$

برقرار است. چون $\phi(n)$ بر $\phi(p_i^{k_i})$ بخشپذیر است، با به توان $[\phi(n)/\phi(p_i^{k_i})]$ رسانیدن هر دو طرف (۲) نتیجه می‌شود

$$a^{\phi(n)} \equiv 1 \ (\text{به پیمانهٔ } p_i^{k_i}), \qquad i = 1, 2, \dots, r$$

چون پیمانه‌های همنهشتیها متباین‌اند، از اینجا نتیجه می‌شود

$$a^{\phi(n)} \equiv 1 (\text{به پیمانهٔ } p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$$

یا

$$a^{\phi(n)} \equiv 1 \ (\text{به پیمانهٔ } n) \qquad \square$$

دربارهٔ سودمندی قضیهٔ اویلر در نظریهٔ اعداد هرچه بگوییم کم گفته‌ایم. به‌عنوان مثال، این قضیه منجر به اثبات متفاوتی برای قضیهٔ باقیماندهٔ چینی می‌شود. به بیان دیگر، می‌خواهیم ثابت کنیم که اگر $\gcd(n_i, n_j) = ۱$، $i \neq j$، آنگاه دستگاه همنهشتیهای خطی

$$x \equiv a_i \ (\text{به پیمانهٔ } n_i), \qquad i = ۱, ۲, \ldots, r$$

جواب دارد. فرض می‌کنیم $n = n_۱ n_۲ \ldots n_r$ و به‌ازای $i = ۱, ۲, \ldots, r$ قرار می‌دهیم $N_i = n/n_i$. در این صورت عدد صحیح

$$x = a_۱ N_۱^{\phi(n_۱)} + a_۲ N_۲^{\phi(n_۲)} + \ldots + a_r N_r^{\phi(n_r)}$$

خواسته‌های ما را برآورده می‌کند. برای ملاحظهٔ این مطلب، نخست توجه کنید که اگر $j \neq i$، آنگاه $N_j \equiv ۰ \ (\text{به پیمانهٔ } n_i)$؛ بنابراین

$$x \equiv a_i N_i^{\phi(n_i)} \ (\text{به پیمانهٔ } n_i)$$

ولی چون $\gcd(N_i, n_i) = ۱$، داریم

$$N_i^{\phi(n_i)} \equiv ۱ \ (\text{به پیمانهٔ } n_i)$$

و بنابراین به‌ازای هر i، $x \equiv a_i \ (\text{به پیمانهٔ } n_i)$.

به‌عنوان کاربرد دیگری از قضیهٔ اویلر نشان می‌دهیم که اگر n عدد صحیح فردی باشد که مضربی از ۵ نیست، آنگاه n، عددصحیحی را که همهٔ رقمهایش برابر ۱ است، می‌شمارد. (به‌عنوان مثال ۱۱۱۱۱۱|۷.) چون $\gcd(n, ۱۰) = ۱$ و $\gcd(۹, ۱۰) = ۱$ داریم $\gcd(۹n, ۱۰) = ۱$. پس، بنابه قضیهٔ ۷ـ۵

$$۱۰^{\phi(۹n)} \equiv ۱ \ (\text{به پیمانهٔ } ۹n)$$

یعنی به‌ازای عدد صحیح k ای، $۱۰^{\phi(۹n)} - ۱ = ۹nk$، یا

$$kn = \frac{۱۰^{\phi(۹n)} - ۱}{۹}$$

طرف راست برابری فوق عددصحیحی است که همهٔ رقمهایش برابر ۱ است، زیرا، به‌وضوح، هر رقم صورت کسر برابر ۹ است.

تمرینهای ۷ـ۳

۱. با استفاده از قضیهٔ اویلر حکمهای زیر را ثابت کنید

(الف) به‌ازای هر عدد صحیح a، (به پیمانهٔ ۱۷۲۹) $a \equiv a^{۳۷}$.

[راهنمایی: $۱۷۲۹ = ۷ \times ۱۳ \times ۱۹$.]

(ب) به‌ازای هر عدد صحیح a، (به پیمانهٔ ۲۷۳۰) $a \equiv a^{۱۳}$.

[راهنمایی: $۲۷۳۰ = ۲ \times ۳ \times ۵ \times ۷ \times ۱۳$.]

(پ) به‌ازای هر عدد صحیح فرد a، (به پیمانهٔ ۴۰۸۰) $a \equiv a^{۳۳}$.

[راهنمایی: $۴۰۸۰ = ۱۵ \times ۱۶ \times ۱۷$.]

۲. با استفاده از قضیهٔ اویلر نشان دهید که به‌ازای هر عدد صحیح $n \geq ۰$

$$۵۱ | ۱۰^{۳۲n+۹} - ۷$$

۳. نشان دهید که به‌ازای هر عدد صحیح a، $۲^{۱۵} - ۲^{۳}$ عدد $a^{۱۵} - a^{۳}$ را می‌شمارد. [راهنمایی: $۲^{۱۵} - ۲^{۳} = ۵ \times ۷ \times ۸ \times ۹ \times ۱۳$.]

۴. نشان دهید که اگر $\gcd(a,n) = \gcd(a-۱,n) = ۱$، آنگاه

$$۱ + a + a^{۲} + \ldots + a^{\phi(n)-۱} \equiv ۰ \ (\text{به پیمانهٔ } n)$$

[راهنمایی: توجه کنید که $a^{\phi(n)} - ۱ = (a-۱)(a^{\phi(n)-۱} + \ldots + a^{۲} + a + ۱)$.]

۵. ثابت کنید که اگر m و n عددهای صحیح مثبت متباینی باشند، آنگاه

$$m^{\phi(n)} + n^{\phi(m)} \equiv ۱ \ (\text{به پیمانهٔ } mn)$$

۶. کاستیهای اثبات زیر از قضیهٔ اویلر را رفع کنید: فرض می‌کنیم p مقسوم‌علیه اولی از n باشد و $\gcd(a,p) = ۱$. بنابه قضیهٔ فرما، (به پیمانهٔ p) $a^{p-۱} \equiv ۱$، بنابراین به‌ازای t ای، $a^{p-۱} = ۱ + tp$. پس

$$a^{p(p-۱)} = (۱+tp)^{p} = ۱ + \binom{p}{۱}(tp) + \ldots + (tp)^{p} \equiv ۱ \ (\text{به پیمانهٔ } p^{۲})$$

و، بنابه استقرا، (به پیمانهٔ p^{k}) $a^{p^{k-۱}(p-۱)} \equiv ۱$، که در آن $k = ۱, ۲, \ldots$. هر دو طرف این همنهشتی را به توان $[\phi(n)/p^{k-۱}(p-۱)]$ می‌رسانیم و به‌دست می‌آوریم (به پیمانهٔ p^{k}) $a^{\phi(n)} \equiv ۱$. پس، (به پیمانهٔ n) $a^{\phi(n)} \equiv ۱$.

۷. رقم یکان 3^{100} را به کمک قضیهٔ اویلر تعیین کنید.

۸. (الف) اگر $\gcd(a, n) = 1$، نشان دهید که همنهشتی خطی $ax \equiv b$ (به پیمانهٔ n) دارای جواب $x \equiv ba^{\phi(n)-1}$ (به پیمانهٔ n) است.

(ب) با استفاده از (الف)، همنهشتیهای $3x \equiv 5$ (به پیمانهٔ ۲۶)، $13x \equiv 2$ (به پیمانهٔ ۴۰) و $10x \equiv 21$ (به پیمانهٔ ۴۹) را حل کنید.

۹. ثابت کنید که هر عدد اول بجز ۲ یا ۵ بینهایت عدد صحیح ۱، ۱۱، ۱۱۱، ۱۱۱۱، ... را می‌شمارد.

۱۰. ثابت کنید هریک از حکمهای زیر به‌ازای هر عدد اول p برقرارند:

(الف) $\tau(p!) = 2\tau((p-1)!)$

(ب) $\sigma(p!) = (p+1)\sigma((p-1)!)$

(پ) $\phi(p!) = (p-1)\phi((p-1)!)$

۱۱. به‌ازای $n \geq 1$، هر مجموعهٔ متشکل از $\phi(n)$ عدد صحیح متباین با n که به پیمانهٔ n ناهمنهشت باشند، مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ n نامیده می‌شود (یعنی، مجموعهٔ تقلیل‌یافتهٔ مانده‌ها شامل عضوهایی از یک مجموعهٔ کامل مانده‌ها به پیمانهٔ n است که با n متباین‌اند). نشان دهید

(الف) عددهای صحیح ۳۱−، ۱۶−، ۸−، ۱۳، ۲۵، ۸۰ مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ ۹ تشکیل می‌دهند؛

(ب) عددهای صحیح 3، 3^2، 3^3، 3^4، 3^5، 3^6 مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ ۱۴ تشکیل می‌دهند؛

(پ) عددهای صحیح 2، 2^2، 2^3، ...، 2^{18} مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ ۲۷ تشکیل می‌دهند؛

۱۲. اگر p عدد اول فردی باشد، نشان دهید عددهای صحیح

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$$

مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ p تشکیل می‌دهند.

۷ـ۴ برخی از ویژگیهای تابع فی

در قضیهٔ بعدی وجه شگفت‌انگیزی از تابع ϕ مطرح می‌شود؛ یعنی، این ویژگی که مجموع مقدارهای $\phi(d)$، وقتی d همهٔ مقسوم‌علیه‌های مثبت n را اختیار کند، برابر خود n است. این حقیقت را نخستین بار گاوس دریافت.

قضیهٔ ۷ـ۶ (گاوس). به‌ازای هر عدد صحیح مثبت $n \geq ۱$

$$n = \sum_{d|n} \phi(d)$$

که در آن، مجموع ناظر به همهٔ مقسوم‌علیه‌های مثبت n است.

اثبات. عددهای صحیح میان ۱ و n، به‌شرح زیر، به رده‌هایی افراز می‌شوند: اگر d مقسوم‌علیه مثبتی از n باشد، عدد صحیح m را به شرطی در ردهٔ S_d قرار می‌دهیم که $\gcd(m, n) = d$. به زبان نمادی داریم

$$S_d = \{m | \gcd(m, n) = d; ۱ \leq m \leq n\}$$

ولی $\gcd(m, n) = d$ اگر و تنها اگر $\gcd(m/d, n/d) = ۱$. پس تعداد عددهای صحیح در ردهٔ S_d برابر با تعداد عددهای صحیح مثبتِ نابیشتر از n/d و متباین با آن است؛ به عبارت دیگر، برابر با $\phi(n/d)$ است. چون هریک از n عدد صحیحِ موجود در مجموعهٔ $\{۱, ۲, \ldots, n\}$ متعلق به دقیقاً یکی از رده‌های S_d است، فرمول

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

را به‌دست می‌آوریم. ولی n/d نیز مانند d همهٔ مقسوم‌علیه‌های مثبت n را اختیار می‌کند؛ پس

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

و قضیه ثابت می‌شود. □

مثال ۷ـ۳

مثال عددی ساده‌ای از آنچه در بالا گفتیم به‌ازای $n = ۱۰$ به‌دست می‌آید. در این مثال، رده‌های S_d عبارت‌اند از

$$S_۱ = \{۱, ۳, ۷, ۹\}$$
$$S_۲ = \{۲, ۴, ۶, ۸\}$$
$$S_۵ = \{۵\}$$
$$S_{۱۰} = \{۱۰\}$$

این رده‌ها شامل، به‌ترتیب، $\phi(۱۰) = ۴$، $\phi(۵) = ۴$، $\phi(۲) = ۱$، و $\phi(۱) = ۱$ عدد صحیح هستند. بنابراین

$$\begin{aligned}\sum_{d|n}\phi(d) &= \phi(۱۰) + \phi(۵) + \phi(۲) + \phi(۱)\\ &= ۴ + ۴ + ۱ + ۱ = ۱۰\end{aligned}$$ ■

ارائهٔ اثبات دیگری از قضیهٔ ۷ـ۶ با استفاده از ویژگی ضربی تابع ϕ، آموزنده است. جزئیات آن به‌شرح زیر است: اگر $n = ۱$، آنگاه به‌وضوح

$$\sum_{d|n}\phi(d) = \sum_{d|۱}\phi(d) = \phi(۱) = ۱ = n$$

به فرض $n > ۱$، تابع حسابی

$$F(n) = \sum_{d|n}\phi(d)$$

را درنظر می‌گیریم. چون می‌دانیم ϕ تابعی ضربی است، بنابه قضیهٔ ۶ـ۴، F نیز ضربی است. پس اگر $n = p_۱^{k_۱}p_۲^{k_۲}\dots p_r^{k_r}$ تجزیهٔ n به عاملهای اول باشد، آنگاه

$$F(n) = F(p_۱^{k_۱})F(p_۲^{k_۲})\dots F(p_r^{k_r})$$

به‌ازای هر مقدار i داریم

$$\begin{aligned}F(p_i^{k_i}) &= \sum_{d|p_i^{k_i}}\phi(d)\\ &= \phi(۱) + \phi(p_i) + \phi(p_i^۲) + \dots + \phi(p_i^{k_i})\\ &= ۱ + (p_i - ۱) + (p_i^۲ - p_i) + (p_i^۳ - p_i^۲)\\ &\quad + \dots + (p_i^{k_i} - p_i^{k_i - ۱})\\ &= p_i^{k_i}\end{aligned}$$

زیرا جمله‌های عبارت فوق یکدیگر را حذف می‌کنند و فقط $p_i^{k_i}$ باقی می‌ماند. پس

$$F(n) = p_۱^{k_۱}p_۲^{k_۲}\dots p_r^{k_r} = n$$

و بنابراین

$$n = \sum_{d|n} \phi(d)$$

که نتیجهٔ مطلوب است.

درضمن باید خاطرنشان کنیم که اتحاد جالب توجه دیگری شامل تابع ϕ وجود دارد.

قضیهٔ ۷ـ۷ به‌ازای $n > ۱$، مجموع عددهای صحیح مثبت کوچکتر از n و متباین با آن برابر با $\frac{۱}{۲}n\phi(n)$ است. به زبان نمادی

$$\frac{۱}{۲}n\phi(n) = \sum_{\substack{gcd(k,n)=۱ \\ ۱\leq k<n}} k$$

اثبات. فرض می‌کنیم $a_۱$، $a_۲$، ...، $a_{\phi(n)}$ عددهای صحیح مثبتِ کوچکتر از n و متباین با آن باشند. چون $\gcd(a, n) = ۱$ اگر و تنها اگر $\gcd(n - a, n) = ۱$، داریم

$$\begin{aligned} a_۱ + a_۲ + \ldots + a_{\phi(n)} =& (n - a_۱) + (n - a_۲) + \ldots + (n - a_{\phi(n)}) \\ =& \phi(n)n - (a_۱ + a_۲ + \ldots + a_{\phi(n)}) \end{aligned}$$

پس

$$۲(a_۱ + a_۲ + \ldots + a_{\phi(n)}) = \phi(n)n$$

که منجر به نتیجهٔ مطلوب می‌شود. □

مثال ۷ـ۴

حالت $n = ۳۰$ را درنظر می‌گیریم. عددهای صحیح کوچکتر از ۳۰ و متباین با آن، که تعدادشان $\phi(۳۰) = ۸$ است، عبارت‌اند از

$$۱, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹$$

بنابراین

$$۱ + ۷ + ۱۱ + ۱۳ + ۱۷ + ۱۹ + ۲۳ + ۲۹ = ۱۲۰ = \frac{۱}{۲} \times ۳۰ \times ۸$$ ■

اکنون موقعیت مناسبی برای ارائهٔ کاربردی از فرمول وارونسازی موبیوس است.

قضیهٔ ۷ـ۸ به‌ازای هر عدد صحیح مثبت n

$$\phi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$$

اثبات. اثبات به ظاهر آسان است: اگر فرمول وارونسازی را بر

$$F(n) = n = \sum_{d|n}\phi(d)$$

اعمال کنیم، نتیجه می‌شود

$$\phi(n) = \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n}\mu(d)\frac{n}{d} \qquad \square$$

دوباره مثالی به‌ازای $n = ۱۰$ می‌زنیم. به‌آسانی می‌توان دید که

$$\begin{aligned} ۱۰\sum_{d|۱۰}\frac{\mu(d)}{d} &= ۱۰\left(\mu(۱) + \frac{\mu(۲)}{۲} + \frac{\mu(۵)}{۵} + \frac{\mu(۱۰)}{۱۰}\right) \\ &= ۱۰\left(۱ + \frac{-۱}{۲} + \frac{-۱}{۵} + \frac{(-۱)^{۲}}{۱۰}\right) \\ &= ۱۰\left(۱ - \frac{۱}{۲} - \frac{۱}{۵} + \frac{۱}{۱۰}\right) = ۱۰ \times \frac{۲}{۵} = ۴ = \phi(۱۰) \end{aligned}$$

با استفاده از قضیهٔ ۷ـ۸ به‌آسانی می‌توان مقدار تابع فی را به‌ازای هر عدد صحیح مثبت n حساب کرد. فرض می‌کنیم $n = p_۱^{k_۱}p_۲^{k_۲}\dots p_r^{k_r}$ تجزیهٔ n به حاصلضرب توانهای عاملهای اول باشد و حاصلضرب

$$P = \prod_{p_i|n}\left(\mu(۱) + \frac{\mu(p_i)}{p_i} + \dots + \frac{\mu(p_i^{k_i})}{p_i^k}\right)$$

را درنظر می‌گیریم. با اجرای عمل ضرب، مجموعی از جمله‌هایِ به‌صورت

$$\frac{\mu(۱)\mu(p_۱^{a_۱})\mu(p_۲^{a_۲})\dots\mu(p_r^{a_r})}{p_۱^{a_۱}p_۲^{a_۲}\dots p_r^{a_r}}, \qquad ۰ \le a_i \le k_i$$

یا، با توجه به ویژگی ضربی μ، به‌صورت

$$\frac{\mu(p_۱^{a_۱}p_۲^{a_۲}\dots p_r^{a_r})}{p_۱^{a_۱}p_۲^{a_۲}\dots p_r^{a_r}} = \frac{\mu(d)}{d}$$

به‌دست می‌آوریم که در آن $d = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ همهٔ مقسوم‌علیه‌های n را اختیار می‌کند. پس، $P = \sum_{d|n} \frac{\mu(d)}{d}$. از قضیهٔ ۷ـ۸ نتیجه می‌شود که

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p_i|n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} + \ldots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right)$$

ولی اگر $a_i \geq 2$، $\mu(p_i^{a_i}) = 0$. درنتیجه، معادلهٔ فوق به‌صورت سادهٔ

$$\phi(n) = n \prod_{p_i|n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} \right) = n \prod_{p_i|n} \left(1 - \frac{1}{p_i} \right)$$

درمی‌آید، و این با فرمولی که پیشتر به روش متفاوتی ثابت شد، مطابق است. امتیاز این شیوهٔ استدلال عدم‌استفادهٔ آن از سرشت ضربی تابع ϕ است.

تمرینهای ۷ـ۴

۱. ثابت کنید که به‌ازای هر عدد صحیح مثبت n

$$\sum_{d|n} (-1)^{\frac{n}{d}} \phi(d) = \begin{cases} 0 & \text{اگر } n \text{ زوج باشد} \\ -n & \text{اگر } n \text{ فرد باشد} \end{cases}$$

[راهنمایی: اگر N فرد باشد و $n = 2^k N$، آنگاه

$$\sum_{d|n} (-1)^{\frac{n}{d}} \phi(d) = \sum_{d|2^{k-1}N} \phi(d) - \sum_{d|N} \phi(2^k d).]$$

۲. نشان دهید $\sum_{d|36} \phi(d) = 36$ و $\sum_{d|36} (-1)^{\frac{36}{d}} \phi(d) = 0$.

۳. ثابت کنید که به‌ازای هر عدد صحیح مثبت n

$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$$

[راهنمایی: به راهنمایی تمرین ۱ نگاه کنید.]

۴. با استفاده از تمرین ۳ ی بخش ۶ـ۲، اثباتی متفاوت برای

$$n \sum_{d|n} \frac{\mu(d)}{d} = \phi(n)$$

ارائه دهید.

۵. اگر $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ تجزیهٔ عدد صحیح $n > 1$ به عاملهای اول باشد، ثابت کنید

(الف) $$\sum_{d|n} \mu(d)\phi(d) = (2-p_1)(2-p_2)\dots(2-p_r)$$

(ب) $$\sum_{d|n} d\phi(d) = \left(\frac{p_1^{2k_1+1}+1}{p_1+1}\right)\left(\frac{p_2^{2k_2+1}+1}{p_2+1}\right)\dots\left(\frac{p_r^{2k_r+1}+1}{p_r+1}\right)$$

(پ) $$\sum_{d|n} \frac{\phi(d)}{d} = \left(1+\frac{k_1(p_1-1)}{p_1}\right)\left(1+\frac{k_2(p_2-1)}{p_2}\right)\dots\left(1+\frac{k_r(p_r-1)}{p_r}\right)$$

[راهنمایی: در مورد قسمت (الف)، از تمرین ۳ در بخش ۶ـ۲ استفاده کنید.]

۶. ثابت کنید که به‌ازای هر عدد صحیح مثبت n، $\sum_{d=1}^{n} \phi(d)[n/d] = [n(n+1)]/2$.
[راهنمایی: این کاربرد مستقیمی از قضیه‌های ۶ـ۱۱ و ۷ـ۶ است.]

۷. اگر n عددی صحیح و خالی از مربع باشد، ثابت کنید که به‌ازای هر عدد صحیح $k \geq 2$، $\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k$.

۸. نشان دهید که به‌ازای عدد صحیح خالی از مربع $n > 1$، $\tau(n^2) = n$ اگر و تنها اگر $n = 3$.

۹. ثابت کنید که به‌ازای هر عدد صحیح مثبت n، $3|\sigma(3n+2)$ و $4|\sigma(4n+3)$.

۱۰. (الف) نشان دهید که به‌ازای هر $k > 0$، دنباله‌ای چون

$$n+1, n+2, \dots, n+k$$

از k عدد صحیح متوالی وجود دارد به‌طوری که

$$\mu(n+1) = \mu(n+2) = \dots = \mu(n+k) = 0$$

[راهنمایی: دستگاه همنهشتیهای خطی

$$x \equiv -1 \ (\text{به پیمانهٔ } 4) \ , \ x \equiv -2 \ (\text{به پیمانهٔ } 9) \ , \ \dots \ , \ x \equiv -k \ (\text{به پیمانهٔ } p_k^2)$$

را که در آن p_k، k امین عدد اول است، درنظر بگیرید.]

(ب) چهار عدد صحیح مثبت متوالی طوری پیدا کنید که $\mu(n) = 0$.

۱۱. حکمهای زیر را ثابت کنید:

(الف) عدد صحیح مثبت n اول است اگر و تنها اگر $\sigma(n) + \phi(n) = n\tau(n)$. [راهنمایی: نخست ثابت کنید $\sum_{d|n} \sigma(d)\phi(n/d) = n\tau(n)$.]

(ب) عدد صحیح مثبت n اول است اگر و تنها اگر $n - ۱ | \phi(n)$ و نیز $n + ۱ | \sigma(n)$.
[راهنمایی: به تمرین ۱۱ (الف) در بخش ۷ـ۲ نگاه کنید.]

۱۲. اگر $n > ۲$، نابرابری $\phi(n^۲) + \phi((n+۱)^۲) \leq ۲n^۲$ را ثابت کنید.

۱۳. نشان دهید به‌ازای هر عدد صحیح n، دست‌کم یک k وجود دارد به‌طوری که $n | \phi(k)$.

۱۴. نشان دهید که اگر n حاصلضرب دو عدد اول دوقلو باشد، مثلاً $n = p(p+۲)$، آنگاه $\phi(n)\sigma(n) = (n+۱)(n-۳)$.

۱۵. ثابت کنید که $\sum_{d|n} \sigma(d)\phi(n/d) = n\tau(n)$.

۱۶. اگر $a_۱$، $a_۲$، …، $a_{\phi(n)}$ مجموعهٔ تقلیل‌یافته‌ای از مانده‌ها به پیمانهٔ n، $n > ۲$، باشد، نشان دهید

$$a_۱ + a_۲ + \ldots + a_{\phi(n)} \equiv ۰ \quad (\text{به پیمانهٔ } n)$$

۷ـ۵ کاربردی در رمزنگاری

در گذشته، ساخت و کشف کدهای رمزی معمولاً مختص امور نظامی و دیپلوماتیک بوده است. با رواج روزافزون ذخیره‌سازی و انتقال داده‌های رقمی به‌وسیلهٔ سیستمهای داده‌پردازی الکترونیک، سازمانها در هر دو بخش خصوصی و عمومی احساس کرده‌اند که لازم است اطلاعات را از دست مخاطبان ناخواسته حفظ کرد. درواقع، رواج گستردهٔ انتقال وجوه از طریق الکترونیک، پنهانکاری را در بیشتر معامله‌های مالی ضروری ساخته است. این است که اخیراً علاقهٔ ریاضیدانان و دانشمندان علوم کامپیوتر به رمزنگاری، یعنی علم مبادلهٔ پیام به روشی که برای افراد غیرمجاز نامفهوم باشد، جلب شده است. رمزنگاری تنها وسیلهٔ عملی موجود برای حفظ اطلاعات ارسال شده از طریق شبکه‌های ارتباطی عمومی، مانند خطهای تلفن، مایکروویو یا ماهواره‌ها، است.

به زبان رمزنگاری، کدها رمز نامیده می‌شوند؛ اطلاعی که قرار است مخفی بماند، قبل از آنکه به رمز درآید، متن آشکار خوانده می‌شود و پس از آن، متن رمزی نامیده می‌شود. فرایند تبدیل متن آشکار به متن رمزی، رمزی‌سازی یا به‌رمز درآوردن و فرایند عکس، یعنی تبدیل متن رمزی به متن آشکار، رمزگشایی نامیده می‌شود.

یکی از نخستین سیستمهای رمزنگاری، در حدود ۵۰ سال پیش از میلاد مسیح، توسط ژولیوس سزار، امپراطور بزرگ رم، به‌کار رفت. وی با استفاده از یک شیوهٔ جایگزینی ابتدایی با سیسرون مکاتبه می‌کرد. در این سیستم، به‌جای X حرف A، به‌جای Y حرف B، به‌جای Z حرف C و به‌جای هر حرف دیگر الفبا حرف سوم بعد از آن گذاشته می‌شد. اگر متن رمزی متناظر را حرف به حرف زیر

متن آشکار بنویسیم، الفبای جایگزینی در رمز سزار به‌دست می‌آید:

متن آشکار:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
متن رمزی:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

به‌عنوان مثال، متن آشکار

CAESAR WAS GREAT (۱)

به متن رمزی

FDHVDU ZDV JUHDV (۲)

تبدیل می‌شود. رمز سزار را می‌توان به‌آسانی با استفاده از نظریهٔ همنهشتی توصیف کرد. نخست هر متن آشکار، تحت تناظری به‌صورت زیر، با ترجمهٔ حرفهای متن به عددها به‌طور عددی بیان می‌شود:

A	B	C	D	E	F	G	H	I	J	K	L	M
۰۱	۰۲	۰۳	۰۴	۰۵	۰۶	۰۷	۰۸	۰۹	۱۰	۱۱	۱۲	۱۳
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶

اگر P متناظر عددیِ حرفی از متن آشکار و C متناظر عددیِ حرفی از متن رمزی باشد، آنگاه

$$C \equiv P + ۳ \text{ (به پیمانهٔ ۲۶)}$$

بنابراین، به‌عنوان نمونه، ترجمهٔ حرفهای پیام (۱) به متناظرهایشان چنین است

(۳) ۰۳ ۰۱ ۰۵ ۱۹ ۰۱ ۱۸ ۲۳ ۰۱ ۱۹ ۰۷ ۱۸ ۰۵ ۰۱ ۲۰

با استفاده از همنهشتی (به پیمانهٔ ۲۶) $C \equiv P + ۳$، (۳) تبدیل به متن رمزی

(۴) ۰۶ ۰۴ ۰۸ ۲۲ ۰۴ ۲۱ ۲۶ ۰۴ ۲۲ ۱۰ ۲۱ ۰۸ ۰۴ ۲۳

می‌شود. برای بازیابی متن آشکار به‌آسانی می‌توان فرایند را با استفاده از همنهشتی

$$P \equiv C - ۳ \equiv C + ۲۳ \text{ (به پیمانهٔ ۲۶)}$$

معکوس کرد. رمز سزار بسیار ساده و بنابراین ایمنی آن فوق‌العاده کم است. خود سزار پس از چندی این رمز را کنار گذاشت، نه‌تنها به‌دلیل ناامن بودنش، بلکه همچنین به‌دلیل عدم اعتماد سزار به سیسرون که بالاجبار از این رمز آگاه بود.

در سیستمهای رمزنگاری متعارف، مانند سیستم سزار، فرستنده و گیرنده دارای کلید رمز مشترکی هستند. فرستنده از این کلید برای رمزی‌سازی متن آشکار ارسالی استفاده می‌کند و گیرنده برای رمزگشایی متن رمزی دریافتی. فرق رمزنگاری به‌وسیلهٔ کلید همگانی با رمزنگاری متعارف در این است که در آن از دو کلید رمزی‌سازی و رمزگشایی استفاده می‌شود. گرچه این دو کلید عکس یکدیگر عمل می‌کنند و بنابراین باهم مرتبط‌اند، روش آسانی برای به‌دست‌آوردن کلید رمزگشایی از کلید رمزی‌سازی وجود ندارد. بنابراین، کلید رمزی‌سازی را می‌توان همگانی کرد بی‌آنکه کلید رمزگشایی در اختیار عموم قرار گرفته باشد؛ هر استفاده‌کننده‌ای می‌تواند پیامها را به رمز درآورد، ولی فقط گیرندهٔ موردنظر (که کلید رمزگشایی او سرّی نگاه داشته می‌شود) می‌تواند آنها را کشف کند. امتیاز عمدهٔ سیستم کلید همگانی این است که در آن نیازی به مبادلهٔ کلید میان فرستنده و گیرنده پیش از تصمیم به برقراری ارتباط نیست.

در ۱۹۷۷، ریوست[1]، شامیر[2]، و ادلمن[3] یک سیستم رمزنگاری با کلید همگانی ابداع کردند که در آن فقط از مفهومهای مقدماتی نظریهٔ اعداد استفاده می‌شود. این سیستم رمزنگاری RSA نامیده می‌شود که از نخستین حرف نامهای خانوادگی ابداع‌کنندگان الگوریتم آن گرفته شده است. امنیت آن بر این فرض استوار است که در وضعیت فعلی تکنولوژی کامپیوتر، تجزیهٔ عددهای مرکبی که عاملهای اول بزرگ دارند، به زمانی فوق‌العاده زیاد نیازمند است.

هر فردی که از سیستم RSA استفاده می‌کند، زوجی از عددهای اول متمایز به اندازهٔ کافی بزرگ مانند p و q انتخاب می‌کند که تجزیهٔ حاصلضرب آنها، یعنی $n = pq$، موسوم به پیمانهٔ رمزی‌سازی، فراتر از توان کامپیوترهای فعلی باشد. به‌عنوان مثال، اگر هریک از p و q عددی ۲۰۰ رقمی انتخاب شود، n کم‌وبیش دارای ۴۰۰ رقم خواهد بود. پس از انتخاب n، استفاده‌کننده عدد صحیح مثبت kای موسوم به نمای رمزی‌سازی را با ضابطهٔ $\gcd(k, \phi(n)) = ۱$، به تصادف انتخاب می‌کند. سپس زوج (n, k) به‌عنوان کلید رمزی‌سازی شخصی استفاده‌کننده در پرونده‌ای عمومی، مشابه راهنمای تلفن، نگاه داشته می‌شود. به این ترتیب هر عضو شبکهٔ ارتباطی می‌تواند

1. R. Rivest　　2. A. Shamir　　3. L. Adleman

پیام مورد نظر خود را رمزی‌سازی و ارسال کند. خاطرنشان می‌کنیم که گرچه n سرّی نیست، در راهنمای کلید همگانی ذکری از عاملهای اول p و q ی n به بیان نمی‌آید.

فرایند رمزی‌سازی با تبدیل پیام ارسالی به عدد صحیح M ای آغاز می‌شود و این کار به کمک یک «الفبای عددی» صورت می‌پذیرد، به این ترتیب که به‌جای هر حرف، عدد، یا علامت سجاوندیِ متن آشکار، یک عدد صحیح دورقمی قرار می‌گیرد. یکی از جایگزینیهای متعارف به این صورت است:

A = ۰۱	K = ۱۱	U = ۲۱	۱ = ۳۱
B = ۰۲	L = ۱۲	V = ۲۲	۲ = ۳۲
C = ۰۳	M = ۱۳	W = ۲۳	۳ = ۳۳
D = ۰۴	N = ۱۴	X = ۲۴	۴ = ۳۴
E = ۰۵	O = ۱۵	Y = ۲۵	۵ = ۳۵
F = ۰۶	P = ۱۶	Z = ۲۶	۶ = ۳۶
G = ۰۷	Q = ۱۷	, = ۲۷	۷ = ۳۷
H = ۰۸	R = ۱۸	. = ۲۸	۸ = ۳۸
I = ۰۹	S = ۱۹	? = ۲۹	۹ = ۳۹
J = ۱۰	T = ۲۰	۰ = ۳۰	! = ۴۰

۰۰ به‌معنی یک فاصله میان کلمه‌هاست. با این فرایند، پیام

$$The\ brown\ fox\ is\ quick$$

به دنبالهٔ عددی

$$M = ۲۰۰۸۰۵۰۰۰۰۲۱۸۱۵۲۳۱۴۰۰۰۰۶۱۵۲۴۰۰۰۰۹۰۹۰۰۱۷۲۱۰۹۰۳۱۱۲۸$$

تبدیل می‌شود. فرض بر این است که M، یعنی عدد متن آشکار، کوچکتر از n، یعنی پیمانهٔ رمزی‌سازی است. اگر چنین نباشد، تشخیص M از هر عدد صحیح بزرگترِ همنهشت با آن به پیمانهٔ n، غیرممکن است. اگر پیام به اندازه‌ای طویل باشد که قابل تبدیل به عدد M ای، $M < n$، نباشد، می‌توان M را به چند تکهٔ عددی M_1، M_2، ...، M_r با اندازه‌های مناسب تقسیم کرد. هر تکه، جداگانه به رمز درآورده می‌شود.

فرستنده، کلید (n, k) ی رمزی‌سازی گیرندهٔ موردنظر را از راهنمای عمومی پیدا می‌کند، عدد متن آشکار یعنی M را به عدد متن رمزی یعنی r تبدیل می‌کند به این ترتیب که M را به توان k

می‌رساند و M^k را به پیمانهٔ n تحویل می‌کند؛ یعنی

$$M^k \equiv r \ (\text{به پیمانهٔ } n)$$

هر پیام ۲۰۰ نمادی را با کامپیوتری سریع می‌توان در عرض چند ثانیه به رمز درآورد. خاطرنشان می‌کنیم که نمای kی رمزی‌سازی همگانی طوری انتخاب می‌شود که $\gcd(k, \phi(n)) = ۱$. هرچند برای k عددهای مناسب متعددی را می‌توان انتخاب کرد، ساده‌ترین کار این است که عامل اولی از $\phi(n) + ۱$ انتخاب شود.

در آن‌سوی خط، دریافت‌کنندهٔ مجاز، برای رمزگشایی اطلاع منتقل‌شده نخست عدد صحیح j موسوم به نمای بازیافت سرّی را که در

$$kj \equiv ۱ \ (\text{به پیمانهٔ } \phi(n))$$

صادق است، تعیین می‌کند. چون $\gcd(k, \phi(n)) = ۱$ ، این همنهشتی خطی جواب یکتایی به پیمانهٔ $\phi(n)$ دارد. درواقع، j را مستقیماً می‌توان از

$$j \equiv k^{\phi(\phi(n))-۱} \ (\text{به پیمانهٔ } n)$$

به‌دست آورد، زیرا با استفاده از قضیهٔ اویلر بیدرنگ نتیجه می‌شود

$$kj \equiv k^{\phi(\phi(n))} \equiv ۱ \ (\text{به پیمانهٔ } \phi(n))$$

نمای بازیافت را فقط فردی می‌تواند محاسبه کند که هم از k و هم از $\phi(n) = (p-۱)(q-۱)$ مطلع باشد، و بنابراین عاملهای اول n یعنی p و q را بشناسد. بنابراین، شخص ثالث غیرمجازی که اطلاعش محدود به کلید همگانی (n, k) است، از j آگاه نیست.

سیستم به‌نحوی طراحی شده است که حال گیرنده می‌تواند فقط با محاسبهٔ r^j به پیمانهٔ n، M را از r به‌دست آورد. چون به‌ازای عدد صحیح t ای، $kj = ۱ + \phi(n)t$، نتیجه می‌شود که اگر $\gcd(M, n) = ۱$

$$\begin{aligned} r^j &\equiv (M^k)^j \equiv M^{۱+\phi(n)t} \\ &\equiv M(M^{\phi(n)})^t \equiv M \times ۱^t \equiv M \ (\text{به پیمانهٔ } n) \end{aligned}$$

به بیان دیگر، به توان j رسانیدن عدد متن رمزی و تحویل آن به پیمانهٔ n، عدد M متن آشکار را به‌دست می‌دهد.

فرض $\gcd(M,n) = ۱$ به این منظور اتخاذ شد که از قضیهٔ اویلر استفاده شود. در حالت غیرمحتملی که M و n متباین نباشند، می‌توان با استدلال مشابهی نشان داد که(به پیمانهٔ p) $r^j \equiv M$ و (به پیمانهٔ q) $r^j \equiv M$، و بنابراین همنهشتی مطلوب (به پیمانهٔ n) $r^j \equiv M$ نتیجه می‌شود. از تفصیل موضوع صرف‌نظر می‌کنیم.

امتیاز بزرگ این فرایند مبتکرانه در این است که رمزی‌سازی پیام نیازی به آگاهی از دو عدد اول p و q ندارد، و اطلاع از حاصلضرب آنها، یعنی n، کافی است؛ نیازی نیست که هیچ‌کسی جز دریافت‌کنندهٔ پیام از عاملهای اولِ حیاتی در فرایند رمزگشایی مطلع باشد.

مثال ۷ـ۵

برای اینکه خواننده با الگوریتم کلید همگانی RSA آشنایی پیدا کند، مثالی می‌زنیم و آن را به تفصیل بررسی می‌کنیم. به‌منظور سادگی مثال، نخست دو عدد اول

$$q = ۵۳ \text{،} p = ۲۹$$

را انتخاب می‌کنیم که البته در واقعیت عددهایی به این کوچکی اختیار نمی‌شوند. در عمل، p و q به اندازهٔ کافی بزرگ انتخاب می‌شوند تا تجزیهٔ عدد غیرسرّی $n = pq$ عملی نباشد. در مثال ما، پیمانهٔ رمزی‌سازی برابر با $n = ۲۹ \times ۵۳ = ۱۵۳۷$ است و

$$\phi(n) + ۱ = ۵۲ \times ۲۸ + ۱ = ۱۴۵۷ = ۳۱ \times ۴۷$$

فرض می‌کنیم نمای رمزی‌سازیِ $k = ۴۷$ انتخاب شده باشد. در این صورت نمای بازیافت، یعنی عدد صحیح یکتای jای که در همنهشتی (به پیمانهٔ $(\phi(n)$) $kj \equiv ۱$ صدق می‌کند، $j = ۳۱$ است. برای رمزی‌سازیِ

NO WAY

نخست به‌جای هر حرف، طبق جایگزینیِ پیشگفته، هم‌ارز عددی آن را قرار می‌دهیم؛ به این ترتیب عدد متن آشکار، یعنی

$$M = ۱۴۱۵۰۰۲۳۰۱۲۵$$

به‌دست می‌آید. می‌خواهیم هر تکه از متن آشکار عددصحیحی کوچکتر از ۱۵۳۷ باشد. با توجه به این محدودیت معقول به‌نظر می‌رسد که، M را به تکه‌های سه‌رقمی تقسیم کنیم. نخستین تکه ۱۴۱ است، و به‌صورت عدد متن رمزی

$$۱۴۱^{۴۷} \equiv ۶۵۸ \text{ (به پیمانهٔ ۱۵۳۷)}$$

به رمز درمی‌آید. اینها نخستین رقمهای انتقال سرّی است. در آن‌سوی خط، گیرندهٔ مجاز با علم به اینکه نمای بازیافت $j = ۳۱$ است، با محاسبهٔ

$$۶۵۸^{۳۱} \equiv ۱۴۱ \text{ (به پیمانهٔ ۱۵۳۷)}$$

شروع به بازیافت عدد متن آشکار می‌کند. کل متن رمزی پیام ما عبارت است از

$$۰۶۵۸ \quad ۱۴۰۸ \quad ۱۲۵۰ \quad ۱۲۵۲$$

برای اینکه سیستم رمز RSA ایمنی داشته باشد نباید بازیافت M، عدد متن آشکار، با استفاده از اطلاعی که شخص ثالث می‌تواند داشته باشد یعنی کلید همگانی (n, k)، از نظر محاسباتی عملی باشد. روش مستقیم کشف رمز، تلاش برای تجزیهٔ n است که عدد صحیح فوق‌العاده بزرگی است؛ زیرا همین که عاملها تعیین شدند، نمای بازیافت j با استفاده از $\phi(n) = (p - ۱)(q - ۱)$ و k قابل‌محاسبه خواهد بود. اعتماد ما به سیستم RSA مبتنی است بر مدت زمان مورد نیاز کامپیوتر برای تجزیهٔ حاصلضرب دو عدد اول بزرگ، که «زمان اجرا» نامیده می‌شود. از دیدگاه محاسباتی، تجزیه کردن مشکلتر از تشخیص عددهای اول از عددهای مرکب است. امروزه با سریعترین کامپیوترها، اول بودن عددی ۲۰۰ رقمی را می‌توان به‌طور عادی در کمتر از ۱۰ دقیقه مشخص کرد، در صورتی که، زمان لازم برای تجزیهٔ عددی مرکب به همان بزرگی فوق‌العاده زیاد است. تخمین زده شده است که سریعترین الگوریتم تجزیهٔ موجود کم‌وبیش به $(۱٫۲)۱۰^{۲۳}$ عمل کامپیوتری برای تجزیهٔ یک عدد صحیح ۲۰۰ رقمی به عاملهای اول نیازمند است؛ به فرض اینکه هر عملی یک میکروثانیه ($۱۰^{-۶}$ ثانیه) طول بکشد، عمل تجزیه حدود $(۳٫۸)۱۰^{۹}$ سال طول خواهد کشید. به‌شرط نامحدود بودن زمان محاسبه و موجود بودن الگوریتم تجزیه‌ای با کارایی غیرقابل‌تصور، سیستم رمز RSA قابل‌کشف است، ولی در حال حاضر کاملاً ایمن به‌نظر می‌رسد. ■

تمرین ۷ـ۵

۱. پیام $RETURN\ HOME$ را با استفاده از رمز سزار به رمز درآورید.

۲. اگر رمز سزار، $KDSSB\ ELUWKGDB$ را تولید کرد، متن آشکار پیام چیست؟

۳. (الف) یک رمز خطی با همنهشتی $C \equiv aP + b$ (به پیمانهٔ ۲۶) تعریف می‌شود که در آن a و b عددهایی صحیح‌اند و $\gcd(a, ۲۶) = ۱$. نشان دهید که همنهشتی رمزگشایی متناظر به‌صورت $P \equiv a'(C - b)$ (به پیمانهٔ ۲۶) است که در آن، عدد صحیح a' در $aa' \equiv ۱$ (به پیمانهٔ ۲۶) صدق می‌کند.

(ب) با استفاده از رمز خطی (به پیمانهٔ ۲۶) $C \equiv ۵P + ۱۱$، پیام *NUMBER THEORY IS EASY* را به رمز درآورید.

(پ) پیام *TZSVIW JQBVMIJ HL MVOOVI* را، که با استفاده از رمز خطی (به پیمانهٔ ۲۶) $C \equiv ۳p + ۷$ تولید شده است، رمزگشایی کنید.

۴. اگر $n = pq = ۲۷۴۲۷۹$ و $\phi(n) = ۲۷۲۳۷۶$، عددهای اول p و q را پیدا کنید [راهنمایی: توجه کنید که

$$p + q = n - \phi(n) + ۱$$

$$p - q = [(p + q)^۲ - ۴n]^{۱/۲}$$

۵. اگر الگوریتم RSA مبتنی بر کلید $(n, k) = (۳۲۳۳, ۳۷)$ باشد، نمای بازیافت سیستم رمزنگاری چیست؟

۶. با استفاده از الگوریتم RSA با کلید $(n, k) = (۲۴۱۹, ۳)$، پیام *GOLD MEDAL* را به رمز درآورید.

۷. متن رمزی تولیدشده به‌وسیلهٔ الگوریتم RSA با کلید $(n, k) = (۱۶۴۳, ۲۲۳)$ عبارت است از

۱۴۵۱ ۰۱۰۳ ۱۲۶۳ ۰۵۶۰ ۰۱۲۷ ۰۸۹۷

پیام متن آشکار اصلی را تعیین کنید. [راهنمایی: نمای بازیافت $j = ۷$ است.]

۸. متن رمزی

۱۰۳۷ ۰۴۳۱ ۰۶۲۹ ۰۶۹۰ ۰۲۰۴ ۲۲۶۷ ۰۵۹۵

را که با استفاده از الگوریتم RSA با کلید $(n, k) = (۲۴۱۹, ۲۱۱)$ به رمز درآورده شده است، رمزگشایی کنید. [راهنمایی: نمای بازیافت ۱۱ است.]

۸

ریشه‌های اولیه و اندیسها

«... اثبات ریاضی مانند الماس قاطع و شفاف است، و با چیزی جز استدلال دقیق نمی‌توان به آن رسید.»

جان لاک

۸ـ۱ مرتبهٔ عدد صحیح به پیمانهٔ n

با توجه به قضیهٔ اویلر، می‌دانیم که اگر $\gcd(a,n) = ۱$، آنگاه (به پیمانهٔ n) $a^{\phi(n)} \equiv ۱$. ولی اغلب توانهاییِ از a کوچکتر از $a^{\phi(n)}$ وجود دارند که به پیمانهٔ n با ۱ همنهشت‌اند. این نکته توجیهی برای تعریف زیر است:

تعریف ۸ـ۱ اگر $n > ۱$ و $\gcd(a,n) = ۱$، آنگاه کوچکترین عدد صحیح مثبت k به‌طوری که (به پیمانهٔ n) $a^k \equiv ۱$، مرتبهٔ a به پیمانهٔ n (یا طبق اصطلاح قدیم: نمایی که a به توان آن به پیمانهٔ n متعلق است) نامیده می‌شود.

توانهای متوالی ۲ به پیمانهٔ ۷ را درنظر می‌گیریم. به‌ازای این پیمانه همنهشتیهای

$$۲^۱ \equiv ۲, ۲^۲ \equiv ۴, ۲^۳ \equiv ۱, ۲^۴ \equiv ۲, ۲^۵ \equiv ۴, ۲^۶ \equiv ۱, \ldots$$

را به‌دست می‌آوریم، که معلوم می‌کند مرتبهٔ عدد صحیح ۲ به پیمانهٔ ۷ برابر ۳ است.

توجه کنید که اگر دو عدد صحیح همنهشت به پیمانهٔ n باشند، مرتبه‌های یکسانی به پیمانهٔ n دارند. زیرا اگر (به پیمانهٔ n) $a \equiv b$ و (به پیمانهٔ n) $a^k \equiv ۱$، بنابه قضیهٔ ۴ـ۲، (به پیمانهٔ n) $a^k \equiv b^k$، و بنابراین (به پیمانهٔ n) $b^k \equiv ۱$.

تأکید می‌کنیم که تعریف ما از مرتبه به پیمانهٔ n فقط ناظر به عددهای صحیح a ای است که $\gcd(a,n) = ۱$. در واقع، اگر $\gcd(a,n) > ۱$، می‌دانیم که بنابه قضیهٔ ۴ـ۷، همنهشتی خطی (به پیمانهٔ n) $ax \equiv ۱$ جواب ندارد؛ پس، رابطهٔ

$$a^k \equiv ۱ \ (\text{به پیمانهٔ } n)، \qquad k \geq ۱$$

نمی‌تواند برقرار باشد، در آن صورت لازم می‌آید $x = a^{k-۱}$ جوابی از (به پیمانهٔ n) $ax \equiv ۱$ باشد. بنابراین، وقتی صحبت از مرتبهٔ a به پیمانهٔ n به‌میان می‌آید، فرض بر این است که $\gcd(a,n) = ۱$، هرچند این موضوع تصریح نشده باشد.

در مثال بالا وقتی داریم (به پیمانهٔ ۷) $۲^k \equiv ۱$ که k مضربی از ۳، یعنی مرتبهٔ ۲ به پیمانهٔ ۷، باشد. قضیهٔ زیر نشان می‌دهد که در حالت کلی نیز چنین است.

قضیهٔ ۸ـ۱ فرض می‌کنیم عدد صحیح a دارای مرتبهٔ k به پیمانهٔ n باشد. در این‌صورت (به پیمانهٔ n) $a^h \equiv ۱$ اگر تنها و اگر $k|h$؛ به‌ویژه، $k|\phi(n)$.

اثبات. فرض می‌کنیم $k|h$، یعنی به‌ازای عدد صحیح j ای، $h = jk$. چون (به پیمانهٔ n) $a^k \equiv ۱$، بنابه قضیهٔ ۴ـ۲، (به پیمانهٔ n) $(a^k)^j \equiv ۱^j$، یا (به پیمانهٔ n) $a^h \equiv ۱$.

برعکس، فرض می‌کنیم h عدد صحیح مثبت دلخواهی است که در (به پیمانهٔ n) $a^h \equiv ۱$ صدق می‌کند. بنابه الگوریتم تقسیم، q و r ای وجود دارند به‌طوری که $h = qk + r$، $۰ \leq r < k$. درنتیجه

$$a^h = a^{qk+r} = (a^k)^q a^r$$

بنابه فرض، هم (به پیمانهٔ n) $a^h \equiv ۱$ و هم (به پیمانهٔ n) $a^k \equiv ۱$، که درنتیجه، (به پیمانهٔ n) $a^r \equiv ۱$. چون $۰ \leq r < k$، بالاخره به $r = ۰$ می‌رسیم وگرنه انتخاب k به‌عنوان کوچکترین عدد صحیح مثبت k ای که (به پیمانهٔ n) $a^k \equiv ۱$، دچار تناقض می‌شود. پس $h = qk$ و $k|h$. □

قضیهٔ ۸ـ۱ محاسبهٔ لازم برای تعیین مرتبهٔ عدد صحیح a به پیمانهٔ n را کوتاه می‌کند: به‌جای آزمودن همهٔ توانهای a، نماها را می‌توان به مقسوم‌علیه‌های $\phi(n)$ محدود کرد. به‌عنوان مثال، مرتبهٔ ۲ به پیمانهٔ ۱۳ را حساب می‌کنیم. چون $\phi(۱۳) = ۱۲$، مرتبهٔ ۲ باید یکی از عددهای صحیح ۱، ۲، ۳، ۴، ۶ و ۱۲ باشد. با توجه به

$$۲^۲ \equiv ۴,\ ۲^۳ \equiv ۸,\ ۲^۴ \equiv ۳,\ ۲^۶ \equiv ۱۲,\ ۲^{۱۲} \equiv ۱ \ (\text{به پیمانهٔ}۱۳)$$

معلوم می‌شود که مرتبهٔ ۲ به پیمانهٔ ۱۳ برابر ۱۲ است.

به‌ازای هر مقسوم علیه d از $\phi(n)$ همیشه عدد صحیح a ای که دارای مرتبهٔ d به پیمانهٔ n باشد وجود ندارد. به‌عنوان مثال، $n = ۱۲$ را درنظر می‌گیریم. گرچه $\phi(۱۲) = ۴$، عدد صحیح مرتبهٔ ۴ ای به پیمانهٔ ۱۲ وجود ندارد؛ در واقع ملاحظه می‌کنیم که

$$۱^۲ \equiv ۵^۲ \equiv ۷^۲ \equiv ۱۱^۲ \equiv ۱ \ (\text{به پیمانهٔ}۱۲)$$

و بنابراین تنها مرتبهٔ انتخابی می‌تواند ۱ یا ۲ باشد.

اکنون قضیهٔ اساسی دیگری دربارهٔ مرتبهٔ عدد صحیح ارائه می‌دهیم.

قضیهٔ ۸ـ۲ اگر مرتبهٔ a به پیمانهٔ n برابر k باشد، آنگاه $a^i \equiv a^j$ (به پیمانهٔ n) اگر و تنها اگر $i \equiv j$ (به پیمانهٔ k).

اثبات. نخست فرض می‌کنیم $a^i \equiv a^j$ (به پیمانهٔ n) و $i \geq j$. چون a با n متباین است، می‌توانیم با حذف توانی از a به $a^{i-j} \equiv ۱$ (به پیمانهٔ n) برسیم. بنابه قضیهٔ ۸ـ۱، همنهشتی اخیر وقتی برقرار است که $k|i-j$ و این دقیقاً معادل است با $i \equiv j$ (به پیمانهٔ k).

برعکس فرض می‌کنیم $i \equiv j$ (به پیمانهٔ k). در این صورت به‌ازای عدد صحیح qای، $i = j + qk$. بنابه تعریف k، $a^k \equiv ۱$ (به پیمانهٔ n). پس

$$a^i \equiv a^{j+qk} = a^j(a^k)^q \equiv a^j \ (\text{به پیمانهٔ } n)$$

که نتیجهٔ مطلوب است. □

فرع. اگر مرتبهٔ a به پیمانهٔ n برابر k باشد، آنگاه عددهای صحیح a، $a^۲$، ...، a^k ناهمنهشت به پیمانهٔ n اند.

اثبات. اگر $1 \le i \le j \le k$ و $a^i \equiv a^j$ (به پیمانهٔ n)، آنگاه قضیه تضمین می‌کند که $i \equiv j$ (به پیمانهٔ k). ولی این غیرممکن است مگر اینکه $i = j$. □

در اینجا پرسشی نسبتاً طبیعی مطرح می‌شود: آیا می‌توان مرتبهٔ هر توان صحیحی از a را برحسب مرتبهٔ a بیان کرد؟ پاسخ در قضیهٔ زیر می‌آید.

قضیهٔ ۸ـ۳ اگر مرتبهٔ عدد صحیح a به پیمانهٔ n برابر k باشد و $h > 0$، آنگاه مرتبهٔ a^h به پیمانهٔ n برابر $k/\gcd(h,k)$ است.

اثبات. فرض می‌کنیم $d = \gcd(h,k)$. در این صورت می‌توانیم بنویسیم $h = h_1 d$ و $k = k_1 d$ و بنابراین $\gcd(h_1, k_1) = 1$. واضح است که

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \ (\text{به پیمانهٔ } n)$$

اگر فرض کنیم مرتبهٔ a^h به‌پیمانهٔ n برابر r است، آنگاه بنابه قضیهٔ ۸ـ۱، $r | k_1$. از سوی دیگر، چون مرتبهٔ a به پیمانهٔ n برابر k است، از همنهشتی

$$a^{hr} \equiv (a^h)^r \equiv 1 \ (\text{به پیمانهٔ } n)$$

نتیجه می‌شود $k | hr$؛ به بیان دیگر، $k_1 d | h_1 dr$ یا $k_1 | h_1 r$. ولی $\gcd(k_1, h_1) = 1$ و بنابراین $k_1 | r$. با تلفیق این رابطه بخشپذیری با رابطهٔ به‌دست آمدهٔ قبلی، حکم ثابت می‌شود:

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h,k)}$$ □

این قضیه دارای فرعی است که اثبات آن به خواننده محول می‌شود.

فرع. فرض می‌کنیم مرتبهٔ a به پیمانهٔ n برابر k باشد. در این صورت مرتبهٔ a^h به پیمانهٔ n نیز k است اگر و تنها اگر $\gcd(h,k) = 1$.

اکنون ببینیم این مطالب چگونه در یک مثال خاص به‌کار می‌آیند.

مثال ۸ـ۱

جدول زیر مرتبه‌های عددهای صحیح کوچکتر از ۱۳ به پیمانهٔ ۱۳ را نشان می‌دهد

عددصحیح	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
مرتبه	۱	۱۲	۳	۶	۴	۱۲	۱۲	۴	۳	۶	۱۲	۲

ملاحظه می‌کنیم که مرتبهٔ ۲ به پیمانهٔ ۱۳ برابر ۱۲ است، در صورتی که مرتبه‌های $۲^۲$ و $۲^۳$ به پیمانهٔ ۱۳، به‌ترتیب، ۶ و ۴ است؛ به آسانی می‌توان تحقیق کرد که طبق قضیهٔ ۸ـ۳ داریم

$$۶ = \frac{۱۲}{\gcd(۲, ۱۲)} \quad و \quad ۴ = \frac{۱۲}{\gcd(۳, ۱۲)}$$

عددهای صحیح دیگری که مرتبهٔ آنها نیز به پیمانهٔ ۱۳ برابر ۱۲ است توانهای ۲^kای هستند که $\gcd(k, ۱۲) = ۱$؛ یعنی

$$۲^۵ \equiv ۶, ۲^۷ \equiv ۱۱, ۲^{۱۱} \equiv ۷ \ (\text{به پیمانهٔ} ۱۳)$$

عدد صحیح a «ریشهٔ اولیه» ای از n نامیده می‌شود اگر a بزرگترین مرتبهٔ ممکن را داشته باشد. ■

تعریف ۸ـ۲ اگر $\gcd(a, n) = ۱$ و مرتبهٔ a به پیمانهٔ n برابر $\phi(n)$ باشد، آنگاه a ریشهٔ اولیه‌ای از n نامیده می‌شود.

به بیان دیگر، a ریشهٔ اولیه‌ای از n است اگر $a^{\phi(n)} \equiv ۱ \ (\text{به پیمانهٔ} n)$، ولی به‌ازای هر عدد صحیح مثبت $k < \phi(n)$، $a^k \not\equiv ۱ \ (\text{به پیمانهٔ } n)$.

به آسانی می‌توان ملاحظه کرد که ۳ ریشهٔ اولیه‌ای از ۷ است زیرا

$$۳^۱ \equiv ۳, ۳^۲ \equiv ۲, ۳^۳ \equiv ۶, ۳^۴ \equiv ۴, ۳^۵ \equiv ۵, ۳^۶ \equiv ۱ \ (\text{به پیمانهٔ } ۷)$$

به‌طور کلیتر، می‌توان این نتیجهٔ اساسی را ثابت کرد که، ریشه‌های اولیه به‌ازای هر پیمانهٔ اول وجود دارند. گرچه ممکن است عدد غیر اول دارای ریشهٔ اولیه باشد (به‌عنوان مثال، ۲ ریشهٔ اولیه‌ای از ۹ است)، دلیلی وجود ندارد که انتظار داشته باشیم هر عدد صحیح n، ریشهٔ اولیه داشته باشد. در واقع، وجود ریشه‌های اولیه بیشتر استثناست تا قاعده.

مثال ۸ـ۲

نشان دهید که اگر $F_n = ۲^{۲^n} + ۱$، $n > ۱$، عددی اول باشد، آنگاه ۲ ریشهٔ اولیه‌ای از F_n نیست. (۲ به‌وضوح ریشهٔ اولیه‌ای از $F_۱ = ۵$ است.) چون $۲^{۲^{n+۱}} - ۱ = (۲^{۲^n} + ۱)(۲^{۲^n} - ۱)$ داریم

$$۲^{۲^{n+۱}} \equiv ۱ \ (\text{به پیمانهٔ} F_n)$$

که از آن نتیجه می‌شود مرتبهٔ ۲ به پیمانهٔ F_n بیشتر از $۲^{n+۱}$ نیست. ولی اگر فرض کنیم F_n عددی اول است، داریم

$$\phi(F_n) = F_n - ۱ = ۲^{۲^n}$$

و استدلال استقرایی مستقیمی نشان می‌دهد که اگر $n > ۱$ آنگاه $۲^{۲^n} > ۲^{n+۱}$. بنابراین مرتبهٔ ۲ به پیمانهٔ F_n کوچکتر از $\phi(F_n)$ است؛ عطف به تعریف ۸ـ۲، ملاحظه می‌کنیم که ۲ نمی‌تواند ریشهٔ اولیه‌ای از F_n باشد. ■

یکی از خاصیتهای برجستهٔ ریشه‌های اولیه در قضیهٔ زیر نهفته است.

قضیهٔ ۸ـ۴ فرض می‌کنیم $\gcd(a, n) = ۱$ و $a_۱$، $a_۲$، ...، $a_{\phi(n)}$ عددهای صحیح مثبت کوچکتر از n و متباین با آن باشند. اگر a ریشهٔ اولیه‌ای از n باشد، آنگاه هریک از عددهای

$$a, a^۲, \ldots, a^{\phi(n)}$$

با یکی از عددهای $a_۱$، $a_۲$، ...، $a_{\phi(n)}$ همنهشت به پیمانهٔ n است.

اثبات. چون a با n متباین است، همهٔ توانهای a نیز با n متباین‌اند؛ پس، هر a^k همنهشت با یکی از a_iها به پیمانهٔ n است. بنابه فرع قضیهٔ ۸ـ۲، $\phi(n)$ عدد متعلق به مجموعهٔ $\{a, a^۲, \ldots, a^{\phi(n)}\}$ ناهمنهشت‌اند، پس این عددها نشان‌دهندهٔ عددهای صحیح $a_۱$، $a_۲$، ...، $a_{\phi(n)}$، نه لزوماً به‌ترتیب نشان داده شده، هستند. □

یکی از نتیجه‌های مطلبی که هم‌اکنون ثابت شد این است که، در حالتهایی که ریشهٔ اولیه‌ای وجود دارد، می‌توانیم تعداد دقیق این ریشه‌ها را تعیین کنیم.

فرع. اگر n ریشهٔ اولیه‌ای داشته باشد، آنگاه n دقیقاً دارای $\phi(\phi(n))$ ریشهٔ اولیه است.

اثبات. فرض می‌کنیم a ریشهٔ اولیه‌ای از n است. بنابه قضیه، هر ریشهٔ اولیهٔ دیگر n عضوی از مجموعهٔ $\{a, a^۲, \ldots, a^{\phi(n)}\}$ است. ولی، تعداد توانهای a^k، $۱ \leq k \leq \phi(n)$، که مرتبهٔ آنها $\phi(n)$ است برابر با تعداد عددهای صحیح k ای است که به‌ازای آنها $\gcd(k, \phi(n)) = ۱$؛ تعداد چنین عددهای صحیحی $\phi(\phi(n))$ است، و بنابراین تعداد ریشه‌های اولیهٔ n برابر $\phi(\phi(n))$ است. □

به‌عنوان مثال، قضیهٔ ۸ـ۴ را به‌ازای $a = ۲$ و $n = ۹$ بررسی می‌کنیم. چون $\phi(۹) = ۶$، شش توان نخست ۲ باید، به‌ترتیبی با عددهای صحیح کوچکتر از ۹ و متباین با آن همنهشت به پیمانهٔ ۹ باشند. ولی عددهای صحیح کوچکتر از ۹ و متباین با آن عبارت‌اند از: ۱، ۲، ۴، ۵، ۷، ۸ و ملاحظه می‌کنیم که

$$۲^۱ \equiv ۲, ۲^۲ \equiv ۴, ۲^۳ \equiv ۸, ۲^۴ \equiv ۷, ۲^۵ \equiv ۵, ۲^۶ \equiv ۱ \text{ (به پیمانهٔ۹)}$$

با توجه به فرع قضیه، دقیقاً $\phi(\phi(۹)) = \phi(۶) = ۲$ ریشهٔ اولیهٔ ۹ وجود دارد. و اینها عبارت‌اند از: ۲ و ۵.

تمرینهای ۸ـ۱

۱. مرتبهٔ عددهای صحیح ۲، ۳، ۵ را (الف) به پیمانهٔ۱۷، (ب) به پیمانهٔ ۱۹، و (پ) به پیمانهٔ ۲۳ تعیین کنید.

۲. هریک از حکمهای زیر را ثابت کنید:

(الف) اگر a دارای مرتبهٔ hk به پیمانهٔ n باشد، آنگاه a^h دارای مرتبهٔ k به پیمانهٔ n است.

(ب) اگر a دارای مرتبهٔ $۲k$ به پیمانهٔ عدد اول فرد p باشد، آنگاه $a^k \equiv -۱ (\text{به پیمانهٔ } p)$.

(پ) اگر مرتبهٔ a به پیمانهٔ n برابر $n - ۱$ باشد، آنگاه n عددی اول است.

۳. ثابت کنید که $n \mid \phi(۲^n - ۱)$ به‌ازای هر $n > ۱$ مضربی از n است. [راهنمایی: عدد صحیح ۲ دارای مرتبهٔ n به پیمانهٔ$۲^n - ۱$است.]

۴. فرض کنید که مرتبهٔ a به پیمانهٔ n برابر h و مرتبهٔ b به پیمانهٔ n برابر k است. نشان دهید که مرتبهٔ ab به پیمانهٔ n، hk را می‌شمارد؛ به خصوص اگر $\gcd(h, k) = ۱$، آنگاه ab دارای مرتبهٔ hk است.

۵. اگر p عددی اول و فرد و a دارای مرتبهٔ ۳ به پیمانهٔ p باشد، نشان دهید مرتبهٔ $a + ۱$ به پیمانهٔ p باید ۶ باشد. [راهنمایی: از $a^۲ + a + ۱ \equiv ۰ \text{ (به پیمانهٔ} p)$ نتیجه می‌شود $(a + ۱)^۲ \equiv a \text{ (به پیمانهٔ } p)$ و $(a + ۱)^۳ \equiv -۱ (\text{به پیمانهٔ } p)$.]

۶. گزاره‌های زیر را ثابت کنید:

(الف) مقسوم‌علیه‌های اول فرد عدد صحیح $n^۲ + ۱$ به‌صورت $۴k + ۱$ هستند. [راهنمایی: اگر p عدد اول فردی باشد، بنابه قضیهٔ ۸ـ۱، از $n^۲ \equiv -۱ \text{ (به پیمانهٔ } p)$ نتیجه می‌شود $۴|\phi(p)$].

(ب) مقسوم‌علیه‌های اول فرد عدد صحیح $n^۴ + ۱$ به‌صورت $۸k + ۱$ هستند.

(پ) همهٔ مقسوم‌علیه‌های اول فرد عدد صحیح $n^{2} + n + 1$، بجز ۳، به‌صورت $6k + 1$ هستند.

۷. ثابت کنید تعداد عددهای اول به هریک از صورتهای $4k + 1$، $6k + 1$، و $8k + 1$ نامتناهی است. [راهنمایی: فرض کنید تعداد عددهای اول به‌صورت $4k + 1$ متناهی است؛ آنها را p_1، p_2، ...، p_r بنامید. عدد صحیح $(2p_1p_2 \dots p_r)^2 + 1$ را درنظر بگیرید و تمرین پیشین را به‌کار ببرید.]

۸. (الف) ثابت کنید که اگر p و q عددهای اول فردی باشند و $q|a^p - 1$، آنگاه یا $q|a - 1$ یا به‌ازای عدد صحیح k ای، $q = 2kp + 1$. [راهنمایی: چون $a^p \equiv 1$ (به پیمانهٔ q)، مرتبهٔ a به پیمانهٔ q یا ۱ یا p است؛ در حالت اخیر، $p|\phi(q)$.]

(ب) با استفاده از قسمت (الف) نشان دهید که اگر p عدد اول فردی باشد، آنگاه مقسوم‌علیه‌های اول $2^p - 1$ به‌صورت $2kp + 1$ هستند.

(پ) کوچکترین مقسوم‌علیه اول عددهای صحیح $2^{17} - 1$ و $2^{29} - 1$ را پیدا کنید.

۹. اگر p عدد اول فردی باشد، نشان دهید تعداد عددهای اولِ به‌صورت $2kp + 1$ نامتناهی است. [راهنمایی: فرض کنید تعداد عددهای اولِ به‌صورت $2kp + 1$ متناهی است؛ آنها را q_1، q_2، ...، q_r بنامید، و عدد صحیح $(q_1q_2 \dots q_r)^p - 1$ را درنظر بگیرید.]

۱۰. (الف) نشان دهید که ۲ ریشهٔ اولیه‌ای از ۱۹ است، ولی ریشهٔ اولیه‌ای از ۱۷ نیست.

(ب) با محاسبهٔ مرتبه‌های ۲، ۴، ۷، ۸، ۱۱، ۱۳، و ۱۴ به پیمانهٔ ۱۵، نشان دهید ۱۵ ریشهٔ اولیه ندارد.

۱۱. فرض کنید r ریشهٔ اولیه‌ای از عدد صحیح n باشد. ثابت کنید r^k ریشهٔ اولیه‌ای از n است اگر و تنها اگر $\gcd(k, \phi(n)) = 1$.

۱۲. (الف) دو ریشهٔ اولیهٔ ۱۰ را پیدا کنید.

(ب) با علم به اینکه ۳ ریشهٔ اولیه‌ای از ۱۷ است، هشت ریشهٔ اولیهٔ ۱۷ را به‌دست آورید.

۱۳. (الف) اگر p و $q > 3$ عددهای اول فردی باشند و $q|R_p$، ثابت کنید که به‌ازای عدد صحیح k ای، $q = 2kp + 1$.

(ب) کوچکترین مقسوم‌علیه‌های اول $R_5 = 11111$ و $R_7 = 1111111$ را پیدا کنید.

۸ـ۲ ریشه‌های اولیهٔ عددهای اول

چون ریشه‌های اولیه در بسیاری از تحقیقات نظری جایگاه بسیار مهمی دارند، توصیف همهٔ

عددهای صحیحِ دارای ریشه‌های اولیه، مسأله‌ای است که طبیعتاً جاذبه دارد. در چند صفحهٔ بعدی ثابت می‌کنیم که هر عدد اولی ریشهٔ اولیه دارد. پیش از انجام این کار، به‌منظور اثبات قضیه‌ای دربارهٔ تعداد جوابهای همنهشتی چندجمله‌ای، کمی از موضوع منحرف می‌شویم.

قضیهٔ ۸ـ۵ (لاگرانژ). اگر p عددی اول باشد و

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \qquad a_n \not\equiv 0 \ (\text{به پیمانهٔ } p)$$

چندجمله‌ای درجهٔ nای، $n \geq 1$، با ضریبهای صحیح باشد، آنگاه همنهشتی

$$f(x) \equiv 0 \ (\text{به پیمانهٔ } p)$$

دارای حداکثر n جواب ناهمنهشت به پیمانهٔ p است.

اثبات. به استقرا بر n یعنی درجهٔ $f(x)$ عمل می‌کنیم. اگر $n = 1$، چندجمله‌ای داده شده به‌صورت

$$f(x) = a_1 x + a_0$$

است. چون $\gcd(a_1, p) = 1$، بنابه قضیهٔ ۴ـ۷ می‌دانیم که همنهشتی $a_1 x \equiv -a_0$ (به پیمانهٔ p) جوابی یکتا به پیمانهٔ p دارد. بنابراین، قضیه به‌ازای $n = 1$ برقرار است.

اکنون به استقرا فرض می‌کنیم قضیه به‌ازای چندجمله‌ایهای درجهٔ $k - 1$ درست است و حالتی را که درجهٔ $f(x)$ برابر k است، درنظر می‌گیریم. یا $f(x) \equiv 0$ (به پیمانهٔ p) جوابی ندارد (و اثبات تمام است) یا حداقل یک جواب دارد، که آن را a می‌نامیم. اگر $f(x)$ بر $x - a$ تقسیم شود، نتیجه می‌شود

$$f(x) = (x - a) q(x) + r$$

که در آن $q(x)$ چندجمله‌ای درجهٔ $k - 1$ ای با ضریبهای صحیح و r عددی صحیح است. با جایگزینی $x = a$، به‌دست می‌آوریم

$$0 \equiv f(a) = (a - a) q(a) + r = r \ (\text{به پیمانهٔ } p)$$

و بنابراین، $f(x) \equiv (x - a) q(x)$ (به پیمانهٔ p).

اگر b جواب ناهمنهشت دیگری از $f(x) \equiv 0$ (به پیمانهٔ p) باشد، آنگاه

$$0 \equiv f(b) = (b - a) q(b) \ (\text{به پیمانهٔ } p)$$

چون (به پیمانهٔ p) $b - a \not\equiv ۰$، نتیجه می‌شود (به پیمانهٔ p) $q(b) \equiv ۰$؛ به بیان دیگر، هر جواب (به پیمانهٔ p) $f(x) \equiv ۰$ که متفاوت با a باشد، باید در (پیمانهٔ p) $q(x) \equiv ۰$ صدق کند. بنا به فرض استقرای ما، همنهشتی اخیر حداکثر $k - ۱$ جواب ناهمنهشت دارد و بنابراین (به پیمانهٔ p) $f(x) \equiv ۰$ بیش از k جواب ناهمنهشت ندارد. به این ترتیب مرحلهٔ استقرا و اثبات به انجام می‌رسد. □

از این قضیه به آسانی نتیجهٔ زیر را می‌گیریم.

فرع. اگر p عددی اول باشد و $d|p - ۱$، آنگاه همنهشتی

$$x^d - ۱ \equiv ۰ \ (\text{به پیمانهٔ } p)$$

دقیقاً d جواب دارد.

اثبات. چون $d|p - ۱$، به‌ازای k ای داریم $p - ۱ = dk$. پس

$$x^{p-۱} - ۱ = (x^d - ۱)f(x)$$

که در آن ضریبهای چندجمله‌ای $f(x) = x^{d(k-۱)} + x^{d(k-۲)} + \ldots + x^d + ۱$ صحیح‌اند و درجهٔ چندجمله‌ای، $d(k - ۱) = p - ۱ - d$ است. بنابه قضیهٔ لاگرانژ، همنهشتی (به پیمانهٔ p) $f(x) \equiv ۰$ حداکثر $p - ۱ - d$ جواب دارد. همچنین بنابه قضیهٔ فرما می‌دانیم که (به پیمانهٔ p) $x^{p-۱} - ۱ \equiv ۰$ دقیقاً $p - ۱$ جواب ناهمنهشت دارد؛ یعنی عددهای صحیح ۱، ۲، ...، $p - ۱$.

اکنون، هر جواب $x = a$ از (به پیمانهٔ p) $x^{p-۱} - ۱ \equiv ۰$ که جوابی از (به پیمانهٔ p) $f(x) \equiv ۰$ نباشد، باید در (به پیمانهٔ p) $x^d - ۱ \equiv ۰$ صدق کند، زیرا از

$$۰ \equiv a^{p-۱} - ۱ = (a^d - ۱)f(a) \ (\text{به پیمانهٔ } p)$$

با استفاده از $p \nmid f(a)$ نتیجه می‌شود $p|a^d - ۱$. و بنابراین (به پیمانهٔ p) $x^d - ۱ \equiv ۰$ باید حداقل

$$p - ۱ - (p - ۱ - d) = d$$

جواب داشته باشد. همنهشتی اخیر نمی‌تواند بیش از d جواب داشته باشد (باز قضیهٔ لاگرانژ وارد کار می‌شود)، پس دارای دقیقاً d جواب است. □

اکنون با استفاده از این فرع، قضیهٔ ویلسن را به روش دیگری ثابت می‌کنیم: به‌ازای عدد اول p، چندجمله‌ای $f(x)$ را به‌صورت

$$f(x) = (x-۱)(x-۲)\ldots(x-(p-۱)) - (x^{p-۱}-۱)$$
$$= a_{p-۲}x^{p-۲} + a_{p-۳}x^{p-۳} + \ldots + a_۱ x + a_۰$$

که از درجهٔ $p-۲$ است، تعریف می‌کنیم. بنابه قضیهٔ فرما، $p-۱$ عدد صحیح ۱، ۲، …، $p-۱$ جوابهای ناهمنهشتِ همنهشتی

$$f(x) \equiv ۰ \ (\text{به پیمانهٔ } p)$$

هستند. ولی این ناسازگار با قضیهٔ لاگرانژ است، مگر اینکه

$$a_{p-۲} \equiv a_{p-۳} \equiv \ldots \equiv a_۱ \equiv a_۰ \equiv ۰ \ (\text{به پیمانهٔ } p)$$

نتیجه می‌شود به‌ازای هر مقدار صحیح x

$$(x-۱)(x-۲)\ldots(x-(p-۱)) - (x^{p-۱}-۱) \equiv ۰ \ (\text{به پیمانهٔ } p)$$

به‌ازای $x = ۰$ به‌دست می‌آوریم

$$(-۱)(-۲)\ldots(-(p-۱)) + ۱ \equiv ۰ \ (\text{به پیمانهٔ } p)$$

یا $(-۱)^{p-۱}(p-۱)! + ۱ \equiv ۰$ (به پیمانهٔ p). حال یا $p-۱$ زوج است یا $p=۲$، که در این حالت $-۱ \equiv ۱$ (به پیمانهٔ p)؛ در هر حالت، به‌دست می‌آوریم

$$(p-۱)! \equiv -۱ \ (\text{به پیمانهٔ } p)$$

قضیهٔ لاگرانژ راه را هموار کرده است. اکنون می‌توانیم ثابت کنیم به‌ازای هر عدد اول p، عددهایی صحیح با مرتبهٔ متناظر با هر مقسوم‌علیه $p-۱$ وجود دارد. به بیان دقیقتر:

قضیهٔ ۸ـ۶ اگر p عددی اول باشد و $d|p-۱$، آنگاه دقیقاً $\phi(d)$ عدد صحیح ناهمنهشت به پیمانهٔ p با مرتبهٔ d وجود دارد.

اثبات. فرض می‌کنیم $d|p-۱$ و $\psi(d)$ تعداد عددهای صحیح k، $۱ \leq k \leq p-۱$، با مرتبهٔ d به پیمانهٔ p باشد. چون هر عدد صحیح میان ۱ و $p-۱$ مرتبهٔ d ای دارد که $d|p-۱$، پس

$$p - ۱ = \sum_{d|p-۱} \psi(d)$$

همچنین، بنابه قضیهٔ گاوس

$$p - ۱ = \sum_{d|p-۱} \phi(d)$$

بنابراین، با مقایسهٔ این دو داریم

$$\sum_{d|p-۱} \psi(d) = \sum_{d|p-۱} \phi(d) \qquad (۱)$$

می‌خواهیم نشان دهیم که به‌ازای هر مقسوم‌علیه d از $p-۱$، $\psi(d) \leq \phi(d)$، زیرا از اینجا با توجه به رابطهٔ (۱) نتیجه می‌شود $\psi(d) = \phi(d) \neq ۰$ (وگرنه، مجموع سمت چپ اکیداً کوچکتر از مجموع سمت راست می‌شود).

اگر d مقسوم‌علیه دلخواهی از $p-۱$ باشد، دو حالت پیش می‌آید: یا $\psi(d) = ۰$ یا $\psi(d) > ۰$. اگر $\psi(d) = ۰$، آنگاه قطعاً $\psi(d) \leq \phi(d)$. فرض می‌کنیم $\psi(d) > ۰$؛ بنابراین عدد صحیح aای با مرتبهٔ d وجود دارد. در این صورت d عدد صحیح a، $a^۲$، ...، a^d به پیمانهٔ p ناهمنهشت‌اند و هریک در همنهشتی چندجمله‌ای

$$x^d - ۱ \equiv ۰ \ (\text{به پیمانهٔ } p) \qquad (۲)$$

صدق می‌کند زیرا، $(a^k)^d = (a^d)^k \equiv ۱ \ (\text{به پیمانهٔ } p)$. بنابه فرع قضیهٔ لاگرانژ، (۲) جواب دیگری نمی‌تواند داشته باشد. نتیجه می‌گیریم که هر عدد صحیح با مرتبهٔ d به پیمانهٔ p باید با یکی از a، $a^۲$، ...، a^d همنهشت باشد. ولی فقط مرتبهٔ $\phi(d)$ تا از توانهای اخیرالذکر برابر dاست، یعنی آن a^k هایی که نمای kی آنها در $\gcd(k,d) = ۱$ صدق می‌کند. پس، در وضعیت فعلی، $\psi(d) = \phi(d)$، و تعداد عددهای صحیح با مرتبهٔ d به پیمانهٔ p برابر با $\phi(d)$ است. بنابراین، اثبات حکم به انجام می‌رسد. □

با فرض $d = p - ۱$ در قضیهٔ ۸ـ۶، به نتیجهٔ زیر می‌رسیم.

فرع. اگر p عددی اول باشد، آنگاه p دقیقاً $\phi(p-۱)$ ریشهٔ اولیهٔ ناهمنهشت دارد.

مثالی به‌ازای $p = ۱۳$ می‌آوریم. با این پیمانه، مرتبهٔ ۱ برابر ۱ است؛ مرتبهٔ ۱۲ برابر ۲ است؛ مرتبهٔ هریک از ۳ و ۹ برابر ۳ است؛ مرتبهٔ هریک از ۵ و ۸ برابر ۴ است؛ مرتبهٔ هریک از ۴ و ۱۰ برابر ۶ است؛ و چهار عدد صحیح، یعنی ۲، ۶، ۷، ۱۱، دارای مرتبهٔ ۱۲ اند. پس، طبق انتظار

$$\begin{aligned}\sum_{d|۱۲} \psi(d) &= \psi(۱) + \psi(۲) + \psi(۳) + \psi(۴) + \psi(۶) + \psi(۱۲)\\ &= ۱ + ۱ + ۲ + ۲ + ۲ + ۴ = ۱۲\end{aligned}$$

همچنین توجه کنید که

$$\begin{aligned}\psi(۱) &= ۱ = \phi(۱), & \psi(۴) &= ۲ = \phi(۴)\\ \psi(۲) &= ۱ = \phi(۲), & \psi(۶) &= ۲ = \phi(۶)\\ \psi(۳) &= ۲ = \phi(۳), & \psi(۱۲) &= ۴ = \phi(۱۲)\end{aligned}$$

ضمناً، روش کوتاهتر و زیباتری برای اثبات $\psi(d) = \phi(d)$ به‌ازای هر $d|p - ۱$ وجود دارد. کافی است وارونسازی موبیوس را در مورد فرمول $d = \sum_{c|d} \psi(c)$ انجام دهیم تا نتیجه بگیریم

$$\psi(d) = \sum_{c|d} \mu(c)(\frac{d}{c})$$

با توجه به قضیهٔ ۷ـ۸، طرف راست این معادله برابر با $\phi(d)$ است. البته، اعتبار این استدلال بسته به این است که بدانیم تابع ψ ضربی است.

با استفاده از قضیهٔ اخیر می‌توانیم اثباتی دیگر برای این حکم که اگر p عددی اول به صورت $۴k + ۱$ باشد، آنگاه همنهشتی درجهٔ دوم $x^۲ \equiv -۱$ (به پیمانهٔ p) جواب دارد، ارائه دهیم. چون $۴|p - ۱$، بنابه قضیهٔ ۸ـ۶، عدد صحیح a ای با مرتبهٔ ۴ به پیمانهٔ p وجود دارد؛ به بیان دیگر

$$a^۴ \equiv ۱ \ (p \text{ به پیمانهٔ})$$

و یا معادلش

$$(a^۲ - ۱)(a^۲ + ۱) \equiv ۰ \ (p \text{ به پیمانهٔ})$$

چون p اول است، نتیجه می‌شود که یا

$$a^۲ - ۱ \equiv ۰ \ (p \text{ به پیمانهٔ}) \text{ یا } a^۲ + ۱ \equiv ۰ \ (p \text{ به پیمانهٔ})$$

اگر همنهشتی سمت راستی برقرار باشد، لازم می‌آید که مرتبهٔ a برابر یا کوچکتر از ۲ باشد، که یک تناقض است. پس، $a^{۲} + ۱ \equiv ۰$ (به پیمانهٔ p)، یعنی، عدد صحیح a جوابی از همنهشتی $x^{۲} \equiv -۱$ (به پیمانهٔ p) است.

اثباتی که برای قضیهٔ ۸ـ۶ ارائه شد، اِشکال واضحی دارد و آن این است که گرچه وجود ریشه‌های اولیهٔ عدد اول داده شده را تضمین می‌کند، اثباتی سازنده نیست. برای پیداکردن ریشهٔ اولیه معمولاً باید به روش آزمون و خطا عمل کرد و یا به جدولهای مفصلِ از پیش تهیه شده متوسل شد. در جدول زیر کوچکترین ریشهٔ اولیهٔ مثبت هر عدد اول کوچکتر از ۲۰۰ ملاحظه می‌شود.

اول	کوچکترین ریشهٔ اولیهٔ مثبت	اول	کوچکترین ریشهٔ اولیهٔ‌مثبت
۲	۱	۸۹	۳
۳	۲	۹۷	۵
۵	۲	۱۰۱	۲
۷	۳	۱۰۳	۵
۱۱	۲	۱۰۷	۲
۱۳	۲	۱۰۹	۶
۱۷	۳	۱۱۳	۳
۱۹	۲	۱۲۷	۳
۲۳	۵	۱۳۱	۲
۲۹	۲	۱۳۷	۳
۳۱	۳	۱۳۹	۲
۳۷	۲	۱۴۹	۲
۴۱	۶	۱۵۱	۶
۴۳	۳	۱۵۷	۵
۴۷	۵	۱۶۳	۲
۵۳	۲	۱۶۷	۵
۵۹	۲	۱۷۳	۲
۶۱	۲	۱۷۹	۲
۶۷	۲	۱۸۱	۲
۷۱	۷	۱۹۱	۱۹
۷۳	۵	۱۹۳	۵
۷۹	۳	۱۹۷	۲
۸۳	۲	۱۹۹	۳

اگر کوچکترین ریشهٔ اولیهٔ مثبت عدد اول p را با $\chi(p)$ نشان دهیم آنگاه به‌طوری که جدول فوق نشان می‌دهد، به‌ازای هر $p < ۲۰۰$، $\chi(p) \leq ۱۹$. در واقع، اگر p بدون محدودیت افزایش یابد، $\chi(p)$ نیز به دلخواه بزرگ می‌شود. از این جدول چنین برمی‌آید، هر چند هنوز ثابت نشده است، که تعداد عددهای اول p با ضابطهٔ $\chi(p) = ۲$ نامتناهی است.

گاوس در کتاب تحقیقات حسابی خود حدس زد که تعداد عددهای اول با ریشهٔ اولیهٔ ۱۰، نامتناهی است. در ۱۹۲۷، امیل آرتین این حدس را به این صورت تعمیم داد: اگر a برابر ۱، ۱− یا مربعی کامل نباشد، تعداد عددهای اول با ریشهٔ اولیهٔ a نامتناهی است. گرچه در درستی این حدس تردید چندانی وجود ندارد، هنوز آن را ثابت نکرده‌اند. تحقیقات اخیر (۱۹۸۶) نشان می‌دهد تعداد عددهای صحیحی که به‌ازای آنها حدس آرتین درست است، نامتناهی است، واین حدس حداکثر به‌ازای دو عدد اول صائب نیست.

اکنون دلیل محدودیتهای موجود در حدس آرتین را توضیح می‌دهیم. فرض می‌کنیم a مربعی کامل، مثلاً $a = x^۲$، و p عدد اول فردی باشد به‌طوری که $\gcd(a,p) = ۱$. اگر $p \nmid x$، آنگاه بنابه قضیهٔ فرما، $x^{p-۱} \equiv ۱$ (به پیمانهٔp)، و بنابراین

$$a^{(p-۱)/۲} = (x^۲)^{(p-۱)/۲} \equiv ۱ \ (\text{به پیمانهٔ } p)$$

پس a نمی‌تواند ریشهٔ اولیه‌ای از p باشد [اگر $p|x$، آنگاه $p|a$ و مطمئناً $a^{p-۱} \not\equiv ۱$ (به پیمانهٔ p)]. به‌علاوه، چون $(-۱)^۲ = ۱$، ۱− ریشهٔ اولیهٔ p، وقتی که $p - ۱ > ۲$، نیست.

مثال ۸ـ۳

روشهای گوناگون این بخش را برای پیداکردن $\phi(۶) = ۲$ عدد صحیح مرتبهٔ ۶ به پیمانهٔ ۳۱ به‌کار می‌گیریم. در آغاز می‌دانیم که تعداد

$$\phi(\phi(۳۱)) = \phi(۳۰) = ۸$$

ریشهٔ اولیه برای ۳۱ وجود دارد. تعیین یکی از اینها با آزمون و خطا صورت می‌گیرد. چون $۲^۵ \equiv ۱$ (به پیمانهٔ ۳۱)، به وضوح عدد صحیح ۲ حذف می‌شود. نیازی به جستجوی خیلی زیاد نیست، زیرا معلوم می‌شود که ۳، ریشهٔ اولیه‌ای از ۳۱ است. توجه کنید که در محاسبهٔ توانهای صحیح ۳ لازم نیست فراتر از $۳^{۱۵}$ را آزمود زیرا مرتبهٔ ۳ باید $\phi(۳۱) = ۳۰$ را بشمارد و محاسبهٔ

$$\begin{aligned} ۳^{۱۵} = (۲۷)^۵ \equiv (-۴)^۵ = (-۶۴)(۱۶) \equiv -۲(۱۶) \\ \equiv -۱ \not\equiv ۱ \ (\text{به پیمانهٔ} ۳۱) \end{aligned}$$

نشان می‌دهد که مرتبهٔ آن بزرگتر از ۱۵ است.

چون ۳ ریشهٔ اولیه‌ای از ۳۱ است، هر عدد صحیح متباین با ۳۱ با عدد صحیحی به‌صورت ۳^k، $۱ \leq k \leq ۳۰$، به پیمانهٔ ۳۱ همنهشت است. بنابه قضیهٔ ۸ـ۳، مرتبهٔ ۳^k برابر با $۳۰/\gcd(k, ۳۰)$ است؛ این برابر ۶ است اگر و تنها اگر $\gcd(k, ۳۰) = ۵$. مقدارهایی از k که به‌ازای آنها برابری اخیر برقرار است عبارت‌اند از: $k = ۵$ و $k = ۲۵$. پس مسالهٔ ما اکنون به محاسبهٔ $۳^۵$ و $۳^{۲۵}$ به پیمانهٔ ۳۱ تبدیل می‌شود. با محاسبه‌ای ساده معلوم می‌شود

$$۳^۵ = (۲۷)۹ \equiv (-۴)۹ \equiv -۳۶ \equiv ۲۶ \ (\text{به پیمانهٔ } ۳۱)$$

$$\begin{aligned} ۳^{۲۵} &\equiv (۳^۵)^۵ \equiv (۲۶)^۵ \equiv (-۵)^۵ \equiv (-۱۲۵)(۲۵) \equiv (-۱)۲۵ \\ &\equiv ۶ \ (\text{به پیمانهٔ } ۳۱) \end{aligned}$$

بنابراین ۶ و ۲۶ تنها عددهای صحیح با مرتبهٔ ۶ به پیمانهٔ ۳۱ اند. ■

تمرینهای ۸ـ۲

۱. اگر p عدد فرد اولی باشد، ثابت کنید

(الف) ۱ و $p - ۱$ تنها جوابهای ناهمنهشتِ $x^۲ \equiv ۱$ (به پیمانهٔ p) اند؛

(ب) همنهشتی $x^{p-۲} + \ldots + x^۲ + x + ۱ \equiv ۰$ (به پیمانهٔ p) دقیقاً $p - ۲$ جواب ناهمنهشت دارد که عبارت‌اند از: عددهای صحیح ۲، ۳، ...، $p - ۱$.

۲. نشان دهید که هریک از همنهشتیهای $x^۲ \equiv ۱$ (به پیمانهٔ ۱۵)، $x^۲ \equiv -۱$ (به پیمانهٔ ۶۵) و $x^۲ \equiv -۲$ (به پیمانهٔ ۳۳) دارای چهار جواب ناهمنهشت است؛ پس، قضیهٔ لاگرانژ، وقتی پیمانهٔ عدد مرکبی باشد، لزوماً برقرار نیست.

۳. همهٔ ریشه‌های اولیهٔ عددهای اول ۱۱، ۱۹، و ۲۳ را تعیین کنید. هریک را به‌صورت توانی از یکی از ریشه‌ها نمایش دهید.

۴. اگر ۳ ریشهٔ اولیه‌ای از ۴۳ باشد، مطلوب است

(الف) همهٔ عددهای صحیح مثبت کوچکتر از ۴۳ با مرتبهٔ ۶ به پیمانهٔ ۴۳؛

(ب) همهٔ عددهای صحیح مثبت کوچکتر از ۴۳ با مرتبهٔ ۲۱ به پیمانهٔ ۴۳.

۵. همهٔ عددهای صحیح مثبت کوچکتر از ۶۱ با مرتبهٔ ۴ به پیمانهٔ ۶۱ را پیدا کنید.

۶. به فرض اینکه r ریشهٔ اولیه‌ای از عدد اول فرد p باشد، حکمهای زیر را ثابت کنید:

(الف) همنهشتی $r^{(p-۱)/۲} \equiv -۱$ (به پیمانهٔ p) برقرار است.

(ب) اگر r' ریشهٔ اولیهٔ دیگری از p باشد، آنگاه rr' ریشهٔ اولیه‌ای از p نیست [راهنمایی: بنابه قسمت (الف)، (به پیمانهٔ p) $(rr')^{(p-1)/2} \equiv 1$.]

(پ) اگر عدد صحیح r' در (به پیمانهٔ p) $rr' \equiv 1$ صدق کند، آنگاه r' ریشهٔ اولیه‌ای از p است.

۷. ثابت کنید که به‌ازای هر عدد اول $p > 3$، ریشه‌های اولیهٔ p به‌صورت جفتهایی چون (r, r') هستند به‌طوری که (به پیمانهٔ p) $rr' \equiv 1$. [راهنمایی: اگر r ریشهٔ اولیه‌ای از p باشد، عدد صحیح $r' = r^{p-2}$ را درنظر بگیرید.]

۸. فرض کنید r ریشهٔ اولیه‌ای از عدد اول فرد p است. ثابت کنید که

(الف) اگر (به پیمانهٔ۴) $p \equiv 1$، آنگاه $-r$ ریشهٔ اولیه‌ای از p است؛

(ب) اگر (به پیمانهٔ ۴) $p \equiv 3$، آنگاه $-r$ دارای مرتبهٔ $(p-1)/2$ به پیمانهٔ p است.

۹. با اثبات اینکه اگر r، ریشهٔ اولیه‌ای از عدد اول (به پیمانهٔ ۴) $p \equiv 1$ باشد، آنگاه $r^{(p-1)/4}$ در همنهشتی درجهٔ دوم (به پیمانهٔ p) $x^2 + 1 \equiv 0$ صدق می‌کند، اثبات دیگری از قضیهٔ ۵ـ۵ ارائه دهید.

۱۰. با استفاده از اینکه هر عدد اول p دارای ریشهٔ اولیه است، اثبات دیگری از قضیهٔ ویلسن ارائه دهید. [راهنمایی: اگر r ریشهٔ اولیه‌ای از p باشد، آنگاه بنا به قضیهٔ ۸ـ۴، (به پیمانهٔ p) $(p-1)! \equiv r^{1+2+\dots+(p-1)}$.]

۱۱. اگر p عددی اول باشد، نشان دهید که حاصلضرب $\phi(p-1)$ ریشهٔ اولیهٔ p با $(-1)^{\phi(p-1)}$ همنهشت به پیمانهٔ p است. [راهنمایی: اگر r ریشهٔ اولیه‌ای از p باشد و $\gcd(k, p-1) = 1$، آنگاه عدد صحیح r^k ریشهٔ اولیه‌ای از p است؛ اکنون از قضیهٔ ۷ـ۷ استفاده کنید.]

۱۲. به‌ازای عدد اول فرد p نشان دهید که

$$1^n + 2^n + 3^n + \dots + (p-1)^n \equiv \begin{cases} 0 \ (\text{به پیمانهٔ } p) & \text{اگر } p-1 \nmid n \\ -1 \ (\text{به پیمانهٔ } p) & \text{اگر } p-1 \mid n \end{cases}$$

[راهنمایی: اگر $p-1 \nmid n$ و r ریشهٔ اولیه‌ای از p باشد، آنگاه مجموع فوق با

$$1 + r^n + r^{2n} + \dots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}$$

همنهشت به پیمانهٔ p است.]

۳ـ۸ عددهای مرکب دارای ریشهٔ اولیه

پیشتر دیدیم که ۲ ریشهٔ اولیه‌ای از ۹ است، بنابراین عددهای مرکب نیز می‌توانند ریشه‌های اولیه داشته باشند. مرحلهٔ بعدی برنامهٔ ما تعیین همهٔ عددهای مرکبی است که ریشهٔ اولیه دارند. در حکمهای منفی زیر اطلاعاتی در این زمینه ارائه می‌شود.

قضیهٔ ۸ـ۷ اگر $k \geq ۳$، عدد صحیح ۲^k ریشهٔ اولیه ندارد.

اثبات. به دلایلی که بعداً معلوم خواهد شد، استدلال را با اثبات اینکه اگر a عدد صحیح فردی باشد، آنگاه به‌ازای $k \geq ۳$

$$a^{۲^{k-۲}} \equiv ۱ \ (\text{به پیمانهٔ } ۲^k)$$

آغاز می‌کنیم. اگر $k = ۳$، این همنهشتی تبدیل به $a^۲ \equiv ۱$ (به پیمانهٔ ۸) می‌شود، که مسلماً برقرار است (در واقع، (به پیمانهٔ ۸) $۱^۲ \equiv ۳^۲ \equiv ۵^۲ \equiv ۷^۲ \equiv ۱$). به‌ازای $k > ۳$، به استقرا بر k عمل می‌کنیم. فرض می‌کنیم حکم به‌ازای عدد صحیح k، $k \geq ۳$، برقرار است؛ یعنی (به پیمانهٔ ۲^k) $a^{۲^{k-۲}} \equiv ۱$. این معادل با معادلهٔ

$$a^{۲^{k-۲}} = ۱ + b۲^k$$

است که در آن b عددی صحیح است. با مربع کردن دو طرف، به‌دست می‌آوریم

$$\begin{aligned} a^{۲^{k-۱}} = (a^{۲^{k-۲}})^۲ &= ۱ + ۲(b۲^k) + (b۲^k)^۲ \\ &= ۱ + ۲^{k+۱}(b + b^۲ ۲^{k-۱}) \\ &\equiv ۱ \ (\text{به پیمانهٔ } ۲^{k+۱}) \end{aligned}$$

پس همنهشتی ادعاشده به‌ازای $k + ۱$ و بنابراین به‌ازای هر $k \geq ۳$ برقرار است.

اکنون عددهای صحیح فرد تنها عددهای متباین با ۲^k هستند؛ همچنین $\phi(۲^k) = ۲^{(k-۱)}$. پس، طبق آنچه ثابت شد، اگر a عددی صحیح فرد باشد و $k \geq ۳$، داریم

$$a^{\frac{\phi(۲^k)}{۲}} \equiv ۱ \ (\text{به پیمانهٔ } ۲^k)$$

و، درنتیجه ۲^k ریشهٔ اولیه ندارد. □

قضیهٔ زیر نیز قضیهٔ دیگری است از همین نوع.

قضیهٔ ۸ـ۸ اگر $m, n > ۲$ و $\gcd(m,n) = ۱$، آنگاه عدد صحیح mn ریشهٔ اولیه ندارد.

اثبات. عدد صحیح دلخواه aای درنظر می‌گیریم که $\gcd(a, mn) = ۱$؛ در این صورت $\gcd(a,n) = ۱$ و $\gcd(a,m) = ۱$. قرار می‌دهیم $h = \operatorname{lcm}(\phi(m), \phi(n))$ و $d = \gcd(\phi(m), \phi(n))$.

چون هر دوی $\phi(m)$ و $\phi(n)$ زوج‌اند (قضیهٔ ۷ـ۴)، مطمئناً $d \geq ۲$. درنتیجه داریم

$$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{۲}$$

ولی، بنابه قضیهٔ اویلر، $a^{\phi(m)} \equiv ۱$ (به پیمانهٔ m). اگر دو طرف معادله را به توان $\phi(n)/d$ برسانیم، به‌دست می‌آوریم

$$a^h = (a^{\phi(m)})^{\frac{\phi(n)}{d}} \equiv ۱^{\frac{\phi(n)}{d}} \equiv ۱ \ (\text{به پیمانهٔ } m)$$

با استدلالی مشابه نتیجه می‌شود $a^h \equiv ۱$ (به پیمانهٔ n). از این همنهشتیها با توجه به فرض $\gcd(m,n) = ۱$ نتیجه می‌گیریم

$$a^h \equiv ۱ \ (\text{به پیمانهٔ } mn)$$

یعنی مرتبهٔ هیچ عدد صحیح متباین با mn بیش از $\phi(mn)/۲$ نیست، بنابراین mn نمی‌تواند ریشهٔ اولیه داشته باشد. □

برخی از حالتهای خاص قضیهٔ ۸ـ۸ اهمیت ویژه‌ای دارند و آنها را در زیر ذکر می‌کنیم.

فرع. اگر عدد صحیح n

(۱) بر دو عدد اول فرد متمایز بخشپذیر باشد، یا

(۲) به‌صورت $n = ۲^m p^k$ باشد که در آن $m \geq ۲$ و p عدد فرد اولی باشد،

آنگاه n ریشه اولیه ندارد.

ویژگی مهم نتایج اخیر آن است که میدان جستجوی ریشه‌های اولیه را به عددهای صحیح ۲، ۴، p^k و $۲p^k$، که p عدد اول فردی است، محدود می‌کنند. در این بخش، ثابت می‌کنیم که هر یک از عددهای اخیرالذکر ریشهٔ اولیه دارد. قسمت اصلی کار، اثبات وجود ریشه‌های اولیه برای توانهای عدد اول فرد است. استدلال تا اندازه‌ای طولانی ولی سر راست است و برای وضوح بیشتر، در چند مرحله صورت می‌گیرد.

لم ۱. اگر p عدد فرد اولی باشد، ریشهٔ اولیه‌ای چون r دارد به‌طوری که (به پیمانهٔ $p^{۲}$) $r^{p-۱} \not\equiv ۱$.

اثبات. بنابه قضیهٔ ۸ـ۶ می‌دانیم که p ریشه‌های اولیه‌ای دارد. یکی از آنها را انتخاب، و آن را r می‌نامیم. اگر (به پیمانهٔ $p^{۲}$) $r^{p-۱} \not\equiv ۱$، اثبات تمام است. در غیر این صورت به‌جای r، $r' = r + p$ را قرار می‌دهیم که آن نیز ریشهٔ اولیه‌ای از p است؛ در این صورت با استفاده از قضیهٔ دوجمله‌ای داریم

$$(r')^{p-۱} \equiv (r+p)^{p-۱} \equiv r^{p-۱} + (p-۱)pr^{p-۲} \quad (\text{به پیمانهٔ } p^{۲})$$

ولی فرض کرده‌ایم (به پیمانهٔ $p^{۲}$) $r^{p-۱} \equiv ۱$؛ پس

$$(r')^{p-۱} \equiv ۱ - pr^{p-۲} \quad (\text{به پیمانهٔ } p^{۲})$$

چون r ریشهٔ اولیه‌ای از p است، $\gcd(r,p) = ۱$ و بنابراین $p \nmid r^{p-۲}$. پس، همانطورکه می‌خواستیم، (به پیمانهٔ $p^{۲}$) $(r')^{p-۱} \not\equiv ۱$. □

فرع. اگر p عدد اول فردی باشد، آنگاه $p^{۲}$ ریشهٔ اولیه‌ای دارد؛ درواقع، به‌ازای هر ریشهٔ اولیه r از p، یا r و یا $r + p$ ریشهٔ اولیه‌ای از $p^{۲}$ است.

اثبات. حکم تقریباً بدیهی است. اگر r ریشهٔ اولیه‌ای از p باشد، آنگاه مرتبهٔ r به پیمانهٔ $p^{۲}$ یا $p - ۱$ است یا $\phi(p^{۲}) = p(p-۱)$. اثبات اخیر نشان می‌دهد که اگر مرتبهٔ r به پیمانهٔ $p^{۲}$ برابر $p - ۱$ باشد، آنگاه $r + p$ ریشهٔ اولیه‌ای از $p^{۲}$ است. □

برای نیل به هدف، لم نسبتاً فنی دیگری مورد نیاز است.

لم ۲. فرض می‌کنیم p یک عدد اول فرد و r ریشهٔ اولیه‌ای از p باشد به‌طوری که (به پیمانهٔ $p^{۲}$) $r^{p-۱} \not\equiv ۱$. در این صورت به‌ازای هر عدد صحیح $k \geq ۲$،

$$r^{p^{k-۲}(p-۱)} \not\equiv ۱ \quad (\text{به پیمانهٔ } p^{k})$$

اثبات. اثبات به استقرا بر k صورت می‌گیرد. بنابه فرض، حکم به‌ازای $k = ۲$ برقرار است. فرض می‌کنیم حکم به‌ازای $k \geq ۲$ ای برقرار است و نشان می‌دهیم به‌ازای $k + ۱$ نیز برقرار است. چون $\gcd(r, p^{k}) = \gcd(r, p^{k-۱}) = ۱$، بنابه قضیهٔ اویلر داریم

$$r^{p^{k-۲}(p-۱)} = r^{\phi(p^{k-۱})} \equiv ۱ \quad (\text{به پیمانهٔ } p^{k-۱})$$

پس، عدد صحیح a ای وجود دارد به‌طوری که

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$

که در آن، بنابه فرض استقرا، $p \nmid a$. طرفین معادلهٔ اخیر را به توان p می‌رسانیم و بسط می‌دهیم. در این صورت

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$$

چون عدد صحیح a بر p بخشپذیر نیست، داریم

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

به این ترتیب، مرحلهٔ استقرا تکمیل می‌شود، و بنابراین لم ثابت می‌گردد. □

بخش دشوار کار در اینجا به اتمام رسیده است. با تلفیق لمهای فوق ثابت می‌کنیم که توانهای هر عدد اول فرد دارای ریشهٔ اولیه‌اند.

قضیهٔ ۸ـ۹ اگر p عدد فرد اولی باشد و $k \geq 1$، آنگاه p^k ریشهٔ اولیه دارد.

اثبات. بنابه دو لم اخیر، p دارای ریشهٔ اولیهٔ r ای است که $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$؛ درواقع، هر r ای که در شرط $r^{p-1} \not\equiv 1 \pmod{p^2}$ صدق کند، این خاصیت را دارد. استدلال می‌کنیم که چنین r ای ریشهٔ اولیهٔ هر توانی از p است.

فرض می‌کنیم n مرتبهٔ r به پیمانهٔ p^k باشد. بنابه قضیهٔ ۸ـ۱، n باید $\phi(p^k) = p^{k-1}(p-1)$ را بشمارد. چون از $r^n \equiv 1 \pmod{p^k}$ نتیجه می‌شود $r^n \equiv 1 \pmod{p}$، داریم $p-1 | n$ (باز بنابه قضیهٔ ۸ـ۱). درنتیجه n ای به‌ازای $0 \leq m \leq k-1$، وجود دارد به‌طوری که $n = p^m(p-1)$. اگر $n \neq p^{k-1}(p-1)$، آنگاه $p^{k-2}(p-1)$ بر n بخشپذیر است و نتیجه می‌گیریم

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$$

که متناقض با نحوهٔ انتخاب اولیهٔ r است. بنابراین، $n = p^{k-1}(p-1)$ و r ریشهٔ اولیه‌ای از p^k است. □

به این ترتیب فقط بررسی حالت $2p^k$ باقی می‌ماند.

فرع. اگر p عددی فرد اول باشد و $k \geq ۱$، $۲p^k$ ریشه‌های اولیه دارد.

اثبات. فرض می‌کنیم r ریشهٔ اولیه‌ای از p^k باشد. بی‌آنکه به کلیت مطلب خللی وارد شود، می‌توان فرض کرد r عدد صحیح فردی است؛ زیرا اگر r زوج باشد، آنگاه $r + p^k$ فرد است و باز ریشهٔ اولیه‌ای از p^k است. پس $\gcd(r, ۲p^k) = ۱$. n، مرتبهٔ عدد r به پیمانهٔ$۲p^k$، باید

$$\phi(۲p^k) = \phi(۲)\phi(p^k) = \phi(p^k)$$

را بشمارد. ولی از (به پیمانهٔ $۲p^k$) $r^n \equiv ۱$ نتیجه می‌شود (به پیمانهٔp^k) $r^n \equiv ۱$، و بنابراین $\phi(p^k)|n$. از تلفیق این شرطهای بخشپذیری نتیجه می‌شود $n = \phi(۲p^k)$، و بنابراین r ریشهٔ اولیه‌ای از $۲p^k$ است. □

عدد اول ۵ دارای $\phi(۴) = ۲$ ریشهٔ اولیه است که عددهای صحیح ۲ و ۳ هستند. چون

$$۲^{۵-۱} \equiv ۱۶ \not\equiv ۱ \ (\text{به پیمانهٔ } ۲۵) \quad \text{و} \quad ۳^{۵-۱} \equiv ۶ \not\equiv ۱ \ (\text{به پیمانهٔ } ۲۵)$$

اینها ریشه‌های اولیهٔ $۵^۲$ و بنابراین ریشه‌های اولیهٔ همهٔ توانهای بالاتر ۵ هستند. اثبات فرع اخیر تضمین می‌کند که ۳ ریشهٔ اولیهٔ هر عدد به‌صورت ۲×۵^k است.

خلاصه مطالب بالا در قضیهٔ زیر می‌آید.

قضیهٔ ۸ـ۱۰ عدد صحیح $n > ۱$ ریشهٔ اولیه دارد اگر و تنها اگر

$$n = ۲, ۴, p^k, ۲p^k$$

که p عدد اول فردی است.

اثبات. بنابه قضیهٔ ۸ـ۷ و ۸ـ۸، تنها عددهای صحیح و مثبتی که ریشهٔ اولیه دارند عددهای مذکور در صورت این قضیه هستند. می‌توان تحقیق کرد که ۱ ریشهٔ اولیه‌ای از ۲، و ۳ ریشهٔ اولیه‌ای از ۴ است؛ و نیز ثابت کردیم که هر توانی از یک عدد فرد اول و دو برابر چنین توانی دارای ریشهٔ اولیه‌اند. □

اکنون بجاست گفته شود که اویلر در سال ۱۷۷۳ اثباتی اساساً درست (هر چند ناکامل) از وجود ریشهٔ اولیه برای هر عدد اول p ارائه کرد و ریشه‌های اولیهٔ همهٔ عددهای اول نابیشتر از ۳۷ را ذکر نمود. لژاندر با استفاده از قضیهٔ لاگرانژ، نقیصه را رفع کرد و نشان داد (در ۱۷۸۵) که به‌ازای هر $d|p-۱$، $\phi(d)$ عدد صحیح مرتبهٔ d وجود دارد. بزرگترین پیشرفتها در این زمینه وقتی حاصل شد که گاوس در ۱۸۰۱ اثباتی منتشر کرد که براساس آن، n دارای ریشهٔ اولیه است اگر و تنها اگر $n = ۲, ۴, p^k, ۲p^k$، که در آن p عدد اول فردی است.

تمرینهای ۸ـ۳

۱. (الف) چهار ریشهٔ اولیهٔ ۲۶ و هشت ریشهٔ اولیهٔ ۲۵ را به‌دست آورید.

(ب) همهٔ ریشه‌های اولیهٔ $۳^۲$، $۳^۳$ و $۳^۴$ را تعیین کنید.

۲. به‌ازای عدد اول فرد p، حکمهای زیر را ثابت کنید.

(الف) تعداد ریشه‌های اولیهٔ p^n و $۲p^n$ برابر است.

(ب) هر ریشهٔ اولیهٔ r از p^n ریشهٔ اولیه‌ای از p نیز هست [راهنمایی: فرض کنید k مرتبهٔ r به پیمانهٔ p باشد. نشان دهید $r^{pk} \equiv ۱$ (به پیمانهٔ $p^۲$)، ...، $r^{p^{n-۱}k} \equiv ۱$ (به پیمانهٔ p^n)، پس $\phi(p^n)|p^{n-۱}k$.]

(پ) اگر $n \geq ۲$، هر ریشهٔ اولیهٔ $p^۲$ ریشهٔ اولیه‌ای از p^n است.

۳. اگر p عددی فرد و اول و r ریشهٔ اولیه‌ای از $p^۲$ باشد، نشان دهید جوابهای همنهشتی $x^{p-۱} \equiv ۱$ (به پیمانهٔ $p^۲$) دقیقاً عددهای صحیح $r^p, r^{۲p}, \ldots, r^{(p-۱)p}$ هستند.

۴. (الف) ثابت کنید ۳ ریشهٔ اولیه‌ای از هر عدد صحیح به‌صورت ۷^k و ۲×۷^k است.

(ب) ریشهٔ اولیه‌ای از هر عدد صحیح به‌صورت ۱۷^k را به‌دست آورید.

۵. همهٔ ریشه‌های اولیهٔ ۴۱ و ۸۲ را پیدا کنید.

۶. (الف) اگر p عددی اول و فرد باشد، ثابت کنید ریشهٔ اولیهٔ r از p^k ریشهٔ اولیه‌ای از $۲p^k$ است اگر و تنها اگر r عدد صحیح فردی باشد.

(ب) نشان دهید ۳، $۳^۳$، $۳^۵$، و $۳^۹$ ریشه‌های اولیهٔ $۵۷۸ = ۲ \times ۱۷^۲$ هستند، ولی $۳^۷$ و $۳^{۱۱}$ نیستند.

۷. فرض کنید r ریشهٔ اولیه‌ای از عدد اول و فرد p باشد و $(r+tp)^{p-۱} \not\equiv ۱$ (به پیمانهٔ $p^۲$). نشان دهید به‌ازای هر $k \geq ۱$، $r+tp$ نیز ریشهٔ اولیه‌ای از p^k است.

۸. اگر $n = ۲^{k_۰}p_۱^{k_۱}p_۲^{k_۲}\ldots p_r^{k_r}$ تجزیهٔ $n > ۱$ به عاملهای اول باشد، نمای عمومی n، که با $\lambda(n)$ نشان داده می‌شود، چنین تعریف می‌شود

$$\lambda(n) = \operatorname{lcm}(\lambda(۲^{k_۰}), \phi(p_۱^{k_۱}), \ldots, \phi(p_r^{k_r}))$$

که در آن $\lambda(۲) = ۱$، $\lambda(۲^۲) = ۲$، و به‌ازای $k \geq ۳$، $\lambda(۲^k) = ۲^{k-۲}$. حکمهای زیر دربارهٔ نمای عمومی را ثابت کنید.

(الف) اگر $n = ۲, ۴, p^k, ۲p^k$ و p عددی فرد و اول باشد، $\lambda(n) = \phi(n)$.

(ب) اگر $\gcd(a, ۲^k) = ۱$، آنگاه $a^{\lambda(۲^k)} \equiv ۱$ (به پیمانهٔ ۲^k). [راهنمایی: از استقرا بر $k \geq ۳$ و اینکه $\lambda(۲^{k+۱}) = ۲\lambda(۲^k)$ استفاده کنید.]

(پ) اگر $\gcd(a, n) = ۱$، آنگاه $a^{\lambda(n)} \equiv ۱$ (به پیمانهٔ n). [راهنمایی: به‌ازای هر عامل p^k در n (p عددی اول است) داریم $a^{\lambda(n)} \equiv ۱$ (به پیمانهٔ p^k).]

۹. تحقیق‌کنیدکه به‌ازای $۱۲{,}۵۰۴۰ = ۲^۴ \times ۳^۲ \times ۵ \times ۷$، $\lambda(۵۰۴۰) = ۱۱۵۲$، و $\phi(۵۰۴۰)$.

۱۰. با استفاده از تمرین ۸ نشان دهید که اگر p عددی اول و فرد باشد و $n \neq ۲, ۴, p^k, ۲p^k$، آنگاه n ریشهٔ اولیه ندارد. [راهنمایی: بجز در حالتهای ۲، ۴، p^k، $۲p^k$ داریم $\lambda(n) | \phi(n)/۲$؛ پس اگر $\gcd(a, n) = ۱$، آنگاه $a^{\phi(n)/۲} \equiv ۱$ (به پیمانهٔ n).]

۱۱. (الف) ثابت کنید که اگر $\gcd(a, n) = ۱$، آنگاه همنهشتی خطی $ax \equiv b$ (به پیمانهٔ n) دارای جواب $x \equiv ba^{\lambda(n)-۱}$ (به پیمانهٔ n) است.

(ب) با استفاده از قسمت (الف)، همنهشتیهای $۱۳x \equiv ۲$ (به پیمانهٔ ۴۰) و $۳x = ۱۳$ (به پیمانهٔ ۷۷) را حل کنید.

۸ـ۴ نظریهٔ اندیسها

باقیماندهٔ این فصل دربارهٔ مفهومی جدید، یعنی، مفهوم اندیس است. فرض می‌کنیم n عددی صحیح باشد که ریشهٔ اولیه‌ای چون r دارد. چنانکه می‌دانیم، $\phi(n)$ توان نخست r یعنی

$$r, r^۲, \dots, r^{\phi(n)}$$

به ترتیبی، با عددهای صحیح کوچکتر از n و متباین با آن همنهشت به پیمانهٔ n اند. پس، اگر a عدد صحیح دلخواه متباینی با n باشد، آنگاه به‌ازای kی مناسبی، $۱ \leq k \leq \phi(n)$، a را می‌توان به‌صورت

$$a \equiv r^k \text{ (به پیمانهٔ } n)$$

نوشت. با این ملاحظات، تعریف زیر را داریم.

تعریف ۸ـ۳ فرض می‌کنیم r ریشهٔ اولیه‌ای از n باشد. اگر $\gcd(a, n) = ۱$، کوچکترین عدد صحیح مثبت k به‌طوری‌که $a \equiv r^k$ (به پیمانهٔ n)، اندیس a نسبت به r نامیده می‌شود.

معمولاً اندیس a نسبت به r با $\text{ind}_r a$ یا، درصورتی‌که بیم ابهام درکار نباشد، با $\text{ind}\ a$ نشان داده می‌شود. واضح است که $۱ \leq \text{ind}_r a \leq \phi(n)$ و

$$r^{\text{ind}_r a} \equiv a \text{ (به پیمانهٔ } n)$$

نماد $\text{ind}_r a$ وقتی با معنی است که $\gcd(a, n) = ۱$؛ درآینده، این نکته به‌طور ضمنی فرض می‌شود.

به‌عنوان مثال، عدد صحیح ۲ ریشهٔ اولیه‌ای از ۵ است و

$$۲^{۱} \equiv ۲, ۲^{۲} \equiv ۴, ۲^{۳} \equiv ۳, ۲^{۴} \equiv ۱ \text{ (به پیمانهٔ ۵)}$$

از اینجا نتیجه می‌شود

$$\text{ind}_{۲}۱ = ۴,\ \ \text{ind}_{۲}۲ = ۱,\ \ \text{ind}_{۲}۳ = ۳,\ \ \text{ind}_{۲}۴ = ۲$$

ملاحظه می‌کنیم که اندیسهایِ عددهای صحیحِ همنهشت به پیمانهٔ n، برابرند. بنابراین، به هنگام تنظیم جدولهای مقدارهای $\text{ind}a$، کافی است عددهای صحیح a ی کوچکتر از پیمانهٔ n و متباین با آن را درنظر گرفت. برای ملاحظهٔ درستی این نکته، فرض می‌کنیم a و b عددهای صحیحی متباین با n باشند و $a \equiv b$ (به پیمانهٔ n). چون $r^{\text{ind}\, a} \equiv a$ (به پیمانهٔ n) و $r^{\text{ind}\, b} \equiv b$ (به پیمانهٔ n)، داریم

$$r^{\text{ind}\, a} \equiv r^{\text{ind}\, b} \text{ (به پیمانهٔ } n)$$

پس، بنابه قضیهٔ ۸ـ۱، می‌توان نتیجه گرفت که $\text{ind}\, a \equiv \text{ind}\, b$ (به پیمانهٔ $\phi(n)$). بنابراین، با توجه به محدودیتهای تحمیلی بر اندازه‌های $\text{ind}\, a$ و $\text{ind}\, b$ داریم $\text{ind}\, a = \text{ind}\, b$.

اندیسها از قاعده‌هایی تبعیت می‌کنند که یادآور قاعده‌های لگاریتمهاست و ریشهٔ اولیه نقشی مشابه پایهٔ لگاریتم ایفا می‌کند.

قضیهٔ ۸ـ۱۱ اگر r ریشهٔ اولیه‌ای از n و $\text{ind}\ a$ اندیس a نسبت به r باشد، آنگاه

(۱) $\text{ind}(ab) \equiv \text{ind}\, a + \text{ind}\, b$ (به پیمانهٔ $\phi(n)$)

(۲) به‌ازای $k > ۰$، $\text{ind}\, a^k \equiv k\ \text{ind}\, a$ (به پیمانهٔ $\phi(n)$)

(۳) $\text{ind}۱ \equiv ۰$ (به پیمانهٔ $\phi(n)$)، $\text{ind}\, r \equiv ۱$ (به پیمانهٔ $\phi(n)$).

اثبات. بنابه تعریف اندیس، $r^{\text{ind}\, a} \equiv a$ (به پیمانهٔ n) و $r^{\text{ind}\, b} \equiv b$ (به پیمانهٔ n). با ضرب این همنهشتیها در یکدیگر، به‌دست می‌آوریم

$$r^{\text{ind}a+\text{ind}b} \equiv ab \text{ (به پیمانهٔ } n)$$

ولی $r^{\text{ind}(ab)} \equiv ab$ (به پیمانهٔ n)، پس

$$r^{\text{ind}\, a+\text{ind}\, b} \equiv r^{\text{ind}(ab)} \text{ (به پیمانهٔ } n)$$

کاملاً محتمل است که $\operatorname{ind} a + \operatorname{ind} b$ بزرگتر از $\phi(n)$ باشد. این امر مشکلی ایجاد نمی‌کند، زیرا بنابه قضیهٔ ۸ـ۱، معادلهٔ آخری وقتی و فقط وقتی برقرار است که نماها همنهشت به پیمانهٔ $\phi(n)$ باشند، یعنی

$$\operatorname{ind} a + \operatorname{ind} b \equiv \operatorname{ind}(ab) \ (\text{به پیمانهٔ } \phi(n))$$

اثبات ویژگی (۲) کم و بیش مشابه اثبات بالاست، زیرا داریم (به پیمانهٔ n) $r^{\operatorname{ind} a^k} \equiv a^k$ درحالی‌که، بنابه قانونهای توانها، (به پیمانهٔ n) $r^{k \operatorname{ind} a} \equiv (r^{\operatorname{ind} a})^k \equiv a^k$؛ پس

$$r^{\operatorname{ind} a^k} \equiv r^{k \operatorname{ind} a} \ (\text{به پیمانهٔ } n)$$

لذا، مانند فوق، نتیجه می‌گیریم (به پیمانهٔ $\phi(n)$) $\operatorname{ind} a^k \equiv k \operatorname{ind} a$. دو بخش (۳) بدیهی‌اند. □

نظریهٔ اندیسها را می‌توان برای حل گونه‌های خاصی از معادله‌های همنهشتی به‌کار برد. به‌عنوان نمونه، همنهشتی دوجمله‌ای

$$x^k \equiv a \ (\text{به پیمانهٔ } n), \qquad k \geq ۲$$

را که در آن n عددی صحیح مثبت با ریشه‌ای اولیه است و $\gcd(a, n) = ۱$، در نظر می‌گیریم. این همنهشتی، بنابه ویژگیهای (۱) و (۲) از قضیهٔ ۸ـ۱۱ هم‌ارز با همنهشتی خطی

$$k \operatorname{ind} x \equiv \operatorname{ind} a \ (\text{به پیمانهٔ } \phi(n))$$

نسبت به مجهول $\operatorname{ind} x$ است. اگر $d = \gcd(k, \phi(n))$ و $d \nmid \operatorname{ind} a$، جوابی وجود ندارد. ولی اگر $d | \operatorname{ind} a$، آنگاه دقیقاً d مقدار برای $\operatorname{ind} x$ وجود دارند که در همنهشتی آخری صدق می‌کنند، یعنی، معادلهٔ (به پیمانهٔ n) $x^k \equiv a$ دقیقاً دارای d جواب ناهمنهشت است.

حالت $k = ۲$ و $n = p$، وقتی که p عدد اول فردی است، اهمیت ویژه‌ای دارد. چون $\gcd(۲, p - ۱) = ۲$، بنابه نکته‌های اخیرالذکر، همنهشتی (به پیمانهٔ p) $x^۲ \equiv a$ جواب دارد اگر و تنها اگر $۲ | \operatorname{ind} a$؛ اگر این شرط برقرار باشد، دقیقاً دو جواب وجود دارد. اگر r ریشه‌ای اولیه از p باشد، آنگاه r^k ($۱ \leq k \leq p - ۱$)، به ترتیبی، عددهای صحیح $۱, ۲, \ldots, p - ۱$ را اختیار می‌کند. توانهای زوج r مقدارهای aای تولید می‌کنند که به‌ازای آنها همنهشتی (به پیمانهٔ p) $x^۲ \equiv a$ حلپذیر است؛ a را دقیقاً به $(p - ۱)/۲$ طریق مختلف می‌توان انتخاب کرد.

مثال ۸ـ۴

به‌عنوان مثالی برای روشن شدن این مفهومها، همنهشتی

$$۴x^۹ \equiv ۷ \text{ (به پیمانهٔ ۱۳)}$$

را حل می‌کنیم. همین‌که ریشهٔ اولیه‌ای از ۱۳ تعیین شود، می‌توان جدولی متشکل از اندیسها تهیه کرد. با استفاده از ریشهٔ اولیهٔ ۲، توانهای $۲, ۲^۲, \ldots, ۲^{۱۲}$ به پیمانهٔ ۱۳ را حساب می‌کنیم. به پیمانهٔ ۱۳ داریم

$$\begin{array}{lll} ۲^۱ \equiv ۲ & ۲^۵ \equiv ۶ & ۲^۹ \equiv ۵ \\ ۲^۲ \equiv ۴ & ۲^۶ \equiv ۱۲ & ۲^{۱۰} \equiv ۱۰ \\ ۲^۳ \equiv ۸ & ۲^۷ \equiv ۱۱ & ۲^{۱۱} \equiv ۷ \\ ۲^۴ \equiv ۳ & ۲^۸ \equiv ۹ & ۲^{۱۲} \equiv ۱ \end{array}$$

و بنابراین جدول ما عبارت است از

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
$\text{ind}_۲ a$	۱۲	۱	۴	۲	۹	۵	۱۱	۳	۸	۱۰	۷	۶

با اندیس‌گیری می‌بینیم که همنهشتی $۴x^۹ \equiv ۷$ (به پیمانهٔ ۱۳) جواب دارد اگر و تنها اگر

$$\text{ind}_۲ ۴ + ۹\,\text{ind}_۲ x \equiv \text{ind}_۲ ۷ \text{ (به پیمانهٔ ۱۲)}$$

با توجه به جدول، $\text{ind}_۲ ۴ = ۲$، $\text{ind}_۲ ۷ = ۱۱$، و معادلهٔ آخری به‌صورت $۹\,\text{ind}_۲ x \equiv ۱۱ - ۲ \equiv ۹$ (به پیمانهٔ ۱۲) ساده می‌شود، و این خود با $\text{ind}_۲ x \equiv ۱$ (به پیمانهٔ ۴) هم‌ارز است. نتیجه می‌شود

$$\text{ind}_۲ x = ۱, ۵, \text{ یا } ۹$$

با مراجعهٔ دوباره به جدول اندیسها، ملاحظه می‌کنیم که همنهشتی $۴x^۹ \equiv ۷$ (به پیمانهٔ ۱۳) دارای سه جواب

$$x \equiv ۲, ۵, ۶ \text{ (به پیمانهٔ ۱۳)}$$

است.

اگر ریشهٔ اولیهٔ متفاوتی انتخاب شود، به‌وضوح مقدار متفاوتی برای اندیس a به‌دست می‌آید؛ ولی برای حل همنهشتی داده شده، مهم نیست از کدام جدول اندیسها استفاده کنیم. تعداد $\phi(\phi(۱۳)) = ۴$ ریشهٔ اولیهٔ ۱۳ به‌صورت $۲^k \; (۱ \le k \le ۱۲)$اند به‌طوری‌که

$$\gcd(k, \phi(۱۳)) = \gcd(k, ۱۲) = ۱$$

اینها عبارت‌اند از

$$۲^۱ \equiv ۲, ۲^۵ \equiv ۶, ۲^۷ \equiv ۱۱, ۲^{۱۱} \equiv ۷ \; (\text{به پیمانهٔ } ۱۳)$$

جدول اندیس به‌ازای، مثلاً، ریشهٔ اولیهٔ ۶ در زیر ملاحظه می‌شود

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
$\mathrm{ind}_۶ a$	۱۲	۵	۸	۱۰	۹	۱	۷	۳	۴	۲	۱۱	۶

با استفاده از این جدول، همنهشتی $۴x^۹ \equiv ۷ \; (\text{به پیمانهٔ } ۱۳)$ که با

$$\mathrm{ind}_۶ ۴ + ۹ \; \mathrm{ind}_۶ x \equiv \mathrm{ind}_۶ ۷ \; (\text{به پیمانهٔ } ۱۲)$$

هم‌ارز است، به‌صورت سادهٔ

$$۹ \; \mathrm{ind}_۶ x \equiv ۷ - ۱۰ \equiv -۳ \equiv ۹ \; (\text{به پیمانهٔ } ۱۲)$$

در می‌آید. بنابراین، $\mathrm{ind}_۶ x = ۱, ۵,$ یا ۹، و بنابراین جوابهای

$$x \equiv ۲, ۵, ۶ (\text{به پیمانهٔ } ۱۳)$$

حاصل می‌شوند که همان جوابهای قبلی‌اند. ■

معیار حلپذیری زیر اغلب سودمند است.

قضیهٔ ۸ـ۱۲ فرض می‌کنیم n عدد صحیحی با ریشه‌ای اولیه باشد و $\gcd(a, n) = ۱$. در این صورت همنهشتی $x^k \equiv a \; (\text{به پیمانهٔ } n)$ جواب دارد اگر و تنها اگر

$$a^{\frac{\phi(n)}{d}} \equiv ۱ \; (\text{به پیمانهٔ } n)$$

که در آن $d = \gcd(k, \phi(n))$؛ و اگر جوابی داشته باشد، دقیقاً d جواب به پیمانهٔ n دارد.

اثبات. با اندیس‌گیری می‌بینیم که همنهشتی $a^{\phi(n)/d} \equiv ۱$ (به پیمانهٔ n) هم‌ارز با

$$\frac{\phi(n)}{d}\operatorname{ind} a \equiv ۰ \ (\text{به پیمانهٔ } \phi(n))$$

است که این برقرار است اگر و تنها اگر $d|\operatorname{ind} a$. پیشتر دیده‌ایم که این شرط لازم و کافی برای حلپذیری همنهشتی $x^k \equiv a$ (به پیمانهٔ n) است. □

فرع (اویلر). فرض می‌کنیم p عددی اول باشد و $\gcd(a, p) = ۱$. در این صورت همنهشتی $x^k \equiv a$ (به پیمانهٔ p) جواب دارد اگر و تنها اگر $a^{(p-۱)/d} \equiv ۱$ (به پیمانهٔ p)، که در آن $d = \gcd(k, p-۱)$.

مثال ۸ـ۵

همنهشتی

$$x^۳ \equiv ۴ \ (\text{به پیمانهٔ } ۱۳)$$

را درنظر می‌گیریم. داریم $d = \gcd(۳, \phi(۱۳)) = \gcd(۳, ۱۲) = ۳$ وبنابراین $\phi(۱۳)/d = ۴$. چون $۴^۴ \equiv ۹ \not\equiv ۱$ (به پیمانهٔ ۱۳)، بنابه قضیهٔ ۸ـ۱۲، همنهشتی داده‌شده حلپذیر نیست.

ولی قضیهٔ مزبور تضمین می‌کند که

$$x^۳ \equiv ۵ \ (\text{به پیمانهٔ } ۱۳)$$

جواب دارد (درواقع، سه جواب ناهمنهشت به پیمانهٔ ۱۳ دارد) زیرا، در این مورد، $۵^۴ \equiv ۶۲۵ \equiv ۱$ (به پیمانهٔ ۱۳). این جوابها را می‌توان به شرح زیر با استفاده از حساب اندیسها به‌دست آورد: همنهشتی $x^۳ \equiv ۵$ (به پیمانهٔ ۱۳) هم‌ارز با

$$۳\operatorname{ind}_۲ x \equiv ۹ \ (\text{به پیمانهٔ } ۱۲)$$

است که این هم به‌صورت

$$\operatorname{ind}_۲ x \equiv ۳ \ (\text{به پیمانهٔ } ۴)$$

در می‌آید. معادلهٔ اخیر سه جواب ناهمنهشت به پیمانهٔ ۱۲ دارد، یعنی

$$\operatorname{ind}_۲ x \equiv ۳, ۷, \text{ یا } ۱۱$$

عددهای صحیح متناظر با این اندیسها، به‌ترتیب، عبارت‌اند از ۸، ۱۱، ۷، بنابراین

$$x \equiv 7, 8, 11 \quad (\text{به پیمانهٔ } 13)$$

تنها جوابهای همنهشتی $x^2 \equiv 5$ (به پیمانهٔ ۱۳) هستند. ■

تمرینهای ۸ـ۴

۱. اندیس ۵ را نسبت به هر یک از ریشه‌های اولیهٔ ۱۳ پیدا کنید.

۲. با استفاده از جدول اندیسهایی به‌ازای ریشهٔ اولیه‌ای از ۱۱، همنهشتیهای

(الف) $7x^3 \equiv 3$ (به پیمانهٔ ۱۱)

(ب) $3x^4 \equiv 5$ (به پیمانهٔ ۱۱)

(پ) $x^8 \equiv 10$ (به پیمانهٔ ۱۱)

را حل کنید.

۳. در زیر، جدولی از اندیسها برای عدد اول ۱۷ نسبت به ریشهٔ اولیهٔ ۳ ملاحظه می‌شود:

a	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶
$\operatorname{ind}_3 a$	۱۶	۱۴	۱	۱۲	۵	۱۵	۱۱	۱۰	۲	۳	۷	۱۳	۴	۹	۶	۸

با استفاده از این جدول، همنهشتیهای زیر را حل کنید:

(الف) $x^{12} \equiv 13$ (به پیمانهٔ ۱۷)، (ب) $8x^5 \equiv 10$ (به پیمانهٔ ۱۷)

(پ) $9x^8 \equiv 8$ (به پیمانهٔ ۱۷)، (ت) $7^x \equiv 7$ (به پیمانهٔ ۱۷)

۴. باقیماندهٔ تقسیم $5^{13} \times 3^{24}$ بر ۱۷ را تعیین کنید. [راهنمایی: از نظریهٔ اندیسها استفاده کنید.]

۵. اگر r و r' ریشه‌های اولیه‌ای از عدد اول فرد p باشند، نشان دهید که به‌ازای هر عدد صحیح a که $\gcd(a, p) = 1$،

$$\operatorname{ind}_{r'} a \equiv (\operatorname{ind}_r a)(\operatorname{ind}_{r'} r) \quad (\text{به پیمانهٔ } p - 1)$$

این متناظر با قاعدهٔ تغییر پایهٔ لگاریتمهاست.

۶. (الف) جدولی از اندیسها برای عدد اول ۱۷ نسبت به ریشهٔ اولیهٔ ۵ تشکیل دهید. [راهنمایی: بنابه تمرین پیشین، $\operatorname{ind}_5 a \equiv 13 \operatorname{ind}_3 a$ (به پیمانهٔ ۱۶).]

(ب) با استفاده از جدول بخش (الف)، همنهشتیهای تمرین ۳ را حل کنید.

۷. اگر r ریشه‌ای اولیه از عدد اول فرد p باشد، نشان دهید که

$$\text{ind}_r(-۱) = \text{ind}_r(p-۱) = \frac{۱}{۲}(p-۱)$$

۸. (الف) عددهای صحیح $a (۱ \leq a \leq ۱۲)$ را طوری تعیین کنید که همنهشتی $ax^۴ \equiv b$ (به پیمانهٔ ۱۳) جوابی به‌ازای $b = ۲, ۵, ۶$ داشته باشد.

(ب) عددهای صحیح $a (۱ \leq a \leq p-۱)$ را طوری پیدا کنید که همنهشتی $x^۴ \equiv a$ (به پیمانهٔ p) جوابی به‌ازای $p = ۷, ۱۱, ۱۳$ داشته باشد.

۹. با استفاده از فرع قضیهٔ ۸ـ۱۲ نشان دهید که اگر p عدد اول فردی باشد، آنگاه

(الف) $x^۲ \equiv -۱$ (به پیمانهٔ p) حلپذیر است اگر و تنها اگر $p \equiv ۱$ (به پیمانهٔ ۴)؛

(ب) $x^۴ \equiv -۱$ (به پیمانهٔ p) حلپذیر است اگر و تنها اگر $p \equiv ۱$ (به پیمانهٔ ۸).

۱۰. همنهشتی $x^۳ \equiv a$ (به پیمانهٔ p) را که در آن $p \geq ۵$ عددی اول است و $\gcd(a,p) = ۱$، درنظر بگیرید. نشان دهید که

(الف) اگر $p \equiv ۱$ (به پیمانهٔ ۶)، همنهشتی یا دارای جواب نیست یا سه جواب ناهمنهشت به پیمانهٔ p دارد.

(ب) اگر $p \equiv ۵$ (به پیمانهٔ ۶)، همنهشتی جواب یکتایی به پیمانهٔ p دارد.

۱۱. نشان دهید همنهشتی $x^۳ \equiv ۳$ (به پیمانهٔ ۱۹) جواب ندارد، ولی $x^۳ \equiv ۱۱$ (به پیمانهٔ ۱۹) سه جواب ناهمنهشت دارد.

۱۲. تعیین کنید کدام یک از همنهشتیهای $x^۵ \equiv ۱۳$ (به پیمانهٔ ۲۳) و $x^۷ \equiv ۱۵$ (به پیمانهٔ ۲۹) حلپذیر است.

۱۳. اگر p عددی اول باشد و $\gcd(k, p-۱) = ۱$، ثابت کنید عددهای صحیح

$$۱^k, ۲^k, ۳^k, \ldots, (p-۱)^k$$

مجموعهٔ تقلیل یافته‌ای از مانده‌ها به پیمانهٔ p تشکیل می‌دهند.

۱۴. فرض می‌کنیم r ریشه‌ای اولیه از عدد اول فرد p باشد و $d = \gcd(k,\ p-۱)$. ثابت کنید $r^d, r^{۲d}, \ldots, r^{[(p-۱)/d]d}$ تنها مقدارهای a هستند که به‌ازای آنها همنهشتی $x^k \equiv a$ (به پیمانهٔ p) حلپذیر است.

۱۵. اگر r ریشه‌ای اولیه از عدد اول فرد p باشد، نشان دهید

$$\text{ind}_r(p-a) \equiv \text{ind}_r a + \frac{p-۱}{۲} \quad (\text{به پیمانهٔ } p-۱)$$

بنابراین، محاسبهٔ فقط نصف جدول اندیسها برای تکمیل جدول کافی است.

۱۶. (الف) فرض می‌کنیم r ریشه‌ای اولیه از عدد اول فرد p باشد. نشان دهید همنهشتی نمایی

$$a^x \equiv b \text{ (به پیمانهٔ } p)$$

جواب دارد اگر و تنها اگر $d|\text{ind}_r b$، که در آن $d = \gcd(\text{ind}_r a, p-1)$؛ در این حالت، d جواب ناهمنهشت به پیمانهٔ p وجود دارد.

(ب) همنهشتیهای نمایی $4^x \equiv 13$ (به پیمانهٔ ۱۷) و $5^x \equiv 4$ (به پیمانهٔ ۱۹) را حل کنید.

۱۷. به‌ازای چه مقدارهای b همنهشتی نمایی $9^x \equiv b$ (به پیمانهٔ ۱۳) حلپذیر است؟

۹

قانون تقابل درجهٔ دوم

«نیروی محرّکهٔ ابداع ریاضی استدلال نیست،
تخیل است.»

ا. دِمورگن

۹ـ۱ معیار اویلر

همان‌طور که از عنوان فصل برمی‌آید، هدف این گفتار تشریح دستاورد مهم دیگری از گاوس یعنی قانون تقابل درجهٔ دوم است. از دید کسانی که نظریّهٔ اعداد را «ملکهٔ ریاضیات» به حساب می‌آورند، این یکی از گوهرهای تاج اوست. زیبایی ذاتی قانون تقابل درجهٔ دوم مدتهای مدید جاذبهٔ غریبی برای ریاضیدانان داشته است. از زمان گاوس، بیش از یک صد اثبات کم و بیش متفاوت برای این قانون انتشار یافته است (درواقع، خود گاوس هفت اثبات ارائه کرد). در میان ریاضیدانان برجستهٔ سدهٔ نوزدهمی که اثباتی ارائه کردند، نامهایی چون کوشی، ژاکوبی، دیریکله، آیزنشتاین، کرونکر، و ددکیند دیده می‌شود.

اجمالاً می‌توان گفت که قانون تقابل درجهٔ دوم به حلپذیری همنهشتیهای درجهٔ دوم مربوط می‌شود. بنابراین مناسب به‌نظر می‌رسد بحث را با بررسی همنهشتی

$$ax^{2} + bx + c \equiv 0 \pmod{p} \qquad (1)$$

آغاز کنیم، که در آن p عددی فرد اول است و $a \not\equiv ۰$ (به پیمانهٔ p)؛ یعنی $\gcd(a,p) = ۱$. از این فرض که p عدد اول فردی است، نتیجه می‌گیریم $\gcd(۴a,p) = ۱$. بنابراین، همنهشتی (۱) هم‌ارز با

$$۴a(ax^۲ + bx + c) \equiv ۰ \ (\text{به پیمانهٔ } p)$$

است. با استفاده از اتحاد

$$۴a(ax^۲ + bx + c) = (۲ax + b)^۲ - (b^۲ - ۴ac)$$

همنهشتی اخیر را می‌توان به‌صورت

$$(۲ax + b)^۲ \equiv (b^۲ - ۴ac) \ (\text{به پیمانهٔ } p)$$

نوشت. با قرار دادن $y = ۲ax + b$ و $d = b^۲ - ۴ac$ به‌دست می‌آوریم

$$y^۲ \equiv d \ (\text{به پیمانهٔ } p) \qquad (۲)$$

اگر $x \equiv x_۰$ (به پیمانهٔ p) جوابی از (۱) باشد، آنگاه $y \equiv ۲ax_۰ + b$ (به پیمانهٔ p) در همنهشتی (۲) صدق می‌کند. برعکس، اگر $y \equiv y_۰$ (به‌پیمانهٔ p) جوابی از (۲) باشد، آنگاه با حل $۲ax \equiv y_۰ - b$ (به پیمانهٔ p) جوابی از (۱) به‌دست می‌آید.

بنابراین، مسألهٔ تعیین جوابی برای همنهشتی درجهٔ دوم (۱) معادل است با تعیین جوابی برای یک همنهشتی خطی و همنهشتی درجهٔ دومی به‌صورت

$$x^۲ \equiv a \ (\text{به پیمانهٔ } p) \qquad (۳)$$

اگر $p|a$، آنگاه $x \equiv ۰$ (به پیمانهٔ p) تنها جواب (۳) است. برای پرهیز از حالتهای بدیهی، فرض می‌کنیم که از این به بعد $p \nmid a$.

با قبول این، هرگاه $x = x_۰$ جوابی از $x^۲ \equiv a$ (به پیمانهٔ p) باشد، $x = p - x_۰$ جواب دیگری از آن است. این جواب دوم با اولی همنهشت نیست زیرا از $x_۰ \equiv p - x_۰$ (به پیمانهٔ p) نتیجه می‌شود $۲x_۰ \equiv ۰$ (به پیمانهٔ p)، یا $x_۰ \equiv ۰$ (به پیمانهٔ p)، که غیرممکن است. این دو جواب، بنا به قضیهٔ لاگرانژ، تنها جوابهای ناهمنهشت $x^۲ \equiv a$ (به پیمانهٔ p) هستند. به‌طور خلاصه، $x^۲ \equiv a$ (به پیمانهٔ p) یا فاقد جواب است، یا دقیقاً دو جواب دارد.

به‌عنوان مثال عددی ساده‌ای از مطلب فوق، همنهشتی

$$۵x^۲ - ۶x + ۲ \equiv ۰ \ (\text{به پیمانهٔ } ۱۳)$$

را درنظر می‌گیریم. برای تعیین جواب، به‌جای این همنهشتی، همنهشتی ساده‌تر

$$y^{۲} \equiv ۹ \text{ (به پیمانهٔ ۱۳)}$$

را که دارای جوابهای (به پیمانهٔ ۱۳) $y \equiv ۳, ۱۰$ است، به‌کار می‌گیریم. سپس، همنهشتیهای خطی

$$۱۰x \equiv ۹ \text{ (به پیمانهٔ ۱۳)}،\quad ۱۰x \equiv ۱۶ \text{ (به پیمانهٔ ۱۳)}$$

را حل می‌کنیم. به آسانی می‌توان ملاحظه کرد که (به پیمانهٔ ۱۳) $x \equiv ۱۰, ۱۲$ در این معادله‌ها و همچنین، با توجه به تذکرهای پیشین، در همنهشتی درجه دوم اصلی صدق می‌کنند.

کار اصلی ما در اینجا، تدارک آزمونی برای وجود جوابهای همنهشتی

$$\gcd(a,p) = ۱ \text{ ، } x^{۲} \equiv a \text{ (به پیمانهٔ } p) \qquad (۴)$$

است. به بیان دیگر، می‌خواهیم عددهای صحیح aای را که (به پیمانهٔ p) مربع کامل هستند، شناسایی کنیم. استفاده از چند اصطلاح اضافی، بحث فشرده دربارهٔ این وضعیت را ممکن می‌سازد.

تعریف ۹ـ۱ فرض می‌کنیم p عدد اول فردی باشد و $\gcd(a,p) = ۱$. اگر همنهشتی (به پیمانهٔ p) $x^{۲} \equiv a$ جوابی داشته باشد، آنگاه a ماندهٔ درجهٔ دوم p نامیده می‌شود. در غیر این صورت، a را ناماندهٔ درجهٔ دوم p می‌نامند.

باید در نظر داشت که اگر (به پیمانهٔ p) $a \equiv b$، a ماندهٔ درجهٔ دومی از p است اگر و تنها اگر b ماندهٔ درجهٔ دومی از p باشد.

بنابراین، برای تعیین اینکه یک عدد صحیح دلخواه، ماندهٔ درجه دومی از p هست یا نه، کافی است تکلیف عددهای صحیح مثبت کوچکتر از p را از این لحاظ معلوم کنیم.

مثال ۹ـ۱

حالتِ عدد اول $p = ۱۳$ را درنظر می‌گیریم. برای تعیین اینکه چه تعداد از عددهای صحیح ۱، ۲، ۳، . . .، ۱۲ مانده‌های درجه دومی از ۱۳ هستند، باید بدانیم کدام یک از همنهشتیهای

$$x^{۲} \equiv a \text{ (به پیمانهٔ ۱۳)}$$

وقتی a بر مجموعهٔ $\{۱،۲، \ldots ، ۱۲\}$ تغییر می‌کند، حلپذیرند. توانهای دوم عددهای صحیح ۱،۲،۳،...،۱۲ به پیمانهٔ ۱۳ عبارت‌اند از

$$۱^۲ \equiv ۱۲^۲ \equiv ۱$$
$$۲^۲ \equiv ۱۱^۲ \equiv ۴$$
$$۳^۲ \equiv ۱۰^۲ \equiv ۹$$
$$۴^۲ \equiv ۹^۲ \equiv ۳$$
$$۵^۲ \equiv ۸^۲ \equiv ۱۲$$
$$۶^۲ \equiv ۷^۲ \equiv ۱۰$$

درنتیجه، مانده‌های درجهٔ دوم ۱۳ عبارت‌اند از ۱، ۳، ۴، ۹، ۱۰، ۱۲، و نامانده‌ها عبارت‌اند از ۲، ۵، ۶، ۷، ۸، ۱۱. ملاحظه می‌کنیم عددهای صحیح میان ۱ و ۱۲ به‌طور مساوی میان مانده‌های درجهٔ دوم و نامانده‌ها توزیع شده‌اند؛ این نمونه‌ای از وضعیت کلی است. ■

اویلر معیار ساده‌ای برای تعیین اینکه آیا عدد صحیح a ماندهٔ درجهٔ دوم عدد اول داده‌شده‌ای چون p هست یا نه، ابداع کرد.

قضیهٔ ۹ـ۱ (معیار اویلر). فرض می‌کنیم p عدد اول فردی باشد و $\gcd(a,p) = ۱$. در این صورت، a ماندهٔ درجهٔ دومی از p است اگر و تنها اگر $a^{(p-۱)/۲} \equiv ۱$ (به پیمانهٔ p).

اثبات. فرض می‌کنیم a ماندهٔ درجهٔ دومی از p باشد؛ در این صورت $x^۲ \equiv a$ (به پیمانهٔ p) جوابی دارد که آن را $x_۱$ می‌نامیم. چون $\gcd(a,p) = ۱$، به وضوح $\gcd(x_۱,p) = ۱$. بنابراین با توسّل به قضیهٔ فرما داریم

$$a^{(p-۱)/۲} \equiv (x_۱^۲)^{(p-۱)/۲} \equiv x_۱^{p-۱} \equiv ۱ \ (\text{به پیمانهٔ } p)$$

حال برعکس فرض می‌کنیم $a^{(p-۱)/۲} \equiv ۱$ (به پیمانهٔ p) برقرار است و r ریشه‌ای اولیه از p است. در این صورت به‌ازای عدد صحیح kای، $۱ \le k \le p-۱$، $a \equiv r^k$ (به پیمانهٔ p). نتیجه می‌گیریم که

$$r^{k(p-۱/۲)} \equiv a^{(p-۱)/۲} \equiv ۱ \ (\text{به پیمانهٔ } p)$$

بنابه قضیهٔ ۸ـ۱، مرتبهٔ r (یعنی، $p-۱$) باید نمای $k(p-۱)/۲$ را بشمارد. درنتیجه k عددی صحیح و زوج است، مثلاً $k = ۲j$. پس

$$(r^j)^۲ = r^{۲j} = r^k \equiv a \text{ (به پیمانهٔ } p)$$

و بنابراین r^j جوابی از همنهشتی $x^۲ \equiv a$ (به پیمانهٔ p) است. یعنی a ماندهٔ درجه دومی از عدد اول p است. □

اکنون اگر p (مانند همیشه) عدد اول فردی باشد و $\gcd(a,p) = ۱$، آنگاه بنابه قضیهٔ فرما داریم

$$(a^{(p-۱)/۲} - ۱)(a^{(p-۱)/۲} + ۱) = a^{p-۱} - ۱ \equiv ۰ \text{ (به پیمانهٔ } p)$$

پس یا $a^{(p-۱)/۲} \equiv ۱$ (به پیمانهٔ p) یا $a^{(p-۱)/۲} \equiv -۱$ (به پیمانهٔ p)، ولی هر دو باهم برقرار نیستند زیرا اگر هردو همنهشتی همزمان برقرار باشند، لازم می‌آید داشته باشیم $۱ \equiv -۱$ (به پیمانهٔ p)، یا معادلش $p|۲$، که با فرض ما ناسازگار است. چون ناماندهٔ درجهٔ دوم p در $a^{(p-۱)/۲} \equiv ۱$ (به پیمانهٔ p) صدق نمی‌کند، بنابراین باید در $a^{(p-۱)/۲} \equiv -۱$ (به پیمانهٔ p) صدق کند. با توجه به این امر، معیار اویلر را می‌توان به‌صورت زیر نیز بیان کرد: عدد صحیح a ناماندهٔ درجه دومی از p است اگر و تنها اگر $a^{(p-۱)/۲} \equiv -۱$ (به پیمانهٔ p).

با تلفیق نتیجه‌های فوق داریم:

فرع. فرض می‌کنیم p عدد اول فردی باشد و $\gcd(a,p) = ۱$. در این صورت a ماندهٔ درجه دومی از p یا ناماندهٔ درجه دومی از آن است اگر، به‌ترتیب،

$$a^{(p-۱)/۲} \equiv ۱ \text{ (به پیمانهٔ } p) \quad \text{یا} \quad a^{(p-۱)/۲} \equiv -۱ \text{ (به پیمانهٔ } p)$$

مثال ۹ـ۲

در حالت $p = ۱۳$ ملاحظه می‌کنیم که

$$۲^{(۱۳-۱)/۲} = ۲^۶ = ۶۴ \equiv ۱۲ \equiv -۱ \text{ (به پیمانهٔ } ۱۳)$$

بنابراین، باتوجه به فرع اخیر، عدد صحیح ۲ یک ناماندهٔ درجهٔ دوم ۱۳ است. چون

$$۳^{(۱۳-۱)/۲} = ۳^۶ = (۲۷)^۲ \equiv ۱^۲ \equiv ۱ \text{ (به پیمانهٔ } ۱۳)$$

طبق همان فرع، ۳ ماندهٔ درجهٔ دومی از ۱۳ است و بنابراین (به پیمانهٔ ۱۳) ۳ $\equiv x^۲$ حلپذیر است؛ درواقع، دو جواب ناهمنهشت آن عبارت‌اند از (به پیمانهٔ ۱۳) ۹ ,۴ $\equiv x$. ■

اثبات دیگری از معیار اویلر (منسوب به دیریکله) وجود دارد که گرچه طولانیتر است، ولی شاید روشنگرتر باشد. اثبات به این شرح است: فرض می‌کنیم a نامانده‌ای درجهٔ دوم از p و c یکی از عددهای صحیح ۱، ۲، ...، $p-۱$ باشد. بنابه نظریهٔ همنهشتیهای خطی، (به پیمانهٔ p) $cx \equiv a$ دارای جواب c' امی است به‌طوری‌که c' نیز عضوی از مجموعهٔ $\{۱،۲،\ldots،p-۱\}$ است. توجه کنید که $c' \neq c$، وگرنه (به پیمانهٔ p) $c^۲ \equiv a$، که متناقض با فرضی است که کرده‌ایم. بنابراین، عددهای صحیح میان ۱ و $p-۱$ را می‌توان به $(p-۱)/۲$ جفت c، c' تقسیم کرد به‌طوری‌که (به پیمانهٔ p) $cc' \equiv a$. به این ترتیب $(p-۱)/۲$ همنهشتی

$$c_۱c'_۱ \equiv a \ (\text{به پیمانهٔ } p)$$

$$c_۲c'_۲ \equiv a \ (\text{به پیمانهٔ } p)$$

$$\vdots$$

$$c_{(p-۱)/۲}c'_{(p-۱)/۲} \equiv a \ (\text{به پیمانهٔ } p)$$

به‌دست می‌آیند. با ضرب اینها در هم و ملاحظهٔ اینکه حاصلضرب

$$c_۱c'_۱c_۲c'_۲\ldots c_{(p-۱)/۲}c'_{(p-۱)/۲}$$

همان $(p-۱)\ldots×۳×۲×۱$ با ترتیبی متفاوت است، به‌دست می‌آوریم

$$(p-۱)! \equiv a^{(p-۱)/۲} \ (\text{به پیمانهٔ } p)$$

اینجاست که قضیهٔ ویلسن پا به صحنه می‌گذارد زیرا (به پیمانهٔ p) $(p-۱)! \equiv -۱$، و بنابراین

$$a^{(p-۱)/۲} \equiv -۱ \ (\text{به پیمانهٔ } p)$$

که همان معیار اویلر است برای اینکه a ناماندهٔ درجه دومی از p باشد.

اکنون حالتی را که a ماندهٔ درجه دومی از p باشد، بررسی می‌کنیم. در این حالت به‌ازای $x_۱$ای، $۱ \leq x_۱ \leq p-۱$، همنهشتی (به پیمانهٔ p) $x^۲ \equiv a$ دارای دو جواب $x = x_۱$ و $x = p - x_۱$ است. اگر $x_۱$ و $p - x_۱$ از مجموعهٔ $\{۱, ۲, \ldots, p-۱\}$ حذف شوند، $p-۳$

عدد صحیح باقیمانده را می‌توان به‌صورت جفتهای c, c' (که $c \neq c'$) طوری دسته‌بندی کرد که $cc' \equiv a$ (به پیمانهٔ p). همنهشتی

$$x_1(p - x_1) \equiv -x_1^2 \equiv -a \ (\text{به پیمانهٔ } p)$$

را به این $(p - 3)/2$ همنهشتی اضافه می‌کنیم. با ضرب کردن همنهشتیهای فوق در یکدیگر، به‌دست می‌آوریم

$$(p - 1)! \equiv -a^{(p-1)/2} \ (\text{به پیمانهٔ } p)$$

که با استفادهٔ درباره از قضیهٔ ویلسن نتیجه می‌شود

$$a^{(p-1)/2} \equiv 1 \ (\text{به پیمانهٔ } p)$$

مطالب بالا را جمعبندی می‌کنیم: نشان داده‌ایم که برحسب اینکه a مانده‌ای درجهٔ دوم یا نامانده‌ای درجهٔ دوم از p باشد، آنگاه، به‌ترتیب، (به پیمانهٔ p) $a^{(p-1)/2} \equiv 1$ یا $a^{(p-1)/2} \equiv -1$.

معیار اویلر به‌عنوان آزمونی عملی برای تعیین اینکه عدد صحیح داده‌شده‌ای مانده درجهٔ دوم است یا نه، توصیه نمی‌شود؛ محاسبه‌های مربوط بسیار پرزحمت‌اند مگر اینکه پیمانه کوچک باشد. ولی، به‌عنوان معیاری قطعی و سهل‌الاستفاده در بررسیهای نظری، هدف را کم و بیش برآورده می‌کند. یک روش محاسبهٔ کاراتر از قانون تقابل درجهٔ دوم به‌دست می‌آید که آن را بعداً در این فصل ثابت خواهیم کرد.

تمرینهای ۹ـ۱

۱. همنهشتیهای درجهٔ دوم زیر را حل کنید:

(الف) $x^2 + 7x + 10 \equiv 0 \ (\text{به پیمانهٔ } 11)$

(ب) $3x^2 + 9x + 7 \equiv 0 \ (\text{به پیمانهٔ } 13)$

(پ) $5x^2 + 6x + 1 \equiv 0 \ (\text{به پیمانهٔ } 23)$

۲. گرچه معادلهٔ $6x^2 + 5x + 1 = 0$ جواب صحیح ندارد، ثابت کنید همنهشتی درجهٔ دوم $6x^2 + 5x + 1 \equiv 0$ (به پیمانهٔ p) به‌ازای هر عدد اول p جواب دارد.

۳. (الف) ثابت کنید به‌ازای هر عدد اول فرد، مانده‌های درجه دوم p با عددهای صحیح

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

به پیمانهٔ p همنهشت‌اند.

(ب) نشان دهید که مانده‌های درجهٔ دوم ۱۷ عبارت‌اند از ۱، ۲، ۴، ۸، ۹، ۱۳، ۱۵، ۱۶.

۴. نشان دهید که ۳، ماندهٔ درجه دومی از ۲۳ و ناماندهٔ درجه دومی از ۳۱ است.

۵. اگر a ماندهٔ دومی از عدد اول فرد p باشد، ثابت کنید

(الف) a ریشهٔ اولیه‌ای از p نیست؛

(ب) برحسب اینکه $p \equiv ۱$ (به پیمانهٔ ۴) یا $p \equiv ۳$ (به پیمانهٔ ۴)، $p - a$ مانده‌ای درجه دوم یا نامانده‌ای درجه دوم از p است؛

(پ) اگر $p \equiv ۳$ (به پیمانهٔ ۴)، آنگاه $x \equiv \pm a^{(p+۱)/۴}$ (به پیمانهٔ p) جوابهایی از $x^۲ \equiv a$ (به پیمانهٔ p) هستند.

۶. فرض کنید p عددی اول و فرد باشد و $\gcd(a,p) = ۱$. نشان دهید همنهشتی درجه دوم $ax^۲ + bx + c \equiv ۰$ (به پیمانهٔ p) حلپذیر است اگر و تنها اگر $b^۲ - ۴ac$ صفر یا ماندهٔ درجه دومی از p باشد.

۷. اگر $p = ۲^k + ۱$ اول باشد، نشان دهید که هر ناماندهٔ درجه دوم p ریشه اولیه‌ای از p است. [راهنمایی: معیار اویلر را به‌کار ببرید.]

۸. فرض می‌کنیم $p \equiv ۱$ (به پیمانهٔ ۸)، و عدد صحیح r ریشه‌ای اولیه از عدد اول p باشد.

(الف) نشان دهید جوابهای همنهشتی درجه دوم $x^۲ \equiv ۲$ (به پیمانهٔ p) عبارت‌اند از

$$x \equiv \pm(r^{۷(p-۱)/۸} + r^{(p-۱)/۸}) \text{ (به پیمانهٔ } p)$$

[راهنمایی: نخست نشان دهید $r^{۳(p-۱)/۴} \equiv -۱$ (به پیمانهٔ p).]

(ب) با استفاده از قسمت (الف) همهٔ جوابهای همنهشتیهای $x^۲ \equiv ۲$ (به پیمانهٔ ۱۷) و $x^۲ \equiv ۲$ (به پیمانهٔ ۴۱) را به‌دست آورید.

۹. (الف) اگر r ماندهٔ درجهٔ دومی از عدد اول فرد p باشد و $ab \equiv r$ (به پیمانهٔ p)، ثابت کنید a و b یا هردو ماندهٔ درجه دوم p و یا هردو ناماندهٔ درجهٔ دوم آن هستند.

(ب) اگر a و b، یا هردو ماندهٔ درجه دوم و یا هردو ناماندهٔ درجهٔ دوم عدد اول فرد p باشند، نشان دهید همنهشتی $ax^۲ \equiv b$ (به پیمانهٔ p) جواب دارد. [راهنمایی: همنهشتی داده‌شده را در a' ضرب کنید که $aa' \equiv ۱$ (به پیمانهٔ p).]

۱۰. فرض می‌کنیم p عددی اول و فرد باشد و $\gcd(a,p) = \gcd(b,p) = ۱$. ثابت کنید یا هر سه همنهشتی

$$x^۲ \equiv a \text{ (به پیمانهٔ } p), \quad x^۲ \equiv b \text{ (به پیمانهٔ } p), \quad x^۲ \equiv ab \text{ (به پیمانهٔ } p)$$

حلپذیرند یا فقط یکی از آنها حلپذیر است.

۱۱. (الف) با علم به اینکه ۲، ریشه‌ای اولیه از ۱۹ است، همهٔ مانده‌های درجهٔ دوم ۱۹ را به‌دست آورید. [راهنمایی: اثبات قضیهٔ ۹ـ۱ را ببینید.]

(ب) مانده‌های درجهٔ دوم ۲۹ و ۳۱ را پیدا کنید.

۱۲. اگر $n > ۲$ و $\gcd(a, n) = ۱$، آنگاه a مانده‌ای درجهٔ دوم از n نامیده می‌شود اگر به‌ازای عدد صحیح xای، $x^۲ \equiv a$ (به پیمانهٔ n). ثابت کنید اگر a ماندهٔ درجه دومی از $n > ۲$ باشد، آنگاه $a^{\phi(n)/۲} \equiv ۱$ (به پیمانهٔ n).

۱۳. نشان دهید حکم تمرین فوق شرطی کافی برای وجود ماندهٔ درجهٔ دومی از n نیست؛ به بیان دیگر، عددهای صحیح متباین a و n را طوری پیدا کنید که $a^{\phi(n)/۲} \equiv ۱$ (به پیمانهٔ n)، و همنهشتی $x^۲ \equiv a$ (به پیمانهٔ n) فاقد جواب باشد.

۹ـ۲ نماد لژاندر و ویژگیهای آن

دامنهٔ پژوهشهای اویلر دربارهٔ مانده‌های درجهٔ دوم به وسیلهٔ آدریان ماری لژاندر[1] (۱۷۵۲ ـ ۱۸۳۳)، ریاضیدان فرانسوی، گسترش بیشتری یافت. رسالهٔ لژاندر تحت عنوان «تحقیقاتی در آنالیز نامعینها»[2] (۱۷۸۵) حاوی شرحی از قانون تقابل درجهٔ دوم و کاربردهای بسیار آن، خلاصه‌ای از نظریهٔ نمایش عدد صحیح به‌صورت مجموع سه مربع، و بیان قضیه‌ای است که بعداً معروف شد: هر تصاعد حسابی $ax + b$ که در آن $\gcd(a, b) = ۱$، حاوی تعدادی نامتناهی عدد اول است. موضوعهای مورد بحث در «تحقیقات» به صورتی جامعتر و اصولیتر در رساله در باب نظریهٔ اعداد[3] او که در ۱۷۹۸ انتشار یافت، ارائه شد. این نخستین رسالهٔ «نوین» بود که منحصراً به نظریهٔ اعداد اختصاص داشت؛ رساله‌های قبلی در این زمینه، ترجمه‌ها یا شرح و تفسیرهایی از اثر دیوفانتوس بیش نبودند. رسالهٔ لژاندر بعداً گسترش یافت و به‌صورت کتاب نظریهٔ اعداد او درآمد. نتیجه‌های مقاله‌های تحقیقی بعدی او، که به میزان زیادی ملهم از گاوس بودند، در ویراست سوم نظریهٔ اعداد وی که در ۱۸۳۰ در دو جلد انتشار یافت، مطرح شدند. سالیانی دراز، این اثر همراه با تحقیقات حسابی گاوس، متون استاندارد در نظریهٔ اعداد به حساب می‌آمدند. گرچه لژاندر کار بدیع مهمی درنظریهٔ اعداد نکرد، پرسشهای بارآوری مطرح کرد که خوراک تحقیقی ریاضیدانان سدهٔ نوزدهم بود.

پیش از آنکه گفتگو دربارهٔ کارهای ریاضی لژاندر را کنار بگذاریم، اضافه می‌کنیم که او به دلیل پژوهشهایش دربارهٔ انتگرالهای بیضوی و کتابش تحت عنوان مبانی هندسه[4] (۱۷۹۴) نیز

1. Adrien Marie Legendre
2. Recherches d'Analyse Indéterminée
3. Essai sur la Théorie des Nombres
4. Eléments de Géométrie

معروف است. وی در این کتاب اصول اقلیدس را با تنظیمی جدید و ساده سازی بسیاری از اثباتها، بی آنکه از دقت متن باستانی کاسته شود، به صورتی در آورد که از نظر آموزشی مناسب باشد. حاصل کار به اندازه‌ای با استقبال مواجه شد که به‌صورت یکی از موفقترین کتابهای درسی تا آن زمان درآمد، و با تجدید چاپها و ترجمه‌های متعدد این کتاب، آموزش هندسه متجاوز از یک سده تحت نفوذ آن بود. در سال ۱۸۲۴ این کتاب را تامس کارلایل[1] نویسنده و مورخ معروف اسکاتلندی، که در جوانی معلم ریاضی بود، به انگلیسی ترجمه کرد؛ ترجمه کارلایل ۳۳ بار در آمریکا تجدید چاپ شد. آخرین چاپ آن در ۱۸۹۰ منتشر شد. درواقع، اثر لژاندر تا حدود ۱۸۸۵، یعنی تا زمانی که کتاب اصول از زمرهٔ کتابهای درسی خارج شد، در دانشگاه ییل مورد استفاده بود.

مباحث آتی ما با استفاده از نماد (a/p) به میزان زیادی تسهیل می‌شود؛ این نماد را لژاندر در رساله‌اش معرفی کرد و طبیعتاً نماد لژاندر نامیده می‌شود.

تعریف ۹ـ۲ فرض می‌کنیم p عدد اول فردی باشد و $\gcd(a,p) = ۱$. نماد لژاندر (a/p) چنین تعریف می‌شود:

$$(a/p) = \begin{cases} ۱ & \text{اگر } a \text{ مانده‌ای درجهٔ دوم از } p \text{ باشد} \\ -۱ & \text{اگر } a \text{ نامانده‌ای درجهٔ دوم از } p \text{ باشد} \end{cases}$$

به دلیل نیاز به اصطلاحات بهتر، a را صورت و p را مخرج نماد (a/p) می‌نامیم. $(a|p)$ و $\frac{a}{b}$ صورتهای متعارف دیگری از نماد (a/p) هستند.

مثال ۹ـ۳

عدد اول $p = ۱۳$ را در نظر می‌گیریم. نتیجه‌های یکی از مثالهای پیشین، با استفاده از نماد لژاندر، چنین بیان می‌شوند

$$(۱/۱۳) = (۳/۱۳) = (۴/۱۳) = (۹/۱۳) = (۱۰/۱۳) = (۱۲/۱۳) = ۱$$

و

$$(۲/۱۳) = (۵/۱۳) = (۶/۱۳) = (۷/۱۳) = (۸/۱۳) = (۱۱/۱۳) = -۱ \quad \blacksquare$$

1. Carlyle

یادداشت: در حالت $p|a$، نماد (a/p) را عمداً تعریف نکرده‌ایم. برخی از مؤلفان ترجیح می‌دهند با فرض $(a/p) = 0$ تعریف لژاندر را به این حالت تعمیم دهند. فایدهٔ این تعمیم این است که در این‌صورت می‌توان تعداد جوابهای (به پیمانهٔ p) $x^2 \equiv a$ را با فرمول سادهٔ $(a/p) + 1$ ارائه کرد.

در قضیهٔ زیر چند حکم مقدماتی دربارهٔ نماد لژاندر بیان می‌شود.

قضیهٔ ۹ـ۲ فرض می‌کنیم p عددی اول و فرد باشد و a و b عددهایی صحیح و متباین با p باشند. در این صورت نماد لژاندر دارای ویژگیهای زیر است:

(۱) اگر (به پیمانهٔ p) $a \equiv b$، آنگاه $(a/p) = (b/p)$.

(۲) $(a^2/p) = 1$.

(۳) (به پیمانهٔ p) $(a/p) \equiv a^{(p-1)/2}$.

(۴) $(ab/p) = (a/p)(b/p)$.

(۵) $(1/p) = 1$ و $(-1/p) = (-1)^{(p-1)/2}$.

اثبات. اگر (به پیمانهٔ p) $a \equiv b$، آنگاه (به پیمانهٔ p) $x^2 \equiv a$ و (به پیمانهٔ p) $x^2 \equiv b$، اگر جوابی داشته باشند، جوابهای یکسان دارند. پس (به پیمانهٔ p) $x^2 \equiv a$ و (به پیمانهٔ p) $x^2 \equiv b$ یا هر دو حلپذیرند، یا هیچ یک جوابی ندارند. این نکته در عبارت $(a/p) = (b/p)$ منعکس است.

در مورد (۲)، ملاحظه می‌کنیم عدد صحیح a به وضوح در همنهشتی (به پیمانهٔ p) $x^2 \equiv a^2$ صدق می‌کند؛ پس $(a^2/p) = 1$. قسمت (۳) بیان دیگری از فرع قضیهٔ ۹ـ۱ برحسب نماد لژاندر است. از (۳) برای اثبات (۴) استفاده می‌کنیم

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (a/b)(b/p) \text{ (به پیمانهٔ } p)$$

ولی نماد لژاندر فقط مقدارهای ۱ و ۱− را می‌پذیرد. اگر $(ab/p) \neq (a/p)(b/p)$، نتیجه می‌شود (به پیمانهٔ p) $1 \equiv -1$ یا (به پیمانهٔ p) $2 \equiv 0$؛ این پذیرفتنی نیست زیرا $p > 2$. نتیجه می‌گیریم که

$$(ab/p) = (a/p)(b/p)$$

و بالاخره، ملاحظه می‌کنیم که برابری نخست در (۵) حالت ویژه‌ای از (۲) است، و دومی از ویژگی (۳) به‌ازای $a = -1$ به‌دست می‌آید. چون کمیتهای $(-1/p)$ و $(-1)^{(p-1)/2}$ برابر ۱ یا ۱− اند، همنهشتی حاصل

$$(-1/p) \equiv (-1)^{(p-1)/2} \text{ (به پیمانهٔ } p) \qquad \square$$

نشان می‌دهد $(-1/p) = (-1)^{(p-1)/2}$.

از قسمتهای (۲) و (۴) قضیهٔ ۹ـ۲، رابطهٔ

$$(ab^{۲}/p) = (a/p)(b^{۲}/p) = (a/p) \qquad (۶)$$

نیز نتیجه می‌شود. به بیان دیگر، هر عامل مربع متباین با p را می‌توان از صورت نماد لژاندر حذف کرد بی‌آنکه مقدارش تغییر کند.

چون $(p-۱)/۲$ به‌ازای p هایِ به‌صورت $۴k+۱$ زوج و به‌ازای p هایِ به‌صورت $۴k+۳$ فرد است، با توجه به معادلهٔ $(-۱/p) = (-۱)^{(p-۱)/۲}$ داریم:

فرع. اگر p عدد اول فردی باشد، آنگاه

$$(-۱/p) = \begin{cases} ۱ & \text{اگر (به پیمانهٔ ۴)} \ p \equiv ۱ \\ -۱ & \text{اگر (به پیمانهٔ ۴)} \ p \equiv ۳ \end{cases}$$

از این نتیجه چنین بر می‌آید که همنهشتی (به پیمانهٔ p) $x^{۲} \equiv -۱$ جواب دارد اگر و تنها اگر p عدد اولی به‌صورت $۴k+۱$ باشد. البته این نتیجه تازه‌ای نیست؛ صرفاً اثباتی دیگر از قضیهٔ ۵ـ۵ ارائه کرده‌ایم.

مثال ۹ـ۴

نشان می‌دهیم همنهشتی (به پیمانهٔ ۱۳) $x^{۲} \equiv -۳۸$ حلپذیر است. این کار را با محاسبهٔ $(-۳۸/۱۳)$ انجام می‌دهیم. نخست با توسل به قسمتهای (۴) و (۵) از قضیهٔ ۹ـ۲ می‌نویسیم

$$(-۳۸/۱۳) = (-۱/۱۳)(۳۸/۱۳) = (۳۸/۱۳)$$

چون (به پیمانهٔ ۱۳) $۳۸ \equiv ۱۲$، نتیجه می‌شود

$$(۳۸/۱۳) = (۱۲/۱۳)$$

پس، بنابه ویژگی (۶) داریم

$$(۱۲/۱۳) = (۳ \times ۲^{۲}/۱۳) = (۳/۱۳)$$

ولی بنابه (۳) از قضیهٔ ۹ـ۲ داریم

$$(۳/۱۳) \equiv ۳^{(۱۳-۱)/۲} \equiv ۳^{۶} \equiv (۲۷)^{۲} \equiv ۱ \ \text{(به پیمانهٔ ۱۳)}$$

پس، $(3/13) = 1$. چون $(-38/13) = 1$، همنهشتی درجه دوم $x^2 \equiv -38$ (به پیمانهٔ ۱۳)
جواب دارد. ■

فرع قضیهٔ ۹ـ۲ کاربردی در مورد توزیع عددهای اول دارد.

قضیهٔ ۹ـ۳ مجموعهٔ عددهای اول به‌صورت $4k + 1$ نامتناهی است.

اثبات. فرض می‌کنیم تعداد این‌گونه عددهای اول متناهی باشد؛ آنها را p_1، p_2، ...، p_n می‌نامیم و عدد صحیح

$$N = (2p_1p_2\dots p_n)^2 + 1$$

را درنظر می‌گیریم. N به‌وضوح فرد است، بنابراین عدد اول فرد p ای وجود دارد به‌طوری‌که $p|N$.
به بیان دیگر

$$(2p_1p_2\dots p_n)^2 \equiv -1 \ (\text{به پیمانهٔ } p)$$

و با استفاده از نماد لژاندر داریم $(-1/p) = 1$. ولی رابطهٔ $(-1/p) = 1$ فقط وقتی برقرار است که p به‌صورت $4k + 1$ باشد. پس، p یکی از عددهای اول p_i است. این نشان می‌دهد که p_i عدد $N - (2p_1p_2\dots p_n)^2$ را می‌شمارد، یا $p_i|1$، که تناقض است. نتیجه: مجموعهٔ عددهای اول به‌صورت $4k + 1$ باید نامتناهی باشد. □

در قضیهٔ زیر، ویژگیهای مانده‌های درجه دوم را عمیقتر بررسی می‌کنیم.

قضیهٔ ۹ـ۴ اگر p عدد اول فردی باشد، آنگاه

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$$

پس، دقیقاً $(p-1)/2$ ماندهٔ درجهٔ دوم و $(p-1)/2$ ناماندهٔ درجهٔ دوم از p وجود دارد.

اثبات. فرض می‌کنیم r ریشه‌ای اولیه از p باشد. می‌دانیم که، به پیمانهٔ p، توانهای r، r^2، ...، r^{p-1} صرفاً جایگشتی از عددهای صحیح ۱، ۲، ...، $p-1$ هستند. پس به‌ازای هر a که $1 \le a \le p-1$، عدد صحیح مثبت یکتای k ای $(1 \le k \le p-1)$ وجود دارد، به‌طوری‌که $a \equiv r^k$ (به پیمانهٔ p). با استفادهٔ مناسب از معیار اویلر، داریم

$$(a/p) = (r^k/p) \equiv (r^k)^{(p-1)/2} = \left(r^{(p-1)/2}\right)^k \equiv (-1)^k \ (\text{به پیمانهٔ } p) \quad (1)$$

که در آن، چون r ریشه‌ای اولیه از p است،(به پیمانهٔ p) $r^{(p-۱)/۲} \equiv -۱$. ولی (a/p) و $(-۱)^k$ برابر با ۱ یا ۱− اند. پس، برابری در (۱) برقرار است. اکنون نمادهای لژاندر مورد بحث را جمع می‌کنیم. در این صورت

$$\sum_{a=۱}^{p-۱}(a/p) = \sum_{k=۱}^{p-۱}(-۱)^k = ۰$$

که نتیجهٔ مطلوب است. □

از اثبات قضیهٔ ۹ـ۴ نتیجه می‌گیریم که

فرع. مانده‌های درجهٔ دوم عدد اول فرد p همنهشت با توانهای زوج ریشه‌ای اولیه از p به پیمانهٔ p هستند؛ نامانده‌های درجه دوم با توانهای فرد r همنهشت‌اند.

برای توضیح ایدهٔ فوق با یک مثال، دوباره عدد اول $p = ۱۳$ را درنظر می‌گیریم. چون ۲ ریشه‌ای اولیه از ۱۳ است، مانده‌های درجهٔ دوم ۱۳ از توانهای زوج ۲ به‌دست می‌آیند، یعنی

$$\begin{array}{ll} ۲^۲ \equiv ۴ & ۲^۸ \equiv ۹ \\ ۲^۴ \equiv ۳ & ۲^{۱۰} \equiv ۱۰ \\ ۲^۶ \equiv ۱۲ & ۲^{۱۲} \equiv ۱ \end{array}$$

و همهٔ همنهشتیها به پیمانهٔ ۱۳ اند. همین‌طور، نامانده‌ها به‌صورت توانهای فرد ۲ ظاهر می‌شوند:

$$\begin{array}{ll} ۲^۱ \equiv ۲ & ۲^۷ \equiv ۱۱ \\ ۲^۳ \equiv ۸ & ۲^۹ \equiv ۵ \\ ۲^۵ \equiv ۶ & ۲^{۱۱} \equiv ۷ \end{array}$$

بیشتر اثباتهای قانون تقابل درجهٔ دوم، و همچنین اثبات ما، در نهایت به لم معروف به لم گاوس متّکی هستند. گرچه این لم مشخص می‌کند که عدد صحیح مفروض، ماندهٔ درجهٔ دوم است یا نه، از لحاظ نظری مفیدتر است تا از لحاظ محاسباتی. این لم را در زیر بیان و ثابت می‌کنیم.

قضیهٔ ۹ـ۵ (لم گاوس). فرض می‌کنیم p عددی فرد و اول باشد و $\gcd(a,p) = ۱$. اگر n تعداد عددهای صحیحی از مجموعهٔ

$$S = \left\{a, ۲a, ۳a, \dots, \left(\frac{p-۱}{۲}\right)a\right\}$$

باشد که باقیماندهٔ تقسیم آنها بر p بزرگتر از $p/۲$ است، آنگاه

$$(a/p) = (-۱)^n$$

اثبات. چون $\gcd(a,p) = ۱$، هیچ یک از $(p-۱)/۲$ عدد صحیح متعلق به S همنهشت با صفر نیست و هیچ دوتای آنها به پیمانهٔ p همنهشت با یکدیگر نیستند. فرض می‌کنیم $r_۱$، $r_۲$، ...، r_m باقیمانده‌های تقسیم بر p ای هستند به‌طوری که $۰ < r_i < p/۲$ و $s_۱$، ...، s_n باقیمانده‌هایی هستند که $p > s_i > p/۲$. در این صورت $m + n = (p-۱)/۲$، و عددهای صحیح

$$r_۱, \ldots, r_m, p - s_۱, \ldots, p - s_n$$

همگی مثبت و کوچکتر از $p/۲$اند.

برای اثبات اینکه همهٔ این عددهای صحیح متمایزند، کافی است نشان دهیم هیچ یک از $p - s_i$ها برابر با r_jای نیست. فرض می‌کنیم برخلاف آن، به‌ازای i و jای داشته باشیم

$$p - s_i = r_j$$

در این صورت عددهای صحیح u و vای وجود دارند که $۱ \leq u, v \leq (p-۱)/۲$ و $s_i \equiv ua$ (به پیمانهٔ p)، $r_j \equiv va$ (به پیمانهٔ p). پس

$$(u+v)a \equiv s_i + r_j \equiv p \equiv ۰ \ (\text{به پیمانهٔ } p)$$

که نتیجه می‌شود $u + v \equiv ۰$ (به پیمانهٔ p). ولی، چون $۱ \leq u + v \leq p - ۱$، همنهشتی اخیر برقرار نیست.

نکته‌ای که می‌خواهیم نشان دهیم این است که $(p-۱)/۲$ عدد

$$r_۱, \ldots, r_m, p - s_۱, \ldots, p - s_n$$

صرفاً جایگشت مفروضی از عددهای صحیح ۱، ۲، ...، $(p-۱)/۲$اند. پس، حاصلضرب آنها $[(p-۱)/۲]!$ است:

$$\begin{aligned}\left(\frac{p-۱}{۲}\right)! &= r_۱ \ldots r_m (p - s_۱) \ldots (p - s_n) \\ &\equiv r_۱ \ldots r_m (-s_۱) \ldots (-s_n) \ (\text{به پیمانهٔ } p) \\ &\equiv (-۱)^n r_۱ \ldots r_m s_۱ \ldots s_n \ (\text{به پیمانهٔ } p)\end{aligned}$$

ولی می‌دانیم که $r_۱$، ...، r_m، $s_۱$، ...، s_n، به ترتیبی، با a، $۲a$، ...، a [$(p-۱/۲)$] به پیمانهٔ p همنهشت‌اند، و بنابراین

$$\left(\frac{p-۱}{۲}\right)! \equiv (-۱)^n a \times ۲a \times \ldots \times \left(\frac{p-۱}{۲}\right) a \ (\text{به پیمانهٔ } p)$$
$$\equiv (-۱)^n a^{(p-۱)/۲} \left(\frac{p-۱}{۲}\right)! \ (\text{به پیمانهٔ } p)$$

چون $[(p-۱)/۲]!$ با p متباین است، با حذف آن از طرفین این همنهشتی داریم

$$۱ \equiv (-۱)^n a^{(p-۱)/۲} \ (\text{به پیمانهٔ } p)$$

یا، با ضرب کردن در $(-۱)^n$

$$a^{(p-۱)/۲} \equiv (-۱)^n \ (\text{به پیمانهٔ} p)$$

اکنون با استفاده از معیار اویلر نتیجهٔ مطلوب به‌دست می‌آید

$$(a/p) \equiv a^{(p-۱)/۲} \equiv (-۱)^n \ (\text{به پیمانهٔ } p)$$

که نتیجه می‌دهد

$$(a/p) = (-۱)^n$$ □

به‌عنوان مثال، فرض می‌کنیم $p = ۱۳$ و $a = ۵$. در این صورت $۶ = (p-۱)/۲$، و بنابراین

$$S = \{۵, ۱۰, ۱۵, ۲۰, ۲۵, ۳۰\}$$

به پیمانهٔ ۱۳، عضوهای S همنهشت با عددهای صحیح

$$۵, ۱۰, ۲, ۷, ۱۲, ۴$$

هستند؛ سه تا از اینها بزرگتر از ۱۳/۲اند؛ پس، $n = ۳$ و بنابه قضیهٔ ۹ـ۵ داریم

$$(۵/۱۳) = (-۱)^۳ = -۱$$

با استفاده از لم گاوس، نتیجه‌های جالب گوناگونی به‌دست می‌آیند. به‌عنوان مثال، با استفاده از آن می‌توان عددهای اول با ماندهٔ درجه دوم ۲ را تعیین کرد.

قضیهٔ ۹ـ۶ اگر p عدد اول فردی باشد، آنگاه

$$(\text{۲}/p) = \begin{cases} \text{۱} & \text{اگر (به پیمانهٔ ۸) ۱} \equiv p \text{ یا (به پیمانهٔ ۸) ۷} \equiv p \\ -\text{۱} & \text{اگر (به پیمانهٔ ۸) ۳} \equiv p \text{ یا (به پیمانهٔ ۸) ۵} \equiv p \end{cases}$$

اثبات. بنابه لم گاوس، $(\text{۲}/p) = (-\text{۱})^n$، که در آن n تعداد عددهای صحیحی متعلق به مجموعهٔ

$$S = \left\{\text{۲}, \text{۲} \times \text{۲}, \text{۳} \times \text{۲}, \ldots, \left(\frac{p-\text{۱}}{\text{۲}}\right) \times \text{۲}\right\}$$

است که باقیماندهٔ تقسیم آنها بر p بزرگتر از $p/\text{۲}$ است. عضوهای S همگی کوچکتر از p اند، بنابراین کافی است تعداد عضوهایی را بشماریم که از $p/\text{۲}$ بزرگترند. به‌ازای $\text{۱} \le k \le (p-\text{۱})/\text{۲}$، $\text{۲}k < p/\text{۲}$ اگر و تنها اگر $k < p/\text{۴}$. اگر $[\,]$ تابع بزرگترین عدد صحیح باشد، تعداد $[p/\text{۴}]$ عضو S کوچکتر از $p/\text{۲}$اند، پس، تعداد

$$n = \frac{p-\text{۱}}{\text{۲}} - \left[\frac{p}{\text{۴}}\right]$$

عضو S بزرگتر از $p/\text{۲}$اند.

اکنون چهار حالت داریم؛ زیرا هر عدد اول فرد به یکی از صورتهای $\text{۸}k+\text{۱}$، $\text{۸}k+\text{۳}$، $\text{۸}k+\text{۵}$، یا $\text{۸}k+\text{۷}$ است. محاسبه‌ای ساده نشان می‌دهد که

اگر $p = \text{۸}k+\text{۱}$، آنگاه $n = \text{۴}k - \left[\text{۲}k + \frac{\text{۱}}{\text{۴}}\right] = \text{۴}k - \text{۲}k = \text{۲}k$

اگر $p = \text{۸}k+\text{۳}$، آنگاه $n = \text{۴}k+\text{۱} - \left[\text{۲}k + \frac{\text{۳}}{\text{۴}}\right] = \text{۴}k+\text{۱}-\text{۲}k = \text{۲}k+\text{۱}$

اگر $p = \text{۸}k+\text{۵}$، آنگاه
$$\begin{aligned} n &= \text{۴}k+\text{۲} - \left[\text{۲}k+\text{۱}+\frac{\text{۱}}{\text{۴}}\right] \\ &= \text{۴}k+\text{۲}-(\text{۲}k+\text{۱}) = \text{۲}k+\text{۱} \end{aligned}$$

اگر $p = \text{۸}k+\text{۷}$، آنگاه
$$\begin{aligned} n &= \text{۴}k+\text{۳} - \left[\text{۲}k+\text{۱}+\frac{\text{۳}}{\text{۴}}\right] \\ &= \text{۴}k+\text{۳}-(\text{۲}k+\text{۱}) = \text{۲}k+\text{۲} \end{aligned}$$

بنابراین، هرگاه p به‌صورت $\text{۸}k+\text{۱}$ یا $\text{۸}k+\text{۷}$ باشد، n زوج است و $(\text{۲}/p) = \text{۱}$؛ از سوی دیگر اگر p به‌صورت $\text{۸}k+\text{۳}$ یا $\text{۸}k+\text{۵}$ باشد، n فرد است و $(\text{۲}/p) = -\text{۱}$. □

ملاحظه می‌کنیم اگر عدد اول فرد p به‌صورت $\text{۸}k \pm \text{۱}$ باشد (به عبارت دیگر $p \equiv \text{۱}$ (به پیمانهٔ ۸) یا $p \equiv \text{۷}$ (به پیمانهٔ۸))، آنگاه

$$\frac{p^{\text{۲}} - \text{۱}}{\text{۸}} = \frac{(\text{۸}k \pm \text{۱})^{\text{۲}} - \text{۱}}{\text{۸}} = \frac{\text{۶۴}k^{\text{۲}} \pm \text{۱۶}k}{\text{۸}} = \text{۸}k^{\text{۲}} \pm \text{۲}k$$

که عدد صحیح زوجی است؛ در این وضعیت، $(\text{۲}/p) = \text{۱} = (-\text{۱})^{(p^{\text{۲}}-\text{۱})/\text{۸}}$. از سوی دیگر، اگر p به‌صورت $\text{۸}k \pm \text{۳}$ باشد (به عبارت دیگر اگر $p \equiv \text{۳}$ (به پیمانهٔ ۸) یا $p \equiv \text{۵}$ (به پیمانهٔ ۸))، آنگاه

$$\frac{p^{\text{۲}} - \text{۱}}{\text{۸}} = \frac{(\text{۸}k \pm \text{۳})^{\text{۲}} - \text{۱}}{\text{۸}} = \frac{\text{۶۴}k^{\text{۲}} \pm \text{۴۸}k + \text{۸}}{\text{۸}} = \text{۸}k^{\text{۲}} \pm \text{۶}k + \text{۱}$$

که فرد است؛ در این حالت داریم $(\text{۲}/p) = -\text{۱} = (-\text{۱})^{(p^{\text{۲}}-\text{۱})/\text{۸}}$. این ملاحظات در فرع زیر از قضیهٔ ۹ـ۶ مستترند.

فرع. اگر p عدد اول فردی باشد، آنگاه

$$(\text{۲}/p) = (-\text{۱})^{(p^{\text{۲}}-\text{۱})/\text{۸}}$$

اکنون فرصت مناسبی است که باز به ریشه‌های اولیه بپردازیم. به‌طوری‌که پیشتر خاطرنشان کردیم، روشی عمومی برای به‌دست آوردن ریشه‌ای اولیه از عدد اول فرد p وجود ندارد، مع‌الوصف قضیهٔ زیر گاهی سودمند است.

قضیهٔ ۹ـ۷ اگر هم p و هم $\text{۲}p + \text{۱}$ عددهای اول فردی باشند، آنگاه عدد صحیح $(-\text{۱})^{(p-\text{۱})/\text{۲}}\text{۲}$ ریشه‌ای اولیه از $\text{۲}p + \text{۱}$ است.

اثبات. برای تسهیل بحث، قرار می‌دهیم $q = \text{۲}p + \text{۱}$. دو حالت درنظر می‌گیریم: $p \equiv \text{۱}$ (به پیمانهٔ ۴) و $p \equiv \text{۳}$ (به پیمانهٔ ۴).

اگر $p \equiv \text{۱}$ (به پیمانهٔ ۴)، آنگاه $\text{۲} = (-\text{۱})^{(p-\text{۱})/\text{۲}}\text{۲}$. چون $\phi(q) = q - \text{۱} = \text{۲}p$، مرتبهٔ ۲ به پیمانهٔ q یکی از عددهای ۱، ۲، p، یا $\text{۲}p$ است. با توجه به (۳) قضیهٔ ۹ـ۲، داریم

$$(\text{۲}/q) \equiv \text{۲}^{(q-\text{۱})/\text{۲}} = \text{۲}^{p} \quad (\text{به پیمانهٔ } q)$$

ولی، در این حالت، $q \equiv \text{۳}$ (به پیمانهٔ ۸)؛ پس $(\text{۲}/q) = -\text{۱}$. نتیجه می‌شود $\text{۲}^{p} \equiv -\text{۱}$ (به پیمانهٔ q)، و بنابراین ۲ نمی‌تواند دارای مرتبهٔ p به پیمانهٔ q باشد. چون مرتبهٔ ۲ نه

۱، ۲ است (از (به پیمانهٔ q) ۱ $\equiv$ ۲^۲ نتیجه می‌شود ۳$|q$، که غیرممکن است) و نه p، نتیجه می‌گیریم که مرتبهٔ ۲ به پیمانهٔ q برابر $۲p$ است. یعنی، ۲ ریشه‌ای اولیه از q است.

اکنون به حالت (به پیمانهٔ ۴) ۳ $\equiv p$ می‌پردازیم. این‌بار، $(-۱)^{(p-۱)/۲}۲ \equiv ۲-$ و

$$(-۲)^p \equiv (-۲/q) = (-۱/q)(۲/q) \ (\text{به پیمانهٔ } q)$$

چون (به پیمانهٔ ۸) ۷ $\equiv q$، بنابه فرع قضیهٔ ۹ـ۲، $(-۱/q) = -۱$، و دوباره داریم $(۲/q) = ۱$. نتیجه می‌شود (به پیمانهٔ q) $(-۲)^p \equiv -۱$. از این به بعد، استدلال عین پاراگراف فوق است. بدون تحلیل بیشتر، اعلام می‌کنیم که: ۲$-$ ریشهٔ اولیه‌ای از q است. □

به‌عنوان مثال، قضیهٔ ۹ـ۷ نشان می‌دهد که ۲ ریشه‌ای اولیه از عددهای اول ۱۱، ۵۹، ۱۰۷ و ۱۷۹ است. همین‌طور، عدد صحیح ۲$-$ ریشه‌ای اولیه از ۷، ۲۳، ۴۷، و ۱۶۷ است.

پیش از خاتمهٔ این بحث، نتیجهٔ دیگری را که سرشت مشابهی دارد عنوان می‌کنیم: اگر هم p و هم $۴p + ۱$ عدد اول باشند، آنگاه ۲ ریشهٔ اولیهٔ $۴p + ۱$ است. بنابراین، به فهرست عددهای اول با ریشهٔ ۲، می‌توان، مثلاً ۱۳، ۲۹، ۵۳، و ۱۷۳ را افزود.

اثبات جذاب دیگری از نامتناهی بودن تعداد عددهای اولِ به‌صورت $۸k - ۱$ وجود دارد که مبتنی است بر قضیهٔ ۹ـ۶.

قضیهٔ ۹ـ۸ تعداد عددهای اول به‌صورت $۸k - ۱$، نامتناهی است.

اثبات. طبق معمول، فرض می‌کنیم فقط تعدادی متناهی از این عددهای اول وجود دارد. اینها را $p_۱$، $p_۲$، ...، p_n می‌نامیم و عدد صحیح

$$N = (۴p_۱p_۲\dots p_n)^۲ - ۲$$

را درنظر می‌گیریم. N دارای حداقل یک مقسوم‌علیه فرد اول p است به‌طوری که

$$(۴p_۱p_۲\dots p_n)^۲ \equiv ۲ \ (\text{به پیمانهٔ } p)$$

یا $(۲/p) = ۱$. با توجه به قضیهٔ ۹ـ۶، (به پیمانهٔ ۸) $p \equiv \pm ۱$. اگر همهٔ مقسوم‌علیه‌های اول فرد N به‌صورت $۸k + ۱$ بود، آنگاه خود N به‌صورت $۱۶a + ۲$ می‌بود؛ این به وضوح غیرممکن است، زیرا N به‌صورت $۱۶a - ۲$ است. پس، N باید مقسوم‌علیه اول q ای به‌صورت $۸k - ۱$ داشته باشد. ولی از $q|N$ و $q|(۴p_۱p_۲\dots p_n)^۲$ نتیجه می‌شود $q|۲$، که متضمن تناقض است. □

نتیجه بعدی، که به ما امکان می‌دهد راهی از لم گاوس به سوی قانون تقابل درجه دوم باز کنیم، مستقلاً اهمیت دارد.

لم. اگر p عددی اول و فرد، و a عددی صحیح و فرد باشد و $\gcd(a,p)=۱$، آنگاه

$$(a/p)=(-۱)^{\sum_{k=۱}^{(p-۱)/۲}[ka/p]}$$

اثبات. از همان نمادهای به‌کار رفته در اثبات لم گاوس استفاده می‌کنیم. مجموعهٔ عددهای صحیح

$$S=\left\{a, ۲a, \ldots, \left(\frac{p-۱}{۲}\right)a\right\}$$

را درنظر می‌گیریم. با تقسیم هریک از این مضربهای a بر p به‌دست می‌آوریم

$$ka=q_kp+t_k، \qquad ۱\le t_k\le p-۱$$

در این صورت $ka/p=q_k+t_k/p$، و بنابراین $q_k=[(ka)/p]$. پس به‌ازای $۱\le k\le (p-۱)/۲$، می‌توانیم ka را به‌صورت

$$ka=[ka/p]p+t_k \tag{۱}$$

بنویسیم. اگر باقیماندهٔ t_k کوچکتر از $p/۲$ باشد، آنگاه t_k یکی از عددهای صحیح $r_۱، \ldots، r_m$ است؛ اگر $t_k>p/۲$، آنگاه t_k یکی از عددهای صحیح $s_۱، \ldots، s_n$ است.

باجمع کردن روابط (۱) به‌دست می‌آوریم

$$\sum_{k=۱}^{(p-۱)/۲} ka=\sum_{k=۱}^{(p-۱)/۲}\left[\frac{ka}{p}\right]p+\sum_{k=۱}^{m} r_k+\sum_{k=۱}^{n} s_k \tag{۲}$$

در اثبات لم گاوس دیدیم که $(p-۱)/۲$ عدد

$$r_۱, \ldots, r_m, p-s_۱, \ldots, p-s_n$$

صرفاً جایگشتی از عددهای صحیح ۱، ۲، ...، $(p-۱)/۲$ هستند. پس

$$\sum_{k=۱}^{(p-۱)/۲} k=\sum_{k=۱}^{m} r_k+\sum_{k=۱}^{n}(p-s_k)=pn+\sum_{k=۱}^{m} r_k-\sum_{k=۱}^{n} s_k \tag{۳}$$

با تفریق (۳) از (۲) نتیجه می‌گیریم

$$(a-۱)\sum_{k=۱}^{(p-۱)/۲} k = p\left(\sum_{k=۱}^{(p-۱)/۲}[ka/p]-n\right)+۲\sum_{k=۱}^{n} s_k \qquad (۴)$$

پس، با توجه به اینکه (به پیمانهٔ ۲) $p \equiv a \equiv ۱$، داریم

$$۰\cdot\sum_{k=۱}^{(p-۱)/۲} k \equiv ۱\cdot\left(\sum_{k=۱}^{(p-۱)/۲}[ka/p]-n\right) \text{ (به پیمانهٔ ۲)}$$

یا

$$n \equiv \sum_{k=۱}^{(p-۱)/۲}[ka/p] \text{ (به پیمانهٔ ۲)}$$

بقیه از لم گاوس نتیجه می‌شود: زیرا همان‌طور که می‌خواستیم، داریم

$$(a/p) = (-۱)^n = (-۱)^{\sum_{k=۱}^{(p-۱)/۲}[ka/p]} \qquad \square$$

به‌عنوان مثالی از نتیجهٔ اخیر، دوباره $p = ۱۳$ و $a = ۵$ را درنظر می‌گیریم. چون $(p-۱)/۲ = ۶$، لازم است $[(ka)/p]$ را به‌ازای $k = ۱, \ldots, ۶$ حساب کنیم

$$[۵/۱۳] = [۱۰/۱۳] = ۰$$
$$[۱۵/۱۳] = [۲۰/۱۳] = [۲۵/۱۳] = ۱$$
$$[۳۰/۱۳] = ۲$$

بنابه لم

$$(۵/۱۳) = (-۱)^{۱+۱+۱+۲} = (-۱)^۵ = -۱$$

که آنچه را پیشتر ملاحظه کردیم، تأیید می‌کند.

تمرینهای ۹ـ۲

۱. مقدار نمادهای لژاندر زیر را پیدا کنید:
(الف) $(۱۹/۲۳)$، (ب) $(-۲۳/۵۹)$، (پ) $(۲۰/۳۱)$، (ت) $(۱۸/۴۳)$، (ث) $(-۷۲/۱۳۱)$.

۲. با استفاده از لم گاوس، هریک از نمادهای لژاندار زیر را حساب کنید (یعنی، در هر حالت عدد صحیح nای به‌دست آورید که $(a/p) = (-۱)^n$):

(الف) (۸/۱۱)، (ب) (۷/۱۳)، (پ) (۵/۱۹)، (ت) (۱۱/۲۳)، (ث) (۶/۳۱).

۳. ثابت کنید که به‌ازای هر عدد اول فرد p، $(p-۱)/۲ - \phi(p-۱)$ ناماندهٔ درجهٔ دوم p وجود دارند که ریشهٔ اولیهٔ p نیستند.

۴. (الف) فرض می‌کنیم p عدد اول فردی باشد. نشان دهید معادلهٔ دیوفانتی

$$x^۲ + py + a = ۰، \quad \gcd(a,p) = ۱$$

جواب صحیح دارد اگر و تنها اگر $(-a/p) = ۱$.

(ب) تعیین کنید که $x^۲ + ۷y - ۲ = ۰$ جواب صحیح دارد یا نه.

۵. ثابت کنید ۲ ریشهٔ اولیهٔ هیچ عدد اولی به‌صورت $p = ۳ \times ۲^n + ۱$، بجز $p = ۱۳$، نیست. [راهنمایی: از قضیهٔ ۹ـ۶ استفاده کنید.]

۶. (الف) ثابت کنید اگر p عدد اول فردی باشد و $\gcd(ab,p) = ۱$، آنگاه حداقل یکی از a، b، یا ab ماندهٔ درجهٔ دومی از p است.

(ب) نشان دهید هر عدد اول p، عدد

$$(n^۲ - ۲)(n^۲ - ۳)(n^۲ - ۶)$$

را به‌ازای $n > ۰$ای می‌شمارد.

۷. اگر p عدد اول فردی باشد، نشان دهید

$$\sum_{a=۱}^{p-۲} (a(a+۱)/p) = -۱$$

[راهنمایی: اگر a' با رابطهٔ $aa' \equiv ۱$ (به‌پیمانهٔ p) تعریف شود، آنگاه $(a(a+۱)/p) = ((۱+a')/p)$. توجه کنید که دامنهٔ تغییرات $۱ + a'$ مجموعهٔ کاملی از مانده‌ها (به پیمانهٔ p)، جز عدد صحیح ۱، است.]

۸. حکمهای زیر را ثابت کنید:

(الف) اگر p و $q = ۲p + ۱$ عددهایی اول و فرد باشند، آنگاه -۴ ریشه‌ای اولیه از q است.

(ب) اگر $p \equiv ۱$ (به پیمانهٔ ۴) عددی اول باشد، آنگاه هردوی -۴ و $(p-۱)/۴$ ماندهٔ درجهٔ دوم p هستند.

۹. اگر $p \equiv ۷$ (به پیمانهٔ ۸)، نشان دهید $p | ۲^{(p-۱)/۲} - ۱$. [راهنمایی: بنابه قضیهٔ ۹ـ۶، $۲^{(p-۱)/۲} \equiv (۲/p) = ۱$ (به پیمانهٔ p).]

۱۰. با استفاده از تمرین ۹ نشان دهید که عددهای $۲^n - ۱$ به ازای

$$n = ۱۱, ۲۳, ۸۳, ۱۳۱, ۱۷۹, ۱۸۳, ۲۳۹, ۲۵۱$$

مرکب‌اند.

۱۱. به فرض اینکه هر دو عدد p و $q = ۴p + ۱$ اول باشند، حکمهای زیر را ثابت کنید:

(الف) هر ناماندهٔ درجهٔ دوم q یا ریشه‌ای اولیه از q است یا از مرتبهٔ ۴ به پیمانهٔ q است. [راهنمایی: اگر a ناماندهٔ درجهٔ دوم q باشد، آنگاه $-۱ = (a/q) \equiv a^{۲p}$ (به پیمانهٔ q)؛ پس مرتبهٔ a به پیمانهٔ q عبارت است از ۱، ۲، ۴، p، $۲p$، یا $۴p$.]

(ب) عدد صحیح ۲ ریشه‌ای اولیه از q است؛ به‌ویژه، ۲ ریشه‌ای اولیه از ۱۳، ۲۹، ۵۳ و ۱۷۳ است.

۱۲. اگر r ریشهٔ اولیهٔ عدد اول فرد p باشد، ثابت کنید حاصلضرب مانده‌های درجهٔ دوم p با $r^{(p^۲-۱)/۴}$، و حاصلضرب نامانده‌های p با $r^{(p-۱)^۲/۴}$، همنهشت به پیمانهٔ pاند. [راهنمایی: فرع قضیهٔ ۹ـ۴ را به‌کار ببرید.]

۱۳. ثابت کنید حاصلضرب مانده‌های درجهٔ دوم عدد اول فرد p، برحسب اینکه $p \equiv ۳$ (به پیمانهٔ ۴) یا $p \equiv ۱$ (به پیمانهٔ ۴)، به‌ترتیب، با ۱ یا ۱− همنهشت به پیمانهٔ p است. [راهنمایی: از تمرین ۱۲ و همنهشتی $r^{(p-۱)/۲} \equiv -۱$ (به پیمانهٔ p) یا، از تمرین ۳ (الف) در بخش ۹ـ۱ و اثبات قضیهٔ ۵ـ۵ استفاده کنید.]

۱۴. (الف) اگر $p > ۳$ عددی اول باشد، نشان دهید مجموع مانده‌های درجهٔ دوم خود را می‌شمارد.

(ب) اگر $p > ۵$ عددی اول باشد، نشان دهید مجموع مربعهای نامانده‌های درجهٔ دوم خود را می‌شمارد.

۱۵. ثابت کنید به‌ازای هر عدد اول $p > ۵$ عددهای صحیح $۱ \leq a, b \leq p - ۱$ وجود دارند به‌طوری که

$$(a/p) = ((a+۱)/p) = ۱ \quad \text{و} \quad (b/p) = ((b+۱)/p) = -۱$$

یعنی مانده‌های درجهٔ دوم متوالی و نامانده‌های درجهٔ دوم متوالی از p وجود دارند.

۱۶. (الف) فرض می‌کنیم p عدد اول فردی باشد و $\gcd(a,p) = \gcd(k,p) = ۱$. نشان دهید که اگر معادلهٔ $x^۲ - ay^۲ = kp$ جواب داشته باشد، آنگاه $(a/p) = ۱$؛ به‌عنوان مثال، $(۲/۷) = ۱$، زیرا $۴ \times ۷ = ۲^۲ \times ۲ - ۶^۲$. [راهنمایی: اگر $x_۰$ و $y_۰$ در معادله صدق کنند، آنگاه $(x_۰ y_۰^{p-۲})^۲ \equiv a$ (به پیمانهٔ p).]

(ب) با بررسی معادلهٔ $x^۲ + ۵y^۲ = ۷$، نشان دهید که عکس حکم قسمت (الف) لزوماً برقرار نیست.

(پ) نشان دهید که، به‌ازای هیچ عدد اول p که (به پیمانهٔ ۸) $p \equiv \pm ۳$، معادلهٔ $x^۲ - ۲y^۲ = p$ جواب ندارد.

۱۷. اگر (به پیمانهٔ ۴) $p \equiv ۱$، ثابت کنید

$$\sum_{a=۱}^{(p-۱)/۲} (a/p) = ۰$$

[راهنمایی: $(a/p) = (p - a/p)$.]

۳ـ۹ تقابل درجهٔ دوم

فرض می‌کنیم p و q دو عدد اول و فرد متمایز باشند. در این صورت هر دو نماد لژاندر (p/q) و (q/p) تعریف می‌شوند. طبیعی است که بخواهیم بدانیم آیا در صورت معلوم بودن مقدار (q/p) می‌توان مقدار (p/q) را تعیین کرد یا نه. به بیانی کلیتر، آیا اصلاً رابطه‌ای میان مقدارهای این دو نماد وجود دارد؟ رابطهٔ اصلی بین آنها را اویلر در ۱۷۸۳ حدس زد و دو سال بعد لژاندر آن را به‌طور ناقص ثابت کرد. لژاندر این رابطه را با استفاده از نماد خود به‌صورت زیبا و ظریفی ارائه کرد که به قانون تقابل درجهٔ دوم معروف شد:

$$(p/q)(q/p) = (-۱)^{\frac{p-۱}{۲}\frac{q-۱}{۲}}$$

لژاندر با فرض برقراری حکمی که اثبات آن به اندازهٔ اثبات خود قانون دشوار است دچار لغزش شد؛ این حکم چنین است که به‌ازای هر عدد اول p، (به پیمانهٔ ۸) $p \equiv ۱$، عدد اول دیگر q ای، (به‌پیمانهٔ ۴) $q \equiv ۳$، وجود دارد، به‌طوری‌که، p ماندهٔ درجهٔ دوم q است. ولی او از میدان به در نرفت و اثبات دیگری در رسالهٔ درباب نظریهٔ اعداد خود (۱۷۹۸) ارائه کرد؛ این اثبات نیز اشکال داشت، زیرا لژاندر نامتناهی بودن تعداد عددهای اول را در تصاعدهای عددی خاصی دانسته فرض کرده بود (حکمی که بالاخره آن را دیریکله در ۱۸۳۷ با استفاده از استدلالهای بسیار پیچیده‌ای از نظریهٔ متغیرهای مختلط ثابت کرد).

گاوس در هجده سالگی (۱۷۹۵)، ظاهراً بدون اطلاع از کار اویلر یا لژاندر، قانون تقابل را دوباره کشف کرد و بعد از یک سال کوشش مداوم، نخستین اثبات کامل آن را به‌دست آورد. گاوس در این باره می‌گوید: «یک سال تمام عذاب کشیدم و کوشش جانفرسایی به‌خرج دادم تا بالاخره، اثباتی را که در

چهارمین بخش تحقیقات حسابی شرح داده شده به‌دست آوردم.» گاوس در تحقیقات حسابی ـــ که گرچه در ۱۷۹۸ به پایان رسید، در ۱۸۰۱ منتشر شد ـــ با این ادعا که قضیه به کسی تعلق دارد که نخستین اثبات دقیق آن را ارائه کرده باشد، قانون تقابل درجهٔ دوم را به خودش نسبت داد. لژاندر برآشفت و زبان به شکوه گشود: «این بی‌شرمی زایدالوصف از شخصی که واجد شایستگیهای کافی است و نیازی به دزدیدن کشفهای دیگران ندارد، باورکردنی نیست.» بحث دربارهٔ تقدم میان این‌دو نفر بیفایده بود زیرا هریک خود را محق می‌دانست و توجهی به دیگری نداشت. گاوس پنج اثبات متفاوت دیگر از این قانون، که آن را «گل سرسبد حساب عالی» می‌نامید، ارائه کرد، اثباتی دیگر نیز میان یادداشتهایش پیدا شد. اثباتی که در زیر عرضه می‌شود، شکل دیگری از یکی از برهانهای خود گاوس است که دانشجویش فردیناند آیزنشتاین[1] (۱۸۲۳ـ۱۸۵۲) به‌دست داده است. این اثبات پیچیده است (شاید توقع اثباتی ساده، معقول هم نباشد)، ولی ایدهٔ زیربنایی آن نسبتاً ساده است.

قضیهٔ ۹ـ۹ (قانون تقابل درجهٔ دوم گاوس). اگر p و q عددهای اول فرد متمایزی باشند، آنگاه

$$(p/q)(q/p) = (-۱)^{\frac{p-۱}{۲}\frac{q-۱}{۲}}$$

اثبات. مستطیلی با رأسهای $(۰,۰)$، $(p/۲,۰)$، $(۰,q/۲)$، و $(p/۲,q/۲)$ در صفحهٔ مختصات xy در نظر می‌گیریم. ناحیهٔ داخلی این مستطیل را، که حاوی هیچ یک از خطهای مرزی نیست، با R نشان می‌دهیم. طرح کلی اثبات، عبارت از شمارش تعداد نقطه‌هایی مشبکه‌ای (یعنی نقطه‌هایی که مختصهای آنها عددهایی صحیح‌اند) در داخل R به دو روش متفاوت است. چون هردوی p و q فردند، نقطه‌های مشبکه‌ای در R عبارت از همهٔ نقطه‌های (n,m)ای هستند که $۱ \leq n \leq (p-۱)/۲$ و $۱ \leq m \leq (q-۱)/۲$؛ تعداد چنین نقطه‌هایی به وضوح برابر است با

$$\frac{p-۱}{۲} \times \frac{q-۱}{۲}$$

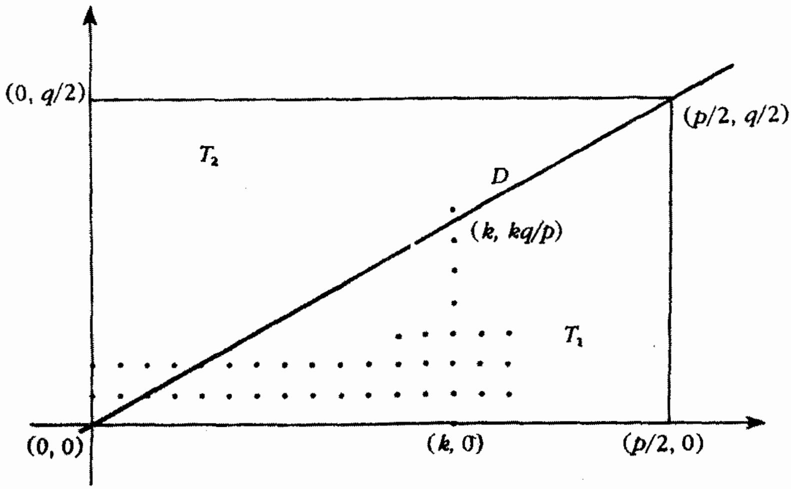
اکنون قطر D از $(۰,۰)$ تا $(p/۲,q/۲)$ را که معادله‌اش به‌صورت $y = (q/p)x$ یا معادلش، $py = qx$ است درنظر می‌گیریم. چون $\gcd(p,q) = ۱$، هیچ یک از نقطه‌های مشبکه‌ای داخل R بر D واقع نیست زیرا p باید مختص x هر نقطهٔ مشبکه‌ای واقع بر خط $py = qx$ را بشمارد، و q باید مختص y آن را بشمارد؛ چنین نقطه‌هایی در R وجود ندارد. فرض می‌کنیم $T_۱$ ناحیه‌ای از R است که زیر قطر D است و $T_۲$ ناحیهٔ بالایی است. طبق آنچه گفتیم، کافی است تعداد نقطه‌های مشبکه‌ای داخل هریک از این مثلثها را بشماریم.

تعداد عددهای صحیح دربازهٔ $۰ < y < (kq)/p$ برابر با $[(kq)/p]$ است. بنابراین، به‌ازای $۱ \leq k \leq (p-۱)/۲$، در $T_۱$ دقیقاً $(kq)/p$ نقطهٔ مشبکه‌ای مستقیماً بالای نقطهٔ $(k,۰)$ و زیر

1. Eisenstein

D، یا به بیان دیگر، واقع بر پاره‌خط عمودی از $(k, ۰)$تا $(k, kq/p)$ وجود دارد. نتیجه می‌گیریم که تعداد کل نقطه‌های مشبکه‌ای واقع در $T_۱$ برابر است با

$$\sum_{k=۱}^{(p-۱)/۲} \left[\frac{kq}{p}\right]$$



محاسبه‌ای مشابه، با تعویض نقشهای p و q، نشان می‌دهد که تعداد نقطه‌های مشبکه‌ای واقع در داخل $T_۲$ برابر است با

$$\sum_{j=۱}^{(q-۱)/۲} \left[\frac{jp}{q}\right]$$

به این ترتیب، شمارش نقطه‌های مشبکه‌ای داخل R تکمیل می‌شود، یعنی

$$\frac{p-۱}{۲} \times \frac{q-۱}{۲} = \sum_{k=۱}^{(p-۱)/۲} \left[\frac{kq}{p}\right] + \sum_{j=۱}^{(q-۱)/۲} \left[\frac{jp}{q}\right]$$

اکنون وقت آن رسیده که لم گاوس نقش خود را ایفا کند:

$$\begin{aligned}(p/q)(q/p) &= (-۱)^{\sum_{j=۱}^{(q-۱)/۲}\left[\frac{jp}{q}\right]} \times (-۱)^{\sum_{k=۱}^{(p-۱)/۲}\left[\frac{kq}{p}\right]} \\ &= (-۱)^{\sum_{j=۱}^{(q-۱)/۲}\left[\frac{jp}{q}\right]+\sum_{k=۱}^{(p-۱)/۲}\left[\frac{kq}{p}\right]} = (-۱)^{\frac{p-۱}{۲}\frac{q-۱}{۲}}\end{aligned}$$

و به این ترتیب، اثبات قانون تقابل درجهٔ دوم به انجام رسیده است. □

یک نتیجهٔ مستقیم آن چنین است:

فرع ۱. اگر p و q عددهای اول متمایزی باشند، آنگاه

$$(p/q)(q/p) = \begin{cases} ۱ & \text{اگر } p \equiv ۱ \text{ (به پیمانهٔ ۴) یا } q \equiv ۱ \text{ (به پیمانهٔ ۴)} \\ -۱ & \text{اگر } p \equiv q \equiv ۳ \text{ (به پیمانهٔ ۴)} \end{cases}$$

اثبات. عدد $(p-۱)/۲ \times (q-۱)/۲$ زوج است اگر و تنها اگر حداقل یکی از عددهای صحیح p و q به‌صورت $۴k+۱$ باشد؛ اگر هردو به‌صورت $۴k+۳$ باشند، آنگاه $(p-۱)/۲ \times (q-۱)/۲$ فرد است. □

با ضرب هردو طرف رابطهٔ تقابل درجهٔ دوم در (q/p) و با استفاده از $(q/p)^۲ = ۱$، نتیجهٔ زیر را به‌دست می‌آوریم

فرع ۲. اگر p و q عددهای اول فرد متمایزی باشند، آنگاه

$$(p/q) = \begin{cases} (q/p) & \text{اگر } p \equiv ۱ \text{ (به پیمانهٔ ۴) یا } q \equiv ۱ \text{ (به پیمانهٔ ۴)} \\ -(q/p) & \text{اگر } p \equiv q \equiv ۳ \text{ (به پیمانهٔ ۴)} \end{cases}$$

ببینیم از این حکمها چه نتیجه‌ای حاصل می‌شود. فرض می‌کنیم p عددی فرد و اول و $a \neq \pm ۱$ عدد صحیحی بخش ناپذیر بر p باشد. به‌علاوه فرض می‌کنیم a دارای تجزیهٔ

$$a = \pm ۲^{k_۰} p_۱^{k_۱} p_۲^{k_۲} \dots p_r^{k_r}$$

باشد که در آن p_i ها عددهای اول فرد متمایزی هستند. چون نماد لژاندر ضربی است، پس

$$(a/p) = (\pm ۱/p)(۲/p)^{k_۰}(p_۱/p)^{k_۱} \dots (p_r/p)^{k_r}$$

برای محاسبهٔ (a/p)، کافی است هریک از نمادهای $(-۱/p)$، $(۲/p)$، و (p_i/p) را حساب کنیم. دربارهٔ مقدارهای $(-۱/p)$ و $(۲/p)$ پیشتر بحث شد، بنابراین تنها مانع (p_i/p) است، که در آن p_i و p عددهای اول فرد متمایزی هستند؛ اینجاست که قانون تقابل درجه دوم وارد میدان می‌شود، زیرا، بنا به فرع ۲، می‌توانیم به‌جای (p_i/p)، نماد لژاندر جدیدی با مخرج کوچکتر درنظر بگیریم. با ادامهٔ معکوس کردن و تقسیم، محاسبه را می‌توان به محاسبهٔ کمیتهای شناختهٔ

$$(-۱/q)\text{،} (۱/q)\text{، و } (۲/q)$$

تحویل کرد. البته همهٔ این مطالب تا اندازه‌ای مبهم‌اند، بنابراین مثالی واقعی می‌آوریم.

مثال ۹ـ۵

به‌عنوان نمونه، نماد لژاندر $(۲۹/۵۳)$ را درنظر می‌گیریم. چون هم (به پیمانهٔ ۴) $۱ \equiv ۲۹$ و هم (به پیمانهٔ ۴) $۱ \equiv ۵۳$، ملاحظه می‌کنیم که

$$\begin{aligned}(۲۹/۵۳) &= (۵۳/۲۹) = (۲۴/۲۹) = (۲/۲۹)\,(۳/۲۹)\,(۴/۲۹)\\ &= (۲/۲۹)\,(۳/۲۹)\end{aligned}$$

بنابه قضیهٔ ۹ـ۶، $۱- = (۲/۲۹)$، و با معکوس کردن دوباره داریم

$$(۳/۲۹) = (۲۹/۳) = (۲/۳) = -۱$$

که در آن از همنهشتی (به پیمانهٔ ۳) $۲ \equiv ۲۹$ استفاده کرده‌ایم. نتیجهٔ نهایی این است که

$$(۲۹/۵۳) = (۲/۲۹)\,(۳/۲۹) = (-۱)(-۱) = ۱$$ ■

با استفاده از قانون تقابل درجهٔ دوم، پاسخ بسیار رضایتبخشی برای مسألهٔ تعیین همهٔ عددهای اول فرد $p \neq ۳$ با ماندهٔ درجهٔ دوم ۳، به‌دست می‌آید. چون (به پیمانهٔ ۴) $۳ \equiv ۳$، بنابه فرع ۲ی فوق

$$(۳/p) = \begin{cases} (p/۳) & \text{اگر (به پیمانهٔ ۴)}\ \ p \equiv ۱ \\ -(p/۳) & \text{اگر (به پیمانهٔ ۴)}\ \ p \equiv ۳ \end{cases}$$

ولی (به پیمانهٔ ۳) $p \equiv ۱$ یا (به پیمانهٔ ۳) $p \equiv ۲$. بنا به قضیه‌های ۹ـ۲ و ۹ـ۶

$$(p/۳) = \begin{cases} ۱ & \text{اگر (به پیمانهٔ ۳)}\ \ p \equiv ۱ \\ -۱ & \text{اگر (به پیمانهٔ ۳)}\ \ p \equiv ۲ \end{cases}$$

که نتیجه می‌دهد $۱ = (۳/p)$ اگر و تنها اگر

(۱) $\qquad$ (به پیمانهٔ ۳) $p \equiv ۱$ $\qquad$ و $\qquad$ (به پیمانهٔ ۴) $p \equiv ۱$

یا

(۲) $\qquad$ (به پیمانهٔ ۳) $p \equiv ۲$ $\qquad$ و $\qquad$ (به پیمانهٔ ۴) $p \equiv ۳$

محدودیتهای (۱) معادل با (به پیمانهٔ ۱۲) ۱ $\equiv p$ و محدودیتهای (۲) معادل با (به پیمانهٔ ۱۲) ۱ − $\equiv$ ۱۱ $\equiv p$ است. نتیجهٔ مطالب بالا این است:

قضیهٔ ۹ـ۱۰ اگر ۳ $\neq p$ عدد اول فردی باشد، آنگاه

$$(۳/p) = \begin{cases} ۱ & p \equiv \pm ۱ \text{ (به پیمانهٔ ۱۲) اگر} \\ -۱ & p \equiv \pm ۵ \text{ (به پیمانهٔ ۱۲) اگر} \end{cases}$$

مثال ۹ـ۶

هدف این مثال بررسی وجود جوابهای همنهشتی

$$x^۲ \equiv ۱۹۶ \text{ (به پیمانهٔ ۱۳۵۷)}$$

است. چون ۵۹ × ۲۳ = ۱۳۵۷، همنهشتی داده‌شده حلپذیر است اگر و تنها اگر هردوی

$$x^۲ \equiv ۱۹۶ \text{ (به پیمانهٔ ۵۹)} \quad \text{و} \quad x^۲ \equiv ۱۹۶ \text{ (به پیمانهٔ ۲۳)}$$

حلپذیر باشند. روش ما تعیین مقدارهای نمادهای لژاندر (۱۹۶/۲۳) و (۱۹۶/۵۹) است.
در محاسبهٔ (۱۹۶/۲۳) به استفاده از قضیهٔ ۹ـ۱۰ نیاز داریم

$$(۱۹۶/۲۳) = (۱۲/۲۳) = (۳/۲۳) = ۱$$

بنابراین، همنهشتی (به پیمانهٔ ۲۳) ۱۹۶ $\equiv x^۲$ جواب دارد. در ارتباط با نماد (۱۹۶/۵۹)، بنابه قانون تقابل درجهٔ دوم می‌توانیم بنویسیم

$$(۱۹۶/۵۹) = (۱۹/۵۹) = -(۵۹/۱۹) = -(۲/۱۹) = -(-۱) = ۱$$

بنابراین می‌توان همنهشتی (به پیمانهٔ ۵۹) ۱۹۶ $\equiv x^۲$ و درنتیجه، همنهشتی (به پیمانهٔ ۱۳۵۷) ۱۹۶ $\equiv x^۲$، را حل کرد. ■

اکنون به‌کاربرد کاملاً متفاوتی از این ایده‌ها می‌پردازیم. در یکی از مراحل قبل، ملاحظه شد که اگر ۱ + $F_n = ۲^{۲^n}$، ۱ $< n$، عددی اول باشد، آنگاه ۲ ریشهٔ اولیه F_n نیست. اکنون وسیلهٔ لازم را در اختیار داریم که نشان دهیم عدد صحیح ۳ ریشه‌ای اولیه از هر چنین F_nای است.

به‌عنوان نخستین گام در این راستا، ملاحظه می‌کنیم که هر F_n به‌صورت $۱۲k + ۵$ است. با استدلال استقرایی ساده‌ای معلوم می‌شود که به‌ازای $m = ۱, ۲, \ldots$، $۴^m \equiv ۴$ (به پیمانهٔ ۱۲)؛ پس باید داشته باشیم

$$F_n = ۲^{۲^n} + ۱ = ۲^{۲m} + ۱ = ۴^m + ۱ \equiv ۵ \ (\text{به پیمانهٔ } ۱۲)$$

اگر F_n عددی اول باشد، بنابه قضیهٔ ۹ـ۱۰ داریم

$$(۳/F_n) = -۱$$

یا، با استفاده از معیار اویلر

$$۳^{\frac{F_n - ۱}{۲}} \equiv -۱ \ (\text{به پیمانهٔ } F_n)$$

با به‌کارگیری تابع ϕ، همنهشتی اخیر به این معنی است که

$$۳^{\phi(F_n)/۲} \equiv -۱ \ (\text{به پیمانهٔ } F_n)$$

از اینجا نتیجه می‌شود که ۳ دارای مرتبهٔ $\phi(F_n)$ به پیمانهٔ F_n است و بنابراین ۳ ریشه‌ای اولیه از F_n است

تمرینهای ۹ـ۳

۱. نمادهای لژاندر زیر را حساب کنید:

(الف) $(۷۱/۷۳)$، (ب) $(-۲۱۹/۳۸۳)$، (پ) $(۴۶۱/۷۷۳)$، (ت) $(۱۲۳۴/۴۵۶۷)$، (ث) $(۳۶۵۸/۱۲۷۰۳)$. [راهنمایی: $۳۶۵۸ = ۲ \times ۳۱ \times ۵۹$.]

۲. ثابت کنید ۳ ناماندهٔ درجهٔ دومی از همهٔ عددهای اول به‌صورت $۲^{۲n} + ۱$ و همهٔ عددهای اول به‌صورت $۲^p - ۱$ است (p عددی اول و فرد). [راهنمایی: به ازای هر n، $۴^n \equiv ۴$ (به پیمانهٔ ۱۲).]

۳. تعیین کنید کدام یک از همنهشتیهای درجهٔ دوم زیر حلپذیر است

(الف) $x^۲ \equiv ۲۱۹$ (به پیمانهٔ ۴۱۹)

(ب) $۳x^۲ + ۶x + ۵ \equiv ۰$ (به پیمانهٔ ۸۹)

(پ) $۲x^۲ + ۵x - ۹ \equiv ۰$ (به پیمانهٔ ۱۰۱)

۴. نشان دهید که اگر p عدد اول فردی باشد، آنگاه

$$(-۲/p) = \begin{cases} ۱ & \text{اگر } p \equiv ۱ \ (\text{به پیمانهٔ } ۸) \text{ یا } p \equiv ۳ \ (\text{به پیمانهٔ } ۸) \\ -۱ & \text{اگر } p \equiv ۵ \ (\text{به پیمانهٔ } ۸) \text{ یا } p \equiv ۷ \ (\text{به پیمانهٔ } ۸) \end{cases}$$

۵. (الف) ثابت کنید که اگر $p > ۳$ عدد اول فردی باشد، آنگاه

$$(-۳/p) = \begin{cases} ۱ & \text{اگر } p \equiv ۱ \text{ (به پیمانهٔ ۶)} \\ -۱ & \text{اگر } p \equiv ۵ \text{ (به پیمانهٔ ۶)} \end{cases}$$

(ب) با استفاده از قسمت (الف)، نشان دهید تعداد عددهای اول به‌صورت $۶k + ۱$ نامتناهی است. [راهنمایی: فرض کنید $p_۱, p_۲, \ldots, p_r$ همگی عددهای اول به‌صورت $۶k + ۱$اند و عدد صحیح $N = (۲p_۱p_۲\ldots p_r)^۲ + ۳$ را درنظر بگیرید.]

۶. با استفاده از قضیهٔ ۹ـ۲ و تمرینهای ۴ و ۵ تعیین کنید کدام عددهای اول، هریک از $n^۲ + ۱$، $n^۲ + ۲$، $n^۲ + ۳$ را به‌ازای n ای می‌شمارند.

۷. ثابت کنید تعداد عددهای اولِ به‌صورت $۸k + ۳$ نامتناهی است. [راهنمایی: فرض کنید فقط تعدادی متناهی عدد اول به‌صورت $۸k + ۳$ وجود دارد، مثلاً $p_۱, p_۲, \ldots, p_r$، و عدد صحیح $N = (p_۱p_۲\ldots p_r)^۲ + ۲$ را درنظر بگیرید.]

۸. عدد اول pای پیدا کنید که همزمان قابل بیان به‌صورت $x^۲ + y^۲$، $u^۲ + ۲v^۲$، $r^۲ + ۳s^۲$ باشد. [راهنمایی: $(-۱/p) = (-۲/p) = (-۳/p) = ۱$.]

۹. اگر به‌ازای aای، عددهای فرد اول p و q در $p = q + ۴a$ صدق کنند، ثابت کنید

$$(a/p) = (a/q)$$

و به‌ویژه، اینکه $(۶/۱۳) = (۶/۳۷)$. [راهنمایی: توجه کنید که $(a/p) = -(-q/p)$ و از قانون تقابل درجهٔ دوم استفاده کنید.]

۱۰. هریک از حکمهای زیر را ثابت کنید:

(الف) $(۵/p) = ۱$ اگر وتنها اگر $p \equiv ۱, ۹, ۱۱, ۱۹$ (به پیمانهٔ ۲۰).

(ب) $(۶/p) = ۱$ اگر و تنها اگر $p \equiv ۱, ۵, ۱۹, ۲۳$ (به پیمانهٔ ۲۴).

(پ) $(۷/p) = ۱$ اگر و تنها اگر $p \equiv ۱, ۳, ۹, ۱۹, ۲۵, ۲۷$ (به پیمانهٔ ۲۸).

۱۱. ثابت کنید تعداد عددهای اولِ به‌صورت $۵k - ۱$ نامتناهی است. [راهنمایی: به‌ازای هر $n > ۱$، عدد صحیح $۵(n!)^۲ - ۱$ دارای مقسوم‌علیه اول pای بزرگتر از n است که به‌صورت $۵k + ۱$ نیست؛ بنابراین، $(۵/p) = ۱$.]

۱۲. نشان دهید که

(الف) مقسوم‌علیه‌های اول مخالف سهٔ عدد صحیح $n^۲ - n + ۱$ به‌صورت $۶k + ۱$ هستند. [راهنمایی: اگر این مقسوم‌علیه‌ها را p بنامیم و $p | n^۲ - n + ۱$، آنگاه $(۲n - ۱)^۲ \equiv -۳$ (به پیمانهٔ p).]

(ب) مقسوم‌علیه‌های اول مخالف پنجِ عدد صحیح $n^۲ + n - ۱$ به‌صورت $۱۰k + ۱$ یا $۱۰k + ۹$ هستند.

(پ) اگر مقسوم‌علیه‌های اول عدد صحیح $۲n(n + ۱) + ۱$ را با p نشان دهیم، این مقسوم‌علیه‌ها به‌صورت (به پیمانهٔ ۴) $p \equiv ۱$ هستند. [راهنمایی: اگر $p|۲n(n + ۱) + ۱$، آنگاه (به پیمانهٔ p) $(۲n + ۱)^۲ \equiv -۱$.]

(ت) مقسوم‌علیه‌های اول pی عدد صحیح $۳n(n + ۱) + ۱$ به‌صورت (به پیمانهٔ ۶) $p \equiv ۱$ هستند.

۱۳. (الف) نشان دهید که اگر p مقسوم‌علیه اولی از $۸۳۹ = ۳۸^۲ - ۵ \times ۱۱^۲$ باشد، آنگاه $(۵/p) = ۱$. با استفاده از این نتیجه نشان دهید ۸۳۹ عددی اول است. [راهنمایی: کافی است عددهای اول $p < ۲۹$ را درنظر بگیرید.]

(ب) ثابت کنید هم $۳۷۹ = ۲۰^۲ - ۳$ و هم $۷۳۳ = ۲۹^۲ - ۳ \times ۶^۲$ عدد اول‌اند.

۱۴. همنهشتی درجهٔ دوم (به پیمانهٔ ۳۵) $x^۲ \equiv ۱۱$ را حل کنید. [راهنمایی: بعد از حل (به پیمانهٔ ۵) $x^۲ \equiv ۱۱$ و (به پیمانهٔ ۷) $x^۲ \equiv ۱۱$، از قضیهٔ باقیماندهٔ چینی استفاده کنید.]

۱۵. نشان دهید ۷ ریشه‌ای اولیه از هر عدد اول فردِ به‌صورت $p = ۲^{۴n} + ۱$ است. [راهنمایی: چون (به پیمانهٔ ۷) ۵یا $p \equiv ۳$، $(۷/p) = (p/۷) = -۱$.]

۱۶. فرض می‌کنیم a و $b > ۱$ عددهایی صحیح متباین باشند و b فرد باشد. اگر $b = p_۱p_۲ \ldots p_r$ تجزیهٔ b به عددهای اول (نه لزوماً متمایز) باشد، آنگاه نماد (a/b)، موسوم به نماد ژاکوبی، به‌صورت

$$(a/b) = (a/p_۱)(a/p_۲) \ldots (a/p_r)$$

تعریف می‌شود که در آن نمادهای سمت راست برابری نمادهای لژاندر هستند. مقادیر نمادهای ژاکوبی

$$(۲۱/۲۲۱)،(۲۱۵/۲۵۳) \text{ و } (۶۳۱/۱۰۹۹)$$

را حساب کنید.

۱۷. تحت فرض تمرین فوق، نشان دهید اگر a ماندهٔ درجهٔ دومی از b باشد، آنگاه $(a/b) = ۱$؛ ولی، عکس این موضوع صادق نیست.

۱۸. ثابت کنید نماد ژاکوبی ویژگیهای زیر را دارد: اگر b و b' عددهای صحیح و مثبت و فردی باشند و $\gcd(aa', bb') = ۱$، آنگاه

(الف) از (به پیمانهٔ b) $a \equiv a'$ نتیجه می‌شود $(a/b) = (a'/b)$.

(ب) $(aa'/b) = (a/b)(a'/b)$

(پ) $(a/bb') = (a/b)(a/b')$

(ت) $(a^۲/b) = (a/b^۲) = ۱$

(ث) $۱/b = ۱$

(ج) $(-۱/b) = (-۱)^{(b-۱)/۲}$ [راهنمایی: اگر u و v عددهای صحیح فردی باشند، آنگاه (به پیمانهٔ ۲) $(uv-۱)/۲ \equiv (u-۱)/۲ + (v-۱)/۲$.]

(چ) $(۲/b) = (-۱)^{(b^۲-۱)/۸}$. [راهنمایی: اگر u و v عددهای صحیح فردی باشند، آنگاه (به پیمانهٔ۲) $[(uv)^۲ - ۱]/۸ \equiv (u^۲-۱)/۸ + (v^۲-۱)/۸$.]

۱۹. قانون تقابل درجهٔ دوم تعمیم‌یافته را ثابت کنید: اگر $a, b > ۱$ عددهای صحیح و فرد و مثبت متباینی باشند، آنگاه

$$(a/b)(b/a) = (-۱)^{\frac{a-۱}{۲}\frac{b-۱}{۲}}$$

[راهنمایی: از راهنمایی ۱۸ (ج) استفاده کنید.]

۲۰. با استفاده از قانون تقابل درجهٔ دوم تعمیم‌یافته، تعیین کنید همنهشتی (به پیمانهٔ ۱۱۰۵) $x^۲ \equiv ۲۳۱$ جواب دارد یا نه.

۹ـ۴ همنهشتیهای درجهٔ دوم با پیمانه‌های مرکب

تا اینجا، در همهٔ مرحله‌های بحث، همنهشتیهای درجهٔ دوم با پیمانه‌های اول (فرد) از اهمیت بسیار زیادی برخوردار بوده‌اند. بقیهٔ قضیه‌ها با کاربرد پیمانهٔ مرکب افق بحث را گسترش می‌دهند. در آغاز وضعیتی را درنظر می‌گیریم که در آن پیمانهٔ توانی از عددی اول است.

قضیهٔ ۹ـ۱۰ اگر p عددی اول و فرد باشد و $\gcd(a, p) = ۱$، آنگاه همنهشتی

$$x^۲ \equiv a \ (\text{به پیمانهٔ } p^n), \quad n \geq ۱$$

جواب دارد اگر و تنها اگر $(a, p) = ۱$.

اثبات. همان‌طور که در بسیاری از قضیه‌های مشتمل بر «اگر و تنها اگر» دیده می‌شود، در اینجا هم نیمی از اثبات بدیهی است و نیمهٔ دیگر است که به تلاش قابل توجهی نیازمند است: اگر (به پیمانهٔ p^n) $x^۲ \equiv a$ جوابی داشته باشد، آنگاه (به پیمانهٔ p) $x^۲ \equiv a$ نیز دارای جواب است ــ در واقع، همان جواب را دارد ــ پس $(a/p) = ۱$.

برعکس، فرض می‌کنیم $(a/p) = ۱$. به استقرا بر n ثابت می‌کنیم $x^۲ \equiv a$ (به پیمانهٔ p^n) نیز حلپذیر است. اگر $n = ۱$، واقعاً چیزی برای اثبات نداریم؛ درواقع، $(a/p) = ۱$ معادل است با اینکه بگوییم $x^۲ \equiv a$ (به پیمانهٔ p) را می‌توان حل کرد. فرض می‌کنیم حکم به ازای $n = k \geq ۱$ برقرار است، یعنی $x^۲ \equiv a$ (به پیمانهٔ p^k) جواب $x_۰$ای دارد. در این صورت به‌ازای bی مناسبی، $x_۰^۲ = a + bp^k$. در گذر از k به $k + ۱$، با استفاده از $x_۰$ و b جواب صریحی برای همنهشتی $x^۲ \equiv a$ (به پیمانهٔ $p^{k+۱}$) به‌دست می‌آوریم.

به این منظور، نخست با حل همنهشتی خطی

$$۲x_۰y \equiv -b \text{ (به پیمانهٔ } p\text{)}$$

جواب یکتای $y_۰$ای به پیمانهٔ p به‌دست می‌آوریم (این کار قطعاً عملی است زیرا $\gcd(۲x_۰, p) = ۱$). سپس، عدد صحیح

$$x_۱ = x_۰ + y_۰p^k$$

را درنظر می‌گیریم. با مربع کردن این عدد صحیح، به‌دست می‌آوریم

$$\begin{aligned}(x_۰ + y_۰p^k)^۲ &= x_۰^۲ + ۲x_۰y_۰p^k + y_۰^۲p^{۲k}\\ &= a + (b + ۲x_۰y_۰)p^k + y_۰^۲p^{۲k}\end{aligned}$$

ولی $p \mid (b + ۲x_۰y_۰)$، که از آن نتیجه می‌شود

$$x_۱^۲ = (x_۰ + y_۰p^k)^۲ \equiv a \text{ (به پیمانهٔ } p^{k+۱}\text{)}$$

بنابراین، همنهشتی $x^۲ \equiv a$ (به پیمانهٔ p^n) دارای جوابی به‌ازای $n = k + ۱$ و، به استقرا، به‌ازای همهٔ عددهای صحیح مثبت n است. □

مثالی مشخص را به تفصیل توضیح می‌دهیم. نخستین مرحله در به‌دست آوردن جوابی از، مثلاً، همنهشتی درجهٔ دوم

$$x^۲ \equiv ۲۳ \text{ (به پیمانهٔ } ۷^۲\text{)}$$

حل $x^۲ \equiv ۲۳$ (به پیمانهٔ ۷)، یا هم‌ارز با آن، همنهشتی

$$x^۲ \equiv ۲ \text{ (به پیمانهٔ } ۷\text{)}$$

است. چون ۱ = (۲/۷)، قطعاً جوابی وجود دارد؛ درواقع ۳ = $x_\circ$ انتخابی بدیهی است. $x_\circ^۲$ را می‌توان به‌صورت

$$۳^۲ = ۹ = ۲۳ + (-۲)۷$$

نوشت به گونه‌ای که ۲− = b (در این حالت ویژه، عدد صحیح ۲۳ نقش a را بازی می‌کند). سپس به پیروی از اثبات قضیهٔ ۹ـ۱۱، y را به‌گونه‌ای تعیین می‌کنیم که

$$۶y \equiv ۲ \ (\text{به پیمانهٔ } ۷)$$

یعنی، (به پیمانهٔ ۷) ۱ ≡ $۳y$. مقدار ۵ ≡ $y_\circ$ در این همنهشتی خطی صدق می‌کند. پس

$$x_\circ + ۷y_\circ = ۳ + ۷ \times ۵ = ۳۸$$

جوابی از همنهشتی اولیهٔ (به پیمانهٔ ۴۹) ۲۳ ≡ $x^۲$ است. باید متوجه بود که (به پیمانهٔ ۴۹) ۱۱ ≡ ۳۸− تنها جواب دیگر معادله است.

اگر به‌جای این همنهشتی، همنهشتی

$$x^۲ \equiv ۲۳ \ (\text{به پیمانهٔ } ۷^۳)$$

برای حل پیشنهاد می‌شد، با شروع کردن از

$$x^۲ \equiv ۲۳ \ (\text{به پیمانهٔ } ۷^۲)$$

جواب ۳۸ = $x_\circ$ را به‌دست می‌آوردیم. چون

$$۳۸^۲ = ۲۳ + ۲۹ \times ۷^۲$$

عدد صحیح b برابر است با ۲۹. سپس جواب یکتای ۱ = $y_\circ$ از همنهشتی خطی

$$۷۶y \equiv -۲۹ \ (\text{به پیمانهٔ } ۷)$$

را به‌دست می‌آوردیم. در این صورت

$$x_\circ + y_\circ \times ۷^۲ = ۳۸ + ۱ \times ۴۹ = ۸۷$$

همراه با (به پیمانهٔ ۷^۳) ۲۵۶ ≡ ۸۷− در (به پیمانهٔ ۷^۳) ۲۳ ≡ $x^۲$ صدق می‌کنند.

حال که بحث مفصلی دربارهٔ عددهای اول فرد کرده‌ایم، حالت $p = ۲$ را درنظر می‌گیریم. قضیهٔ زیر، اطلاعات مربوطه را ارائه می‌کند.

قضیهٔ ۹ـ۱۱ فرض می‌کنیم a یک عدد صحیح فرد باشد. در این صورت

(۱) (به پیمانهٔ ۲) $x^۲ \equiv a$ همیشه جواب دارد؛

(۲) (به پیمانهٔ ۴) $x^۲ \equiv a$ جواب دارد اگر و تنها اگر (به پیمانهٔ ۴) $a \equiv ۱$؛

(۳) (به پیمانهٔ ۲^n) $x^۲ \equiv a$، به‌ازای $n \geq ۳$، جواب دارد اگر و تنها اگر (به پیمانهٔ ۸) $a \equiv ۱$.

اثبات. حکم نخست بدیهی است. دومی مبتنی بر این نکته است که مربع هر عدد صحیح فرد همنهشت با ۱ به پیمانهٔ ۴ است. پس، (به پیمانهٔ ۴) $x^۲ \equiv a$ را فقط وقتی a به‌صورت $۴k + ۱$ است، می‌توان حل کرد؛ در این حالت، دو جواب به پیمانهٔ ۴ وجود دارد، یعنی $x = ۱$، $x = ۳$.

اکنون حالت $n \geq ۳$ را در نظر می‌گیریم. چون مربع هر عدد صحیح فرد همنهشت با ۱ به پیمانهٔ ۸ است، ملاحظه می‌کنیم برای آنکه معادلهٔ (به پیمانهٔ ۲^n) $x^۲ \equiv a$ حلپذیر باشد، لازم است a به‌صورت $۸k + ۱$ باشد. به عکس، فرض می‌کنیم (به پیمانهٔ ۸) $a \equiv ۱$ و با استقرا روی n ادامه می‌دهیم. اگر $n = ۳$، همنهشتی (به پیمانهٔ ۲^n) $x^۲ \equiv a$ قطعاً حلپذیر است؛ درواقع، هریک از عددهای صحیح ۱، ۳، ۵، ۷ در (به پیمانهٔ ۸) $x^۲ \equiv ۱$ صدق می‌کنند. مقداری از $n > ۳$ را ثابت نگاه می‌داریم و، به‌عنوان فرض استقرا، فرض می‌کنیم همنهشتی (به پیمانهٔ ۲^n) $x^۲ \equiv a$ جواب $x_۰$ای داشته باشد. در این‌صورت عدد صحیح bای هست که به‌ازای آن

$$x_۰^۲ = a + b \times ۲^n$$

چون a فرد است، عدد صحیح $x_۰$ نیز فرد است. بنابراین می‌توان جواب یکتای $y_۰$ای از همنهشتی خطی

$$x_۰y \equiv -b \ (\text{به پیمانهٔ ۲})$$

به‌دست آورد. ادعا می‌کنیم که عدد صحیح

$$x_۱ = x_۰ + y_۰ \times ۲^{n-۱}$$

در همنهشتی (به پیمانهٔ $۲^{n+۱}$) $x^۲ \equiv a$ صدق می‌کند. داریم

$$\begin{aligned}(x_۰ + y_۰ \times ۲^{n-۱})^۲ &= x_۰^۲ + x_۰y_۰ \times ۲^n + y_۰^۲ \times ۲^{۲n-۲}\\ &= a + (b + x_۰y_۰)۲^n + y_۰^۲ \times ۲^{۲n-۲}\end{aligned}$$

$y_\circ$ طوری انتخاب شد که $\text{۲}|(b + x_\circ y_\circ)$، پس

$$x_\text{۱}^\text{۲} = (x_\circ + y_\circ \text{۲}^{n-\text{۱}})^\text{۲} \equiv a \ (\text{به پیمانهٔ } \text{۲}^{n+\text{۱}})$$

(می‌توان از نابرابری $\text{۲}n - \text{۲} = n + \text{۱} + (n - \text{۳}) > n + \text{۱}$ نیز استفاده کرد.) بنابراین $x^\text{۲} \equiv a$ (به پیمانهٔ $\text{۲}^{n+\text{۱}}$) حلپذیر است و به این ترتیب مرحلهٔ استقرا و اثبات به انجام می‌رسد. □

به‌عنوان مثال: همنهشتی $x^\text{۲} \equiv \text{۵}$ (به پیمانهٔ ۴) جواب دارد، ولی $x^\text{۲} \equiv \text{۵}$ (به پیمانهٔ ۸) جواب ندارد. از سوی دیگر، $x^\text{۲} \equiv \text{۱۷}$ (به پیمانهٔ ۱۶) و $x^\text{۲} \equiv \text{۱۷}$ (به پیمانهٔ ۳۲) هردو حلپذیرند.

از لحاظ نظری می‌توانیم مسالهٔ تعیین شرایط وجود جواب برای همنهشتی

$$x^\text{۲} \equiv a \ (\text{به پیمانهٔ } n),\quad \gcd(a,n) = \text{۱},\quad n > \text{۱}$$

را کاملاً حل کنیم. فرض می‌کنیم

$$n = \text{۲}^{k_\circ} p_\text{۱}^{k_\text{۱}} p_\text{۲}^{k_\text{۲}} \dots p_r^{k_r},\quad k_\circ \geq \circ,\quad k_i > \circ$$

تجزیهٔ n به عاملهای اول باشد به‌طوری که p_iها عددهای اول فرد متمایزی هستند. چون مسألهٔ حل همنهشتی درجهٔ دوم $x^\text{۲} \equiv a$ (به پیمانهٔ n) معادل با حلّ دستگاه همنهشتیهای

$$x^\text{۲} \equiv a \ (\text{به پیمانهٔ } \text{۲}^{k_\circ})$$
$$x^\text{۲} \equiv a \ (\text{به پیمانهٔ } p_\text{۱}^{k_\text{۱}})$$
$$\vdots$$
$$x^\text{۲} \equiv a \ (\text{به پیمانهٔ } p_r^{k_r})$$

است، با تلفیق دو نتیجهٔ اخیر می‌توان نتیجهٔ کلّی زیر را ارائه کرد.

قضیهٔ ۹ـ۱۲ اگر $n = \text{۲}^{k_\circ} p_\text{۱}^{k_\text{۱}} p_\text{۲}^{k_\text{۲}} \dots p_r^{k_r}$ تجزیهٔ $n > \text{۱}$ به عاملهای اول باشد و $\gcd(a,n) = \text{۱}$، آنگاه $x^\text{۲} \equiv a$ (به پیمانهٔ n) حلپذیر است اگر و تنها اگر

(۱) به‌ازای $i = \text{۱}, \text{۲}, \dots, r$، $(a/p_i) = \text{۱}$

(۲) چنانچه $\text{۴}|n$ و $\text{۸} \nmid n$، $a \equiv \text{۱}$ (به پیمانهٔ ۴)؛ چنانچه $\text{۸}|n$، $a \equiv \text{۱}$ (به پیمانهٔ ۸).

تمرینهای ۹ـ۴

۱. (الف) نشان دهید که ۷ و ۱۸ تنها جوابهای ناهمنهشت (به پیمانهٔ $۵^۲$) $x^۲ \equiv -۱$ هستند.
(ب) با استفاده از قسمت (الف)، جوابهای (به پیمانهٔ $۵^۳$) $x^۲ \equiv -۱$ را پیدا کنید.

۲. هریک از همنهشتیهای درجهٔ دوم زیر را حل کنید
(الف) (به پیمانهٔ $۳^۳$) $x^۲ \equiv ۷$
(ب) (به پیمانهٔ $۵^۳$) $x^۲ \equiv ۱۴$
(پ) (به پیمانهٔ $۷^۳$) $x^۲ \equiv ۲$

۳. همنهشتی (به پیمانهٔ $۱۱^۴$) $x^۲ \equiv ۳۱$ را حل کنید.

۴. جوابهای (به پیمانهٔ $۵^۳$) $x^۲+۵x+۶ \equiv ۰$ و (به پیمانهٔ $۳^۳$) $x^۲+x+۳ \equiv ۰$ را به‌دست آورید.

۵. ثابت کنید اگر همنهشتی (به پیمانهٔ ۲^n) $x^۲ \equiv a$، $n \geq ۳$، جواب داشته باشد، آنگاه دارای دقیقاً چهار جواب ناهمنهشت است. [راهنمایی: اگر $x_۰$ جوابی باشد، آنگاه چهار عدد صحیح $x_۰$، $-x_۰$، $x_۰ + ۲^{n-۱}$، $-x_۰ + ۲^{n-۱}$، ناهمنهشت به پیمانهٔ ۲^n هستند و همهٔ جوابها را تشکیل می‌دهند.]

۶. با توجه به (به پیمانهٔ $۲^۷$) $۱۷ \equiv ۲۳^۲$، سه جواب دیگر همنهشتی (به پیمانهٔ $۲^۷$) $x^۲ \equiv ۱۷$ را به‌دست آورید.

۷. نخست مقدارهای a را طوری تعیین کنید که همنهشتیهای زیر حلپذیر باشند و سپس جوابهای این همنهشتیها را تعیین کنید:
(الف) (به پیمانهٔ $۲^۴$) $x^۲ \equiv a$
(ب) (به پیمانهٔ $۲^۵$) $x^۲ \equiv a$
(پ) (به پیمانهٔ $۲^۶$) $x^۲ \equiv a$

۸. نشان دهید که به‌ازای $n > ۱$ ثابت، تعداد جوابهای همهٔ همنهشتیهای حلپذیر (به پیمانهٔ n) $x^۲ \equiv a$ یکسان است.

۹. (الف) تعداد جوابهای همنهشتیهای (به پیمانهٔ $۲۳^۲ \times ۱۱^۲$) $x^۲ \equiv ۳$ و (به پیمانهٔ $۵^۲ \times ۳ \times ۲^۳$) $x^۲ \equiv ۹$ را، بدون پیدا کردن جوابها، تعیین کنید.
(ب) همنهشتی (به پیمانهٔ $۵^۲ \times ۳ \times ۲^۳$) $x^۲ \equiv ۹$ را حل کنید.

۱۰. (الف) اگر p عدد اول فردی باشد، ثابت کنید همنهشتی (به پیمانهٔ p) $۲x^۲ + ۱ \equiv ۰$ جواب دارد اگر و تنها اگر (به پیمانهٔ ۸) ۳ یا ۱ $p \equiv$.

(ب) همنهشتی (به پیمانهٔ $۱۱^۲$) $۲x^۲ + ۱ \equiv ۰$ را حل کنید. [راهنمایی: عددهای صحیح به‌صورت $x_۰ + ۱۱k$ را، که $x_۰$ جوابی از (به پیمانهٔ ۱۱) $۲x^۲ + ۱ \equiv ۰$ است، درنظر بگیرید.]

۱۰

عددهای تام

«در بسیاری از شاخه‌های علم، هر نسل آنچه را نسل قبلی ساخته است ویران می‌سازد، و چیزی را که کسی بنا کرده دیگری از میان برمی‌دارد. فقط در ریاضیات است که هر نسل طبقهٔ جدیدی به ساختمان قدیم می‌افزاید.»

هرمان هانکل

۱۰ـ۱ جستجوی عددهای تام

تاریخ نظریهٔ اعداد مملو از حدسهای معروف و پرسشهایی است که هنوز به آنها پاسخ داده نشده است. گفتار حاضر ناظر به برخی حدسهای بسیار جالب دربارهٔ عددهای تام است. گرچه معدودی از آنها کاملاً حل و فصل شده‌اند، بسیاری هنوز حل نشده باقی مانده‌اند. همهٔ آنها در پیشرفت کلی موضوع مؤثر بوده‌اند.

از نظر فیثاغورسیان، اینکه عدد ۶ برابر با مجموع مقسوم‌علیه‌های مثبت خود بجز ۶ است، نکته‌ای قابل توجه بوده است:

$$۶ = ۱ + ۲ + ۳$$

اولین عدد بعد از ۶ که این ویژگی را دارد، ۲۸ است؛ زیرا مقسوم‌علیه‌های مثبت ۲۸ عبارت‌اند از ۱، ۲، ۴، ۷، ۱۴، و ۲۸، و

$$۲۸ = ۱ + ۲ + ۴ + ۷ + ۱۴$$

فیثاغورسیان طبق فلسفهٔ خود که خواص اسرارآمیزی برای اعداد قائل بودند، چنین عددهایی را «تام » نامیدند. به بیان دقیقتر:

تعریف ۱۰ـ۱ عدد صحیح مثبت n تام نامیده می‌شود اگر برابر با مجموع همهٔ مقسوم‌علیه‌های مثبت خود، بجز خود n، باشد.

مجموع مقسوم‌علیه‌های مثبت عدد صحیح n، که هر یک از آنها کوچکتر از n باشند، با $\sigma(n) - n$ نشان داده می‌شود. پس ، شرط «n تام است» هم ارز با این است که $\sigma(n) - n = n$، یا

$$\sigma(n) = ۲n$$

به‌عنوان مثال، داریم

$$\sigma(۶) = ۱ + ۲ + ۳ + ۶ = ۲ \times ۶$$

و

$$\sigma(۲۸) = ۱ + ۲ + ۴ + ۷ + ۱۴ + ۲۸ = ۲ \times ۲۸$$

بنابراین هردوی ۶ و ۲۸ عدد تام هستند.

طی سده‌های متمادی، فیلسوفان بیشتر به جنبهٔ اسرارآمیز یا مذهبی عددهای تام توجه داشتند تا به ویژگیهای ریاضی آن. آگوستینِ قدیس می‌گوید: گرچه خداوند می‌توانست جهان را در یک آن بیافریند، ولی ترجیح داد این کار را در شش روز انجام دهد، زیرا کمال کار در عدد (تام=کامل) ۶ متجلی می‌شود. مفسران اولیهٔ تورات استدلال می‌کردند که کمال جهان در عدد ۲۸، یعنی، تعداد روزهایی که طول می‌کشد تا ماه دور زمین بگردد، متجلی است. درهمین راستا، آلکویین روحانی اهل یورک در سدهٔ هشتم میلادی، متذکر شد که کل نژاد بشری از هشت فرد حاضر درکشتی نوح به‌وجود آمده است و این آفرینش دوم به اندازهٔ قبلی کامل نیست زیرا ۸ عددی غیر تام است.

یونانیان فقط چهار عدد تام را می‌شناختند. اینها را نیکوماخوس در حساب مقدماتی[1] خود (درحدود ۱۰۰ میلادی) به شرح زیر معرفی می‌کند

$$P_۱ = ۶,\ P_۲ = ۲۸,\ P_۳ = ۴۹۶,\ P_۴ = ۸۱۲۸$$

1. Introductio Arithmeticae

او می‌گوید این عددها به‌صورتی «مرتب» پدیدار می‌شوند، یکی در میان عددهای یک‌رقمی، یکی درمیان عددهای دورقمی، یکی درمیان عددهای سه‌رقمی، و یکی درمیان عددهای چهاررقمی. با توجه به این شواهد عددی اندک، حدس زده شد که

۱. n امین عدد تام، یعنی P_n، شامل دقیقاً n رقم است؛ و

۲. عددهای تام زوج متناوباً به ۶ و ۸ ختم می‌شوند.

هر دو حدس فوق نادرست است. عدد تام ۵ رقمی وجود ندارد؛ عدد تام بعدی (که نخستین بار به درستی در دستنوشته‌ای فاقد نام نویسنده متعلق به سدهٔ پانزدهم ذکر شده است) عبارت است از

$$P_{۵} = ۳۳۵۵۰۳۳۶$$

گرچه آخرین رقم $P_{۵}$ عدد ۶ است، عدد تام بعدی یعنی

$$P_{۶} = ۸۵۸۹۸۶۹۰۵۶$$

نیز به ۶ ختم می‌شود، نه طبق حدس به ۸. ولی برای اینکه حرف مثبتی هم دربارهٔ این حدسها زده باشیم، بعداً نشان خواهیم داد که عددهای تام زوج همیشه به ۶ یا ۸ ختم می‌شوند ــ ولی نه لزوماً به‌طور متناوب.

توجه به بزرگی عدد $P_{۶}$ کافی است تا خواننده را متقاعد کند که عددهای تام نادرند. هنوز معلوم نیست که تعداد آنها متناهی است یا نامتناهی.

مسأله تعیین صورت کلی همهٔ عددهای تام تقریباً از آغاز تاریخ ریاضی سابقه دارد. قسمتی از این مسأله را اقلیدس حل کرد. او در مقالهٔ نهم کتاب اصول ثابت کرد که اگر مجموع

$$۱ + ۲ + ۲^{۲} + ۲^{۳} + \ldots + ۲^{k-۱} = p$$

عدد اولی باشد، آنگاه $۲^{k-۱}p$ عددی تام است (لزوماً زوج). به‌عنوان مثال، $۷ = ۴ + ۲ + ۱$ عدد اولی است؛ پس $۲۸ = ۷ \times ۴$ عددی تام است. در استدلال اقلیدس از فرمول مجموع تصاعد هندسی

$$۱ + ۲ + ۲^{۲} + ۲^{۳} + \ldots + ۲^{k-۱} = ۲^{k} - ۱$$

استفاده می‌شود که درکتابهای مختلف فیثاغورسیان آمده است. با این نماد، حکم چنین بیان می‌شود: اگر $۲^{k} - ۱$، $k > ۱$، اول باشد، آنگاه $n = ۲^{k-۱}(۲^{k} - ۱)$ عددی تام است. حدود ۲۰۰۰ سال

بعد از اقلیدس، اویلر با اثبات اینکه هر عدد تام زوجی باید به این صورت باشد، گامی سرنوشت‌ساز در حل این مسأله برداشت. از تلفیق این دو حکم، نخستین قضیهٔ این فصل به‌دست می‌آید.

قضیهٔ ۱۰ـ۱ اگر $۲^k - ۱$، $k > ۱$، اول باشد، آنگاه $n = ۲^{k-۱}(۲^k - ۱)$ تام است و هر عدد تام زوج به این صورت است.

اثبات. فرض می‌کنیم $p = ۲^k - ۱$ عددی اول است، و عدد صحیح $n = ۲^{k-۱}p$ را درنظر می‌گیریم. چون $\gcd(۲^{k-۱}, p) = ۱$، بنابه ضربی بودن σ (و همچنین قضیهٔ ۶ـ۲) داریم

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

یعنی n عددی تام است.

برعکس، فرض می‌کنیم n عدد تام زوجی باشد. می‌نویسیم $n = ۲^{k-۱}m$، که در آن m عددی صحیح و فرد است و $k \geq ۲$. از $\gcd(۲^{k-۱}, m) = ۱$ نتیجه می‌شود

$$\sigma(n) = \sigma(۲^{k-۱}m) = \sigma(۲^{k-۱})\sigma(m) = (۲^k - ۱)\sigma(m)$$

و چون n عددی تام است

$$\sigma(n) = ۲n = ۲^k m$$

پس، با مقایسهٔ این رابطه‌ها داریم

$$۲^k m = (۲^k - ۱)\sigma(m)$$

که نتیجه می‌شود $(۲^k - ۱)|۲^k m$. ولی ۲^k و $۲^k - ۱$ متباین‌اند، پس $(۲^k - ۱)|m$؛ مثلاً $m = (۲^k - ۱)M$. اگر این مقدار m را در آخرین برابری منظور کنیم و $۲^k - ۱$ را حذف کنیم، به‌دست می‌آوریم $\sigma(m) = ۲^k M$. چون هردوی m و M مقسوم‌علیه m هستند (و $M < m$)، داریم

$$۲^k M = \sigma(m) \geq m + M = ۲^k M$$

یعنی $\sigma(m) = m + M$. نتیجهٔ حاصل از این برابری این است که m فقط دو مقسوم‌علیه مثبت دارد، یعنی M و خود m. بنابراین باید m عددی اول باشد و $M = ۱$؛ به بیان دیگر، $m = (۲^k - ۱)M = ۲^k - ۱$ عددی اول است، و اثبات به انجام می‌رسد. □

چون مسألهٔ پیداکردن عددهای تام زوج به جستجوی عددهای اولِ به‌صورت $۲^k - ۱$ تحویل می‌شود، نگاه دقیقتری به این عددهای صحیح سودمند است. می‌توان ثابت کرد که اگر $۲^k - ۱$ عددی اول باشد، آنگاه نمای k باید خودش اول باشد. به بیان کلیتر:

لم. اگر $a^k - ۱$ اول باشد ($a > ۰$، $k \geq ۲$)، آنگاه $a = ۲$ و k نیز عددی اول است.

اثبات. به‌آسانی می‌توان نشان داد که

$$a^k - ۱ = (a - ۱)(a^{k-۱} + a^{k-۲} + \ldots + a + ۱)$$

که در آن، با توجه به فرضها داریم

$$a^{k-۱} + a^{k-۲} + \ldots + a + ۱ \geq a + ۱ > ۱$$

چون بنا بر فرض $a^k - ۱$ اول است، عامل دیگر باید ۱ باشد؛ یعنی $a - ۱ = ۱$ یا $a = ۲$.

اگر k مرکب باشد، می‌توانیم بنویسیم $k = rs$، $۱ < r$ و $۱ < s$. پس

$$a^k - ۱ = (a^r)^s - ۱ = (a^r - ۱)(a^{r(s-۱)} + a^{r(s-۲)} + \ldots + a^r + ۱)$$

و هریک از عاملهای طرف راست به‌وضوح بزرگتر از ۱ است. ولی این با اول بودن $a^k - ۱$ سازگار نیست. با توجه به این تناقض، k باید اول باشد. □

به‌ازای $p = ۲, ۳, ۵, ۷$، مقدارهای ۳، ۷، ۳۱، ۱۲۷ از $۲^p - ۱$ اول هستند. پس

$$۲(۲^۲ - ۱) = ۶$$

$$۲^۲(۲^۳ - ۱) = ۲۸$$

$$۲^۴(۲^۵ - ۱) = ۴۹۶$$

$$۲^۶(۲^۷ - ۱) = ۸۱۲۸$$

همگی عدد تام هستند.

در قدیم خیلیها به‌اشتباه گمان می‌کردند که به‌ازای هر عدد اول p، $۲^p - ۱$ اول است. اما هودالریکوس رگیوس[1] در سال ۱۵۳۶ در رساله‌ای[2] تجزیهٔ صحیح

$$۲^{۱۱} - ۱ = ۲۰۴۷ = ۲۳ \times ۸۹$$

1. Hudalrichus Regius

۲. با عنوان Utriusque Arithmetices

را نشان می‌دهد. اگر توجه کنیم که محاسبه‌های او به احتمال قوی با استفاده از رقمهای رومی و به‌کمک چرتکه صورت گرفته است (تا اواخر سدهٔ شانزدهم رقمهای عربی کاملاً جایگزین رقمهای رومی نشده بودند)، معلوم می‌شود که محاسبهٔ فوق کار کوچکی نبوده است. رگیوس همچنین نشان داد $p = ۱۳$ نخستین مقدار بعدی p است که به‌ازای آن $۲^p - ۱$ عددی اول است. از اینجا، پنجمین عدد تام

$$۲^{۱۲}(۲^{۱۳} - ۱) = ۳۳۵۵۰۳۳۶$$

به‌دست می‌آید. یکی از دشواریهای پیداکردن عددهای تام دیگر، عدم وجود جدولهای عددهای اول بود. در ۱۶۰۳، پیتروکاتالدی[1]، که از او بیشتر به‌دلیل ابداع نماد کسرهای مسلسل یاد می‌شود، فهرستی از همهٔ عددهای اول کوچکتر از ۵۱۵۰ منتشر کرد. کاتالدی با روش تقسیم مستقیم بر همهٔ عددهای اول نابیشتر از جذر عدد، نشان داد که $۲^{۱۷} - ۱$ عددی اول است و، در نتیجه

$$۲^{۱۶}(۲^{۱۷} - ۱) = ۸۵۸۹۸۶۹۰۵۶$$

ششمین عدد تام است.

پرسشی که بیدرنگ به ذهن می‌آید این است که آیا تعداد عددهای اولِ به‌صورت $۲^p - ۱$، (p عددی اول)، نامتناهی است یا نه. اگر پاسخ مثبت باشد، آنگاه باید تعداد عددهای تام (زوج) نامتناهی باشد. متأسفانه، این یکی دیگر از مسأله‌های حل نشدهٔ معروف است.

به‌نظر می‌رسد موقعیت مناسبی است که قضیهٔ خود دربارهٔ آخرین رقم عددهای تام زوج را ثابت کنیم.

قضیهٔ ۱۰ـ۲ آخرین رقم سمت راست هر عدد تام زوج ۶ یا ۸ است؛ یعنی $n \equiv ۶$ (به پیمانه ۱۰) یا $n \equiv ۸$ (به پیمانهٔ ۱۰).

اثبات. n را به‌عنوان عددی تام زوج می‌توان به‌صورت $n = ۲^{k-۱}(۲^k - ۱)$، که در آن $۲^k - ۱$ عددی اول است، نوشت. بنابه لم اخیر، نمای k نیز باید اول باشد. اگر $k = ۲$، آنگاه $n = ۶$ و حکم برقرار است. پس توجه خود را به حالت $k > ۲$ معطوف می‌کنیم. برحسب اینکه k به‌صورت $۴m + ۱$ یا $۴m + ۳$ باشد، اثبات در دو قسمت صورت می‌گیرد.

اگر k به‌صورت $۴m + ۱$ باشد، آنگاه

$$\begin{aligned} n &= ۲^{۴m}(۲^{۴m+۱} - ۱) \\ &= ۲^{۸m+۱} - ۲^{۴m} = ۲ \times ۱۶^{۲m} - ۱۶^m \end{aligned}$$

---

1. Pietro Cataldi

با استدلال استقرایی سرراستی می‌توان نشان داد که به‌ازای هر عدد صحیح مثبت t، (به پیمانهٔ ۱۰) $۶ \equiv ۱۶^t$. با استفاده از این همنهشتی، به‌دست می‌آوریم

$$n \equiv ۲ \times ۶ - ۶ \equiv ۶ \quad (\text{به پیمانهٔ } ۱۰)$$

حال در حالتی که $k = ۴m + ۳$، داریم

$$\begin{aligned} n &= ۲^{۴m+۲}(۲^{۴m+۳} - ۱) \\ &= ۲^{۸m+۵} - ۲^{۴m+۲} = ۲ \times ۱۶^{۲m+۱} - ۴ \times ۱۶^m \end{aligned}$$

اگر از همنهشتی (به پیمانهٔ ۱۰) $۶ \equiv ۱۶^t$ استفاده کنیم، ملاحظه می‌کنیم که

$$n \equiv ۲ \times ۶ - ۴ \times ۶ \equiv -۱۲ \equiv ۸ \quad (\text{به پیمانهٔ } ۱۰)$$

درنتیجه ، آخرین رقم سمت راست هر عدد تام زوج ۶ یا ۸ است. □

اگر استدلال را کمی بیشتر ادامه دهیم، نتیجه‌ای دقیقتر به‌دست می‌آوریم، یعنی اینکه هر عدد تام زوج $n = ۲^{k-۱}(۲^k - ۱)$ همیشه به ۶ یا ۲۸ ختم می‌شود. چون هر عدد صحیح همنهشت با دو رقم آخر سمت راست خود به پیمانهٔ ۱۰۰ است، کافی است ثابت کنیم که اگر k به‌صورت $۴m + ۳$ باشد، آنگاه (به پیمانهٔ ۱۰۰) $n \equiv ۲۸$. برای ملاحظهٔ این امر، توجه کنید که

$$۲^{k-۱} = ۲^{۴m+۲} = ۱۶^m \times ۴ \equiv ۶ \times ۴ \equiv ۴ \quad (\text{به پیمانهٔ } ۱۰)$$

به‌علاوه، به‌ازای $k > ۲$، داریم $۴|۲^{k-۱}$ و بنابراین عدد متشکّل از دو رقم آخر سمت راست $۲^{k-۱}$ بر ۴ بخشپذیر است. حاصل اینکه: آخرین رقم سمت راست $۲^{k-۱}$ برابر ۴ است، و ۴ دو رقم آخر سمت راست را می‌شمارد. حالتهای ممکن به پیمانهٔ ۱۰۰ عبارت‌اند از

$$۲^{k-۱} \equiv ۴, ۲۴, ۴۴, ۶۴, \ \text{یا} \ ۸۴$$

ولی از این نتیجه می‌شود که

$$۲^k - ۱ = ۲ \times ۲^{k-۱} - ۱ \equiv ۷, ۴۷, ۸۷, ۲۷, \ \text{یا} \ ۶۷ \quad (\text{به پیمانهٔ } ۱۰۰)$$

و بنابراین

$$n = ۲^{k-۱}(۲^k - ۱)$$
$$\equiv ۴, ۷, ۲۴ \times ۴۷, ۴۴ \times ۸۷, ۰۴ \times ۲۷, \text{ یا } ۸۴ \times ۶۷ \ (\text{به پیمانهٔ } ۱۰۰)$$

نشان دادن اینکه هریک از حاصلضربهای سمت راست همنهشتی اخیر همنهشت با ۲۸ به پیمانهٔ ۱۰۰ است، تمرینی معمولی است و آن را به خواننده واگذار می‌کنیم.

تمرینهای ۱۰ـ۱

۱. نشان دهید عدد صحیح $n = ۲^{۱۰}(۲^{۱۱} - ۱)$ عدد تام نیست؛ به این منظور نشان دهید $\sigma(n) \neq ۲n$. [راهنمایی: $۲^{۱۱} - ۱ = ۲۳ \times ۸۹$.]

۲. هریک از حکمهای زیر را ثابت کنید:

(الف) هیچ توانی از عددی اول نمی‌تواند عدد تام باشد.

(ب) مربع کامل نمی‌تواند عدد تام باشد.

(پ) حاصلضرب دو عدد اول فرد هرگز عدد تام نیست. [راهنمایی: با بسط نابرابری $(p-۱)(q-۱) > ۲$ نتیجه بگیرید $pq > p+q+۱$.]

۳. اگر n عدد تامی باشد، ثابت کنید $\sum_{d|n} ۱/d = ۲$.

۴. ثابت کنید هر عدد تام زوج، عددی مثلثی است.

۵. به فرض اینکه n، عدد تام زوجی باشد، مثلاً $n = ۲^{k-۱}(۲^k - ۱)$، نشان دهید که $n = ۱ + ۲ + ۳ + \ldots + (۲^k - ۱)$ و نیز $\phi(n) = ۲^{k-۱}(۲^{k-۱} - ۱)$.

۶. به‌ازای عدد تام زوج $n > ۶$ نشان دهید:

(الف) مجموع رقمهای n، همنهشت با ۱ به پیمانهٔ ۹ است. [راهنمایی: همنهشتی $۲^۶ \equiv ۱$ (به پیمانهٔ ۹) و اینکه هر عدد اول $p \geq ۵$ به‌صورت $۶k + ۱$ یا $۶k + ۳$ است، نشان می‌دهد $n = ۲^{p-۱}(۲^p - ۱) \equiv ۱$ (به پیمانهٔ ۹).]

(ب) عدد صحیح n را می‌توان به‌صورت مجموعی از مکعبهای فرد متوالی نوشت. [راهنمایی: با استفاده از بخش ۱ـ۱، تمرین ۱ (ث)، اتحاد

$$۱^۳ + ۳^۳ + ۵^۳ + \ldots + (۲^k - ۱)^۳ = ۲^{k-۲}(۲^{۲k-۱} - ۱)$$

را به‌ازای $k \geq ۱$ ثابت کنید.]

۷. نشان دهید هیچ مقسوم‌علیهی از عددی تام نمی‌تواند تام باشد.[راهنمایی: نتیجهٔ تمرین ۳ را به‌کار ببرید.]

۸. دو رقم آخر سمت راست عدد تام

$$n = ۲^{۱۹۹۳۶}(۲^{۱۹۹۳۷} - ۱)$$

را پیدا کنید.

۹. اگر $k \geq ۳$ و $\sigma(n) = kn$، آنگاه عدد صحیح مثبت n یک عدد kـتام (و گاهی، یک عدد چندگانه‌ـ تام) نامیده می‌شود. حکمهای زیر دربارهٔ عددهای kـتام را ثابت کنید:

(الف) $۵۲۳۷۷۶ = ۲^۹ \times ۳ \times ۱۱ \times ۳۱$ عددی ۳ـتام است.

$۳۰۲۴۰ = ۲^۵ \times ۳^۳ \times ۵ \times ۷$ عددی ۴ـتام است.

$۱۴۱۸۲۴۳۹۰۴۰ = ۲^۷ \times ۳^۴ \times ۵ \times ۷ \times ۱۱^۲ \times ۱۷ \times ۱۹$ عددی ۵ـتام است.

(ب) اگر n عددی ۳ـتام باشد و $۳ \nmid n$، آنگاه $۳n$ عددی ۴ـتام است.

(پ) اگر n عددی ۵ـتام باشد و $۵ \nmid n$، آنگاه $۵n$ عددی ۶ـتام است.

(ت) اگر $۳n$ عددی $۴k$ـتام باشد و $۳ \nmid n$، آنگاه n عددی $۳k$ـتام است.

۱۰. نشان دهید ۱۲۰ و ۶۷۲ تنها عددهای ۳ـتام به‌صورت $n = ۲^k \times ۳ \times p$، p عددی اول و فرد، هستند.

۱۱. عدد صحیح مثبت n ضربی‌ـتام نامیده می‌شود اگر n با حاصلضرب همهٔ مقسوم‌علیه‌های مثبت خود، بجز خود n، برابر باشد ؛ به بیان دیگر، $n^۲ = \Pi_{d|n} d$. همهٔ عددهای ضربی‌ـتام را تعیین کنید. [راهنمایی: توجه کنید که $n^۲ = n^{\frac{\tau(n)}{۲}}$.]

۱۲. (الف) اگر $n > ۶$ عدد تام زوجی باشد، ثابت کنید که $n \equiv ۴$ (به پیمانهٔ ۶). [راهنمایی: به‌ازای هر عدد اول فرد p، $۲^{p-۱} \equiv ۱$ (به پیمانهٔ ۳).]

(ب) ثابت کنید اگر $n \neq ۲۸$ عدد تام زوجی باشد، آنگاه $n \equiv ۱$ یا -۱ (به پیمانهٔ ۷).

۱۳. نشان دهید به‌ازای هر عدد تام زوج $n = ۲^{k-۱}(۲^k - ۱)$ داریم $۲^k | \sigma(n^۲) + ۱$.

۱۴. عددهای nای که $\sigma(\sigma(n)) = ۲n$، عددهای اَبَر تام نامیده می‌شوند.

(الف) اگر $n = ۲^k$ و $۲^{k+۱} - ۱$ اول باشد، ثابت کنید n ابر تام است؛ پس، ۱۶ و ۶۴ ابرتام هستند.

(ب) همهٔ عددهای تام زوج $n = ۲^{k-۱}(۲^k - ۱)$ را که ابر تام نیز هستند، پیدا کنید. [راهنمایی: نخست برابری $\sigma(\sigma(n)) = ۲^k(۲^{k+۱} - ۱)$ را ثابت کنید.]

۱۵. میانگین همساز مقسوم‌علیه‌های مثبت عدد صحیح مثبت n، که با $H(n)$ نشان داده می‌شود، با فرمول

$$\frac{۱}{H(n)} = \frac{۱}{\tau(n)} \sum_{d|n} \frac{۱}{d}$$

تعریف می‌شود. نشان دهید اگر n عددی تام باشد، $H(n)$ باید عددی صحیح باشد. [راهنمایی: ملاحظه کنید که $H(n) = n\tau(n)/\sigma(n)$.]

۱۶. عددهای اول دوقلوی ۵ و ۷ این ویژگی را دارند که نصف مجموع آنها عددی تام است. آیا عددهای اول دوقلوی دیگری با این ویژگی وجود دارند؟ [راهنمایی: به‌ازای عددهای اول دوقلوی $p > ۵$ و $p + ۲$، $k > ۱$ای وجود دارد به‌طوری که $\frac{p+p+۲}{۲} = ۶k$.]

۱۷. ثابت کنید اگر $۲^k - ۱$ اول باشد، آنگاه مجموع

$$۲^{k-۱} + ۲^k + ۲^{k+۱} + \ldots + ۲^{۲k-۲}$$

عددی تام است. به‌عنوان مثال، $۲^۳ - ۱$ اول است و $۲۸ = ۲^۲ + ۲^۳ + ۲^۴$، که عددی تام است.

۱۸. به فرض اینکه n عددی تام است، مثلاً $n = ۲^{k-۱}(۲^k - ۱)$، ثابت کنید حاصلضرب مقسوم‌علیه‌های مثبت n برابر با n^k است؛ یا به زبان نمادین

$$\Pi_{d|n} d = n^k$$

۱۹. اگر $n_۱$، $n_۲$، ...، n_r عددهای تام زوج متمایزی باشند، نشان دهید

$$\phi(n_۱ n_۲ \ldots n_r) = ۲^{r-۱}\phi(n_۱)\phi(n_۲)\ldots\phi(n_r)$$

[راهنمایی: به تمرین ۵ مراجعه کنید.]

۲۰. اگر $n = ۲^{k-۱}(۲^k - ۱)$ عدد تام زوجی باشد، نشان دهید

$$۲^k | \sigma(n^۲) + ۱$$

۱۰ـ۲ عددهای اول مرسن

عددهایِ به شکل

$$M_n = ۲^n - ۱ \, (n \geq ۱)$$

به‌نام راهب فرانسوی، مارین مرسن (۱۵۸۸ـ ۱۶۴۸)، که اظهار نظری نادرست ولی وسوسه‌انگیز دربارهٔ اول بودن آنها کرد، به عددهای مرسن معروف شده‌اند. عددهای مرسنی که اتفاقاً اول نیز هستند، عددهای اول مرسن نامیده می‌شوند. با توجه به آنچه در بخش ۱۰ـ۱ ثابت کردیم، تعیین عددهای اول مرسن M_n ــ و نیز، عددهای تام زوج ــ به حالتی که خود n اول است، محدود می‌شود.

مرسن در مقدمهٔ رساله‌اش با عنوان تأملاتی در فیزیک ریاضی[1] (۱۶۴۴) ادعا کرد که M_p به‌ازای $p = ۲, ۳, ۵, ۷, ۱۳, ۱۷, ۱۹, ۳۱, ۶۷, ۱۲۷, ۲۵۷$ اول و به‌ازای هر عدد اول دیگر $p < ۲۵۷$ مرکب است. از نظر ریاضیدانان دیگر بدیهی بود که مرسن نمی‌توانسته است اول بودن همهٔ عددهایی را که اعلام کرده، آزموده باشد؛ ولی آنها نیز نمی‌توانستند. اویلر (در ۱۷۷۲) با بررسی همهٔ مقسوم‌علیه‌های اول احتمالی تا ۴۶۳۳۹ نشان داد که $M_{۳۱}$ عددی اول است، ولی بررسی $M_{۶۷}$، $M_{۱۲۷}$، و $M_{۲۵۷}$ با روشهای او ممکن نبود. به هر صورت، به این ترتیب هشتمین عدد تام، یعنی عدد

$$۲^{۳۰}(۲^{۳۱} - ۱) = ۲۳۰۵۸۴۳۰۰۸۱۳۹۹۵۲۱۲۸$$

به‌دست آمد.

بالاخره در ۱۹۴۷، بر اثر تلاشی طاقت‌فرسا و با استفاده از حسابگرهای رومیزی غیرقابل اعتماد، بررسی اول بودن یا مرکب بودن M_p به ازای ۵۵ عدد اول موجود در محدودهٔ $p \leq ۲۵۷$ به انجام رسید. اکنون می‌دانیم که مرسن مرتکب پنج لغزش شده‌است. وی به اشتباه نتیجه گرفته که $M_{۶۷}$ و $M_{۲۵۷}$ اول‌اند، و $M_{۶۱}$، $M_{۸۹}$، و $M_{۱۰۷}$ را از فهرست عددهای اول پیش بینی شدهٔ خود حذف کرده بود. شگفت‌آور است که بیش از ۳۰۰ سال طول کشید تا دعاوی آن کشیش خوب تصحیح شود.

اکنون همهٔ عددهای مرکب M_n، $n < ۲۵۷$، کاملا تجزیه شده‌اند. دشوارترین تجزیه، یعنی تجزیهٔ $M_{۲۵۱}$، پس از ۳۲ ساعت جستجو با استفاده از یک ابرکامپیوتر در ۱۹۸۴ به‌دست آمد.

یکی از شگفتیهای تاریخی این است که، در ۱۸۷۶، ادوارد لوکاس آزمونی ابداع کرد که با آن توانست مرکب بودن عدد مرسن $M_{۶۷}$ را ثابت کند، ولی نتوانست عوامل تجزیه را عملاً به‌دست آورد. در گردهمایی انجمن ریاضی آمریکا در اکتبر ۱۹۰۳، فرانک نلسن کول[2]، ریاضیدان آمریکایی، مقاله‌ای در این زمینه با عنوانی نسبتاً متواضعانه: «در باب تجزیهٔ عددهای بزرگ»، ارائه کرد. وقتی از او خواسته شد سخنرانی کند، به سمت تخته رفت، و بی آنکه کلمه‌ای به زبان بیاورد، آغاز به محاسبهٔ توان ۶۷ام عدد صحیح ۲ کرد، سپس به دقت ۱ را از عدد حاصل کم کرد؛ بعد بدون اینکه تخته

1. Cogitata Physica-Mathematica
2. Frank Nelson Cole

را پاک کند یا چیزی بگوید به طرف قسمت خالی تخته رفت و با حوصله ضرب زیر را انجام داد

$$۱۹۳۷۰۷۷۲۱ \times ۷۶۱۸۳۸۲۵۷۲۸۷$$

نتیجهٔ دو محاسبه یکسان بود. چنانکه نقل می‌کنند، برای نخستین بار در تاریخ انجمن مزبور، مدعوین بپا خواستند تا ارائه دهندهٔ مقاله‌ای را تحسین کنند. کول بی‌آنکه کلمه‌ای ادا کند در صندلیش نشست و احدی از وی پرسشی نکرد. (بعداً، محرمانه به دوستی اظهار کرد که پیدا کردن عاملهای $M_{۶۷}$ وقتِ بعدازظهرهای یکشنبهٔ او را به مدت بیست سال گرفته بود.)

در مطالعهٔ عددهای مرسن، نکتهٔ شگفت انگیزی ملاحظه می‌شود: اگر هریک از چهار عدد اول مرسن نخست (یعنی، ۳، ۷، ۳۱، و ۱۲۷) جایگزین n در فرمول $۲^n - ۱$ شود، عدد اول مرسن بزرگتری به‌دست می‌آید. ریاضیدانان امیدوار بودند که با این فرایند، مجموعه‌ای نامتناهی از عددهای اول مرسن به‌دست آید؛ به عبارت دیگر، حدس زده شد که اگر عدد M_n اول باشد، آنگاه M_{M_n} نیز عددی اول است. متأسفانه، در ۱۹۵۳، کامپیوتری پر سرعت نشان داد که

$$M_{M_{۱۳}} = ۲^{M_{۱۳}} - ۱ = ۲^{۸۱۹۱} - ۱$$

(عددی با ۲۴۶۶ رقم) مرکب است.

روشهای گوناگونی برای تعیین اول یا مرکب بودن برخی ازگونه‌های ویژهٔ عددهای مرسن وجود دارد. یکی از آزمونهای مزبور در زیر می‌آید.

قضیهٔ ۱۰ـ۳ اگر p و $q = ۲p + ۱$ اول باشند، آنگاه فقط یکی از دو حالت $q|M_p$ یا $q|M_p + ۲$ برقرار است.

اثبات. با توجه به قضیهٔ فرما می‌دانیم که

$$۲^{q-۱} - ۱ \equiv ۰ \quad (\text{به پیمانهٔ } q)$$

و با تجزیهٔ سمت چپ داریم

$$\begin{aligned}(۲^{(q-۱)/۲} - ۱)(۲^{(q-۱)/۲} + ۱) &= (۲^p - ۱)(۲^p + ۱)\\ &\equiv ۰ \quad (\text{به پیمانهٔ } q)\end{aligned}$$

یا

$$M_p(M_p + ۲) \equiv ۰ \quad (\text{به پیمانهٔ } q)$$

اکنون حکم از قضیهٔ ۳ـ۱ نتیجه می‌شود. دو حالت $q|M_p$ و $q|M_p + ۲$ نمی‌توانند با هم برقرار باشند، زیرا در این صورت، $q|۲$، که غیرممکن است. □

برای روشن شدن قضیهٔ ۱۰ـ۳ کافی است آن را در یک مثال به‌کار بریم: اگر $p = ۲۳$، آنگاه $q = ۲p + ۱ = ۴۷$ نیز عددی اول است، بنابراین می‌توانیم مورد $M_{۲۳}$ را درنظر بگیریم. اکنون تحقیق می‌کنیم که آیا $۴۷|M_{۲۳}$، و یا، به عبارت دیگر، آیا $۲^{۲۳} \equiv ۱$ (به پیمانهٔ ۴۷) یا نه. داریم

$$۲^{۲۳} = ۲^{۳}(۲^{۵})^{۴} \equiv ۲^{۳}(-۱۵)^{۴} \quad (\text{به پیمانهٔ } ۴۷)$$

ولی

$$(-۱۵)^{۴} = (۲۲۵)^{۲} \equiv (-۱۰)^{۲} \equiv ۶ \quad (\text{به پیمانهٔ } ۴۷)$$

با تلفیق این دو همنهشتی ملاحظه می‌کنیم

$$۲^{۲۳} \equiv ۲^{۳} \times ۶ \equiv ۴۸ \equiv ۱ \quad (\text{به پیمانهٔ } ۴۷)$$

و بنابراین $M_{۲۳}$ مرکب است.

خاطر نشان می‌کنیم که قضیهٔ ۱۰ـ۳، مثلاً، در آزمون اول بودن $M_{۲۹}$ کارساز نیست؛ در این مثال، $۵۹ \nmid M_{۲۹}$، ولی در عوض $۵۹|M_{۲۹} + ۲$.

با توجه به دو امکان $q|M_p$ یا $q|M_p + ۲$، منطقی است سؤال شود: q چه شرطهایی داشته باشد تا حتماً $q|M_p$؟ در پاسخ، قضیهٔ زیر را داریم.

قضیهٔ ۱۰ـ۴ اگر $q = ۲n + ۱$ اول باشد، آنگاه

(۱) $q|M_n$، به شرط اینکه $q \equiv ۱$ (به پیمانهٔ ۸) یا $q \equiv ۷$ (به پیمانهٔ ۸)؛

(۲) $q|M_n + ۲$، به شرط اینکه $q = ۳$ (به پیمانهٔ ۸) یا $q \equiv ۵$ (به پیمانهٔ ۸).

اثبات. برقراری $q|M_n$ معادل با برقراری

$$۲^{(q-۱)/۲} = ۲^{n} \equiv ۱ \quad (\text{به پیمانهٔ } q)$$

است. برحسب نماد لژاندر، شرط اخیر معادل با $(۲/q) = ۱$ است، و بنابه قضیهٔ ۹ـ۶، $(۲/q) = ۱$ اگر $q \equiv ۱$ (به پیمانهٔ ۸) یا $q \equiv ۷$ (به پیمانهٔ ۸). اثبات (۲) به روشِ مشابهی صورت می‌گیرد. □

نتیجه‌ای مستقیم از قضیهٔ ۴ـ۱۰ را درنظر می‌گیریم.

فرع. اگر p و $q = ۲p + ۱$ هردو عددهای اول فردی باشند و $p \equiv ۳$ (به پیمانهٔ ۴)، آنگاه $q|M_p$.

اثبات. هر عدد اول فرد یا به‌صورت $۴k + ۱$ و یا به‌صورت $۴k + ۳$ است. اگر $p = ۴k + ۳$، آنگاه $q = ۸k + ۷$ و قضیهٔ ۱۰ـ۴ نتیجه می‌دهد $q|M_p$. در حالت $p = ۴k + ۱$، $q = ۸k + ۳$، بنابراین $q \nmid M_p$. □

عددهای $p = ۱۱, ۲۳, ۸۳, ۱۳۱, ۱۷۹, ۱۸۱, ۲۳۹, ۲۵۱$ چند تا از عددهای اول $p \equiv ۳$ (به پیمانهٔ ۴) هستند که به‌ازای هریک، $q = ۲p + ۱$ نیز عددی اول است. همچنین به‌ازای هر یک، M_p مرکب است.

برای اینکه موضوع را کمی بیشتر بشکافیم، به دو قضیه فرما می‌پردازیم که مقسوم‌علیه‌های M_p را محدود می‌کنند. اولی چنین است.

قضیهٔ ۱۰ـ۵ اگر p عدد اول فردی باشد، آنگاه هر مقسوم‌علیه M_p به صورت $۲kp + ۱$ است.

اثبات. فرض می‌کنیم q مقسوم‌علیه اولی از M_p باشد؛ پس $۲^p \equiv ۱$ (به پیمانهٔ q). اگر مرتبهٔ ۲ به پیمانهٔ q، k باشد (یعنی، اگر k کوچکترین عدد صحیح مثبتی باشد که در $۲^k \equiv ۱$ (به پیمانهٔ q) صدق کند)، آنگاه بنابه قضیهٔ ۸ـ۱، $k|p$. حالت $k = ۱$ نمی‌تواند رخ بدهد زیرا در آن صورت لازم می‌آید $q|۱$، که وضعیتی غیرممکن است. بنابراین، چون $k|p$ و $k > ۱$، از اول بودن p نتیجه می‌شود $k = p$.

بنا به قضیهٔ فرما داریم $۲^{q-۱} \equiv ۱$ (به پیمانهٔ q) و از این رو، با استفادهٔ دوباره از قضیهٔ ۸ـ۱، $k|q - ۱$. بالاخره از آنجا که می‌دانیم $k = p$، داریم $p|q - ۱$. قرار می‌دهیم $q - ۱ = pt$؛ پس $q = pt + ۱$. با توجه به اینکه اگر t فردباشد، آنگاه باید q زوج باشد و تناقضی پیش می‌آید، اثبات به انجام رسیده است. پس، به‌ازای kی مناسبی، $q = ۲kp + ۱$ و این همان صورت مطلوب q است. □

قضیهٔ زیر را به‌عنوان غربال دیگری برای ظاهر ساختن مقسوم‌علیه‌های ممکن M_p ذکر می‌کنیم.

قضیهٔ ۱۰ـ۶ اگر p عدد اول فردی باشد، آنگاه هر مقسوم‌علیه اول q از M_p به‌صورت $q \equiv \pm ۱$ (به پیمانهٔ ۸) است.

اثبات. فرض می‌کنیم $q = ۲n + ۱$ مقسوم‌علیه اولی از M_p باشد. اگر $a = ۲^{(p+۱)/۲}$، آنگاه

$$a^۲ - ۲ = ۲^{p+۱} - ۲ = ۲M_p \equiv ۰ \quad (\text{به پیمانهٔ } q)$$

اگر هر دو طرف همنهشتی $a^۲ \equiv ۲$ (به پیمانهٔ q) را به توان n برسانیم، به‌دست می‌آوریم

$$a^{q-۱} = a^{۲n} \equiv ۲^n \quad (\text{به پیمانهٔ } q)$$

چون q عدد صحیح فردی است، داریم $\gcd(a,\ q) = ۱$ و بنابراین، $a^{q-۱} \equiv ۱$ (به پیمانهٔ q).
با مقایسه دو همنهشتی اخیر می‌بینیم $۲^n \equiv ۱$ (به پیمانهٔ q) ، یا، از دیدگاه دیگری، $q|M_n$. پس بنابه قضیهٔ ۱۰ـ۴، $q \equiv \pm ۱$ (به پیمانهٔ ۸). □

برای روشن شدن نحوهٔ استفاده از این قضیه‌ها، $M_{۱۷}$ را درنظر می‌گیریم . عددهای صحیح به‌صورت $۳۴k + ۱$ که کوچکتر از $۳۶۲\sqrt{M_{۱۷}}$ هستند، عبارت اند از

$$۳۵, ۶۹, ۱۰۳, ۱۳۷, ۱۷۱, ۲۰۵, ۲۳۹, ۲۷۳, ۳۰۷, ۳۴۱$$

چون کوچکترین مقسوم‌علیه (نابدیهی) $M_{۱۷}$ باید اول باشد، کافی است عددهای اولِ موجود در میان ده عدد فوق را درنظر بگیریم یعنی

$$۱۰۳, ۱۳۷, ۲۳۹, ۳۰۷$$

با توجه به اینکه $۳۰۷ \not\equiv \pm ۱$ (پیمانهٔ ۸)، کار را تا اندازه‌ای می‌توان کوتاهتر کرد. بنابراین، می‌توان ۳۰۷ را از فهرست خود حذف کرد. حال، $M_{۱۷}$ یا اول است یا بر یکی از سه عدد باقیمانده بخشپذیر است. محاسبه‌ای کوتاه نشان می‌دهد که $M_{۱۷}$ بر هیچ یک از ۱۰۳، ۱۳۷، و ۲۳۹ بخشپذیر نیست؛ یعنی $M_{۱۷}$ اول است.

بعد از کشف هشتمین عدد تام، $۲^{۳۰}(۲^{۳۱} - ۱)$، بارلو[1] درکتاب نظریهٔ اعدادش (که در ۱۸۱۱ منتشر شد)، با توجه به بزرگی این عدد، نتیجه می‌گیرد که «عدد تامی بزرگتر از این کشف نخواهد شد زیرا این اعداد گرچه شگفت‌انگیزند، مفید نیستند، و محتمل به‌نظر نمی‌رسد که کسی بخواهد عدد تامی بزرگتر از این پیدا کند.» حداقل چیزی که می‌توان گفت این است که بارلو کنجکاوی لاعلاج بشر را دست کم گرفت. گرچه جستجوهای بعدی برای یافتن عددهای تام بزرگتر یکی از فصلهای جذاب تاریخ ریاضیات را تشکیل می‌دهد، بحث گسترده‌تر در این مورد، مناسب این کتاب نیست.

شایان ذکر است که دوازده عدد اول مرسِن نخست (و بنابراین، دوازده عدد تام) از ۱۹۱۴ معلوم بوده‌اند. دوازدهمین از نظر ترتیب اکتشاف، یعنی $M_{۸۹}$، آخرین عدد اول مرسنی بود که با محاسبهٔ دستی کشف شد؛ اول بودن آن را در سال ۱۹۱۴، پاورز[2] و کانینگام[3]، مستقل از یکدیگر و با استفاده از روشهای متفاوتی نشان دادند. عدد اول $M_{۱۲۷}$ را لوکاس در ۱۸۷۶ کشف کرد و تا ۷۵ سال بعد بزرگترین عدد اولِ شناخته شده بود.

---

1. Barlow 2. Powers 3. Cunningham

محاسبه‌هایی که به‌دلیل طولانی و ملال‌آور بودن مورد نفرت ریاضیدانها هستند، خوراک خوبی برای کامپیوترهای الکترونیک‌اند. از ۱۹۵۲ به بعد، هجده عدد اول مرسن (که همگی بسیار بزرگ بوده‌اند)، کشف شده‌اند. بیست و پنجمین عدد اول مرسن یعنی $M_{۲۱۷۰۱}$، در ۱۹۷۸ به‌وسیلهٔ دو دانش‌آموز هجده ساله، لورا نیکل[1] و کرت نول[2]، با مصرف ۴۴۰ ساعت وقتِ کامپیوتری بزرگ، کشف شد. چند ماه بعد، نول نشان داد که $M_{۲۳۲۰۹}$ نیز اول است. با پیدایش کامپیوترهای بسیار سریعتر، فهرست این عددهای اول بازگسترده‌تر شد. عدد اول مرسن $M_{۲۱۶۰۹۱}$ در ۱۹۸۵ کشف شد و تاکنون بزرگترین عدد اول شناخته شده به حساب می‌آید. این نیز بزرگترین عدد تام زوج شناخته شده، یعنی سی‌امین عدد تام را، به‌دست می‌دهد:

$$P_{۳۰} = ۲^{۲۱۶۰۹۰}(۲^{۲۱۶۰۹۱} - ۱)$$

که عددی فوق‌العاده بزرگ با ۱۳۰۱۰۰ رقم است.

به هنگام نگارش این کتاب، دو متخصص کامپیوتر در «مرکز تحقیقاتی منطقهٔ هوستن» اعلام کردند که سی و یکمین عدد اول مِرسن یعنی $M_{۱۱۰۵۰۳}$ را کشف کرده‌اند. آنها با شگفتی دیدند که این عدد اول در فاصلهٔ میان دو عدد اول مرسنی که پیشتر کشف شده بودند قرار دارد. جالب توجه است که جستجوی این عدد را با یک ابرکامپیوتر در مدتی که به‌طور باور نکردنی کوتاه بود، یعنی ۱۱ دقیقه، انجام دادند.

برای سهولت کار خواننده، فهرست ۳۰ عدد تام زوج، تعداد رقمهای هریک، و زمان تقریبی کشف آنها را در اینجا می‌آوریم.

	عدد	تعداد رقمها	تاریخ کشف
۱	$۲(۲^{۲} - ۱)$	۱	نامعلوم
۲	$۲^{۲}(۲^{۳} - ۱)$	۲	نامعلوم
۳	$۲^{۴}(۲^{۵} - ۱)$	۳	نامعلوم
۴	$۲^{۶}(۲^{۷} - ۱)$	۴	نامعلوم
۵	$۲^{۱۲}(۲^{۱۳} - ۱)$	۸	۱۴۵۶
۶	$۲^{۱۶}(۲^{۱۷} - ۱)$	۱۰	۱۵۸۸
۷	$۲^{۱۸}(۲^{۱۹} - ۱)$	۱۲	۱۵۸۸
۸	$۲^{۳۰}(۲^{۳۱} - ۱)$	۱۹	۱۷۷۲
۹	$۲^{۶۰}(۲^{۶۱} - ۱)$	۳۷	۱۸۸۳

1. Laura Nickel 2. Curt Noll

۱۰	$۲^{۸۸}(۲^{۸۹}-۱)$	۵۴	۱۹۱۱
۱۱	$۲^{۱۰۶}(۲^{۱۰۷}-۱)$	۶۵	۱۹۱۴
۱۲	$۲^{۱۲۶}(۲^{۱۲۷}-۱)$	۷۷	۱۸۷۶
۱۳	$۲^{۵۲۰}(۲^{۵۲۱}-۱)$	۳۱۴	۱۹۵۲
۱۴	$۲^{۶۰۶}(۲^{۶۰۷}-۱)$	۳۶۶	۱۹۵۲
۱۵	$۲^{۱۲۷۸}(۲^{۱۲۷۹}-۱)$	۷۷۰	۱۹۵۲
۱۶	$۲^{۲۲۰۲}(۲^{۲۲۰۳}-۱)$	۱۳۲۷	۱۹۵۲
۱۷	$۲^{۲۲۸۰}(۲^{۲۲۸۱}-۱)$	۱۳۷۳	۱۹۵۲
۱۸	$۲^{۳۲۱۶}(۲^{۳۲۱۷}-۱)$	۱۹۳۷	۱۹۵۷
۱۹	$۲^{۴۲۵۲}(۲^{۴۲۵۳}-۱)$	۲۵۶۱	۱۹۶۱
۲۰	$۲^{۴۴۲۲}(۲^{۴۴۲۳}-۱)$	۲۶۶۳	۱۹۶۱
۲۱	$۲^{۹۶۸۸}(۲^{۹۶۸۹}-۱)$	۵۸۳۴	۱۹۶۳
۲۲	$۲^{۹۹۴۰}(۲^{۹۹۴۱}-۱)$	۵۹۸۵	۱۹۶۳
۲۳	$۲^{۱۱۲۱۲}(۲^{۱۱۲۱۳}-۱)$	۶۷۵۱	۱۹۶۳
۲۴	$۲^{۱۹۹۳۶}(۲^{۱۹۹۳۷}-۱)$	۱۲۰۰۳	۱۹۷۱
۲۵	$۲^{۲۱۷۰۰}(۲^{۲۱۷۰۱}-۱)$	۱۳۰۶۶	۱۹۷۸
۲۶	$۲^{۲۳۲۰۸}(۲^{۲۳۲۰۹}-۱)$	۱۳۹۷۳	۱۹۷۸
۲۷	$۲^{۴۴۴۹۶}(۲^{۴۴۴۹۷}-۱)$	۲۶۷۹۰	۱۹۷۹
۲۸	$۲^{۸۶۲۴۲}(۲^{۸۶۲۴۳}-۱)$	۵۱۹۲۴	۱۹۸۳
۲۹	$۲^{۱۳۲۰۴۸}(۲^{۱۳۲۰۴۹}-۱)$	۷۹۵۰۲	۱۹۸۳
۳۰	$۲^{۲۱۶۰۹۰}(۲^{۲۱۶۰۹۱}-۱)$	۱۳۰۱۰۰	۱۹۸۵

گرچه بسیاری از ریاضیدانان اعتقاد دارند که مجموعهٔ عددهای اول مرسن نامتناهی است، اثبات این موضوع به گونهٔ ناامیدکننده‌ای دور از دسترس به‌نظر می‌رسد. با افزایش p، عددهای اول مرسن به وضوح پراکنده‌تر می‌شوند. حدس زده شده است که به‌طور متوسط به‌ازای همهٔ اعداد اول p دربازهٔ $x < p < ۲x$، تقریباً دو عدد اول M_p وجود دارد؛ این حدس را شواهد عددی تقویت می‌کنند.

عددهای تامِ مذکور در جدول تنها عددهایِ تامی هستند که کشف شده‌اند. یکی از مسأله‌های معروف نظریهٔ اعداد وجود یا عدم وجود عدد تام فرد است. گرچه تاکنون عدد تام فردی به‌دست نیامده است، احتمال پیدا کردن شرطهای ویژه‌ای در مورد وجود آنها منتفی نیست. قدیمیترین اینها منسوب به اویلر است، که ثابت کرد اگر n عدد تام فردی باشد، آنگاه

$$n = p_۱^{k_۱} p_۲^{۲j_۲} \dots p_r^{۲j_r}$$

که در آن p_iها عددهای اول فرد متمایزی هستند و $p \equiv \alpha \equiv ۱$ (به پیمانهٔ ۴). در ۱۹۳۷

اشتویروالت[1] نشان داد که همهٔ β_iها نمی‌توانند برابر با ۱ باشند؛ یعنی اگر $n = p^a q_1^2 q_2^2 \ldots q_r^r$ عددی فرد باشد و $p \equiv \alpha \equiv 1$ (به پیمانهٔ ۴)، آنگاه n تام نیست. چهار سال بعد، کانلد[2] ثابت کرد که نه تنها همهٔ β_iها نمی‌توانند ۲ باشند بلکه ممکن نیست یکی از β_iها برابر ۲ و بقیه برابر ۱ باشند. در چند سال اخیر شاهد پیشرفت بیشتری بوده‌ایم: هاگیس[3] و مک دانیل[4] (۱۹۷۲) ثابت کردند که همهٔ β_iها نمی‌توانند برابر ۳ باشند.

این نکته‌ها را کنار می‌گذاریم و به اثبات قضیهٔ اویلر می‌پردازیم.

قضیهٔ ۱۰ـ۷ (اویلر). اگر n عدد تام فردی باشد، آنگاه

$$n = p_1^{k_1} p_2^{2j_2} \ldots p_r^{2j_r}$$

که در آن p_iها عددهایی اول و فرد و متمایزند و $p_1 \equiv k_1 \equiv 1$ (به پیمانهٔ ۴).

اثبات. فرض می‌کنیم $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ تجزیهٔ n به عاملهای اول باشد. چون n تام است، می‌توانیم بنویسیم

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \ldots \sigma(p_r^{k_r})$$

چون n عدد صحیح فردی است، (به پیمانهٔ ۴) $n \equiv 1$ یا (به پیمانهٔ ۴) $n \equiv 3$؛ در هر صورت، (به پیمانهٔ ۴) $2n \equiv 2$. پس، گرچه $\sigma(n) = 2n$ بر ۲ بخشپذیر است، بر ۴ بخشپذیر نیست. نتیجه اینکه یکی از $\sigma(p_i^{k_i})$ها، مثلاً $\sigma(p_1^{k_1})$، باید عددی زوج (ولی بخش ناپذیر بر ۴)، و بقیهٔ $\sigma(p_i^{k_i})$ها عددهای صحیح فردی باشند.

به‌ازای هر p_i، دو حالت را باید درنظر گرفت: (به پیمانهٔ ۴) $p_i \equiv 1$ و (به پیمانهٔ ۴) $p_i \equiv 3$. اگر (به پیمانهٔ ۴) $p_i \equiv 3 \equiv -1$، خواهیم داشت

$$\begin{aligned}
\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \ldots + p_i^{k_i} \\
&\equiv 1 + (-1) + (-1)^2 + \ldots + (-1)^{k_i} \quad \text{(به پیمانهٔ ۴)} \\
&\equiv \begin{cases} 0 & \text{اگر } k_i \text{ فرد باشد (به پیمانهٔ ۴)} \\ 1 & \text{اگر } k \text{ زوج باشد (به پیمانهٔ ۴)} \end{cases}
\end{aligned}$$

چون (به پیمانهٔ ۴) $\sigma(p_1^{k_1}) \equiv 2$، نتیجه می‌شود (به پیمانهٔ ۴) $p_1 \not\equiv 3$ یا، به صورتی مثبت، (به پیمانهٔ ۴) $p_1 \equiv 1$. به علاوه، همنهشتی (به پیمانهٔ ۴) $\sigma(p_i^{k_i}) \equiv 0$ به این معنی است که

1. Steuerwald 2. Kanold 3. Hagis 4. McDaniel

$\sigma(p_i^{k_i})$ بر ۴ تقسیم‌پذیر است، که ممکن نیست. نتیجه: اگر (به‌پیمانهٔ ۴) $p_i \equiv ۳$، $i = ۲, \ldots, r$، نمای k_iی آن عدد صحیح زوجی است.

اگر (به پیمانهٔ ۴) $p_i \equiv ۱$، که قطعاً به‌ازای $i = ۱$، چنین است، آنگاه

$$\begin{aligned}\sigma(p_i^{k_i}) &= ۱ + p_i + p_i^۲ + \ldots + p_i^{k_i} \\ &\equiv ۱ + ۱^۱ + ۱^۲ + \ldots + ۱^{k_i} \quad (\text{به پیمانهٔ } ۴) \\ &\equiv k_i + ۱ \quad (\text{به پیمانهٔ } ۴)\end{aligned}$$

شرط (به پیمانهٔ ۴) $\sigma(p_۱^{k_۱}) \equiv ۲$ ایجاب می‌کند که (به پیمانهٔ ۴) $k_۱ \equiv ۱$. به‌ازای مقدارهای دیگر i، می‌دانیم (به پیمانهٔ ۴) ۳ یا $\sigma(p_i^{k_i}) \equiv ۱$ و بنابر این (به پیمانهٔ ۴) ۲ یا $k_i \equiv ۰$. در هر حالت، k_i باید عدد صحیح زوجی باشد. کلام آخر اینکه، در هر دو حالتِ (به پیمانهٔ ۴) $p_i \equiv ۱$ و (به پیمانهٔ ۴) $p_i \equiv ۳$، k_i به‌ازای $i \neq ۱$ همیشه زوج است. به این ترتیب اثبات به انجام می‌رسد. □

با توجه به قضیهٔ فوق، عدد تام فرد n را می‌توان به‌صورت

$$\begin{aligned}n &= p_۱^{k_۱} p_۲^{۲j_۲} \ldots p_r^{۲j_r} = p_۱^{k_۱}(p_۲^{j_۲} \ldots p_r^{j_r})^۲ \\ &= p_۱^{k_۱} m^۲\end{aligned}$$

نشان داد. از این مستقیماً نتیجه می‌شود:

فرع. اگر n عدد تام فردی باشد، آنگاه n به‌صورت

$$n = p^k m^۲$$

است که در آن p عددی اول است، $p \nmid m$، و (به پیمانهٔ ۴) $p \equiv k \equiv ۱$؛ درنتیجه، داریم (به پیمانهٔ ۴) $n \equiv ۱$.

اثبات. فقط قسمت آخر کاملاً بدیهی نیست. چون (به پیمانهٔ ۴) $p \equiv ۱$، خواهیم داشت (به پیمانهٔ ۴) $p^k \equiv ۱$. توجه کنید که m باید فرد باشد؛ پس، (به پیمانهٔ ۴) ۳ یا $m \equiv ۱$ و بنابراین، با به توان ۲ رساندن داریم (به پیمانهٔ ۴) $m^۲ \equiv ۱$. نتیجه می‌شود که (به پیمانهٔ ۴)

$$n = p^k m^۲ \equiv ۱ \times ۱ \equiv ۱$$

و حکم ثابت می‌شود. □

براورد اندازهٔ عدد تام فرد n یکی از زمینه‌های تحقیق است. کران پایین کلاسیک را تورکانینوف[1] در ۱۹۰۸ به‌دست آورد: n حداقل پنج عامل اول متمایز دارد و بزرگتر از ۲×۱۰^{۶} است. با پیدایش کامپیوترهای الکترونیک، کران پایین به‌صورت $n > ۱۰^{۱۵۰}$ اصلاح شد. بررسیهای اخیر نشان داده‌اند که n باید بر حداقل هشت عامل اول متمایز بخشپذیر باشد که بزرگترینشان بزرگتر از ۱۰۰۱۲۹ و عامل بزرگتر بعدی، بزرگتر از ۱۰۰۹ باشد؛ اگر $۳ \nmid n$، آنگاه تعداد عاملهای اول متمایز n حداقل یازده است.

گرچه همهٔ این ملاحظات اعتقاد به عدم وجود عددهای تام فرد را تقویت می‌کنند، فقط اثبات عدم وجود آنهاست که تکلیف را روشن خواهد کرد. در آن صورت با وضعیت غریبی رو به رو خواهیم شد زیرا نظریهٔ کاملی دربارهٔ رده‌ای از عددها ساخته‌ایم که وجود ندارد. جوزف سیلوسبر ریاضیدان نامی در ۱۸۸۸ نوشت «امتیاز کشف رده‌ای از عددهای تام که عضوهایش به احتمال زیاد تنها عددهای تام هستند، همیشه متعلق به هندسه‌دانان یونانی خواهد بود.»

گروه دیگری از عددها که سابقه‌ای ممتد از یونان باستان تا به امروز دارند، عددهای متحاب‌اند. دو عدد مانند ۲۲۰ و۲۸۴ متحاب یا دوست نامیده می‌شوند، زیرا این خاصیّت قابل توجه را دارند که هریک «در دلِ» دیگری است، به این معنی که هریک برابر با مجموع همهٔ مقسوم‌علیه‌های مثبت عدد دیگر، بجز خود آن عدد، است. مثلاً در مورد مقسوم‌علیه‌های ۲۲۰ داریم

$$۱ + ۲ + ۴ + ۵ + ۱۰ + ۱۱ + ۲۰ + ۲۲ + ۴۴ + ۵۵ + ۱۱۰ = ۲۸۴$$

و در مورد ۲۸۴

$$۱ + ۲ + ۴ + ۷۱ + ۱۴۲ = ۲۲۰$$

عددهای متحاب m و n (یا زوجی متحاب) برحسب تابع σ با معادله‌های

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

یا معادلش

$$\sigma(m) = m + n = \sigma(n)$$

تعریف می‌شوند.

بررسی تاریخ شگفت‌انگیز و جالب عددهای متحاب نشان می‌دهد که این عددها در جادوگری و نجوم، طالع‌بینی، ساخت طلسم، و درست کردن داروی محبت نقش مهمی داشته‌اند. یونانیان معتقد بودند که این عددها در ایجاد و تحکیم دوستی میان انسانها تأثیر ویژه‌ای دارند. ایامبلیخوس[2]،

1. Turcaninov 2. Iamblichus

فیلسوف اهل خالکیس[1] (۲۵۰ ـ ۳۳۰ بعد از میلاد) کشف زوج ۲۲۰ و ۲۸۴ را به فیثاغورسیان نسبت می‌دهد. او می‌نویسد:

> آنها (فیثاغورسیان) برخی از عددها را عددهای متحاب می‌نامند، و برای عددهایی مانند ۲۲۰ و ۲۸۴، فضیلتها و کیفیتهای اجتماعی قائل هستند زیرا اجزای هریک قادر به تولید دیگری است.

مفسران کتاب مقدس پی بردند که در سِفر پیدایش (۱۴ : ۳۲)، تعداد حیوانات اهدایی یعقوب به عیسو متشکل از ۲۰۰ بز ماده و ۲۰ بز نر که مجموعاً ۲۲۰ است، عضو کوچکترِ زوج کلاسیکی از اعداد متحاب است. به گفتهٔ یکی از مفسران، یعقوب برای تأمین دوستی عیسو تعداد هدایای خویش را «به‌ترتیب اسرارآمیزی» خردمندانه انتخاب کرد. عربی به نام المجریطی اهل مادرید که در سدهٔ یازدهم می‌زیست، نقل کرده که تأثیر احساسی این دو عدد را آزمایش کرده است به این ترتیب که یک شیرینی به شکل عدد ۲۲۰ به کسی تعارف کرده و خود یک شیرینی به شکل ۲۸۰ را خورده است. اما المجریطی نتیجهٔ کار را توصیف نکرده است.

یکی از نشانه‌های کُندیِ پیشرفت نظریهٔ اعداد این است که تا دهۀ ۱۶۳۰ کسی نتوانسته بود به زوجی از عددهای متحاب که توسّط یونانیها کشف شد، زوج دیگری اضافه کند. نخستین قاعدهٔ صریحی که برای پیدا کردن بعضی از گونه‌های عددهای متحاب وضع شد، منسوب به ثابت‌بن‌قره، ریاضیدان عرب سدهٔ نهم است. او در یکی از دستنوشته‌هایش نشان می‌دهد که:

> اگر سه عدد $p = ۳ \times ۲^{n-۱} - ۱$، $q = ۳ \times ۲^{n} - ۱$، و $r = ۹ \times ۲^{۲n-۱} - ۱$ همگی اول باشند و $n \geq ۲$، آنگاه $۲^n pq$ و $۲^n r$ متحاب هستند.

قاعدهٔ ثابت زمانی مثمرثمر شد که دوباره توسط فرما و دکارت کشف شد و با استفاده از آن دومین و سومین زوج عددهای متحاب به‌دست آمد. فرما در نامه‌ای به مرسن در سال ۱۶۳۶، اعلام کرد که ۱۷۲۹۶ و ۱۸۴۱۶ زوجی متحاب است و دکارت در نامه‌اش به مرسن در ۱۶۳۸، نوشت که موفق به پیداکردن زوج متحاب ۹۳۶۳۵۸۴ و ۹۴۳۷۰۵۶ شده است. زوج فرما به ازای $n = ۴$ از قاعدهٔ ثابت به‌دست آمد (عددهای اول متناظر عبارت‌اند از $p = ۲۳$، $q = ۴۷$، $r = ۱۱۵۱$) و زوج دکارت نیز به‌ازای $n = ۷$ حاصل شد (عددهای اول متناظر عبارت‌اند از $p = ۱۹۱$، $q = ۳۸۳$، $r = ۷۳۷۲۷$).

در دهۀ ۱۷۰۰ تا ۱۷۱۰، اویلر یکجا فهرستی از شصت و چهار زوج متحاب عرضه کرد؛ بعدها متحاب نبودن دو تا از این زوجها، یکی در سال ۱۹۰۹ و دیگری در سال ۱۹۱۴، معلوم شد. در ۱۸۳۰، آدریان ماری لژاندر زوج دیگری پیدا کرد: ۲۱۷۲۶۴۹۲۱۶ و ۲۱۹۰۸۵۲۰۱۹۱.

با جستجوهای گستردهٔ کامپیوتری، بیش از ۷۵۰۰ زوج متحاب که برخی تا ۲۸۲ رقم دارند،

1. Chalcis

به‌دست آمده است؛ اینها شامل همهٔ عددهای متحابی هستند که مقدارشان از $۱۰^{۱۰}$ کوچکتر است. تاکنون نه‌تنها متناهی یا نامتناهی بودن تعداد زوجهای متحاب معلوم نشده است، زوج متحابی که عددهای آن متباین باشند، نیز به‌دست نیامده است. فقط ثابت شده است که هریک از عددهای هر زوج از عددهای متباین متحاب باید بزرگتر از $۱۰^{۲۵}$ باشد؛ و حاصلضرب آنها باید بر حداقل ۲۲ عامل اول متمایز بخشپذیر باشد. برخلاف عددهای تام (زوج) که، فرمول واحدی برای تولید آنها وجود دارد، قاعدهٔ شناخته شده‌ای برای پیداکردن همهٔ زوجهای متحاب عددها وجود ندارد، و این بخشی از دشواریهای کار است.

تمرینهای ۱۰ـ۲

۱. ثابت کنید عدد مرسن $M_{۱۳}$ اول است و بنابراین عدد صحیح $n = ۲^{۱۲}(۲^{۱۳} - ۱)$ تام است. [راهنمایی: چون $۹۱ > \sqrt{M_{۱۳}}$، بنابه قضیهٔ ۱۰ـ۵، تنها مقسوم‌علیه‌های اول احتمالی $M_{۱۳}$ عبارت‌اند از ۵۳ و ۷۹.]

۲. ثابت کنید عدد مرسن $M_{۱۹}$ اول است، و بنابراین عدد صحیح $n = ۲^{۱۸}(۲^{۱۹} - ۱)$ تام است. [راهنمایی: بنابه قضیه‌های ۱۰ـ۵ و ۱۰ـ۶، تنها مقسوم‌علیه‌های اول احتمالی ۱۹۱، ۴۵۷، و ۶۴۷ هستند.]

۳. ثابت کنید عدد مرسن $M_{۲۹}$ مرکب است.

۴. عدد صحیح مثبت n یک عدد زائد نامیده می‌شود اگر $\sigma(n) > ۲n$ و یک عدد ناقص نامیده می‌شود اگر $\sigma(n) < ۲n$. هریک از حکمهای زیر را ثابت کنید:

(الف) تعداد عددهای ناقص نامتناهی است. [راهنمایی: عددهای صحیح $n = p^k$ را، که p عددی اول و فرد باشد و $k \geq ۱$، درنظر بگیرید.]

(ب) تعداد عددهای زائد زوج نامتناهی است. [راهنمایی: عددهای صحیح $n = ۲^k \times ۳$، $k > ۱$، را درنظر بگیرید.]

(پ) تعداد عددهای زائد فرد نامتناهی است. [راهنمایی: عددهای صحیح $n = ۹۴۵k$ را، که در آن k عددی صحیح مثبت دلخواه و بخش‌ناپذیر بر ۲، ۳، ۵، یا ۷ است، درنظر بگیرید. چون $۹۴۵ = ۳^۳ \times ۵ \times ۷$، نتیجه می‌شود $\gcd(۹۴۵, k) = ۱$ و بنابراین $\sigma(n) = \sigma(۹۴۵)\sigma(k)$.]

۵. اگر n عددی تام زوج باشد و $d|n$، $۱ < d < n$، نشان دهید که d ناقص است.

۶. نشان دهید هر مضرب عدد تام، زائد است.

۷. نشان دهید زوجهای عددهای صحیح زیر متحاب‌اند:

(الف) $۲۲۰ = ۲^۲ \times ۵ \times ۱۱$ و $۲۸۴ = ۲^۲ \times ۷۱$ (فیثاغورس، ۵۰۰ قبل از میلاد)؛

(ب) $۴۷ \times ۲۳ \times ۲^۴ = ۱۷۲۹۶$ و $۱۱۵۱ \times ۲^۴ = ۱۸۴۱۶$ (فرما، ۱۶۳۶)؛

(پ) $۳۸۳ \times ۱۹۱ \times ۲^۷ = ۹۳۶۳۵۸۴$ و $۷۳۷۲۷ \times ۲^۷ = ۹۴۳۷۰۵۶$ (دکارت، ۱۶۳۸).

۸. ثابت کنید به‌ازای هر زوج متحاب m و n داریم

$$(\sum_{d|m} \frac{۱}{d})^{-۱} + (\sum_{d|n} \frac{۱}{d})^{-۱} = ۱$$

۹. حکمهای زیر دربارهٔ عددهای متحاب را ثابت کنید:

(الف) اگر p عددی اول باشد، هیچ‌یک از p و $p^۲$ نمی‌تواند یکی از عددهایِ یک زوج متحاب باشد.

(ب) عدد صحیح بزرگتر در هر زوج متحاب، عددی ناقص است.

(پ) اگر m و n زوجی متحاب باشند و m زوج و n فرد باشد، آنگاه n مربعی کامل است. [راهنمایی: اگر p عدد اول فردی باشد، آنگاه $۱ + p + p^۲ + \ldots + p^k$ فقط وقتی فرد است که k عدد صحیح زوجی باشد.]

۱۰. در سال ۱۸۸۶، یک پسر ۱۶ ساله ایتالیایی اعلام کرد که $۱۱۸۴ = ۲^۵ \times ۳۷$ و $۱۲۱۰ = ۲ \times ۵ \times ۱۱^۲$ زوجی متحاب از عددها تشکیل می‌دهند ولی اشاره‌ای به روش کشف خود نکرد. این ادعا را بررسی کنید.

۱۱. «قاعدهٔ ثابت بن‌قره» در مورد زوجهای متحاب را ثابت‌کنید. اگر هر سه عدد $p = ۳ \times ۲^{n-۱} - ۱$، $q = ۳ \times ۲^n - ۱$ و $r = ۹ \times ۲^{۲n-۱} - ۱$، $n \geq ۲$، اول باشند آنگاه $۲^n pq$ و $۲^n r$ زوجی متحاب هستند. این قاعده از میان اعداد $۲ \leq n \leq ۲۰۰۰۰$، فقط به‌ازای $n = ۲, ۴, ۷$ زوج متحابی تولید می‌کند.

۱۲. منظور از سه‌تایی متحاب، سه عدد صحیحی است که مجموع هر دو تا از آنها برابر با مجموع مقسوم‌علیه‌های سومی، بجز خود عدد سوم، باشد. تحقیق کنید که $۲^۵ \times ۳ \times ۱۳ \times ۲۹۳ \times ۳۳۷$، $۲^۵ \times ۳ \times ۵ \times ۱۳ \times ۱۶۵۶۱$، و $۲^۵ \times ۳ \times ۱۳ \times ۹۹۳۷۱$ یک سه‌تایی متحاب هستند.

۱۳. دنباله‌ای متناهی از عددهای صحیح مثبت، زنجیرهٔ اجتماعی نامیده می‌شود اگر هریک از آن عددها برابر با مجموع مقسوم‌علیه‌های مثبت عدد صحیح بلافصل قبلی، جز خودش، باشد (عدد آخری، عدد ماقبلِ اولین عدد دنباله به حساب می‌آید). نشان دهید عددهای صحیح زیر زنجیره‌ای اجتماعی تشکیل می‌دهند

$$۱۲۴۹۶, ۱۴۲۸۸, ۱۵۴۷۲, ۱۴۵۳۶, ۱۴۲۶۴$$

تا ۱۹۷۰، که نه زنجیرهٔ اجتماعی، هرکدام متشکل از چهار عدد صحیح، ارائه شد، فقط دو زنجیرهٔ اجتماعی شناخته شده بود.

۱۴. ثابت کنید

(الف) هر عدد تام فرد n را می‌توان به‌صورت $n = pa^۲$، که p عدد اول باشد، نشان داد.

(ب) اگر $n = pa^۲$ عدد تام فردی باشد، آنگاه (به پیمانهٔ ۸) $n \equiv p$.

۱۵. ثابت کنید هر عدد تام فرد n حداقل سه عامل اول متمایز دارد. [راهنمایی: فرض کنید $n = p^k q^{۲j}$، که در آن (به پیمانهٔ ۴) $p \equiv k \equiv ۱$. با استفاده از نابرابری $۲ \equiv \sigma(n)/(n) \leq [p/(p-۱)][q/(q-۱)]$ به تناقض برسید.]

۱۶. اگر عدد صحیح $n > ۱$ حاصلضرب چند عدد اول متمایز مرسن باشد، نشان دهید که به ازای kای، $\sigma(n) = ۲^k$.

۳ـ۱۰ عددهای فرما

برای تکمیل بحث، ردهٔ دیگری از عددها موسوم به عددهای فرما راکه منبع پرمایه‌ای از حدسهاست معرفی می‌کنیم. این اعداد را می‌توان حالت خاصی از عددهای صحیحِ به‌صورت $۲^m + ۱$ درنظر گرفت. متذکر می‌شویم که اگر $۲^m + ۱$ عددی اول باشد، آنگاه به‌ازای $n > ۰$ای، $m = ۲^n$؛ زیرا اگر برخلاف آن فرض کنیم m دارای مقسوم‌علیه فردی به‌صورت $۲k + ۱ > ۱$ باشد، مثلاً $m = (۲k+۱)r$، آنگاه

$$
\begin{aligned}
۲^m + ۱ &= ۲^{(۲k+۱)r} + ۱ = (۲^r)^{۲k+۱} + ۱ \\
&= (۲^r + ۱)(۲^{۲kr} - ۲^{(۲k-۱)r} + \ldots + ۲^{۲r} - ۲^r + ۱)
\end{aligned}
$$

که غیرممکن است. به‌طور خلاصه، $۲^m + ۱$ وقتی اول است که m توانی از ۲ باشد.

تعریف ۱۰ـ۲ هر عدد صحیح به‌صورت

$$F_n = ۲^{۲^n} + ۱ \qquad n \geq ۰$$

عدد فرما نامیده می‌شود.

F_n اگر اول باشد، عدد اول فرما نامیده می‌شود.

فرما، که شهود ریاضی او معمولاً قابل اعتماد بود، ملاحظه کرد که عددهای صحیح

$$F_۰ = ۳, F_۱ = ۵, F_۲ = ۱۷, F_۳ = ۲۵۷, F_۴ = ۶۵۵۳۷$$

همگی عددهایی اول هستند و حدس زد که به‌ازای هر مقدار n، F_n عددی اول است. در نامه‌ای به مرسن با اطمینان اعلام کرد: «دریافته‌ام که عددهای به‌صورت $۲^{۲^n} + ۱$ همواره عددهایی اول هستند و مدتهاست که درستی این قضیه را به ریاضیدانان اعلام کرده‌ام.» مع‌الوصف، فرما از ناتوانیش در ارائهٔ اثبات ابراز ناراحتی می‌کرد و از دلخوری فزاینده‌اش در نامه‌های بعدی معلوم می‌شود که دائماً سعی می‌کرده قضیه را اثبات کند. اویلر در ۱۷۳۲ با ارائهٔ

$$F_۵ = ۲^{۲^۵} + ۱ = ۴۲۹۴۹۶۷۲۹۷$$

که بر ۶۴۱ بخشپذیر است، خطّ بطلانی بر حدس فرما کشید. چنین عددی به نظر ما خیلی بزرگ نمی‌رسد، ولی بررسی اول بودن آن در زمان فرما دشوار بود و واضح است که او این کار را انجام نداد.

اثبات مقدّماتی زیر از $۶۴۱|F_۵$، مستقیماً سر و کاری با تقسیم ندارد و متعلق به بنت[1] است.

قضیهٔ ۱۰ـ۸ عدد فرمای $F_۵$ بر ۶۴۱ بخشپذیر است.

اثبات. به‌ازای $a = ۲^۷$ و $b = ۵$ داریم

$$۱ + ab = ۱ + ۲^۷ \times ۵ = ۶۴۱$$

به آسانی ملاحظه می‌شود

$$۱ + ab - b^۴ = ۱ + (a - b^۳)b = ۱ + ۳b = ۲^۴$$

پس

$$\begin{aligned} F_۵ = ۲^{۲^۵} + ۱ &= ۲^{۳۲} + ۱ \\ &= ۲^۴a^۴ + ۱ \\ &= (۱ + ab - b^۴)a^۴ + ۱ \\ &= (۱ + ab)a^۴ + (۱ - a^۴b^۴) \\ &= (۱ + ab)[a^۴ + (۱ - ab)(۱ + a^۲b^۲)] \end{aligned}$$

که نشان می‌دهد $۶۴۱|F_n$. □

---

1. G. Bennett

تا امروز هنوز معلوم نشده است که تعداد عددهای اول فرما نامتناهی است یا نه، و عدد اول فرمایی بعد از $F_۴$ وجود دارد یا نه. «حدس» غالب این است که همهٔ عددهای فرمای $F_n > F_۴$ مرکب‌اند.

بخشی از علاقه به عددهای اول فرما ناشی از کشف ارتباط جالب توجه آنهاست با مسأله قدیمی تعیین همهٔ چند ضلعیهای منتظمی که با خط‌کش و پرگار (بدون استفاده از وسیلهٔ دیگر) قابل ترسیم‌اند (که اولی فقط برای رسم خطهای راست و دومی فقط برای رسم کمان به‌کار می‌رود). گاوس در هفتمین و آخرین بخش تحقیقات حسابی ثابت کرد n ضلعی منتظم به این روش قابل ترسیم است اگر و تنها اگر

$$n = ۲^k p_۱ p_۲ \dots p_r \quad \text{یا} \quad n = ۲^k$$

که در آن $k \geq ۰$ و $p_۱، p_۲، \dots، p_r$ عددهای اول فرمای متمایزی هستند. شیوهٔ رسم چندضلعیهای منتظم با ۲^k، ۳×۲^k، ۵×۲^k، ۱۵×۲^k ضلع از زمان هندسه‌دانان یونانی معلوم بوده است. به‌ویژه، آنها می‌توانستند n ضلعی منتظم را به‌ازای $n = ۳, ۴, ۵, ۶, ۸, ۱۰, ۱۲, ۱۵, ۱۶$ بسازند. چیزی که پیش از گاوس انتظارش را نداشتند، امکان ترسیم ۱۷ ضلعی منتظم با خط‌کش و پرگار بود. گاوس به اندازه‌ای به این کشف خود افتخار می‌کرد که وصیت کرد ۱۷ ضلعی منتظمی بر سنگ قبر او حکّاکی شود؛ این وصیت به دلایلی هرگز اجرا نشد، ولی چنین چندضلعیی بر وجهی از بنای یادبودی که به افتخار گاوس در زادگاهش در برانشوایک آلمان ساخته شد، حکّ گردید.

یک ویژگی مفید عددهای فرما این است که آنها نسبت به هم متباین‌اند.

قضیهٔ ۱۰ـ۹ به‌ازای عددهای فرمای F_n و F_m، $m > n \geq ۰$، داریم $\gcd(F_m, F_n) = ۱$.

اثبات. قرار می‌دهیم $d = \gcd(F_m, F_n)$. چون عددهای فرما عددهای صحیح فردی هستند، d باید فرد باشد. اگر قرار دهیم $x = ۲^{۲^n}$ و $k = ۲^{m-n}$، آنگاه

$$\begin{aligned} \frac{F_m - ۲}{F_n} &= \frac{(۲^{۲^n})^{۲^{m-n}} - ۱}{۲^{۲^n} + ۱} \\ &= \frac{x^k - ۱}{x + ۱} = x^{k-۱} - x^{k-۲} + \dots - ۱ \end{aligned}$$

یعنی، $F_n | (F_m - ۲)$. ولی $d | F_n$، پس $d | (F_m - ۲)$. بنابراین، با توجه به اینکه $d | F_m$، معلوم می‌شود $d | ۲$ و چون d عددی فرد است، $d = ۱$، و حکم مورد ادّعا ثابت می‌شود. □

با استفاده از این قضیه می‌توان نامتناهی بودن عددهای اول را به روش کوتاه و جالبی ثابت کرد: می‌دانیم که هریک از عددهای فرمای $F_۰$، $F_۱$، ...، F_n بر عدد اولی بخشپذیر است که،

بنابه قضیهٔ ۱۰ـ۹، F_kی دیگری را نمی‌شمارد. پس حداقل $n+1$ عدد اول متمایز نابیشتر از F_n وجود دارد. چون تعداد عددهای فرما نامتناهی است، تعداد عددهای اول نیز نامتناهی است.

در سال ۱۸۷۷، پپین[1] آزمونی عملی برای تشخیص اول بودن F_n ابداع کرد که در قضیهٔ زیر آمده است:

قضیهٔ ۱۰ـ۱۰ (پپین). به‌ازای $n \geq 1$، عدد فرمای $F_n = 2^{2^n} + 1$ اول است اگر وتنها اگر

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

اثبات. نخست فرض می‌کنیم

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

با مجذور کردن طرفین به‌دست می‌آوریم

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

همین همنهشتی به‌ازای هر مقسوم‌علیه F_n مانند p برقرار است:

$$3^{F_n-1} \equiv 1 \pmod{p}$$

اکنون فرض می‌کنیم k مرتبهٔ ۳ به پیمانهٔ p باشد. بنابه قضیهٔ ۸ـ۱، $k|F_n - 1$ یا به عبارت دیگر، $k|2^{2^n}$؛ بنابراین k باید توانی از ۲ باشد.

به‌ازای هر r که $r \leq 2^n - 1$، داریم $k \neq 2^r$؛ زیرا در غیر این صورت با مجذور کردن پیاپی همنهشتی $3^k \equiv 1 \pmod{p}$ به‌دست می‌آوریم

$$3^{2^{2^n-1}} \equiv 1 \pmod{p}$$

یا، به عبارت دیگر

$$3^{(F_n-1)/2} \equiv 1 \pmod{p}$$

از اینجا به $-1 \equiv 1 \pmod{p}$ و بنابراین به $p = 2$ می‌رسیم، که متضمن تناقض است. پس فقط این حالت باقی می‌ماند که

$$k = 2^{2^n} = F_n - 1$$

1. Pepin

بنابه قضیهٔ فرما می‌دانیم $k \leq p-1$، که ازاین هم نتیجه می‌شود $F_n = k+1 \leq p$. چون $p|F_n$، همچنین داریم $p < F_n$. با تلفیق این نابرابریها نتیجه می‌گیریم $F_n = p$، و بنابراین F_n اول است.

برعکس، فرض می‌کنیم که F_n، $n \geq 1$، اول باشد. بنابه قانون تقابل درجهٔ دوم داریم

$$(3/F_n) = (F_n/3) = (2/3) = -1$$

که درآن از $F_n \equiv (-1)^{2^n}+1 = 2$ (به‌پیمانهٔ ۳) استفاده‌کرده‌ایم. باکاربرد معیاراویلر نتیجه می‌شود

$$3^{(F_n-1)/2} \equiv -1 \quad (\text{به پیمانهٔ } F_n)$$

اول بودن $F_3 = 257$ را با استفاده از آزمون پپین نشان می‌دهیم. به پیمانهٔ ۲۵۷ داریم

$$\begin{aligned} 3^{(F_3-1)/2} &= 3^{128} = 3^3(3^5)^{25} \\ &\equiv 27(-14)^{25} \\ &\equiv 27 \times 14^{24}(-14) \\ &\equiv 27(-17)(-14) \\ &\equiv 27 \times 19 \equiv 513 \equiv -1 \quad (\text{به پیمانهٔ} 257) \end{aligned}$$

بنابراین، F_3 اول است. □

در سال ۱۹۰۵، مورهد[1] و وسترن[2]، مستقل از هم ، آزمون پپین را در مورد F_7 اجرا کردند و مرکب بودن آن را تقریباً به طور همزمان اعلام کردند. ۶۶ سال طول کشید تا بریل‌هارت[3] و موریسن در سال ۱۹۷۱ تجزیهٔ F_7 به حاصلضرب عاملهای اول را کشف کردند:

$$\begin{aligned} F_7 &= 2^{128}+1 \\ &= 59649589127497217 \times 5704689200685129054721 \end{aligned}$$

(احتمال به‌دست آوردن چنین تجزیه‌ای بدون استفاده ازکامپیوترهای سریع با حافظهٔ بزرگ بسیار ضعیف است.) در ۱۹۰۹، مورهد و وسترن محاسبه‌ای مشابه برای تشخیص مرکب بودن F_8 انجام دادند (هریک نصف کار را به عهده داشت)؛ ولی تا سال ۱۹۸۱ هیچ‌یک از عوامل آن عملاً به‌دست نیامد . درآن سال برنت[4] و پولارد[5] نشان دادند عدد

$$1238926361552897$$

1. J. C. Morehead 2. A. E. Western 3. Brillhart 4. Brent
5. Pollard

کوچکترین عامل اول F_8 است. عامل دیگر F_8، ۶۲ رقمی است و اندکی بعد نشان داده شد که اول است. F_n بزرگی که با آزمون پپین بررسی شده، F_{14} است که عددی است ۴۹۳۳ رقمی. سلفریج[1] و هورویتس[2] در ۱۹۶۳ نشان دادند که این عدد فرما مرکب است، ولی تاکنون مقسوم‌علیهی از آن به دست نیامده است.

آخرین قضیهٔ ما که متعلق به اویلر و لوکاس است، ابزار کارامدی در تعیین مقسوم‌علیه‌های عددهای فرماست. اویلر در سال ۱۷۴۷ ثابت کرد که هر عامل اول F_n باید به‌صورت $k \times ۲^{n+1} + ۱$ باشد؛ متجاوز از ۱۰۰ سال بعد، در ۱۸۷۹، ادوارد لوکاس متخصص فرانسوی نظریهٔ اعداد با اثبات زوج بودن k نتیجهٔ اویلر را به‌صورت بهتری درآورد.

قضیهٔ ۱۰ـ۱۱ هر مقسوم‌علیه pی عددی فرمای $F_n = ۲^{۲^n} + ۱$، که $n \geq ۲$، به صورت $p = k \times ۲^{n+2} + ۱$ است.

اثبات. به‌ازای هر مقسوم‌علیه اول p از F_n داریم

$$۲^{۲^n} \equiv -۱ \quad (\text{به پیمانهٔ } p)$$

و با مجذور کردن خواهیم داشت

$$۲^{۲^{n+1}} \equiv ۱ \quad (\text{به پیمانهٔ } p)$$

اگر h مرتبهٔ ۲ به پیمانهٔ p باشد، بنابه این همنهشتی داریم

$$h | ۲^{n+1}$$

اگر $۱ \leq r \leq n$، آنگاه $h \neq ۲^r$، زیرا در غیر این‌صورت لازم می‌آید

$$۲^{۲^n} \equiv ۱ \quad (\text{به پیمانهٔ } p)$$

و بنابراین $p = ۲$،که متضمن تناقض است. پس $h = ۲^{n+1}$. چون مرتبهٔ ۲ به پیمانهٔ p، $\phi(p) = p - ۱$ را می‌شمارد، نتیجه می‌گیریم $۲^{n+1} | p - ۱$. نکته این است که به‌ازای $n \geq ۲$، $p \equiv ۱$ (به پیمانهٔ ۸) و بنابراین، بنابه قضیه ۹ـ۶، نماد لژاندار $(۲/p)$ برابر ۱ است. با استفاده از معیار اویلر بیدرنگ نتیجه می‌شود

$$۲^{(p-1)/2} \equiv (۲/p) = ۱ \quad (\text{به پیمانهٔ } p)$$

1. Selfridge 2. Hurwitz

اثبات با توسل به قضیهٔ ۸ـ۱ کامل می‌شود؛ بنا به قضیهٔ مزبور، $h|(p-۱)/۲$، یا معادلش $۲^{n+۱}|(p-۱)/۲$. پس $۲^{n+۲}|p-۱$، و از این‌رو، به‌ازای عدد صحیح kای، $p = k\times ۲^{n+۲}+۱$. □

قضیهٔ ۱۰ـ۱۱ به ما امکان می‌دهد سرشت $F_۴ = ۲^{۱۶}+۱ = ۶۵۵۳۷$ را به آسانی معلوم کنیم. مقسوم‌علیه‌های اول $F_۴$ باید به‌صورت $۲^۶k+۱ = ۶۴k+۱$ باشند. فقط یک عدد اول نابیشتر از $\sqrt{F_۴}$ به این شکل وجود دارد که عدد اول ۱۹۳ است. چون $F_۴$ بر ۱۹۳ بخشپذیر نیست، نتیجه می‌گیریم که خود $F_۴$ عددی اول است.

با رواج روزافزون کامپیوتر و افزایش سرعت آن، دامنهٔ جستجوی عاملهای اول عددهای فرما به‌میزان قابل توجهی گسترش یافته است. در ۱۹۸۰، گاستین[1] عامل اول ۳۱۰۶۵۰۳۷۶۰۲۸۱۷ از $F_{۱۷}$ را کشف کرد (هیچ‌یک از این عاملها پیشتر تعیین نشده بود). پیشرفت محاسباتی دیگر کاربرد موفقیت‌آمیز آزمون پپین در مورد $F_{۲۰}$ (در سال ۱۹۸۷) توسط یانگ[2] و بوئل[3] بود. این عدد ۳۱۵۶۵۳ رقمی است؛ پیش از این، $F_{۱۴}$ بزرگترین عدد فرمایی بود که تحت آزمون قرار گرفته بود. اکنون معلوم شده است که F_n به‌ازای $۵ \leq n \leq ۲۰$ و همچنین به‌ازای ۶۰ مقدار دیگر n، که بزرگترینشان $n = ۲۳۴۷۳$ است، مرکب است. در مورد $F_{۲۲}$، بررسی ادامه دارد: این کوچکترین عدد فرماست که وضعیت آن هنوز معلوم نیست. با توجه به اندازهٔ $F_{۲۲}$، محتمل به‌نظر نمی‌رسد که تکلیف آن به این زودی مشخص شود.

خلاصه‌ای از اطلاعات موجود دربارهٔ وضعیت عددهای فرمای F_n (از لحاظ اول بودن یا نبودن و عاملهای مربوطه) به‌ازای $۰ \leq n \leq ۳۰$ در زیر ملاحظه می‌شود.

n	وضعیت F_n
۰, ۱, ۲, ۳, ۴	اول
۵, ۶, ۷, ۸, ۹	کاملاً تجزیه شده است
۱۰, ۱۱, ۱۲, ۱۹, ۳۰	دو یا چهار عامل تعیین شده است
۱۳, ۱۵, ۱۶, ۱۷, ۱۸, ۲۱, ۲۳, ۲۵, ۲۶, ۲۷	فقط یک عامل اول شناخته شده است
۱۴, ۲۰	مرکب است ولی عاملی به‌دست نیامده است
۲۲, ۲۴, ۲۸, ۲۹	نامعلوم

وضع $F_{۱۶}$ در ۱۹۵۳ روشن شد و این حدس وسوسه‌انگیز که همهٔ جمله‌های دنبالهٔ

$$۲+۱,\ ۲^۲+۱,\ ۲^{۲^۲}+۱,\ ۲^{۲^{۲^۲}}+۱,\ ۲^{۲^{۲^{۲^۲}}}+۱, \ldots$$

1. G. Gostin 2. Young 3. Buell

عددهایی اول هستند، باطل گردید. نکتهٔ جالب توجه این است که عددهای فرما بر مربع هیچ‌یک از عاملهای اول شناخته شده‌شان بخشپذیر نیستند؛ در واقع، حدس زده می‌شود که عددهای فرما خالی از مربع‌اند.

عددهای به‌صورت $k \times ۲^n + ۱$، که در فرایند جستجوی عاملهای اول عددهای فرما مطرح می‌شوند، به خودی‌خود نیز اهمیت زیادی دارند. در بعضی موردها، کوچکترین nای که به‌ازای آن $k \times ۲^n + ۱$ عددی اول است، ممکن است خیلی بزرگ باشد؛ به‌عنوان نمونه، $n = ۵۸۳$ نخستین nای است که به‌ازای آن $۴۷ \times ۲^n + ۱$ اول است. ولی مقدارهایی برای k وجود دارد که $k \times ۲^n + ۱$ همیشه مرکب است. در واقع، در ۱۹۶۰ ثابت شد عددهای صحیح فرد kای به تعداد نامتناهی وجود دارند به‌طوری که به‌ازای هر $n \geq ۱$، عدد $k \times ۲^n + ۱$ مرکب است. مسألهٔ تعیین کوچکترین k با این ویژگی، هنوز حل نشده است. تاکنون، $k = ۷۸۵۵۷$ کوچکترین kی شناخته‌ای است که به‌ازای آن $k \times ۲^n + ۱$ به‌ازای هیچ nای اول نیست.

تمرینهای ۱۰ـ۳

۱. همنهشتی (به پیمانهٔ ۶۴۱) $۵ \times ۲^۷ \equiv -۱$ را به توان چهار رسانده نتیجه بگیرید (به پیمانهٔ ۶۴۱) $۲^{۳۲} + ۱ \equiv ۰$؛ بنابراین، $۶۴۱ | F_۵$.

۲. گاوس (در ۱۷۹۶) کشف کرد که p ضلعی منتظم، چنانچه p عددی اول باشد، با خط‌کش و پرگار قابل رسم است اگر و فقط اگر $p - ۱$ توانی از ۲ باشد. نشان دهید این شرط هم‌ارز با این است که p یک عدد اول فرما باشد.

۳. به‌ازای $n > ۰$، ثابت کنید که

(الف) بینهایت عدد مرکب به‌صورت $۲^{۲^n} + ۳$ وجود دارد؛ [راهنمایی: با استفاده از اینکه به‌ازای k ای، $۲^{۲^n} = ۳k + ۱$، ثابت کنید $۷ | ۲^{۲^{۲n+۱}} + ۳$.]

(ب) هریک عددهای $۲^{۲^n} + ۵$ مرکب است.

۴. عددهای صحیح مرکب nای که به‌ازای آنها $n | ۲^n - ۲$، اولنما نامیده می‌شوند. نشان دهید

(الف) اگر n عدد اولنمای فردی باشد، آنگاه عدد مرسن M_n نیز اولنما است؛ پس، بینهایت عدد اولنما وجود دارد. [راهنمایی: از رابطهٔ $۲n | ۲^n - ۲$ نتیجه می‌شود $n | ۲^{n-۱} - ۱$، پس به‌ازای kای، $kn = ۲^{n-۱} - ۱$. بنابراین $۲^{M_n-۱} - ۱ = ۲^{۲kn} - ۱ = (۲^n)^{۲k} - ۱$، که نشان می‌دهد $۲^n - ۱ | ۲^{M_n-۱} - ۱$.]

(ب) هر عدد فرمای F_n یا اول است یا اولنما. [راهنمایی: همنهشتی (به پیمانهٔ F_n) $۲^{۲^n} \equiv -۱$ را به توان $۲^{۲^n - n}$ برسانید.]

۵. نشان دهید که به‌ازای $n \geq ۲$، آخرین رقم سمت راست عدد فرمای $F_n = ۲^{۲^n} + ۱$ برابر ۷ است. [راهنمایی: به استقرا بر n، به‌ازای $n \geq ۲$، نشان دهید (به پیمانهٔ ۱۰) $۲^{۲^n} \equiv ۶$.]

۶. نشان دهید $۲^{۲^n} - ۱$ حداقل n مقسوم‌علیه اول متمایز دارد. [راهنمایی: از استقرا بر n و اتحاد $(۲^{۲^{n-۱}} - ۱)(۲^{۲^{n-۱}}) = ۲^{۲^n} - ۱$ استفاده کنید.]

۷. در سال ۱۸۶۹، لاندری[1] نوشت: «تجزیهٔ هیچ‌یک از عددهای $۲^n \pm ۱$ به‌اندازهٔ $۲^{۵۸} + ۱$ ما را به زحمت نینداخت.» نشان دهید که $۲^{۵۸} + ۱$ را می‌توان با استفاده از اتحاد

$$۴x^۴ + ۱ = (۲x^۲ - ۲x + ۱)(۲x^۲ + ۲x + ۱)$$

نسبتاً به‌آسانی تجزیه کرد.

۸. با استفاده از تمرین ۵ نتیجه بگیرید که

(الف) عدد فرمای F_n هرگز مربع کامل نیست؛

(ب) به‌ازای $n > ۰$، F_n هرگز عددی مثلثی نیست.

۹. (الف) نشان دهید که به‌ازای هر عدد صحیح فرد n، $۳|۲^n + ۱$.

(ب) اگر p و q عددهای اول فردی باشند و $q|۲^p + ۱$، آنگاه یا $q = ۳$ یا به‌ازای عدد صحیح kای، $q = ۲kp + ۱$. [راهنمایی: چون (به پیمانهٔ q) $۲^{۲p} \equiv ۱$، مرتبهٔ ۲ به پیمانهٔ q یا ۲ است یا $۲p$؛ در حالت اخیر، $۲p|\phi(q)$.]

(پ) کوچکترین مقسوم‌علیه اول بزرگتر از ۳ی هریک از عددهای صحیح $۲^{۲۹} + ۱$ و $۲^{۴۱} + ۱$ را پیدا کنید.

۱۰. مطلوب است یافتنِ کوچکترین عدد صحیح فرد $n > ۱$ با این ویژگی که $۲^n - ۱$ بر زوجی از عددهای اول دوقلوی p و q، $p < q$، بخشپذیر باشد. [راهنمایی: از آنجا که p نخستین عضو زوجی از اوّلهای دوقلو است، داریم (به پیمانهٔ ۶) $p \equiv -۱$. چون $(۲/q) = (۲/p) = ۱$، بنابه قضیهٔ ۹ـ۶، (به پیمانهٔ ۸) $p \equiv q \equiv \pm ۱$؛ پس، (به پیمانهٔ ۲۴) $p \equiv -۱$ و (به پیمانهٔ ۲۴) $q \equiv ۱$. اکنون از اینکه مرتبه‌های ۲ به پیمانه‌های p و q باید n را بشمارند، استفاده کنید.]

۱۱. همهٔ عددهای اول pای را پیدا کنید که p عدد $۲^p + ۱$ را بشمارد؛ همین کار را در مورد $۲^p - ۱$ تکرار کنید.

۱۲. فرض کنید به‌ازای $n \geq ۱$، $p = ۳ \times ۲^n + ۱$ عددی اول باشد. (تاکنون بیست و پنج عدد اول از این نوع شناخته شده است که کوچکترین آنها به‌ازای $n = ۱$ و بزرگترینشان به‌ازای $n = ۳۹۱۲$ به‌دست می‌آید.) هریک از حکمهای زیر را ثابت کنید

---

1. Landry

(الف) به‌ازای kای که $0 \leq k \leq n$، مرتبهٔ ۲ به پیمانهٔ p یا 2^k است و یا 3×2^k.

(ب) بجز وقتی $p = 13$، ۲ ریشهٔ اولیهٔ p نیست. [راهنمایی: اگر ۲ ریشه‌ای اولیه از p باشد، آنگاه $(2/p) = -1$.]

(پ) مرتبهٔ ۲ به پیمانهٔ p بر ۳ بخشپذیر نیست اگر و تنها اگر p عدد فرمای F_kای را، که $0 \leq k \leq n - 1$، بشمارد. [راهنمایی: از اتحاد $F_0 F_1 \ldots F_{k-1} = 2^{2^k} - 1$ استفاده کنید.]

(ت) عدد فرمایی وجود ندارد که بر ۷، ۱۳، یا ۹۷ بخشپذیر باشد.

۱۳. ثابت کنید که هر عدد فرمای $F_n = 2^{2^n} + 1$، برحسب اینکه n فرد یا زوج باشد، به‌ترتیب، همنهشت با ۵ یا همنهشت با ۸ به پیمانهٔ ۹ است. [راهنمایی: نخست با استقرا نشان دهید که $2^{2^n} \equiv 2^{2^{n-2}}$ (پیمانهٔ ۹).]

۱۴. با استفاده از اینکه مقسوم‌علیه‌های اول F_5 به‌صورت $2^7 k + 1 = 128k + 1$ هستند، نشان دهید $641 | F_5$.

۱۵. ثابت کنید که به‌ازای هر عدد اول $p > 3$

(الف) $\frac{1}{3}(2^p + 1)$ بر ۳ بخشپذیر نیست.[راهنمایی: اتحاد

$$\frac{2^p + 1}{2 + 1} = 2^{p-1} - 2^{p-2} + \ldots - 2 + 1$$

را درنظر بگیرید.]

(ب) $\frac{1}{3}(2^p + 1)$ مقسوم‌علیه اولی بزرگتر از p دارد. [راهنمایی: تمرین ۹ (ب).]

(پ) هر دو عدد صحیح $\frac{1}{3}(2^{19} + 1)$ و $\frac{1}{3}(2^{23} + 1)$ اول هستند.

۱۶. با استفاده از تمرین قبل، نتیجه بگیرید که بینهایت عدد اول وجود دارد.

۱۷. (الف) ثابت کنید ۳، ۵، و ۷ نامانده‌های درجهٔ دوم هر عدد اول فرمای F_n هستند. [راهنمایی: آزمون پیپن و تمرین ۱۵ در بخش ۹ـ۳.]

(ب) نشان دهید هر ناماندهٔ درجهٔ دوم عدد اول فرمای F_n ریشهٔ اولیه‌ای از F_n است.

۱۸. نشان دهید که هر عدد اول فرمای F_n را می‌توان به‌صورت تفاضل دو مربع نوشت، ولی نمی‌توان آن‌را به‌صورت تفاضل دو مکعب نوشت. [راهنمایی: از اتخاذ

$$F_n = 2^{2^n} + 1 = (2^{2^n - 1} + 1)^2 - (2^{2^n - 1})^2$$

استفاده کنید.]

۱۹. به‌ازای $n \geq 1$، نشان دهید $\gcd(F_n, n) = 1$. [راهنمایی: قضیهٔ ۱۰ـ۱۱.]

۱۱

حدس فرما

«کسی که در جستجوی روش است بی‌آنکه مسأله‌ای مشخص در ذهن داشته باشد، اغلب به نتیجه‌ای نمی‌رسد.»

داوید هیلبرت

۱۱ـ۱ سه‌تاییهای فیثاغورسی

فرما که بسیاری او را پدر نظریهٔ جدید اعداد به حساب می‌آورند، عادتی غریب و نامتناسب با این نقش داشت. شخصاً یافته‌هایش را بسیار کم منتشر می‌کرد و ترجیح می‌داد آنها را در نامه‌هایی خطاب به دوستانش مطرح کند (آن هم با عباراتی بسیار کوتاه حاکی از اینکه اثباتی در دست دارد) یا به‌صورت یادداشتهایی برای خود محفوظ دارد. تعدادی از این یادداشتها را در حاشیهٔ صفحات نسخه‌ای از ترجمهٔ باشه[1] از حساب دیوفانتوس نوشته است. معروفترین اظهارنظر درمیان این یادداشتهای حاشیه‌ای، که احتمالاً در ۱۶۳۷ نوشته شده است، چنین است:

> غیر ممکن است مکعبی را به‌صورت مجموع دو مکعب، توان چهارمی را به‌صورت مجموع دو توان چهارم، و به‌طورکلی هر توانی فراتر از توان دوم را به‌صورت مجموعی از دو توان مشابه نوشت. برای این

1. Bachet

مطلب، اثباتی به راستی شگفت‌انگیز یافته‌ام که در این حاشیه نمی‌گنجد.

فرما با این عبارات وسوسه‌انگیز می‌خواهد بگوید که اگر $n > ۲$، آنگاه معادلهٔ دیوفانتی

$$x^n + y^n = z^n$$

بجز جوابهای بدیهی، یعنی جوابهایی که در آنها حداقل یکی از متغیرها صفر باشد، جوابی در اعداد صحیح ندارد.

قولی که در بالا نقل شد به آخرین قضیهٔ فرما یا، دقیقتر، به حدس فرما معروف شده است. بعدها نتیجه‌هایی که فرما در حاشیه‌های کتاب حساب دیوفانتوس یادداشت کرده بود، بجز آخرین قضیه‌اش که هنوز در انتظار اثبات یا ابطال است[۱]، درست از آب درآمدند. اگر هم فرما «اثباتی به‌راستی شگفت‌انگیز» داشته بوده باشد این اثبات هنوز به‌دست نیامده است. تا امروز، این حدس فقط به‌ازای مقدارهای خاصی از نمای n ثابت شده است (کامپیوترهای الکترونیک نشان داده‌اند که هیچ جوابی نابدیهی در محدودهٔ $۳ \leq n < ۱۵۰۰۰۰$ وجود ندارد)، و اثبات کلی آن در آیندهٔ نزدیکی محتمل به‌نظر نمی‌رسد[۲].

هر مثال ناقض صریح حدس فرما [در صورت وجود] حاوی عددهای صحیح بزرگی خواهد بود. نشان داده شده است که اگر p عدد اول فردی باشد، $xyz \neq ۰$، و $x^p + y^p = z^p$، آنگاه x باید حداقل ۸٫۱ میلیون رقم و x^p حداقل ۲×۱۰^{۱۱} رقم داشته باشد. در نماد اعشاری، به متجاوز از یکصد صفحه برای نوشتن x و دست کم ده هزار جلد یکهزار صفحه‌ای برای نوشتن x^p نیاز خواهیم داشت.

مع‌الوصف، فرما اثباتی از آخرین قضیه‌اش به‌ازای $n = ۴$ بجا نهاده است. برای تسهیل شرح این اثبات، نخست همهٔ جوابهای صحیح مثبت معادلهٔ

$$x^۲ + y^۲ = z^۲ \qquad (۱)$$

را تعیین می‌کنیم. چون میان z طول وتر مثلث قائم‌الزاویه و x و y طولهای ضلعهای مجاور به زاویهٔ قائمه آن اتحاد معروف فیثاغورسی $z^۲ = x^۲ + y^۲$ برقرار است، مسألهٔ جستجوی همهٔ عددهای صحیح مثبتی که در (۱) صدق کنند معادل با مسألهٔ تعیین همهٔ مثلثهای قائم‌الزاویه با ضلعهایِ به طول صحیح است. این مسأله در زمان بابلیها مطرح شد و یکی از مسأله‌های مورد علاقهٔ هندسه‌دانان یونان باستان بود. فرمول

$$x = ۲n + ۱, \quad y = ۲n^۲ + ۲n, \quad z = ۲n^۲ + ۲n + ۱$$

---

۱ و ۲. قضیهٔ آخر فرما در سال ۱۳۷۳ به‌دست اندرو وایلز ریاضیدان انگلیسی با همکاری شاگردش ریچارد تیلر به اثبات رسید.ـم.

که در آن nعدد صحیح مثبت دلخواهی است، و تعدادی نامتناهی از این مثلثها را به‌دست می‌دهد، منسوب به خود فیثاغورس است. از این فرمول همهٔ مثلثهای قائم‌الزاویه با ضلعهای صحیح به‌دست نمی‌آیند و تا زمانی که اقلیدس اصول خود را ننوشت، حل کامل این مسأله در دست نبود.

تعریف زیر روش فشرده‌ای برای یاد کردن از جوابهای (۱) ارائه می‌کند.

تعریف ۱۱ـ۱ سه‌تایی فیثاغورسی مجموعه‌ای از سه عدد صحیح x، y و z است به‌طوری‌که $x^2 + y^2 = z^2$؛ چنین سه‌تایی اولیه نامیده می‌شود اگر $\gcd(x, y, z) = 1$.

شاید معروفترین مثالها از سه‌تاییهای اولیهٔ فیثاغورثی ۳، ۴، ۵ و ۵، ۱۲، ۱۳ و مثالی با وضوح کمتر، ۱۲، ۳۵، ۳۷ باشد.

در اینجا ذکر چند نکته لازم است. فرض می‌کنیم x، y و z یک سه‌تایی فیثاغورسی باشد و $d = \gcd(x, y, z)$. اگر بنویسیم $x = dx_1$، $y = dy_1$، $z = dz_1$، آنگاه به آسانی ملاحظه می‌شود که

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2$$

و $\gcd(x_1, y_1, z_1) = 1$. به‌طور خلاصه، x_1، y_1، z_1، یک سه‌تایی فیثاغورسی اولیه تشکیل می‌دهند. بنابراین، کافی است همّ خود را فقط صرف تعیین همهٔ سه‌تاییهای فیثاغورسی اولیه کنیم؛ هر سه‌تایی فیثاغورسی از ضرب سه‌تایی اولیه‌ای در عدد صحیح ناصفر مناسبی به‌دست می‌آید. جستجو را می‌توان به سه‌تاییهای فیثاغورسی اولیهٔ x، y، zای محدود کرد که $x > 0$، $y > 0$، $z > 0$، زیرا بقیه را می‌توان از سه‌تاییهای مثبت با تغییر علامت ساده‌ای به‌دست آورد.

بررسی ما به دو لم مقدماتی، که نخستینِ آنها حاوی نکته‌ای اساسی در مورد سه‌تاییهای فیثاغورسی اولیه است، نیازمنداست.

لم ۱. اگر x، y، z سه‌تایی فیثاغورسی اولیه‌ای باشد، آنگاه یکی از عددهای صحیح x و y فرد و دیگری زوج است.

اثبات. اگر هر دوی x و y زوج باشند، آنگاه $2 \mid (x^2 + y^2)$ یا $2 \mid z^2$، و درنتیجه $2 \mid z$. بنابراین $\gcd(x, y, z) \geq 2$، که می‌دانیم قابل قبول نیست. از سوی دیگر، اگر هم x و y فرد باشند، آنگاه $x^2 \equiv 1$ (به پیمانهٔ ۴) و $y^2 \equiv 1$ (به پیمانهٔ ۴)، که نتیجه می‌هد

$$z^2 = x^2 + y^2 \equiv 2 \ (\text{به پیمانهٔ } 4)$$

ولی این نیز غیر ممکن است، زیرا مربع هر عدد صحیح باید همنهشت با ۰ یا ۱ به پیمانهٔ ۴ باشد. □

اگر x، y، z سه‌تایی فیثاغورسی اولیه‌ای باشد، دقیقاً یکی از این عددهای صحیح زوج و دوتای دیگر آن فردند (اگر x، y، z همگی فرد باشند، آنگاه $x^۲ + y^۲$ زوج است، در حالی که $z^۲$ فرد است.). لم فوق نشان می‌دهد که یا x زوج است یا y؛ برای پرهیز از ابهام، از این به بعد فرض می‌کنیم که در سه‌تاییهای فیثاغورسی مورد بحث ما x زوج و y فرد است؛ البته در این صورت، z فرد است.

شایان توجه است (و ما از این حکم استفاده خواهیم کرد) که هر زوج از عددهای صحیح x، y و z باید متباین باشد، زیرا اگر $\gcd(x, y) = d > ۱$، عدد اول p ای وجود دارد که $p|d$. چون $d|x$ و $d|y$، لازم می‌آید $p|x$ و $p|y$، بنابراین $p|x^۲$ و $p|y^۲$. ولی در این صورت $p|(x^۲ + y^۲)$، یا $p|z^۲$، که نتیجه می‌دهد $p|z$. این با فرض $\gcd(x, y, z) = ۱$ سازگار نیست، و بنابراین $d = ۱$. به روش مشابهی می‌توان نشان داد که $\gcd(y, z) = \gcd(x, z) = ۱$.

بنابه لم ۱، سه‌تایی فیثاغورسی اولیهٔ x، y، z به‌طوری که هر سه عدد اول باشند، وجود ندارد. سه‌تاییهای فیثاغورسی اولیه‌ای که در آنها z و فقط یکی از x یا y اول باشد، موجودند؛ به‌عنوان مثال، ۳، ۴، ۵؛ ۱۱، ۶۰، ۶۱؛ و ۱۹، ۱۸۰، ۱۸۱. اینکه آیا تعداد چنین سه‌تاییهایی نامتناهی است یا نه، معلوم نیست.

مانع بعدی در سر راه ما اثبات این نکته است که اگر حاصلضرب دو عدد صحیح مثبت متباین a و b، مربع کامل باشد، آنگاه خود a و b نیز مربع کامل‌اند. به کمک قضیهٔ بنیادی حساب می‌توانیم حکم بسیار کلیتری را ثابت کنیم که لم زیر است.

لم ۲. اگر $\gcd(a, b) = ۱$ و $ab = c^n$، آنگاه هر یک از a و b به‌صورت توان n ام است؛ یعنی، عددهای صحیح مثبت $a_۱$ و $b_۱$ ای وجود دارند به‌طوری‌که $a = a_۱^n$، $b = b_۱^n$.

اثبات. بی‌آنکه به کلیت مطلب خللی وارد شود، فرض می‌کنیم $a > ۱$ و $b > ۱$. اگر

$$a = p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}, b = q_۱^{j_۱} q_۲^{j_۲} \ldots q_s^{j_s}$$

تجزیهٔ a و b به عددهای اول باشند، آنگاه، با توجه به اینکه $\gcd(a, b) = ۱$، هیچ p_i ای نمی‌تواند جزو q_i ها باشد. درنتیجه، تجزیهٔ ab به عاملهای اول عبارت است از

$$ab = p_۱^{k_۱} \ldots p_r^{k_r} q_۱^{j_۱} \ldots q_s^{j_s}$$

فرض می‌کنیم بتوان c را به‌صورت $c = u_۱^{l_۱} u_۲^{l_۲} \ldots u_t^{l_t}$ به حاصلضرب عاملهای اول تجزیه کرد. در این صورت از شرط $ab = c^n$ نتیجه می‌شود

$$p_۱^{k_۱} \ldots p_r^{k_r} q_۱^{j_۱} \ldots q_s^{j_s} = u_۱^{nl_۱} \ldots u_t^{nl_t}$$

از اینجا ملاحظه می‌شود که عددهای اول $u_1, \ldots, u_t$ (به‌ترتیبی) $p_1, \ldots, p_r$، $q_1, \ldots, q_s$ هستند، و $nl_1, \ldots, nl_t$ نماهای متناظر $k_1, \ldots, k_r$، $j_1, \ldots, j_s$ هستند. نتیجه: هریک از عددهای صحیح k_i و j_i باید بر n بخشپذیر باشند. اکنون اگر قرار دهیم

$$a_1 = p_1^{\frac{k_1}{n}} p_2^{\frac{k_2}{n}} \ldots p_r^{\frac{k_r}{n}}$$
$$b_1 = q_1^{\frac{j_1}{n}} q_2^{\frac{j_2}{n}} \ldots q_s^{\frac{j_s}{n}}$$

آنگاه طبق انتظار، $a_1^n = a$ و $b_1^n = b$. □

با این مقدمات، اکنون رده‌بندی همهٔ سه‌تاییهای فیثاغورسی اولیه کار ساده‌ای است.

قضیهٔ ۱۱ـ۱ همهٔ جوابهای معادلهٔ فیثاغورسی

$$x^2 + y^2 = z^2$$

که در شرطهای

$$\gcd(x, y, z) = 1,\quad 2|x,\quad x > 0,\ y > 0,\ z > 0$$

صدق می‌کنند، از فرمولهای

$$x = 2st,\quad y = s^2 - t^2,\quad z = s^2 + t^2$$

نتیجه می‌شوند که در آنها s و t عددهایی صحیح‌اند، $s > t > 0$، $\gcd(s, t) = 1$، و $s \not\equiv t$ (به پیمانهٔ ۲).

اثبات. در شروع کار فرض می‌کنیم x، y، z سه‌تایی فیثاغورسی اولیهٔ مثبتی باشد. چون توافق کرده‌ایم x را زوج و هر دوی y و z را فرد بگیریم، $z - y$ و $z + y$ عددهای صحیح زوجی هستند، مثلاً $z - y = 2u$ و $z + y = 2v$. اکنون معادلهٔ $x^2 + y^2 = z^2$ را می‌توانیم به‌صورت

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

بنویسیم؛ بنابراین

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv$$

ملاحظه می‌کنیم که u و v متباین‌اند؛ زیرا اگر $\gcd(u, v) = d > 1$، آنگاه $d|(u - v)$ و $d|(u + v)$، یا معادلش ، $d|y$ و $d|z$، که ناسازگار با $\gcd(y, z) = 1$ است. با توسل به لم ۲، نتیجه می‌گیریم هر یک از u و v مربع کامل است؛ مثلاً

$$u = t^2 \, , \, v = s^2$$

که s و t عددهای صحیح مثبتی هستند، این مقدارهای u و v را جایگزین می‌کنیم

$$z = u + v = s^2 + t^2$$

$$y = v - u = s^2 - t^2$$

$$x^2 = 4uv = 4s^2t^2$$

که رابطهٔ آخر معادل است با $x = 2st$. چون هر عامل مشترک s و t هر دوی y و z را می‌شمارد، از شرط $\gcd(y, z) = 1$ نتیجه می‌شود $\gcd(s, t) = 1$. می‌ماند اینکه توجه کنیم اگر هر دوی s و t زوج یا هر دو فرد باشند، آنگاه لازم می‌آید هر یک از y و z زوج باشند، که ممکن نیست. پس، دقیقاً یکی از دو عنصر s و t زوج و دیگری فرد است؛ به‌طور نمادین داریم (به پیمانهٔ ۲) $s \not\equiv t$.

برعکس، فرض می‌کنیم s و t دو عدد صحیح مقید به شرطهای توصیف‌شده در فوق باشند. اینکه $x = 2st$، $y = s^2 - t^2$، $z = s^2 + t^2$ تشکیل سه‌تایی فیثاغورسی می‌دهند، از اتحاد

$$x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2 = z^2$$

نتیجه می‌شود. این اتحاد به‌سادگی قابل اثبات است. برای اینکه نشان دهیم این سه‌تایی اولیه است، فرض می‌کنیم $\gcd(x, y, z) = d > 1$ و مقسوم‌علیه اول p از d را انتخاب می‌کنیم. توجه می‌کنیم که $p \neq 2$، زیرا p عدد فرد z را می‌شمارد (یکی از s و t فرد و دیگری زوج است، پس $z = s^2 + t^2$ باید فرد باشد). از $p|y$ و $p|z$ به‌دست می‌آوریم $p|(z + y)$ و $p|(z - y)$، یا به بیان دیگر، $p|2s^2$ و $p|2t^2$. ولی در این صورت $p|s$ و $p|t$، که ناسازگار با $\gcd(s, t) = 1$ است. نتیجه این است که $d = 1$ و بنابراین، x، y، z سه‌تایی فیثاغورسی اولیه‌ای تشکیل می‌دهند. به این ترتیب، قضیهٔ ۱۱ـ۱ ثابت می‌شود. □

جدول زیر برخی از سه‌تاییهای فیثاغورسی اولیه، به‌ازای مقدارهای کوچکی از s و t، را نشان می‌دهد. به‌ازای هر مقدار $s = 1, 2, 3, \ldots, 7$ مقدارهایی از t را انتخاب کرده‌ایم که با s متباین، کوچکتر از s، و در صورت فردبودن s، زوج‌اند.

		x	y	z
s	t	$(2st)$	$(s^2 - t^2)$	$(s^2 + t^2)$
۲	۱	۴	۳	۵
۳	۲	۱۲	۵	۱۳
۴	۱	۸	۱۵	۱۷
۴	۳	۲۴	۷	۲۵
۵	۲	۲۰	۲۱	۲۹
۵	۴	۴۰	۹	۴۱
۶	۱	۱۲	۳۵	۳۷
۶	۵	۶۰	۱۱	۶۱
۷	۲	۲۸	۴۵	۵۳
۷	۴	۵۶	۳۳	۶۵
۷	۶	۸۴	۱۳	۸۵

خواننده ممکن است با توجه به این جدول یا جدولی مفصلتر، حدس بزند که در هر سه‌تایی فیثاغورسی اولیهٔ x، y، z، دقیقاً یکی از عددهای صحیح x یا y بر ۳ بخشپذیر است. این حدس درست است زیرا بنابه قضیهٔ ۱۱ـ۱ داریم

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2$$

به‌طوری‌که $\gcd(s,t) = 1$. اگر $3|s$ یا $3|t$، آنگاه به‌وضوح $3|x$، و نیازی به استدلال بیشتر نیست. فرض می‌کنیم $3 \nmid s$ و $3 \nmid t$. بنابه قضیهٔ فرما

$$s^2 \equiv 1 \ (\text{به پیمانهٔ } 3), \ t^2 \equiv 1 (\text{به پیمانهٔ } 3)$$

و بنابراین

$$y = s^2 - t^2 \equiv 0 \ (\text{به پیمانهٔ } 3)$$

به بیان دیگر، y بر سه بخشپذیر است، و این نکته‌ای بود که می‌خواستیم نشان دهیم.

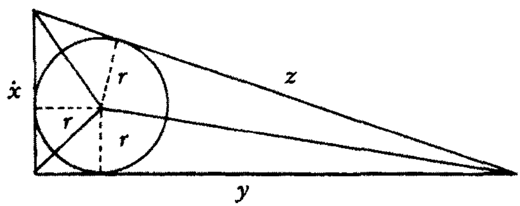
مثلث قائم‌الزاویه را مثلث فیثاغورسی می‌نامیم اگر طول ضلعهای آن عددهایی صحیح باشند. از یافته‌های ما می‌توان نتیجهٔ هندسی جالبی دربارهٔ مثلثهای فیثاغورسی به شرح زیر گرفت:

قضیهٔ ۱۱ـ۲ طول شعاع دایرهٔ محاطی مثلث فیثاغورسی همواره عددی صحیح است.

اثبات. فرض می‌کنیم r طول شعاع دایرهٔ محاط در یک مثلث قائم‌الزاویه باشد که طول وتر آن مثلث z و طول ضلعهای آن x و y است. مساحت مثلث برابر با مجموع مساحتهای سه‌مثلثی است که مرکز دایره رأس آنهاست، پس

$$\frac{1}{2}xy = \frac{1}{2}rx + \frac{1}{2}ry + \frac{1}{2}rz = \frac{1}{2}r(x+y+z)$$

وضعیت در شکل زیر ملاحظه می‌شود.



داریم $z^2 = x^2 + y^2$. به‌علاوه، می‌دانیم جوابهای صحیح مثبت این معادله به‌ازای عددهای صحیح مثبت k، s و t ی مناسبی از فرمولهای

$$x = 2kst,\ \ y = k(s^2 - t^2),\ \ z = k(s^2 + t^2)$$

به‌دست می‌آیند. با قراردادن این مقدارها به‌جای x، y، z در $xy = r(x+y+z)$ و حل معادلهٔ حاصل نسبت به r به‌دست می آوریم

$$\begin{aligned} r &= \frac{2k^2st(s^2-t^2)}{k(2st+s^2-t^2+s^2+t^2)} \\ &= \frac{kt(s^2-t^2)}{s+t} = kt(s-t) \end{aligned}$$

که عددی صحیح است. □

با اغتنام فرصت، حکم دیگری را که مربوط به مثلثهای فیثاغورسی است عنوان می‌کنیم. متوجه هستیم که ممکن است مثلثهای فیثاغورسی متفاوتی، مساحتِ برابر داشته باشند؛ به‌عنوان نمونه، مساحت هریک از مثلثهای قائم‌الزاویهٔ متناظر با سه‌تاییهای فیثاغورسی اولیهٔ ۲۰، ۲۱، ۲۹ و ۱۲، ۳۵، ۵۷ برابر ۲۱۰ است. فرما این حکم را ثابت کرد: به‌ازای هر عدد صحیح $n > 1$، n مثلث فیثاغورسی با وترهای متفاوت و مساحتهای یکسان وجود دارد. از تفصیل مطلب صرف‌نظر می‌کنیم.

تمرینهای ۱۱ـ۱

۱. (الف) ۳ سه‌تایی فیثاغورسی متفاوت به‌صورت ۱۶، y، z، که لزوماً اولیه نباشند، پیدا کنید.

(ب) همهٔ سه‌تاییهای فیثاغورسی اولیهٔ x، y، z با $x = ۴۰$ را به‌دست آورید؛ همین کار را به‌ازای $x = ۶۰$ انجام دهید.

۲. اگر x، y، z سه‌تایی فیثاغورسی اولیه‌ای باشد، ثابت کنید $x + y$ و $x - y$ همنهشت با ۱ یا ۷ به پیمانهٔ ۸ هستند.

۳. (الف) ثابت کنید اگر $n \not\equiv ۲$ (به پیمانهٔ ۴)، مثلث فیثاغورسی اولیهٔ x، y، z ای وجود دارد که در آن x یا y برابر n است.

(ب) اگر $n \geq ۳$ دلخواه باشد، سه‌تایی فیثاغورسی (نه لزوماً اولیه) ای پیدا کنید که n یکی از عضوهایش باشد. [راهنمایی: به‌ازای n فرد، سه‌تایی n، $\frac{۱}{۲}(n^۲ - ۱)$ و $\frac{۱}{۲}(n^۲ + ۱)$ را درنظر بگیرید؛ به‌ازای n زوج، سه‌تایی n، $(n^۲/۴) - ۱$ و $(n^۲/۴) + ۱$ را درنظر بگیرید.]

۴. ثابت کنید در هر سه‌تایی فیثاغورسی اولیه x، y، z، حاصلضرب xy بر ۱۲ بخشپذیر است، بنابراین $۶۰|xyz$.

۵. نشان دهید که به‌ازای هر عدد صحیح مثبت n، حداقل n سه‌تایی فیثاغورسی با عضو نخست یکسان وجود دارد. [راهنمایی: به‌ازای $k = ۰, ۱, ۲, \ldots, n - ۱$ قرار دهید $y_k = ۲^k(۲^{۲n-۲k} - ۱)$ و $z_k = ۲^k(۲^{۲n-۲k} + ۱)$. در این‌صورت $۲^{n+۱}$، y_k، z_k همگی سه‌تایی فیثاغورسی هستند.]

۶. نشان دهید ۳، ۴، ۵ تنها سه‌تایی فیثاغورسی اولیهٔ متشکل از سه عدد صحیح مثبت متوالی است.

۷. نشان دهید $۳n$، $۴n$، $۵n$، که $n = ۱, ۲, \ldots$، تنها سه‌تاییهای فیثاغورسی هستند که عضوهایشان تشکیل تصاعد عددی می‌دهد. [راهنمایی: سه‌تایی مورد بحث را به‌صورت $x - d$، x، $x + d$ درنظر بگیرید، و x را برحسب d به‌دست آورید.]

۸. همهٔ مثلثهای فیثاغورسیی را پیدا کنید که مساحت آنها با محیطشان برابر باشد [راهنمایی: از معادله‌های $x^۲ + y^۲ = z^۲$ و $x + y + z = \frac{۱}{۲}xy$ نتیجه می‌شود که $(x - ۴)(y - ۴) = ۸$.]

۹. (الف) ثابت کنید که اگر x و z در سه‌تایی فیثاغورسی اولیهٔ x، y، z عددهای صحیح مثبت متوالی باشند، آنگاه به‌ازای $t > ۰$ ای

$$x = ۲t(t + ۱), \quad y = ۲t + ۱, \quad z = ۲t(t + ۱) + ۱$$

[راهنمایی: از معادلهٔ $۱ = z - x = s^۲ + t^۲ - ۲st$ نتیجه می‌شود $s - t = ۱$.]

(ب) ثابت کنید که اگر در سه‌تایی فیثاغورسی اولیهٔ x، y، z، $z - y = ۲$، آنگاه به‌ازای $t > ۱$ ای،

$$x = ۲t, \quad y = t^۲ - ۱, \quad z = t^۲ + ۱$$

۱۰. نشان دهید تعدادی نامتناهی سه‌تایی فیثاغورسی اولیهٔ x، y، z وجود دارد که درآنها عضو x زوج و مربع کامل است. [راهنمایی: سه‌تایی $۴n^۲$، $n^۴ - ۴$، $n^۴ + ۴$ را که در آن n عدد فرد دلخواهی است، درنظر بگیرید.]

۱۱. نشان دهید به‌ازای هر عدد صحیح مثبت n، مثلثی فیثاغورسی وجود دارد که شعاع دایرهٔ محاطی آن n است. [راهنمایی: اگر r شعاع دایرهٔ محاط در یک مثلث فیثاغورسی با ضلعهای a و b و وتر c باشد، آنگاه $r = \frac{۱}{۲}(a + b - c)$. اکنون سه‌تایی $۲n + ۱$، $۲n^۲ + ۲n$، $۲n^۲ + ۲n + ۱$ را درنظر بگیرید.]

۱۲. (الف) ثابت کنید تعداد نامتناهی سه‌تایی فیثاغورسی اولیهٔ x، y، z وجود دارد که در آنها، x و y عددهای صحیح مثبت متوالی‌اند. پنج تا از اینها را ارائه کنید. [راهنمایی: اگر x، $x + ۱$، z یک سه‌تایی فیثاغورسی تشکیل دهند، سه‌تایی $۳x + ۲z + ۱$، $۳x + ۲z + ۲$، $۴x + ۳z + ۲$ نیز سه‌تایی فیثاغورسی است.]

(ب) نشان دهید تعداد نامتناهی سه‌تایی فیثاغورسی x، y، z وجود دارد که در آنها x و y عددهای مثلثی متوالی‌اند. سه تا از اینها را ارائه دهید. [راهنمایی: اگر x، $x + ۱$، z یک سه‌تایی فیثاغورسی تشکیل دهند، $t_{۲x}$، $t_{۲x+۱}$، $z(۲x + ۱)$ نیز سه‌تایی فیثاغورسی تشکیل می‌دهند.]

۱۳. با استفاده از تمرین ۱۲ نشان دهید تعداد نامتناهی عدد مثلثی مربع کامل وجود دارد. پنج تا از چنین عددهای مثلثی را ارائه کنید. [راهنمایی: اگر x، $x + ۱$، z یک سه‌تایی فیثاغورسی باشند، با جایگزینی $u = z - x - ۱$، $v = x + (۱ - z)/۲$ نتیجه می‌شود $u(u + ۱)/۲ = v^۲$.]

۱۱ـ۲ «آخرین قضیهٔ» معروف فرما

با اطلاعاتی که دربارهٔ سه‌تاییهای فیثاغورسی کسب کرده‌ایم، اکنون آماده‌ایم به تنها حالتی از حدس فرما که خود فرما اثباتی برای آن ارائه کرد، یعنی $n = ۴$، بپردازیم. روش به‌کاررفته در این اثبات صورتی از استقراء است که گاهی «روش نزول نامتناهی فرما» نامیده می‌شود. به‌طور خلاصه، روش مزبور را می‌توان به این شرح توصیف کرد: فرض می‌شود جوابی از مسألهٔ مورد بحث برحسب عددهای صحیح مثبت موجود باشد. با استفاده از این جواب، جواب جدیدتری برحسب عددهای صحیح مثبت کوچکتر ساخته می‌شود، و این هم باز منجر به جواب کوچکتری می‌شود و الی آخر.

چون کاهش اندازهٔ عددهای صحیح مثبت نمی‌تواند نامتناهی باشد، نتیجه می‌شود فرض اولیه باید نادرست باشد، و بنابراین، جوابی موجود نیست.

به‌جای ارائهٔ اثباتی از حدس فرما به‌ازای $n = ۴$، حکمی را که اندکی قویتر ولی اثباتش آسانتر است، ثابت می‌کنیم، یعنی، امکان‌ناپذیری حل معادلهٔ $x^۴ + y^۴ = z^۲$ در مجموعهٔ عددهای صحیح مثبت.

قضیهٔ ۱۱ـ۳ (فرما). معادلهٔ دیوفانتی $x^۴ + y^۴ = z^۲$ جوابی برحسب عددهای مثبت x، y، z ندارد.

اثبات. با برهان خلف عمل می‌کنیم و فرض می‌کنیم که جواب مثبت $x_۰$، $y_۰$، $z_۰$ای برای $x^۴ + y^۴ = z^۲$ وجود دارد. همچنین اگر فرض کنیم $\gcd(x_۰, y_۰) = ۱$ خللی در کلیت مطلب پدید نمی‌آید؛ زیرا چنانچه این برابری برقرار نباشد با قراردادن $\gcd(x_۰, y_۰) = d$، $x_۰ = dx_۱$، $y_۰ = dy_۱$، $z_۰ = d^۲z_۱$، به‌دست می‌آوریم $x_۱^۴ + y_۱^۴ = z_۱^۲$ که در آن $\gcd(x_۱, y_۱) = ۱$.

با نمایش معادلهٔ مفروض $x_۰^۴ + y_۰^۴ = z_۰^۲$ به‌صورت

$$(x_۰^۲)^۲ + (y_۰^۲)^۲ = z_۰^۲$$

ملاحظه می‌کنیم که $x_۰^۲$، $y_۰^۲$، $z_۰$ در همهٔ شرطهای سه‌تایی فیثاغورسی اولیه صدق می‌کند، و بنابراین می‌توان از قضیهٔ ۱۱ـ۱ استفاده کرد. در چنین سه‌تاییهایی، یکی از عددهای صحیح $x_۰^۲$ یا $y_۰^۲$ لزوماً زوج و دیگری فرد است. با زوج اختیارکردن $x_۰^۲$ (و بنابراین $x_۰$)، عددهای صحیح متباین $s > t > ۰$ وجود دارند به‌طوری که

$$x_۰^۲ = ۲st$$

$$y_۰^۲ = s^۲ - t^۲$$

$$z_۰ = s^۲ + t^۲$$

و فقط یکی از s و t زوج است. اگر s زوج باشد، داریم

$$۱ \equiv y_۰^۲ = s^۲ - t^۲ \equiv ۰ - ۱ \equiv ۳ (\text{به‌پیمانهٔ}\ ۴)$$

که ممکن نیست. پس s باید عدد صحیح فردی باشد و درنتیجه t زوج است. قرار می‌دهیم $t = ۲r$. در این‌صورت، معادلهٔ $x_۰^۲ = ۲st$ به‌صورت $x_۰^۲ = ۴sr$ درمی‌آید که نتیجه می‌دهد

$$\left(\frac{x_۰}{۲}\right)^۲ = sr$$

ولی بنابه لم ۲، حاصلضرب دو عدد صحیح متباین [از $1 = \gcd(s,t)$ نتیجه می‌شود $1 = \gcd(s,r)$] فقط وقتی مربع کامل است که هریک از آن دو عدد مربع کامل باشد؛ پس، به‌ازای عددهای صحیح مثبت z_1 و w_1ای داریم $s = z_1^2$ و $r = w_1^2$.

دوباره قضیهٔ ۱۱ـ۱ را، ولی این بار در مورد معادلهٔ

$$t^2 + y_0^2 = s^2$$

به‌کار می‌بریم. چون $1 = \gcd(s,t)$، نتیجه می‌شود $1 = \gcd(t, y_0, s)$، یعنی t، y_0، s، سه‌تایی فیثاغورسی اولیه‌ای است. به‌ازای tی زوج، عددهای صحیح مثبت متباین $0 < v < u$ وجود دارند به‌طوری که

$$t = 2uv$$

$$y_0 = u^2 - v^2$$

$$s = u^2 + v^2$$

پس

$$uv = \frac{t}{2} = r = w_1^2$$

و این نشان می‌دهد که هر دوی u و v مربع کامل هستند (باز با استفاده از لم ۲)؛ مثلاً $u = x_1^2$ و $v = y_1^2$. اگر این مقدارها را در معادلهٔ $s = u^2 + v^2$ قرار دهیم، نتیجه می‌شود

$$z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4$$

نکتهٔ اصلی این است که، علاوه بر مثبت بودن z_1 و t، نابرابری

$$0 < z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0$$

را نیز داریم.

ماجرا از این قرار است: با شروع از یک جواب x_0، y_0، z_0 برای $x^4 + y^4 = z^2$، جواب دیگر x_1، y_1، z_1 را طوری ساخته‌ایم که $0 < z_1 < z_0$. با تکرار کل استدلال، جواب دوم نیز منجر به جواب سوم x_2، y_2، z_2 با ضابطهٔ $0 < z_2 < z_1$ می‌شود که این نیز منجر به چهارمی می‌شود. با تکرار نامتناهی این فرایند، دنبالهٔ نامتناهی نزولی زیر از عددهای صحیح مثبت تولید می‌شود:

$$z_0 > z_1 > z_2 > \cdots$$

چون تعداد عددهای صحیح مثبت کوچکتر از $z_{\circ}$ متناهی است، به تناقض می‌رسیم. نتیجه می‌گیریم $x^{4} + y^{4} = z^{2}$ در مجموعهٔ عددهای صحیح مثبت حل‌پذیر نیست. □

یک نتیجهٔ مستقیم این قضیه این چنین است.

فرع. معادلهٔ $x^{4} + y^{4} = z^{4}$ در مجموعهٔ عددهای صحیح مثبت جواب ندارد.

اثبات. اگر $x_{\circ}$، $y_{\circ}$، $z_{\circ}$ جواب مثبتی از $x^{4} + y^{4} = z^{4}$ باشد، آنگاه $x_{\circ}$، $y_{\circ}$، $z_{\circ}^{2}$ در معادلهٔ $x^{4} + y^{4} = z^{2}$ صدق می‌کند، و این با قضیه ۱۱ـ۳ سازگار نیست. □

اگر $n > 2$، n یا توانی از ۲ است یا بر عدد اول فرد p ای بخشپذیر است. در حالت نخست، به‌ازای $k \geq 1$ای داریم $n = 4k$، و می‌توان معادلهٔ فرما، $x^{n} + y^{n} = z^{n}$، را به‌صورت

$$(x^{k})^{4} + (y^{k})^{4} = (z^{k})^{4}$$

نوشت. به‌طوری که دیدیم این معادله نمی‌تواند جوابی برحسب عددهای صحیح مثبت داشته باشد. در حالت دوم، $n = pk$، و معادلهٔ فرما را می‌توان به‌صورت

$$(x^{k})^{p} + (y^{k})^{p} = (z^{k})^{p}$$

نوشت. اگر بتوان نشان داد که معادلهٔ $u^{p} + v^{p} = w^{p}$ جواب ندارد، آنگاه، از جمله جوابی به‌صورت $u = x^{k}$، $v = y^{k}$، $w = z^{k}$ نیز در کار نخواهد بود و بنابراین $x^{n} + y^{n} = z^{n}$ حلپذیر نخواهد بود. درنتیجه، حدس فرما به این صورت درمی‌آید: به‌ازای هیچ عدد اول فرد p ای معادلهٔ

$$x^{p} + y^{p} = z^{p}$$

در مجموعهٔ عددهای صحیح مثبت جواب ندارد.

گرچه این مسأله ذهن برجسته‌ترین ریاضیدانان ۳۰۰ سال اخیر را به خود مشغول داشته است، کوششهای آنها جز نتیجه‌هایی جزئی و اثباتهایی در حالتهای ویژه حاصلی نداشته است[۱]. اویلر در ۱۷۷۰ نخستین اثبات حدس فرما در حالت $p = 3$ را ارائه کرد؛ مرحله‌ای از استدلال او ناقص بود، ولی بعداً لژاندر این اثبات را تکمیل کرد. دیریکله و لژاندر در سال ۱۸۲۵، مستقل از هم، حالت $p = 5$ را با استفاده از روش نزول نامتناهی حل کردند. چند سالی بعد، در ۱۸۳۹، لامه

۱. پانوشت صفحهٔ ۲۹۹ را نگاه کنید.

حدس را به‌ازای $p = ۷$ ثابت کرد. با پیچیده‌شدن فزایندهٔ استدلالها، معلوم شد که حل موفقیت‌آمیز مسأله در حالت کلی به روشهای متفاوتی نیازمند است. به‌نظر رسید شاید بهترین شیوهٔ بررسی این حدس، تعمیم معنی «عدد صحیح» به ردهٔ وسیعتری از عددها و بررسی مسأله در این دستگاه وسیعتر باشد؛ زیرا در این صورت اطلاعی که می‌توان به‌دست آورد بیش از اطلاعی است که فقط با استفاده از عددهای صحیح معمولی به‌دست می‌آید.

کومر ریاضیدان آلمانی دستاورد مهمی در این زمینه کسب کرد. وی در ۱۸۴۳، برهانی را که گمان می‌کرد اثبات حدس فرماست به دیریکله ارائه کرد که بر پایهٔ توسیعی از عددهای صحیح مشتمل بر «عددهای جبری» استوار بود (یعنی عددهایی مختلط که در چند جمله‌ایهایی با ضریبهای گویا صدق می کنند) دیریکله که خودش وقت زیادی صرف این مسأله کرده بود، فوراً توانست اشکال استدلال را پیدا کند: کومر این موضوع را مسلم گرفته بود که عددهای جبری، مانند عددهای صحیح معمولی، تجزیهٔ یکتا دارند حال آنکه در حالت کلی چنین نیست.

ولی کومر بدون هراس از این وضعیت بغرنج به پژوهشهایش با کوششی مضاعف ادامه داد. برای تعمیم یکتایی تجزیه به عددهای جبری، به ابداع مفهوم عددهای ایده‌آل پرداخت. با الحاق این موجودات جدید به عددهای جبری، موفق شد حدس فرما را به‌ازای ردهٔ بزرگی از عددهای اول، که آنها را «عددهای اول منتظم» نامید ثابت کند (اهمیت این دستاورد از آنجا معلوم می شود که ۳۷، ۵۹، و ۶۷ تنها عددهای اول نامنتظم کوچکتر از ۱۰۰ هستند.) متأسفانه، گرچه ینسن[1] در ۱۹۱۵ نامتناهی بودن عددهای اول نامنتظم را ثابت کرد، نامتناهی بودن عددهای اول منتظم هنوز معلوم نیست. تقریباً همهٔ پیشرفتهای بعدی در زمینهٔ این مسأله در چارچوب پیشنهادی کومر صورت گرفته است.

در ۱۹۸۳، گرت فالتینگس[2] ریاضیدان ۲۹ سالهٔ آلمانی ثابت کرد که به‌ازای هر نمای $n > ۲$، معادلهٔ فرما، $x^n + y^n = z^n$، حداکثر می‌تواند تعدادی متناهی (در تقابل با تعدادی نامتناهی) جواب صحیح داشته باشد. ممکن است این نتیجه در نگاه نخست پیشرفت بزرگی به‌نظر نیاید، ولی اگر بتوان نشان داد که این تعداد متناهی جواب در هر حالت صفر است، آنگاه پروندهٔ حدس فرما برای همیشه بسته می‌شود.

در مقطع کوتاهی در ۱۹۸۸، به‌نظر رسید که آخرین گام برداشته شده است. انبوهی از گزارشهای مطبوعاتی حاکی بود که این حدس را یوئی‌شی میاوکا[3]، از دانشگاه متروپولیتن توکیو، به‌نحو مطلوبی حل کرده است. ولی بررسی دقیق اثبات فوق‌العاده پیچیدهٔ او نشان داد که اثبات دارای لغزشهایی ظریف ولی اساسی است. شکست کوشش اولیهٔ میاوکا در عالم تحقیقات ریاضی امری واقعاً

---

1. Jensen 2. Gerd Faltings 3. Yoichi Miyaoka

شگفت‌انگیز یا غیرعادی نیست. اثباتهای پیشنهادی معمولاً ماهها پیش از اعلام رسمی برای بررسی و کشف نقصهای احتمالی به‌طور خصوصی دست به‌دست می گردد. در مورد کار میائوکا، معروفیت این حدس به اینکه تعیین تکلیف آن یکی از دشوارترین کارها در نظریهٔ اعداد است موجب اعلام عمومی پیش از موقع و ناامیدی بعدی جامعهٔ ریاضی شد.

برای تکمیل بحث تاریخی اضافه می کنیم که در ۱۹۰۸ جایزه‌ای ۱۰۰۰۰۰ مارکی در اختیار آکادمی علوم گوتینگن قرارگرفت تا به نخستین اثبات کامل حدس فرما اختصاص یابد. نتیجهٔ آنی این اقدام سرازیر شدن سیلی از اثباتهای نادرست از سوی ریاضیدانهای آماتور بود. چون فقط اثباتهای منتشرشده پذیرفته می‌شد، حدس فرما به‌عنوان مسأله‌ای ریاضی که دربارهٔ آن بیشترین تعداد اثباتهای نادرست به چاپ رسیده است، شهرت دارد؛ در واقع از ۱۹۰۸ تا ۱۹۱۲ بیش از ۱۰۰۰ به‌اصطلاح اثبات ارائه شد، که اغلب به‌صورت جزوه‌هایی شخصی چاپ شده بودند. برای حسن ختام می‌گوییم همین که به دلیل تورم دههٔ ۱۹۲۰ در آلمان ارزش پولی جایزه از میان رفت، علاقه به اثبات نیز فروکش کرد.

توجه خود را از $x^4 + y^4 = z^2$ به معادله‌ای دیوفانتی که ارتباط نزدیکی با آن دارد، یعنی $x^4 - y^4 = z^2$، معطوف می‌کنیم. اثبات حل‌ناپذیری آن مشابه اثبات قضیهٔ ۱۱ـ۳ است، ولی تغییری جزئی در روش نزول نامتناهی می‌دهیم.

قضیهٔ ۱۱ـ۴ (فرما). معادلهٔ دیوفانتی $x^4 - y^4 = z^2$ جوابی برحسب عددهای صحیح مثبت x، y، z ندارد.

اثبات. اثبات با برهان خلف انجام می‌شود. فرض می‌کنیم معادله دارای جواب برحسب عددهای صحیح مثبت است و در میان جوابهایش x_0، y_0، z_0 جوابی با کوچکترین مقدار x است؛ بنابه این فرض، x_0 باید فرد باشد (چرا؟). اگر $\gcd(x_0, y_0) = d > 1$، درصورت قراردادن $x_0 = dx_1$، $y_0 = dy_1$، به‌دست می‌آوریم $d^4(x_1^4 - y_1^4) = z_0^2$، بنابراین $d^2 | z_0$ یا به‌ازای $z_1 > 0$ ای، $z_0 = d^2 z_1$. نتیجه می‌شود x_1، y_1، z_1 جوابی از معادلهٔ مورد نظر است و $0 < x_1 < x_0$، که غیرممکن است. پس می‌توانیم فرض کنیم x_0، y_0، z_0 جوابی است که در آن $\gcd(x_0, y_0) = 1$. بقیهٔ استدلال، برحسب اینکه y_0 فرد یا زوج باشد، به دو حالت تقسیم می‌شود.

نخست حالتی راکه y_0 عدد صحیح فردی است، درنظر می‌گیریم. اگر معادلهٔ $x_0^4 - y_0^4 = z_0^2$ به‌صورت $z_0^2 + (y_0^2)^2 = (x_0^2)^2$ نوشته شود، ملاحظه می‌شود که x_0^2، y_0^2، z_0 تشکیل سه‌تایی فیثاغورسی اولیه‌ای می‌دهند. بنابه قضیهٔ ۱۱ـ۱ عددهای صحیح متباین $s > t > 0$ ای وجود دارند که

$$z_0 = 2st$$

$$y_0^2 = s^2 - t^2$$
$$x_0^2 = s^2 + t^2$$

بنابراین

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2 = (x_0 y_0)^2$$

یعنی، s، t، $x_0 y_0$ جوابی (مثبت) از معادلهٔ $x^4 - y^4 = z^2$ است. چون

$$0 < s < \sqrt{s^2 + t^2} = x_0$$

به تناقض رسیده‌ایم زیرا فرض کردیم x_0 کوچکترین مقدار را دارد.

در مورد حالت دوم اثبات، فرض می‌کنیم y_0 عدد صحیح زوجی باشد. با استفاده از فرمولهای سه‌تاییهای فیثاغورسی اولیه داریم

$$y_0^2 = 2st$$
$$z_0 = s^2 - t^2$$
$$x_0^2 = s^2 + t^2$$

که در آنها می توان s را زوج و t را فرد انتخاب کرد. در این صورت، در رابطهٔ $y_0^2 = 2st$، داریم $\gcd(2s, t) = 1$. پس، بنابه لم ۲، هریک از $2s$ و t مربع عدد صحیح مثبتی است؛ مثلاً $2s = w^2$، $t = v^2$. چون w لزوماً باید عدد صحیح زوجی باشد، به فرض $w = 2u$ به‌دست می‌آوریم $s = 2u^2$. پس

$$x_0^2 = s^2 + t^2 = 4u^4 + v^4$$

و بنابراین $2u^2$، v^2، x_0 تشکیل سه‌تایی فیثاغورسی اولیه‌ای می‌دهند. دوباره با توجه به قضیهٔ ۱۱ـ۱، عددهای صحیح $a > b > 0$ ای وجود دارند که به‌ازای آنها

$$2u^2 = 2ab$$
$$v^2 = a^2 - b^2$$
$$x_0 = a^2 + b^2$$

و $\gcd(a,b) = 1$. با توجه به برابری $ab = u^2$، a و b مربع کامل هستند، مثلاً، $a = c^2$ و $b = d^2$. با دانستن این موضوع، بقیهٔ اثبات آسان است، زیرا با جایگزینی به‌دست می‌آوریم

$$v^2 = a^2 - b^2 = c^4 - d^4$$

نتیجهٔ کار، جواب جدید c، d، v ای از معادلهٔ $x^4 - y^4 = z^2$ است و مهمتر از آن، صدق این جواب در

$$0 < c = \sqrt{a} < a^2 + b^2 = x.$$

است و این خلاف فرض مربوط به x. است.

تنها نتیجهٔ این تناقضها این است که معادلهٔ $x^4 - y^4 = z^2$ نمی‌تواند در مجموعهٔ عددهای صحیح مثبت دارای جواب باشد. □

فرما در حاشیهٔ کتاب حساب دیوفانتوس خود بیان و ثابت می‌کند که: مساحت مثلث قائم‌الزاویه‌ای با ضلعهای گویا نمی‌تواند مربع عددی گویا باشد. این حکم، با حذف کسرها، به قضیه‌ای دربارهٔ مثلثهای فیثاغورسی تحویل می‌شود، یعنی:

قضیهٔ ۱۱ـ۵ مساحت مثلث فیثاغورسی هرگز نمی‌تواند مربع کامل (صحیح) باشد.

اثبات. مثلثی فیثاغورسی درنظر می‌گیریم که طول وتر آن z و طول دو ضلع دیگر آن x و y باشد، یعنی، $x^2 + y^2 = z^2$. مساحت این مثلث $(1/2)xy$ است و اگر این عدد مربع کاملی، مثلاً u^2، باشد، لازم می‌آید که $2xy = 4u^2$. با افزودن و کاستن معادلهٔ اخیر از $x^2 + y^2 = z^2$، به‌دست می‌آوریم

$$(x+y)^2 = z^2 + 4u^2 \quad \text{و} \quad (x-y)^2 = z^2 - 4u^2$$

اگر دو معادلهٔ اخیر در هم ضرب شوند، نتیجه می‌شود تفاضل دو توان چهارم، مربعی کامل است:

$$(x^2 - y^2)^2 = z^4 - 16u^4 = z^4 - (2u)^4$$

چون این مغایر با قضیهٔ ۱۱ـ۴ است، مثلثی فیثاغورسی که مساحتش مربع کامل باشد، نمی‌تواند موجود باشد. □

تعدادی مسألهٔ ساده مربوط به مثلثهای فیثاغورسی وجود دارد که هنوز حل نشده‌اند. فرع

قضیهٔ ۱۱ـ۳ را می‌توان به این صورت بیان کرد که مثلث فیثاغورسیی که همهٔ ضلعهایش مربع کامل باشند وجود ندارد. مع‌الوصف، ارائهٔ مثلثی فیثاغورسی که ضلعهایش، در صورت جمع شدن با ۱، مربع می‌شوند، دشوار نیست. به‌عنوان مثال، می‌توان مثلثهای متناظر با سه‌تاییهای $۱۳^۲ - ۱$، $۱۰^۲ - ۱$، $۱۴^۲ - ۱$ و $۲۸۷^۲ - ۱$، $۲۶۵^۲ - ۱$، $۳۲۹^۲ - ۱$ را نام برد. پرسشی بدیهی ـــ که هنوز پاسخ نیافته ـــ این است که آیا تعداد چنین مثلثهایی نامتناهی است یا نه. می‌توان مثلثی فیثاغورسی مثال زد که هر ضلع آن عددی مثلثی باشد. [منظور از عدد مثلثی، عدد صحیحی به‌صورت $t_n = n(n+۱)/۲$ است.] مثالی از چنین مثلثی، مثلث متناظر با $t_{۱۳۲}$، $t_{۱۴۳}$، $t_{۱۶۴}$ است. نامتناهی بودن تعداد این نوع مثلثهای فیثاغورسی نیز معلوم نیست.

به‌عنوان حسن‌ختام، شایان ذکر است که کوششهای به‌عمل آمده برای اثبات حدس فرما بسیار بارآور بوده است. ریاضیات جدیدی که در این رهگذر پدید آمد، مبانی نظریهٔ جبری اعداد و نیز نظریهٔ ایده‌آلها در جبر مجرد نوین را پایه‌ریزی کرد. حق این است که ارزش اینها به مراتب از خود حدس بیشتر است.

تمرینهای ۱۱ـ۲

۱. نشان دهید که معادلهٔ $x^۲ + y^۲ = z^۳$ بینهایت جواب برحسب عددهای صحیح مثبت x، y، z دارد. [راهنمایی: فرض کنید به‌ازای هر $n > ۳$، $x = n(n^۲ - ۳)$ و $y = ۳n^۲ - ۱$.]

۲. این قضیه را ثابت کنید: تنها جوابهای معادلهٔ $x^۲ + ۲y^۲ = z^۲$ برحسب عددهای صحیح نامنفی x، y، z به‌طوری که $\gcd(x, y, z) = ۱$، عبارت اند از

$$x = \pm(۲s^۲ - t^۲), \quad y = ۲st, \quad z = ۲s^۲ + t^۲$$

که در آن s و t عددهای صحیح و نامنفی‌اند. [راهنمایی: اگر u، v، w طوری انتخاب شوند که $y = ۲w$، $z + x = ۲u$ و $z - x = ۲v$، آنگاه معادله به‌صورت $۲w^۲ = uv$ در می‌آید.]

۳. ثابت کنید در سه‌تایی فیثاغورسی x، y، z، حداکثر یکی از x، y، z می‌تواند مربع کامل باشد.

۴. هر یک از حکمهای زیر را ثابت کنید:

(الف) دستگاه معادله‌های

$$x^۲ + y^۲ = z^۲ - ۱ \qquad \text{و} \qquad x^۲ - y^۲ = w^۲ - ۱$$

دارای تعداد نامتناهی جواب برحسب عددهای صحیح مثبت x، y، z، w است [راهنمایی: به‌ازای عدد صحیح دلخواه $n \geq ۱$، قرار دهید $x = ۲n^۲$ و $y = ۲n$.]

(ب) دستگاه معادله‌های

$$x^۲ - y^۲ = w^۲ \quad \text{و} \quad x^۲ + y^۲ = z^۲$$

جوابی برحسب عددهای صحیح مثبت x، y، z، w ندارد.

(پ) دستگاه معادله‌های

$$x^۲ - y^۲ = w^۲ + ۱ \quad \text{و} \quad x^۲ + y^۲ = z^۲ + ۱$$

تعداد نامتناهی جواب برحسب عددهای صحیح مثبت x، y، z، w دارد. [راهنمایی: به‌ازای عدد صحیح دلخواه $n \geq ۱$، قرار دهید $x = ۸n^۴ + ۱$ و $y = ۸n^۳$.]

۵. با استفاده از تمرین ۴ نشان دهید که دستگاه معادله‌های

$$x^۲ + ۲y^۲ = w^۲ \quad \text{و} \quad x^۲ + y^۲ = z^۲$$

جوابی برحسب عددهای صحیح مثبت ندارد. [راهنمایی: هر جواب دستگاه داده‌شده در $z^۲ + y^۲ = w^۲$ و $z^۲ - y^۲ = x^۲$ نیز صدق می کند.]

۶. نشان دهید دستگاه معادله‌های

$$x^۲ + z^۲ = w^۲ \quad \text{و} \quad x^۲ + y^۲ = z^۲$$

جوابی برحسب عددهای صحیح مثبت ندارد، پس مثلثی فیثاغورسی که وتر و یکی از ضلعهایش دو ضلع زاویهٔ قائمه مثلث فیثاغورسی دیگری باشد، وجود ندارد. [راهنمایی: هر جواب دستگاه داده‌شده در $x^۲ + (wy)^۲ = z^۴$ نیز صدق می‌کند.]

۷. ثابت کنید معادلهٔ $x^۴ - y^۴ = ۲z^۲$ جوابی برحسب عددهای صحیح مثبت x، y، z ندارد. [راهنمایی: چون x و y باید یا هر دو فرد و یا هر دو زوج باشند، به‌ازای a، b، c ای $x^۲ + y^۲ = ۲a^۲$، $x + y = ۲b^۲$، $x - y = ۲c^۲$؛ پس، $a^۲ = b^۴ + c^۴$.]

۸. نشان دهید که $x = y = z = ۱$ تنها جواب معادلهٔ $x^۴ + y^۴ = ۲z^۲$ برحسب عددهای صحیح مثبت متباین است. [راهنمایی: هر جواب معادلهٔ داده‌شده در معادلهٔ

$$z^۴ - (xy)^۴ = \left(\frac{x^۴ - y^۴}{۲}\right)^۲$$

نیز صدق می‌کند.]

۹. ثابت کنید که معادلهٔ دیوفانتی $x^۴ - ۴y^۴ = z^۲$ جوابی برحسب عددهای صحیح مثبت x، y، z ندارد. [راهنمایی: معادلهٔ داده شده را به‌صورت $(x^۲)^۲ = z^۲ + (۲y^۲)^۲$ بنویسید و از قضیهٔ ۱۱ـ۱ استفاده کنید.]

۱۰. با استفاده از تمرین ۹ ثابت کنید مثلثی فیثاغورسی که مساحت آن دو برابر یک عدد مربع کامل باشد، وجود ندارد. [راهنمایی: فرض کنید بر خلاف آن داشته باشیم $x^۲ + y^۲ = z^۲$ و $\frac{۱}{۲}xy = ۲w^۲$. در این صورت $(x+y)^۲ = z^۲ + ۸w^۲$ و $(x-y)^۲ = z^۲ - ۸w^۲$. نتیجه می‌شود $z^۴ - ۴(۲w)^۴ = (x^۲ - y^۲)^۲$.]

۱۱. این قضیه را ثابت کنید: تنها جوابهای معادلهٔ

$$\frac{۱}{x^۲} + \frac{۱}{y^۲} = \frac{۱}{z^۲}, \qquad \gcd(x, y, z) = ۱$$

برحسب عددهای صحیح مثبت به‌صورت

$$x = ۲st(s^۲ + t^۲), \quad y = s^۴ - t^۴, \quad z = ۲st(s^۲ - t^۲)$$

است که در آن s و t عددهای صحیح مثبت متباین، $s > t$، و یکی از s و t زوج است.

۱۲. نشان دهید که معادلهٔ $۱/x^۴ + ۱/y^۴ = ۱/z^۲$ جوابی برحسب عددهای صحیح مثبت ندارد.

۱۲

نمایش عددهای صحیح به‌صورت مجموع چند مربع

«هدف فیزیک نظری کشف قانونهای جهانِ قابل فهم است؛ هدف ریاضیات محض کشف قانونهای فهم بشر است.»

جِی. جِی. سیلوستر

۱۲ـ۱ ژوزف لویی لاگرانژ

در طی متجاوز از یک سده بعد از درگذشت دکارت، پاسکال، و فرما، ریاضیدانی همتراز با آنها در فرانسه ظهور نکرد. در این فاصله، در انگلستان نخست نیوتن و سپس تیلر، استرلینگ، و مکلورن با شور و اشتیاقی هر چه تمامتر به پیشبرد ریاضیات پرداختند. در آلمان لایب نیتس ستارهٔ صحنه بود. مشخصهٔ فعالیت ریاضی در سوئیس نیز کارهای برنولیها و اویلر بود. با ظهور لاگرانژ، لاپلاس و لژاندر در اواخر سدهٔ هجدهم. که شکوهی تازه به ریاضیات فرانسه بخشیدند، پاریس دوباره مرکز مطالعات ریاضی شد.

ژوزف لویی لاگرانژ (۱۷۳۶ ـ ۱۸۱۳) که در ایتالیا متولد شد، سالها در آلمان به‌سر برد، و بالاخره به

تابعیّت فرانسه درآمد، بعد از اویلر پرآوازه‌ترین ریاضیدان سدهٔ هجدهم است. وقتی وارد دانشگاه تورین شد، بیشتر به فیزیک علاقه داشت، ولی، همین که امکان مطالعهٔ رساله‌ای از هالی دربارهٔ فایده‌های حساب دیفرانسیل و انتگرال نیوتنی را به‌دست آورد، فریفتهٔ ریاضیات جدیدی شد که در حال دگرگون ساختنِ مکانیک سماوی بود. با چنان جدّیتی به مطالعهٔ ریاضیات پرداخت که در هجده‌سالگی به استادی هندسه در مدرسهٔ توپخانهٔ سلطنتی در تورین منصوب شد. بعد از مدت کوتاهی، آکادمی علوم فرانسه لاگرانژ را در فهرست نامزدهای جایزه‌های دوسالانهٔ خود قرار داد: از ۱۷۶۴ تا ۱۷۸۸، پنج بار جایزه‌های پرطرفدار آکادمی را به خاطر کاربرد ریاضیات در مسأله‌های نجومی برد.

در ۱۷۶۶، وقتی اویلر برلین را به سوی سن‌پترزبورگ ترک کرد، فردریک کبیر پادشاه پروس با ارسال پیامی متواضعانه لاگرانژ را برای تصدّیِ کرسی خالی شده دعوت کرد. در این پیام آمده بود: لازم است بزرگترین هندسه‌دان اروپا درکنار بزرگترین پادشاه اروپا زندگی کند. (شاه به دالامبر، که لاگرانژ را به این منظور پیشنهاد کرده بود، نوشت: «به خاطر دلسوزی و توصیه‌تان، که باعث شد ریاضیدانی با دو چشم جانشین ریاضیدانی نیمه‌کور شود، و به ویژه عضوهای «کالبداندیش» آکادمی را خشنود خواهد کرد، نسبت به شما احساس دین می‌کنم.») لاگرانژ بیست سال بعد را در سمت مدیر بخش ریاضی آکادمی برلین خدمت کرد و به تولید آثار بسیار ممتازی پرداخت که نقطهٔ اوج آنها رسالهٔ جاودانه‌اش، مکانیک تحلیلی[1] بود (که در ۱۷۸۸ در چهار جلد به چاپ رسید) در این اثر مکانیک عمومی را یکپارچه کرد و از آن، همان‌طور که همیلتنِ ریاضیدان بعدها گفت، «نوعی نظم علمی» پدید آورد. لاگرانژ با این اعتقاد که مکانیک واقعاً شاخه‌ای از ریاضیات محض است، طوری مفهومهای هندسی را از مکانیک تحلیلی کنارگذاشت که توانست در مقدمه کتاب با افتخار بنویسد که حتی یک نمودار در صفحه‌های کتاب دیده نمی‌شود.

فردریک در ۱۷۸۷ وفات یافت، و لاگرانژ که دیگر جو دربار پروس را موافق خود نمی‌دید، تصمیم گرفت دعوت لویی شانزدهم را برای اقامت در پاریس بپذیرد. در این مقطع بود که به تابعیّت فرانسه درآمد. اما سالها فعالیت مداوم او را خسته کرده بود؛ وی دچار افسردگی عمیقی شد به‌طوری که علاقه‌اش به ریاضیات از میان رفت. به اندازه‌ای از این موضوع متنفر شد که نخستین نسخهٔ چاپی مکانیک تحلیلی‌اش ـــ که حاصل ربع قرن تلاش او بود ـــ متجاوز از دو سال بی آنکه آن را بررسی کند روی میزش قرار داشت. با کمال شگفتی، ناآرامیهای انقلابِ فرانسه بود که وی را از حالت رخوت به‌در آورد. به دنبال تعطیل شدن همهٔ دانشگاههای قدیمی فرانسه (آکادمی علوم نیز برچیده شد) در ۱۷۹۳، انقلابیون دو مدرسهٔ جدید، با عنوانهای فروتنانهٔ اکول نرمال [=مدرسهٔ معمولی] و اکول پلی‌تکنیک [=دارالفنون] تأسیس کردند، و لاگرانژ برای تدریس آنالیز دعوت شد.

1. Mécanique Analytique

او گرچه از روزهای نخست ورودش به تورین تدریس نکرده، و همهٔ این مدت را تحت حمایت دربار زیسته بود، ظاهراً از این انتصاب استقبال کرده است. مدرسان، طبق قرار و تحت نظارت مداوم، متعهّد بودند «چیزی از حافظه نقل نکنند»، و جزوه‌های درسی آنها توسط مسؤلین بازبینی می‌شدند. علی‌رغم مشکلاتی جزئی که برایش ایجاد می‌کردند، لاگرانژ به‌عنوان معلمی الهامبخش معروف شد. جزوه‌های درسی او در حساب دیفرانسیل مبنای اثر کلاسیک دیگری با عنوان «نظریهٔ تابعهای تحلیلی»[1] قرار گرفت.

گرچه پژوهشهای لاگرانژ طیف فوق‌العاده وسیعی از موضوعات را در بر می‌گرفت، وی همچون دیوفانتوس و فرما درگذشته، استعداد ویژه‌ای در نظریهٔ اعداد داشت. اهّم فعالیتهای او در این زمینه عبارت است از: نخستین اثبات برای قضیهٔ ویلسن که حاکی است اگر n عددی اول باشد، آنگاه $(n-۱)! \equiv -۱$ (به پیمانهٔ n)؛ بررسی شرطهایی که تحت آنها ±۲ و ±۵ مانده‌های درجهٔ دوم یا نامانده‌های درجهٔ دوم عدد اول فردی باشند (اویلر دربارهٔ -۱ و ±۳ بحث کرده است.) تعیین همهٔ جوابهای صحیح معادلهٔ $x^۲ - ay^۲ = ۱$؛ و حلّ تعدادی از مسأله‌های طرح شده توسط فرما در ارتباط با نمایشپذیری بعضی عددهای اول به صورتهایی خاص (مثلاً، حکمی به این مضمون که هر عدد اول $p \equiv ۳$ (به پیمانهٔ ۸) به‌صورت $p = a^۲ + ۲b^۲$ است). گفتار حاضر معطوف به کشفی است که بیشتر معروفیّت لاگرانژ در نظریهٔ اعداد ناشی از آن است، یعنی اثبات اینکه هر عدد صحیح مثبت را می‌توان به‌صورت مجموع چهار مربع کامل نوشت.

۱۲ـ۲ مجموعهای دو مربع

از نظر تاریخی، نمایش عددها به‌صورت مجموع چند عدد مربع کامل یکی از مسأله‌هایی است که مورد توجه بسیار بوده است. در این فصل با تمهیدات کافی این پرسش را به‌طور کامل پاسخ می‌دهیم: کوچکترین مقدار n به طوری که هر عدد صحیح مثبت را بتوان به‌صورت مجموع حداکثر n مربع نوشت، چیست؟ با بررسی چند عدد صحیح مثبت نخست معلوم می‌شود که

$$
\begin{aligned}
۱ &= ۱^۲\\
۲ &= ۱^۲ + ۱^۲\\
۳ &= ۱^۲ + ۱^۲ + ۱^۲\\
۴ &= ۲^۲\\
۵ &= ۲^۲ + ۱^۲
\end{aligned}
$$

1. Théorie des Fonctions Analytique

$$۶ = ۲^۲ + ۱^۲ + ۱^۲$$
$$۷ = ۲^۲ + ۱^۲ + ۱^۲ + ۱^۲$$

چون برای نمایش ۷ به چهار مربع نیاز است، پاسخی ناقص به پرسش ما این است که $n \geq ۴$. نیازی به گفتن نیست که ممکن است عددهای صحیحی به بیش از چهار مربع نیازمند باشند. قضیه‌ای از لاگرانژ که به حق قضیهٔ معروفی است و در ۱۷۷۰ ثابت شد، می‌گوید که چهار مربع کافی است؛ یعنی، هر عدد صحیح مثبت را می‌توان به‌صورت مجموع چهار مربع صحیح، که برخی ممکن است $۰^۲ = ۰$ باشند، نوشت. این صورت قضیهٔ ۱۲ـ۷ ماست.

برای اینکه بحث را با مطالب ساده‌تری شروع کنیم، نخست شرطهای لازم و کافی را برای نمایشپذیری عدد صحیح مثبت به‌صورت مجموع دو مربع تعیین می‌کنیم. بنابه لم زیر، مسأله را می‌توان به بررسی عددهای اول تحویل کرد.

لم. اگر هر یک از m و n مجموع دو مربع باشد، آنگاه حاصلضربشان mn نیز مجموع دو مربع است.

اثبات. اگر به‌ازای عددهای صحیح a، b، c، d ای، $m = a^۲ + b^۲$ و $n = c^۲ + d^۲$، آنگاه

$$mn = (a^۲ + b^۲)(c^۲ + d^۲) = (ac + bd)^۲ + (ad - bc)^۲ \qquad \square$$

بدیهی است هر عدد اولی را نمی‌توان به‌صورت مجموع دو مربع نوشت؛ به‌عنوان نمونه، عددهای صحیح a و b ای وجود ندارند که در $۳ = a^۲ + b^۲$ صدق کنند. به‌طور کلیتر، می‌توان ثابت کرد:

قضیهٔ ۱۲ـ۱ عدد اول p ای به‌صورت $۴k + ۳$، مجموع دو مربع نیست.

اثبات. به‌ازای هر عدد صحیح a به پیمانهٔ ۴ داریم $a \equiv ۰, ۱, ۲, ۳$؛ پس، $a^۲ \equiv ۰$ (به پیمانهٔ ۴) یا $a^۲ \equiv ۱$ (به پیمانهٔ ۴). نتیجه می‌شود که، به‌ازای عددهای صحیح دلخواه a و b

$$a^۲ + b^۲ \equiv ۰, ۱ \text{ یا } ۲ \pmod{۴}$$

چون $p \equiv ۳$ (به پیمانهٔ ۴)، معادله $p = a^۲ + b^۲$ ممتنع است. $\square$

از سوی دیگر، هر عدد اول همنهشت با ۱ به پیمانهٔ ۴ به‌صورت مجموع دو مربع قابل نمایش است. در اثباتی که ما ارائه خواهیم کرد، از قضیه‌ای در بارهٔ همنهشتیها متعلق به آکسل تو[1] ریاضیدان نروژی استفاده می‌شود. این قضیه نیز به «اصل لانهٔ کبوتر» معروف دیریکله متکی است.

1. Axel Thue

اصل لانهٔ کبوتر. اگر n شیٔ در m جعبه (یا لانهٔ کبوتر) قرار داده شوند و اگر $n > m$، آنگاه جعبه‌ای حاوی لااقل دو شیٔ خواهد بود.

به بیان ریاضیتر، این اصل ساده حاکی است که اگر مجموعه‌ای n عضوی اجتماع m زیرمجموعهٔ خودش باشد و اگر $n > m$، آنگاه یکی از این زیرمجموعه‌ها حداقل دو عضو دارد.

لم (تو). فرض می‌کنیم p عددی اول باشد و $\gcd(a,p) = ۱$. در این‌صورت همنهشتی

$$ax \equiv y \pmod{p} \quad (\text{به پیمانهٔ } p)$$

دارای جواب $x_\circ$، $y_\circ$ ای است به‌طوری که

$$\circ < |x_\circ| < \sqrt{p} \quad \text{و} \quad \circ < |y_\circ| < \sqrt{p}$$

اثبات. فرض می‌کنیم $k = [\sqrt{p}] + ۱$ و مجموعهٔ عددهای صحیح زیر

$$S = \{ax - y | \circ \leq x \leq k - ۱, \circ \leq y \leq k - ۱\}$$

را درنظر می‌گیریم. چون $k^۲ > p$، $ax - y$ مقدار ممکن دارد، اصل لانهٔ کبوتر تضمین می‌کند که حداقل دو عضو S باید به پیمانهٔ p همنهشت باشند؛ اینها را $ax_۱ - y_۱$ و $ax_۲ - y_۲$ می‌نامیم که در آنها $x_۱ \neq x_۲$ یا $y_۱ \neq y_۲$. در این‌صورت می‌توانیم بنویسیم

$$a(x_۱ - x_۲) \equiv y_۱ - y_۲ \quad (\text{به پیمانهٔ } p)$$

با قرار دادن $x_\circ = x_۱ - x_۲$ و $y_\circ = y_۱ - y_۲$، نتیجه می‌شود $x_\circ$، $y_\circ$ جوابی از همنهشتی $ax \equiv y$ (به پیمانهٔ p) است. اگر $x_\circ$ یا $y_\circ$ برابر صفر باشد، با استفاده از $\gcd(a,p) = ۱$ می‌توان نشان داد که دیگری نیز باید صفر باشد، که مغایر با فرض است. پس $\circ < |x_\circ| \leq k - ۱ < \sqrt{p}$ و $\circ < |y_\circ| \leq k - ۱ < \sqrt{p}$. □

اکنون آماده‌ایم یکی از قضیه‌های فرما را استنتاج کنیم که حاکی است هر عدد اول به‌صورت $۴k + ۱$ را می‌توان به‌صورت مجموع مربعهای دو عدد صحیح نوشت. (از لحاظ تقدم، ژیرار چند سال زودتر به این قضیه پی برد و بنابراین گاهی آن را قضیهٔ ژیرار می‌نامند.) فرما این قضیه را طی نامه‌ای، به تاریخ ۲۵ دسامبر ۱۶۴۰، به مرسن اطلاع داد و ادعا کرد که برای آن اثباتی قطعی یافته است. مع‌الوصف، اویلر نخستین کسی بود که، در ۱۷۵۴، اثباتی از قضیه را منتشر کرد و به‌علاوه موفق شد نشان دهد که نمایش مزبور یکتاست.

قضیهٔ ۱۲ـ۲ (فرما). عدد اول فرد p قابل نمایش به‌صورت مجموع دو مربع است اگر و تنها اگر $p \equiv ۱$ (به پیمانهٔ ۴).

اثبات. گرچه قسمت «تنها اگر» در قضیهٔ ۱۲ـ۱ مستتر است، در اینجا اثبات دیگری برای آن می‌آوریم. فرض می‌کنیم p را بتوان به‌صورت مجموع دو مربع نوشت، مثلاً $p = a^۲ + b^۲$. چون p عددی اول است، داریم $p \nmid a$، و $p \nmid b$. (اگر $p|a$، آنگاه $p|b^۲$ و بنابراین $p|b$، که منجر به تناقض $p^۲|p$ می‌شود.) بنابراین، بنابه نظریهٔ همنهشتیهای خطی، عدد صحیح c ای وجود دارد به‌طوری‌که $bc \equiv ۱$ (به پیمانهٔ p). پس با توجه به رابطهٔ $(ac)^۲ + (bc)^۲ = pc^۲$ داریم

$$(ac)^۲ \equiv -۱ \quad (\text{به پیمانهٔ } p)$$

که نشان می‌دهد ۱− ماندهٔ درجه دومی از p است. اکنون فرع قضیهٔ ۹ـ۲ به کمک ما می‌آید زیرا $(-۱/p) = ۱$ فقط وقتی که $p \equiv ۱$ (به پیمانهٔ ۴).

برعکس، فرض می‌کنیم $p \equiv ۱$ (به پیمانهٔ ۴). چون ۱− ماندهٔ درجهٔ دومی از p است، می‌توانیم عدد صحیح a را طوری پیدا کنیم که $a^۲ \equiv -۱$ (به پیمانهٔ p)؛ در واقع، بنابه قضیهٔ ۵ـ۳، $a = [(p-۱)/۲]!$ یک چنین عدد صحیحی است. ولی $\gcd(a, p) = ۱$، پس بنابه لم تو، همنهشتی

$$ax \equiv y \quad (\text{به پیمانهٔ } p)$$

دارای جواب $x_\circ$ و $y_\circ$ ای است به‌طوری‌که $\circ < |x_\circ| < \sqrt{p}$، $\circ < |y_\circ| < \sqrt{p}$. پس،

$$-x_\circ^۲ \equiv a^۲x_\circ^۲ \equiv (ax_\circ)^۲ \equiv y_\circ^۲ \quad (\text{به پیمانهٔ } p)$$

یا $x_\circ^۲ + y_\circ^۲ \equiv \circ$ (به پیمانهٔ p). از اینجا نتیجه می‌شود که به‌ازای عدد صحیح k ای ناکمتر از ۱ داریم

$$x_\circ^۲ + y_\circ^۲ = kp$$

چون $\circ < |x_\circ| < \sqrt{p}$ و $\circ < |y_\circ| < \sqrt{p}$، به‌دست می‌آوریم $\circ < x_\circ^۲ + y_\circ^۲ < ۲p$، که نتیجه می‌دهد $k = ۱$. پس، $x_\circ^۲ + y_\circ^۲ = p$، و اثبات کامل است. □

اگر $a^۲$ و $(-a)^۲$ را یکی بگیریم، حکم زیر را داریم.

فرع. هر عدد اول p به‌صورت $۴k + ۱$ را می‌توان به گونه‌ای یکتا (صرف‌نظر از ترتیب عاملهای مجموع) به‌صورت مجموع دو مربع نوشت.

اثبات. برای اثبات یکتایی، فرض می‌کنیم به‌ازای عددهای صحیح مثبت a، b، c، و d ای

$$p = a^۲ + b^۲ = c^۲ + d^۲$$

در این صورت

$$a^۲d^۲ - b^۲c^۲ = p(d^۲ - b^۲) \equiv ۰ \quad (\text{به پیمانهٔ } p)$$

و بنابراین $ad \equiv bc$ (به پیمانهٔ p) یا $ad \equiv -bc$ (به پیمانهٔ p). چون a، b، c، d همگی کوچکتر از $\sqrt{p}$اند، از این رابطه‌ها نتیجه می‌شود

$$ad - bc = ۰ \qquad \text{یا} \qquad ad + bc = p$$

اگر $ad + bc = p$، به‌دست می‌آوریم $ac = bd$ زیرا

$$\begin{aligned} p^۲ = (a^۲ + b^۲)(c^۲ + d^۲) &= (ad + bc)^۲ + (ac - bd)^۲ \\ &= p^۲ + (ac - bd)^۲ \end{aligned}$$

و بنابراین $ac - bd = ۰$.نتیجه می‌گیریم که

$$ad = bc \qquad \text{یا} \qquad ac = bd$$

فرض می‌کنیم مثلاً $ad = bc$. در این‌صورت $a|bc$، که چون $\gcd(a, b) = ۱$، نتیجهٔ می‌شود $a|c$؛ حال فرض می‌کنیم مثلاً $c = ka$، در این صورت رابطهٔ $ad = bc = b(ka)$ به‌صورت $d = bk$ ساده می‌شود. ولی با توجه به

$$p = c^۲ + d^۲ = k^۲(a^۲ + b^۲)$$

معلوم می‌شود $k = ۱$. در این حالت، به‌دست می‌آوریم $a = c$ و $b = d$. با استدلالی مشابه، شرط $ac = bd$ منجر به $a = d$ و $b = c$ می‌شود. نکتهٔ مهم این است که، در هر دو حالت

$$a^۲ + b^۲ = c^۲ + d^۲$$

و حکم ثابت می‌شود. □

مرحله‌های اثبات قضیهٔ ۱۲ـ۲ را به‌ازای عدد اول $p = ۱۳$ تعقیب می‌کنیم. عدد صحیح a را می‌توان برابر با $۷۲۰ = !۶$ انتخاب کرد. جوابی از همنهشتی (به پیمانهٔ ۱۳) $۷۲۰x \equiv y$، یا هم‌ارز با آن

$$۵x \equiv y \quad (\text{به پیمانهٔ } ۱۳)$$

با بررسی مجموعهٔ

$$S = \{۵x - y | ۰ \leq x, y < ۴\}$$

به‌دست می‌آید. عنصرهای S دقیقاً عبارت‌اند از

۰	۵	۱۰	۱۵
۱-	۴	۹	۱۴
۲-	۳	۸	۱۳
۳-	۲	۷	۱۲

که به پیمانهٔ ۱۳، به‌صورت

۰	۵	۱۰	۲
۱۲	۴	۹	۱
۱۱	۳	۸	۰
۱۰	۲	۷	۱۲

ساده می‌شوند. در میان امکانات مختلف، داریم

$$۵ \times ۱ - ۳ \equiv ۲ \equiv ۵ \times ۳ - ۰ \quad (\text{به پیمانهٔ } ۱۳)$$

یا

$$۵(۱ - ۳) \equiv ۳ \quad (\text{به پیمانهٔ } ۱۳)$$

بنابراین، با فرض $x_۰ = -۲$ و $y_۰ = ۳$ به‌دست می‌آوریم

$$۱۳ = x_۰^۲ + y_۰^۲ = ۲^۲ + ۳^۲$$

یادداشت: برخی از نویسندگان ادعا می‌کنند که هر عدد اول (به پیمانهٔ ۴) $p \equiv ۱$ را می‌توان به هشت روش به‌صورت مجموع دو مربع نوشت. مثلاً، به‌ازای $p = ۱۳$ داریم

$$\begin{aligned} ۱۳ &= ۲^۲ + ۳^۲ = ۲^۲ + (-۳)^۲ = (-۲)^۲ + ۳^۲ = (-۲)^۲ + (-۳)^۲ \\ &= ۳^۲ + ۲^۲ = ۳^۲ + (-۲)^۲ = (-۳)^۲ + ۲^۲ = (-۳)^۲ + (-۲)^۲ \end{aligned}$$

چون همهٔ این هشت نمایش را می‌توان از هر یک از آنها با تعویض علامتهای ۲ و ۳ یا با جابه‌جایی عاملهای جمع به‌دست آورد، «درواقع» فقط به یک روش می‌توان این کار را انجام داد. بنابراین، از دیدگاه ما، ۱۳ را فقط به یک روش می‌توان به‌صورت مجموع دو مربع نوشت.

نشان داده‌ایم که هر عدد اول p به‌صورت (به پیمانهٔ ۴) ۱ $\equiv p$ را می‌توان به‌صورت مجموع دو مربع نوشت. ولی عددهای صحیح دیگری نیز این ویژگی را دارند، به‌عنوان نمونه

$$۱۰ = ۱^۲ + ۳^۲$$

مرحلهٔ بعدیِ برنامهٔ ما تعیین ویژگی عددهای صحیح مثبتی است که قابل نمایش به‌صورت مجموع دو مربع هستند.

قضیهٔ ۱۲ـ۳ فرض می‌کنیم عدد صحیح مثبت n به‌صورت $n = N^۲m$، که m خالی از مربع است، نوشته شده باشد. در این صورت n را می‌توان به‌صورت مجموع دو مربع نوشت اگر و تنها اگر m دارای عامل اولی به‌صورت $۴k + ۳$ نباشد.

اثبات. برای شروع، فرض می‌کنیم m دارای عامل اولی به‌صورت $۴k + ۳$ نباشد. اگر $m = ۱$، آنگاه $n = N^۲ + ۰^۲$ و کار تمام است. در حالت $m > ۱$، فرض می‌کنیم $m = p_۱p_۲\ldots p_r$ تجزیهٔ m به حاصلضرب تعدادی عدد اول متمایز باشد. هریک از این عددهای اول p_i را که برابر با ۲ یا به‌صورت $۴k + ۱$ است، می‌توان به‌صورت مجموع دو مربع نوشت. اکنون اتحاد

$$(a^۲ + b^۲)(c^۲ + d^۲) = (ac + bd)^۲ + (ad - bc)^۲$$

نشان می‌دهد که حاصلضرب دو (و، به استقرا، هر تعداد متناهی) عدد صحیح قابل نمایش به‌صورت مجموع دو مربع، خودش قابل نمایش به‌صورت مجموع دو مربع است. بنابراین عددهای صحیح x و yای وجود دارند به‌طوری‌که $m = x^۲ + y^۲$. بنابراین

$$n = N^۲m = N^۲(x^۲ + y^۲) = (Nx)^۲ + (Ny)^۲$$

که مجموع دو مربع است.

برعکس، فرض می‌کنیم n را بتوان به‌صورت مجموع دو مربع نوشت:

$$n = a^۲ + b^۲ = N^۲m$$

و p مقسوم‌علیه اول فردی از m باشد (بی آنکه خللی به کلیت مطلب وارد شود، می‌توان فرض کرد $m > ۱$). اگر $\gcd(a, b) = d$، آنگاه $a = rd$، $b = sd$، که در آن $\gcd(r, s) = ۱$. داریم

$$d^۲(r^۲ + s^۲) = N^۲m$$

و بنابراین، چون m خالی از مربع است، $d^۲|N^۲$. ولی در این صورت به‌ازای عدد صحیح t ای داریم

$$r^۲ + s^۲ = (\frac{N^۲}{d^۲})m = tp$$

و از این‌رو

$$r^۲ + s^۲ \equiv ۰ \quad (\text{به پیمانهٔ } p)$$

اکنون از شرط $\gcd(r, s) = ۱$ نتیجه می‌شود که یکی از r یا s، مثلاً r، با p متباین است. فرض می‌کنیم r' در همنهشتی

$$rr' \equiv ۱ \quad (\text{به پیمانهٔ } p)$$

صدق می‌کند. اگر معادلهٔ $r^۲ + s^۲ \equiv ۰$ (به پیمانهٔ p) در $(r')^۲$ ضرب شود، به‌دست می‌آوریم

$$(sr')^۲ + ۱ \equiv ۰ \quad (\text{به پیمانهٔ } p)$$

یا، به عبارت دیگر، $(-۱/p) = ۱$. چون -۱ ماندهٔ درجه دومی از p است، قضیهٔ ۹ـ۳ تضمین می‌کند که $p \equiv ۱$ (به پیمانهٔ ۴). نتیجهٔ استدلال ما این است که m دارای عامل اولی به‌صورت $۴k + ۳$ نیست. □

از تحلیل فوق می‌توان نتیجهٔ زیر را گرفت.

فرع. عدد صحیح مثبت n به‌صورت مجموع دو مربع قابل نمایش است اگر و تنها اگر نمای هر عامل اول به‌صورتِ $۴k + ۳$ آن زوج باشد.

مثال ۱۲ـ۱

عدد ۴۵۹ را نمی‌توان به‌صورت مجموع دو مربع نوشت زیرا $۴۵۹ = ۳^۳ \times ۱۷$ و نمای عدد اول ۳ فرد است. ولی $۱۵۳ = ۳^۲ \times ۱۷$ را می‌توان به‌صورت

$$۱۵۳ = ۳^۲(۴^۲ + ۱^۲) = ۱۲^۲ + ۳^۲$$

نمایش داد. مثال $n = ۵ \times ۷^۲ \times ۱۳ \times ۱۷$ تا اندازه‌ای پیچیده‌تر است. در این حالت داریم

$$n = ۷^۲ \times ۵ \times ۱۳ \times ۱۷ = ۷^۲(۲^۲ + ۱^۲)(۳^۲ + ۲^۲)(۴^۲ + ۱^۲)$$

با دوبار استفاده از اتحاد مذکور در قضیهٔ ۱۲ـ۳ نتیجه می‌شود

$$(۳^۲ + ۲^۲)(۴^۲ + ۱^۲) = (۱۲ + ۲)^۲ + (۳ - ۸)^۲ = ۱۴^۲ + ۵^۲$$

و

$$(۲^۲ + ۱^۲)(۱۴^۲ + ۵^۲) = (۲۸ + ۵)^۲ + (۱۰ - ۱۴)^۲ = ۳۳^۲ + ۴^۲$$

با تلفیق اینها به‌دست می‌آوریم

$$n = ۷^۲(۳۳^۲ + ۴^۲) = ۲۳۱^۲ + ۲۸^۲ \qquad \blacksquare$$

عددهای صحیح مثبت خاصی وجود دارند (البته عددهای اول به‌صورت $۴k + ۱$ از اینها نیستند) که به بیش از یک روش قابل نمایش به‌صورت مجموع دو مربع‌اند. کوچکترین اینها عبارت است از

$$۲۵ = ۴^۲ + ۳^۲ = ۵^۲ + ۰^۲$$

اگر $a \equiv b$ (به پیمانهٔ ۲)، با استفاده از رابطهٔ

$$ac = \left(\frac{a+b}{۲}\right)^۲ - \left(\frac{a-b}{۲}\right)^۲$$

می‌توان مثالهای متنوعی از این نوع ساخت: برای نمونه فرض می‌کنیم $n = ۱۵۳$؛ داریم

$$۱۵۳ = ۱۷ \times ۹ = \left(\frac{۱۷+۹}{۲}\right)^۲ - \left(\frac{۱۷-۹}{۲}\right)^۲ = ۱۳^۲ - ۴^۲$$

و

$$۱۵۳ = ۵۱ \times ۳ = \left(\frac{۵۱+۳}{۲}\right)^۲ - \left(\frac{۵۱-۳}{۲}\right)^۲ = ۲۷^۲ - ۲۴^۲$$

بنابراین

$$۱۳^۲ - ۴^۲ = ۲۷^۲ - ۲۴^۲$$

به این ترتیب دو نمایش متمایز

$$۲۷^۲ + ۴^۲ = ۲۴^۲ + ۱۳^۲ = ۷۴۵$$

به‌دست می‌آید.

در این مرحله، پرسشی طبیعی مطرح می‌شود: چه عددهای صحیح مثبتی را می‌توان به‌صورت تفاضل دو مربع نمایش داد؟ این پرسش را در زیر پاسخ می‌دهیم.

قضیهٔ ۱۲ـ۴ عدد صحیح مثبت n را می‌توان به‌صورت تفاضل دو مربع نوشت اگر و تنها اگر n به‌صورت $۴k + ۲$ نباشد.

اثبات. چون به‌ازای هر عدد صحیح a، (به پیمانهٔ ۴) ۱ یا $a^۲ \equiv ۰$، نتیجه می‌شود

$$a^۲ - b^۲ \equiv ۰, ۱, \text{ یا } ۳ \text{ (به پیمانهٔ ۴)}$$

بنابراین، اگر (به پیمانهٔ ۴) $n \equiv ۲$، هرگز نمی‌توانیم به‌ازای a و b ای، بنویسیم $n = a^۲ - b^۲$.

برعکس، فرض می‌کنیم عدد صحیح n به‌صورت $۴k + ۲$ نیست، یعنی در پیمانهٔ ۴ داریم ۳ یا $n \equiv ۰, ۱$. اگر (به پیمانهٔ ۴) ۳ یا $n \equiv ۱$، آنگاه هردوی $n + ۱$ و $n - ۱$ عددهایی صحیح زوج‌اند؛ پس، n را می‌توان به‌صورت تفاضل دو مربع یعنی

$$n = \left(\frac{n+۱}{۲}\right)^۲ - \left(\frac{n-۱}{۲}\right)^۲$$

نوشت. اگر (به پیمانهٔ ۴) $n \equiv ۰$، آنگاه داریم

$$n = \left(\frac{n}{۴}+۱\right)^۲ - \left(\frac{n}{۴}-۱\right)^۲ \qquad \square$$

فرع. هر عدد اول فرد تفاضل دو مربع متوالی است.

مثالهایی از این فرع عبارت‌اند از

$$۱۱ = ۶^۲ - ۵^۲, \quad ۱۷ = ۹^۲ - ۸^۲, \quad ۲۹ = ۱۵^۲ - ۱۴^۲$$

نکتهٔ قابل ذکر دیگر اینکه نمایش عدد اول p به‌صورت تفاضل دو مربع، یکتاست. برای ملاحظهٔ این مطلب، فرض می‌کنیم

$$p = a^۲ - b^۲ = (a-b)(a+b)$$

که در آن $a > b > ۰$. چون ۱ و p تنها عاملهای pاند، لزوماً داریم

$$a + b = p \quad \text{و} \quad a - b = ۱$$

که از آنها نتیجه می‌شود

$$b = \frac{p-۱}{۲} \quad \text{و} \quad a = \frac{p+۱}{۲}$$

بنابراین، هر عدد اول فرد را می‌توان دقیقاً به یک روش به‌صورت تفاضل مربعات دو عدد صحیح نوشت یعنی، به‌صورت

$$p = \left(\frac{p+۱}{۲}\right)^۲ - \left(\frac{p-۱}{۲}\right)^۲$$

اگر به‌جای عددهای اول، عددهای صحیح دلخواه را در نظر بگیریم، وضعیت فرق می‌کند. فرض می‌کنیم n عددی صحیح و مثبت است که نه اول است و نه به‌صورتِ $۴k + ۲$. با شروع از یک مقسوم‌علیه n مانند d، قرار می‌دهیم $d' = \frac{n}{d}$ (فرض می‌کنیم $d \geq d'$). حال اگر هردوی d و d' زوج یا هردو فرد باشند، آنگاه $\frac{d+d'}{۲}$ و $\frac{d-d'}{۲}$ عددهایی صحیح‌اند. به علاوه، می‌توانیم بنویسیم

$$n = dd' = \left(\frac{d+d'}{۲}\right)^۲ - \left(\frac{d-d'}{۲}\right)^۲$$

به‌عنوان مثال، عدد صحیح $n = ۲۴$ را درنظر می‌گیریم. داریم

$$۲۴ = ۱۲ \times ۲ = \left(\frac{۱۲+۲}{۲}\right)^۲ - \left(\frac{۱۲-۲}{۲}\right)^۲ = ۷^۲ - ۵^۲$$

و

$$۲۴ = ۶ \times ۴ = \left(\frac{۶+۴}{۲}\right)^۲ - \left(\frac{۶-۴}{۲}\right)^۲ = ۵^۲ - ۱^۲$$

و به این ترتیب دو نمایش متفاوت ۲۴ به‌صورت تفاضل مربعها حاصل می‌شود.

تمرینهای ۱۲ـ۲

۱. هریک از عددهای اول ۱۱۳، ۲۲۹، و ۳۷۳ را به‌صورت مجموع دو مربع نمایش دهید.

۲. (الف) حدس زده شده که تعداد نامتناهی عدد اول p وجود دارد به‌طوری که به‌ازای عدد صحیح مثبت n ای، $p = n^۲ + (n+۱)^۲$؛ به‌عنوان مثال، $۵ = ۱^۲ + ۲^۲$ و $۱۳ = ۲^۲ + ۳^۲$. پنج عدد اول دیگر را که از این نوع باشند پیدا کنید.

(ب) حدس دیگر این است که تعداد نامتناهی عدد اول p به‌صورت $p = ۲^۲ + p_۱^۲$، که $p_۱$ عددی اول است، وجود دارد. ۵ عدد اول را که از این نوع باشند پیدا کنید.

۳. هر یک از حکمهای زیر را ثابت کنید:

(الف) هر عدد صحیح ۲^n، که در آن $n = ۱, ۲, ۳, \ldots$، مجموع دو مربع است؛

(ب) اگر (به پیمانهٔ ۹) ۶ یا ۳ $\equiv n$، n را نمی‌توان به‌صورت مجموع دو مربع نمایش داد؛

(پ) اگر n مجموع دو عدد مثلثی باشد، آنگاه $۴n + ۱$ مجموع دو مربع است؛

(ت) هر عدد فرمای $F_n = ۲^{۲^n} + ۱$، $n \geq ۱$، را می‌توان به‌صورت مجموع دو مربع نوشت.

(ث) هر عدد تام فرد (در صورت وجود) مجموع دو مربع است. [راهنمایی: به فرع قضیهٔ ۱۰ـ۷ نگاه کنید.]

۴. ثابت کنید عدد اول p را می‌توان به‌صورت مجموع دو مربع نوشت اگر و تنها اگر همنهشتی $x^۲ + ۱ \equiv ۰$ (به پیمانهٔ p) دارای جواب باشد.

۵. (الف) نشان دهید عدد صحیح مثبت n مجموع دو مربع است اگر وتنها اگر $n = ۲^m a^۲ b$، که در آن $m \geq ۰$، a عددی صحیح فرد، و هر مقسوم‌علیه اول b به‌صورت $۴k + ۱$ است.

(ب) عددهای صحیح $۱۳ \times ۷^۲ \times ۵ = ۳۱۸۵$، $۳۹۶۹۰ = ۲ \times ۳^۴ \times ۵ \times ۷^۲$، و $۶۲۹۲۰ = ۲^۳ \times ۵ \times ۱۱^۲ \times ۱۳$ را به‌صورت مجموع دو مربع بنویسید.

۶. عدد صحیح مثبتی پیدا کنید که صرف‌نظر از علامت و ترتیب عاملها، دارای حداقل سه نمایش متفاوت به‌صورت مجموع دو مربع باشد. [راهنمایی: عدد صحیحی پیدا کنید که سه عامل اول متمایز به‌صورت $۴k + ۱$ داشته باشد.]

۷. نشان دهید که اگر عدد صحیح مثبت n مجموع مربعهای دو عدد صحیح نباشد، نمی‌تواند مجموع مربعهای دو عدد گویا باشد. [راهنمایی: بنا به قضیهٔ ۱۲ـ۳، عدد اول $p \equiv ۳$ (به پیمانهٔ ۴) و عدد صحیح فرد k ای وجود دارد به طوری که $p^k | n$ ولی $p^{k+۱} \nmid n$. اگر $n = (a/b)^۲ + (c/d)^۲$، آنگاه نمای p در سمت چپ معادلهٔ $n(bd)^۲ = (ad)^۲ + (bc)^۲$ فرد و در سمت راست زوج خواهد بود.]

۸. نشان دهید تعداد نمایشهای ممکن عدد صحیح مثبت n به‌صورت مجموع دو مربع برابر با تعداد نمایشهای ممکن عدد صحیح $۲n$ به‌صورت مجموع دو مربع است. [راهنمایی: با شروع از نمایشی از n به‌صورت مجموع دو مربع، نمایشی مشابه از $۲n$ به‌دست آورید و برعکس.]

۹. (الف) اگر n عددی مثلثی باشد، نشان دهید هریک از سه عدد صحیح متوالی $۸n^۲$، $۸n^۲ + ۱$، $۸n^۲ + ۲$ را می‌توان به‌صورت مجموع دو مربع نوشت.

(ب) ثابت کنید از هر چهار عدد صحیح متوالی، لااقل یکی قابل نمایش به‌صورت مجموع دو مربع نیست.

۱۰. ثابت کنید که:

(الف) اگر عدد اولی مجموع مربعات دو یا چهار عدد اول متفاوت باشد، آنگاه یکی از این عددهای اول باید برابر ۲ باشد.

(ب) اگر یک عدد اول مجموع مربعات سه عدد اول متفاوت باشد، آنگاه یکی از این عددهای اول باید برابر ۳ باشد.

۱۱. (الف) فرض می‌کنیم p عدد اول فردی باشد. اگر $\gcd(a,b) = ۱$ و $p|a^۲ + b^۲$، ثابت کنید $p \equiv ۱$ (به پیمانهٔ ۴). [راهنمایی: همنهشتی $a^۲ \equiv -b^۲$ (به پیمانهٔ p) را به توان $(p-۱)/۲$ برسانید و با استفاده از قضیهٔ فرما نتیجه بگیرید $(-۱)^{(p-۱)/۲} = ۱$.]

(ب) با استفاده از قسمت (الف) نشان دهید هر مقسوم‌علیه مثبتِ مجموعِ دو مربع متباین، خود مجموع دو مربع است.

۱۲. ثابت‌کنید هر عدد اول p ای راکه به‌صورت $۸k + ۱$ یا $۸k + ۳$ باشد می‌توان به‌ازای عددهای صحیح a و b ای به‌صورت $p = a^۲ + ۲b^۲$ نوشت. [راهنمایی: از اثبات قضیهٔ ۱۲ـ۲ تقلید کنید.]

۱۳. ثابت کنید

(الف) عدد صحیح مثبت قابل نمایش به‌صورت تفاضل دو مربع است اگر و تنها اگر حاصلضرب دو عامل زوج یا دو عامل فرد باشد.

(ب) عدد صحیح مثبت زوج را می‌توان به‌صورت تفاضل دو مربع نوشت اگر و تنها اگر بر ۴ بخشپذیر باشد.

۱۴. نشان دهید که ۴۵ کوچکترین عدد صحیح مثبتی است که سه نمایش متمایز به‌صورت تفاضل دو مربع دارد. [راهنمایی: به قسمت (الف) تمرین قبل نگاه کنید.]

۱۵. نشان دهید که به‌ازای هر $n > ۰$ عدد صحیح مثبتی وجود دارد که می‌توان آن را به n روش متمایز به‌صورت تفاضل دو مربع نوشت. [راهنمایی: توجه کنید که به‌ازای $k = ۱, ۲, \ldots, n$، $۲^{۲n+۱} = (۲^{۲n-k} + ۲^{k-۱})^۲ - (۲^{۲n-k} - ۲^{k-۱})^۲$.]

۱۶. ثابت کنید هر عدد اول $p \equiv ۱$ (به پیمانهٔ ۴) مجموع دو مربع متباین را که هر یک بزرگتر از ۳ باشد، می‌شمارد. [راهنمایی: به‌ازای هر ریشهٔ اولیهٔ فرد r از p، $r^k \equiv ۲$ (به پیمانهٔ p)؛ پس $r^{۲[k+(p-۱)/۴]} \equiv -۴$ (به پیمانهٔ p).]

۱۷. نشان دهید معادلهٔ $n^۲ + (n+۱)^۲ = m^۳$ ریشه‌ای برحسب عددهای صحیح مثبت ندارد.

۱۸. جی. اچ. هاردی، متخصص انگلیسیِ نظریهٔ اعداد، که حامی و مشوق رامانوجان بود، این حکایت را دربارهٔ او نقل می‌کند: به‌خاطر می‌آورم که روزی به عیادت او که در بیمارستان بستری بود می‌رفتم. مسیر را با یک تاکسی با شمارهٔ پلاک ۱۷۲۹ طی کردم. این شماره به‌نظرم عددی بی‌خاصیت آمد و آرزو کردم بدشگون نباشد. وقتی موضوع را در بیمارستان با او درمیان گذاشتم، پاسخ داد: «نه، عدد بسیار جالبی است، کوچکترین عددی است که می‌توان آن را به دو شکل متفاوت به‌صورت مجموع دو مکعب نوشت.» درستی ادعای راما نوجان را تحقیق کنید.

۳ـ۱۲ مجموعهایِ بیش از دو مربع

دیدیم که هر عدد صحیح مثبتی را نمی‌توان به صورت مجموع دو مربع نمایش داد. اکنون ببینیم در مورد امکان نمایش عدد صحیح مثبت به‌صورت مجموع سه مربع چه می‌توان گفت (^{۲} ۰ در اینجا هم مجاز است). با توجه به اینکه مربع دیگری اضافه می‌کنیم، به‌نظر منطقی می‌رسد که استثناهای کمتری وجود داشته باشد. به‌عنوان نمونه، اگر فقط دو مربع مجاز باشد، نمایشی برای مثلاً ۱۴، ۳۳، و ۶۷ نداریم، حال آنکه

$$۱۴ = ۳^{۲} + ۲^{۲} + ۱^{۲}, \quad ۳۳ = ۵^{۲} + ۲^{۲} + ۲^{۲}, \quad ۶۷ = ۷^{۲} + ۳^{۲} + ۳^{۲}$$

مع‌الوصف، عددهای صحیحی وجود دارند که قابل نمایش به‌صورت مجموع سه مربع نیستند. قضیه‌ای مربوط به این موضوع عبارت است از

قضیهٔ ۱۲ـ۵ عدد صحیح مثبتی به‌صورت $۴^{n}(۸m+۷)$ را نمی‌توان به‌صورت مجموع سه مربع نوشت.

اثبات. در شروع کار، نشان می‌دهیم عدد صحیح $۸m + ۷$ به‌صورت مجموع سه مربع قابل بیان نیست. به‌ازای هر عدد صحیح a، داریم (به پیمانهٔ ۸) ۴ یا $a^{۲} \equiv ۰, ۱$. نتیجه می‌شود که به‌ازای هر a، b، c ی انتخابی

$$a^{۲} + b^{۲} + c^{۲} \equiv ۰, ۱, ۲, ۳, ۴, ۵, \text{ یا } ۶ \text{ (به پیمانهٔ ۸)}$$

چون (به پیمانهٔ ۸) $۸m + ۷ \equiv ۷$، معادلهٔ $a^{۲} + b^{۲} + c^{۲} = ۸m + ۷$ ممتنع است.

سپس فرض می‌کنیم $۴^{n}(۸m + ۷)$، $n \geq ۱$، را بتوان به‌صورت

$$۴^{n}(۸m + ۷) = a^{۲} + b^{۲} + c^{۲}$$

نوشت. در این صورت هریک از عددهای صحیح a، b، c باید زوج باشد. با قرار دادن $a = ۲a_{۱}$، $b = ۲b_{۱}$، $c = ۲c_{۱}$ به‌دست می‌آوریم

$$۴^{n-۱}(۸m + ۷) = a_{۱}^{۲} + b_{۱}^{۲} + c_{۱}^{۲}$$

اگر $n - ۱ \geq ۱$، استدلال را تا جایی که $۸m + ۷$ بالاخره به‌صورت مجموع سه عدد صحیح مربع نمایش داده شود، ادامه می‌دهیم؛ این، البته، مغایر با نتیجهٔ پاراگراف نخست است. □

می‌توان ثابت کرد که برای نمایشپذیری عدد صحیحی به‌صورت مجموع سه مربع، شرط قضیهٔ ۱۲ـ۵ کافی نیز هست؛ ولی، استدلال پیچیده‌تر از آن است که بتوان آن را در این کتاب آورد. بخشی از این پیچیدگی به این دلیل است که، برخلاف حالت دو (یا حتی چهار مربع)، اتحادی جبری که حاصلضرب مجموعهای سه مربع را به‌صورت مجموع سه مربع ارائه دهد وجود ندارد.

به بیان نکته‌هایی تاریخی می‌پردازیم. درواقع، دیوفانتوس بود که حدس زد عددی به‌صورت $۸m + ۷$ قابل نمایش به‌صورت مجموع سه مربع نیست، این حکم را دکارت در ۱۶۳۸ به‌سادگی ثابت کرد. فرما را به حق می‌توانیم نخستین فردی بدانیم که معیار زیر را به‌طور کامل بیان کرد: عددی را می‌توان به‌صورت مجموع سه مربع نوشت اگر و تنها اگر به‌صورت $۴^n(۸m + ۷)$، که در آن m، و n عددهای صحیح نامنفی هستند، نباشد. درستی این معیار در ۱۷۹۸ به روشی پیچیده توسط لژاندر و در ۱۸۰۱ به روشی واضحتر (ولی نه آسانتر) توسط گاوس ثابت شد.

به‌طوری‌که اشاره شد، عددهای صحیح مثبتی وجود دارند که قابل نمایش به‌صورت مجموع دو یا سه مربع نیستند (به عنوان مثالهایی ساده، می‌توان ۷ و ۱۵ را درنظر گرفت). وضعیت در حالتِ چهار مربع به کلی متفاوت است؛ در این حالت ابداً استثنایی درکار نیست!

باشه نخستین فردی بود که (در ۱۶۲۱) به صراحت امکان نمایش هر عدد صحیح مثبت به‌صورت مجموع چهار مربع را، با احتساب ۰^۲، اعلام کرد و درستی این حدس را در مورد همهٔ عددهای صحیح مثبت تا ۳۲۵ تحقیق کرد. پانزده سال بعد، فرما ادعا کرد اثباتی برای این حدس، با استفاده از روش مورد علاقه‌اش، یعنی نزول نامتناهی، به‌دست آورده است، ولی، طبق معمول، توضیحی دربارهٔ اثبات نداد. هم فرما و هم باشه، احساس می‌کردند که دیوفانتوس بایستی به این نتیجه واقف بوده باشد؛ دلیل آن کاملاً حدسی است: دیوفانتوس شرطهایی لازم برای نمایشپذیری عدد به‌صورت مجموع دو یا سه مربع ارائه کرد، ولی از شرطی برای نمایشپذیری به‌صورت مجموع چهار مربع، ذکری به میان نیاورد.

یکی از نشانه‌های دشواری مسأله این است که، علی‌رغم دستاوردهای درخشان اویلر در زمینه‌های دیگر، تلاش چهل سالهٔ او برای تعیین تکلیف این حدس به جایی نرسید. مع‌الوصف، کارهای او بعدها در حل نهایی مسأله کارساز واقع شد؛ اویلر اتحادی اساسی کشف کرد که طبق آن می‌توان حاصلضرب دو عدد را که هریک مجموع چهار مربع است به‌صورت مجموعی مشابه نوشت و نیز به این حکم اساسی رسید که همنهشتی $x^۲ + y^۲ + ۱ \equiv ۰ \pmod{p}$ به‌ازای هر عدد اول p حلپذیر است. اثبات کاملی از حدس چهار مربع را لاگرانژ در ۱۷۷۲ منتشر کرد. وی اذعان کرد که این اثبات بر اساس اندیشه‌های اویلر صورت گرفته است. سال بعد، اویلر اثبات به مراتب ساده‌تری ارائه کرد که در اساس همان اثباتی است که در این کتاب ارائه خواهد شد.

به منظور پرهیز از هرگونه وقفه‌ای در روند اصلی استدلال در مرحله‌های دشوار، مناسب است دو لم مقدماتی را بیان و اثبات کنیم. اثبات لم نخست حاوی اتحادی جبری است که تحویل مسأله چهار مربع به بررسی عددهای اول را ممکن می‌سازد.

لم ۱ (اویلر). اگر هریک از عددهای صحیح m و n مجموع چهار مربع باشد، آنگاه mn نیز مجموع چهار مربع است.

اثبات. اگر به‌ازای عددهای صحیح a_i و b_iای، $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ و $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$، آنگاه

$$\begin{aligned}
mn &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2)\\
&= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2\\
&\quad + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2\\
&\quad + (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2\\
&\quad + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2
\end{aligned}$$

درستی این اتحاد را می‌توان به‌طور مستقیم با محاسبهٔ طرفین و ساده کردن تحقیق کرد. □

نکتهٔ اساسی دیگر در بحث ما، لم زیر است.

لم ۲. اگر p عدد اول فردی باشد، آنگاه همنهشتی

$$x^2 + y^2 + 1 \equiv 0 \quad (\text{به پیمانهٔ } p)$$

دارای جواب x_0، y_0ای است به‌طوری‌که $0 \le x_0 \le (p-1)/2$ و $0 \le y_0 \le (p-1)/2$.

اثبات. راه اثبات با توجه به دو مجموعهٔ زیر گشوده می‌شود:

$$S_1 = \left\{1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}$$
$$S_2 = \left\{-0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}$$

واضح است که هیچ دو عضو S_1 همنهشت به پیمانهٔ p نیستند زیرا اگر (به پیمانهٔ p) $1+x_1^2 \equiv 1+x_2^2$، آنگاه یا (به پیمانهٔ p) $x_1 \equiv x_2$ یا (به پیمانهٔ p) $x_1 \equiv -x_2$. ولی نتیجهٔ اخیر غیرممکن است زیرا

$\circ < x_\text{۱} + x_\text{۲} < p$ (مگر اینکه $x_\text{۱} = x_\text{۲} = \circ$)، بنابراین $x_\text{۱} \equiv x_\text{۲}$ (به پیمانهٔ p)، که نتیجه می‌دهد $x_\text{۱} = x_\text{۲}$. به همین روش، هیچ دو عضو $S_\text{۲}$ همنهشت (به پیمانهٔ p) نیستند.

$S_\text{۱}$ و $S_\text{۲}$ مجموعاً دارای $\text{۲}[\text{۱} + (p - \text{۱})/\text{۲}] = p + \text{۱}$ عضو هستند. بنابه اصل لانهٔ کبوتر، عدد صحیحی در $S_\text{۱}$ باید با عدد صحیحی در $S_\text{۲}$ همنهشت به پیمانهٔ p باشد؛ یعنی، $x_\circ$، $y_\circ$ ای وجود دارد به‌طوری‌که

$$\text{۱} + x_\circ^\text{۲} \equiv -y_\circ^\text{۲} \ \ (\text{به پیمانهٔ } p)$$

که در آن $\circ \le x_\circ \le (p - \text{۱})/\text{۲}$ و $\circ \le y_\circ \le (p - \text{۱})/\text{۲}$. □

فرع. به‌ازای عدد اول فرد دادهٔ شدهٔ p عدد صحیح $k < p$ ای وجود دارد به‌طوری‌که kp مجموع چهار مربع است.

اثبات. بنابه قضیه، می‌توانیم عددهای صحیح $x_\circ$ و $y_\circ$ ای پیدا کنیم به‌طوری‌که

$$\circ \le x_\circ < p/\text{۲} \qquad \text{و} \qquad \circ \le y_\circ < p/\text{۲}$$

و به‌ازای k ی مناسبی داریم

$$x_\circ^\text{۲} + y_\circ^\text{۲} + \text{۱}^\text{۲} + \circ^\text{۲} = kp$$

از محدودیتهایی که اندازه‌های $x_\circ$ و $y_\circ$ دارند نتیجه می‌شود

$$kp = x_\circ^\text{۲} + y_\circ^\text{۲} + \text{۱} < \frac{p^\text{۲}}{\text{۴}} + \frac{p^\text{۲}}{\text{۴}} + \text{۱} < p_\text{۲}$$

یعنی، همان طورکه در فرع گفته شده، $k < p$. □

به منظور بررسی یک مثال، بحث را موقتاً کنار می‌گذاریم. اگر $p = \text{۱۷}$، آنگاه مجموعه‌های $S_\text{۱}$ و $S_\text{۲}$ عبارت‌اند از

$$S_\text{۱} = \{\text{۱}, \text{۲}, \text{۵}, \text{۱۰}, \text{۱۷}, \text{۲۶}, \text{۳۷}, \text{۵۰}, \text{۶۵}\}$$

و

$$S_\text{۲} = \{\circ, -\text{۱}, -\text{۴}, -\text{۹}. -\text{۱۶}, -\text{۲۵}, -\text{۳۶}, -\text{۴۹}, -\text{۶۴}\}$$

به پیمانهٔ ۱۷، مجموعهٔ $S_\text{۱}$ از عددهای صحیح ۱، ۲، ۵، ۱۰، ۰، ۹، ۳، ۱۶، ۱۴ و مجموعهٔ $S_\text{۲}$ از ۰، ۱۶، ۱۳، ۸، ۱، ۹، ۱۵، ۲، ۴ تشکیل می‌شود. لم ۲ می‌گوید که عضوی به‌صورت $x^\text{۲} + \text{۱}$ از

مجموعهٔ نخست با عضوی به‌صورت $-y^۲$ از مجموعهٔ دوم همنهشت است. در میان امکانهای گوناگون، داریم

$$۱ + ۵^۲ \equiv ۹ \equiv -۵^۲ \quad (\text{به پیمانهٔ } ۱۷)$$

یا $۱ + ۵^۲ + ۵^۲ \equiv ۰$ (به پیمانهٔ ۱۷). نتیجه می‌گیریم

$$۳ \times ۱۷ = ۱^۲ + ۵^۲ + ۵^۲ + ۰^۲$$

مضربی از ۱۷ است که به‌صورت مجموع چهار مربع نوشته شده است.

لم ۲ به اندازه‌ای در بحث ما اساسی است که می‌ارزد اثباتی دیگر برای آن ارائه کنیم. این اثبات با استفاده از نظریهٔ مانده‌های درجهٔ دوم صورت می‌گیرد. اگر $p \equiv ۱$ (به پیمانهٔ ۴)، می‌توانیم $x_۰$ را جوابی از $x^۲ \equiv -۱$ (به پیمانهٔ p) (که بنابه فرع قضیهٔ ۹ـ۲ مجاز است) و $y_۰$ را برابر ۰ انتخاب کنیم، در این صورت

$$x_۰^۲ + y_۰^۲ + ۱ \equiv ۰ \quad (\text{به پیمانهٔ } p)$$

بنابراین، کافی است حالت $p \equiv ۳$ (به پیمانهٔ ۴) را درنظر بگیریم. نخست عدد صحیح a را به‌عنوان کوچکترین ناماندهٔ درجهٔ دوم مثبت p انتخاب می‌کنیم (توجه کنید که $a \geq ۲$، زیرا ۱ مانده‌ای درجهٔ دوم است). پس

$$(-a/p) = (-۱/p)(a/p) = (-۱)(-۱) = ۱$$

یعنی، $-a$ ماندهٔ درجه دومی از p است. پس، همنهشتی

$$x^۲ \equiv -a \quad (\text{به پیمانهٔ } p)$$

دارای جواب $x_۰$ای، $۰ < x_۰ \leq (p-۱)/۲$، است. ولی $a - ۱$ که مثبت و کوچکتر از a است، باید خودش مانده‌ای درجهٔ دوم از p باشد. بنابراین، عدد صحیح $y_۰$ای، $۰ < y_۰ \leq (p-۱)/۲$، وجود دارد که در همنهشتی زیر صدق می‌کند

$$y^۲ \equiv a - ۱ \quad (\text{به پیمانهٔ } p)$$

نتیجه:

$$x_۰^۲ + y_۰^۲ + ۱ \equiv -a + (a-۱) + ۱ \equiv ۰ \quad (\text{به پیمانهٔ } p)$$

اکنون با در دست داشتن این دو لم، اطلاعات ضروری را برای اثبات نمایش‌پذیری هر عدد اول به‌صورت مجموع چهار عدد صحیح مربع در اختیار داریم.

قضیهٔ ۱۲ـ۶ هر عدد اول p را می‌توان به‌صورت مجموع چهار مربع نوشت.

اثبات. قضیه قطعاً به‌ازای $p = ۲$ درست است زیرا $۲ = ۱^۲ + ۱^۲ + ۰^۲ + ۰^۲$. بنابراین، از این به بعد توجه خود را به عددهای اول فرد معطوف می‌کنیم. فرض می‌کنیم k کوچکترین عدد صحیح مثبتی است که به‌ازای آن kp مجموع چهار مربع است: مثلاً

$$kp = x^۲ + y^۲ + z^۲ + w^۲$$

بنا به فرع پیشگفته، $k < p$. می‌خواهیم استدلال کنیم که $k = ۱$.

با اثبات اینکه k عددی صحیح فردی است، آغاز می‌کنیم. در اینجا برهان خلف را به کار می‌گیریم. فرض می‌کنیم k زوج است. در این صورت x، y، z، w یا همگی زوج‌اند، یا همگی فردند، یا دوتا از آنها زوج و دوتا فرد است. در هر صورت، می‌توانیم طوری آنها را مرتّب کنیم که

$$x \equiv y \pmod{۲} \quad \text{و} \quad z \equiv w \pmod{۲}$$

نتیجه می‌شود که

$$\frac{۱}{۲}(x-y)،\ \frac{۱}{۲}(x+y)،\ \frac{۱}{۲}(z-w)،\ \frac{۱}{۲}(z+w)$$

همگی عددهایی صحیح‌اند و

$$\frac{۱}{۲}(kp) = \left(\frac{x-y}{۲}\right)^۲ + \left(\frac{x+y}{۲}\right)^۲ + \left(\frac{z-w}{۲}\right)^۲ + \left(\frac{z+w}{۲}\right)^۲$$

نمایشی از $(k/۲)p$ به‌صورت مجموع چهار مربع است. این مغایر است با کوچکترین بودن k، و به تناقض می‌رسیم.

هنوز اثبات $k = ۱$ باقی مانده است. فرض می‌کنیم این برابری برقرار نباشد پس k ، به عنوان عددی صحیح فرد، حداقل ۳ است. بنابراین می‌توان عددهای صحیح a، b، c، d را طوری انتخاب کرد که

$$a \equiv x \pmod{k}،\ b \equiv y \pmod{k}،\ c \equiv z \pmod{k}،\ d \equiv w \pmod{k}$$

و

$$|a| < \frac{k}{۲}،\ |b| < \frac{k}{۲}،\ |c| < \frac{k}{۲}،\ |d| < \frac{k}{۲}$$

(به عنوان نمونه، برای به‌دست آوردن عدد صحیح a، r یعنی باقیماندهٔ تقسیم x بر k را به‌دست می‌آوریم؛ برحسب اینکه $r < k/۲$ یا $r > k/۲$ قرار می‌دهیم $a = r$ یا $a = r - k$.) در این صورت

$$a^۲ + b^۲ + c^۲ + d^۲ \equiv x^۲ + y^۲ + z^۲ + w^۲ \equiv ۰ \quad (\text{به پیمانهٔ } k)$$

و بنابراین به‌ازای عدد صحیح نامنفی nای داریم

$$a^۲ + b^۲ + c^۲ + d^۲ = nk$$

به دلیل محدودیت اندازه‌های a، b، c، d داریم

$$۰ \leq nk = a^۲ + b^۲ + c^۲ + d^۲ < ۴(\frac{k}{۲})^۲ = k^۲$$

$n = ۰$ ممکن نیست زیرا در این صورت لازم می‌آید $a = b = c = d = ۰$ و، درنتیجه، k هریک از عددهای صحیح x، y، z، w را می‌شمارد. بنابراین $k^۲|kp$، یا $k|p$، که با توجه به نابرابری $۱ < k < p$ پذیرفتنی نیست. رابطهٔ $nk < k^۲$ نیز نتیجه می‌دهد $n < k$. پس در مجموع: $۰ < n < k$. با تلفیق نتیجه‌های حاصل، به‌دست می‌آوریم

$$\begin{aligned} k^۲np &= (kp)(kn) = (x^۲ + y^۲ + z^۲ + w^۲)(a^۲ + b^۲ + c^۲ + d^۲) \\ &= r^۲ + s^۲ + t^۲ + u^۲ \end{aligned}$$

که در آن

$$r = xa + yb + zc + wd$$

$$s = xb - ya + zd - wc$$

$$t = xc - yd - za + wb$$

$$u = xd + yc - zb - wa$$

قابل توجه است که هر چهار عدد صحیح r، s، t، u بر k بخشپذیرند. به‌عنوان مثال، در مورد عدد صحیح r داریم

$$r = xa + yb + zc + wd \equiv a^۲ + b^۲ + c^۲ + d^۲ \equiv ۰ \quad (\text{به پیمانهٔ } k)$$

به‌همین نحو، (به پیمانهٔ k) $s \equiv t \equiv u \equiv ۰$. از اینجا نتیجه می‌شود

$$np = \left(\frac{r}{k}\right)^۲ + \left(\frac{s}{k}\right)^۲ + \left(\frac{t}{k}\right)^۲ + \left(\frac{u}{k}\right)^۲$$

که در آن r/k، s/k، t/k، u/k همگی عددهایی صحیح‌اند. اما چون $k > n > ۰$، این متناقض است با انتخاب k به‌عنوان کوچکترین عدد صحیحی که به‌ازای آن kp مجموع چهار مربع است. با این تناقض، $k = ۱$، و اثبات بالاخره به انجام می‌رسد. □

به این ترتیب به آستانهٔ هدف نهایی خود، یعنی، قضیهٔ کلاسیک لاگرانژ، رسیده‌ایم.

قضیهٔ ۱۲ـ۷ (لاگرانژ). هر عدد صحیح مثبت n را می‌توان به‌صورت مجموع چهار مربع، که برخی ممکن است صفر باشند، نوشت.

اثبات. عدد صحیح ۱ به وضوح به‌صورت $۱ = ۱^۲ + ۰^۲ + ۰^۲ + ۰^۲$ یعنی، مجموع چهار مربع، قابل نمایش است. فرض می‌کنیم $n > ۱$ و $n = p_۱ p_۲ \ldots p_r$ تجزیهٔ n به عددهای اول (نه لزوماً متمایز) باشد. چون هر p_i قابل نمایش به‌صورت مجموع چهار مربع است، حاصلضرب هر دو عدد اولی را می‌توانیم با استفاده از اتحاد اویلر، به‌صورت مجموع چهار مربع نمایش دهیم. بنابه استقرا، این را به هر تعداد متناهی از عاملهای اول می‌توان تعمیم داد، و بنابراین، با r بار کاربرد اتحاد، نمایش مطلوب n را به‌دست می‌آوریم. □

مثال ۱۲ـ۲

برای نمایش عدد صحیح $۴۵۹ = ۳^۳ \times ۱۷$ به‌صورت مجموع چهار مربع، از اتحاد اویلر به شرح زیر استفاده می‌کنیم

$$\begin{aligned}
۴۵۹ &= ۳^۲ \times ۳ \times ۱۷ \\
&= ۳^۲(۱^۲ + ۱^۲ + ۱^۲ + ۰^۲)(۴^۲ + ۱^۲ + ۰^۲ + ۰^۲) \\
&= ۳^۲[(۴ + ۱ + ۰ + ۰)^۲ + (۱ - ۴ + ۰ - ۰)^۲ \\
&\quad + (۰ - ۰ - ۴ + ۰)^۲ + (۰ + ۰ - ۱ - ۰)^۲] \\
&= ۳^۲[۵^۲ + ۳^۲ + ۴^۲ + ۱^۲] \\
&= ۱۵^۲ + ۹^۲ + ۱۲^۲ + ۳^۲
\end{aligned}$$

■

گرچه همهٔ توجه ما تاکنون معطوف به مربعها بوده است، بسیاری از ایده‌های مربوطه قابل تعمیم به توانهای بزرگترند.

ادوارد وارینگ درکتاب خود با عنوان تأملاتی در جبر[1] (۱۷۷۰)، نوشت که هر عدد صحیح مثبت به‌صورت مجموع حداکثر ۹ مکعب، و نیز مجموع حداکثر ۱۹ توان چهارم، و غیره قابل بیان است. ادعای فوق مبنای طرح این پرسش بوده است: آیا هر عدد صحیح مثبتی را می‌توان به‌صورت مجموع حداکثر $g(k)$ توان kام، که در آن $g(k)$ فقط به k بستگی دارد و نه به عدد مورد نمایش، نمایش داد؟ به بیان دیگر، به‌ازای هر kی داده شده، عدد $g(k)$ای مورد نظر است که هر $n > ۰$ را بتوان حداقل به یک روش به‌صورت

$$n = a_۱^k + a_۲^k + \ldots + a_{g(k)}^k$$

نمایش داد که در آن a_iها عددهایی صحیح نامنفی و نه لزوماً متمایز باشند. این مسأله سرآغاز پژوهشهای بسیاری در حوزه‌ای از نظریهٔ اعداد است که به «مسألهٔ وارینگ» معروف است. به‌نظر می‌رسد که به احتمال قوی، وارینگ نه‌تنها اثباتی بر مدعای خود در اختیار نداشته است، بلکه مثالهای عددی او در توجیه مدّعایش نیز محدود بوده است.

همان‌طور که در قضیهٔ لاگرانژ عنوان کردیم، $g(۲) = ۴$. بجز در حالتِ مربعها، نخستین قضیه از نوع قضیهٔ وارینگ که واقعاً ثابت شده، به لیوویل (۱۸۵۹) نسبت داده می‌شود: هر عدد صحیح مثبت، مجموع حداکثر ۵۳ توان چهارم است. این کران بالا برای $g(۴)$ تا اندازه‌ای بزرگ است، و به مرور زمان به تدریج کوچکتر شده است. وجود $g(k)$ به‌ازای هر مقدار k را هیلبرت در ۱۹۰۹ ثابت کرد؛ متأسفانه اثبات او متّکی بر ابزارهای فراوان (از جمله یک انتگرال ۲۵ گانه در مرحله‌ای) است و ابداً سازنده نیست.

همین که معلوم شود مسأله وارینگ جواب دارد، طبیعتاً این پرسش مطرح می‌شود که $g(k)$ به چه بزرگی است؟» مقاله‌های بسیاری دربارهٔ این وجه مسأله نوشته شده، ولی خود مسأله هنوز حل‌نشده است. نتیجه‌ای ساده، که دیکسن آن را به‌دست آورد، این است که $g(۳) = ۹$، و

$$۲۳ = ۲^۳ + ۲^۳ + ۱^۳ + ۱^۳ + ۱^۳ + ۱^۳ + ۱^۳ + ۱^۳ + ۱^۳$$

و

$$۲۳۹ = ۴^۳ + ۴^۳ + ۳^۳ + ۳^۳ + ۳^۳ + ۳^۳ + ۱^۳ + ۱^۳ + ۱^۳$$

تنها عددهای صحیحی‌اند که واقعاً در نمایش آنها به ۹ مکعب نیاز است؛ هر عدد صحیح بزرگتر

1. Meditationes Algebraicae

از ۲۳۹ را می‌توان به‌صورت مجموع حداکثر ۸ مکعب نمایش داد. در ۱۹۴۲، لینیک[1] ثابت کرد که فقط تعدادی متناهی از عددهای صحیح به ۸ مکعب نیازمندند؛ از مرحله‌ای به بعد ۷ تا کافی است. اینکه آیا ۶ مکعب نیز برای نمایش همهٔ عددهای صحیح مثبت، بجز تعدادی متناهی از آنها، کافی است یا نه، هنوز مشخص نیست.

معلوم شده است که حالتهای $k = ۴$ و $k = ۵$ دشوارترین حالتها هستند. طی سالهای متمادی، بهترین نتیجهٔ موجود این بوده که $g(۴)$ جایی در محدودهٔ $۱۹ \leq g(۴) \leq ۳۵$ قرار دارد و $g(۵)$ در $۳۷ \leq g(۵) \leq ۵۴$ صدق می‌کند. پژوهش بعدی (۱۹۶۴) نشان داده است که $g(۵) = ۳۷$. در خلال دههٔ اخیر، کران بالای $g(۴)$ به‌طور چشمگیری کاهش یافته است و براساس دقیقترین برآورد، $g(۴) \leq ۲۰$. همچنین، ثابت شده است که هر عدد صحیح کوچکتر از $۱۰^{۱۴۰}$ یا بزرگتر از $۱۰^{۳۶۷}$ را می‌توان به‌صورت مجموع حداکثر ۱۹ توان چهارم نوشت؛ بنابراین، علی‌الاصول $g(۴)$ را می‌توان محاسبه کرد. به‌نظر می‌رسد گزارش اخیر (۱۹۸۶) مبنی بر اینکه درواقع ۱۹ توان چهارم برای نمایش همهٔ عددهای صحیح کافی است، تکلیف این حالت را کاملاً روشن کرده باشد. تا جایی که مربوط به $k \geq ۶$ است، ثابت شده است که جز احتمالاً به‌ازای تعدادی متناهی از مقدارهای k، فرمول

$$g(k) = \left(\frac{۳}{۲}\right)^k + ۲^k - ۲$$

برقرار است. شواهد قابل توجهی درستی این فرمول را به‌ازای هر k تأیید می‌کنند.

به‌ازای $k \geq ۳$، برای نمایش همهٔ عددهای صحیح به اندازهٔ کافی بزرگ، کمتر از $g(k)$ توان kام لازم است. این نکته تعریفی کلی را القاء می‌کند: فرض می‌کنیم $G(k)$ نشان‌دهندهٔ کوچکترین عدد صحیح rای باشد با این ویژگی که هر عدد صحیح به‌اندازهٔ کافی بزرگ، مجموع حداکثر r توان kام است. واضح است که $G(k) \leq g(k)$. مقدارهای دقیق $G(k)$ فقط در دو حالت شناخته شده است یعنی، $G(۲) = ۴$ و $G(۴) = ۱۶$. نتیجهٔ لینیک دربارهٔ مکعبها نشان می‌دهد $G(۳) \leq ۷$، درحالی‌که ژاکوبی در ۱۸۵۱ حدس زده بود $۵ \leq G(۳)$. در سالهای اخیر ثابت شده است که $G(۵) \leq ۱۹$ و $G(۶) \leq ۲۹$.

مسألهٔ دیگری که توجه زیادی را به خود جلب کرده است این است که آیا می‌توان توان nامی را، که $n > ۳$، به‌صورت مجموع n توان nام نوشت؟ نخستین گام در جهت پاسخگویی به این پرسش در ۱۹۱۱ با کشف کوچکترین جواب برحسب توانهای چهارم برداشته شد:

$$۳۵۳^۴ = ۳۰^۴ + ۱۲۰^۴ + ۲۷۲^۴ + ۳۱۵^۴$$

1. Linnik

کوچکترین جواب برحسب توانهای پنجم عبارت است از

$$۷۲^۵ = ۱۹^۵ + ۴۳^۵ + ۴۶^۵ + ۴۷^۵ + ۶۷^۵$$

ولی هنوز در مورد توانهای ششم یا بالاتر جوابی دردست نیست.

پرسشی در این زمینه مطرح است: «آیا اصلاً می‌توان توان n امی را به‌صورت مجموع کمتر از n توان nام نوشت؟» اویلر حدس زد که این غیرممکن است، ولی در ۱۹۶۸، لاندر[1] و پارکین[2] نشان دادند:

$$۱۴۴^۵ = ۲۷^۵ + ۸۴^۵ + ۱۱۰^۵ + ۱۳۳^۵$$

در پرتو پیشرفتهای بعدی کامپیوتر، الکیز[3] (۱۹۸۷) توانست نشان دهد که در حالت توانهای چهارم، تعدادی نامتناهی مثال ناقضِ حدس اویلر وجود دارد. کوچکترین این مثالها عبارت است از

$$۴۲۲۴۸۱^۴ = ۹۵۸۰۰^۴ + ۲۱۷۵۱۹^۴ + ۴۱۴۵۶۰^۴$$

تمرینهای ۱۲ـ۳

۱. بدون جمع کردن مربعها، نشان دهید که رابطه‌های زیر برقرارند:

(الف) $۱^۲ + ۲^۲ + ۳^۲ + \ldots + ۲۳^۲ + ۲۴^۲ = ۷۰^۲$

(ب) $۱۸^۲ + ۱۹^۲ + ۲۰^۲ + \ldots + ۲۷^۲ + ۲۸^۲ = ۷۷^۲$

(پ) $۲^۲ + ۵^۲ + ۸^۲ + \ldots + ۲۳^۲ + ۲۶^۲ = ۴۸^۲$

(ت) $۶^۲ + ۱۲^۲ + ۱۸^۲ + \ldots + ۴۲^۲ + ۴۸^۲ = ۹۵^۲ - ۴۱^۲$

۲. رگیومونتانوس مسألهٔ تعیین بیست مربع را که مجموعشان مربعی بزرگتر از ۳۰۰۰۰۰ باشد، مطرح کرد. دو جواب برای این مسأله ارائه دهید. [راهنمایی: اتحاد

$$\begin{aligned}
&(a_۱^۲ + a_۲^۲ + \ldots + a_n^۲)^۲ \\
&= (a_۱^۲ + a_۲^۲ + \ldots + a_{n-۱}^۲ - a_n^۲)^۲ \\
&\quad + (۲a_۱a_n)^۲ + (۲a_۲a_n)^۲ + \ldots + (۲a_{n-۱}a_n)^۲
\end{aligned}$$

را درنظر بگیرید.]

۳. نشان دهید که اگر $۱^۲ + ۲^۲ + ۳^۲ + \ldots + k^۲$ ناماندهٔ درجهٔ دومی از $k + ۱$ باشد، $n^۲ + (n+۱)^۲ + (n+۲)^۲ + \ldots + (n+k)^۲$ مربع نیست.

---

1. Lander 2. Parkin 3. Elkies

۴. نشان دهید معادلهٔ $a^۲ + b^۲ + c^۲ + a + b + c = ۱$ جوابی برحسب عددهای صحیح ندارد. [راهنمایی: معادلهٔ موردنظر با معادلهٔ $(۲a + ۱)^۲ + (۲b + ۱)^۲ + (۲c + ۱)^۲ = ۷$ هم‌ارز است.]

۵. نشان دهید به‌ازای هر عدد صحیح مثبت n، یا n و یا $۲n$ مجموع سه مربع است.

۶. یکی از مسأله‌های حل‌نشده، بینهایت بودن یا نبودن تعداد عددهای اول p است به‌طوری‌که، به‌ازای $n > ۰$ ای، $p = n^۲ + (n + ۱)^۲ + (n + ۲)^۲$. سه مثال از چنین عددهای اولی پیدا کنید.

۷. در بررسی $n = ۴۵۹$، نمایشی به‌صورت مجموع دو مربع به‌دست نیاوردیم. ۴۵۹ را به‌صورت مجموع سه مربع بیان کنید.

۸. هریک از گزاره‌های زیر را ثابت کنید:

(الف) هر عدد صحیح فرد مثبت به‌صورت $a^۲ + b^۲ + ۲c^۲$ است که در آن a، b، c عددهایی صحیح‌اند. [راهنمایی: اگر $n > ۰$، $۴n + ۲$ را می‌توان به‌ازای x و y فردی و z زوجی به‌صورت $۴n + ۲ = x^۲ + y^۲ + z^۲$ نوشت. بنابراین

$$۲n + ۱ = \frac{۱}{۲}(x + y)^۲ + \frac{۱}{۲}(x - y)^۲ + ۲(z/۲)^۲.]$$

(ب) هر عدد صحیح مثبتی یا به‌صورت $a^۲ + b^۲ + c^۲$ و یا به‌صورت $a^۲ + b^۲ + ۲c^۲$ است که در آن، a، b، c عددهایی صحیح‌اند. [راهنمایی: اگر $n > ۰$ قابل نمایش به‌صورت $a^۲ + b^۲ + c^۲$ نباشد، آنگاه n به‌صورت $۴^m(۸k + ۷)$ است. قسمت (الف) را در مورد عدد صحیح فرد $۸k + ۷$ به‌کار ببرید.]

(پ) هر عدد صحیح مثبتی، به‌ازای عددهای صحیح a، b، c ای، به‌صورت $a^۲ + b^۲ - c^۲$ است. [راهنمایی: به‌ازای $n > ۰$، a را طوری انتخاب کنید که $n - a^۲$ عدد صحیح فرد مثبتی باشد و قضیهٔ ۱۲ـ۴ را به‌کار ببرید.]

۹. حکمهای زیر را ثابت کنید:

(الف) عدد صحیحی به‌صورت $۹k + ۴$ یا $۹k + ۵$ را نمی‌توان به‌صورت مجموع سه مکعب یا کمتر نوشت. [راهنمایی: توجه کنید که به‌ازای هر عدد صحیح a، (به پیمانهٔ ۹) $a^۳ \equiv ۰, ۱,$ یا ۸.]

(ب) $p = ۲$ تنها عدد اولی است که قابل نمایش به‌صورت مجموع دو مکعب است. [راهنمایی: از اتحاد $a^۳ + b^۳ = (a + b)[(a - b)^۲ + ab]$ استفاده کنید.]

(پ) عدد اول p را می‌توان به‌صورت تفاضل دو مکعب نوشت اگر و تنها اگر، به‌ازای k ای، $p = ۳k(k + ۱) + ۱$.

۱۰. هریک از عددهای اول ۷، ۱۹، ۳۷، ۶۱، و ۱۲۷ را به‌صورت تفاضل دو مکعب بنویسید.

۱۱. ثابت کنید هر عدد صحیح مثبتی را می‌توان به‌صورت مجموع سه عدد مثلثی یا کمتر نوشت. [راهنمایی: به‌ازای $n > ۰$، $۸n + ۳$ را به‌صورت مجموع سه مربع فرد بنویسید و سپس n را با حل معادلهٔ حاصل به‌دست آورید.]

۱۲. نشان دهید تعداد نامتناهی عدد اول p به‌صورت $p = a^۲ + b^۲ + c^۲ + ۱$، که در آن a، b و c عددهایی صحیح‌اند، وجود دارد. [راهنمایی: بنا به قضیه ۹ـ۸، تعداد نامتناهی عدد اول به‌صورت $p = ۸k + ۷$ وجود دارد. به‌ازای a، b، و c ای، بنویسید $p - ۱ = ۸k + ۶ = a^۲ + b^۲ + c^۲$.]

۱۳. عددهای صحیح $۲۳۱ = ۳ \times ۷ \times ۱۱$، $۳۹۱ = ۱۷ \times ۲۳$، و $۲۱۰۹ = ۳۷ \times ۵۷$ را به‌صورت مجموعهای چهار مربع بنویسید.

۱۴. (الف) ثابت کنید هر عدد صحیح $n \geq ۱۷۰$ مجموع پنج مربع ناصفر است. [راهنمایی: به‌ازای عددهای صحیح a، b، c، d ای $n - ۱۶۹$ را به‌صورت $a^۲ + b^۲ + c^۲ + d^۲$ بنویسید و حالتهایی را که حداقل یکی از a، b، c صفر باشد، درنظر بگیرید.]

(ب) ثابت کنید هر مضرب مثبتی از ۸، مجموع هشت عدد مربع فرد است. [راهنمایی: اگر $n = a^۲ + b^۲ + c^۲ + d^۲$، آنگاه $۸n + ۸$ مجموع مربعات $۲a \pm ۱$، $۲b \pm ۱$، $۲c \pm ۱$، و $۲d \pm ۱$ است.]

۱۵. با استفاده از اتحاد $n^۳ \equiv n$ (به پیمانهٔ ۶) نتیجه بگیرید که هر عدد صحیح n را می‌توان به‌صورت مجموع مکعبهای پنج عدد صحیح مثبت یا منفی نوشت. [راهنمایی: از اتحاد $n^۳ - ۶k = n^۳ - (k + ۱)^۳ - (k - ۱)^۳ + k^۳ + k^۳$ استفاده کنید.]

۱۶. ثابت کنید هر عدد صحیح فرد، مجموع چهار مربع است که دوتای آنها متوالی‌اند. [راهنمایی: به‌ازای $n > ۰$، $۴n + ۱$ مجموع سه مربع است که تنها یکی از آنها فرد است؛ به‌علاوه، از $۴n + ۱ = (۲a)^۲ + (۲b)^۲ + (۲c + ۱)^۲$ نتیجه می‌شود $۲n + ۱ = (a + b)^۲ + (a - b)^۲ + c^۲ + (c + ۱)^۲$.]

۱۷. ثابت کنید تعداد عددهایی مثلثی که هم به‌صورت مجموع دو مکعب و هم به‌صورت تفاضل دومکعب قابل نمایش‌اند، نامتناهی است. نمایشهای یکی از چنین اعداد مثلثی را ارائه دهید. [راهنمایی: در اتحاد

$$\begin{aligned}(۲۷k^۶)^۲ - ۱ &= (۹k^۴ - ۳k)^۳ + (۹k^۳ - ۱)^۳\\ &= (۹k^۴ + ۳k)^۳ - (۹k^۳ + ۱)^۳\end{aligned}$$

k را عددی صحیح فرد درنظر بگیرید و نتیجه بگیرید

$$(۲n+۱)^۲ - ۱ = (۲a)^۳ + (۲b)^۳ = (۲c)^۳ - (۲d)^۳$$

یا معادلش، $t_n = a^۳ + b^۳ = c^۳ - d^۳$.]

۱۸. (الف) اگر هر دوی $n - ۱$ و $n + ۱$ اول باشند، نشان دهید عدد صحیح $۲n^۲ + ۲$ را می‌توان به‌صورت مجموع ۲، ۳، ۴، و ۵ مربع نوشت.

(ب) درستی قسمت (الف) را به‌ازای $n = ۴, ۶, ۱۲$ نشان دهید.

۱۳

عددهای فیبوناتچی و کسرهای مسلسل

«... آنچه مادی است، تابع قانونهای ریاضی است، و آنچه معنوی است، تابع قانونهای الهی؛ و قانونهای ریاضی چیزی جز بیان اندیشه‌های الهی نیستند.»

توماس هیل

۱۳ـ۱ دنبالهٔ فیبوناتچی

شاید بزرگترین ریاضیدان سده‌های میانه لئوناردوی پیسایی[1] باشد که نوشته‌هایش را با نام فیبوناتچی، مخفف فیلیوس بوناتچی[2] یعنی پسر بوناتچی، منتشر می‌کرد. دستگاه رقمهای هندی ـ عربی از طریق کتاب او، لیبر آباکی [کتاب محاسبه]، که در ۱۲۰۲ نوشته شد و فقط نسخهٔ تجدیدنظر شدهٔ آن در ۱۲۲۸ به‌جا مانده است، به اروپای غربی راه یافت. نکتهٔ طنزآمیز این است که علی‌رغم دستاوردهای متعدد فیبوناتچی، بیشتر معروفیت او به این دلیل است که ادوارد لوکاس متخصص نظریهٔ اعداد در سدهٔ نوزدهم، نام او را روی دنباله‌ای گذاشت که در مسألهٔ ساده‌ای در لیبر آباکی دیده می‌شود. به بیان دقیق، فیبوناتچی مسألهٔ زیر را در ارتباط با تعداد خرگوشهای تولید شده از

1. Leonardo of Pisa 2. filius Bonacci

قِبَلِ زوجی خرگوش خیالی مطرح کرد:

> شخصی یک زوج خرگوش [نر و ماده] را در محلی کاملاً محصور قرار می‌دهد. اگر طبیعت این خرگوشها طوری باشد که هر زوج هر ماه یک زوج دیگر تولید کند که آن هم از ماه دوم بعد از تولد، زاد و ولد کند، در ظرف یک سال چند زوج خرگوش از قِبَلِ زوج اولیه تولید می‌شود؟

به فرض اینکه هیچ یک از خرگوشها نمیرد، در خلال ماه نخست زوجی متولد می‌شود، بنابراین دو زوج موجود است. در خلال ماه دوم، زوج اولیه زوج دیگری تولید می‌کند. ماه بعد زوج اولیه و نیز زوجی که زودتر متولد شده هر یک زوجی تولید می‌کنند، و بنابراین سه زوج بالغ و دو زوج نابالغ موجود خواهد بود، و الی آخر. (آمار مربوطه در جدول زیر ملاحظه می‌شود.)

رشد جامعهٔ خرگوشها

ماه	زوجهای بالغ	زوجهای نابالغ	مجموع
۱	۱	۱	۲
۲	۲	۱	۳
۳	۳	۲	۵
۴	۵	۳	۸
۵	۸	۵	۱۳
۶	۱۳	۸	۲۱
۷	۲۱	۱۳	۳۴
۸	۳۴	۲۱	۵۵
۹	۵۵	۳۴	۸۹
۱۰	۸۹	۵۵	۱۴۴
۱۱	۱۴۴	۸۹	۲۳۳
۱۲	۲۳۳	۱۴۴	۳۷۷

نکته‌ای که باید درنظر داشت این است که هرماه زوجهای نابالغ رشد می‌کنند و بالغ می‌شوند و بنابراین درایهٔ «بالغ» جدید در جدول برابر با درایهٔ «بالغ» قبلی به‌علاوهٔ درایهٔ «نابالغ» قبلی است. هر یک از زوجهای بالغ ماه پیش زوج نابالغی تولید می‌کنند، بنابراین درایهٔ «نابالغ» جدید برابر با درایهٔ «بالغ» قبلی است.

اگر این فرایند به‌طور نامتناهی ادامه یابد، دنبالهٔ حاصل در مسألهٔ خرگوش، یعنی

$$۱, ۱, ۲, ۳, ۵, ۸, ۱۳, ۲۱, ۳۴, ۵۵, ۸۹, ۱۴۴, ۲۳۳, ۳۷۷, \ldots$$

دنبالهٔ فیبوناتچی، و جمله‌هایش، عددهای فیبوناتچی، نامیده می‌شوند. مکان هر عدد در این دنباله معمولاً با اندیسی مشخص می‌شود، مانند $u_۱ = ۱$، $u_۲ = ۱$، $u_۳ = ۲$، و الی آخر؛ بنابراین u_n

نشان‌دهندهٔ nامین عدد فیبوناتچی است.

دنبالهٔ فیبوناتچی دارای ویژگی جالب توجهی است، یعنی،

$$\begin{aligned} u_۳ &= u_۲ + u_۱ & \text{یا} && ۲ &= ۱ + ۱ \\ u_۴ &= u_۳ + u_۲ & \text{یا} && ۳ &= ۲ + ۱ \\ u_۵ &= u_۴ + u_۳ & \text{یا} && ۵ &= ۳ + ۲ \\ u_۶ &= u_۵ + u_۴ & \text{یا} && ۸ &= ۵ + ۳ \end{aligned}$$

تا اینجا، قاعدهٔ کلی تشکیل دنباله باید مشخص شده باشد:

$$u_۱ = u_۲ = ۱ \text{، و به‌ازای } n \geq ۳ \text{،} \quad u_n = u_{n-۱} + u_{n-۲}$$

یعنی، هر جملهٔ دنباله (بعد از دومین جمله) برابر با مجموع دو جملهٔ بلافصل قبلی است. چنین دنباله‌هایی، که در آنها از مرحله‌ای به بعد، هر جمله را بتوان به‌صورت ترکیبی خطی از جمله‌های قبلی نمایش داد، دنباله‌های بازگشتی نامیده می‌شوند. دنبالهٔ فیبوناتچی نخستین دنبالهٔ بازگشتی شناخته شده در ریاضیات است. احتمالاً خود فیبوناتچی متوجه طبیعت بازگشتی دنباله‌اش بود، ولی نخستین بار در ۱۶۳۴ بود که، با پیشرفت کافی در نمادگذاری ریاضی، آلبر ژیرار فرمول آن را نوشت.

شاید متوجه شده باشید که در بخشی از دنبالهٔ فیبوناتچی که نوشته‌ایم، جمله‌های متوالی متباین‌اند. اکنون ثابت می‌کنیم که این امر تصادفی نیست.

قضیهٔ ۱۳ـ۱ در دنبالهٔ فیبوناتچی به‌ازای هر $n \geq ۱$، $\gcd(u_n, u_{n+۱}) = ۱$.

اثبات. فرض می‌کنیم عدد صحیح $d > ۱$ هر دوی u_n و $u_{n+۱}$ را می‌شمارد. در این‌صورت لازم می‌آید تفاضلشان یعنی $u_{n+۱} - u_n = u_{n-۱}$ نیز بر d بخشپذیر باشد. از این و از رابطهٔ $u_n - u_{n-۱} = u_{n-۲}$، نتیجه می‌شود $d|u_{n-۲}$. تکرار قهقرایی این استدلال نشان می‌دهد که $d|u_{n-۳}$، $d|u_{n-۴}$، ...، و بالاخره $d|u_۱$. ولی $u_۱ = ۱$، که قطعاً بر هیچ $d > ۱$ بخشپذیر نیست. با این تناقض اثبات به انجام می‌رسد. □

چون $u_۳ = ۲$، $u_۵ = ۵$، $u_۷ = ۱۳$، و $u_{۱۱} = ۸۹$ همگی عددهایی اول هستند، ممکن است تصور شود که به‌ازای هر اندیس اول $n > ۲$، u_n عددی اول است. این تصور به‌زودی نقش برآب می‌شود زیرا با اندک کندوکاوی معلوم می‌شود که

$$u_{۱۹} = ۴۱۸۱ = ۳۷ \times ۱۱۳$$

نه تنها روشی برای پیش‌بینی u_nهای اول در دست نیست، بلکه حتی، نامتناهی بودن تعداد عددهای فیبوناتچی اول نیز معلوم نیست. مع‌الوصف، حکم مثبت سودمندی وجود دارد که اثباتش را به‌دلیل پیچیدگی نمی‌آوریم: به‌ازای هر عدد اول p، تعداد نامتناهی عدد فیبوناتچی بخشپذیر بر p وجود دارد و اینها در دنبالهٔ فیبوناتچی به فاصلهٔ مساوی توزیع شده‌اند. به‌عنوان مثال، عدد ۳ هر جملهٔ چهارم دنبالهٔ فیبوناتچی، ۵ هر جملهٔ پنجم، و ۷ هر جملهٔ هشتم را می‌شمارد.

همان‌طور که می‌دانیم، بزرگترین مقسوم‌علیه مشترک دو عدد صحیح مثبت را می‌توان با الگوریتم اقلیدسی پس از تقسیماتی به دفعات متناهی به‌دست آورد. با انتخاب مناسب عددهای صحیح، تعداد دفعات تقسیم مورد نیاز را می‌توان به دلخواه افزایش داد. صورت دقیق قضیه این است: به‌ازای هر $n > ۰$، عددهای صحیح مثبت a و bای وجود دارند به‌طوری که برای محاسبهٔ بزرگترین مقسوم‌علیه مشترک a و b با الگوریتم اقلیدسی دقیقاً n بار تقسیم مورد نیاز است. برای اثبات، کافی است فرض کنیم $a = u_{n+۲}$ و $b = u_{n+۱}$. الگوریتم اقلیدسی برای تعیین $\gcd(u_{n+۲}, u_{n+۱})$ به دستگاه معادله‌های

$$\begin{aligned} u_{n+۲} &= ۱ \times u_{n+۱} + u_n \\ u_{n+۱} &= ۱ \times u_n + u_{n-۱} \\ &\vdots \\ u_۴ &= ۱ \times u_۳ + u_۲ \\ u_۳ &= ۲ \times u_۲ + ۰ \end{aligned}$$

منجر می‌شود. تعداد دفعات تقسیم مورد نیاز در اینجا به‌وضوح n است. بی‌گمان، خواننده به‌خاطر دارد که آخرین باقیماندهٔ ناصفر در الگوریتم تقسیم، مقدار $\gcd(u_{n+۲}, u_{n+۱})$ را به‌دست می‌دهد. پس

$$\gcd(u_{n+۲}, u_{n+۱}) = u_۲ = ۱$$

و این تأیید دیگری است بر متباین بودن جمله‌های متوالی فیبوناتچی.

به‌عنوان مثال، فرض می‌کنیم $n = ۶$. محاسبه‌های زیر نشان می‌دهند که برای تعیین بزرگترین مقسوم‌علیه مشترک عددهای صحیح $u_۸ = ۲۱$ و $u_۷ = ۱۳$، ۶ تقسیم ضروری است:

$$\begin{aligned} ۲۱ &= ۱ \times ۱۳ + ۸ \\ ۱۳ &= ۱ \times ۸ + ۵ \\ ۸ &= ۱ \times ۵ + ۳ \\ ۵ &= ۱ \times ۳ + ۲ \end{aligned}$$

$$\text{۳} = \text{۱} \times \text{۲} + \text{۱}$$
$$\text{۲} = \text{۲} \times \text{۱} + \text{۰}$$

یکی از جنبه‌های جالب توجه دنبالهٔ فیبوناتچی این است که بزرگترین مقسوم‌علیه مشترک دو عدد فیبوناتچی، خود عددی فیبوناتچی است. اتحاد

$$u_{m+n} = u_{m-\text{۱}}u_n + u_m u_{n+\text{۱}} \tag{۱}$$

در اثبات این نکته بسیار مهم است. به‌ازای m ثابت، این اتحاد به استقرا بر n ثابت می‌شود. اگر $n = \text{۱}$، (۱) به‌صورت

$$u_{m+\text{۱}} = u_{m-\text{۱}}u_\text{۱} + u_m u_\text{۲} = u_{m-\text{۱}} + u_m$$

درمی‌آید که به وضوح برقرار است. بنابراین فرض می‌کنیم فرمول مورد بحث به‌ازای $n = \text{۱}, \text{۲}, \ldots, k$ برقرار است و برقراری آن‌را به‌ازای $n = k + \text{۱}$ ثابت می‌کنیم. بنا به فرض استقرا

$$u_{m+k} = u_{m-\text{۱}}u_k + u_m u_{k+\text{۱}}$$
$$u_{m+(k-\text{۱})} = u_{m-\text{۱}}u_{k-\text{۱}} + u_m u_k$$

از جمع این دو معادله نتیجه می‌شود

$$u_{m+k} + u_{m+(k-\text{۱})} = u_{m-\text{۱}}(u_k + u_{k-\text{۱}}) + u_m(u_{k+\text{۱}} + u_k)$$

پس بنا به تعریف دنبالهٔ فیبوناتچی

$$u_{m+(k+\text{۱})} = u_{m-\text{۱}}u_{k+\text{۱}}u_m u_{k+\text{۲}}$$

که همان فرمول (۱) است وقتی $k + \text{۱}$ جایگزین n شده باشد. بنابراین، مرحلهٔ استقرا کامل است و (۱) به‌ازای هر m و nای برقرار است.

آوردن یک مثال از فرمول (۱) باید کافی باشد:

$$u_\text{۹} = u_{\text{۶}+\text{۳}} = u_\text{۵}u_\text{۳} = \text{۵} \times \text{۲} + \text{۸} \times \text{۳} = \text{۳۴}$$

قضیهٔ بعدی، صرف‌نظر از اهمیتی که برای نتیجهٔ نهایی موردنظر ما دارد، خود به خود نیز جذاب است.

قضیهٔ ۱۳ـ۲ اگر $m \geq ۱$، $n \geq ۱$، آنگاه u_{mn} بر u_m بخشپذیر است.

اثبات. دوباره به استقرا بر n استدلال می‌کنیم. حکم قطعاً به‌ازای $n = ۱$ برقرار است. به‌عنوان فرض استقرا، فرض می‌کنیم که به‌ازای $n = ۱, ۲, \ldots, k$، u_{mn} بر u_m بخشپذیر است. رسیدن به حالت $u_{m(k+۱)} = u_{mk+m}$ با استفاده از فرمول (۱) صورت می‌پذیرد: در واقع

$$u_{m(k+۱)} = u_{mk-۱}u_m + u_{mk}u_{m+۱}$$

چون بنا به فرض u_{mk} بر u_m بخشپذیر است، طرف راست برابری فوق (و بنابراین، طرف چپ نیز) باید بر u_m بخشپذیر باشد. پس طبق انتظار، $u_m | u_{m(k+۱)}$. □

پیش از محاسبهٔ $\gcd(u_m, u_n)$، لمی فنی ارائه می‌دهیم.

لم. اگر $m = qn + r$، آنگاه $\gcd(u_m, u_n) = \gcd(u_r, u_n)$.

اثبات. با استفاده از فرمول (۱) می‌توانیم بنویسیم

$$\begin{aligned} \gcd(u_m, u_n) &= \gcd(u_{qn+r}, u_n) \\ &= \gcd(u_{qn-۱}u_r + u_{qn}u_{r+۱}, u_n) \end{aligned}$$

با توسل به قضیهٔ ۱۳ـ۲ و اینکه به‌شرط $b|c$ داریم $\gcd(a+c, b) = \gcd(a, b)$، نتیجه می‌شود

$$\gcd(u_{qn-۱}u_r + u_{qn}u_{r+۱}, u_n) = \gcd(u_{qn-۱}u_r, u_n)$$

ادعا می‌کنیم $\gcd(u_{qn-۱}, u_n) = ۱$. برای نشان دادن این مطالب، قرار می‌دهیم $d = \gcd(u_{qn-۱}, u_n)$. از رابطه‌های $d|u_n$ و $u_n|u_{qn}$ نتیجه می‌شود $d|u_{qn}$، و بنابراین d مقسوم‌علیه مشترک (مثبتی) از عددهای فیبوناتچی متوالی $u_{qn-۱}$ و u_{qn} است. چون عددهای فیبوناتچی متوالی متباین‌اند، نتیجه می‌گیریم $d = ۱$.

برای تکمیل اثبات، خواننده باید نشان دهد که هرگاه $\gcd(c, d) = ۱$، آنگاه $\gcd(a, bc) = \gcd(a, b)$. با معلوم بودن این موضوع، بلافاصله به‌دست می‌آوریم

$$\gcd(u_m, u_n) = \gcd(u_{qn-۱}u_r, u_n) = \gcd(u_r, u_n)$$

که نتیجهٔ مطلوب است. □

با در دست داشتن این لم، دیگر کاری جز تلفیق نتیجه‌های حاصل نمانده است.

قضیهٔ ۱۳ـ۳ بزرگترین مقسوم‌علیه مشترک دو عدد فیبوناتچی، باز عددی فیبوناتچی است؛ به‌طور مشخص

$$\gcd(u_m, u_n) = u_d \quad \text{که در آن} \quad d = \gcd(m, n)$$

اثبات. فرض کنیم $m \geq n$. با کاربرد الگوریتم اقلیدسی در مورد m و n دستگاه معادله‌های زیر را به‌دست می‌آوریم

$$\begin{array}{ll}
m = q_1 n + r_1 & 0 < r_1 < n \\
n = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 &
\end{array}$$

بنا به لم فوق داریم

$$\begin{aligned}
\gcd(u_m, u_n) &= \gcd(u_{r_1}, u_n) = \gcd(u_{r_1}, u_{r_2}) \\
&= \ldots = \gcd(u_{r_{n-1}}, u_{r_n})
\end{aligned}$$

چون $r_n | r_{n-1}$، از قضیهٔ ۱۳ـ۲ نتیجه می‌شود $u_{r_n} | u_{r_{n-1}}$، و بنابراین $\gcd(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$. ولی r_n که آخرین باقیماندهٔ ناصفر در الگوریتم اقلیدسی به‌ازای m و n است، برابر با $\gcd(m, n)$ است. از این رو

$$\gcd(u_m, u_n) = u_{\gcd(m,n)}$$

و به این ترتیب قضیه ثابت می‌شود. □

جالب توجه است که عکس قضیهٔ ۱۳ـ۲ را می‌توان از این قضیه نتیجه گرفت؛ به بیان دیگر، اگر u_n بر u_m بخشپذیر باشد، می‌توانیم نتیجه بگیریم که n بر m بخشپذیر است. در واقع، اگر $u_m | u_n$، آنگاه $\gcd(u_m, u_n) = u_m$. ولی، بنا به قضیهٔ ۱۳ـ۳، مقدار $\gcd(u_m, u_n)$ باید برابر با $u_{\gcd(m,n)}$ باشد. پس $\gcd(m, n) = m$، و بنابراین $m | n$. این ملاحظات را به‌صورت زیر جمعبندی می‌کنیم:

فرع. در دنبالهٔ فیبوناتچی، $u_m | u_n$ اگر و تنها اگر $m | n$ و $m \geq 2$.

محاسبهٔ $\gcd(u_{۱۶}, u_{۱۲}) = \gcd(۹۸۷, ۱۴۴)$، مثال خوبی از قضیهٔ ۱۳ـ۳ است. با استفاده از الگوریتم اقلیدسی داریم

$$۹۸۷ = ۶ \times ۱۴۴ + ۱۲۳$$
$$۱۴۴ = ۱ \times ۱۲۳ + ۲۱$$
$$۱۲۳ = ۵ \times ۲۱ + ۱۸$$
$$۲۱ = ۱ \times ۱۸ + ۳$$
$$۱۸ = ۶ \times ۳ + ۰$$

و بنابراین $\gcd(۹۸۷, ۱۴۴) = ۳$. یعنی، موافق با حکم قضیهٔ ۱۳ـ۳ داریم

$$\gcd(u_{۱۶}, u_{۱۲}) = ۳ = u_{۴} = u_{\gcd(۱۶,۱۲)}$$

تمرینهای ۱۳ـ۱

۱. می‌دانیم که به‌ازای هر عدد اول $p \neq ۵$، یا $u_{p-۱}$ و یا $u_{p+۱}$ بر p بخشپذیر است. صحت این مطلب را به‌ازای عددهای اول ۷، ۱۱، ۱۳، و ۱۷ نشان دهید.

۲. نشان دهید که به‌ازای $n = ۱, ۲, \ldots ۱۰$، $۵u_n^۲ + ۴(-۱)^n$ همیشه مربعی کامل است.

۳. ثابت کنید اگر $۲|u_n$، آنگاه $۴|(u_{n+۱}^۲ - u_{n-۱}^۲)$؛ همچنین، اگر $۳|u_n$، آنگاه $۹|(u_{n+۱}^۳ - u_{n-۱}^۳)$.

۴. ثابت کنید که در دنبالهٔ فیبوناتچی

(الف) $u_{n+۳} \equiv u_n$ (به پیمانهٔ ۲)، بنابراین $u_۳$، $u_۶$، $u_۹$، ... همگی عددهای صحیح زوجی هستند؛

(ب) $u_{n+۵} \equiv ۳u_n$ (به پیمانهٔ ۵)، بنابراین $u_۵$، $u_{۱۰}$، $u_{۱۵}$، ...، همگی بر ۵ بخشپذیرند.

۵. نشان دهید مجموع مربعهای n عدد فیبوناتچی نخست را می‌توان از فرمول

$$u_۱^۲ + u_۲^۲ + u_۳^۲ + \ldots + u_n^۲ = u_n\, u_{n+۱}$$

نتیجه گرفت. [راهنمایی: به‌ازای $n \geq ۲$، $u_n^۲ = u_n u_{n+۱} - u_n u_{n-۱}$.]

۶. با استفاده از اتحاد تمرین ۵ ثابت کنید که به‌ازای $n \geq ۳$ داریم

$$u_{n+۱}^۲ = u_n^۲ + ۳u_{n-۱}^۲ + ۲(u_{n-۲}^۲ + u_{n-۱}^۲ + \ldots + u_۲^۲ + u_۱^۲)$$

۷. $\gcd(u_۹, u_{۱۲})$، $\gcd(u_{۱۵}, u_{۲۰})$، و $\gcd(u_{۲۴}, u_{۳۶})$ را حساب کنید.

۸. عددهای فیبوناتچی‌ای پیدا کنید که هم $u_{۲۴}$ و هم $u_{۳۶}$ را بشمارند.

۹. با استفاده از فرع قضیهٔ ۱۳ـ۳، درستی هر یک از حکمهای زیر را نشان دهید.

(الف) $۲|u_n$ اگر و تنها اگر $۳|n$

(ب) $۳|u_n$ اگر و تنها اگر $۴|n$

(پ) $۴|u_n$ اگر و تنها اگر $۶|n$

(ت) $۵|u_n$ اگر و تنها اگر $۵|n$

۱۰. اگر $\gcd(m,n) = ۱$، ثابت کنید به‌ازای هر $m, n \geq ۱$، u_{mn} بر $u_m u_n$ بخشپذیر است.

۱۱. می‌توان نشان داد که اگر r باقیماندهٔ تقسیم u_n بر u_m باشد $(n > m)$، آنگاه یا r یا $u_m - r$ عددی فیبوناتچی است. برای هرحالت مثالی ارائه کنید.

۱۲. حدس زده می‌شود که فقط پنج عدد فیبوناتچی وجود دارند که در عین حال، عددهایی مثلثی نیز هستند. اینها را پیدا کنید.

۱۳. ثابت کنید که به‌ازای $n \geq ۱$، (به پیمانهٔ ۵) $۲^{n-۱} u_n \equiv n$. [راهنمایی: از استقرا و نیز از رابطهٔ $۲^n u_{n+۱} = ۲(۲^{n-۱} u_n) + ۴(۲^{n-۲} u_{n-۱})$ استفاده کنید.]

۱۴. اگر به‌ازای nای ناکمتر از ۳، $u_n < a < u_{n+۱} < b < u_{n+۲}$، ثابت کنید مجموع $a + b$ نمی‌تواند عددی فیبوناتچی باشد.

۱۵. ثابت کنید عدد صحیح مثبت nای وجود ندارد که به‌ازای آن

$$u_۱ + u_۲ + u_۳ + \ldots + u_{۲n} = ۱۶!$$

[راهنمایی: بنا به قضیهٔ ویلسن، این معادله هم‌ارز با (به پیمانهٔ ۱۷) $u_{۲n+۲} \equiv ۰$ است. چون $۱۷|u_۹$، $۱۷|u_m$ اگر و تنها اگر $۹|m$.]

۱۶. اگر $n + m$ بر ۳ بخشپذیر باشد، نشان دهید $u_{n-m-۱} u_n + u_{n-m} u_{n+۱}$ عدد صحیح زوجی است.

۱۷. نشان دهید که به‌ازای $n \geq ۱$، n عدد فیبوناتچی متوالی مرکب وجود دارد.

۱۸. ثابت کنید $۹|u_{n+۲۴}$ اگر و تنها اگر $۹|u_n$. [راهنمایی: با استفاده از فرمول (۱) نشان دهید (به‌پیمانهٔ ۹) $u_{n+۲۴} \equiv u_n$.]

۱۹. با استفاده از استقرا نشان دهید که به‌ازای $n \geq ۱$، (به پیمانهٔ ۵) $u_{۲n} \equiv n(-۱)^{n+۱}$.

۲۰. اتحاد

$$u_{n+۲} = ۳u_{n+۱} - u_{n-۱} \qquad n \geq ۲$$

را ثابت کنید. [راهنمایی: فرمول (۱) را به‌کار ببرید.]

۲ـ۱۳ اتحادهایی مربوط به عددهای فیبوناتچی

در ادامهٔ بحث، چند اتحاد اساسی در مورد عددهای فیبوناتچی به‌دست می‌آوریم؛ اینها در حل تمرینهای آخر بخش سودمندند. یکی از ساده‌ترینِ این اتحادها، حاکی است که مجموع n عدد فیبوناتچی نخست برابر با $u_{n+۲} - ۱$ است. به‌عنوان نمونه، اگر هشت عدد فیبوناتچی نخست با هم جمع شوند، به‌دست می‌آوریم

$$۱ + ۱ + ۲ + ۳ + ۵ + ۸ + ۱۳ + ۲۱ = ۵۴ = ۵۵ - ۱ = u_{۱۰} - ۱$$

اینکه در حالت کلی نیز چنین است، با جمع رابطه‌های

$$\begin{aligned} u_۱ &= u_۳ - u_۲ \\ u_۲ &= u_۴ - u_۳ \\ u_۳ &= u_۵ - u_۴ \\ &\vdots \\ u_{n-۱} &= u_{n+۱} - u_n \\ u_n &= u_{n+۲} - u_{n-۱} \end{aligned}$$

معلوم می‌شود، زیرا می‌بینیم که سمت چپ برابر با مجموع n عدد نخست فیبوناتچی است در حالی‌که در سمت راست، جمله‌ها دو به دو حذف می‌شوند و فقط $u_{n+۲} - u_۲$ باقی می‌ماند. نتیجه اینکه

$$u_۱ + u_۲ + u_۳ + \ldots + u_n = u_{n+۲} - ۱ \qquad (۲)$$

ویژگی قابل ذکر دیگری از اعداد فیبوناتچی، اتحاد

$$u_n^۲ = u_{n+۱}u_{n-۱} + (-۱)^{n-۱} \qquad n \geq ۲ \qquad (۳)$$

است. درستی این اتحاد را مثلاً به‌ازای $n = ۶$ و $n = ۷$، می‌توان ملاحظه کرد:

$$\begin{aligned} u_۶^۲ &= ۸^۲ = ۱۳ \times ۵ - ۱ = u_۷u_۵ - ۱ \\ u_۷^۲ &= ۱۳^۲ = ۲۱ \times ۸ + ۱ = u_۸u_۶ + ۱ \end{aligned}$$

برای اثبات فرمول (۳)، نخست می‌نویسیم

$$\begin{aligned} u_n^۲ - u_{n+۱}u_{n-۱} &= u_n(u_{n-۱} + u_{n-۲}) - u_{n+۱}u_{n-۱} \\ &= (u_n - u_{n+۱})u_{n-۱} + u_nu_{n-۲} \end{aligned}$$

بنا به قاعدهٔ تشکیل دنبالهٔ فیبوناتچی داریم $u_{n+۱} = u_n + u_{n-۱}$، و بنابراین با قرار دادن جملهٔ

$-u_{n-1}$ به‌جای عبارت داخل پرانتز نتیجه می‌شود

$$u_n^2 - u_{n+1}u_{n-1} = (-1)(u_{n-1}^2 - u_n u_{n-2})$$

نکتهٔ مهم این است که صرف‌نظر از علامت اولیه، سمت راست این رابطه عین سمت چپ آن است با این تفاوت که در سمت راست، از همهٔ اندیسها یک واحد کاسته شده است. با تکرار استدلال می‌توان نشان داد که $u_{n-1}^2 - u_n u_{n-2}$ برابر با $(-1)(u_{n-2}^2 - u_{n-1}u_{n-3})$ است، و بنابراین

$$u_n^2 - u_{n+1}u_{n-1} = (-1)^2(u_{n-2}^2 - u_{n-1}u_{n-3})$$

کار را به همین نحو ادامه می‌دهیم. پس از $n-2$ مرحله، به

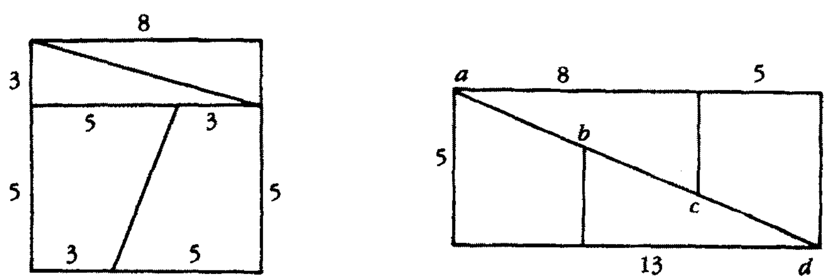
$$\begin{aligned} u_n^2 - u_{n+1}u_{n-1} &= (-1)^{n-2}(u_2^2 - u_3u_1) \\ &= (-1)^{n-2}(1^2 - 2\times 1) = (-1)^{n-1} \end{aligned}$$

می‌رسیم که در پی اثبات آن بودیم

به‌ازای $n = 2k$، فرمول (۳) به‌صورت

$$u_{2k}^2 = u_{2k+1}u_{2k-1} - 1 \qquad (4)$$

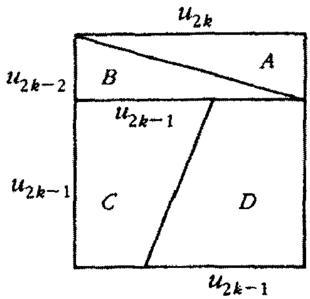
در می‌آید. این اتحاد مبنای ترفند هندسی معروفی است برای تقسیم مربعی به ضلع ۸ واحد به قطعه‌هایی که ظاهراً می‌توان با کنار هم گذاشتن آنها مستطیلی ۵ در ۱۳ ساخت. برای انجام این کار، مربع را، طبق شکل سمت چپ در زیر به چهار قسمت تقسیم می‌کنیم و قطعه‌ها را به‌طوری که در سمت راست نشان داده شده، کنار هم می‌چینیم.



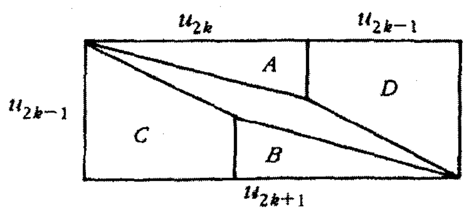
مساحت مربع $64 = 8^2$ است، درحالی‌که مساحت مستطیل که به‌نظر می‌رسد اجزای تشکیل‌دهندهٔ آن عین اجزای مربع باشند $65 = 13 \times 5$ است، و بنابراین مساحت مستطیل ظاهراً ۱ واحد

مربع بیشتر است. توضیح معما آسان است: نقطه‌های a، b، c، d همگی بر قطر مستطیل واقع نیستند، بلکه رأسهای متوازی‌الاضلاعی‌اند که مساحت آن البته برابر با یک واحد مساحت اضافی است.

این ترفند را می‌توان در مورد هر مربعی که ضلعهایش برابر با عدد فیبوناتچی u_{2k}ای باشد اجرا کرد. اگر مربع به روشی که در زیر ملاحظه می‌شود، تقسیم گردد،



می‌توان قطعه‌ها را طوری کنار هم چید که یک مستطیل با شکافی به شکل یک متوازی‌الاضلاع باریک ایجاد شود (شکل ما تا اندازه‌ای مبالغه‌آمیز است).



تعبیری از اتحاد $u_{2k-1}u_{2k+1} - 1 = u_{2k}^2$ این است که مساحت مربع اولیه دقیقاً برابر با مساحت مستطیل منهای مساحت متوازی‌الاضلاع است. می‌توان نشان داد که ارتفاع بزرگتر متوازی‌الاضلاع برابر با

$$\frac{1}{\sqrt{u_{2k}^2 + u_{2k-2}^2}}$$

است. اگر مقدار u_{2k} در حد معقولی بزرگ باشد (مثلاً $u_{2k} = 144$، که در این‌صورت $u_{2k-2} = 55$)، آنگاه شکاف به‌اندازه‌ای باریک است که تقریباً قابل رؤیت با چشم نیست.

فهرست پنجاه عدد فیبوناتچی نخست			
$u_{۱}$	۱	$u_{۲۶}$	۱۲۱۳۹۳
$u_{۲}$	۱	$u_{۲۷}$	۱۹۶۴۱۸
$u_{۳}$	۲	$u_{۲۸}$	۳۱۷۸۱۱
$u_{۴}$	۳	$u_{۲۹}$	۵۱۴۲۲۹
$u_{۵}$	۵	$u_{۳۰}$	۸۳۲۰۴۰
$u_{۶}$	۸	$u_{۳۱}$	۱۳۴۶۲۶۹
$u_{۷}$	۱۳	$u_{۳۲}$	۲۱۷۸۳۰۹
$u_{۸}$	۲۱	$u_{۳۳}$	۳۵۲۴۵۷۸
$u_{۹}$	۳۴	$u_{۳۴}$	۵۷۰۲۸۸۷
$u_{۱۰}$	۵۵	$u_{۳۵}$	۹۲۲۷۴۶۵
$u_{۱۱}$	۸۹	$u_{۳۶}$	۱۴۹۳۰۳۵۲
$u_{۱۲}$	۱۴۴	$u_{۳۷}$	۲۴۱۵۷۸۱۷
$u_{۱۳}$	۲۳۳	$u_{۳۸}$	۳۹۰۸۸۱۶۹
$u_{۱۴}$	۳۷۷	$u_{۳۹}$	۶۳۲۴۵۹۸۶
$u_{۱۵}$	۶۱۰	$u_{۴۰}$	۱۰۲۳۳۴۱۵۵
$u_{۱۶}$	۹۸۷	$u_{۴۱}$	۱۶۵۵۸۰۱۴۱
$u_{۱۷}$	۱۵۹۷	$u_{۴۲}$	۲۶۷۹۱۴۲۹۶
$u_{۱۸}$	۲۵۸۴	$u_{۴۳}$	۴۳۳۴۹۴۴۳۷
$u_{۱۹}$	۴۱۸۱	$u_{۴۴}$	۷۰۱۴۰۸۷۳۳
$u_{۲۰}$	۶۷۶۵	$u_{۴۵}$	۱۱۳۴۹۰۳۱۷۹
$u_{۲۱}$	۱۰۹۴۶	$u_{۴۶}$	۱۸۳۶۳۱۱۹۰۳
$u_{۲۲}$	۱۷۷۱۱	$u_{۴۷}$	۲۹۷۱۲۱۵۰۷۳
$u_{۲۳}$	۲۸۶۵۷	$u_{۴۸}$	۴۸۰۷۵۲۶۹۷۶
$u_{۲۴}$	۴۶۳۶۸	$u_{۴۹}$	۷۷۷۸۷۴۲۰۴۹
$u_{۲۵}$	۷۵۰۲۵	$u_{۵۰}$	۱۲۵۸۶۲۶۹۰۲۵

حکم دیگری که می‌خواهیم ثابت کنیم این است که هر عدد صحیح مثبت را می‌توان به‌صورت مجموع چند عدد فیبوناتچی متمایز نوشت. به‌عنوان مثال، چند عدد صحیح مثبت را درنظر می‌گیریم:

$$۱ = u_{۱} \qquad ۵ = u_{۵} = u_{۴} + u_{۳}$$

$$۲ = u_{۳} \qquad ۶ = u_{۵} + u_{۱} = u_{۴} + u_{۳} + u_{۱}$$

$$۳ = u_{۴} \qquad ۷ = u_{۵} + u_{۳} = u_{۴} + u_{۳} + u_{۲} + u_{۱}$$

$$۴ = u_{۴} + u_{۱} \qquad ۸ = u_{۶} = u_{۵} + u_{۴}$$

کافی است به استقرا بر $n > ۲$ نشان دهیم که هر یک از عددهای صحیح ۱، ۲، ۳، . . .، $u_n - ۱$ مجموع عددهایی متمایز متعلق به مجموعهٔ $\{u_{۱}, u_{۲}, \dots , u_{n-۲}\}$ است. با فرض اینکه حکم به‌ازای $n = k$ برقرار است، N را طوری انتخاب می‌کنیم که $u_k - ۱ < N < u_{k+۱}$. چون $N - u_{k-۱} < u_{k+۱} - u_{k-۱} = u_k$، نتیجه می‌گیریم عدد صحیح $N - u_{k-۱}$ به‌صورت مجموع

عددهای متمایزی از $\{u_1, u_2, \dots, u_{k-2}\}$ قابل نمایش است. بنابراین N و، در نتیجه، هر یک از عددهای صحیح ۱، ۲، ۳، ...، $u_{k+1} - 1$ را می‌توان به‌صورت مجموع چند عدد متمایز متعلق به مجموعهٔ $\{u_1, u_2, \dots, u_{k-2}, u_{k-1}\}$ نوشت. به این ترتیب، مرحلهٔ استقرا به انجام می‌رسد.

برای راحتی خواننده، این نتیجه را به‌صورت قضیهٔ زیر عنوان می‌کنیم.

قضیهٔ ۱۳ـ۴ هر عدد صحیح مثبت را می‌توان به‌صورت مجموع تعداد متناهی از عددهای فیبوناتچی متمایز نشان داد.

تمرینهای ۱۳ـ۲

۱. به استقرا بر عدد صحیح مثبت n، فرمولهای زیر را ثابت کنید:

(الف) $$u_1 + 2u_2 + 3u_3 + \dots + nu_n = (n+1)u_{n+2} - u_{n+4} + 2$$

(ب) $$u_2 + 2u_4 + 3u_6 + \dots + nu_{2n} = nu_{2n+1} - u_{2n}$$

۲. (الف) نشان دهید مجموع n عدد فیبوناتچی نخست با اندیسهای فرد از فرمول

$$u_1 + u_3 + u_5 + \dots + u_{2n-1} = u_{2n}$$

به‌دست می‌آید. [راهنمایی: برابریهای $u_1 = u_2$، $u_3 = u_4 - u_2$، $u_5 = u_6 - u_4$، ...، را با هم جمع کنید.]

(ب) نشان دهید که مجموع n عدد فیبوناتچی نخست با اندیسهای زوج از فرمول

$$u_2 + u_4 + u_6 + \dots + u_{2n} = u_{2n+1} - 1$$

به‌دست می‌آید. [راهنمایی: قسمت (الف) را همراه با اتحاد (۲) به‌کار ببرید.]

(پ) فرمول مجموع متناوب n عدد فیبوناتچی نخست (فرمول زیر) را ثابت کنید:

$$u_1 - u_2 + u_3 - u_4 + \dots + (-1)^{n+1}u_n = 1 + (-1)^{n+1}u_{n-1}$$

۳. از فرمول (۱) نتیجه بگیرید که به‌ازای $n \geq 2$ داریم

$$u_{2n} = u_{n+1}^2 - u_{n-1}^2 \ ، \ u_{2n-1} = u_n^2 + u_{n-1}^2$$

۴. با استفاده از نتیجه‌های تمرین ۳ اتحادهای زیر را ثابت کنید:

(الف) $$u_{n+1}^2 + u_{n-2}^2 = 2u_{2n-1} \text{،} \quad n \geq 3$$

(ب) $u_{n+2}^2 + u_{n-1}^2 = 2(u_n^2 + u_{n+1}^2)$، $n \geq 2$

۵. نشان دهید که به‌ازای $n \geq 2$، فرمول

$$u_n u_{n-1} = u_n^2 - u_{n-1}^2 + (-1)^n$$

برقرار است و با استفاده از آن نتیجه بگیرید که عددهای فیبوناتچی متوالی متباین هستند.

۶. اتحادهای زیر را بدون استفاده از استقرا ثابت کنید:

(الف) $u_{n+1}^2 - 4u_n u_{n-1} = u_{n-2}^2$، $n \geq 3$

[راهنمایی: با به توان ۲ رسانیدن $u_{n-2} = u_n - u_{n-1}$ و $u_{n+1} = u_n + u_{n-1}$ آغاز کنید.]

(ب) $u_{n+1}u_{n-1} - u_{n+2}u_{n-2} = 2(-1)^n$، $n \geq 3$

[راهنمایی: قرار دهید $u_{n+2} = u_{n+1} + u_n$، $u_{n-2} = u_n - u_{n-1}$ و از فرمول (۳) استفاده کنید.]

(پ) $u_n^2 - u_{n+2}u_{n-2} = (-1)^n$، $n \geq 3$

[راهنمایی: از اثبات فرمول (۳) تقلید کنید.]

(ت) $u_n^2 - u_{n+3}u_{n-3} = 4(-1)^{n+1}$، $n \geq 4$

(ث) $u_n u_{n+1} u_{n+3} u_{n+4} = u_{n+2}^4 - 1$، $n \geq 1$

[راهنمایی: بنا به قسمت (پ)، $u_{n+4}u_n = u_{n+2}^2 + (-1)^{n+1}$، در حالی‌که بنا به فرمول (۳)، $u_{n+1}u_{n+3} = u_{n+2}^2 + (-1)^{n+2}$.]

(ج) $u_{2n+2}u_{2n-1} - u_{2n}u_{2n+1} = 1$، $n \geq 1$

۷. عددهای صحیح ۵۰، ۷۵، ۱۰۰، و ۱۲۵ را به‌صورت مجموعهای چند عدد فیبوناتچی متمایز بنویسید.

۸. ثابت کنید هر عدد صحیح مثبت را می‌توان به‌صورت مجموع جمله‌هایی متمایز از دنبالهٔ $u_2, u_3, u_4, \ldots$ (یعنی، دنبالهٔ فیبوناتچی با حذف u_1) نوشت.

۹. اتحاد

$$(u_n u_{n+3})^2 + (2u_{n+1}u_{n+2})^2 = (u_{2n+3})^2 \text{،} \quad n \geq 1$$

را ثابت کنید و با استفاده از آن پنج سه‌تایی فیثاغورسی اولیه به‌دست آورید.

۱۰. ثابت کنید $u_n u_{n+1} u_{n+2} u_{n+3}$، حاصلضرب هر چهار عدد فیبوناتچی متوالی، با مساحت مثلثی فیثاغورسی برابر است. [راهنمایی: به تمرین پیشین نگاه کنید.]

۱۱. فرض می‌کنیم $\alpha = (1+\sqrt{5})/2$ و $\beta = (1-\sqrt{5})/2$ ریشه‌های معادلهٔ $x^2 = x+1$ باشند. به استقرا نشان دهید که به‌ازای هر $n \geq 1$، فرمول بینه[1]، یعنی

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

برقرار است.

۱۲. نشان دهید که به‌ازای $n \geq 1$، حاصلضرب $u_{2n-1} u_{2n+5}$ را می‌توان به‌صورت مجموع دو مربع نشان داد. [راهنمایی: تمرین ۶ (ث).]

۱۳. ثابت کنید که اگر $p = 4k+3$ اول باشد، آنگاه p نمی‌تواند عددی فیبوناتچی با اندیس فرد را بشمارد؛ یعنی، به‌ازای هر $n \geq 1$، $p \nmid u_{2n-1}$. [راهنمایی: اگر چنین نباشد، $u_n^2 + u_{n-1}^2 = u_{2n-1} \equiv 0 \pmod{p}$. تمرین ۱۲ در بخش ۵ـ۴ را ببینید.]

۱۴. تحقیق کنید که حاصلضرب سه عدد فیبوناتچی متوالی با اندیسهای زوج، $u_{2n} u_{2n+2} u_{2n+4}$، برابر با حاصلضرب سه عدد صحیح متوالی است؛ به‌عنوان مثال، $u_4 u_6 u_8 = 504 = 7 \times 8 \times 9$. [راهنمایی: نخست نشان دهید $u_{2n} u_{2n+4} = u_{2n+2}^2 - 1$.]

۱۵. با استفاده از فرمولهای (۱) و (۲) نشان دهید مجموع هر بیست عدد فیبوناتچی متوالی بر u_{10} بخشپذیر است.

۱۶. ثابت کنید که $u_n + 1$، $n \geq 4$، اول نیست. [راهنمایی: کافی است اتحادهای

$$u_{4k} + 1 = u_{2k-1}(u_{2k} + u_{2k+2})$$

$$u_{4k+1} + 1 = u_{2k+1}(u_{2k-1} + u_{2k+1})$$

$$u_{4k+2} + 1 = u_{2k+2}(u_{2k+1} + u_{2k-1})$$

$$u_{4k+3} + 1 = u_{2k+1}(u_{2k+1} + u_{2k+3})$$

را ثابت کرد.]

۱۷. عددهای لوکاس با همان فرمول بازگشتیِ عددهای فیبوناتچی یعنی

$$L_n = L_{n-1} + L_{n-2} \qquad (n \geq 3)$$

1. Binet

منتها با $L_۱ = ۱$ و $L_۲ = ۳$ تعریف می‌شوند؛ از اینجا دنبالهٔ $۱, ۳, ۴, ۷, ۱۱, ۱۸, ۲۹, ۴۷, ۷۶, ۱۲۳, ۱۹۹, ۳۲۲, \ldots$ به‌دست می‌آید. هر یک از اتحادهای زیر را در مورد عددهای لوکاس ثابت کنید:

(الف) $L_۱ + L_۲ + L_۳ + \ldots + L_n = L_{n+۲} - ۳$، $n \geq ۱$

(ب) $L_۱ + L_۳ + L_۵ + \ldots + L_{۲n-۱} = L_{۲n} - ۲$، $n \geq ۱$

(پ) $L_۲ + L_۴ + L_۶ + \ldots + L_{۲n} = L_{۲n+۱} - ۱$، $n \geq ۱$

(ت) $L_n^۲ = L_{n+۱}L_{n-۲} + ۵(-۱)^n$، $n \geq ۱$

(ث) $L_۱^۲ + L_۲^۲ + L_۳^۲ + \ldots + L_n^۲ = L_nL_{n+۱} - ۲$، $n \geq ۱$

(ج) $L_{n+۱}^۲ - L_n^۲ = L_{n-۱}L_{n+۲}$ ، $n \geq ۲$

۱۸. رابطه‌های زیر میان عددهای فیبوناتچی و لوکاس را ثابت کنید:

(الف) $L_n = u_{n+۱} + u_{n-۱} = u_n + ۲u_{n-۱}$، $n \geq ۲$ [راهنمایی: به استقرا بر n استدلال کنید.]

(ب) $L_n = u_{n+۲} - u_{n-۲}$، $n \geq ۳$

(پ) $u_{۲n} = u_nL_n$، $n \geq ۱$

(ت) $L_{n+۱} + L_{n-۱} = ۵u_n$، $n \geq ۲$

(ث) $L_n^۲ = u_n^۲ + ۴u_{n+۱}u_{n-۱}$، $n \geq ۲$

(ج) $۲u_{m+n} = u_mL_n + L_mu_n$، $m \geq ۱$، $n \geq ۱$

(چ) $\gcd(u_n, L_n) = ۱$ یا ۲، $n \geq ۱$

۱۹. اگر $\alpha = (۱ + \sqrt{۵})/۲$ و $\beta = (۱ - \sqrt{۵})/۲$، ثابت کنید که به‌ازای $n \geq ۱$،

$$L_n = \alpha^n + \beta^n$$

و بنابراین

$$\alpha^n = \frac{L_n + \sqrt{۵}u_n}{۲} \quad \text{و} \quad \beta^n = \frac{L_n - \sqrt{۵}u_n}{۲}$$

[راهنمایی: تمرین ۱۱ را ببینید.]

۲۰. لوکاس در سال ۱۸۷۶ فرمول زیر را برای محاسبهٔ عددهای فیبوناتچی برحسب ضریبهای

دوجمله‌ای کشف کرد: اگر j بزرگترین عدد صحیح نابیشتر از $(n-۱)/۲$ باشد، آنگاه

$$u_n = \binom{n-۱}{۰} + \binom{n-۲}{۱} + \ldots + \binom{n-j}{j-۱} + \binom{n-j-۱}{j}$$

این فرمول را ثابت کنید. [راهنمایی: با استفاده از رابطهٔ $u_n = u_{n-۱} + u_{n-۲}$، به استقرا استدلال کنید. همچنین توجه کنید که $\binom{m}{k} = \binom{m-۱}{k} + \binom{m-۱}{k-۱}$.]

۲۱. ثابت کنید که به‌ازای $n \geq ۱$ داریم

(الف) $$\binom{n}{۱}u_۱ + \binom{n}{۲}u_۲ + \binom{n}{۳}u_۳ + \ldots + \binom{n}{n}u_n = u_{۲n}$$

(ب) $$-\binom{n}{۱}u_۱ + \binom{n}{۲}u_۲ - \binom{n}{۳}u_۳ + \ldots + (-۱)^n\binom{n}{n}u_n = -u_n$$

۲۲. ثابت کنید مجموع هر ۲۴ عدد فیبوناتچی متوالی بر ۲۴ بخشپذیر است. [راهنمایی: اتحاد

$$u_n + u_{n+۱} + \ldots + u_{n+k-۱} = u_{n-۱}(u_{k+۱} - ۱) + u_n(u_{k+۲} - ۱)$$

را درنظر بگیرید.]

۲۳. فرض می‌کنیم n عددی صحیح مثبت است و $m = n^{۱۳} - n$. نشان دهید u_m بر ۳۰۲۹۰ بخشپذیر است. [راهنمایی: تمرین ۱ (ب) از بخش ۳.۷ را ببینید.]

۱۳ـ۳ کسرهای مسلسل متناهی

در بخشی از لیبر آباکی مربوط به تجزیهٔ کسرها به کسرهای واحد، فیبوناتچی گونه‌ای از "کسر مسلسل" را معرفی کرد. به‌عنوان مثال، نماد ۱۱۱/۳۴۵ را به‌عنوان صورت فشردهٔ

$$\frac{۱ + \frac{۱ + \frac{۱}{۵}}{۴}}{۳} = \frac{۱}{۳} + \frac{۱}{۳ \times ۴} + \frac{۱}{۳ \times ۴ \times ۵}$$

به‌کاربرد. ولی امروز معمولاً کسرهای مسلسل را به‌صورتی پلکانی می‌نویسند؛ به‌عنوان مثال

$$۲ + \cfrac{۱}{۴ + \cfrac{۱}{۱ + \cfrac{۱}{۳ + \cfrac{۱}{۲}}}}$$

چنین کسر چندگانه‌ای کسر مسلسل سادهٔ متناهی نامیده می‌شود. به بیان رسمی:

تعریف ۱۳ـ۱ منظور از کسر مسلسل متناهی کسری به‌صورت

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \; \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

است که در آن a_0، a_1، ...، a_n عددهایی حقیقی‌اند، و همگی، مگر احتمالاً a_0 مثبت‌اند. عددهای a_1،a_2،...،a_n مخرجهای جزئی این کسرند. چنین کسری ساده نامیده می‌شود اگر همهٔ a_iها عدد صحیح باشند.

گرچه امتیاز این کشف به حق به فیبوناتچی تعلق گرفته است، به‌نظر بسیاری از صاحب‌نظران، نظریهٔ کسرهای مسلسل با کارهای رافائل بُمبلی[1]، آخرین جبردان بزرگ دورهٔ رنسانس ایتالیا، آغاز می‌شود. بُمبلی در کتاب عملهای جبری[2] خود (۱۵۷۲) کوشید ریشه‌های دوم را با استفاده از کسرهای مسلسل نامتناهی به‌دست آورد که روشی مبتکرانه و جدید بود. وی در واقع ثابت کرد $\sqrt{13}$ را می‌توان به‌صورت کسر مسلسل

$$\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}$$

نوشت. جالب توجه است که بدانیم بُمبلی نخستین فردی بود که غرب لاتینی را با کارهای دیوفانتوس آشنا کرد. ابتدا تصمیم گرفت حساب دیوفانتوس را از روی نسخهٔ متعلق به کتابخانهٔ واتیکان (احتمالاً همان نسخه‌ای که رگیومونتانوس آن‌را کشف کرد) ترجمه کند، ولی به‌علت اشتغال به امور دیگر هرگز

1. Rafael Bombelli 2. L' Algebra Opera

این کار را تمام نکرد. در عوض همهٔ مسأله‌های چهار مقالهٔ نخست حساب دیوفانتوس را در کتاب جبر خود آورد. وی گرچه این مسأله‌ها را متمایز نکرد، ولی تصدیق کرد که مسأله‌هایی را به‌دلخواه از کتاب حساب به عاریت گرفته است.

واضح است که مقدار هر کسر مسلسل سادهٔ متناهی همیشه عددی گویاست. به‌عنوان مثال، مقدار کسر مسلسل

$$۳+\cfrac{۱}{۴+\cfrac{۱}{۱+\cfrac{۱}{۴+\cfrac{۱}{۲}}}}$$

برابر با ۱۷۰/۵۳ است:

$$\begin{aligned}
۳+\cfrac{۱}{۴+\cfrac{۱}{۱+\cfrac{۱}{۴+\cfrac{۱}{۲}}}} &= ۳+\cfrac{۱}{۴+\cfrac{۱}{۱+\cfrac{۲}{۹}}}\\
&= ۳+\cfrac{۱}{۴+\cfrac{۹}{۱۱}}\\
&= ۳+\frac{۱۱}{۵۳}\\
&= \frac{۱۷۰}{۵۳}
\end{aligned}$$

قضیهٔ ۱۳ـ۵ هر عدد گویا را می‌توان به‌صورت کسر مسلسل سادهٔ متناهی نوشت.

اثبات. فرض می‌کنیم a/b، $b > ۰$، عددی گویا باشد. با استفاده از الگوریتم اقلیدس برای تعیین بزرگترین مقسوم‌علیه مشترک a و b رابطه‌های زیر را به‌دست می‌آوریم

$$\begin{aligned}
a &= ba_۰ + r_۱, & ۰ &< r_۱ < b\\
b &= r_۱a_۱ + r_۲, & ۰ &< r_۲ < r_۱\\
r_۱ &= r_۲a_۲ + r_۳, & ۰ &< r_۳ < r_۲\\
&\vdots\\
r_{n-۲} &= r_{n-۱}a_{n-۱} + r_n, & ۰ &< r_n < r_{n-۱}\\
r_{n-۱} &= r_na_n + ۰
\end{aligned}$$

توجه می‌کنیم که چون هر یک از باقیمانده‌های r_k عدد صحیح مثبتی است، a_1، a_2، ...، a_n همگی مثبت هستند. رابطه‌های الگوریتم را به‌صورت زیر می‌نویسیم

$$\begin{aligned}
a/b &= a_0 + r_1/b = a_0 + 1/(b/r_1) \\
b/r_1 &= a_1 + r_2/r_1 = a_1 + 1/(r_1/r_2) \\
r_1/r_2 &= a_2 + r_3/r_2 = a_2 + 1/(r_2/r_3) \\
&\vdots \\
r_{n-1}/r_n &= a_n
\end{aligned}$$

اگر b/r_1 را از نخستین رابطه حذف کنیم، داریم

$$\frac{a}{b} = a_0 + \frac{1}{\left(\frac{b}{r_1}\right)} = a_0 + \frac{1}{a + \frac{1}{\left(\frac{r_1}{r_2}\right)}}$$

مقدار r_1/r_2 را، به‌صورتی که رابطهٔ سوم مشخص کرده است، در این نتیجه قرار می‌دهیم

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\left(\frac{r_2}{r_3}\right)}}}$$

با ادامهٔ این فرایند، به‌دست می‌آوریم

$$a/b = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\ddots}{\qquad \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

و به این ترتیب، اثبات کامل می‌شود. □

برای روشن ساختن فرایند به‌کار رفته در اثبات قضیهٔ ۱۳ـ۵، ۱۹/۵۱ را به‌صورت کسری مسلسل نمایش می‌دهیم. با کاربرد الگوریتم اقلیدسی در مورد عددهای صحیح ۱۹ و ۵۱، رابطه‌های زیر به‌دست می‌آیند

$$\begin{array}{lcl}
\dfrac{۵۱}{۱۹} = ۲ + \dfrac{۱۳}{۱۹} & \text{یا} & ۵۱ = ۲ \times ۱۹ + ۱۳ \\[2ex]
\dfrac{۱۹}{۱۳} = ۱ + \dfrac{۶}{۱۳} & \text{یا} & ۱۹ = ۱ \times ۱۳ + ۶ \\[2ex]
\dfrac{۱۳}{۶} = ۲ + \dfrac{۱}{۶} & \text{یا} & ۱۳ = ۲ \times ۶ + ۱ \\[2ex]
\dfrac{۶}{۶} = ۱ & \text{یا} & ۶ = ۶ \times ۱ + ۰
\end{array}$$

با جایگزینیهای مناسب، ملاحظه می‌کنیم که

$$\begin{aligned}
\frac{۱۹}{۵۱} = \frac{۱}{\left(\dfrac{۵۱}{۱۹}\right)} &= \cfrac{۱}{۲ + \cfrac{۱۳}{۱۹}} \\
&= \cfrac{۱}{۲ + \cfrac{۱}{\cfrac{۱۹}{۱۳}}} \\
&= \cfrac{۱}{۲ + \cfrac{۱}{۱ + \cfrac{۶}{۱۳}}} \\
&= \cfrac{۱}{۲ + \cfrac{۱}{۱ + \cfrac{۱}{\cfrac{۱۳}{۶}}}} \\
&= \cfrac{۱}{۲ + \cfrac{۱}{۱ + \cfrac{۱}{۲ + \cfrac{۱}{۶}}}}
\end{aligned}$$

که کسر مسلسل متناظر با ۱۹/۵۱ است.

چون تایپ یا نوشتن کسرهای مسلسل به این صورت دشوار و جاگیر است، قرارداد می‌کنیم کسر مسلسل را با نمادی که نشان‌دهندهٔ خارج‌قسمتهای جزئی آن است، نشان دهیم، مثلاً با نماد

$[a_\circ; a_1, \ldots, a_n]$. با این نماد، بسط ۱۹/۵۱ به‌صورت

$$[\circ; 2, 1, 2, 6]$$

و کسر مسلسل متناظر با $172/51 = 3 + 19/51$ با

$$[3; 2, 1, 2, 6]$$

نشان داده می‌شود.

عدد صحیح نخستین در نماد $[a_\circ; a_1, \ldots, a_n]$ وقتی صفر است که مقدار کسر مثبت ولی کوچکتر از ۱ باشد.

نمایش عدد گویا به‌صورت کسر مسلسل سادهٔ متناهی یکتا نیست: وقتی این نمایش به‌دست آمد، جملهٔ آخر کسر مسلسل را همیشه می‌توان تغییر داد زیرا اگر $a_n > 1$، آنگاه

$$a_n = (a_n - 1) + 1 = (a_n - 1) + \frac{1}{1}$$

که در آن، $a_n - 1$ عدد صحیح مثبتی است، و بنابراین

$$[a_\circ; a_1, \ldots, a_n] = [a_\circ; a_1, \ldots, a_{n-1}, 1]$$

از سوی دیگر، اگر $a_n = 1$، آنگاه

$$a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{1} = a_{n-1} + 1$$

و بنابراین

$$[a_\circ; a_1, \ldots, a_{n-1}, a_n] = [a_\circ; a_1, \ldots, a_{n-2}, a_{n-1} + 1]$$

هر عدد گویا دارای دو نمایش به‌صورت کسر مسلسل ساده است، یکی با تعداد زوجی مخرج جزئی و دیگری با تعدادی فرد (ثابت می‌شود که فقط این دو نمایش وجود دارد). در مورد ۱۹/۵۱ داریم

$$\frac{19}{51} = [\circ; 2, 1, 2, 6] = [\circ; 2, 1, 2, 5, 1]$$

مثال ۱۳ـ۱

به دنبالهٔ فیبوناتچی باز می‌گردیم و نمایش خارج قسمت دو عدد فیبوناتچی متوالی (یعنی، عدد گویای u_{n+1}/u_n) به‌صورت کسر مسلسل ساده را درنظر می‌گیریم. به‌طوری که پیشتر خاطر نشان

شد، الگوریتم اقلیدسی برای تعیین بزرگترین مقسوم‌علیه مشترک u_n و $u_{n+۱}$، $n-۱$ رابطهٔ

$$u_{n+۱} = ۱ \times u_n + u_{n-۱}$$
$$u_n = ۱ \times u_{n-۱} + u_{n-۲}$$
$$\vdots$$
$$u_۴ = ۱ \times u_۳ + u_۲$$
$$u_۳ = ۲ \times u_۲ + ۰$$

را تولید می‌کند. چون خارج‌قسمتهای تولید شده توسط الگوریتم، مخرجهای جزئی کسر مسلسل‌اند، می‌توانیم بنویسیم

$$\frac{u_{n+۱}}{u_n} = [۱; ۱, \dots, ۱, ۲]$$

ولی $u_{n+۱}/u_n$ همچنین به‌وسیلهٔ کسر مسلسلی که یک مخرج جزئی بیشتر از $[۱; ۱, ۱, \dots, ۱, ۲]$ دارد نشان داده می‌شود یعنی

$$u_{n+۱}/u_n = [۱; ۱, ۱, \dots, ۱, ۱, ۱]$$

که در آن عدد صحیح ۱، $n+۱$ بار تکرار می‌شود. بنابراین، کسر $u_{n+۱}/u_n$ دارای بسطی به‌صورت کسر مسلسل است که توصیف آن بسیار ساده است: n مخرج جزئی وجود دارد که همگی برابر ۱ اند. ■

به‌عنوان آخرین مطلب این بخش، نحوهٔ کاربرد نظریهٔ کسرهای مسلسل در حل معادله‌های دیوفانتی [دیوفانتوسی] خطی را شرح می‌دهیم. این امر مستلزم اطلاع از نکته‌هایی مربوط به "همگراها"ی کسر مسلسل است، و بنابراین بحث را با تشریح و اثبات آنها آغاز می‌کنیم.

تعریف ۱۳ـ۲ اگر از کسر مسلسل $[a_۰; a_۱, \dots, a_n]$ قسمت پس از a_k (kامین مخرج جزئی) را حذف کنیم، کسری به‌دست می‌آید که kامین همگرای کسر مسلسل مزبور نامیده و با C_k نشان داده می‌شود؛ به زبان نمادین می‌نویسیم

$$C_k = [a_۰; a_۱, \dots, a_k], \qquad (۱ \le k \le n)$$

عدد $a_۰$ را صفرمین همگرا می‌نامیم و با $C_۰$ نشان می‌دهیم.

یک نکتهٔ قابل توجه این است که اگر $k < n$ و به‌جای a_k مقدار $a_k + 1/a_{k+1}$ قرار گیرد، همگرای C_k به همگرای C_{k+1} تبدیل می‌شود:

$$[a_0; a_1, \dots, a_{k-1}, a_k + a_k + 1/a_{k+1}]$$
$$= [a_0; a_1, \dots, a_{k-1}, a_k, a_{k+1}] = C_{k+1}$$

بدیهی است آخرین همگرا، یعنی C_n، همیشه برابر با عدد گویایی است که با کسر مسلسل اولیه نمایش داده می‌شود.

در مورد مثال $19/51 = [0; 2, 1, 2, 6]$، همگراهای متوالی عبارت‌اند از

$$C_0 = 0$$
$$C_1 = [0; 2] = 0 + \frac{1}{2} = \frac{1}{2}$$
$$C_2 = [0; 2, 1] = 0 + \cfrac{1}{2 + \cfrac{1}{1}} = \frac{1}{3}$$
$$C_3 = [0; 2, 1, 2] = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2}}} = \frac{3}{8}$$
$$C_4 = [0; 2, 1, 2, 6] = \frac{19}{51}$$

جز آخرین همگرا یعنی C_4، اینها یک در میان کوچکتر یا بزرگتر از $19/51$اند، به‌طوری که هر همگرا به $19/51$ نزدیکتر از قبلی است.

با اثبات فرمولهایی برای صورت و مخرج همگراهای کسر مسلسل $[a_0; a_1, \dots, a_n]$، می‌توان زحمت محاسبهٔ همگراها را تا حد زیادی کاهش داد. به این منظور عددهای p_k و q_k، $k = 0, 1, \dots, n$، را به‌صورت زیر تعریف می‌کنیم. به‌ازای $k = 2, 3, \dots, n$

$$\begin{aligned}
p_0 &= a_0 & \text{و} \quad q_0 &= 1 \\
p_1 &= a_1 a_0 + 1 & q_1 &= a_1 \\
&\vdots & &\vdots \\
p_k &= a_k p_{k-1} + p_{k-2} & q_k &= a_k q_{k-1} + q_{k-2}
\end{aligned}$$

با محاسبه‌ای مستقیم معلوم می‌شود که چند همگرای نخست $[a_0; a_1, \ldots, a_n]$ عبارت‌اند از

$$C_0 = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$$
$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{p_1}{q_1}$$
$$C_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{a_2(a_1 a_0 + 1) + a_0}{a_2 a_1 + 1} = \frac{p_2}{q_2}$$

موفقیت ما بستگی به این دارد که بتوانیم نشان دهیم این رابطه همواره برقرار است. قضیهٔ زیر حاکی از این مطلب است.

قضیهٔ ۱۳ـ۶ kامین همگرای کسر مسلسل سادهٔ $[a_0; a_1, \ldots, a_n]$ دارای مقدار

$$C_k = \frac{p_k}{q_k} \qquad (0 \le k \le n)$$

است

اثبات. ملاحظات فوق نشان می‌دهند که حکم به‌ازای $k = 0, 1, 2$ برقرار است. فرض می‌کنیم حکم به‌ازای $k = m$، $2 \le m < n$، برقرار باشد؛ یعنی، به‌ازای این m داشته باشیم

$$C_m = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}} \qquad (*)$$

توجه می‌کنیم که عددهای صحیح p_{m-1}، q_{m-1}، p_{m-2}، q_{m-2} به $m - 1$ مخرج جزئی نخست a_1، a_2، …، a_{m-1} بستگی دارند و بنابراین مستقل از a_m هستند. پس فرمول $(*)$، در صورت قرار دادن مقدار $a_m + 1/a_{m+1}$ به‌جای a_m نیز برقرار است:

$$\left[a_0; a_1, \ldots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right]$$
$$= \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}}$$

همان‌طور که پیشتر توضیح داده‌ایم، تأثیر این جایگزینی تبدیل C_m به همگرای C_{m+1} است، بنابراین

$$C_{m+1} = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}}$$
$$= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}}$$
$$= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}$$

ولی، این دقیقاً صورتی است که قضیه باید به‌ازای $k = m + 1$ داشته باشد، پس بنا به استقرا، حکم عنوان شده برقرارست. □

اکنون صدق این قضیه را در یک مورد مشخص ملاحظه می‌کنیم. در مثال ما، $19/51 = [0; 2, 1, 2, 6]$

$$\begin{aligned} p_0 &= 0 & \text{و} \quad q_0 &= 1 \\ p_1 &= 0 \times 2 + 1 = 1 & q_1 &= 2 \\ p_2 &= 1 \times 1 + 0 = 1 & q_2 &= 1 \times 2 + 1 = 3 \\ p_3 &= 2 \times 1 + 1 = 3 & q_3 &= 2 \times 3 + 2 = 8 \\ p_4 &= 6 \times 3 + 1 = 19 & q_4 &= 6 \times 8 + 3 = 51 \end{aligned}$$

بنابراین، همگراهای $[0, 2, 1, 2, 6]$ عبارت‌اند از

$$C_0 = \frac{p_0}{q_0} = 0, \quad C_1 = \frac{p_1}{q_1} = \frac{1}{2}, \quad C_2 = \frac{p_2}{q_2} = \frac{1}{3}$$
$$C_3 = \frac{p_3}{q_3} = \frac{3}{8}, \quad C_4 = \frac{p_4}{q_4} = \frac{19}{51}$$

که می‌دانیم باید همینها باشند.

با قضیهٔ زیر، به تشریح ویژگیهای همگراها ادامه می‌دهیم.

قضیهٔ ۱۳ـ۷ اگر $C_k = p_k/q_k$، kامین همگرای کسر مسلسل سادهٔ $[a_0; a_1, \ldots, a_n]$ باشد، آنگاه

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}, \quad 1 \le k \le n$$

اثبات. اثبات با استقرا بر k به‌سادگی انجام می‌شود، و رابطهٔ

$$p_1q_0 - q_1p_0 = (a_1a_0 + 1) \times 1 - a_1 \times a_0 = 1 = (-1)^{1-1}$$

نشان‌دهندهٔ درستی حکم به‌ازای $k = 1$ است. فرض می‌کنیم فرمول مورد بحث به‌ازای $k = m$، $n \geq m \geq 1$، برقرار باشد. در این‌صورت

$$\begin{aligned} p_{m+1}q_m - q_{m+1}p_m &= (a_{m+1}p_m + p_{m-1})q_m - (a_{m+1}q_m + q_{m-1})p_m \\ &= -(p_mq_{m-1} - q_mp_{m-1}) \\ &= -(-1)^{m-1} = (-1)^m \end{aligned}$$

و بنابراین، هرگاه فرمول به‌ازای $k = m$ برقرار باشد، به‌ازای $k = m + 1$ نیز برقرار است. بنا به استقرا نتیجه می‌گیریم که به‌ازای هر k، $n \geq k \geq 1$، برقرار است. □

یک نتیجهٔ قابل توجهِ این حکم این است که صورت و مخرج هر همگرا متباین‌اند و بنابراین همگراها همیشه به ساده‌ترین صورت ممکن هستند.

فرع. به‌ازای $n \geq k \geq 1$، p_k و q_k متباین‌اند.

اثبات. اگر $d = \gcd(p_k, q_k)$، بنا به قضیه داریم $d|(-1)^{k-1}$، و بنابراین چون $d > 0$، نتیجه می‌گیریم $d = 1$. □

مثال ۱۳_۲

کسر مسلسل $[0; 1, 1, \ldots, 1]$ را که همهٔ مخرجهای جزئی آن برابر ۱ هستند، درنظر می‌گیریم. چند همگرای نخست این کسر عبارت‌اند از

$$C_0 = \frac{0}{1},\ C_1 = \frac{1}{1},\ C_2 = \frac{2}{1},\ C_3 = \frac{3}{2},\ C_4 = \frac{5}{3}, \ldots$$

چون صورت kامین همگرای C_k برابر است با

$$p_k = 1 \times p_{k-1} + p_{k-2} = p_{k-1} + p_{k-2}$$

و مخرج برابر است با

$$q_k = 1 \times q_{k-1} + q_{k-2} = q_{k-1} + q_{k-2}$$

روشن است که

$$C_k = \frac{u_{k+1}}{u_k} \quad (k \geq 2)$$

که در آن u_k نشان‌دهندهٔ kامین عدد فیبوناتچی است. در اینجا، اتحاد $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$ مذکور در قضیهٔ ۱۳ـ۷ صورت

$$u_{k+1} u_{k-1} - u_k^2 = (-1)^{k-1}$$

را به خود می‌گیرد و این فرمول (۳) در بخش ۱۳ـ۲ است. ■

اکنون به معادلهٔ دیوفانتی خطی

$$ax + by = c$$

که در آن a، b، c عددهای صحیح مفروضی هستند، می‌پردازیم. چون اگر $d \nmid c$، که $d = \gcd(a, b)$، این معادله جوابی ندارد، می‌توان فرض کرد $d|c$، بی‌آنکه خللی در کلیت مطلب وارد شود. در واقع، کافی است حالتی را درنظر بگیریم که ضریبها متباین‌اند زیرا اگر $\gcd(a, b) = d > 1$، می‌توان با تقسیم معادله بر d به معادله

$$\left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y = \frac{c}{d}$$

رسید. این دو معادله جوابهای یکسانی دارند، و در حالت اخیر، می‌دانیم که $\gcd(a/d, b/d) = 1$. به‌علاوه، ملاحظه می‌کنیم که برای به‌دست آوردن جوابی از معادلهٔ

$$ax + by = c, \quad \gcd(a, b) = 1$$

می‌توان نخست معادلهٔ دیوفانتی

$$ax + by = 1, \quad \gcd(a, b) = 1$$

را حل کرد. درواقع، اگر بتوان عددهای صحیح x_0 و y_0 را طوری به‌دست آورد که $ax_0 + by_0 = 1$، آنگاه با ضرب کردن هر دو طرف در c نتیجه می‌شود

$$a(cx_0) + b(cy_0) = c$$

پس $x = cx_۰$ و $y = cy_۰$ جواب مطلوب $ax + by = c$ است.

برای تعیین زوجی از عددهای صحیح x و y که در معادلهٔ $ax + by = ۱$ صدق کند، عدد گویای a/b را به‌صورت کسر مسلسل ساده‌ای بسط می‌دهیم؛ مثلاً

$$\frac{a}{b} = [a_۰; a_۱, \ldots , a_n]$$

دو همگرای آخر این کسر مسلسل عبارت‌اند از

$$C_n = \frac{p_n}{q_n} = \frac{a}{b} \quad و \quad C_{n-۱} = \frac{p_{n-۱}}{q_{n-۱}}$$

چون $\gcd(a, b) = ۱ = \gcd(p_n, q_n)$، می‌توان نتیجه گرفت

$$p_n = a \quad و \quad q_n = b$$

بنا به قضیهٔ ۱۳ـ۷ داریم

$$p_n q_{n-۱} - q_n p_{n-۱} = (-۱)^{n-۱}$$

یا، با تغییر نمادها

$$aq_{n-۱} = bp_{n-۱} = (-۱)^{n-۱}$$

بنابراین، به‌ازای $x = q_{n-۱}$ و $y = -p_{n-۱}$ داریم

$$ax + by = (-۱)^{n-۱}$$

اگر n فرد باشد، معادلهٔ $ax + by = ۱$ دارای جواب خاص $x_۰ = q_{n-۱}$، $y_۰ = -p_{n-۱}$ است، در حالی‌که اگر n عدد صحیح زوجی باشد، جوابی به‌صورت $x_۰ = -q_{n-۱}$، $y_۰ = p_{n-۱}$ به‌دست می‌آید. پیشتر در نظریهٔ معادله‌های دیوفانتی خطی دیده‌ایم که، در این‌صورت، جواب عمومی عبارت است از

$$x = x_۰ + bt \ ، \ y = y_۰ - at \ ، \ (t = ۰, \pm ۱, \pm ۲, \ldots)$$

مثال ۱۳ـ۳

معادلهٔ دیوفانتی خطی

$$۱۷۲x + ۲۰y = ۱۰۰۰$$

را با استفاده ازکسرهای مسلسل ساده حل می‌کنیم. چون $۴ = \gcd(۱۷۲, ۲۰)$، این معادله را می‌توان با معادلهٔ

$$۴۳x + ۵y = ۲۵۰$$

تعویض کرد. گام نخست تعیین جوابی خاص از

$$۴۳x + ۵y = ۱$$

است. به این منظور، ۴۳/۵ (یا در صورت تمایل، ۵/۴۳) را به‌صورت کسر مسلسل ساده‌ای می‌نویسیم. دنبالهٔ برابریهای حاصل ازکاربرد الگوریتم اقلیدسی در مورد عددهای ۴۳ و ۵ عبارت است از

$$۴۳ = ۸ \times ۵ + ۳$$
$$۵ = ۱ \times ۳ + ۲$$
$$۳ = ۱ \times ۲ + ۱$$
$$۲ = ۲ \times ۱$$

و بنابراین $\frac{۴۳}{۵} = [۸; ۱, ۱, ۲] = ۸ + \cfrac{۱}{۱ + \cfrac{۱}{۱ + ۱/۲}}$. همگراهای این کسر مسلسل عبارت‌اند از

$$C_۰ = \frac{۸}{۱},\ C_۱ = \frac{۹}{۱},\ C_۲ = \frac{۱۷}{۲},\ C_۳ = \frac{۴۳}{۵}$$

که از آن نتیجه می‌شود $p_۲ = ۱۷$، $q_۲ = ۲$، $p_۳ = ۴۳$ و $q_۵ = ۵$. با توسل دوباره به قضیه ۱۳ـ۷ داریم

$$p_۳q_۲ - q_۳p_۲ = (-۱)^{۳-۱}$$

یا معادلش

$$۴۳ \times ۲ - ۵ \times ۱۷ = ۱$$

اگر این رابطه در ۲۵۰ ضرب شود، به‌دست می‌آوریم

$$۴۳ \times ۵۰۰ + ۵(-۴۲۵۰) = ۲۵۰$$

بنابراین جوابی خاص از معادلهٔ دیوفانتی $۴۳x + ۵y = ۲۵۰$ عبارت است از

$$y_۰ = -۴۲۵۰ \quad ، \quad x_۰ = ۵۰۰$$

جواب عمومی با رابطه‌های

$$(t = ۰, \pm ۱, \pm ۲, \dots) \;، y = -۴۲۵۰ - ۴۳t \;، x = ۵۰۰ + ۵t$$

مشخص می‌شود ■

برای اثبات قضیه‌ای دربارهٔ رفتار همگراهای با اندیسهای فرد و زوجِ کسر مسلسل ساده، لمی مقدماتی مورد نیاز است.

لم. اگر q_k مخرج kامین همگرای C_kی کسر مسلسل سادهٔ $[a_۰; a_۱, \dots, a_n]$ باشد، آنگاه به‌ازای $۱ \leq k \leq n$، $q_{k-۱} \leq q_k$، و این نابرابری به شرط $k > ۱$ اکید است.

اثبات. لم را به استقرا ثابت می‌کنیم. اولاً، $q_۰ = ۱ \leq a_۱ = q_۱$، و بنابراین حکم به‌ازای $k = ۱$ برقرار است. پس فرض می‌کنیم حکم به‌ازای $k = m$، $۱ \leq m \leq n$، برقرار باشد. در این صورت

$$q_{m+۱} = a_{m+۱}q_m + q_{m-۱} > a_{m+۱}q_m \geq ۱ \times q_m = q_m$$

و در نتیجه، نابرابری به‌ازای $k = m + ۱$ نیز درست است. □

با در دست داشتن این اطلاع، به‌آسانی می‌توان قضیهٔ زیر را ثابت کرد.

قضیهٔ ۱۳ـ۸

(۱) همگراهایِ با اندیس زوج، دنباله‌ای اکیداً صعودی تشکیل می‌دهند:

$$C_۰ < C_۲ < C_۴ < \dots$$

(۲) همگراهای با اندیس فرد، دنباله‌ای اکیداً نزولی تشکیل می‌دهند:

$$C_۱ > C_۳ > C_۵ \dots$$

(۳) هر همگرا با اندیس فرد از هر همگرا با اندیس زوج بزرگتر است.

اثبات. بنا به قضیهٔ ۱۳ـ۷، ملاحظه می‌کنیم که

$$\begin{aligned} C_{k+۲} - C_k &= (C_{k+۲} - C_{k+۱}) + (C_{k+۱} - C_k) \\ &= \left(\frac{p_{k+۲}}{q_{k+۲}} - \frac{p_{k+۱}}{q_{k+۱}}\right) + \left(\frac{p_{k+۱}}{q_{k+۱}} - \frac{p_k}{q_k}\right) \\ &= \frac{(-۱)^{k+۱}}{q_{k+۲}q_{k+۱}} + \frac{(-۱)^k}{q_{k+۱}q_k} \\ &= \frac{(-۱)^k(q_{k+۲} - q_k)}{q_k q_{k+۱} q_{k+۲}} \end{aligned}$$

با یادآوری اینکه به‌ازای هر $i \geq ۰$، $q_i > ۰$، و بنا به لم، $q_{k+۲} - q_k > ۰$، بدیهی است که علامت جبری $C_{k+۲} - C_k$ با علامت جبری $(-۱)^k$ یکی است. بنابراین، اگر k عدد صحیح زوجی باشد، مثلاً $k = ۲j$، آنگاه $C_{۲j+۲} > C_{۲j}$؛ از این رو

$$C_۰ < C_۲ < C_۴ < \dots$$

همین‌طور، اگر k عدد صحیح فردی باشد، مثلاً $k = ۲j - ۱$، آنگاه $C_{۲j+۱} < C_{۲j-۱}$؛ پس

$$C_۱ > C_۳ > C_۵ > \dots$$

می‌ماند اینکه نشان دهیم هر همگرای با اندیس فرد، $C_{۲r-۱}$، بزرگتر از هر همگرای با اندیس زوج، $C_{۲s}$، است. چون $p_k q_{k-۱} - q_k p_{k-۱} = (-۱)^{k-۱}$، با تقسیم هر دو طرف این رابطه بر $q_k q_{k-۱}$ به‌دست می‌آوریم

$$C_k - C_{k-۱} = \frac{p_k}{q_k} - \frac{p_{k-۱}}{q_{k-۱}} = \frac{(-۱)^{k-۱}}{q_k q_{k-۱}}$$

یعنی، $C_{۲j} < C_{۲j-۱}$. با مقایسهٔ این چند نابرابری به‌دست می‌آوریم

$$C_{۲s} < C_{۲s+۲r} < C_{۲s+۲r-۱} < C_{۲r-۱}$$

که مطلوب ماست. □

به‌عنوان مثالی مشخص، کسر مسلسل $[۲; ۳, ۲, ۵, ۲, ۴, ۲]$ را درنظر می‌گیریم. با محاسبهٔ کوتاهی معلوم می‌شود که

$$C_۰ = \frac{۲}{۱},\ C_۱ = \frac{۷}{۳},\ C_۲ = \frac{۱۶}{۷},\ C_۳ = \frac{۸۷}{۳۸}$$
$$C_۴ = \frac{۱۹۰}{۸۳},\ C_۵ = \frac{۸۴۷}{۳۷۰},\ C_۶ = \frac{۱۸۸۴}{۸۲۳}$$

بنا به قضیهٔ ۱۳ـ۸، این همگراها در زنجیرهٔ نابرابریهای

$$۲ < \frac{۱۶}{۷} < \frac{۱۹۰}{۸۳} < \frac{۱۸۸۴}{۸۲۳} < \frac{۸۴۷}{۳۷۰} < \frac{۸۷}{۳۸} < \frac{۷}{۳}$$

صدق می‌کنند. این نکته را می‌توان به‌آسانی با توجه به صورت اعشاری عددها ملاحظه کرد:

$$۲ < ۲{,}۲۸۵۷۱\ldots < ۲{,}۲۸۹۱۵\ldots < ۲{,}۲۸۹۱۸\ldots$$
$$< ۲{,}۲۸۹۴۷\ldots < ۲{,}۳۳۳۳۳\ldots$$

تمرینهای ۱۳ـ۳

۱. هر یک از عددهای گویای زیر را به‌صورت کسر مسلسل سادهٔ متناهی نمایش دهید:
(الف) $-۱۹/۵۱$ (ب) $۱۸۷/۵۷$ (پ) $۷۱/۵۵$ (ت) $۱۱۸/۳۰۳$

۲. عددهای گویایی را که با کسرهای مسلسل سادهٔ زیر نشان داده شده‌اند تعیین کنید
(الف) $[-۲; ۲, ۴, ۶, ۸]$ (ب) $[۴; ۲, ۱, ۳, ۱, ۲, ۴]$
(پ) $[۰; ۱, ۲, ۳, ۴, ۳, ۲, ۱]$

۳. اگر $r > ۱$ و $r = [a_۰; a_۱, a_۲, \ldots, a_n]$، نشان دهید

$$\frac{۱}{r} = [a_۰; a_۰, a_۱, \ldots, a_n]$$

۴. کسرهای مسلسل سادهٔ زیر را به‌صورتی هم‌ارز، شامل مخرجهای جزئی به تعداد فرد، نمایش دهید
(الف)، $[۰; ۳, ۱, ۲, ۳]$ (ب) $[-۱; ۲, ۱, ۶, ۱]$ (پ) $[۲; ۳, ۱, ۲, ۱, ۱, ۱]$

۵. همگراهای کسرهای مسلسل سادهٔ زیر را حساب کنید:
(الف) $[۱; ۲, ۳, ۳, ۲, ۱]$ (ب) $[-۳; ۱, ۱, ۱, ۱, ۳]$ (پ) $[۰; ۲, ۴, ۱, ۸, ۲]$

۶. (الف) اگر $C_k = p_k/q_k$، kامین همگرای کسر مسلسل سادهٔ $[۱; ۲, ۳, ۴, \ldots, n, n+۱]$ باشد، نشان دهید

$$p_n = np_{n-۱} + np_{n-۲} + (n-۱)p_{n-۳} + \ldots + ۳p_۱ + ۲p_۰ + (p_۰ + ۱)$$

[راهنمایی: به‌ازای $k = ۲, ۳, \ldots, n$ رابطه‌های $p_۰ = ۱$، $p_۱ = ۳$، $p_k = (k+۱)p_{k-۱} + p_{k-۲}$ را با هم جمع کنید.]

(ب) قسمت (الف) را با محاسبهٔ $p_۴$، صورت همگرای چهارم کسر $[۱; ۲, ۳, ۴, ۵]$، نشان دهید.

۷. به‌ازای هر یک ازکسرهای مسلسل سادهٔ زیر، p_k، q_k، و C_k $(k = ۰, ۱, \ldots, ۸)$ را حساب کنید؛ توجه کنید که همگراها تقریبی از عددهای گنگ داخل پرانتزها به‌دست می‌دهند:

(الف) $[1; 2, 2, 2, 2, 2, 2, 2, 2]$ $(\sqrt{2})$

(ب) $[1; 1, 2, 1, 2, 1, 2, 1, 2]$ $(\sqrt{3})$

(پ) $[2; 4, 4, 4, 4, 4, 4, 4, 4]$ $(\sqrt{5})$

(ت) $[2; 2, 4, 2, 4, 2, 4, 2, 4]$ $(\sqrt{6})$

(ث) $[2; 1, 1, 1, 4, 1, 1, 1, 4]$ $(\sqrt{7})$

۸. اگر $C_k = p_k/q_k$، kامین همگرای مسلسل سادهٔ $[a_0; a_1, \ldots, a_n]$ باشد، ثابت کنید

$$q_k \geq 2^{\frac{k-1}{2}} \qquad (2 \leq k \leq n)$$

[راهنمایی: توجه کنید که $q_k = a_k q_{k-1} + q_{k-2} \geq 2q_{k-2}$.]

۹. کسرهای مسلسل سادهٔ متناظر با ۳٫۱۴۱۶ و ۳٫۱۴۱۵۹ را به‌دست آورید.

۱۰. اگر $C_k = p_k/q_k$، k امین همگرای کسر مسلسل سادهٔ $[a_0; a_1 \ldots, a_n]$ باشد و $a_0 > 0$، نشان دهید

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0]$$

و

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_2, a_1]$$

[راهنمایی: توجه کنید که در مورد نخست، داریم $\frac{p_k}{p_k - 1} = a_k + \frac{p_{k-2}}{p_{k-1}} = a_k + \frac{1}{\frac{p_{k-1}}{p_{k-2}}}$.]

۱۱. جوابهای عمومی هر یک از معادله‌های دیوفانتی زیر را با استفاده از کسرهای مسلسل تعیین کنید:

(الف) $19x + 51y = 1$ (ب) $364x + 227y = 1$

(پ) $18x + 5y = 24$ (ت) $158x - 57y = 1$

۱۲. درستی قضیهٔ ۱۳ـ۸ را به‌ازای کسر مسلسل سادهٔ $[1; 1, 1, 1, 1, 1, 1, 1]$ تحقیق کنید.

۱۳ـ۴ کسرهای مسلسل نامتناهی

تا اینجا فقط کسرهای مسلسل متناهی بررسی شده‌اند؛ این کسرها، وقتی ساده‌اند، عددهای گویا را نمایش می‌دهند. یکی از کاربردهای عمدهٔ نظریهٔ کسرهای مسلسل پیداکردن مقدارهای تقریبی عددهای گنگ است. بنابراین، مفهوم کسر مسلسل نامتناهی ضروری است.

اگر $a_۰$، $a_۱$، $a_۲$، ... دنباله‌ای نامتناهی از عددهای صحیح و همه، احتمالاً بجز $a_۰$، مثبت باشند، آنگاه عبارت

$$a_۰ + \cfrac{۱}{a_۱ + \cfrac{۱}{a_۲ + \cfrac{۱}{a_۳ + \ddots}}}$$

که به‌صورت ساده‌تر $[a_۰; a_۱, a_۲, \ldots]$ نشان داده می‌شود، کسر مسلسل سادهٔ نامتناهی نامیده می‌شود. برای اینکه معنایی ریاضی به این عبارت بدهیم، ملاحظه می‌کنیم که هر یک از کسرهای مسلسل متناهی

$$C_n = [a_۰; a_۱, \ldots, a_n] \qquad (n \geq ۰)$$

تعریف می‌شوند، بنابراین، منطقی به‌نظر می‌رسد که مقدار کسر مسلسل نامتناهی $[a_۰; a_۱, a_۲, \ldots]$ را به‌صورت حد دنبالهٔ عددهای گویای C_n، البته در صورت وجود این حد، تعریف کنیم. به تسامح، نماد $[a_۰; a_۱, a_۲, \ldots]$ را نه تنها برای نشان دادن کسر مسلسل نامتناهی، بلکه به‌عنوان مقدار آن نیز به‌کار می‌بریم.

مسألهٔ وجود حد فوق به‌آسانی قابل حل و فصل است. زیرا تحت فرض ما، حد نه تنها موجود است بلکه همیشه عددی گنگ است. برای ملاحظهٔ این مطلب، توجه می‌کنیم که فرمولهای به‌دست آمدهٔ پیشین در مورد کسرهای مسلسل متناهی، در مورد کسرهای مسلسل نامتناهی نیز برقرارند زیرا نحوهٔ استخراج این فرمولها به متناهی بودن کسر بستگی نداشت. اگر از حدهای بالا برای اندیسها صرف‌نظر شود، بنا به قضیهٔ ۱۳ــ۸، C_nها یعنی همگراهای کسر $[a_۰; a_۱, a_۲, \ldots]$ در زنجیره‌ای نامتناهی از نابرابریها صدق می‌کنند

$$C_۰ < C_۲ < C_۴ < \ldots < C_{۲n} < \ldots < C_{۲n+۱} < \ldots < C_۵ < C_۳ < C_۱$$

چون همگراهای با اندیس زوج، $C_{۲n}$ها، دنباله‌ای یکنوای صعودی باکران بالای $C_۱$ تشکیل می‌دهند، به حد αای میل می‌کنند که از هر $C_{۲n}$ای بزرگتر است. همین‌طور، دنبالهٔ یکنوای نزولی متشکل از همگراهای با اندیس فرد، $C_{۲n+۱}$ها، دارای کران پایین $C_۰$ است و بنابراین حد α'ای دارد که از هر $C_{۲n+۱}$ای کوچکتر است. نشان می‌دهیم این دو حد برابرند. با توجه به رابطهٔ

$p_{2n+1}q_{2n} - q_{2n+1}p_{2n} = (-1)^n$ ملاحظه می‌کنیم که

$$\alpha' - \alpha < C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n}q_{2n+1}}$$

و بنابراین

$$0 \leq |\alpha' - \alpha| < \frac{1}{q_{2n}q_{2n+1}} < \frac{1}{q_{2n}^2}$$

چون q_iها با افزایش i بدون محدودیت بزرگ می‌شوند، سمت راست این نابرابری را می‌توان به‌دلخواه کوچک کرد. اگر α' و α برابر نباشند، تناقضی پدید می‌آید (به بیانی دقیقتر، $1/q_{2n}^2$ را می‌توان کوچکتر از مقدار $|\alpha' - \alpha|$ کرد). بنابراین، دو دنبالهٔ متشکل از همگراهایِ با اندیسهای فرد و زوج دارای مقدار حدی یکسان α هستند، و این نشان می‌دهد که دنبالهٔ همگراهای C_n دارای حد α است.

با الهام‌گیری از این نکته‌ها، تعریف زیر را می‌آوریم

تعریف ۱۳ـ۳ اگر $a_0, a_1, a_2, \ldots$ دنباله‌ای نامتناهی از عددهای صحیح باشد، و همهٔ a_iها، بجز احتمالاً a_0، مثبت باشند، آنگاه مقدار کسر مسلسل سادهٔ نامتناهی $[a_0; a_1, a_2 \ldots]$ برابر است با

$$\lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n]$$

باید دوباره تأکید کرد که صفت «ساده» به این معناست که همهٔ مخرجهای جزئی a_k عددهایی صحیح‌اند؛ چون فقط کسرهای مسلسل نامتناهی ساده موردنظرند، از این به بعد، اغلب صفت ساده را حذف می‌کنیم و آنها را کسرهای مسلسل نامتناهی می‌نامیم.

شاید کسر مسلسل نامتناهی $[1; 1, 1, 1, \ldots]$ مقدماتیترین نمونه باشد. مثال ۱۳ـ۱ نشان داد که nامین همگرای $C_n = [1; 1, 1, \ldots, 1]$ متشکل از $n+1$ جملهٔ ۱، برابر است با

$$C_n = \frac{u_{n+1}}{u_n} \qquad (n \geq 0)$$

که خارج‌قسمت عددهای فیبوناتچی متوالی است. اگر x مقدار کسر مسلسل $[1; 1, 1, 1, \ldots, 1]$ باشد، آنگاه

$$x = \lim_{n\to\infty} C_n = \lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \lim_{n\to\infty} \frac{u_n + u_{n-1}}{u_n}$$
$$= \lim_{n\to\infty} 1 + \frac{1}{\dfrac{u_n}{u_{n-1}}} = 1 + \frac{1}{\lim\limits_{n\to\infty}\left(\dfrac{u_n}{u_{n-1}}\right)} = 1 + \frac{1}{x}$$

ازاینجا معادلهٔ درجهٔ دوم $x^{۲}-x-۱=۰$ به‌دست می‌آید که تنها ریشهٔ مثبت آن $x=(۱+\sqrt{۵})/۲$ است. پس

$$\frac{۱+\sqrt{۵}}{۲}=[۱;۱,۱,۱,\ldots]$$

حالتی وجود دارد که به کرات پیش می‌آید و بنابراین شایستهٔ اصطلاحی ویژه است. هر کسر مسلسل نامتناهی مانند $[۳;۱,۲,۱,۶,۱,۲,۱,۶,\ldots]$ که شامل یک دسته مخرجهای جزئی $b_۱,b_۲,\ldots,b_n$ باشد که بینهایت بار تکرار شود، دوره‌ای نامیده می‌شود. معمولاً کسر مسلسل دوره‌ای $[a_۰;a_۱,\ldots,a_m,b_۱,\ldots,b_n,b_۱,\ldots,b_n,\ldots]$ را به‌صورت فشرده‌تر

$$[a_۰;a_۱,\ldots,a_m,\overline{b_۱,\ldots,b_n}]$$

می‌نویسند، که در آن، خط افقی در بالای $b_۱,b_۲,\ldots,b_n$ به این معناست که این دسته از عددهای صحیح به دفعات نامتناهی تکرار می‌شود. اگر $b_۱,b_۲,\ldots,b_n$ کوچکترین دسته از عددهای صحیح باشد که به‌طور مداوم تکرار می‌شود، می‌گوییم که $b_۱,b_۲,\ldots,b_n$ دورهٔ بسط است و طول دوره n است. بنابراین، به‌عنوان مثال، $[۳;\overline{۱,۲,۱,۶}]$ نشان‌دهندهٔ $[۳;۱,۲,۱,۶,۱,۲,۱,۶,\ldots]$ است، که کسر مسلسلی با دورهٔ $۱,۲,۱,۶$ به طول ۴ است.

پیشتر دیدیم که هر کسر مسلسل متناهی با عددی گویا نمایش داده می‌شود. اکنون مقدار کسر مسلسل نامتناهی را بررسی می‌کنیم:

قضیهٔ ۱۳ـ۹ مقدار هر کسر مسلسل نامتناهی عددی گنگ است.

اثبات. فرض می‌کنیم x مقدار کسر مسلسل نامتناهی $[a_۰;a_۱,a_۲,\ldots]$ باشد یعنی x حد دنبالهٔ همگراهای

$$C_n=[a_۰;a_۱,a_۲,\ldots,a_n]=\frac{p_n}{q_n}$$

باشد. چون x اکیداً میان همگراهای متوالی C_n و $C_{n+۱}$ قرار دارد، داریم

$$۰<|x-C_n|<|C_{n+۱}-C_n|=\left|\frac{p_{n+۱}}{q_{n+۱}}-\frac{p_n}{q_n}\right|=\frac{۱}{q_nq_{n+۱}}$$

به‌منظور رسیدن به تناقض، فرض می‌کنیم x عددی گویاست؛ مثلاً $x=a/b$، که در آن a و b عددهای صحیح مثبتی هستند. در این صورت

$$۰<\left|\frac{a}{b}-\frac{p_n}{q_n}\right|<\frac{۱}{q_nq_{n+۱}}$$

و بنابراین، با ضرب کردن در عدد مثبت bq_n داریم

$$\circ < |aq_n - bp_n| < \frac{b}{q_{n+\text{۱}}}$$

یادآوری می‌کنیم که q_iها با افزایش i بدون محدودیت بزرگ می‌شوند. اگر n به اندازه‌ای بزرگ اختیار شود که $b < q_{n+\text{۱}}$، نتیجه می‌شود

$$\circ < |aq_n - bp_n| < \text{۱}$$

این رابطه می‌گوید که عدد صحیح مثبتی، یعنی $|aq_n - bp_n|$، میان ۰ و ۱ وجود دارد، که به‌وضوح غیر ممکن است. □

اکنون این پرسش را مطرح می‌کنیم که آیا ممکن است دو کسر مسلسل نامتناهی متفاوت عدد گنگ واحدی را نمایش دهند یا نه. پیش از ارائهٔ حکم مربوطه، توجه کنید که بنا به ویژگیهای حد می‌توانیم کسر مسلسل نامتناهی $[a_\circ; a_\text{۱}, a_\text{۲}, \ldots]$ را به‌صورت زیر بنویسیم

$$\begin{aligned}
[a_\circ; a_\text{۱}, a_\text{۲}, \ldots] &= \lim_{n\to\infty} [a_\circ; a_\text{۱}, \ldots, a_n] \\
&= \lim_{n\to\infty} \left(a_\circ + \frac{\text{۱}}{[a_\text{۱}; a_\text{۲}, \ldots, a_n]}\right) \\
&= a_\circ + \frac{\text{۱}}{\lim\limits_{n\to\infty} [a_\text{۱}; a_\text{۲}, \ldots, a_n]} \\
&= a_\circ + \frac{\text{۱}}{[a_\text{۱}; a_\text{۲}, a_\text{۳}, \ldots]}
\end{aligned}$$

قضیهٔ ۱۳ـ۱۰ اگر کسرهای مسلسل نامتناهی $[a_\circ; a_\text{۱}, a_\text{۲}, \ldots]$ و $[b_\circ; b_\text{۱}, b_\text{۲}, \ldots]$ برابر باشند، آنگاه به‌ازای هر $n \geq \circ$، $a_n = b_n$.

اثبات. اگر $x = [a_\circ; a_\text{۱}, a_\text{۲}, \ldots]$، آنگاه $C_\circ < x < C_\text{۱}$، که هم‌ارز با $a_\circ < x < a_\circ + \text{۱}/a_\text{۱}$ است. پس، با توجه به اینکه $a_\text{۱} \geq \text{۱}$، داریم $a_\circ < x < a_\circ + \text{۱}$. بنابراین، $[x] = a_\circ$، که منظور از $[x]$، نماد سنتی بزرگترین عدد صحیح یا تابع «کروشه» است (بخش ۳.۶).

اکنون فرض می‌کنیم $[a_\circ; a_\text{۱}, a_\text{۲}, \ldots] = x = [b_\circ; b_\text{۱}, b_\text{۲}, \ldots]$ یا، به‌عبارت دیگر

$$a_\circ + \frac{\text{۱}}{[a_\text{۱}; c_\text{۲}, \ldots]} = x = b_\circ + \frac{\text{۱}}{[b_\text{۱}; b_\text{۲}, \ldots]}$$

بنا به نتیجهٔ پاراگراف نخست، داریم $a_۰ = [x] = b_۰$، و از اینجا: $[a_۱; a_۲, \ldots] = [b_۱; b_۲, \ldots]$. با تکرار استدلال نتیجه می‌گیریم $a_۱ = b_۱$ و $[a_۲; a_۳, \ldots] = [b_۲; b_۳, \ldots]$. اکنون به استقرای ریاضی معلوم می‌شود که به‌ازای هر $n \geq ۰$، $a_n = b_n$. □

فرع. دو کسر مسلسل نامتناهی متمایز نشان‌دهندهٔ دو عدد گنگ متمایزند.

مثال ۱۳ـ۴

برای تعیین عدد گنگ یکتایی که به‌وسیلهٔ کسر مسلسل نامتناهی $x = [۳; ۶, \overline{۱, ۴}]$ نمایش داده می‌شود، می‌نویسیم $x = [۳; ۶, y]$ که در آن

$$y = [\overline{۱, ۴}] = [۱; ۴, y]$$

در این صورت

$$y = ۱ + \cfrac{۱}{۴ + \cfrac{۱}{y}} = ۱ + \frac{y}{۴y + ۱} = \frac{۵y + ۱}{۴y + ۱}$$

یا

$$۴y^۲ - ۴y - ۱ = ۰$$

چون $y > ۰$ و این معادلهٔ درجهٔ دوم فقط یک ریشهٔ مثبت دارد، نتیجه می‌گیریم که

$$y = \frac{۱ + \sqrt{۲}}{۲}$$

بنابراین، با توجه به اینکه $x = [۳; ۶, y]$، داریم

$$x = ۳ + \cfrac{۱}{۶ + \cfrac{۱}{\cfrac{۱ + \sqrt{۲}}{۲}}} = \frac{۲۵ + ۱۹\sqrt{۲}}{۸ + ۶\sqrt{۲}}$$

$$= \frac{(۲۵ + ۱۹\sqrt{۲})(۸ - ۶\sqrt{۲})}{(۸ + ۶\sqrt{۲})(۸ - ۶\sqrt{۲})} = \frac{۱۴ - \sqrt{۲}}{۴}$$

یعنی، $[۳; ۶, \overline{۱, ۴}] = (۱۴ - \sqrt{۲})/۴$. ■

قضیهٔ فوق نشان می‌دهد که هر کسر مسلسل نامتناهی نمایش دهندهٔ عدد گنگ یکتایی است. اکنون، به‌عکس، نشان می‌دهیم هر عدد گنگ $x_\circ$ را می‌توان به‌صورت یک کسر مسلسل نامتناهی $[a_\circ, a_۱, a_۲, \ldots]$، که به مقدار $x_\circ$ میل می‌کند، بسط داد. دنبالهٔ عددهای صحیح $a_\circ$، $a_۱$، $a_۲$، ... چنین تعریف می‌شود: نخست با استفاده از تابع کروشه قرار می‌دهیم

$$x_۱ = \frac{۱}{x_\circ - [x_\circ]},\ x_۲ = \frac{۱}{x_۱ - [x_۱]},\ x_۳ = \frac{۱}{x_۲ - [x_۲]}, \ldots$$

سپس قرار می‌دهیم

$$a_\circ = [x_\circ],\ a_۱ = [x_۱],\ a_۲[x_۲],\ a_۳[x_۳], \ldots$$

به‌طور کلی، a_kها به استقرا به‌صورت زیر تعریف می‌شوند

$$k \geq \circ \qquad ،x_{k+۱} = \frac{۱}{x_k - a_k} \qquad ،a_k = [x_k]$$

هرگاه x_k گنگ باشد، $x_{k+۱}$ نیز به‌وضوح گنگ است، و چون بحث را به حالتی محدود کرده‌ایم که $x_\circ$ عددی گنگ است، همهٔ x_kها به استقرا گنگ‌اند. بنابراین

$$\circ < x_k - a_k = x_k - [x_k] < ۱$$

و ملاحظه می‌کنیم که

$$x_{k+۱} = \frac{۱}{x_k - a_k} > ۱$$

یعنی، به‌ازای هر $k \geq \circ$، $a_{k+۱} = [x_{k+۱}] \geq ۱$. پس با این فرایند به دنباله‌ای نامتناهی از عددهای صحیح $(a_\circ, a_۱, a_۲, \ldots)$ می‌رسیم که همهٔ جمله‌های آن، مگر احتمالاً $a_\circ$، مثبت‌اند.

با به‌کارگیری تعریف استقراییمان به‌صورت

$$x_k = a_k + \frac{۱}{x_{k+۱}} \qquad (x \geq \circ)$$

و با جایگزینیهای متوالی، به‌ازای هر عدد صحیح مثبت n به‌دست می‌آوریم

$$\begin{aligned} x_0 &= a_0 + \cfrac{1}{x_1} \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}} \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{x_3}}} \\ &\vdots \\ &= [a_0; a_1, a_2, \ldots, a_n, x_{n+1}] \end{aligned}$$

اکنون حدس می‌زنیم و باید نشان دهیم که x_0 مقدار کسر مسلسل نامتناهی $[a_0; a_1, a_2, \ldots]$ است.

به‌ازای هر n ثابتی، $n+1$ همگرای نخست $C_k = p_k/q_k$، $0 \leq k \leq n$، از $[a_0; a_1, a_2, \ldots]$، با $n+1$ همگرای نخست کسر مسلسل متناهی $[a_0; a_1, a_2, \ldots, a_n, x_{n+1}]$ یکی هستند. اگر $(n+2)$امین همگرای کسر اخیر را با C'_{n+1} نشان دهیم، استدلال مورد استفاده در اثبات قضیهٔ ۱۳ـ۶ برای به‌دست آوردن C_{n+1} از C_n با قرار دادن $a_n + 1/a_{n+1}$ به‌جای a_n، در وضعیت فعلی نیز کارساز است؛ به این ترتیب می‌توانیم C'_{n+1} را از C_n با قرار دادن x_{n+1} به‌جای a_{n+1} به‌دست آوریم

$$\begin{aligned} x_0 = C'_{n+1} &= [a_0; a_1, a_2, \ldots, a_n, x_{n+1}] \\ &= \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} \end{aligned}$$

بنابراین

$$\begin{aligned} x_0 - C_n &= \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{(-1)(p_n q_{n-1} - q_n p_{n-1})}{(x_{n+1}q_n + q_{n-1})q_n} = \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n} \end{aligned}$$

که رابطهٔ آخر مبتنی‌بر قضیهٔ ۱۳ـ۷ است. به‌علاوه، چون $x_{n+1} > a_{n+1}$،

$$|x_0 - C_n| = \frac{1}{(x_{n+1}q_n + q_{n-1})q_n} < \frac{1}{(a_{n+1}q_n + q_{n-1})q_n} = \frac{1}{q_{n+1}q_n}$$

چون عددهای صحیح q_k صعودی‌اند، نتیجه می‌گیریم

$$x_\circ = \lim_{n\to\infty} C_n = [a_\circ; a_۱, a_۲, \ldots]$$

این نتیجه‌ها را در قالب قضیهٔ زیر جمعبندی می‌کنیم.

قضیهٔ ۱۳ـ۱۱ هر عدد گنگی دارای نمایش یکتایی به‌صورت یک کسر مسلسل نامتناهی است، و این نمایش از الگوریتم کسر مسلسل که در بالا شرح داده شد به‌دست می‌آید.

ضمناً، استدلال ما روشنگر نتیجه‌ای است که شایسته است جداگانه ذکر شود.

فرع. اگر p_n/q_n، nامین همگرای متناظر با عدد گنگ x باشد، آنگاه

$$|x - \frac{p_n}{q_n}| < \frac{۱}{q_{n+۱}q_n} < \frac{۱}{q_n^۲}$$

برای روشن ساختن نحوهٔ استفاده از الگوریتم کسر مسلسل در پیداکردن نمایش عدد گنگ مفروض به‌صورت کسر مسلسل نامتناهی، دو مثال می‌آوریم.

مثال ۱۳ـ۵

به‌عنوان مثال نخست، $x = \sqrt{۲۳} \approx ۴٫۸$ را درنظر می‌گیریم. عددهای گنگ متوالی x_k (و بنابراین عددهای صحیح $a_k = [x_k]$) را تقریباً به‌آسانی می‌توان حساب کرد. محاسبات را در زیر ملاحظه می‌کنید

$$x_\circ = \sqrt{۲۳} = ۴ + (\sqrt{۲۳} - ۴) \qquad a_\circ = ۴$$

$$x_۱ = \frac{۱}{x_\circ - [x_\circ]} = \frac{۱}{\sqrt{۲۳} - ۴} = \frac{\sqrt{۲۳} + ۴}{۷} = ۱ + \frac{\sqrt{۲۳} - ۳}{۷} \qquad a_۱ = ۱$$

$$x_۲ = \frac{۱}{x_۱ - [x_۱]} = \frac{۷}{\sqrt{۲۳} - ۳} = \frac{\sqrt{۲۳} + ۳}{۲} = ۳ + \frac{\sqrt{۲۳} - ۳}{۲} \qquad a_۲ = ۳$$

$$x_۳ = \frac{۱}{x_۲ - [x_۲]} = \frac{۲}{\sqrt{۲۳} - ۳} = \frac{\sqrt{۲۳} + ۳}{۷} = ۱ + \frac{\sqrt{۲۳} - ۴}{۷} \qquad a_۳ = ۱$$

$$x_۴ = \frac{۱}{x_۳ - [x_۳]} = \frac{۷}{\sqrt{۲۳} - ۴} = \sqrt{۲۳} + ۴ = ۸ + (\sqrt{۲۳} - ۴) \qquad a_۴ = ۸$$

چون $x_۱ = x_۵$، نیز $x_۲ = x_۶$، $x_۳ = x_۷$، $x_۴ = x_۸$، به‌دست می‌آوریم $x_۱ = x_۵ = x_۹$ و الی آخر، که نشان می‌دهد دستهٔ عددهای صحیح ۱, ۳, ۱, ۸ بینهایت بار تکرار می‌شود. نتیجه

می‌گیریم بسط $\sqrt{۲۳}$ به‌صورت کسر مسلسل، دوره‌ای است و داریم

$$\sqrt{۲۳} = [۴; ۱, ۳, ۱, ۸, ۱, ۳, ۱, ۸, \dots] = [۴; \overline{۱, ۳, ۱, ۸}] \quad \blacksquare$$

مثال ۱۳ـ۶

برای آوردن مثالی دیگر، تعدادی از همگراهای کسر مسلسل متناظر با عدد

$$\pi = ۳{,}۱۴۱۵۹۲۶۵۳\dots$$

را که طبق تعریف یونانیان باستان، نسبت محیط دایره به قطر آن است، درنظر می‌گیریم. حرف π، که از واژهٔ یونانی «پریمتروس» گرفته شده، هرگز در دوران باستان به معنای این نسبت به‌کار نمی‌رفت؛ اویلر بود که π را به معنای مزبور در کتابهای درسی معروف متعددش به‌کار برد و شناخت و استفاده از آن را در سطح وسیعی ترویج کرد.

با محاسبه‌هایی سر راست ملاحظه می‌شود که

$$\begin{array}{ll}
x_۰ = \pi = ۳ + (\pi - ۳) & a_۰ = ۳ \\
x_۱ = \dfrac{۱}{x_۰ - [x_۰]} = \dfrac{۱}{۰{,}۱۴۱۵۹۲۶۵\dots} = ۷{,}۰۶۲۵۱۳۳۰\dots & a_۱ = ۷ \\
x_۲ = \dfrac{۱}{x_۱ - [x_۱]} = \dfrac{۱}{۰{,}۰۶۲۵۱۳۳۰\dots} = ۱۵{,}۹۹۶۵۹۴۴۰ & a_۲ = ۱۵ \\
x_۳ = \dfrac{۱}{x_۲ - [x_۲]} = \dfrac{۱}{۰{,}۹۹۶۵۹۴۴۰\dots} = ۱{,}۰۰۳۴۱۷۲۳ & a_۳ = ۱ \\
x_۴ = \dfrac{۱}{x_۳ - [x_۳]} = \dfrac{۱}{۰{,}۰۰۳۴۱۷۲۳\dots} = ۲۹۲{,}۶۳۷۲۴ & a_۴ = ۲۹۲ \\
\vdots &
\end{array} \quad \blacksquare$$

بنابراین، کسر مسلسل نامتناهی متناظر با π به‌صورت

$$\pi = [۳; ۷, ۱۵, ۱, ۲۹۲, \dots]$$

است، ولی، برخلاف مورد $\sqrt{۲۳}$ که در آن همهٔ مخرجهای جزئی a_n معلوم‌اند، الگویی برای ارائهٔ دنبالهٔ کامل a_nها وجود ندارد. پنج همگرای نخست عبارت‌اند از

$$\frac{۳}{۱}, \frac{۲۲}{۷}, \frac{۳۳۳}{۱۰۶}, \frac{۳۵۵}{۱۱۳}, \frac{۱۰۳۹۹۳}{۳۳۱۰۲}$$

برای آزمودن درستی فرع قضیهٔ ۳ـ۱۱ توجه کنید که باید داشته باشیم

$$|\pi - \frac{۲۲}{۷}| < \frac{۱}{۷^۲}$$

ولی $۲۲/۷ > \pi > ۳۱۴/۱۰۰$ و بنابراین، همان‌طور که انتظار داریم

$$|\pi - \frac{۲۲}{۷}| < \frac{۲۲}{۷} - \frac{۳۱۴}{۱۰۰} = \frac{۱}{۷ \times ۵۰} < \frac{۱}{۷^۲}$$

اگر عدد گنگ x به‌صورت بسیار خاصی نباشد، ممکن است تعیین بسط آن به‌صورت کسر مسلسل کامل عملی نباشد. به‌عنوان نمونه، می‌توان ثابت کرد بسط x سرانجام به‌صورت دوره‌ای در می‌آید اگر و تنها اگر x ریشهٔ گنگی از معادلهٔ درجه دومی با ضریبهای صحیح باشد؛ یعنی اگر x به‌صورت $r + s\sqrt{d}$ باشد که در آن، r و $s \neq ۰$ عددهایی گویا باشند و d عددی صحیح مثبت باشد که مربع کامل نیست. میان عددهای گنگ دیگر، تعداد بسیار کمی وجود دارند که بسط آنها از نظمی برخوردار باشد. یکی از این موارد استثنایی، مقدار مثبت دیگری است که سده‌های متمادی توجه ریاضیدانان را به‌خود مشغول داشته است، یعنی

$$e = ۲{,}۷۱۸۲۸۱۸۲۸$$

که پایهٔ دستگاه لگاریتمهای طبیعی است. اویلر در ۱۷۳۷ نشان داد که

$$\frac{e - ۱}{e + ۱} = [۰; ۲, ۶, ۱۰, ۱۴, ۱۸, \ldots]$$

که در آن مخرجهای جزئی تشکیل تصاعدی حسابی می‌دهند، و

$$\frac{e^۲ - ۱}{e^۲ + ۱} = [۰; ۱, ۳, ۵, ۷, ۹, \ldots]$$

نمایش خود e به‌صورت کسر مسلسل (که آن نیز توسط اویلر به‌دست آمد) اندکی پیچیده‌تر است، و به‌صورت

$$e = [۲; ۱, ۲, ۱, ۱, ۴, ۱, ۱, ۶, ۱, ۱, ۸, \ldots]$$

است که در آن، عددهای صحیح زوج به‌ترتیب ظاهر می‌شوند و میان هر دو عدد زوج متوالی، دو تا ۱ قرار دارد. خود نمای e را نیز نخست اویلر به‌کار برد و نخستین بار به‌صورت چاپی در یکی از کتابهای درسی او ظاهر شد.

در آنالیز مقدماتی، معمولاً نشان می‌دهند که e را می‌توان به‌صورت سری نامتناهی

$$e = ۱ + \frac{۱}{۱!} + \frac{۱}{۲!} + \frac{۱}{۳!} + \frac{۱}{۴!} + \dots$$

تعریف کرد. اگر این تعریف را بپذیریم، به‌آسانی می‌توان اثبات اویلر از گنگ بودن e را عرضه کرد: فرض می‌کنیم e عددی گویا باشد مثلاً به‌صورت $e = a/b$، که در آن a و b عددهایی صحیح مثبت‌اند. در این صورت، به‌ازای $n > b$ و نیز $n > ۱$، عدد

$$\begin{aligned} N &= n!\left[e - \left(۱ + \frac{۱}{۱!} + \frac{۱}{۲!} + \dots + \frac{۱}{n!}\right)\right] \\ &= n!\left(\frac{a}{b} - ۱ - \frac{۱}{۱!} - \frac{۱}{۲!} - \dots - \frac{۱}{n!}\right) \end{aligned}$$

عدد صحیح مثبتی است. اگر به‌جای e بسط آن را به‌صورت سری درنظر بگیریم، نتیجه می‌شود

$$\begin{aligned} N &= \frac{۱}{n+۱} + \frac{۱}{(n+۱)(n+۲)} + \frac{۱}{(n+۱)(n+۲)(n+۳)} + \dots \\ &< \frac{۱}{n+۱} + \frac{۱}{(n+۱)(n+۲)} + \frac{۱}{(n+۲)(n+۳)} \dots \\ &= \frac{۱}{n+۱} + \left(\frac{۱}{n+۱} - \frac{۱}{n+۲}\right) + \left(\frac{۱}{n+۲} - \frac{۱}{n+۳}\right) + \dots \\ &= \frac{۲}{n+۱} < ۱ \end{aligned}$$

چون برقراری نابرابری $۰ < N < ۱$ به‌ازای عددی صحیح ممکن نیست، e باید گنگ باشد. طبیعت خاص عدد π متضمن پیچیدگیهای بیشتری است؛ در ۱۷۶۱، لامبرت[1] (۱۷۲۸ـ۱۷۷۷)، اثباتی اساساً دقیق از گنگ بودن π به آکادمی علوم برلین ارائه کرد.

اگر x عددی گنگ باشد، طبیعی است که بخواهیم بدانیم x را با چه میزان دقتی می‌توان با عددهای گویا تقریب زد. یکی از روشهای بررسی این مسأله درنظرگرفتن همهٔ عددهای گویا با مخرج ثابت $b > ۰$ است. چون x میان دو عدد گویا از این نوع قرار دارد، مثلاً $c/b < x < (c+۱)/b$، نتیجه می‌شود

$$\left|x - \frac{c}{b}\right| < \frac{۱}{b}$$

و بهتر از این، می‌توانیم بنویسیم

$$\left|x - \frac{a}{b}\right| < \frac{۱}{۲b}$$

1. J. H. Lambert

که در آن، $a = c$ یا $a = c + ۱$، بسته به اینکه کدام یک مناسب باشد. فرایند کسر مسلسل امکان اثبات حکمی را فراهم کرد که به‌وسیلهٔ آن می‌توان نابرابری اخیر را به‌میزان قابل توجهی قویتر کرد، یعنی: به‌ازای هر عدد گنگ x، بینهایت عدد گویای a/b به ساده‌ترین صورت ممکن وجود دارند به‌طوری که

$$\left|x - \frac{a}{b}\right| < \frac{۱}{b^۲}$$

در واقع، بنا به فرع قضیهٔ ۱۳ـ۱۱، هر یک از همگراهای p_n/q_n در بسط x به‌صورت کسر مسلسل می‌تواند نقش عدد گویای a/b را ایفا کند. بنا به قضیهٔ بعدی، همگراهای p_n/q_n بهترین تقریبهای x در میان همهٔ عددهای گویای a/b با مخرجهای نابیشتر از q_n هستند.

برای وضوح مطلب، بخش تکنیکی قضیه را در قالب لم زیر ارائه می‌کنیم.

لم. فرض می‌کنیم p_n/q_n، nامین همگرای کسر مسلسل نمایش‌دهندهٔ عدد گنگ x باشد. اگر a و b عددهایی صحیح باشند و $۱ \leq b \leq q_{n+۱}$، آنگاه

$$|q_n x - p_n| \leq |bx - a|$$

اثبات. دستگاه معادله‌های

$$p_n\alpha + p_{n+۱}\beta = a$$
$$q_n\alpha + q_{n+۱}\beta = b$$

را درنظر می‌گیریم. چون دترمینان ضریبها برابر با $p_n q_{n+۱} - q_n p_{n+۱} = (-۱)^{n+۱}$ است، دستگاه دارای جواب صحیح یکتای

$$\alpha = (-۱)^{n+۱}(aq_{n+۱} - bp_{n+۱})$$
$$\beta = (-۱)^{n+۱}(bp_n - aq_n)$$

است. جالب توجه است که $\alpha \neq ۰$. در واقع، از $\alpha = ۰$ نتیجه می‌شود $aq_{n+۱} = bp_{n+۱}$ و چون $\gcd(p_{n+۱}, q_{n+۱}) = ۱$، لازم می‌آید $q_{n+۱} | b$ یا $b \geq q_{n+۱}$، که برخلاف فرض است. در حالتی که $\beta = ۰$، نابرابری مذکور در لم به‌وضوح برقرار است. زیرا اگر $\beta = ۰$، لازم می‌آید $a = p_n\alpha$، $b = q_n\alpha$ و، در نتیجه

$$|bx - a| = |\alpha|\ |q_n x - p_n| \geq |q_n x - p_n|$$

بنابراین، می‌توانیم از این به بعد فرض کنیم که $\beta \neq 0$.

به‌فرض $\beta \neq 0$، نشان می‌دهیم α و β باید مختلف‌العلامت باشند. اگر $\beta < 0$، از معادلهٔ $q_n\alpha = b - q_{n+1}\beta$ نتیجه می‌شود $q_n\alpha > 0$ و، بنابراین، $\alpha > 0$. از سوی دیگر، اگر $\beta > 0$، آنگاه از $b < q_{n+1}$ لازم می‌آید $b < \beta q_{n+1}$، و بنابراین $\alpha q_n = b - q_{n+1}\beta < 0$؛ پس $\alpha < 0$.

همچنین نتیجه می‌گیریم که، چون x میان همگراهای متوالی p_n/q_n و p_{n+1}/q_{n+1} است

$$q_{n+1}x - p_{n+1} \quad \text{و} \quad q_n x - p_n$$

مختلف‌العلامت‌اند. نکتهٔ اصلی این استدلال این است که عددهای

$$\beta(q_{n+1}x - p_{n+1}) \quad \text{و} \quad \alpha(q_n x - p_n)$$

باید همعلامت باشند؛ در نتیجه، قدر مطلق مجموعشان با مجموع قدر مطلقهایشان برابر است. به‌دلیل همین حقیقت اساسی است که می‌توانیم به‌آسانی اثبات را کامل کنیم

$$\begin{aligned}
|bx - a| &= |(q_n\alpha + q_{n+1}\beta)x - (p_n\alpha + p_{n+1}\beta)| \\
&= |\alpha(q_n x - p_n) + \beta(q_{n+1}x - p_{n+1})| \\
&= |\alpha||q_n x - p_n| + |\beta||q_{n+1}x - p_{n+1}| \\
&> |\alpha||q_n x - p_n| \geq |q_n x - p_n|
\end{aligned}$$

که همان نابرابری مطلوب است. □

همگراهای p_n/q_n از این نظر بهترین تقریبهای عدد گنگ x هستند که اختلاف x با هر عدد گویای دیگری با مخرج q_n یا مخرج کوچکتر، بزرگتر از $|x - p_n/q_n|$ است.

قضیهٔ ۱۳ـ۱۲ اگر a/b عددی گویا باشد و $1 \leq b \leq q_n$، آنگاه

$$\left|x - \frac{p_n}{q_n}\right| \leq \left|x - \frac{a}{b}\right|$$

اثبات. اگر

$$\left|x - \frac{p_n}{q_n}\right| > \left|x - \frac{a}{b}\right|$$

لازم می‌آید

$$\begin{aligned}|q_n x - p_n| &= q_n \left|x - \frac{p_n}{q_n}\right| > b\left|x - \frac{a}{b}\right| \\ &= |bx - a|\end{aligned}$$

که مغایر با حکم لم است. □

مورخان ریاضیات توجه زیادی به تلاشهای جوامع قدیم در به‌دست آوردن تقریبی از π مبذول داشته‌اند، و دلیل آن شاید این باشد که دقت فزایندهٔ نتیجه‌ها در این زمینه، ظاهراً شاخصی از مهارتهای ریاضی تمدنهای گوناگون به‌دست می‌دهد. نخستین اثر مکتوب از تلاش علمی برای محاسبهٔ π در رسالهٔ اندازه‌گیری دایره اثر ارشمیدس (۲۸۷ـ۲۱۲ پیش از میلاد) ریاضیدان بزرگ سیراکوز باستانی دیده می‌شود. در واقع، روش او برای پیدا کردن مقدار π مبتنی‌بر محاط کردن چند ضلعیهایی منتظم در دایره و محیط کردن چند ضلعیهایی منتظم بر آن، تعیین محیطهای آنها، و استفاده از این محیطها به‌عنوان کرانهای پایین و بالای محیط دایره بود. به این روش، و با استفاده از یک ۹۶ ضلعی، دو تقریب مذکور در نابرابری $۲۲/۷ > \pi > ۲۲۳/۷۱$ را به‌دست آورد.

با توجه به قضیهٔ ۱۳ـ۱۲، دلیل استفادهٔ فراوان از ۲۲/۷، موسوم به «مقدار ارشمیدسی π» به‌جای π معلوم می‌شود؛ کسر ساده‌ای با مخرج کوچکتر برای تقریب بهتر وجود ندارد. گرچه

$$\left|\pi - \frac{۲۲}{۷}\right| \approx ۰٫۰۰۱۲۶۴۵ \quad \text{و} \quad \left|\pi - \frac{۲۲۳}{۷۱}\right| \approx ۰٫۰۰۰۷۴۷۶$$

مقدار ارشمیدسی ۲۲۳/۷۱ که همگرایی از π نیست، مخرجی بزرگتر از $q_۲ = ۷$ دارد. بنا به قضیهٔ ۱۳ـ۱۲، ۳۳۳/۱۰۶ (تقریبی از π که در اروپای سدهٔ شانزدهم به‌کار می‌رفت) π را بهتر از هر عدد گویایی با مخرج کوچکتر یا برابر با ۱۰۶، تقریب می‌زند؛ در واقع

$$\left|\pi - \frac{۳۳۳}{۱۰۶}\right| \approx ۰٫۰۰۰۰۸۳۲$$

با توجه به اندازهٔ $q_۴ = ۳۳۱۰۲$، همگرای $p_۳/q_۳ = ۳۵۵/۱۱۳$، π را با دقت چشمگیری تقریب می‌زند؛ بنا به فرع قضیهٔ ۱۳ـ۱۱، داریم

$$\left|\pi - \frac{۳۵۵}{۱۱۳}\right| < \frac{۱}{۱۳۳ \times ۳۳۱۰۲} < \frac{۳}{۱۰^۷}$$

تسوچونگ ـ چی[1]، ریاضیدان چین قدیم (۴۳۰ـ۵۰۱) کسر جالب توجه ۳۵۵/۱۱۳ را می‌شناخت؛ او کسر ۲۲/۷ را به‌عنوان «مقدار غیر دقیق» و ۳۵۵/۱۱۳ را به‌عنوان «مقدار دقیق» π به‌دست داد بدون آنکه استدلالی بیاورد. در اروپا تا پایان سدهٔ شانزدهم تقریبی از π که به اندازهٔ کسر اخیر دقیق باشد به‌دست نیاورده بودند. در این زمان آدریان آنتونیسون[2] (۱۵۲۷ـ۱۶۱۷) به کشف دوبارهٔ این مقدار نایل شد.

اکنون مناسب است قضیه‌ای ذکر کنیم که می‌گوید: هر تقریب گویایی از x که (به معنایی مناسب) «نزدیک» به x باشد باید همگرایی از x باشد. اگر می‌توانستیم به‌ازای nای، از

$$\left|x - \frac{a}{b}\right| < \frac{۱}{b^۲}$$

نتیجه بگیریم $a/b = p_n/q_n$، بحث شسته رفته‌تر می‌شد؛ گرچه این توقع نابجاست اما اگر نابرابری را کمی دقیقتر کنیم، این نتیجه به‌دست می‌آید.

قضیهٔ ۱۳ـ۱۳ فرض می‌کنیم x عددی گنگ باشد. اگر عدد گویای a/b با ضابطه‌های $b \geq ۱$ و $\gcd(a, b) = ۱$ در

$$\left|x - \frac{a}{b}\right| < \frac{۱}{۲b^۲}$$

صدق کند، آنگاه a/b یکی از همگراهای p_n/q_n در نمایش کسر مسلسلِ x است.

اثبات. فرض می‌کنیم a/b همگرایی از x نباشد. با توجه به اینکه q_kها دنباله‌ای صعودی تشکیل می‌دهند، ملاحظه می‌کنیم عدد صحیح n یکتایی وجود دارد به‌طوری که $q_n \leq b < q_{n+۱}$. بنا به لم اخیر و به‌ازای این n، نخستین نابرابریِ زنجیرهٔ

$$|q_n x - p_n| \leq |bx - a| = b\left|x - \frac{a}{b}\right| < \frac{۱}{۲b}$$

نتیجه می‌شود و بنابراین

$$\left|x - \frac{p_n}{q_n}\right| < \frac{۱}{۲bq_n}$$

با توجه به فرض $a/b \neq p_n/q_n$، تفاضل $bp_n - aq_n$ عدد صحیح ناصفری است، و لذا $|bp_n - aq_n| \geq ۱$. بیدرنگ می‌توانیم نتیجه بگیریم که

$$\frac{۱}{bq_n} \leq \left|\frac{bp_n - aq_n}{bq_n}\right| = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{a}{b}\right| < \frac{۱}{۲bq_n} + \frac{۱}{۲b^۲}$$

از اینجا به تناقض $b < q_n$ می‌رسیم، که اثبات را پایان می‌دهد. □

1. Tsu Chung-chih 2. Adriaen Anthoniszoon

تمرینهای ۱۳ـ۴

۱. هر یک از کسرهای مسلسل سادهٔ نامتناهی زیر را حساب کنید

(الف) $[\overline{۲;۳}]$ (ب) $[۰;\overline{۱,۲,۳}]$ (پ) $[۲;\overline{۱,۲,۱}]$

(ت) $[۱;۲,\overline{۳,۱}]$ (ث) $[۱;۲,۱,۲,\overline{۱۲}]$

۲. ثابت کنید که اگر عدد گنگ $x > ۱$ با کسر مسلسل نامتناهی $[a;a_۱,a_۲,\dots]$ نمایش داده شود، آنگاه $۱/x$ دارای بسط $[۰;a_۰,a_۱,a_۲,\dots]$ است. با استفاده از این مطلب، مقدار $[۰;\overline{۱}] = [۰;۱,۱,۱,\dots]$ را پیدا کنید.

۳. $[۱;۲,\overline{۱}]$ و $[۱;۲,۳,\overline{۱}]$ را حساب کنید.

۴. هر یک از عددهای گنگ زیر را به‌صورت کسر مسلسل نامتناهی نمایش دهید

(الف) $\sqrt{۵}$ (ب) $\sqrt{۷}$ (پ) $\dfrac{۱+\sqrt{۱۳}}{۲}$

(ت) $\dfrac{۵+\sqrt{۳۷}}{۴}$ (ث) $\dfrac{۱۱+\sqrt{۳۰}}{۱۳}$

۵. (الف) نشان دهید که به‌ازای هر عدد صحیح مثبت n، $\sqrt{n^۲+۱} = [n;\overline{۲n}]$، $\sqrt{n^۲+۲} = [n;\overline{n,۲n}]$ و $\sqrt{n^۲+۲n} = [n;\overline{۱,۲n}]$. [راهنمایی: توجه کنید که

$$n+\sqrt{n^۲+۱} = ۲n + (\sqrt{n^۲+۱}-n)$$
$$\Big[= ۲n + \frac{۱}{n+\sqrt{n^۲+۱}}\Big]$$

(ب) با استفاده از (الف) نمایشهای $\sqrt{۲}$، $\sqrt{۳}$، $\sqrt{۱۵}$ و $\sqrt{۳۷}$ به‌صورت کسر مسلسل را به‌دست آورید.

۶. از میان همگراهای $\sqrt{۱۵}$، عددی گویا پیدا کنید که $\sqrt{۱۵}$ را با دقت چهار رقم اعشار تقریب بزند.

۷. (الف) تقریبی گویا از $e = [۲;۱,۲,۱,۱,۴,۱,۱,۶,\dots]$ پیدا کنید که تا چهار رقم اعشار درست باشد.

(ب) اگر a و b عددهایی صحیح مثبت باشند و $e < a/b < ۸۷/۳۲$، نشان دهید $b \geq ۳۹$.

۸. ثابت کنید از میان هر دو همگرای متوالی عدد گنگ x، حداقل یکی، مثلاً a/b، در نابرابری

$$\left|x-\frac{a}{b}\right| < \frac{۱}{۲b^۲}$$

صدق می‌کند.

[راهنمایی: چون x میان هر دو همگرای متوالی قرار دارد،

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|x - \frac{p_{n+1}}{q_{n+1}}\right| + \left|x - \frac{p_n}{q_n}\right|$$

سپس، به برهان خلف استدلال کنید.]

۹. بهترین تقریب گویای a/b را برای کسر مسلسل نامتناهی $[1; 3, 1, 5, 1, 7, 1, 9, \ldots]$ طوری پیدا کنید که

(الف) $b < 25$ ؛ (ب) $b < 225$

۱۰. نخست نشان دهید $|(1 + \sqrt{10})/3 - 18/13| < 1/(2 \times 13^2)$؛ و سپس نشان دهید که $18/13$ همگرایی از $(1 + \sqrt{10})/3$ است.

۱۱. قضیهٔ معروفی از هورویتس (۱۹۸۱) حاکی است که به‌ازای هر عدد گنگ x، تعداد نامتناهی عدد گویای a/b وجود دارد به‌طوری که

$$\left|x - \frac{a}{b}\right| < \frac{1}{\sqrt{5} b^2}$$

به‌ازای $x = \pi$، سه عدد گویا طوری پیدا کنید که در این نابرابری صدق کنند.

۱۲. فرض کنید نمایش عدد گنگ x به‌صورت کسر مسلسل، بالاخره دوره‌ای شود. با روش به‌کار رفته در مثال ۱۳ـ۴ ثابت کنید x به‌صورت $r + s\sqrt{d}$ است، که در آن r و $s \neq 0$ عددهایی گویا هستند و $d > 0$ عددی صحیح و نامربع است.

۱۳. اگر x عددی گنگ با همگراهای p_n/q_n باشد، نشان دهید که به‌ازای هر $n \geq 0$ داریم

(الف)
$$\frac{1}{2 q_n q_{n+1}} < \left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

(ب) همگراها متوالیاً به x نزدیکتر می‌شوند به این معنی که

$$\left|x - \frac{p_n}{q_n}\right| < \left|x - \frac{p_{n-1}}{q_{n-1}}\right|$$

[راهنمایی: معادلهٔ

$$x = \frac{x_{n+1} q_n + p_{n-1}}{x_{n+1} q_n + q_{n-1}}$$

را به‌صورت

$$x_{n+1}(x q_n - p_n) = -q_{n-1}\left(x - \frac{p_{n-1}}{q_{n-1}}\right)$$

بنویسید.]

۱۳ـ۵ معادلهٔ پِل[1]

اقدامات اندکی که فرما برای معرفی کشفهایش انجام داد، به شکل دعوت از ریاضیدانان دیگر به مبارزه و رقابت بود. شاید امیدوار بود به این روش آنها را متقاعد سازد که شیوهٔ جدید او در نظریهٔ اعداد شایستهٔ پیگیری است. فرما در ژانویهٔ ۱۶۵۷ دو مسأله به جامعهٔ ریاضی اروپا پیشنهاد کرد ــ شاید منظور وی در وهلهٔ نخست، جان والیس، مشهورترین ریاضیدان حرفه‌ای انگلستان پیش از نیوتون بود:

۱. مکعبی پیدا کنید که حاصل جمع آن با مجموع مقسوم‌علیه‌های سره‌اش مربع کامل باشد؛ به‌عنوان مثال $۲۰^۲ = (۱ + ۷ + ۷^۲) + ۷^۳$.

۲. مربعی پیدا کنید که حاصل جمع آن با مجموع مقسوم‌علیه‌های سره‌اش مکعب باشد.

برنار فرنیکل د بسی ، طرف مکاتبهٔ مورد علاقهٔ فرما، به محض اطلاع از موضوع، جوابهایی برای مسأله نخست ارائه کرد؛ مثلاً $(۴۷ \times ۴۱ \times ۱۳ \times ۵ \times ۳ \times ۲)^۳$، که اگر با مجموع مقسوم‌علیه‌های سره‌اش جمع شود، مجموع حاصل برابر با $(۲۹ \times ۱۷ \times ۱۳ \times ۷ \times ۵^۲ \times ۳^۲ \times ۲^۷)^۲$ خواهد شد. در حالی‌که فرنیکل سرگرم جستجوی جوابهایی متشکل از عددهای مرکب بزرگتر بود، والیس مسأله‌های مزبور را شایستهٔ بررسی ندانست و نوشت «صرف‌نظر از محتوای مسأله‌ها، به‌اندازه‌ای گرفتارم که فعلاً نمی‌توانم وقتی به آنها اختصاص دهم؛ مع‌الوصف، ۱ تنها جوابی است که در این لحظه می‌توانم ارائه کنم: عدد ۱ به تنهایی در هر دو مسأله صدق می‌کند.» فرنیکل در حالی‌که به زحمت دلخوریش را پنهان می‌کرد، از اینکه ریاضیدانی با تجربه مانند والیس فقط پاسخی بدیهی ارائه کرده است و با جدیتر نگرفتن مسأله، شأن فرما را رعایت نکرده است، ابراز شگفتی کرد.

در واقع علاقهٔ فرما معطوف به روشهای کلی بود نه به محاسبهٔ کسل‌کنندهٔ حالتهای خاص. هم فرنیکل و هم والیس از جنبهٔ نظری این مسأله‌های تأمل‌انگیز، که در صورت بررسی دقیق آشکار می‌شد، غفلت کردند. گرچه صورت مسأله‌ها کاملاً دقیق نبود، واضح به‌نظر می‌رسد که منظور فرما این بوده که مسألهٔ نخست فقط به‌ازای مکعب عددهای اول حل شود. به بیان دیگر، خواست مسأله تعیین همهٔ جوابهای صحیح معادلهٔ

$$۱ + x + x^۲ + x^۳ = y^۲$$

بوده است که هم‌ارز با

$$(۱ + x)(۱ + x^۲) = y^۲$$

است و x عدد فردی است. چون ۲ تنها عدد اولی است که هر دو عامل سمت چپ این معادله

---

1. Pell

را می‌شمارد، می‌توان معادله را به‌صورت

$$ab = \left(\frac{y}{۲}\right)^۲ \qquad \gcd(a,b) = ۱$$

نوشت. ولی اگر حاصلضرب دو عدد صحیح متباینْ مربعی کامل باشد، هر یک از آنها نیز باید مربع کامل باشد؛ پس به‌ازای u و vای داریم

$$۱ + x = ۲a = ۲u^۲ \qquad ، \qquad ۱ + x^۲ = ۲b = ۲v^۲$$

این نشان می‌دهد که هر عدد صحیح xای که در مسألهٔ نخست فرما صدق می‌کند، باید در دو معادلهٔ

$$x = ۲u^۲ - ۱، \qquad x^۲ = ۲v^۲ - ۱$$

نیز صادق باشد که دومی حالت خاصی از معادلهٔ $x^۲ = dy^۲ \pm ۱$ است.

در فوریهٔ ۱۶۵۷، فرما به دومین مبارزطلبی خود دست زد که این بار مستقیماً در قالبی نظری بود: عدد y را طوری پیدا کنید که $dy^۲ + ۱$، که در آن d عددی صحیح و مثبت و غیر مربع است، مربع کامل باشد؛ به‌عنوان مثال، $۲^۲ = ۱ + ۱^۲ \times ۳$ و $۹^۲ = ۱ + ۴^۲ \times ۵$. فرما اضافه کرد که اگر نتوانستید قاعده‌ای کلی بیابید، کوچکترین مقدار y را طوری پیدا کنید که به‌ازای آن $x^۲ = ۱ + ۶۱y^۲$؛ یا $x^۲ = ۱ + ۱۰۹y^۲$. فرنیکل آغاز به محاسبهٔ کوچکترین جوابهای مثبت $x^۲ - dy^۲ = ۱$ به‌ازای همه مقدارهای مجاز d تا ۱۵۰ کرد و پیشنهاد کرد والیس جدول مربوط را تا $d = ۲۰۰$ کامل کند، یا لااقل $x^۲ - ۱۵۱y^۲ = ۱$ و $x^۲ - ۳۱۳y^۲ = ۱$ را حل کند، و اشاره کرد که احتمالاً حل معادلهٔ دومی در توان والیس نیست. در پاسخ، لرد ویلیام برونکر[1] ایرلندی، حامی و مشوق والیس، ادعا کرد که فقط با صرف حدود یک ساعت وقت توانسته است کشف کند که

$$(۱۲۶۸۶۲۳۶۸)^۲ - ۳۱۳(۷۱۷۰۶۸۵)^۲ = -۱$$

و بنابراین $y = ۲ \times ۷۱۷۰۶۸۵ \times ۱۲۶۸۶۲۳۶۸$ جوابی از $x^۲ - ۳۱۳y^۲ = ۱$ است؛ والیس با ارائهٔ

$$(۱۷۲۸۱۴۸۰۴۰)^۲ - ۱۵۱(۱۴۰۶۳۴۶۹۳)^۲ = ۱$$

مورد مشخص دیگر را حل کرد.

از مقایسهٔ اندازهٔ این عددها با آنهایی که به‌ازای دیگر مقدارهای d به‌دست می‌آیند، چنین بر می‌آید که فرما راه‌حل کامل مسأله را در دست داشت، هر چند هرگز آن را ارائه نکرد (بعدها

1. Brouncker

اظهار داشت که روش نزول نامتناهی‌اش را در اثبات وجود بینهایت جواب برای $x^{۲} - dy^{۲} = ۱$ به‌کار برده است). برونکر با این استنباط نادرست که علاوه‌بر مقدارهای صحیح، مقدارهای گویا نیز مجازند، به‌راحتی جوابی ارائه کرد؛ وی با تقسیم رابطهٔ

$$(r^{۲} + d)^{۲} - d(۲r)^{۲} = (r^{۲} - d)^{۲}$$

بر $(r^{۲} - d)^{۲}$، به‌سادگی به‌جواب

$$y = \frac{۲r}{r^{۲} - d} \quad \text{و} \quad x = \frac{r^{۲} + d}{r^{۲} - d}$$

که در آن $r \neq d$ عدد گویای دلخواهی است، رسید. نیازی به‌گفتن نیست که فرما این جواب را نپذیرفت و نوشت که «جوابهای کسری، که بیدرنگ با استفاده از پیش پاافتاده‌ترین مطالب حساب به‌دست می‌آیند، مورد قبول من نیست». برونکر و والیس سپس با اطلاع از همهٔ شرطهای مسأله، مشترکاً روشی آزمایشی برای حل $x^{۲} - dy^{۲} = ۱$ برحسب عددهای صحیح ابداع کردند ولی نتوانستند کارایی آن‌را در همهٔ موارد ثابت کنند. ظاهراً افتخار این ابداع از آنِ برونکر بود، زیرا والیس با غرور خاصی به‌وی تبریک گفت که نگذاشته است شهرت برتری انگلیسیها بر فرانسویان خدشه‌دار شود.

با این همه، باید خاطرنشان کنیم که تلاش جهتدار فرما برای برقراری سنت جدیدی در حساب از طریق برانگیختن رقابت ریاضی تا حدود زیادی با شکست مواجه شد. صرف‌نظر از فرنیکل، که فاقد استعداد کافی برای جدال فکری با فرما بود، نظریهٔ اعداد جذابیت خاصی برای هیچ از معاصرین او نداشت. این نظریه به بوتهٔ فراموشی سپرده شد تا آنکه اویلر، بعد از گذشت تقریباً یک سده، به مطالعهٔ آن از جایی که فرما رها کرده بود، پرداخت. هم اویلر و هم لاگرانژ به حل مسألهٔ معروف سال ۱۶۵۷ پرداختند. گرچه اویلر (در ۱۷۵۹) با تبدیل $\sqrt{d}$ به یک کسر مسلسل نامتناهی روشی برای تعیین کوچکترین جواب صحیح $x^{۲} - dy^{۲} = ۱$ ابداع کرد، ولی نتوانست نشان دهد که با روش او می‌توان به جوابی بجز $x = ۱$ و $y = ۰$ رسید. رفع این معضل را لاگرانژ به‌عهده گرفت. لاگرانژ برای نخستین بار در ۱۷۶۸، با تکمیل نظریهٔ به‌جا مانده از اویلر، اثبات دقیقی از اینکه همهٔ جوابها با استفاده از بسط $\sqrt{d}$ به‌صورت کسر مسلسل به‌دست می‌آیند، انتشار داد.

براثر انتسابی نادرست، موضوع اصلی رقابت یعنی معادلهٔ $x^{۲} - dy^{۲} = ۱$، به «معادلهٔ پِل» معروف شد. انتساب نادرست حل معادلهٔ مزبور به جان پل (۱۶۱۱ـ۱۶۸۵) ریاضیدان انگلیسی که چندان در این مسأله کار نکرده بود، خطایی غیر عمدی از طرف اویلر بود. اویلر پس از مطالعهٔ شتابزدهٔ رسالهٔ عملهای ریاضی[1] به قلم والیس (۱۶۹۳) که مشتمل بر روش برونکر برای حل

1. Opera Mathematica

معادله و اطلاعاتی دربارهٔ کار پل در آنالیز دیوفانتی است، احتمالاً کارهای آنها را با یکدیگر خلط کرده است: از هر لحاظ منصفانه است که $x^۲ - dy^۲ = ۱$ را «معادلهٔ فرما» بنامیم زیرا وی نخستین کسی بود که این معادله را به‌طور اصولی بررسی کرد. گرچه دیر زمانی از تشخیص اشتباه تاریخی مزبور می‌گذرد، نام پِل همچنان به‌گونه‌ای نازدودنی با این معادله همراه بوده است.

بدیهی است که به‌ازای هر مقدار صحیح d، $x = \pm ۱$، $y = ۰$ در معادلهٔ $x^۲ - dy^۲ = ۱$ صدق می‌کند. اگر $d < -۱$، $x^۲ - dy^۲ \geq ۱$ (مگر به‌ازای $x = y = ۰$) و بنابراین، اینها تنها جوابهای معادله‌اند؛ اگر $d = -۱$ دو جواب دیگر موجودند، یعنی $x = ۰$، $y = \pm ۱$. به‌آسانی می‌توان حالتی را که d مربع کامل باشد کنار گذاشت، زیرا اگر به‌ازای nای، $d = n^۲$، آنگاه $x^۲ - dy^۲ = ۱$ را می‌توان به‌صورت

$$(x + ny)(x - ny) = ۱$$

نوشت که برقرار است اگر و تنها اگر $x + ny = x - ny = \pm ۱$؛ نتیجه می‌شود

$$x = \frac{(x + ny) + (x - ny)}{۲} = \pm ۱$$

و معادله بجز جوابهای بدیهی $x = \pm ۱$، $y = ۰$ جواب دیگری ندارد.

از این پس، بررسی معادلهٔ پل $x^۲ - dy^۲ = ۱$ را به تنها حالت جالب آن، یعنی حالتی که d یک عدد صحیح مثبت نامربع است، محدود می‌کنیم. جواب x، y را جواب مثبت این معادله می‌نامیم در صورتی‌که هم x و هم y مثبت باشند. چون همهٔ جوابها بجز جوابهای با $y = ۰$ را می‌توان برحسب ترکیبات مختلف علامتهای $\pm x$ و $\pm y$ در مجموعه‌های چهارتایی قرار داد، واضح است که به‌محض تعیین همهٔ جوابهای مثبت، همهٔ جوابها به‌دست می‌آیند. به این دلیل، فقط به تعیین جوابهای مثبت $x^۲ - dy^۲ = ۱$ می‌پردازیم.

نقطهٔ شروع کار ما قضیهٔ زیر است که حاکی است هر زوج از عددهای مثبت صحیحی را که در معادلهٔ پِل صدق کند، می‌توان با استفاده از کسر مسلسل نمایش‌دهندهٔ عدد گنگ $\sqrt{d}$ به‌دست آورد.

قضیهٔ ۱۴-۱۳ اگر p، q جواب مثبتی از $x^۲ - dy^۲ = ۱$ باشد، آنگاه p/q همگرایی از بسط کسر مسلسلِ $\sqrt{d}$ است.

اثبات. با توجه به فرض $p^۲ - dq^۲ = ۱$ داریم

$$(p - q\sqrt{d})(p + q\sqrt{d}) = ۱$$

و بنابراین، $p > q\sqrt{d}$ و

$$\frac{p}{q} - \sqrt{d} = \frac{۱}{q(p + q\sqrt{d})}$$

در نتیجه

$$۰ < \frac{p}{q} - \sqrt{d} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{۲q^۲\sqrt{d}} = \frac{۱}{۲q^۲}$$

با توسل مستقیم به قضیهٔ ۱۳ـ۱۳ معلوم می‌شود که p/q باید همگرایی از $\sqrt{d}$ باشد. □

در حالت کلی، عکس قضیهٔ فوق برقرار نیست: هر همگرای p_n/q_n از $\sqrt{d}$ جوابی از $x^۲ - dy^۲ = ۱$ به‌دست نمی‌دهد. مع‌الوصف، دربارهٔ اندازهٔ مقدارهای ممکن دنبالهٔ $p_n^۲ - dq_n^۲$ قضیهٔ زیر برقرار است.

قضیهٔ ۱۳ـ۱۵ اگر p/q همگرایی از بسط کسر مسلسلِ $\sqrt{d}$ باشد، آنگاه $x = p$، $y = q$ جوابی از یکی از معادله‌های

$$x^۲ - dy^۲ = k$$

است که $|k| < ۱ + ۲\sqrt{d}$.

اثبات. اگر p/q همگرایی از $\sqrt{d}$ باشد، آنگاه بنا به نتیجهٔ قضیهٔ ۱۳ـ۱۱

$$|\sqrt{d} - \frac{p}{q}| < \frac{۱}{q^۲}$$

و بنابراین

$$|p - q\sqrt{d}| < \frac{۱}{q}$$

پس

$$|p + q\sqrt{d}| = |(p - q\sqrt{d}) + ۲q\sqrt{d}| < \frac{۱}{q} + ۲q\sqrt{d} < (۱ + ۲\sqrt{d})q$$

از ترکیب این دو نابرابری نتیجه می‌شود

$$|p^۲ - dq^۲| = |p - q\sqrt{d}||p + q\sqrt{d}| < \frac{۱}{q}(۱ + ۲\sqrt{d})q = ۱ + ۲\sqrt{d}$$

و این دقیقاً همان است که قرار بود ثابت شود. □

به‌عنوان مثال، حالت $d = ۷$ را درنظر می‌گیریم. با استفاده از بسط $\sqrt{۷}$ به کسر مسلسل: $\sqrt{۷} = [۲; \overline{۱, ۱, ۱, ۴}]$ معلوم می‌شود که چند همگرای نخست $\sqrt{۷}$ عبارت‌اند از

$$\frac{۲}{۱}, \frac{۳}{۱}, \frac{۵}{۲}, \frac{۸}{۳}, \ldots$$

با محاسبهٔ جمله‌های نخست دنبالهٔ $p_n^۲ - ۷q_n^۲$، ملاحظه می‌کنیم که

$$۲^۲ - ۷ \times ۱^۲ = -۳,\ ۳^۲ - ۷ \times ۱^۲ = ۲,\ ۵^۲ - ۷ \times ۲^۲ = -۳,\ ۸^۲ - ۷ \times ۳^۲ = ۱$$

و بنابراین، $x = ۸$، $y = ۳$ جواب مثبتی از معادلهٔ $x^۲ - ۷y^۲ = ۱$ است.

گرچه می‌توان کسرهای مسلسل دوره‌ای را به تفصیل بررسی کرد، کند وکاو در این بحث جزو برنامهٔ ما نیست. همان‌طور که خواننده پیشتر توجه کرده است، کسر مسلسل نمایش‌دهندهٔ $\sqrt{d}$ در همهٔ مثالهایی که تاکنون آورده‌ایم به‌صورت

$$\sqrt{d} = [a_۰; \overline{a_۱, a_۲, \ldots, a_n}]$$

بوده است که در آن، بخش دوره‌ای پس از یک جمله آغاز می‌شود که $[\sqrt{d}]$ است. به‌علاوه، آخرین جملهٔ دوره، یعنی a_n، همیشه برابر با $۲a_۰$ است و دوره پس از حذف آخرین جمله‌اش، متقارن است (بخش متقارن ممکن است جملهٔ وسط داشته باشد یا نداشته باشد). این الگویی از وضعیت کلی است. در این مورد به بیان قضیه‌ای بدون اثبات بسنده می‌کنیم: اگر d عددی صحیح مثبت باشد که مربع کامل نباشد، آنگاه بسط کسر مسلسلیِ $\sqrt{d}$ لزوماً به‌صورت

$$\sqrt{d} = [a_۰; \overline{a_۱, a_۲, a_۳, \ldots, a_۳, a_۲, a_۱, ۲a_۰}]$$

است. به‌عنوان مثال، اگر $d = ۱۹$ داریم

$$\sqrt{۱۹} = [۴; \overline{۲, ۱, ۳, ۱, ۲, ۸}]$$

و اگر $d = ۳۷$ آنگاه

$$\sqrt{۳۷} = [۸; \overline{۱, ۱, ۵, ۵, ۱, ۱, ۱۶}]$$

در میان همهٔ dهای کوچکتر از ۱۰۰، $\sqrt{۹۴}$ دارای درازترین دوره است که شانزده جمله دارد:

$$\sqrt{۹۴} = [۹; \overline{۱, ۲, ۳, ۱, ۱, ۵, ۱, ۸, ۱, ۵, ۱, ۱, ۳, ۲, ۱, ۱۸}]$$

جدول زیر بسطهای کسر مسلسلیِ $\sqrt{d}$ را به‌ازای dهایی نشان می‌دهد که مربع کامل نیستند و d بین ۲ و ۴۰ است.

$$\sqrt{۲} = [۱; \overline{۲}]$$
$$\sqrt{۳} = [۱; \overline{۱, ۲}]$$
$$\sqrt{۵} = [۲; \overline{۴}]$$
$$\sqrt{۶} = [۲; \overline{۲, ۴}]$$
$$\sqrt{۷} = [۲; \overline{۱, ۱, ۱, ۴}]$$
$$\sqrt{۸} = [۲; \overline{۱, ۴}]$$
$$\sqrt{۱۰} = [۳; \overline{۶}]$$
$$\sqrt{۱۱} = [۳; \overline{۳, ۶}]$$
$$\sqrt{۱۲} = [۳; \overline{۲, ۶}]$$
$$\sqrt{۱۳} = [۳; \overline{۱, ۱, ۱, ۱, ۶}]$$
$$\sqrt{۱۴} = [۳; \overline{۱, ۲, ۱, ۶}]$$
$$\sqrt{۱۵} = [۳; \overline{۱, ۶}]$$
$$\sqrt{۱۷} = [۴; \overline{۸}]$$
$$\sqrt{۱۸} = [۴; \overline{۴, ۸}]$$
$$\sqrt{۱۹} = [۴; \overline{۲, ۱, ۳, ۱, ۲, ۸}]$$
$$\sqrt{۲۰} = [۴; \overline{۲, ۸}]$$
$$\sqrt{۲۱} = [۴; \overline{۱, ۳, ۱, ۸}]$$
$$\sqrt{۲۲} = [۴; \overline{۱, ۲, ۴, ۲, ۱, ۸}]$$
$$\sqrt{۲۳} = [۴; \overline{۱, ۳, ۱, ۸}]$$
$$\sqrt{۲۴} = [۴; \overline{۱, ۸}]$$
$$\sqrt{۲۶} = [۵; \overline{۱۰}]$$
$$\sqrt{۲۷} = [۵; \overline{۵, ۱۰}]$$
$$\sqrt{۲۸} = [۵; ۳, ۲, ۳, ۱۰]$$
$$\sqrt{۲۹} = [۵; \overline{۲, ۱, ۱, ۲, ۱۰}]$$
$$\sqrt{۳۰} = [۵; \overline{۲, ۱۰}]$$
$$\sqrt{۳۱} = [۵; \overline{۱, ۱, ۳, ۵, ۳, ۱, ۱, ۱۰}]$$
$$\sqrt{۳۲} = [۵; \overline{۱, ۱, ۱, ۱۰}]$$
$$\sqrt{۳۳} = [۵; \overline{۱, ۲, ۱, ۱۰}]$$
$$\sqrt{۳۴} = [۵; \overline{۱, ۴, ۱, ۱۰}]$$
$$\sqrt{۳۵} = [۵; \overline{۱, ۱۰}]$$
$$\sqrt{۳۷} = [۶; \overline{۱۲}]$$
$$\sqrt{۳۸} = [۶; \overline{۶, ۱۲}]$$
$$\sqrt{۳۹} = [۶; \overline{۴, ۱۲}]$$
$$\sqrt{۴۰} = [۶; \overline{۳, ۱۲}]$$

قضیهٔ ۱۳ـ۱۴ نشان می‌دهد که اگر معادلهٔ $x^{۲} - dy^{۲} = ۱$ جوابی داشته باشد، آنگاه جوابهای مثبت آن را باید در میان $(x = p_k, y = q_k)$هایی جستجو کرد که p_k/q_kها همگراهای $\sqrt{d}$ باشند. دورهٔ بسط کسر مسلسلیِ $\sqrt{d}$ اطلاع مورد نیاز را برای تشخیص اینکه $x^{۲} - dy^{۲} = ۱$ جوابی صحیح دارد یا نه، در اختیار می‌گذارد. در واقع تعداد جوابها نامتناهی است و همگی را می‌توان از همگراهای $\sqrt{d}$ به‌دست آورد. اثبات این حکم با استفاده از لم زیر امکان‌پذیر است.

لم. فرض می‌کنیم p_k/q_kها همگراهای بسط کسر مسلسلیِ $\sqrt{d}$ باشد. اگر طول دورهٔ بسط کسر مسلسلیِ $\sqrt{d}$، n باشد، آنگاه

$$p_{kn-۱}^{۲} - dq_{kn-۱}^{۲} = (-۱)^{kn} \qquad (k = ۱, ۲, ۳, \ldots)$$

اثبات. به‌ازای $k \geq 1$، بسط کسر مسلسلیِ $\sqrt{d}$ را می‌توان به‌صورت

$$\sqrt{d} = [a_0; a_1, a_2, \dots, a_{kn-1}, x_{kn}]$$

نوشت که در آن

$$x_{kn} = [2a_0; \overline{a_1, \dots, a_{n-1}, 2a_0}] = a_0 + \sqrt{d}$$

است. مانند اثبات قضیهٔ ۱۳ـ۶ داریم

$$\sqrt{d} = \frac{x_{kn}p_{kn-1} + p_{kn-2}}{x_{kn}q_{kn-1} + q_{kn-2}}$$

با جایگزینی $x_{kn} = a_0 + \sqrt{d}$ و ساده‌سازی، نتیجه می‌شود

$$\sqrt{d}(a_0 q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0 p_{kn-1} + p_{kn-2} - dq_{kn-1}$$

چون سمت راست گویا و $\sqrt{d}$ گنگ است، این رابطه مستلزم آن است که

$$a_0 p_{kn-1} + p_{kn-2} = dq_{kn-1} \quad \text{و} \quad a_0 q_{kn-1} + q_{kn-2} = p_{kn-1}$$

با ضرب رابطهٔ سمت راستی در p_{kn-1} و ضرب رابطهٔ سمت‌چپی در $-q_{kn-1}$ و جمع رابطه‌های حاصل داریم

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2}$$

ولی، بنا به قضیهٔ ۱۳ـ۷، $p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2} = (-1)^{kn-2} = (-1)^{kn}$، و بنابراین

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn}$$

که حکم موردنظر است. □

اکنون می‌توانیم همهٔ جوابهای مثبت $x^2 - dy^2 = 1$ را، وقتی $d > 0$ عدد صحیح غیر مربعی است، ارائه دهیم. قضیهٔ اصلی ما عبارت است از

قضیهٔ ۱۳ـ۱۶ فرض می‌کنیم p_k/q_kها همگراهای بسط کسر مسلسلیِ $\sqrt{d}$، و n طول دورهٔ بسط باشد.

(۱) اگر n زوج باشد، آنگاه همهٔ جوابهای مثبت $x^{۲} - dy^{۲} = ۱$ عبارت‌اند از

$$x = p_{kn-۱},\ y = q_{kn-۱} \quad (k = ۱, ۲, ۳, \ldots)$$

(۲) اگر n فرد باشد آنگاه همهٔ جوابهای مثبت $x^{۲} - dy^{۲} = ۱$ عبارت‌اند از

$$x = p_{۲kn-۱},\ y = q_{۲kn-۱} \quad (k = ۱, ۲, ۳, \ldots)$$

اثبات. پیشتر ثابت شد که هر جواب مثبت $x_{\circ}$، $y_{\circ}$ از $x^{۲} - dy^{۲} = ۱$، به‌ازای همگرای p_k/q_kای، به‌صورت $x_{\circ} = p_k$، $y_{\circ} = q_k$ است.

بنا به لم، $x = p_{kn-۱}$، $y = q_{kn-۱}$ جواب است اگر و تنها اگر $(-۱)^{kn} = ۱$. اگر n زوج باشد، این شرط به‌ازای هر عدد صحیح k برقرار است؛ اگر n فرد باشد، شرط وقتی و تنها وقتی برقرار است که k عدد صحیح زوجی باشد. □

مثال ۱۳ـ۷

به‌عنوان نخستین نمونه از کاربرد قضیهٔ ۱۳ـ۱۶، دوباره معادلهٔ $x^{۲} - ۷y^{۲} = ۱$ را درنظر می‌گیریم. چون $\sqrt{۷} = [۲; \overline{۱, ۱, ۱, ۴}]$، دوازده همگرای نخست عبارت‌اند از

$$\frac{۲}{۱}, \frac{۳}{۱}, \frac{۵}{۲}, \frac{۸}{۳}, \frac{۳۷}{۱۴}, \frac{۴۵}{۱۷}, \frac{۸۲}{۳۱}, \frac{۱۲۷}{۴۸}, \frac{۵۹۰}{۲۲۳}, \frac{۷۱۷}{۲۷۱}, \frac{۱۳۰۷}{۴۹۴}, \frac{۲۰۲۴}{۷۶۵}$$

چون بسط کسر مسلسلِ $\sqrt{۷}$ دارای دوره‌ای به‌طول ۴ است، صورت و مخرج هر یک از همگراهای $(p_{۴k-۱})/(q_{۴k-۱})$، جوابی از $x^{۲} - ۷y^{۲} = ۱$ تشکیل می‌دهند. بنابراین، به‌عنوان مثال، $p_{۳}/q_{۳} = ۸/۳$، $p_{۷}/q_{۷} = ۱۲۷/۴۸$، $p_{۱۱}/q_{۱۱} = ۲۰۲۴/۷۶۵$ سه جواب مثبت نخست را تشکیل می‌دهند؛ این جوابها عبارت‌اند از

$$x_{۱} = ۸،\ y_{۱} = ۳؛\ x_{۲} = ۱۲۷،\ y_{۲} = ۴۸؛\ x_{۳} = ۲۰۲۴،\ y_{۳} = ۷۶۵ \quad ■$$

مثال ۱۳ـ۸

برای تعیین کوچکترین جواب مثبت $x^{۲} - ۱۳y^{۲} = ۱$ در اعداد صحیح، ملاحظه می‌کنیم که $\sqrt{۱۳} = [۳; \overline{۱, ۱, ۱, ۱, ۶}]$ و طول دورهٔ آن ۵ است. ده همگرای نخست $\sqrt{۱۳}$ عبارت‌اند از

$$\frac{۳}{۱}, \frac{۴}{۱}, \frac{۷}{۲}, \frac{۱۱}{۳}, \frac{۱۸}{۵}, \frac{۱۱۹}{۳۳}, \frac{۱۳۷}{۳۸}, \frac{۲۵۶}{۷۱}, \frac{۳۹۳}{۱۰۹}, \frac{۶۴۹}{۱۸۰}$$

با توجه به قسمت (۲)ی قضیهٔ ۱۳ـ۱۶، کوچکترین جواب مثبت $x^۲ - ۱۳y^۲ = ۱$ عبارت است از $x_۱ = ۶۴۹$، $y_۱ = ۱۸۰$، که از همگرای $p_۹/q_۹ = ۶۴۹/۱۸۰$ به‌دست می‌آید. ■

روش سریعی وجود دارد که با آن می‌توان با استفاده از یک جواب معادلهٔ پل، جوابهای دیگر را به‌دست آورد. پیش از توضیح این روش، خاطر نشان می‌کنیم که کوچکترین جواب مثبت معادلهٔ $x^۲ - dy^۲ = ۱$ جواب اساسی آن نامیده می‌شود؛ یعنی جواب اساسی عبارت است از جوابی مثبت چون $x_۰$، $y_۰$ که به‌ازای هر جواب مثبت x'، y' دیگر، در ضوابط $x_۰ < x'$ و $y_۰ < y'$ صدق می‌کند. بنا به قضیهٔ ۱۳ـ۱۶: اگر طول دورهٔ بسط کسر مسلسلِ $\sqrt{d}$ برابر با n باشد، آنگاه جواب اساسی $x^۲ - dy^۲ = ۱$، برحسب زوج یا فرد بودن n، به‌ترتیب، $x = p_{n-۱}$، $y = q_{n-۱}$ و $x = p_{۲n-۱}$، $y = q_{۲n-۱}$ است. بنابراین، معادلهٔ $x^۲ - dy^۲ = ۱$ را می‌توان در n یا $۲n$ مرحله حل کرد.

تعیین جواب اساسی ممکن است دشوار باشد، زیرا حتی به‌ازای مقدارهای نسبتاً کوچک d، مقادیر این جواب ممکن است به‌طور نامنتظره‌ای بزرگ باشد. به‌عنوان مثال، کوچکترین جواب مثبت معادلهٔ $x^۲ - ۹۹۱y^۲ = ۱$ که به‌ظاهر معادله‌ای بی‌دردسر است، این است

$$x = ۳۷۹\ ۵۱۶\ ۴۰۰\ ۹۰۶\ ۸۱۱\ ۹۳۰\ ۶۳۸\ ۰۱۴\ ۸۹۶\ ۰۸۰$$

$$y = ۱۲\ ۰۵۵\ ۷۳۵\ ۷۹۰\ ۳۳۱\ ۳۵۹\ ۴۴۷\ ۴۴۲\ ۵۳۸\ ۷۶۷$$

وضعیت در مورد $x^۲ - ۱۰۰۰۰۹۹y^۲ = ۱$ بدتر است، زیرا کوچکترین عدد صحیح مثبت xای که در این معادله صدق می‌کند، ۱۱۱۸ رقم دارد. نیازی به توضیح نیست که، همه چیز به بسط کسر مسلسلِ $\sqrt{d}$ بستگی دارد و، در مورد $d = \sqrt{۱۰۰۰۰۹۹}$، دوره ۲۱۷۴ جمله دارد.

همچنین ممکن است، به‌ازای مقدار داده شده‌ای از d، عددهای صحیح مورد نیاز برای حل $x^۲ - dy^۲ = ۱$ کوچک و به‌ازای مقدار بعدی d، بسیار بزرگ باشند. به‌عنوان مثالی شاخص از این تغییر، می‌توان معادلهٔ $x^۲ - ۶۱y^۲ = ۱$ را در نظر گرفت که جواب اساسیش

$$x = ۱۷۶۶۳۳۱۹۰۴۹،\quad y = ۲۲۶۱۵۳۹۸۰$$

است. این عددها، در مقایسه با حالت $d = ۶۰$، که جواب اساسی در آن حالت $x = ۳۱$، $y = ۴$ است، یا حالت $d = ۶۲$، که جواب اساسی $x = ۶۳$، $y = ۸$ است، بسیار بزرگ‌اند.

به‌کمک جواب اساسی ــ که می‌توان آن‌را به وسیلهٔ کسرهای مسلسل یا با جایگزینی متوالی مقادیر $y = ۱, ۲, ۳, \ldots$ در عبارت $dy^۲ + ۱$ تا هنگام مربع کامل شدن آن یافت ــ می‌توانیم همهٔ جوابهای مثبت دیگر را به‌دست آوریم.

قضیهٔ ۱۳ـ۱۷ اگر x_1، y_1 جواب اساسی $x^2 - dy^2 = 1$ باشد، آنگاه هر زوج از عددهای صحیح x_n، y_nای که در شرط

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \qquad (n = 1, 2, 3, \dots)$$

صدق کند، نیز جوابی مثبت است.

اثبات. خواننده می‌تواند به‌سادگی نشان دهد که

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$$

به‌علاوه، چون x_1 و y_1 مثبت هستند، هر دوی x_n و y_n عددهای صحیح مثبتی‌اند. با توجه به اینکه x_1، y_1 جوابی از $x^2 - dy^2 = 1$ است، به‌دست می‌آوریم

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n \\ &= (x_1^2 - dy_1^2)^n = 1^n = 1 \end{aligned}$$

و بنابراین x_n، y_n جواب است. □

بحث را لحظه‌ای برای ملاحظهٔ مثالی به کنار می‌گذاریم. با جستجو و آزمایش می‌بینیم که $x_1 = 6$، $y_1 = 1$ جواب اساسی $x^2 - 35y^2 = 1$ است. جواب مثبت دیگری چون x_2، y_2 را می‌توان از فرمول

$$x_2 + y_2\sqrt{35} = (6 + \sqrt{35})^2 = 71 + 12\sqrt{35}$$

به‌دست آورد. نتیجه می‌شود $x_2 = 71$، $y_2 = 12$. این عددهای صحیح در معادلهٔ $x^2 - 35y^2 = 1$ صدق می‌کنند زیرا

$$71^2 - 35 \times 12^2 = 5041 - 5040 = 1$$

سومین جواب مثبت از

$$\begin{aligned} x_3 + y_3\sqrt{35} &= (6 + \sqrt{35})^3 \\ &= (71 + 12\sqrt{35})(6 + \sqrt{35}) = 846 + 143\sqrt{35} \end{aligned}$$

حاصل می‌شود. بنابراین، $x_۳ = ۸۴۶$، $y_۳ = ۱۴۳$، و در واقع

$$۸۴۶^۲ - ۳۵ \times ۱۴۳^۲ = ۷۱۵۷۱۶ - ۷۱۵۷۱۵ = ۱$$

که معلوم می‌شود این مقدارها جواب دیگری را تشکیل می‌دهند.

با بازگشت به معادلهٔ $x^۲ - dy^۲ = ۱$، قضیه‌ای در پایان می‌آوریم که حاکی است هر جواب مثبت را می‌توان از فرمول

$$x_n + y_n\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n$$

که در آن n عدد صحیحی است، به‌دست آورد؛ یعنی، اگر u، v جواب مثبتی از $x^۲ - dy^۲ = ۱$ باشد، آنگاه به‌ازای عدد صحیح مناسب nای، $u = x_n$، $v = y_n$.

قضیهٔ ۱۳ـ۱۸ اگر $x_۱$، $y_۱$ جواب اساسی معادلهٔ $x^۲ - dy^۲ = ۱$ باشد، آنگاه هر جواب مثبت دیگر آن به‌صورت x_n، y_n است به‌طوری که x_n و y_n عددهای صحیحی‌اند که با

$$x_n + y_n\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n \quad (n = ۱, ۲, ۳, \dots)$$

معین می‌شوند.

اثبات. برخلاف حکم، فرض می‌کنیم جواب مثبت u، vای وجود دارد که از فرمول $u + v\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n$ به‌دست نمی‌آید. چون $x_۱ + y_۱\sqrt{d} > ۱$، توانهای $x_۱ + y_۱\sqrt{d}$ به‌دلخواه بزرگ می‌شوند؛ یعنی، $u + v\sqrt{d}$ باید میان دو توان متوالی $x_۱ + y_۱\sqrt{d}$ قرار بگیرد، مثلاً

$$(x_۱ + y_۱\sqrt{d})^n < u + v\sqrt{d} < (x_۱ + y_۱\sqrt{d})^{n+۱}$$

یا، به‌عبارت دیگر

$$x_n + y_n\sqrt{d} < u + v\sqrt{d} < (x_n + y_n\sqrt{d})(x_۱ + y_۱\sqrt{d})$$

با ضرب این نابرابری در عدد مثبت $x_n - y_n\sqrt{d}$ و با توجه به اینکه $x_n^۲ - dy_n^۲ = ۱$، به‌دست می‌آوریم

$$۱ < (x_n - y_n\sqrt{d})(u + v\sqrt{d}) < x_۱ + y_۱\sqrt{d}$$

اکنون عددهای صحیح r و s را طوری تعریف می‌کنیم که

$$r + s\sqrt{d} = (x_n - y_n\sqrt{d})(u + v\sqrt{d})$$

یعنی، فرض می‌کنیم

$$s = x_n v - y_n u \quad \text{و} \quad r = x_n u - y_n v d$$

با محاسبه‌ای ساده معلوم می‌شود

$$r^۲ - ds^۲ = (x_n^۲ - dy_n^۲)(u^۲ - dv^۲) = ۱$$

و بنابراین r، s جوابی از $x^۲ - dy^۲ = ۱$ است که در $۱ < r + s\sqrt{d} < x_۱ + y_۱\sqrt{d}$ صدق می‌کند.

برای تکمیل اثبات، کافی است نشان دهیم که r، s جوابی مثبت است. چون $۱ < r + s\sqrt{d}$، ملاحظه می‌کنیم که $۰ < r - s\sqrt{d} < ۱$. در نتیجه

$$۲r = (r + s\sqrt{d}) + (r - s\sqrt{d}) > ۱ + ۰ > ۰$$
$$s\sqrt{d} = (r + s\sqrt{d}) - (r - s\sqrt{d}) > ۱ - ۱ = ۰$$

و بنابراین هر دوی r و s مثبت‌اند. نتیجه اینکه چون $x_۱$، $y_۱$ جواب اساسی $x^۲ - dy^۲ = ۱$ است، باید داشته باشیم $x_۱ < r$ و $y_۱ < s$؛ ولی در این‌صورت $x_۱ + y_۱\sqrt{d} < r + s\sqrt{d}$، که متناقض با یکی از نابرابریهای قبلی است. با رسیدن به این تناقض اثباتمان کامل می‌شود. □

معادلهٔ پِل قرنها نظر ریاضیدانان را به‌خود جلب کرده است. بنا به شواهد تاریخی، یونانیان در حدود ۴۰۰ سال پیش از میلاد مسیح روشهایی برای حل این معادله داشته‌اند. ارشمیدس مسألهٔ معروفی از آنالیز نامعین موسوم به «مسألهٔ گله» را در قالب لطیفه‌ای جهت آزمودن دانشمندان اسکندریه برای اراتستن فرستاد. در این مسأله، که خواسته می‌شود تعداد گاوهای نر و ماده از هر یک از چهار رنگ مفروض تعیین شود، نُه معادله و هشت مجهول وجود دارد. این معادله‌ها بالاخره به معادلهٔ پِل

$$x^۲ - ۴۷۲۹۴۹۴y^۲ = ۱$$

منجر می‌شوند که جوابهای بسیار بزرگی دارد؛ مقدار یکی از این هشت مجهول، عددی با ۲۰۶۵۴۵ رقم است (به فرض اینکه ۱۵ رقم چاپی فضایی به اندازهٔ یک اینچ اشغال کنند، طول این عدد متجاوز از ۱/۵ مایل خواهد بود). گرچه توافق عمومی وجود دارد که این مسأله از ریاضیدان برجستهٔ سیراکوزی است، کسی باور ندارد که ارشمیدس واقعاً همهٔ مرحله‌های ضروری محاسبه را به انجام رسانیده باشد.

این‌گونه معادله‌ها و قاعده‌هایی جزمی و بدون اثبات برای محاسبهٔ جوابهای معادله‌ها، بیش از یک‌هزار سال پیش از آنکه در اروپا مطرح شود در هند رواج یافت. در سدهٔ هفتم میلادی،

برهمگوپته اظهار کرد که هر کس بتواند در عرض یک سال معادلهٔ $x^{۲} - ۹۲y^{۲} = ۱$ را حل کند، ریاضیدان است؛ در آن زمان، چنین کسی دست کم حسابدان خوبی به‌حساب می‌آمد، زیرا $x = ۱۱۵۱$، $y = ۱۲۰$ کوچکترین جواب مثبت است. از نظر محاسباتی، تعیین عددهایی صحیح که در $x^{۲} - ۹۴y^{۲} = ۱$ صدق کنند، دشوارتر است زیرا در مورد این معادله، $x = ۲۱۴۳۲۹۵$، $y = ۲۲۱۰۶۴$ جواب اساسی است.

بنابراین، فرما نه تنها نخستین پیشنهاد دهندهٔ حل معادلِ $x^{۲} - dy^{۲} = ۱$ نبود، بلکه نخستین طراح روش کلی حل آن نیز نبود. ولی شاید نخستین کسی بود که اظهار داشت به‌ازای هر مقدار صحیح غیر مربع d، تعداد جوابهای معادله نامتناهی است. به‌علاوه، تلاشهای او برای تعیین جوابهای صحیح این مسأله و مسأله‌های دیگر نقطهٔ عطفی در نظریهٔ اعداد بود که آن‌را به کلی از سنت کلاسیک حساب دیوفانتوس متمایز ساخت.

تمرینهای ۱۳ـ۵

۱. اگر $x_{۰}$، $y_{۰}$ جواب مثبتی از معادلهٔ $x^{۲} - dy^{۲} = ۱$ باشد، نشان دهید که $x_{۰} > y_{۰}$.

۲. اگر d برابر با

(الف) ۷ (ب) ۱۱ (پ) ۱۸ (ت) ۳۰ (ث) ۳۹

باشد، با استفاده از روش جایگزینی متوالی $y = ۱, ۲, ۳, \ldots$ در معادلهٔ $dy^{۲} + ۱$، کوچکترین جواب مثبت $x^{۲} - dy^{۲} = ۱$ را در هر حالت تعیین کنید.

۳. همهٔ جوابهای مثبت هر یک از معادله‌های زیر را به شرط $y < ۲۵۰$، به‌دست آورید

(الف) $x^{۲} - ۲y^{۲} = ۱$ (ب) $x^{۲} - ۳y^{۲} = ۱$ (پ) $x^{۲} - ۵y^{۲} = ۱$

۴. نشان دهید تعداد عددهای صحیح زوج n به‌طوری که هم $n + ۱$ و هم $(n/۲) + ۱$ مربع کامل باشند، نامتناهی است. دو مثال بیاورید.

۵. دو جواب مثبت هر یک از معادله‌های زیر را به‌دست آورید

(الف) $x^{۲} - ۲۳y^{۲} = ۱$ (ب) $x^{۲} - ۲۶y^{۲} = ۱$ (پ) $x^{۲} - ۳۳y^{۲} = ۱$

۶. جوابهای اساسی

(الف) $x^{۲} - ۲۹y^{۲} = ۱$ (ب) $x^{۲} - ۴۱y^{۲} = ۱$ (پ) $x^{۲} - ۷۴y^{۲} = ۱$

را به‌دست آورید. [راهنمایی: $\sqrt{۴۱} = [۶; \overline{۲, ۲, ۱۲}]$ و $\sqrt{۷۴} = [۸; \overline{۱, ۱, ۱, ۱, ۱۶}]$.]

۷. جوابی از هر یک از معادله‌های زیر به‌دست آورید

(الف) $x^{۲} - ۱۳y^{۲} = -۱$ (ب) $x^{۲} - ۲۹y^{۲} = -۱$

(پ) $x^{۲} - ۴۱y^{۲} = -۱$

۸. نشان دهید که اگر $x_\circ$، $y_\circ$ جوابی از معادلهٔ $x^{۲} - dy^{۲} = -۱$ باشد، آنگاه $x = ۲x_\circ^{۲} + ۱$، $y = ۲x_\circ y_\circ$ در $x^{۲} - dy^{۲} = ۱$ صدق می‌کند. برونکر از این حکم در حل $x^{۲} - ۳۱۳y^{۲} = ۱$ استفاده کرد.

۹. اگر d بر عدد اول (به پیمانهٔ ۴) $p \equiv ۳$ بخشپذیر باشد، نشان دهید معادلهٔ $x^{۲} - dy^{۲} = -۱$ جواب ندارد.

۱۰. اگر $x_۱$، $y_۱$ جواب اساسی $x^{۲} - dy^{۲} = ۱$ باشد و

$$x_n + y_n\sqrt{d} = (x_۱ + y_۱\sqrt{d})^n \qquad (n = ۱, ۲, ۳, \ldots)$$

ثابت کنید زوج عددهای صحیح x_n، y_n از فرمولهای

$$x_n = \frac{۱}{۲}[(x_۱ + y_۱\sqrt{d})^n + (x_۱ - y_۱\sqrt{d})^n]$$
$$y_n = \frac{۱}{۲\sqrt{d}}[x_۱ + y_۱\sqrt{d})^n - (x_۱ - y_۱\sqrt{d})^n]$$

به‌دست می‌آیند.

۱۱. نشان دهید که عددهای صحیح x_n، y_n در تمرین فوق را می‌توان به‌طور استقرایی با

$$x_{n+۱} = x_۱x_n + dy_۱y_n$$
$$y_{n+۱} = x_۱y_n + x_ny_۱$$

به‌ازای $n = ۱, ۲, ۳, \ldots$ یا با

$$x_{n+۱} = ۲x_۱x_n - x_{n-۱}$$
$$y_{n+۱} = ۲x_۱y_n - y_{n-۱}$$

به‌ازای $n = ۲, ۳, \ldots$، تعریف کرد.

۱۲. با اطلاع از اینکه $x_۱ = ۱۵$، $y_۱ = ۲$ جواب اساسی $x^{۲} - ۵۶y^{۲} = ۱$ است، دو جواب مثبت دیگر آن‌را به‌دست آورید.

۱۳. (الف) ثابت کنید اگر معادلهٔ $x^{۲} - dy^{۲} = c$ حلپذیر باشد، بینهایت جواب دارد. [راهنمایی: اگر u، v در $x^{۲} - dy^{۲} = c$ صدق کند و r، s در $x^{۲} - cy^{۲} = ۱$، آنگاه

$$(ur \pm dvs)^{۲} - d(us \pm vr)^{۲} = (u^{۲} - dv^{۲})(r^{۲} - ds^{۲}) = c$$.]

(ب) اگر $x = 16$، $y = 6$ جوابی از $x^2 - 7y^2 = 4$ باشد، دو جواب مثبت دیگر آن‌را به‌دست آورید.

(پ) اگر $x = 18$، $y = 3$ جوابی از $x^2 - 35y^2 = 9$ باشد، دو جواب مثبت دیگر آن‌را به‌دست آورید.

۱۴. با استفاده از نظریهٔ مذکور در این بخش نشان دهید تعداد سه‌تاییهای فیثاغورسی اولیه x، y، zای که در آنها x و y عددهایی صحیح متوالی باشند، نامتناهی است.

ضمیمه‌ها

- قضیهٔ عددهای اول
- مراجع عمومی
- مراجعی برای مطالعه بیشتر
- جدولها
- پاسخهای تمرینهای انتخابی

قضیهٔ عددهای اول

گرچه دنبالهٔ عددهای اول بی‌نظمیهای زیادی دارد، درکل از نوعی نظم برخوردار است. قضیهٔ معروف عددهای اول به ما امکان می‌دهد، حداقل به‌طور تقریبی، تعداد عددهای اول کوچکتر از عدد داده‌شده‌ای را بدون به‌دست‌آوردن آنها تعیین کنیم. بنابه قضیهٔ مزبور، به‌ازای هر عددطبیعی n حدوداً $n/\log n$ عدد اول کوچکتر از n وجود دارد (منظور از $\log n$، لگاریتم طبیعی n است). بنابراین، با توجه به قضیهٔ عددهای اول، می‌توان به‌نحوهٔ توزیع عددهای اول «درکل» یا «به‌طور میانگین» یا «به‌معنی احتمالی» پی برد.

یکی از شاخصهای توزیع عددهای اول تابع $\pi(x)$ است که، به‌ازای هر عددحقیقی x، تعداد عددهای اول نابیشتر از x را نشان می‌دهد؛ به‌صورت نمادین، $\pi(x) = \sum_{p\leq x} 1$. در فصل ۳ ثابت کردیم تعداد عددهای اول نامتناهی است، که بیان نمادین آن به‌صورت $\lim_{x\to\infty}\pi(x) = \infty$ است. از طرف دیگر، روشن است که پراکندگی عددهای اول در بخشهای بالاتر هر جدول عددهای اول، به‌طور میانگین، بیشتر می‌شود؛ به بیانی غیررسمی، می‌توان گفت که تقریباً همهٔ عددهای صحیح مثبت مرکب هستند.

برای توجیه ادعای اخیر خود، نشان می‌دهیم که $\lim_{x\to+\infty}\pi(x)/x = 0$. چون به‌ازای هر $x > 0$، $\pi(x)/x \geq 0$، مسأله تحویل می‌شود به اینکه ثابت کنیم اگر x به اندازهٔ کافی بزرگ اختیار شود می‌توان $\pi(x)/x$ را به اندازهٔ دلخواه کوچک کرد. به بیان دقیقتر، آنچه می‌خواهیم نشان دهیم این است که به‌ازای هر عدد $\varepsilon > 0$، عددصحیح مثبت N ای باید موجود باشد به‌گونه‌ای که اگر $x \geq N$، آنگاه $\pi(x)/x < \varepsilon$.

در آغاز استدلال، فرض می‌کنیم n عدد صحیح مثبتی است و با استفاده از حدس برتران

عدد اول p را طوری انتخاب می‌کنیم که $۲^{n-۱} < p \le ۲^n$. در این صورت $p \nmid (۲^{n-۱})!$ و $p|(۲^n)!$، و بنابراین ضریب دوجمله‌ای $\binom{۲^n}{۲^{n-۱}}$ بر p بخشپذیر است. درنتیجه

$$۲^{۲^n} \ge \binom{۲^n}{۲^{n-۱}} \ge \prod_{۲^{n-۱}<p\le ۲^n} p \ge \left(۲^{n-۱}\right)^{\pi(۲^n)-\pi(۲^{n-۱})}$$

و، از مقایسهٔ نماهای ۲ در دو طرف، نتیجه می‌شود

$$\pi(۲^n) - \pi(۲^{n-۱}) \le \frac{۲^n}{n-۱} \qquad (*)$$

اگر در $(*)$ متوالیاً قرار دهیم $n = ۲k, ۲k-۱, ۲k-۲, \ldots, ۳$، و نابرابریهای حاصل را باهم جمع کنیم، به‌دست می‌آوریم

$$\pi(۲^{۲k}) - \pi(۲^۲) \le \sum_{r=۳}^{۲k} \frac{۲^r}{r-۱}$$

ولی به‌وضوح داریم $\pi(۲^۲) < ۲^۲$، و بنابراین

$$\pi(۲^{۲k}) < \sum_{r=۲}^{۲k} \frac{۲^r}{r-۱} = \sum_{r=۲}^{k} \frac{۲^r}{r-۱} + \sum_{r=k+۱}^{۲k} \frac{۲^r}{r-۱}$$

اگر به‌جای مخرج $r-۱$ در دو جملهٔ سمت راست، به‌ترتیب، ۱ و k را قرار دهیم، به‌دست می‌آوریم

$$\pi(۲^{۲k}) < \sum_{r=۲}^{k} ۲^r + \sum_{r=k+۱}^{۲k} \frac{۲^r}{k} < ۲^{k+۱} + \frac{۲^{۲k+۱}}{k}$$

چون $k < ۲^k$، به‌ازای $k \ge ۲$ داریم $(۲^{۲k+۱})/k > ۲^{k+۱}$ و بنابراین

$$\pi(۲^{۲k}) < ۲\left(\frac{۲^{۲k+۱}}{k}\right) = ۴\left(\frac{۲^{۲k}}{k}\right)$$

که می‌توان آن را به‌صورت

$$\frac{\pi(۲^{۲k})}{۲^{۲k}} < \frac{۴}{k} \qquad (**)$$

نوشت. با این نابرابری، استدلال ما سریعاً به نتیجهٔ خود می‌رسد. به‌ازای هر عددحقیقی $x \ge ۲$، عددصحیح یکتای kای وجود دارد که در $۲^{۲k-۲} < x \le ۲^{۲k}$ صدق می‌کند. از $(**)$ نتیجه می‌شود

$$\frac{\pi(x)}{x} \le \frac{\pi(۲^{۲k})}{x} < \frac{\pi(۲^{۲k})}{۲^{۲k-۲}} = ۴\left(\frac{\pi(۲^{۲k})}{۲^{۲k}}\right) < \frac{۱۶}{k}$$

اکنون اگر ε عدد مثبت دلخواهی باشد و $x \geq N = ۲^{۲([\frac{۱۶}{\varepsilon}]+۱)}$، آنگاه $k \geq [(۱۶)/\varepsilon] + ۱$؛ درنتیجه، طبق انتظار ما

$$\frac{\pi(x)}{x} < \frac{۱۶}{[\frac{۱۶}{\varepsilon}] + ۱} < \varepsilon$$

تابع زتا

$$\zeta(s) = \sum_{n=۱}^{\infty} \frac{۱}{n^s} = ۱^{-s} + ۲^{-s} + ۳^{-s} + \ldots$$

که اثبات قضیهٔ عددهای اول نهایتاً به ویژگیهای آن بستگی دارد، توسط اویلر (احتمالاً در حوالی ۱۷۴۰) وارد آنالیز شد. کار اساسی اویلر در این زمینه، ارائهٔ فرمولی برای نمایش $\zeta(s)$ به‌صورت حاصلضربی نامتناهی و همگراست؛ یعنی

$$\zeta(s) = \prod_{p} \left(۱ - \frac{۱}{p^s}\right)^{-۱} \qquad (s > ۱)$$

که در آن p هر مقدار اول را می‌پذیرد؛ اهمیت این فرمول از این واقعیت سرچشمه می‌گیرد که مبین برابری دو عبارت است که یکی به‌صراحت حاوی عددهای اول است و دیگری چنین نیست. اویلر $\zeta(s)$ را فقط به‌عنوان تابعی از متغیر حقیقی درنظر گرفت؛ مع‌الوصف، فرمول او نشان‌دهندهٔ ارتباط عمیقی میان نظریهٔ عددهای اول و ویژگیهای تحلیلی تابع زتاست.

فرمول اویلر برای $\zeta(s)$ از بسط هریک از عاملهای سمت راست به‌صورت

$$\frac{۱}{۱ - \frac{۱}{p^s}} = ۱ + \frac{۱}{p^s} + \frac{۱}{(p^s)^۲} + \frac{۱}{(p^s)^۳} + \ldots$$

و با توجه به این نکته به‌دست می‌آید که حاصلضرب آنها مجموع همهٔ جمله‌هایِ به‌صورت

$$\frac{۱}{(p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r})^s}$$

است که در آنها $p_۱$، $p_۲$، …، p_r عددهای اول متمایزی هستند. چون هر عددصحیح مثبت n را می‌توان به‌طور یکتا به‌صورت حاصلضرب توانهای عددهای اول نوشت، هر جملهٔ $۱/(n^s)$ دقیقاً یک بار در این مجموع ظاهر می‌شود؛ یعنی مجموع برابر با $\sum_{n=۱}^{\infty} ۱/(n^s)$ است.

فرمول اویلر برای تابع زتا به اثبات ظاهراً کوتاهی از نامتناهی‌بودن عددهای اول منجر می‌شود؛ ظهور حاصلضربی متناهی در سمت راست متناقض با $\lim_{s\to۱}\zeta(s) = \infty$ است.

لژاندر نخستین فردی است که دربارهٔ تابعهایی که تقریب خوبی از $\pi(x)$ به‌ازای مقدارهای بزرگ x به‌دست می‌دهند، حدس قابل‌توجهی زد. وی در کتابش تحت‌عنوان رساله دربارهٔ نظریهٔ اعداد[1] (۱۷۹۸)، ادعا کرد که $\pi(x)$ تقریباً با تابع

$$\frac{x}{\log x - ۱٫۰۸۳۶۶}$$

برابر است. گاوس با تهیهٔ جدولهای مفصلی دربارهٔ نحوهٔ توزیع عددهای اول در دسته‌های متشکل از ۱۰۰۰ عددصحیح متوالی، نتیجه گرفت که $\pi(x)$ تقریباً با همان سرعتِ هریک از تابعهای $x/(\log x)$ و

$$\mathrm{Li}(x) = \int_۲^x \frac{du}{\log u}$$

بزرگ می‌شود و انتگرال لگاریتمی $\mathrm{Li}(x)$ تقریب عددیِ به مراتب بهتری به‌دست می‌دهد. یافته‌های گاوس طی نامه‌ای در ۱۸۴۹ به اطلاع انکه[2] منجم معروف رسید و برای نخستین بار در ۱۸۶۳ چاپ شد، ولی به‌نظر می‌رسد این کشفیات از حوالی ۱۷۹۱، وقتی که گاوس چهارده‌ساله بوده است، آغاز شده باشد و ــ نیازی به گفتن ندارد که ــ این کار مدتها پیش از نوشته‌شدن کتاب لژاندر صورت گرفته است.

جالب است که این ملاحظات با محتوای جدولها سنجیده شود:

x	$\pi(x)$	$\frac{x}{\log x - ۱٫۰۸۳۶۶}$	$\frac{x}{\log x}$	$\mathrm{Li}(x)$	$\frac{\pi(x)}{(\frac{x}{\log x})}$
۱۰۰۰	۱۶۸	۱۷۲	۱۴۵	۱۷۸	۱٫۱۵۹
۱۰۰۰۰	۱۲۲۹	۱۲۳۱	۱۰۸۶	۱۲۴۶	۱٫۱۳۲
۱۰۰۰۰۰	۹۵۹۲	۹۵۸۸	۸۶۸۶	۹۶۳۰	۱٫۱۰۴
۱۰۰۰۰۰۰	۷۸۴۹۸	۷۸۵۳۴	۷۲۳۸۲	۷۸۶۲۸	۱٫۰۸۴
۱۰۰۰۰۰۰۰	۶۶۴۵۷۹	۶۶۵۱۳۸	۶۲۰۴۲۰	۶۶۴۹۱۸	۱٫۰۷۱
۱۰۰۰۰۰۰۰۰	۵۷۶۱۴۵۵	۵۷۶۹۳۴۱	۵۴۲۸۶۸۱	۵۷۶۲۲۰۹	۱٫۰۶۱

نخستین پیشرفت قابل‌ملاحظه در راستای مقایسهٔ $\pi(x)$ با $x/(\log x)$ توسط چبیشف[3] ریاضیدان روسی به‌عمل آمد. او در ۱۸۵۰ ثابت کرد که ثابتهای مثبت a و b ای، $a < ۱ < b$،

1. Essai sur la Théorie des Nombres
2. Encke
3. Tchebychef

وجود دارند به‌طوری که به‌ازای x های به اندازهٔ کافی بزرگ داریم

$$a\left(\frac{x}{\log x}\right) < \pi(x) < b\left(\frac{x}{\log x}\right)$$

به‌علاوه نشان داد که اگر در صورت افزایش x خارج‌قسمت $\pi(x)/(x\log x)$ دارای حدی باشد، مقدار این حد باید ۱ باشد. هرچند کار چبیشف خیلی جالب بود، قرین موفقیت نشد: آنچه او نتوانست ثابت کند این بود که حد فوق‌الذکر واقعاً وجود دارد، و بنابراین نتوانست قضیهٔ عدد اول را ثابت کند. حدود ۴۵ سال طول کشید تا این نقیصه رفع شد.

می‌توان نشان داد که بنابه نتیجهٔ چبیشف، سری $\sum_p 1/p$ که در آن p همهٔ عددهای اول را می‌پذیرد، واگراست. برای ملاحظهٔ این مطلب، فرض می‌کنیم p_n، nامین عدد اول باشد. پس $\pi(p_n) = n$. چون به‌ازای x های به اندازهٔ کافی بزرگ داریم

$$\pi(x) > a\left(\frac{x}{\log x}\right)$$

نتیجه می‌شود که به‌ازای n های به اندازهٔ کافی بزرگ، نابرابری

$$n = \pi(p_n) > a\left(\frac{p_n}{\log p_n}\right) > \sqrt{p_n}$$

برقرار است. ولی از $n^2 > p_n$ نتیجه می‌شود $\log p_n < 2\log n$ و به‌ازای n های بزرگ به‌دست می‌آوریم

$$ap_n < n\log p_n < 2n\log n$$

بنابراین، با مقایسه با سری واگرای شناخته‌شدهٔ $\sum_{n=2}^{\infty} \frac{1}{(n\log n)}$ معلوم می‌شود که سری $\sum_{n=1}^{\infty} 1/(p_n)$ واگراست.

نکته‌ای ضمنی این است که برون[1]، در حوالی ۱۹۲۰، نشان داد عددهای اول دوقلو به اندازه‌ای پراکنده‌اند که مجموع عکسهایشان همگراست.

مفهومهای اساساً نوینی که مسیر اثباتی از قضیهٔ عددهای اول را هموار کرد، در رسالهٔ بسیار مهم ریمان تحت عنوان «دربارهٔ تعداد عددهای اول در یک کمیت بزرگ مفروض»[2] در ۱۸۵۹ (تنها مقالهٔ او دربارهٔ نظریهٔ اعداد) معرفی شد. اویلر تابع زتای $\zeta(s)$ را به مقدارهای حقیقی s محدود کرده بود، ولی ریمان ارتباط میان توزیع عددهای اول و رفتار $\zeta(s)$ به‌عنوان تابعی از متغیر مختلط $s = a + bi$ را کشف کرد. به‌علاوه، تعدادی از ویژگیهای تابع زتا و اتحاد قابل‌توجهی

---

1. V. Brun   2. Uber die Anzahl der Primzahlen unter einer gegebenen Grösse

معروف به فرمول صریح ریمان را عرضه کرد که این فرمول، $\pi(x)$ را با صفرهای $\zeta(s)$ در sـصفحه مربوط می‌کند. این نتیجه نظر ریاضیدانان را به خود جلب کرد زیرا مرتبط‌کردن دو مقولهٔ به‌ظاهر نامربوط، یعنی، نظریهٔ اعداد که به مطالعهٔ کمیات گسسته می‌پردازد و آنالیز مختلط که با فرایندهای پیوسته سروکار دارد، بسیار غیرمنتظره بود.

ریمان در رساله‌اش حدسهایی دربارهٔ توزیع صفرهای تابع زتا مطرح کرد. معروفترین آنها معروف به فرض ریمان است که حاکی است همهٔ صفرهای غیرحقیقی $\zeta(s)$ نقطه‌هایی به‌صورت $۱/۲ + bi$ در صفحهٔ مختلط‌اند؛ یعنی، روی «خط بحرانی» $Re(s) = ۱/۲$ قرار دارند. اخیراً در پی محاسباتی مفصل و صرف بیش از هزار ساعت وقت با ابر رایانه‌ای جدید، معلوم شد که فرض ریمان در مورد همهٔ $۱٫۵ \times ۱۰^{۹}$ صفر نخست صحیح است. این حدس معروف تاکنون رد یا اثبات نشده است، و بدون تردید مهمترین مسألهٔ حل‌نشدهٔ مطرح در ریاضیات امروز است.

آدامار و دُ لا واله پوسن[1] در سال ۱۸۹۶ مستقل از یکدیگر و تقریباً به‌طور همزمان موفق شدند با استفاده از پژوهشهای ریمان ثابت کنند که

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = ۱$$

از آن زمان، حکمی که این فرمول بیانگر آن است به قضیهٔ عددهای اول معروف شده است. دُ لا واله پوسن در تحقیق خود بسیار فراتر رفت. او نشان داد که، به‌ازای مقدارهای بزرگ x، $\pi(x)$ با انتگرال لگاریتمی $\mathrm{Li}(x)$ بهتر تقریب زده می‌شود تا با تابع

$$\frac{x}{\log x - A}$$

صرف‌نظر از اینکه ثابت A چه مقداری داشته باشد، و مطلوبترین مقدار آن در فرمول لژاندر، ۱ است. این نتیجه متفاوت با نظر اولیهٔ لژاندر است مبنی بر اینکه $A = ۱٫۰۸۳۶۶$، ولی مدتهای مدیدی بود که معلوم شده بود براورد او (براساس جدولهایی که فقط تا $x = ۴۰۰۰۰۰$ را دربر داشتند) صرفاً از نظر تاریخی جالب است.

امروزه اطلاعات بسیار بیشتری دربارهٔ رابطهٔ میان $\pi(x)$ و $\mathrm{Li}(x)$ در دست است. از میان آنها فقط به ذکر قضیهٔ لیتلوود می‌پردازیم که حاکی است: اگر x بر مجموعهٔ همهٔ عددهای صحیح مثبت تغییر کند، آنگاه تفاضل $\pi(x) - \mathrm{Li}(x)$ هم مقادیر مثبت و هم مقادیر منفی را بینهایت بار اختیار می‌کند. قضیهٔ لیتلوود صرفاً یک «قضیهٔ وجودی» است و تاکنون مقداری عددی برای x که به‌ازای آن $\pi(x) - \mathrm{Li}(x)$ مثبت باشد، به‌دست نیامده است. شگفت‌آور اینکه کران بالایی

1. de la Vallée Poussin

برای نخستین x ای که در $\pi(x) > \mathrm{Li}(x)$ صدق می‌کند پیدا شده است. چنین x ای کوچکتر از عددی با بزرگی غیرقابل‌تصور

$$e^{e^{e^{۷۹}}} \approx ۱۰^{۱۰^{۱۰^{۳۴}}}$$

است. این کران بالا، که اسکیوز[1] در ۱۹۳۳ آن را به‌دست آورد، به عدد اسکیوز معروف است. مدتی بعد (در ۱۹۵۵)، اسکیوز بالاترین نمای عدد خود را از ۳۴ به ۳ تقلیل داد. در ۱۹۸۶، با اثبات وجود بیش از $۱۰^{۱۸۰}$ عدد صحیح متوالی میان $(۶٫۶۲)۱۰^{۳۷۰}$ و $(۶٫۶۹)۱۰^{۳۷۰}$ که به‌ازای آنها $\pi(x) > \mathrm{Li}(x)$، کران اسکیوز به‌طور قابل‌ملاحظه‌ای تقلیل یافت. مع‌الوصف، هنوز مقدار عددی مشخصی از x به‌طوری که $\pi(x) > \mathrm{Li}(x)$، خارج از دسترس هر رایانه‌ای است. نکته‌ای که شاید قابل‌توجه باشد این است که به‌ازای هر x ای که مقدار دقیق $\pi(x)$ برای آن محاسبه‌شده یعنی به‌ازای هر $x < ۴ \times ۱۰^{۱۶}$، $\pi(x) < \mathrm{Li}(x)$؛ مقادیر $\pi(x)$ و $\mathrm{Li}(x) - \pi(x)$ به‌ازای مقدارهایی از x در جدول زیر ملاحظه می‌شود:

x	$\pi(x)$	$\mathrm{Li}(x) - \pi(x)$
$۱۰^{۹}$	۵۰۸۴۷۵۳۴	۱۷۰۱
$۱۰^{۱۰}$	۴۵۵۰۵۲۵۱۱	۳۱۰۴
$۱۰^{۱۱}$	۴۱۱۸۰۵۴۸۱۳	۱۱۵۸۸
$۱۰^{۱۲}$	۳۷۶۰۷۹۱۲۰۱۸	۳۸۲۶۳
$۱۰^{۱۳}$	۳۴۶۰۶۵۵۳۶۸۳۹	۱۰۸۹۷۱
$۱۰^{۱۴}$	۳۲۰۴۹۴۱۷۵۰۸۰۲	۳۱۴۸۹۰
$۱۰^{۱۵}$	۲۹۸۴۴۵۷۰۴۲۲۶۶۹	۱۰۵۲۶۱۹
$۱۰^{۱۶}$	۲۷۹۲۳۸۳۴۱۰۳۳۹۲۵	۳۲۱۴۶۳۲
۴×۱۰^{۱۶}	۱۰۷۵۲۹۲۷۷۸۷۵۳۱۵۰	۵۵۳۸۸۶۱

گرچه از این جدول چنین برمی‌آید که $\mathrm{Li}(x) - \pi(x)$ همیشه مثبت است و متناسب با افزایش x بزرگتر می‌شود، ولی سرانجام مقدارهای منفی بر مقدارهای مثبت چیره خواهند شد.

نکتهٔ فرعی مفیدی در ارتباط با قضیهٔ عددهای اول وجود دارد که قابل‌توجه است؛ داریم

$$\lim_{n\to\infty} \frac{n\log n}{p_n} = ۱$$

1. S. Skewes

زیرا اگر از رابطهٔ

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=۱$$

شروع کنیم و با توجه به پیوستگی تابع لگاریتمی، لگاریتم بگیریم، به‌دست می‌آوریم

$$\lim_{x\to\infty}[\log \pi(x)+\log(\log x)-\log x]=۰$$

یا معادلش

$$\lim_{x\to\infty}\frac{\log \pi(x)}{\log x}=۱-\lim_{x\to\infty}\frac{\log(\log x)}{\log x}$$

ولی $\lim_{x\to\infty}\log(\log x)/\log x=۰$، که نتیجه می‌دهد

$$\lim_{x\to\infty}\frac{\log \pi(x)}{\log x}=۱$$

بنابراین

$$۱=\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=\lim_{x\to\infty}\frac{\pi(x)\log \pi(x)}{x}\times\frac{\log x}{\log \pi(x)}$$
$$=\lim_{x\to\infty}\frac{\pi(x)\log \pi(x)}{x}$$

اگر قرار دهیم $x=p_n$، آنگاه $\pi(p_n)=n$، و نتیجه می‌شود

$$\lim_{n\to\infty}\frac{n\log n}{p_n}=۱$$

این نتیجه را می‌توان چنین تعبیر کرد که اگر در بازه‌ای n عدد اول موجود باشد، طول بازه تقریباً $n\log n$ است.

تا این اواخر، عقیدهٔ رایج این بود که اثبات قضیهٔ عددهای اول بدون استفاده از ویژگیهای تابع زتا و بدون توسل به نظریهٔ توابع مختلط ممکن نیست. بنابراین، کشف اثباتی کاملاً حسابی توسط آتله‌سلبرگ[1] ریاضیدان نروژی، در ۱۹۴۹، مایهٔ شگفتی فراوان گردید. مقالهٔ او تحت عنوان اثباتی مقدماتی از قضیهٔ عددهای اول، گرچه به لحاظ پرهیز از روشهای آنالیز نوین «مقدماتی» است، محتوای آن فوق‌العاده پیچیده است. سلبرگ در ۱۹۵۰، به‌خاطر دستاوردهایش در این زمینه به دریافت مدال فیلدز ازکنگرهٔ بین‌المللی ریاضی‌دانان نائل شد. مدال فیلدز در ریاضیات همتراز جایزهٔ نوبل شمرده می‌شود. (عقیدهٔ عمومی بر این است که رابطهٔ بد آلفرد نوبل با گوستامیتتاگ ـ لفلر[2] [ریاضیدان معروف سوئدی] باعث شد که نوبل جایزه‌ای در ریاضیات مقرر نکند.)

1. Atle Selberg　　2. Gösta Mittag-Leffler

مراجع عمومی

1. Adams, W., and L. Goldstein. 1976. *Introduction to Number Theory.* Englewood Cliffs, N.J.: Prentice-Hall.
2. Agnew, Jeanne. 1972. *Exploring Number Theory.* Monterey, Calif.: Brooks/Cole.
3. Archibald, Ralph. 1970. *An Introduction to the Theory of Numbers.* Columbus, Ohio: Charles E. Merrill.
4. Baker, Alan. 1984. *A Concise Introduction to the Theory of Numbers.* Cambridge, England: Cambridge University Press.
5. Barnett, I. A. 1972. *Elements of Number Theory.* Rev. ed. Boston: Prindle, Weber & Schmidt.
6. Beck, A., M. Bleicher, and D. Crowe. 1969. *Excursions into Mathematics.* New York: Worth.
7. Beiler, A. H. 1966. *Recreations in the Theory of Numbers.* 2d ed. New York: Dover.
8. Burton, David. 1985. *The History of Mathematics: An Introduction.* Boston: Allyn and Bacon.
9. Dantzig, Tobias. 1956. *Number: The Language of Science.* Garden City, N.Y.: Doubleday.
10. Dickson, Leonard. 1920. *History of the Theory of Numbers.* Vols. 1, 2, 3. Washington, D.C.: Carnegie Institute of Washington. (Reprinted, New York: Chelsea, 1952).
11. Edwards, Harold. 1977. *Fermat's Last Theorem.* New York: Springer-Verlag.
12. Eves, Howard. 1983. *An Introduction to the History of Mathematics.* 5th ed. Philadelphia: Saunders College Publishing.
13. Guy, Richard. 1981. *Unsolved Problems in Number Theory.* New York: Springer-Verlag.
14. Hardy, G. H. and E. M. Wright. 1975. *An Introduction to the Theory of Numbers.* 5th ed. London: Oxford University Press.
15. Heath, Thomas. 1910. *Diophantus of Alexandria.* Cambridge, England: Cambridge University Press. (Reprinted, New York: Dover, 1964.)
16. Hoggatt, Jr., Verner E. 1969. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin.
17. Ireland, K. and M. Rosen. 1972. *Elements of Number Theory: Including an Introduction to Equations over Finite Fields.* Tarrytown-on-Hudson, N.Y.: Bogden and Quigley.

18. Landau, E. 1952. *Elementary Number Theory.* Trans. Goodman. New York: Chelsea.
19. Le Veque, William. 1977. *Fundamentals of Number Theory.* Reading, Mass.: Addison-Wesley.
20. Long, Calvin. 1972. *Elementary Introduction to Number Theory.* 2d ed. Lexington, Mass.: D. C. Heath.
21. Maxfield, J. and M. Maxfield. 1972. *Discovering Number Theory.* Philadelphia: W. B. Saunders.
22. Nagell, Trygve. 1964. *Introduction to Number Theory.* 2d ed. New York: Chelsea.
23. Niven, I. and H. Zuckerman. 1980. *An Introduction to the Theory of Numbers.* 4th ed. New York: John Wiley and Sons.
24. Ogilvy, C. S. and J. Anderson. 1966. *Excursions in Number Theory.* New York: Oxford University Press.
25. Olds, Carl D. 1963. *Continued Fractions.* New York: Random House.
26. Ore, Oystein. 1948. *Number Theory and Its History.* New York: McGraw-Hill.
27. ———. 1967. *Invitation to Number Theory.* New York: Random House.
28. Ribenboim, Paulo. 1979. *13 Lectures on Fermat's Last Theorem.* New York: Springer-Verlag.
29. ———. 1988. *The Book of Prime Number Records.* New York: Springer-Verlag.
30. Riesel, Hans. 1985. *Prime Numbers and Computer Methods for Factorization.* Boston: Birkhauser.
31. Roberts, Joe. 1977. *Elementary Number Theory.* Cambridge, Mass.: MIT Press.
32. Rosen, Kenneth. 1987. *Elementary Number Theory and Its Applications.* 2d. ed. Reading, Mass.: Addison-Wesley.
33. Scharlu, W. and H. Opolka. 1984. *From Fermat to Minkowski.* New York: Springer-Verlag.
34. Schroeder, Manfred. 1987. *Number Theory in Science and Communication.* 2d. ed. New York: Springer-Verlag.
35. Shanks, Daniel. 1985. *Solved and Unsolved Problems in Number Theory.* 3d ed. New York: Chelsea.
36. Shoemaker, Richard. 1973. *Perfect Numbers.* Washington, D.C.: National Council of Teachers of Mathematics.
37. Sierpinski, Waclaw. 1964. *Elementary Theory of Numbers.* Trans. Hulanicki. Warsaw: Panstwowe Wydawnictwo Naukowe.
38. ———. 1962. *Pythagorean Triangles.* Trans. Sharma. New York: Academic Press.

39. Starke, Harold. 1970. *An Introduction to Number Theory.* Chicago: Markham.
40. Stewart, B. M. 1964. *Theory of Numbers.* 2d ed. New York: Macmillan.
41. Struik, Dirk. 1969. *A Source Book in Mathematics 1200–1800.* Cambridge: Harvard University Press.
42. Upensky, J. and M. A. Heaslet. 1939. *Elementary Number Theory.* New York: McGraw-Hill.
43. Vorobyov, N. 1963. *The Fibonacci Numbers.* Boston: D. C. Heath.
44. Weil, Andre. 1984. *Number Theory: An Approach through History.* Boston: Birkhauser.

مراجعی برای مطالعهٔ بیشتر

1. Bezuska, Stanley. "Even Perfect Numbers—An Update." *Mathematics Teacher* 74(1981): 460–63.
2. Brown, Ezra. "The First Proof of the Quadratic Reciprocity Law, Revisited." *American Mathematical Monthly* 88(1981): 257–64.
3. Collison, Mary Joan. "The Unique Factorization Theorem: From Euclid to Gauss." *Mathematics Magazine* 53(1980): 96–100.
4. Cox, David. "Quadratic Reciprocity: Its Conjecture and Application." *American Mathematical Monthly* 95 (1988): 442–48.
5. Devlin, Keith. "Factoring Fermat Numbers." *New Scientist* 111, no. 1527(1986): 41–44.
6. Dixon, John. "Factorization and Primality Tests." *American Mathematical Monthly* 91(1984): 333–51.
7. Dudley, Underwood. "Formulas for Primes." *Mathematics Magazine* 56(1983): 17–22.
8. Edwards, Harold. "Euler and Quadratic Recriprocity." *Mathematics Magazine* 56(1983): 285–91.
9. Erdos, Paul. "Some Unconventional Problems in Number Theory." *Mathematics Magazine* 52(1979): 67–70.
10. ———. "Some Remarks and Problems in Number Theory Related to the Work of Euler." *Mathematics Magazine* 56(1983): 292–98.
11. Francis, Richard. "Mathematical Haystacks: Another Look at Repunit Numbers." *College Mathematics Journal* 19 (1988): 240–46.
12. Gardner, Martin. "Simple Proofs of the Pythagorean Theorem, and Sundry Other Matters." *Scientific American* 211(Oct. 1964): 118–26.
13. ———. "A Short Treatise on the Useless Elegance of Perfect Numbers and Amicable Pairs." *Scientific American* 218(March 1968): 121–26.
14. ———. "The Fascination of the Fibonacci Sequence." *Scientific American* 220(March 1969): 116–20.
15. ———. "Diophantine Analysis and the Problem of Fermat's Legendary 'Last Theorem.' " *Scientific American* 223(July, 1970): 117–19.
16. ———. "On Expressing Integers as the Sums of Cubes and Other Unsolved Number-Theory Problems." *Scientific American* 229(Dec. 1973): 118–21.
17. ———. "A New Kind of Cipher That Would Take Millions of Years to Break." *Scientific American* 237(Aug. 1977): 120–24.

18. ———. "Patterns in Primes Are a Clue to the Strong Law of Small Numbers." *Scientific American* 243(Dec. 1980): 18–28.

19. Goldstein, Larry. "A History of the Prime Number Theorem." *American Mathematical Monthly* 80(1973): 599–615.

20. Honsberger, Ross. "An Elementary Gem Concerning $\pi(n)$, the Number of Primes $< n$." *Two-Year College Mathematics Journal* 11(1980): 305–11.

21. Lee, Elvin, and Joseph Madachy. "The History and Discovery of Amicable Numbers—Part I." *Journal of Recreational Mathematics* 5(1972): 77–93.

22. Luciano, Dennis and Gordon Prichett. "Cryptography: From Caesar Ciphers to Public-Key Cryptosystems." *College Mathematics Journal* 18 (1987): 2–17.

23. Mahoney, Michael. "Fermat's Mathematics: Proofs and Conjectures." *Science* 178(Oct. 1972): 30–36.

24. McCarthy, Paul. "Odd Perfect Numbers." *Scripta Mathematica* 23(1957): 43–47.

25. Matkovic, David. "The Chinese Remainder Theorem: An Historical Account." *Pi Mu Epsilon Journal* 8 (1988): 493–502.

26. Ondrejka, Rudolf. "Ten Extraordinary Primes." *Journal of Recreational Mathematics* 18(1985–86): 87–92.

27. Pomerance, Carl. "Recent Developments in Primality Testing." *The Mathematical Intelligencer* 3(1981): 97–105.

28. ———. "The Search for Prime Numbers." *Scientific American* 247(Dec. 1982): 122–30.

29. Reid, Constance. "Perfect Numbers." *Scientific American* 88(March, 1953): 84–86.

30. Ribenboim, Paulo. "Lecture: Recent Results on Fermat's Last Theorem." *Canadian Mathematical Bulletin* 20(1977): 229–42.

31. Schroeder, Manfred. "Where Is the Next Mersenne Prime Hiding?" *The Mathematical Intelligencer* 5, no. 3 (1983): 31–33.

32. Sierpinski, Waclaw. "On Some Unsolved Problems of Arithmetic." *Scripta Mathematica* 25(1960): 125–36.

33. Slowinski, David. "Searching for the 27th Mersenne Prime." *Journal of Recreational Mathematics* 11(1978–79): 258–61.

34. Small, Charles. "Waring's Problem." *Mathematics Magazine* 50(1977): 12–16.

35. Uhler, Horace. "A Brief History of the Investigations on Mersenne Numbers and the Latest Immense Primes." *Scripta Mathematica* 18(1952): 122–31.

36. Vandiver, H. S. "Fermat's Last Theorem." *American Mathematical Monthly* 53(1946): 555–78.

37. Wagon, Stan. "Fermat's Last Theorem." *The Mathematical Intelligencer* 8, no. 1 (1986): 59–61.

38. ———. "Carmichael's 'Empirical Theorem.'" *The Mathematical Intelligencer* 8, no. 2 (1986): 61–63.

39. Yates, Samuel. "Peculiar Properties of Repunits." *Journal of Recreational Mathematics* 2(1969): 139–46.

40. ———. "The Mystique of Repunits." *Mathematics Magazine* 51(1978): 22–28.

جدولها

جدول ۱ جدول زیر، کوچکترین ریشهٔ اولیه (r) از هر عدد اول p، $2 \le p \le 1000$ را به‌دست می‌دهد.

p	r	p	r	p	r	p	r	p	r	p	r
2	1	127	3	283	3	467	2	661	2	877	2
3	2	131	2	293	2	479	13	673	5	881	3
5	2	137	3	307	5	487	3	677	2	883	2
7	3	139	2	311	17	491	2	683	5	887	5
11	2	149	2	313	10	499	7	691	3	907	2
13	2	151	6	317	2	503	5	701	2	911	17
17	3	157	5	331	3	509	2	709	2	919	7
19	2	163	2	337	10	521	3	719	11	929	3
23	5	167	5	347	2	523	2	727	5	937	5
29	2	173	2	349	2	541	2	733	6	941	2
31	3	179	2	353	3	547	2	739	3	947	2
37	2	181	2	359	7	557	2	743	5	953	3
41	6	191	19	367	6	563	2	751	3	967	5
43	3	193	5	373	2	569	3	757	2	971	6
47	5	197	2	379	2	571	3	761	6	977	3
53	2	199	3	383	5	577	5	769	11	983	5
59	2	211	2	389	2	587	2	773	2	991	6
61	2	223	3	397	5	593	3	787	2	997	7
67	2	227	2	401	3	599	7	797	2		
71	7	229	6	409	21	601	7	809	3		
73	5	233	3	419	2	607	3	811	3		
79	3	239	7	421	2	613	2	821	2		
83	2	241	7	431	7	617	3	823	3		
89	3	251	6	433	5	619	2	827	2		
97	5	257	3	439	15	631	3	829	2		
101	2	263	5	443	2	641	3	839	11		
103	5	269	2	449	3	643	11	853	2		
107	2	271	6	457	13	647	5	857	3		
109	6	277	5	461	2	653	2	859	2		
113	3	281	3	463	3	659	2	863	5		

جدول ۲ در جدول زیر، کوچکترین عامل اول هر عدد صحیح فرد n، $3 \le n \le 4999$، که بر ۵ تقسیم‌پذیر نباشد، آمده است. علامت تیره (ـ) نشان‌دهندهٔ این است که n خودش اول است.

1		101	—	201	3	301	7	401	—
3	—	103	—	203	7	303	3	403	13
7	—	107	—	207	3	307	—	407	11
9	3	109	—	209	11	309	3	409	—
11	—	111	3	211	—	311	—	411	3
13	—	113	—	213	3	313	—	413	7
17	—	117	3	217	7	317	—	417	3
19	—	119	7	219	3	319	11	419	—
21	3	121	11	221	13	321	3	421	—
23	—	123	3	223	—	323	17	423	3
27	3	127	—	227	—	327	3	427	7
29	—	129	3	229	—	329	7	429	3
31	—	131	—	231	3	331	—	431	—
33	3	133	7	233	—	333	3	433	—
37	—	137	—	237	3	337	—	437	19
39	3	139	—	239	—	339	3	439	—
41	—	141	3	241	—	341	11	441	3
43	—	143	11	243	3	343	7	443	—
47	—	147	3	247	13	347	—	447	3
49	7	149	—	249	3	349	—	449	—
51	3	151	—	251	—	351	3	451	11
53	—	153	3	253	11	353	—	453	3
57	3	157	—	257	—	357	3	457	—
59	—	159	3	259	7	359	—	459	3
61	—	161	7	261	3	361	19	461	—
63	3	163	—	263	—	363	3	463	—
67	—	167	—	267	3	367	—	467	—
69	3	169	13	269	—	369	3	469	7
71	—	171	3	271	—	371	7	471	3
73	—	173	—	273	3	373	—	473	11
77	7	177	3	277	—	377	13	477	3
79	—	179	—	279	3	379	—	479	—
81	3	181	—	281	—	381	3	481	13
83	—	183	3	283	—	383	—	483	3
87	3	187	11	287	7	387	3	487	—
89	—	189	3	289	17	389	—	489	3
91	7	191	—	291	3	391	17	491	—
93	3	193	—	293	—	393	3	493	17
97	—	197	—	297	3	397	—	497	7
99	3	199	—	299	13	399	3	499	—

جدول ۲ (ادامه)

501	3	601	—	701	—	801	3	901	17
503	—	603	3	703	19	803	11	903	3
507	3	607	—	707	7	807	3	907	—
509	—	609	3	709	—	809	—	909	3
511	7	611	13	711	3	811	—	911	—
513	3	613	—	713	23	813	3	913	11
517	11	617	—	717	3	817	19	917	7
519	3	619	—	719	—	819	3	919	—
521	—	621	3	721	7	821	—	921	3
523	—	623	7	723	3	823	—	923	13
527	17	627	3	727	—	827	—	927	3
529	23	629	17	729	3	829	—	929	—
531	3	631	—	731	17	831	3	931	7
533	13	633	3	733	—	833	7	933	3
537	3	637	7	737	11	837	3	937	—
539	7	639	3	739	—	839	—	939	3
541	—	641	—	741	3	841	29	941	—
543	3	643	—	743	—	843	3	943	23
547	—	647	—	747	3	847	7	947	—
549	3	649	11	749	7	849	3	949	13
551	19	651	3	751	—	851	23	951	3
553	7	653	—	753	3	853	—	953	—
557	—	657	3	757	—	857	—	957	3
559	13	659	—	759	3	859	—	959	7
561	3	661	—	761	—	861	3	961	31
563	—	663	3	763	7	863	—	963	3
567	3	667	23	767	13	867	3	967	—
569	—	669	3	769	—	869	11	969	3
571	—	671	11	771	3	871	13	971	—
573	3	673	—	773	—	873	3	973	7
577	—	677	—	777	3	877	—	977	—
579	3	679	7	779	19	879	3	979	11
581	7	681	3	781	11	881	—	981	3
583	11	683	—	783	3	883	—	983	—
587	—	687	3	787	—	887	—	987	3
589	19	689	13	789	3	889	7	989	23
591	3	691	—	791	7	891	3	991	—
593	—	693	3	793	13	893	19	993	3
597	3	697	17	797	—	897	3	997	—
599	—	699	3	799	17	899	29	999	3

جدول ۲ (ادامه)

1001	7	1101	3	1201	—	1301	—	1401	3
1003	17	1103	—	1203	3	1303	—	1403	23
1007	19	1107	3	1207	17	1307	—	1407	3
1009	—	1109	—	1209	3	1309	7	1409	—
1011	3	1111	11	1211	7	1311	3	1411	17
1013	—	1113	3	1213	—	1313	13	1413	3
1017	3	1117	—	1217	—	1317	3	1417	13
1019	—	1119	3	1219	23	1319	—	1419	3
1021	—	1121	19	1221	3	1321	—	1421	7
1023	3	1123	—	1223	—	1323	3	1423	—
1027	13	1127	7	1227	3	1327	—	1427	—
1029	3	1129	—	1229	—	1329	3	1429	—
1031	—	1131	3	1231	—	1331	11	1431	3
1033	—	1133	11	1233	3	1333	31	1433	—
1037	17	1137	3	1237	—	1337	7	1437	3
1039	—	1139	17	1239	3	1339	13	1439	—
1041	3	1141	7	1241	17	1341	3	1441	11
1043	7	1143	3	1243	11	1343	17	1443	3
1047	3	1147	31	1247	29	1347	3	1447	—
1049	—	1149	3	1249	—	1349	19	1449	3
1051	—	1151	—	1251	3	1351	7	1451	—
1053	3	1153	—	1253	7	1353	3	1453	—
1057	7	1157	13	1257	3	1357	23	1457	31
1059	3	1159	19	1259	—	1359	3	1459	—
1061	—	1161	3	1261	13	1361	—	1461	3
1063	—	1163	—	1263	3	1363	29	1463	7
1067	11	1167	3	1267	7	1367	—	1467	3
1069	—	1169	7	1269	3	1369	37	1469	13
1071	3	1171	—	1271	31	1371	3	1471	—
1073	29	1173	3	1273	19	1373	—	1473	3
1077	3	1177	11	1277	—	1377	3	1477	7
1079	13	1179	3	1279	—	1379	7	1479	3
1081	23	1181	—	1281	3	1381	—	1481	—
1083	3	1183	7	1283	—	1383	3	1483	—
1087	—	1187	—	1287	3	1387	19	1487	—
1089	3	1189	29	1289	—	1389	3	1489	—
1091	—	1191	3	1291	—	1391	13	1491	3
1093	—	1193	—	1293	3	1393	7	1493	—
1097	—	1197	3	1297	—	1397	11	1497	3
1099	7	1199	11	1299	3	1399	—	1499	—

جدول ۲ (ادامه)

1501	19	1601	—	1701	3	1801	—	1901	—
1503	3	1603	7	1703	13	1803	3	1903	11
1507	11	1607	—	1707	3	1807	13	1907	—
1509	3	1609	—	1709	—	1809	3	1909	23
1511	—	1611	3	1711	29	1811	—	1911	3
1513	17	1613	—	1713	3	1813	7	1913	—
1517	37	1617	3	1717	17	1817	23	1917	3
1519	7	1619	—	1719	3	1819	17	1919	19
1521	3	1621	—	1721	—	1821	3	1921	17
1523	—	1623	3	1723	—	1823	—	1923	3
1527	3	1627	—	1727	11	1827	3	1927	41
1529	11	1629	3	1729	7	1829	31	1929	3
1531	—	1631	7	1731	3	1831	—	1931	—
1533	3	1633	23	1733	—	1833	3	1933	—
1537	29	1637	—	1737	3	1837	11	1937	13
1539	3	1639	11	1739	37	1839	3	1939	7
1541	23	1641	3	1741	—	1841	7	1941	3
1543	—	1643	31	1743	3	1843	19	1943	29
1547	7	1647	3	1747	—	1847	—	1947	3
1549	—	1649	17	1749	3	1849	43	1949	—
1551	3	1651	13	1751	17	1851	3	1951	—
1553	—	1653	3	1753	—	1853	17	1953	3
1557	3	1657	—	1757	7	1857	3	1957	19
1559	—	1659	3	1759	—	1859	11	1959	3
1561	7	1661	11	1761	3	1861	—	1961	37
1563	3	1663	—	1763	41	1863	3	1963	13
1567	—	1667	—	1767	3	1867	—	1967	7
1569	3	1669	—	1769	29	1869	3	1969	11
1571	—	1671	3	1771	7	1871	—	1971	3
1573	11	1673	7	1773	3	1873	—	1973	—
1577	19	1677	3	1777	—	1877	—	1977	3
1579	—	1679	23	1779	3	1879	—	1979	—
1581	3	1681	41	1781	13	1881	3	1981	7
1583	—	1683	3	1783	—	1883	7	1983	3
1587	3	1687	7	1787	—	1887	3	1987	—
1589	7	1689	3	1789	—	1889	—	1989	3
1591	37	1691	19	1791	3	1891	31	1991	11
1593	3	1693	—	1793	11	1893	3	1993	—
1597	—	1697	—	1797	3	1897	7	1997	—
1599	3	1699	—	1799	7	1899	3	1999	—

جدول ۲ (ادامه)

2001	3	2101	11	2201	31	2301	3	2401	7
2003	—	2103	3	2203	—	2303	7	2403	3
2007	3	2107	7	2207	—	2307	3	2407	29
2009	7	2109	3	2209	47	2309	—	2409	3
2011	—	2111	—	2211	3	2311	—	2411	—
2013	3	2113	—	2213	—	2313	3	2413	19
2017	—	2117	29	2217	3	2317	7	2417	—
2019	3	2119	13	2219	7	2319	3	2419	41
2021	43	2121	3	2221	—	2321	11	2421	3
2023	7	2123	11	2223	3	2323	23	2423	—
2027	—	2127	3	2227	17	2327	13	2427	3
2029	—	2129	—	2229	3	2329	17	2429	7
2031	3	2131	—	2231	23	2331	3	2431	11
2033	19	2133	3	2233	7	2333	—	2433	3
2037	3	2137	—	2237	—	2337	3	2437	—
2039	—	2139	3	2239	—	2339	—	2439	3
2041	13	2141	—	2241	3	2341	—	2441	—
2043	3	2143	—	2243	—	2343	3	2443	7
2047	23	2147	19	2247	3	2347	—	2447	—
2049	3	2149	7	2249	13	2349	3	2449	31
2051	7	2151	3	2251	—	2351	—	2451	3
2053	—	2153	—	2253	3	2353	13	2453	11
2057	11	2157	3	2257	37	2357	—	2457	3
2059	29	2159	17	2559	3	2359	7	2459	—
2061	3	2161	—	2261	7	2361	3	2461	23
2063	—	2163	3	2263	31	2363	17	2463	3
2067	3	2167	11	2267	—	2367	3	2467	—
2069	—	2169	3	2269	—	2369	23	2469	3
2071	19	2171	13	2271	3	2371	—	2471	7
2073	3	2173	41	2273	—	2373	3	2473	—
2077	31	2177	7	2277	3	2377	—	2477	—
2079	3	2179	—	2279	43	2379	3	2479	37
2081	—	2181	3	2281	—	2381	—	2481	3
2083	—	2183	37	2283	3	2383	—	2483	13
2087	—	2187	3	2287	—	2387	7	2487	3
2089	—	2189	11	2289	3	2389	—	2489	19
2091	3	2191	7	2291	29	2391	3	2491	47
2093	7	2193	3	2293	—	2393	—	2493	3
2097	3	2197	13	2297	—	2397	3	2497	11
2099	—	2199	3	2299	11	2399	—	2499	3

جدول ۲ (ادامه)

2501	41	2601	3	2701	37	2801	—	2901	3
2503	—	2603	19	2703	3	2803	—	2903	—
2507	23	2607	3	2707	—	2807	7	2907	3
2509	13	2609	—	2709	3	2809	53	2909	—
2511	3	2611	7	2711	—	2811	3	2911	41
2513	7	2613	3	2713	—	2813	29	2913	3
2517	3	2617	—	2717	11	2817	3	2917	—
2519	11	2619	3	2719	—	2819	—	2919	3
2521	—	2621	—	2721	3	2821	7	2921	23
2523	3	2623	43	2723	7	2823	3	2923	37
2527	7	2627	37	2727	3	2827	11	2927	—
2529	3	2629	11	2729	—	2829	3	2929	29
2531	—	2631	3	2731	—	2831	19	2931	3
2533	17	2633	—	2733	3	2833	—	2933	7
2537	43	2637	3	2737	7	2837	—	2937	3
2539	—	2639	7	2739	3	2839	17	2939	—
2541	3	2641	19	2741	—	2841	3	2941	17
2543	—	2643	3	2743	13	2843	—	2943	3
2547	3	2647	—	2747	41	2847	3	2947	7
2549	—	2649	3	2749	—	2849	7	2949	3
2551	—	2651	11	2751	3	2851	—	2951	13
2553	3	2653	7	2753	—	2853	3	2953	—
2557	—	2657	—	2757	3	2857	—	2957	—
2559	3	2659	—	2759	31	2859	3	2959	11
2561	13	2661	3	2761	11	2861	—	2961	3
2563	11	2663	—	2763	3	2863	7	2963	—
2567	17	2667	3	2767	—	2867	47	2967	3
2569	7	2669	17	2769	3	2869	19	2969	—
2571	3	2671	—	2771	17	2871	3	2971	—
2573	31	2673	3	2773	47	2873	13	2973	3
2577	3	2677	—	2777	—	2877	3	2977	13
2579	—	2679	3	2779	7	2879	—	2979	3
2581	29	2681	7	2781	3	2881	43	2981	11
2583	3	2683	—	2783	11	2883	3	2983	19
2587	13	2687	—	2787	3	2887	—	2987	29
2589	3	2689	—	2789	—	2889	3	2989	7
2591	—	2691	3	2791	—	2891	7	2991	3
2593	—	2693	—	2793	3	2893	11	2993	41
2597	7	2697	3	2797	—	2897	—	2997	3
2599	23	2699	—	2799	3	2899	13	2999	—

جدول ۲ (ادامه)

3001	—	3101	7	3201	3	3301	—	3401	19
3003	3	3103	29	3203	—	3303	3	3403	41
3007	31	3107	13	3207	3	3307	—	3407	—
3009	3	3109	—	3209	—	3309	3	3409	7
3011	—	3111	3	3211	13	3311	7	3411	3
3013	23	3113	11	3213	3	3313	—	3413	—
3017	7	3117	3	3217	—	3317	31	3417	3
3019	—	3119	—	3219	3	3319	—	3419	13
3021	3	3121	—	3221	—	3321	3	3421	11
3023	—	3123	3	3223	11	3323	—	3423	3
3027	3	3127	53	3227	7	3327	3	3427	23
3029	13	3129	3	3229	—	3329	—	3429	3
3031	7	3131	31	3231	3	3331	—	3431	47
3033	3	3133	13	3233	53	3333	3	3433	—
3037	—	3137	—	3237	3	3337	47	3437	7
3039	3	3139	43	3239	41	3339	3	3439	19
3041	—	3141	3	3241	7	3341	13	3441	3
3043	17	3143	7	3243	3	3343	—	3443	11
3047	11	3147	3	3247	17	3347	—	3447	3
3049	—	3149	47	3249	3	3349	17	3449	—
3051	3	3151	23	3251	—	3351	3	3451	7
3053	43	3153	3	3253	—	3353	7	3453	3
3057	3	3157	7	3257	—	3357	3	3457	—
3059	7	3159	3	3259	—	3359	—	3459	3
3061	—	3161	29	3261	3	3361	—	3461	—
3063	3	3163	—	3263	13	3363	3	3463	—
3067	—	3167	—	3267	3	3367	7	3467	—
3069	3	3169	—	3269	7	3369	3	3469	—
3071	37	3171	3	3271	—	3371	—	3471	3
3073	7	3173	19	3273	3	3373	—	3473	23
3077	17	3177	3	3277	29	3377	11	3477	3
3079	—	3179	11	3279	3	3379	31	3479	7
3081	3	3181	—	3281	17	3381	3	3481	59
3083	—	3183	3	3283	7	3383	17	3483	3
3087	3	3187	—	3287	19	3387	3	3487	11
3089	—	3189	3	3289	11	3389	—	3489	3
3091	11	3191	—	3291	3	3391	—	3491	—
3093	3	3193	31	3293	37	3393	3	3493	7
3097	19	3197	23	3297	3	3397	43	3497	13
3099	3	3199	7	3299	—	3399	3	3499	—

جدول ۲ (ادامه)

3501	3	3601	13	3701	—	3801	3	3901	47
3503	31	3603	3	3703	7	3803	—	3903	3
3507	3	3607	—	3707	11	3807	3	3907	—
3509	11	3609	3	3709	—	3809	13	3909	3
3511	—	3611	23	3711	3	3811	37	3911	—
3513	3	3613	—	3713	47	3813	3	3913	7
3517	—	3617	—	3717	3	3817	11	3917	—
3519	3	3619	7	3719	—	3819	3	3919	—
3521	7	3621	3	3721	61	3821	—	3921	3
3523	13	3623	—	3723	3	3823	—	3923	—
3527	—	3627	3	3727	—	3827	43	3927	3
3529	—	3629	19	3729	3	3829	7	3929	—
3531	3	3631	—	3731	7	3831	3	3931	—
3533	—	3633	3	3733	—	3833	—	3933	3
3537	3	3637	—	3737	37	3837	3	3937	31
3539	—	3639	3	3739	—	3839	11	3939	3
3541	—	3641	11	3741	3	3841	23	3941	7
3543	3	3643	—	3743	19	3843	3	3943	—
3547	—	3647	7	3747	3	3847	—	3947	—
3549	3	3649	41	3749	23	3849	3	3949	11
3551	53	3651	3	3751	11	3851	—	3951	3
3553	11	3653	13	3753	3	3853	—	3953	59
3557	—	3657	3	3757	13	3857	7	3957	3
3559	—	3659	—	3759	3	3859	17	3959	37
3561	3	3661	7	3761	—	3861	3	3961	17
3563	7	3663	3	3763	53	3863	—	3963	3
3567	3	3667	19	3767	—	3867	3	3967	—
3569	43	3669	3	3769	—	3869	53	3969	3
3571	—	3671	—	3771	3	3871	7	3971	11
3573	3	3673	—	3773	7	3873	3	3973	29
3577	7	3677	—	3777	3	3877	—	3977	41
3579	3	3679	13	3779	—	3879	3	3979	23
3581	—	3681	3	3781	19	3881	—	3981	3
3583	—	3683	29	3783	3	3883	11	3983	7
3587	17	3687	3	3787	7	3887	13	3987	3
3589	37	3689	7	3789	3	3889	—	3989	—
3591	3	3691	—	3791	17	3891	3	3991	13
3593	—	3693	3	3793	—	3893	17	3993	3
3597	3	3697	—	3797	—	3897	3	3997	7
3599	59	3699	3	3799	29	3899	7	3999	3

جدول ۲ (ادامه)

4001	—	4101	3	4201	—	4301	11	4401	3
4003	—	4103	11	4203	3	4303	13	4403	7
4007	—	4107	3	4207	7	4307	59	4407	3
4009	19	4109	7	4209	3	4309	31	4409	—
4011	3	4111	—	4211	—	4311	3	4411	11
4013	—	4113	3	4213	11	4313	19	4413	3
4017	3	4117	23	4217	—	4317	3	4417	7
4019	—	4119	3	4219	—	4319	7	4419	3
4021	—	4121	13	4221	3	4321	29	4421	—
4023	3	4123	7	4223	41	4323	3	4423	—
4027	—	4127	—	4227	3	4327	—	4427	19
4029	3	4129	—	4229	—	4329	3	4429	43
4031	29	4131	3	4231	—	4331	61	4431	3
4033	37	4133	—	4233	3	4333	7	4433	11
4037	11	4137	3	4237	19	4337	—	4437	3
4039	7	4139	—	4239	3	4339	—	4439	23
4041	3	4141	41	4241	—	4341	3	4441	—
4043	13	4143	3	4243	—	4343	43	4443	3
4047	3	4147	11	4247	31	4347	3	4447	—
4049	—	4149	3	4249	7	4349	—	4449	3
4051	—	4151	7	4251	3	4351	19	4451	—
4053	3	4153	—	4253	—	4353	3	4453	61
4057	—	4157	—	4257	3	4357	—	4457	—
4059	3	4159	—	4259	—	4359	3	4459	7
4061	31	4161	3	4261	—	4361	7	4461	3
4063	17	4163	23	4263	3	4363	—	4463	—
4067	7	4167	3	4267	17	4367	11	4467	3
4069	13	4169	11	4269	3	4369	17	4469	41
4071	3	4171	43	4271	—	4371	3	4471	17
4073	—	4173	3	4273	—	4373	—	4473	3
4077	3	4177	—	4277	7	4377	3	4477	11
4079	—	4179	3	4279	11	4379	29	4479	3
4081	7	4181	37	4281	3	4381	13	4481	—
4083	3	4183	47	4283	—	4383	3	4483	—
4087	61	4187	53	4287	3	4387	41	4487	7
4089	3	4189	59	4289	—	4389	3	4489	67
4091	—	4191	3	4291	7	4391	—	4491	3
4093	—	4193	7	4293	3	4393	23	4493	—
4097	17	4197	3	4297	—	4397	—	4497	3
4099	—	4199	13	4299	3	4399	53	4499	11

جدول ۲ (ادامه)

4501	7	4601	43	4701	3	4801	—	4901	13
4503	3	4603	—	4703	—	4803	3	4903	—
4507	—	4607	17	4707	3	4807	11	4907	7
4509	3	4609	11	4709	17	4809	3	4909	—
4511	13	4611	3	4711	7	4811	17	4911	3
4513	—	4613	7	4713	3	4813	—	4913	17
4517	—	4617	3	4717	53	4817	—	4917	3
4519	—	4619	31	4719	3	4819	61	4919	—
4521	3	4621	—	4721	—	4821	3	4921	7
4523	—	4623	3	4723	—	4823	7	4923	3
4527	3	4627	7	4727	29	4827	3	4927	13
4529	7	4629	3	4729	—	4829	11	4929	3
4531	23	4631	11	4731	3	4831	—	4931	—
4533	3	4633	41	4733	—	4833	3	4933	—
4537	13	4637	—	4737	3	4837	7	4937	—
4539	3	4639	—	4739	7	4839	3	4939	11
4541	19	4641	3	4741	11	4841	47	4941	3
4543	7	4643	—	4743	3	4843	29	4943	—
4547	—	4647	3	4747	47	4847	37	4947	3
4549	—	4649	—	4749	3	4849	13	4949	7
4551	3	4651	—	4751	—	4851	3	4951	—
4553	29	4653	3	4753	7	4853	23	4953	3
4557	3	4657	—	4757	67	4857	3	4957	—
4559	47	4659	3	4759	—	4859	43	4959	3
4561	—	4661	59	4761	3	4861	—	4961	11
4563	3	4663	—	4763	11	4863	3	4963	7
4567	—	4667	13	4767	3	4867	31	4967	—
4569	3	4669	7	4769	19	4869	3	4969	—
4571	7	4671	3	4771	13	4871	—	4971	3
4573	17	4673	—	4773	3	4873	11	4973	—
4577	23	4677	3	4777	17	4877	—	4977	3
4579	19	4679	—	4779	3	4879	7	4979	13
4581	3	4681	31	4781	7	4881	3	4981	17
4583	—	4683	3	4783	—	4883	19	4983	3
4587	3	4687	43	4787	—	4887	3	4987	—
4589	13	4689	3	4789	—	4889	—	4989	3
4591	—	4691	—	4791	3	4891	67	4991	7
4593	3	4693	13	4793	—	4893	3	4993	—
4597	—	4697	7	4797	3	4897	59	4997	19
4599	3	4699	37	4799	—	4899	3	4999	—

جدول ۳ در جدول زیر، عددهای اول بین ۵۰۰۰ و ۱۰۰۰۰ آمده‌اند.

5003	5387	5693	6053	6367	6761	7103
5009	5393	5701	6067	6373	6763	7109
5011	5399	5711	6073	6379	6779	7121
5021	5407	5717	6079	6389	6781	7127
5023	5413	5737	6089	6397	6791	7129
5039	5417	5741	6091	6421	6793	7151
5051	5419	5743	6101	6427	6803	7159
5059	5431	5749	6113	6449	6823	7177
5077	5437	5779	6121	6451	6827	7187
5081	5441	5783	6131	6469	6829	7193
5087	5443	5791	6133	6473	6833	7207
5099	5449	5801	6143	6481	6841	7211
5101	5471	5807	6151	6491	6857	7213
5107	5477	5813	6163	6521	6863	7219
5113	5479	5821	6173	6529	6869	7229
5119	5483	5827	6197	6547	6871	7237
5147	5501	5839	6199	6551	6883	7243
5153	5503	5843	6203	6553	6899	7247
5167	5507	5849	6211	6563	6907	7253
5171	5519	5851	6217	6569	6911	7283
5179	5521	5857	6221	6571	6917	7297
5189	5527	5861	6229	6577	6947	7307
5197	5531	5867	6247	6581	6949	7309
5209	5557	5869	6257	6599	6959	7321
5227	5563	5879	6263	6607	6961	7331
5231	5569	5881	6269	6619	6967	7333
5233	5573	5891	6271	6637	6971	7349
5237	5581	5903	6277	6653	6977	7351
5261	5591	5923	6287	6659	6983	7369
5273	5623	5927	6299	6661	6991	7393
5279	5639	5939	6301	6673	6997	7411
5281	5641	5953	6311	6679	7001	7417
5297	5647	5981	6317	6689	7013	7433
5303	5651	5987	6323	6691	7019	7451
5309	5653	6007	6329	6701	7027	7457
5323	5657	6011	6337	6703	7039	7459
5333	5659	6029	6343	6709	7043	7477
5347	5669	6037	6353	6719	7057	7481
5351	5683	6043	6359	6733	7069	7487
5381	5689	6047	6361	6737	7079	7489

جدول ۳ (ادامه)

7499	7759	8111	8431	8741	9049	9377	9679
7507	7789	8117	8443	8747	9059	9391	9689
7517	7793	8123	8447	8753	9067	9397	9697
5723	7817	8147	8461	8761	9091	9403	9719
7529	7823	8161	8467	8779	9103	9413	9721
7537	7829	8167	8501	8783	9109	9419	9733
7541	7841	8171	8513	8803	9127	9421	9739
7547	7853	8179	8521	8807	9133	9431	9743
7549	7867	8191	8527	8819	9137	9433	9749
7559	7873	8209	8537	8821	9151	9437	9767
7561	7877	8219	8539	8831	9157	9439	9769
7573	7879	8221	8543	8837	9161	9461	9781
7577	7883	8231	8563	8839	9173	9463	9787
7583	7901	8233	8573	8849	9181	9467	9791
7589	7907	8237	8581	8861	9187	9473	9803
7591	7919	8243	8597	8863	9199	9479	9811
7603	7927	8263	8599	8867	9203	9491	9817
7607	7933	8269	8609	8887	9209	9497	9829
7621	7937	8273	8623	8893	9221	9511	9833
7639	7949	8287	8627	8923	9227	9521	9839
7643	7951	8291	8629	8929	9239	9533	9851
7649	7963	8293	8641	8933	9241	9539	9857
7669	7993	8297	8647	8941	9257	9547	9859
7673	8009	8311	8663	8951	9277	9551	9871
7681	8011	8317	8669	8963	9281	9587	9883
7687	8017	8329	8677	8969	9283	9601	9887
7691	8039	8353	8681	8971	9293	9613	9901
7699	8053	8363	8689	8999	9311	9619	9907
7703	8059	8369	8693	9001	9319	9623	9923
7717	8069	8377	8699	9007	9323	9629	9929
7723	8081	8387	8707	9011	9337	9631	9931
7727	8087	8389	8713	9013	9341	9643	9941
7741	8089	8419	8719	9029	9343	9649	9949
7753	8093	8423	8731	9041	9349	9661	9967
7757	8101	8429	8737	9043	9371	9677	9973

جدول ۴ در جدول زیر تعداد عددهای اول و تعداد زوجهای دوقلوی اول در بازه‌های ذکر شده آمده‌اند.

بازه	تعداد عددهای اول	تعداد زوجهای دوقلوی اول
1-100	25	8
101-200	21	7
201-300	16	4
301-400	16	2
401-500	17	3
501-600	14	2
601-700	16	4
701-800	14	0
801-900	15	5
901-1000	14	0
2501-2600	11	2
2601-2700	15	2
2701-2800	14	3
2801-2900	12	1
2901-3000	11	1
10001-10100	11	4
10101-10200	12	1
10201-10300	10	1
10301-10400	12	2
10401-10500	10	2
29501-29600	10	1
29601-29700	8	1
29701-29800	7	1
29801-29900	10	1
29901-30000	7	0
100001-100100	6	0
100101-100200	9	1
100201-100300	8	0
100301-100400	9	2
100401-100500	8	0
299501-299600	7	1
299601-299700	8	1
299701-299800	8	1
299801-299900	6	0
299901-300000	9	0

جدول ۵ جدول زیر، مربع و مکعب عددهای صحیح n، ۱ $\leq n \leq$ ۴۹۹، را به‌دست می‌دهد.

n	n^2	n^3	n	n^2	n^3
			35	1 225	42 875
1	1	1	36	1 296	46 656
2	4	8	37	1 369	50 653
3	9	27	38	1 444	54 872
4	16	64	39	1 521	59 319
5	25	125	40	1 600	64 000
6	36	216	41	1 681	68 921
7	49	343	42	1 764	74 088
8	64	512	43	1 849	79 507
9	81	729	44	1 936	85 184
10	100	1 000	45	2 025	91 125
11	121	1 331	46	2 116	97 336
12	144	1 728	47	2 209	103 823
13	169	2 197	48	2 304	110 592
14	196	2 744	49	2 401	117 649
15	225	3 375	50	2 500	125 000
16	256	4 096	51	2 601	132 651
17	289	4 913	52	2 704	140 608
18	324	5 832	53	2 809	148 877
19	361	6 859	54	2 916	157 464
20	400	8 000	55	3 025	166 375
21	441	9 261	56	3 136	175 616
22	484	10 648	57	3 249	185 193
23	529	12 167	58	3 364	195 112
24	576	13 824	59	3 481	205 379
25	625	15 625	60	3 600	216 000
26	676	17 576	61	3 721	226 981
27	729	19 683	62	3 844	238 328
28	784	21 952	63	3 969	250 047
29	841	24 389	64	4 096	262 144
30	900	27 000	65	4 225	274 625
31	961	29 791	66	4 356	287 496
32	1 024	32 768	67	4 489	300 763
33	1 089	35 937	68	4 624	314 432
34	1 156	39 304	69	4 761	328 509

جدول ۵ (ادامه)

n	n^2	n^3	n	n^2	n^3
70	4 900	343 000	110	12 100	1 331 000
71	5 041	357 911	111	12 321	1 367 631
72	5 184	373 248	112	12 544	1 404 928
73	5 329	389 017	113	12 769	1 442 897
74	5 476	405 224	114	12 996	1 481 544
75	5 625	421 875	115	13 225	1 520 875
76	5 776	438 976	116	13 456	1 560 896
77	5 929	456 533	117	13 689	1 601 613
78	6 084	474 552	118	13 924	1 643 032
79	6 241	493 039	119	14 161	1 685 159
80	6 400	512 000	120	14 400	1 728 000
81	6 561	531 441	121	14 641	1 771 561
82	6 724	551 368	122	14 884	1 815 848
83	6 889	571 787	123	15 129	1 860 867
84	7 056	592 704	124	15 376	1 906 624
85	7 225	614 125	125	15 625	1 953 125
86	7 396	636 056	126	15 876	2 000 376
87	7 569	658 503	127	16 129	2 048 383
88	7 744	681 472	128	16 384	2 097 152
89	7 921	704 969	129	16 641	2 146 689
90	8 100	729 000	130	16 900	2 197 000
91	8 281	753 571	131	17 161	2 248 091
92	8 464	778 688	132	17 424	2 299 968
93	8 649	804 357	133	17 689	2 352 637
94	8 836	830 584	134	17 956	2 406 104
95	9 025	857 375	135	18 225	2 460 375
96	9 216	884 736	136	18 496	2 515 456
97	9 409	912 673	137	18 769	2 571 353
98	9 604	941 192	138	19 044	2 628 072
99	9 801	970 299	139	19 321	2 685 619
100	10 000	1 000 000	140	19 600	2 744 000
101	10 201	1 030 301	141	19 881	2 803 221
102	10 404	1 061 208	142	20 164	2 863 288
103	10 609	1 092 727	143	20 449	2 924 207
104	10 816	1 124 864	144	20 736	2 985 984
105	11 025	1 157 625	145	21 025	3 048 625
106	11 236	1 191 016	146	21 316	3 112 136
107	11 449	1 225 043	147	21 609	3 176 523
108	11 664	1 259 712	148	21 904	3 241 792
109	11 881	1 295 029	149	22 201	3 307 949

جدول ۵ (ادامه)

n	n^2	n^3	n	n^2	n^3
150	22 500	3 375 000	190	36 100	6 859 000
151	22 801	3 442 951	191	36 481	6 967 871
152	23 104	3 511 808	192	36 864	7 077 888
153	23 409	3 581 577	193	37 249	7 189 057
154	23 716	3 652 264	194	37 636	7 301 384
155	24 025	3 723 875	195	38 025	7 414 875
156	24 336	3 796 416	196	38 416	7 529 536
157	24 649	3 869 893	197	38 809	7 645 373
158	24 964	3 944 312	198	39 204	7 762 392
159	25 281	4 019 679	199	39 601	7 880 599
160	25 600	4 096 000	200	40 000	8 000 000
161	25 921	4 173 281	201	40 401	8 120 601
162	26 244	4 251 528	202	40 804	8 242 408
163	26 569	4 330 747	203	41 209	8 365 427
164	26 896	4 410 944	204	41 616	8 489 664
165	27 225	4 492 125	205	42 025	8 615 125
166	27 556	4 574 296	206	42 436	8 741 816
167	27 889	4 657 463	207	42 849	8 869 743
168	28 224	4 741 632	208	43 264	8 998 912
169	28 561	4 826 809	209	43 681	9 129 329
170	28 900	4 913 000	210	44 100	9 261 000
171	29 241	5 000 211	211	44 521	9 393 931
172	29 584	5 088 448	212	44 944	9 528 128
173	29 929	5 117 717	213	45 369	9 663 597
174	30 276	5 268 024	214	45 796	9 800 344
175	30 625	5 359 375	215	46 225	9 938 375
176	30 976	5 451 776	216	46 656	10 077 696
177	31 329	5 545 233	217	47 089	10 218 313
178	31 684	5 639 752	218	47 524	10 360 232
179	32 041	5 735 339	219	47 961	10 503 459
180	32 400	5 832 000	220	48 400	10 648 000
181	32 761	5 929 741	221	48 841	10 793 861
182	33 124	6 028 568	222	49 284	10 941 048
183	33 489	6 128 487	223	49 729	11 089 567
184	33 856	6 229 504	224	50 176	11 239 424
185	34 225	6 331 625	225	50 625	11 390 625
186	34 596	6 434 856	226	51 076	11 543 176
187	34 969	6 539 203	227	51 529	11 697 083
188	35 344	6 644 672	228	51 984	11 852 352
189	35 721	6 751 269	229	52 441	12 008 989

n	n^2	n^3	n	n^2	n^3
230	52 900	12 167 000	270	72 900	19 683 000
231	53 361	12 326 391	271	73 441	19 902 511
232	53 824	12 487 168	272	73 984	20 123 648
233	54 289	12 649 337	273	74 529	20 346 417
234	54 756	12 812 904	274	75 076	20 570 824
235	55 225	12 977 875	275	75 625	20 796 875
236	55 696	13 144 256	276	76 176	21 024 576
237	56 169	13 312 053	277	76 729	21 253 933
238	56 644	13 481 272	278	77 284	21 484 952
239	57 121	13 651 919	279	77 841	21 717 639
240	57 600	13 824 000	280	78 400	21 952 000
241	58 081	13 997 521	281	78 961	22 188 041
242	58 564	14 172 488	282	79 524	22 425 768
243	59 049	14 348 907	283	80 089	22 665 187
244	59 536	14 526 784	284	80 656	22 906 304
245	60 025	14 706 125	285	81 225	23 149 125
246	60 516	14 886 936	286	81 796	23 393 656
247	61 009	15 069 223	287	82 369	23 639 903
248	61 504	15 252 992	288	82 944	23 887 872
249	62 001	15 438 249	289	83 521	24 137 569
250	62 500	15 625 000	290	84 100	24 389 000
251	63 001	15 813 251	291	84 681	24 642 171
252	63 504	16 003 008	292	85 264	24 897 088
253	64 009	16 194 277	293	85 849	25 153 757
254	64 516	16 387 064	294	86 436	25 412 184
255	65 025	16 581 375	295	87 025	25 672 375
256	65 536	16 777 216	296	87 616	25 934 336
257	66 049	16 974 593	297	88 209	26 198 073
258	66 564	17 173 512	298	88 804	26 463 592
259	67 081	17 373 979	299	89 401	26 730 899
260	67 600	17 576 000	300	90 000	27 000 000
261	68 121	17 779 581	301	90 601	27 270 901
262	68 644	17 984 728	302	91 204	27 543 608
263	69 169	18 191 447	303	91 809	27 818 127
264	69 696	18 399 744	304	92 416	28 094 464
265	70 225	18 609 625	305	93 025	28 372 625
266	70 756	18 821 096	306	93 636	28 652 616
267	71 289	19 034 163	307	94 249	28 934 443
268	71 824	19 248 832	308	94 864	29 218 112
269	72 361	19 465 109	309	95 481	29 503 629

جدول ۵ (ادامه)

n	n^2	n^3	n	n^2	n^3
310	96 100	29 791 000	350	122 500	42 875 000
311	96 721	30 080 231	351	123 201	43 243 551
312	97 344	30 371 328	352	123 904	43 614 208
313	97 969	30 664 297	353	124 609	43 986 977
314	98 596	30 959 144	354	125 316	44 361 864
315	99 225	31 255 875	355	126 025	44 738 875
316	99 856	31 554 496	356	126 736	45 118 016
317	100 489	31 855 013	357	127 449	45 499 293
318	101 124	32 157 432	358	128 164	45 882 712
319	101 761	32 461 759	359	128 881	46 268 279
320	102 400	32 768 000	360	129 600	46 656 000
321	103 041	33 076 161	361	130 321	47 045 881
322	103 684	33 386 248	362	131 044	47 437 928
323	104 329	33 698 267	363	131 769	47 832 147
324	104 976	34 012 224	364	132 496	48 228 544
325	105 625	34 328 125	365	133 225	48 627 125
326	106 276	34 645 976	366	133 956	49 027 896
327	106 929	34 965 783	367	134 689	49 430 863
328	107 584	35 287 552	368	135 424	49 836 032
329	108 241	35 611 289	369	136 161	50 243 409
330	108 900	35 937 000	370	136 900	50 653 000
331	109 561	36 264 691	371	137 641	51 064 811
332	110 224	36 594 368	372	138 384	51 478 848
333	110 889	36 926 037	373	139 129	51 895 117
334	111 556	37 259 704	374	139 876	52 313 624
335	112 225	37 595 375	375	140 625	52 734 375
336	112 896	37 933 056	376	141 376	53 157 376
337	113 569	38 272 753	377	142 129	53 582 633
338	114 244	38 614 472	378	142 884	54 010 152
339	114 921	38 958 219	379	143 641	54 439 939
340	115 600	39 304 000	380	144 400	54 872 000
341	116 281	39 651 821	381	145 161	55 306 341
342	116 964	40 001 688	382	145 924	55 742 968
343	117 649	40 353 607	383	146 689	56 181 887
344	118 336	40 707 584	384	147 456	56 623 104
345	119 025	41 063 625	385	148 225	57 066 625
346	119 716	41 421 736	386	148 996	57 512 456
347	120 409	41 781 923	387	149 769	57 960 603
348	121 104	42 144 192	388	150 544	58 411 072
349	121 801	42 508 549	389	151 321	58 863 869

جدول ۵ (ادامه)

n	n^2	n^3	n	n^2	n^3
390	152 100	59 319 000	430	184 900	79 507 000
391	152 881	59 776 471	431	185 761	80 062 991
392	153 664	60 236 288	432	186 624	80 621 568
393	154 449	60 698 457	433	187 489	81 182 737
394	155 236	61 162 984	434	188 356	81 746 504
395	156 025	61 629 875	435	189 225	82 312 875
396	156 816	62 099 136	436	190 096	82 881 856
397	157 609	62 570 773	437	190 969	83 453 453
398	158 404	63 044 792	438	191 844	84 027 672
399	159 201	63 521 199	439	192 721	84 604 519
400	160 000	64 000 000	440	193 600	85 184 000
401	160 801	64 481 201	441	194 481	85 766 121
402	161 604	64 964 808	442	195 364	86 350 888
403	162 409	65 450 827	443	196 249	86 938 307
404	163 216	65 939 264	444	197 136	87 528 384
405	164 025	66 430 125	445	198 025	88 121 125
406	164 836	66 923 416	446	198 916	88 716 536
407	165 649	67 419 143	447	199 809	89 314 623
408	166 464	67 917 312	448	200 704	89 915 392
409	167 281	68 417 929	449	201 601	90 518 849
410	168 100	68 921 000	450	202 500	91 125 000
411	168 921	69 426 531	451	203 401	91 733 851
412	169 744	69 934 528	452	204 304	92 345 408
413	170 569	70 444 997	453	205 209	92 959 677
414	171 396	70 957 944	454	206 116	93 576 664
415	172 225	71 473 375	455	207 025	94 196 375
416	173 056	71 991 296	456	207 936	94 818 816
417	173 889	72 511 713	457	208 849	95 443 993
418	174 724	73 034 632	458	209 764	96 071 912
419	175 561	73 560 059	459	210 681	96 702 579
420	176 400	74 088 000	460	211 600	97 336 000
421	177 241	74 618 461	461	212 521	97 972 181
422	178 084	75 151 448	462	213 444	98 611 128
423	178 929	75 686 967	463	214 369	99 252 847
424	179 776	76 225 024	464	215 296	99 897 344
425	180 625	76 765 625	465	216 225	100 544 625
426	181 476	77 308 776	466	217 156	101 194 696
427	182 329	77 854 483	467	218 089	101 847 563
428	183 184	78 402 752	468	219 024	102 503 232
429	184 041	78 953 589	469	219 961	103 161 709

جدول ۵ (ادامه)

n	n^2	n^3	n	n^2	n^3
470	220 900	103 823 000	485	235 225	114 084 125
471	221 841	104 487 111	486	236 196	114 791 256
472	222 784	105 154 048	487	237 169	115 501 303
473	223 729	105 823 817	488	238 144	116 214 272
474	224 676	106 496 424	489	239 121	116 930 169
475	225 625	107 171 875	490	240 100	117 649 000
476	226 576	107 850 176	491	241 081	118 370 771
477	227 529	108 531 333	492	242 064	119 095 488
478	228 484	109 215 352	493	243 049	119 823 157
479	229 441	109 902 239	494	244 036	120 553 784
480	230 400	110 592 000	495	245 025	121 287 375
481	231 361	111 284 641	496	246 016	122 023 936
482	232 324	111 980 168	497	247 009	122 763 473
483	233 289	112 678 587	498	248 004	123 505 992
484	234 256	113 379 904	499	249 001	124 251 499

جدول ۶ جدول زیر، مقادیر $\tau(n)$، $\sigma(n)$، $\phi(n)$، و $\mu(n)$ را به‌ازای $1 \leq n \leq 100$ به‌دست می‌دهد

n	$\tau(n)$	$\sigma(n)$	$\phi(n)$	$\mu(n)$	n	$\tau(n)$	$\sigma(n)$	$\phi(n)$	$\mu(n)$
1	1	1	1	1	41	2	42	40	−1
2	2	3	1	−1	42	8	96	12	−1
3	2	4	2	−1	43	2	44	42	−1
4	3	7	2	0	44	6	84	20	0
5	2	6	4	−1	45	6	78	24	0
6	4	12	2	1	46	4	72	22	1
7	2	8	6	−1	47	2	48	46	−1
8	4	15	4	0	48	10	124	16	0
9	3	13	6	0	49	3	57	42	0
10	4	18	4	1	50	6	93	20	0
11	2	12	10	−1	51	4	72	32	1
12	6	28	4	0	52	6	98	24	0
13	2	14	12	−1	53	2	54	52	−1
14	4	24	6	1	54	8	120	18	0
15	4	24	8	1	55	4	72	40	1
16	5	31	8	0	56	8	120	24	0
17	2	18	16	−1	57	4	80	36	1
18	6	39	6	0	58	4	90	28	1
19	2	20	18	−1	59	2	60	58	−1
20	6	42	8	0	60	12	168	16	0
21	4	32	12	1	61	2	62	60	−1
22	4	36	10	1	62	4	96	30	1
23	2	24	22	−1	63	6	104	36	0
24	8	60	8	0	64	7	127	32	0
25	3	31	20	0	65	4	84	48	1
26	4	42	12	1	66	8	144	20	−1
27	4	40	18	0	67	2	68	66	−1
28	6	56	12	0	68	6	126	32	0
29	2	30	28	−1	69	4	96	44	1
30	8	72	8	−1	70	8	144	24	−1
31	2	32	30	−1	71	2	72	70	−1
32	6	63	16	0	72	12	195	24	0
33	4	48	20	1	73	2	74	72	−1
34	4	54	16	1	74	4	114	36	1
35	4	48	24	1	75	6	124	40	0
36	9	91	12	0	76	6	140	36	0
37	2	38	36	−1	77	4	96	60	1
38	4	60	18	1	78	8	168	24	−1
39	4	56	24	1	79	2	80	78	−1
40	8	90	16	0	80	10	186	32	0

جدول ۶ (ادامه)

n	$\tau(n)$	$\sigma(n)$	$\phi(n)$	$\mu(n)$	n	$\tau(n)$	$\sigma(n)$	$\phi(n)$	$\mu(n)$
81	5	121	54	0	91	4	112	72	1
82	4	126	40	1	92	6	168	44	0
83	2	84	82	−1	93	4	128	60	1
84	12	224	24	0	94	4	144	46	1
85	4	108	64	1	95	4	120	72	1
86	4	132	42	1	96	12	252	32	0
87	4	120	56	1	97	2	98	96	−1
88	8	180	40	0	98	6	171	42	0
89	2	90	88	−1	99	6	156	60	0
90	12	234	24	0	100	9	217	40	0

پاسخهای تمرینهای انتخابی

بخش ۱ـ۱

۵. (الف) ۴، ۵، و ۷ (ب) $(۳ \times ۲)! \neq ۳! \times ۲!$، $(۳ + ۲)! \neq ۳! + ۲!$

بخش ۱ـ۳

۵. (الف) $t_۶ = ۲۱$ و $t_۵ = ۱۵$

۶. $t_۱ = ۱^۲$، $t_۸ = ۶^۲$، $t_{۲۸۸} = ۲۰۴^۲$

۷. (ب) $t_۶ = t_۳ + t_۵$، $t_{۱۰} = t_۴ + t_۹$

بخش ۲ـ۳

۱. ۱، ۹، و ۱۷

۲. (الف) $x = ۴$، $y = -۳$ (ب) $x = ۶$، $y = -۱$

(پ) $x = ۷$، $y = -۳$ (ت) $x = ۳۹$، $y = -۲۹$

۸. ۳۲۴۶۱، ۲۲۳۳۸، و ۲۳۶۶۴

۱۲. $x = ۱۷۱$، $y = ۱۱۴$، $z = -۲$

بخش ۲ـ۴

۲. (الف) $x = ۲۰ + ۹t$، $y = -۱۵ - ۷t$

(ب) $x = ۱۸ + ۲۳t$، $y = -۳ - ۴t$

(پ) $x = ۱۷۶ + ۳۵t$، $y = -۱۱۱۱ - ۲۲۱t$

۳. (الف) $x = ۱$، $y = ۶$

(ب) $x = ۲$، $y = ۳۸$؛ $x = ۹$، $y = ۲۰$؛ $x = ۱۶$، $y = ۲$

(پ) فاقد جواب

(ت) $x = ۱۷ - ۵۷t$، $y = ۴۷ - ۱۵۸t$، به‌شرطی که $t \leqslant ۰$

۵. (ب) $x = ۸ + ۲k$، $y = -۴۸ - ۱۵k - ۵t$، $z = ۱۶ + ۵k + ۲t$

۶. (الف) حداقل تعداد سکه‌ها وقتی است که ۳ سکه ده تومانی و ۱۷ سکهٔ بیست و پنج تومانی داشته باشد، و حداکثر آن وقتی که ۴۳ سکهٔ ده تومانی و ۱ سکهٔ بیست و پنج تومانی داشته باشد. داشتن ۱۳ سکهٔ ده تومانی و ۱۳ سکهٔ بیست و پنج تومانی ممکن است.

(ب) ۴۰ بزرگسال و ۲۴ خردسال، یا ۴۵ بزرگسال و ۱۲ خردسال، یا ۵۰ بزرگسال.

(پ) شش ۶ و ده ۹

۷. ۵ گوساله، ۴۱ بره، و ۵۴ بز؛ یا ۱۰ گوساله، ۲۲ بره، ۶۸ بز؛ یا ۱۵ گوساله، ۳ بره، و ۸۲ بز.

۸. ۱۰٫۲۱ دلار

۹. (ب) یک جواب، ۲۸ موز در هر خوشه است.

(ت) یک جواب این است: ۱ مرد، ۵ زن و ۱۴ کودک.

(ث) ۵۶ و ۴۴

بخش ۳ـ۱

۲. ۲۵ یک مثالِ ناقض است.

۷. همهٔ عددهای اول نابیشتر از ۴۷.

۱۱. (الف) $۲^{۱۳} - ۱$ عددی اول است.

بخش ۳ـ۲

۱۱. $۵۳ - ۴۷ = ۵۹ - ۵۳$، $۱۵۷ - ۱۵۱ = ۱۶۳ - ۱۵۷$

۱۳. (ب) $R_{۱۰} = ۱۱ \times ۴۱ \times ۲۷۱ \times ۹۰۹۱$

بخش ۳ـ۳

۳. ۲ و ۵

۱۱. $h(۲۲) = ۲۳ \times ۶۷$

۱۴. ۷۱، ۱۳۸۵۹

۱۶. $۳۷ = -۱ + ۲ + ۳ + ۵ + ۷ + ۱۱ - ۱۳ + ۱۷ - ۱۹ + ۲۳ - ۲۹ + ۳۱,$

$$۳۱ = -۱ + ۲ - ۳ + ۵ - ۷ - ۱۱ + ۱۳ + ۱۷ - ۱۹ - ۲۳ + ۲(۲۹)$$

۱۹.
$$۸۱ = ۳ + ۵ + ۷۳$$
$$۱۲۵ = ۵ + ۱۳ + ۱۰۷$$

۲۸. (ب) $n = ۱$

بخش ۴ـ۲

۴. (الف) ۴ و ۶ (ب) ۰

بخش ۴ـ۳

۲. ۸۹

۵. (الف) ۹، (ب) ۴، (پ) ۵، (ت) ۹.

۸. ۷

۱۰. $x = ۷$ ، $y = ۸$

۱۱. ۱۴۳

۱۴. $n = ۱,۳$

۲۰. $R_۶ = ۳ \times ۷ \times ۱۱ \times ۱۳ \times ۳۷$

۲۲. $x = ۳$، $y = ۲$

۲۳. $x = ۲$، $y = ۱$، $z = ۲$

بخش ۴ـ۴

۱. (الف) (به پیمانهٔ ۲۹) $x \equiv ۱۸$ (ب) (به پیمانهٔ ۲۶) $x \equiv ۱۶$

(پ) (به پیمانهٔ ۲۱) $x \equiv ۶, ۱۳, ۲۰$ (ت) فاقد جواب

(ث) (به پیمانهٔ ۸۹) $x \equiv ۴۵, ۹۴$

(ج) (به پیمانهٔ ۳۰۱) $x \equiv ۱۶, ۵۹, ۱۰۲, ۱۴۵, ۱۸۸, ۲۳۱, ۲۴۷$

۲. (الف) $x = ۱۵ + ۵۱t$، $y = -۱ - ۴t$

(ب) $x = ۱۳ + ۲۵t$، $y = ۷ - ۱۲t$

(پ) $x = ۱۴ + ۵۳t$، $y = ۱ + ۵t$

۳. (به پیمانهٔ ۱۳) $x \equiv ۱۱ + t$، (به پیمانهٔ ۱۳) $y \equiv ۵ + ۶t$

۴. (الف) (به پیمانهٔ ۱۰۵) $x \equiv ۵۲$ (ب) (به پیمانهٔ ۹۸۸۹) $x \equiv ۴۹۴۴$

(پ) (به پیمانهٔ ۱۱۲۲) $x \equiv ۷۸۵$ (ت) (به پیمانهٔ ۷۷۰) $x \equiv ۶۵۳$

۵. (به پیمانهٔ ۲۱۰) $x \equiv ۹۹$

۶. ۶۲

۷. (الف) ۵۴۸، ۵۴۹، ۵۵۰ (ب) ۳۵۰|$۵^۲$، ۳۵۱|$۳^۳$، ۳۵۲|$۲^۴$

۸. ۱۱۹

۹. ۳۰۱

۱۰. ۳۹۳۰

۱۴. ۸۳۸

۱۵. (الف) ۱۷ (ب) ۵۹ (پ) ۱۱۰۳

۱۶. (به پیمانهٔ ۱۵) $n \equiv ۱, ۷, ۱۳$

۱۷. (به پیمانهٔ ۱۳) $x \equiv ۷$، (به پیمانهٔ ۱۳) $y \equiv ۹$

۱۸. (به پیمانهٔ ۲۱۰) $x \equiv ۵۹, ۱۶۴$

بخش ۵ـ۲

۱. (ب) ۸۳ × ۱۲۷ (پ) ۴۹۳ × ۶۹۱

۳. ۲۳ × ۸۹

۴. ۱۷ × ۲۹، ۱۳ × ۲۹۲۵

بخش ۵ـ۳

۶. ۱

۹. (ب) (به پیمانهٔ ۳۱) $x \equiv ۱۶$، (به پیمانهٔ ۱۱) $x \equiv ۱۰$، (به پیمانهٔ ۲۹) $x \equiv ۲۵$

بخش ۵ـ۴

۸. ۵، ۱۳

۱۱. ۱۲، ۱۷؛ ۶، ۳۱

بخش ۶ـ۱

۲. ۶، ۶۳۰۰۴۰۲

۱۲. $p^۹$ و $p^۴q$؛ $۴۸ = ۲^۴ \times ۳$

بخش ۶ـ۳

۳. ۲۴۹، ۳۳۰

۵. (ب) ۱۵۰!، ۱۵۱!، ۱۵۲!، ۱۵۳!، ۱۵۴!

۸. (ب) ۳۶، ۳۹۶

۹. ۴۰۵

بخش ۷ـ۲

۱. ۷۲۰، ۱۱۵۲، ۹۶۰۰

۱۸. اگر $n = ۱۷, ۳۲, ۳۴, ۴۰, ۴۸, ۶۰$، آنگاه $\phi(n) = ۱۶$؛ اگر $n = ۳۵, ۳۹, ۴۵, ۵۲, ۵۶, ۷۰, ۷۲, ۷۸, ۸۴, ۹۰$، آنگاه $\phi(n) = ۲۴$.

بخش ۷ـ۳

۷. ۱

۸. (ب) $x \equiv ۱۹$ (به پیمانهٔ ۲۶)، $x \equiv ۳۴$ (به پیمانهٔ ۴۰)، $x \equiv ۷$ (به پیمانهٔ ۴۹)

بخش ۷ـ۵

۴. ۱۷۴۷، ۱۵۷

۵. ۲۵۳

۶. ۱۷۲۸ ۰۳۳۷ ۱۶۳۱ ۲۱۹۷ ۱۱۰۶ ۱۹۳۲ ۲۳۱۸

۷. REPLY NOW

۸. SELL SHORT

بخش ۸ـ۱

۱. (الف) ۸، ۱۶، ۱۶

(ب) ۱۸، ۱۸، ۹

(پ) ۱۱، ۱۱، ۲۲

۸. (پ) $۲^{۱۷} - ۱$ اول است؛ $۲۳۳ | ۲^{۲۹} - ۱$

۱۲. (الف) ۳، ۷ (ب) ۳، ۵، ۶، ۷، ۱۰، ۱۱، ۱۲، ۱۴

۱۳. (ب) ۴۱، ۲۳۹

بخش ۸ـ۲

۲. ۱، ۴، ۱۱، ۱۴؛ ۸، ۱۸، ۴۷، ۵۷؛ ۸، ۱۴، ۱۹، ۲۵.

۳. ۲، $۲^{۹} \equiv ۶$، $۲^{۷} \equiv ۷$، ۸؛

۲، $۲^{۱۳} \equiv ۳$، $۲^{۱۷} \equiv ۱۰$، $۲^{۵} \equiv ۱۳$، $۲^{۷} \equiv ۱۴$، $۲^{۱۱} \equiv ۱۵$؛

۵، $۵^{۱۹} \equiv ۷$، $۵^{۳} \equiv ۱۰$، $۵^{۹} \equiv ۱۱$، $۵^{۲۱} \equiv ۱۴$، $۵^{۱۷} \equiv ۱۵$، $۵^{۷} \equiv ۱۷$، $۵^{۱۵} \equiv ۱۹$،

$۵^{۵} \equiv ۲۰$، $۵^{۱۳} \equiv ۲۱$.

۴. (الف) ۷، ۳۷ (ب) ۹، ۱۰، ۱۳، ۱۴، ۱۵، ۱۷، ۲۳، ۲۴، ۲۵، ۳۱، ۳۸، ۴۰.

۵. ۱۱، ۵۰

بخش ۸ـ۳

۱. (الف) ۷، ۱۱، ۱۵، ۱۹؛ ۲، ۳، ۸، ۱۲، ۱۳، ۱۷، ۲۲، ۲۳.

(ب) ۲، ۵؛

۲، ۵، ۱۱، ۱۴، ۲۰، ۲۳؛

۲، ۵، ۱۱، ۱۴، ۲۰، ۲۳، ۲۹، ۳۲، ۳۸، ۴۱، ۴۷، ۵۰، ۵۶، ۵۹، ۶۵، ۶۸، ۷۴، ۷۷.

۴. (ب) ۳

۵. ۶، ۷، ۱۱، ۱۲، ۱۳، ۱۵، ۱۷، ۱۹، ۲۲، ۲۴، ۲۶، ۲۸، ۲۹، ۳۰، ۳۴، ۳۵؛

۷، ۱۱، ۱۳، ۱۵، ۱۷، ۱۹، ۲۹، ۳۵، ۴۷، ۵۳، ۶۳، ۶۵، ۶۷، ۶۹، ۷۱، ۷۵.

۱۱. (ب) (به پیمانهٔ ۴۰) $x \equiv ۳۴$، (پیمانهٔ ۷۷) $x \equiv ۳۰$.

بخش ۸ـ۴

۱. $\mathrm{ind}_{۲}۵ = ۹$، $\mathrm{ind}_{۶}۵ = ۹$، $\mathrm{ind}_{۷}۵ = ۳$، $\mathrm{ind}_{۱۱}۵ = ۳$

۲. (الف) (به پیمانهٔ ۱۱) $x \equiv ۷$؛ (ب) (به پیمانهٔ ۱۱) $x \equiv ۵,۶$؛ (پ) فاقد جواب.

۳. (الف) (پیمانهٔ ۱۷) $x \equiv ۶,۷,۱۰,۱۱$؛ (ب) (به پیمانهٔ ۱۷) $x \equiv ۵$.

(پ) (به پیمانهٔ ۱۷) $x \equiv ۳,۵,۶,۷,۱۰,۱۱,۱۲,۱۴$؛ (ت) (به پیمانهٔ ۱۶) $x \equiv ۱$.

۴. ۱۴

۸. (الف) در هر حالت، $a = ۲,۵,۶$.

(ب) ۱، ۲، ۴؛ ۱، ۳، ۴، ۵، ۹؛ ۱، ۳، ۹.

۱۲. فقط معادلهٔ نخست جواب دارد.

۱۶. (ب) (به پیمانهٔ ۱۶) $x \equiv ۳, ۷, ۱۱, ۱۵$؛ (به پیمانهٔ ۱۸) $x \equiv ۸, ۱۷$.

۱۷. (به پیمانهٔ ۱۳) $b \equiv ۱, ۳, ۹$

بخش ۹ـ۱

۱. (الف) (به پیمانهٔ ۱۱) $x \equiv ۶, ۹$؛ (ب) (به پیمانهٔ ۱۳) $x \equiv ۴, ۶$؛
(پ) (به پیمانهٔ ۲۳) $x \equiv ۹, ۲۲$.

۸. (ب) ۶، ۱۱؛ ۱۷، ۲۴

۱۱. (الف) ۱، ۴، ۵، ۶، ۷، ۹، ۱۱، ۱۶، ۱۷
(ب) ۱، ۴، ۵، ۶، ۷، ۹، ۱۳، ۱۶، ۲۰، ۲۲، ۲۳، ۲۴، ۲۵، ۲۸؛
۱، ۲، ۴، ۵، ۷، ۸، ۹، ۱۰، ۱۴، ۱۶، ۱۸، ۱۹، ۲۰، ۲۵، ۲۸.

بخش ۹ـ۲

۱. (الف) −۱ (ب) ۱ (پ) ۱ (ت) −۱ (ث) ۱

۲. (الف) $(-۱)^{۳}$ (ب) $(-۱)^{۳}$ (پ) $(-۱)^{۴}$
(ت) $(-۱)^{۵}$ (ث) $(-۱)^{۹}$

بخش ۹ـ۳

۱. (الف) ۱ (ب) −۱ (پ) −۱ (ت) ۱ (ث) ۱

۳. (الف) حلپذیر (ب) حل‌ناپذیر (پ) حلپذیر

۶. $p = ۲$ یا (به پیمانهٔ ۴) $p \equiv ۱$؛ $p = ۲$ یا (به پیمانهٔ ۸) $p \equiv ۱$ یا ۳؛
$p = ۲$ یا (به پیمانهٔ ۶) $p \equiv ۱$

۸. ۷۳

۱۴. (به پیمانهٔ ۳۵) $x \equiv ۹, ۱۶, ۱۹, ۲۶$

۱۶. −۱، −۱، ۱

۲۰. ندارد

بخش ۹ـ۴

۱. (ب) (به پیمانهٔ $۵^{۳}$) $x \equiv ۵۷, ۶۸$

۲. (الف) (به پیمانهٔ $۳^{۳}$) $x \equiv ۱۳, ۱۴$؛ (ب) (به پیمانهٔ $۵^{۳}$) $x \equiv ۴۲, ۸۳$؛
(پ) (به پیمانهٔ $۷^{۳}$) $x \equiv ۱۰۸, ۱۳۵$.

۳. $x \equiv ۵۰۰۸, ۹۶۳۳$ (به پیمانهٔ $۱۱^۴$)

۴. $x \equiv ۱۲۲, ۱۲۳$ (به پیمانهٔ $۵^۳$)؛ $x \equiv ۱۱, ۱۵$ (به پیمانهٔ $۳^۳$)

۶. $x \equiv ۴۱, ۸۷, ۱۰۵$ (به پیمانهٔ $۲^۷$)

۷. (الف) اگر $a = ۱$، $x \equiv ۱, ۷, ۹, ۱۵$ (به پیمانهٔ $۲^۴$)

اگر $a = ۹$، $x \equiv ۳, ۵, ۱۱, ۱۳$ (به پیمانهٔ $۲^۴$)

(ب) اگر $a = ۱$، $x \equiv ۱, ۱۵, ۱۷, ۳۱$ (به پیمانهٔ $۲^۵$)

اگر $a = ۹$، $x \equiv ۳, ۱۳, ۱۹, ۲۹$ (به پیمانهٔ $۲^۵$)

اگر $a = ۱۷$، $x \equiv ۷, ۹, ۲۳, ۲۵$ (به پیمانهٔ $۲^۵$)

(پ) اگر $a = ۱$، $x \equiv ۱, ۳۱, ۳۳, ۶۳$ (به پیمانهٔ $۲^۶$)

اگر $a = ۹$، $x \equiv ۳, ۲۹, ۳۵, ۶۱$ (به پیمانهٔ $۲^۶$)

اگر $a = ۱۷$، $x \equiv ۷, ۲۵, ۳۹, ۵۷$ (به پیمانهٔ $۲^۶$)

اگر $a = ۲۵$، $x \equiv ۵, ۲۷, ۳۷, ۵۹$ (به پیمانهٔ $۲^۶$)

اگر $a = ۳۳$، $x \equiv ۱۵, ۱۷, ۴۷, ۴۹$ (به پیمانهٔ $۲^۶$)

اگر $a = ۴۱$، $x \equiv ۱۳, ۱۹, ۴۵, ۵۱$ (به پیمانهٔ $۲^۶$)

اگر $a = ۴۹$، $x \equiv ۷, ۲۵, ۳۹, ۵۷$ (به پیمانهٔ $۲^۶$)

اگر $a = ۵۷$، $x \equiv ۱۱, ۲۱, ۴۳, ۵۳$ (به پیمانهٔ $۲^۶$)

۹. (الف) ۴، ۴ (ب) $x \equiv ۳, ۱۴۷, ۴۵۳, ۵۹۷$ (به پیمانهٔ $۲^۳ \times ۳ \times ۵^۲$)

۱۰. (ب) $x \equiv ۵۱, ۷۰$ (به پیمانهٔ $۱۱^۲$)

بخش ۱۰ـ۱

۱. $\sigma(n) = ۲۱۶۰(۲^{۱۱} - ۱) \neq ۲۰۴۸(۲^{۱۱} - ۱)$

۸. ۵۶

۱۱. $p^۳$، pq

۱۴. (ب) $n = ۶$

۱۶. نه

بخش ۱۰ـ۲

۳. $۲۳۳ | M_{۲۹}$

بخش ۱۰ـ۳

۳. (ب) $۳|۲^{۲^n}+۵$

۷. $۲^{۵۸}+۱=(۲^{۲۹}-۲^{۱۵}+۱)(۲^{۲۹}+۲^{۱۵}+۱)=۵\times ۱۰۷۳۶۷۶۲۹\times ۵۳۶۹۰۳۶۸۱$

۹. (پ) $۸۳|۲^{۴۱}+۱$ و $۵۹|۲^{۲۹}+۱$

۱۰. $n=۳۱۵$، $p=۷۱$، $q=۷۳$

۱۱. $۳|۲^{۳}+۱$

بخش ۱۱ـ۱

۱. (الف) $(۱۶,۱۲,۲۰)$، $(۱۶,۶۳,۶۵)$، $(۱۶,۳۰,۳۴)$.

(ب) $(۴۰,۹,۴۱)$، $(۴۰,۳۹۹,۴۰۱)$؛ $(۶۰,۱۱,۶۱)$، $(۶۰,۹۱,۱۰۹)$، $(۶۰,۲۲۱,۲۲۹)$، $(۶۰,۸۹۹,۹۰۱)$

۸. $(۱۲,۵,۱۳)$، $(۸,۶,۱۰)$.

۱۲. (الف) $(۳,۴,۵)$، $(۲۰,۲۱,۲۹)$، $(۱۱۹,۱۲۰,۱۶۹)$، $(۶۹۶,۶۹۷,۹۸۵)$، $(۴۰۵۹,۴۰۶۰,۵۷۴۱)$

(ب) $(t_{۶},t_{۷},۳۵)$، $(t_{۴۰},t_{۴۱},۱۱۸۹)$، $(t_{۲۳۸},t_{۲۳۹},۳۰۳۹۱)$.

۱۳. $t_{۱}=۱^{۲}$، $t_{۸}=۶^{۲}$، $t_{۴۹}=۳۵^{۲}$، $t_{۲۸۸}=۲۰۴^{۲}$، $t_{۱۶۸۱}=۱۱۸۹^{۲}$

بخش ۱۲ـ۲

۱. $۱۱۳=۷^{۲}+۸^{۲}$، $۲۲۹=۲^{۲}+۱۵^{۲}$، $۳۷۳=۷^{۲}+۱۸^{۲}$.

۲. (الف) $۶۱۳=۱۷^{۲}+۱۸^{۲}$

۵. (ب) $۳۱۸۵=۵۶^{۲}+۷^{۲}$، $۳۹۶۹۰=۱۸۹^{۲}+۶۳^{۲}$، $۶۲۹۲۰=۲۴۴^{۲}+۶۶^{۲}$.

۶. $۱۱۰۵=۵\times ۱۳\times ۱۷=۹^{۲}+۳۲^{۲}=۱۲^{۲}+۳۱^{۲}=۲۳^{۲}+۲۴^{۲}$؛ توجه کنید که $۳۲۵=۵^{۲}\times ۱۳=۱^{۲}+۱۸^{۲}=۶^{۲}+۱۷^{۲}=۱۰^{۲}\times ۱۵^{۲}$

۱۴. $۴۵=۷^{۲}-۲^{۲}=۹^{۲}-۶^{۲}=۲۳^{۲}-۲۲^{۲}$

۱۸. $۱۷۲۹=۱^{۳}+۱۲^{۳}=۹^{۳}+۱۰^{۳}$

بخش ۱۲ـ۳

۳. (به پیمانهٔ $k+۱$) $\sum_{j=۰}^{k}(n+j)^{۲}\equiv\sum_{۱}^{k}j^{۲}$

۶. $۵۰۹=۱۲^{۲}+۱۳^{۲}+۱۴^{۲}$

۷. $۴۵۹ = ۱۵^۲ + ۱۵^۲ + ۳^۲$

۱۰. $۱۲۷ = ۷^۳ - ۶^۳$، $۶۱ = ۵^۳ - ۴^۳$

۱۳. $۲۳۱ = ۱۵^۲ + ۲^۲ + ۱^۲ + ۱^۲$، $۳۹۱ = ۱۵^۲ + ۹^۲ + ۹^۲ + ۲^۲$

$۲۱۰۹ = ۴۴^۲ + ۱۲^۲ + ۵^۲ + ۲^۲$

۱۷. $t_{۱۳} = ۳^۳ + ۴^۳ = ۶^۳ - ۵^۳$

۱۸.

$$
\begin{aligned}
۲۹۰ &= ۱۳^۲ + ۱۱^۲ = ۱۶^۲ + ۵^۲ + ۳^۲ = ۱۴^۲ + ۹^۲ + ۳^۲ + ۲^۲ \\
&= ۱۵^۲ + ۶^۲ + ۴^۲ + ۳^۲ + ۲^۲
\end{aligned}
$$

بخش ۱۳ـ۱

۷. ۲، ۵، ۱۴۴.

۸. $u_۱$، $u_۲$، $u_۳$، $u_۴$، $u_۶$، $u_{۱۲}$.

۱۱. $u_{۱۱} = ۲u_۹ + u_۸$، $u_{۱۲} = ۶u_۸ + (u_۸ - u_۴)$.

۱۲. $u_۱$، $u_۲$، $u_۴$، $u_۸$، $u_{۱۰}$.

بخش ۱۳ـ۲

۷. $۵۰ = u_۴ + u_۷ + u_۹$، $۷۵ = u_۳ + u_۵ + u_۷ + u_{۱۰}$، $۱۰۰ = u_۱ + u_۳ + u_۶ + u_{۱۱}$، $۱۲۰ = u_۳ + u_۹ + u_{۱۱}$.

۹. $(۳, ۴, ۵)$، $(۵, ۱۲, ۱۳)$، $(۸, ۱۵, ۱۷)$، $(۳۹, ۸۰, ۸۹)$، $(۱۰۵, ۲۰۸, ۲۳۳)$.

بخش ۱۳ـ۳

۱. (الف) $[-۱; ۱, ۱, ۱, ۲, ۶]$. (ب) $[۳; ۳, ۱, ۱, ۳, ۲]$.

(پ) $[۱; ۳, ۲, ۳, ۲]$. (ت) $[۰; ۲, ۱, ۱, ۳, ۵, ۳]$.

۲. (الف) $\frac{-۷۱۰}{۴۵۷}$. (ب) $\frac{۷۴۱}{۱۷۰}$. (پ) $\frac{۳۲۱}{۴۶۰}$.

۴. (الف) $[۰; ۳, ۱, ۲, ۲, ۱]$. (ب) $[-۱; ۲, ۱, ۷]$. (پ) $[۲; ۳, ۱, ۲, ۱, ۲]$.

۵. (الف) ۱، $\frac{۳}{۲}$، $\frac{۱۰}{۷}$، $\frac{۳۳}{۲۳}$، $\frac{۷۶}{۵۳}$، $\frac{۱۰۹}{۷۶}$.

(ب) -۳، -۲، $-\frac{۵}{۲}$، $-\frac{۷}{۳}$، $-\frac{۱۲}{۵}$، $-\frac{۴۳}{۱۸}$.

(پ) ۰، $\frac{۱}{۲}$، $\frac{۴}{۹}$، $\frac{۵}{۱۱}$، $\frac{۴۴}{۹۷}$، $\frac{۹۳}{۲۰۵}$.

۶. (ب) $۲۲۵ = ۴ \times ۴۳ + ۴ \times ۱۰ + ۳ \times ۳ + ۲ \times ۱ + ۲$

۷. (الف) ۱، $\frac{۳}{۲}$، $\frac{۷}{۵}$، $\frac{۱۷}{۱۲}$، $\frac{۴۱}{۲۹}$، $\frac{۹۹}{۷۰}$، $\frac{۲۳۹}{۱۶۹}$، $\frac{۵۷۷}{۴۰۸}$، $\frac{۱۳۹۳}{۹۸۵}$.

(ب) ۱، ۲، $\frac{۵}{۳}$، $\frac{۷}{۴}$، $\frac{۱۹}{۱۱}$، $\frac{۲۶}{۱۵}$، $\frac{۷۱}{۴۱}$، $\frac{۹۷}{۵۶}$، $\frac{۲۶۵}{۱۵۳}$.

(پ) ۲، $\frac{۹}{۴}$، $\frac{۳۸}{۱۷}$، $\frac{۱۶۱}{۷۲}$، $\frac{۶۸۲}{۳۰۵}$، $\frac{۲۸۸۹}{۱۲۵۲}$، $\frac{۱۲۲۳۸}{۵۴۷۳}$، $\frac{۵۱۸۴۱}{۲۳۱۸۴}$، $\frac{۲۱۹۶۰۲}{۹۸۲۰۹}$.

(ت) ۲، $\frac{۵}{۲}$، $\frac{۲۲}{۹}$، $\frac{۴۹}{۲۰}$، $\frac{۲۱۸}{۸۹}$، $\frac{۴۸۵}{۱۹۸}$، $\frac{۲۱۵۸}{۸۸۱}$، $\frac{۴۸۰۱}{۱۹۶۰}$، $\frac{۲۱۶۳۲}{۸۷۲۱}$.

(ث) ۲، ۳، $\frac{۵}{۲}$، $\frac{۸}{۳}$، $\frac{۳۷}{۱۴}$، $\frac{۴۵}{۱۷}$، $\frac{۸۲}{۳۱}$، $\frac{۱۲۷}{۴۸}$، $\frac{۵۹۰}{۲۲۳}$

۹. $[۳; ۷, ۱۵, ۱, ۲۶]$, $[۳; ۷, ۱۶, ۱۱]$

۱۱. (الف) $x = -۸ + ۵۱t$، $y = ۳ - ۱۹t$

(ب) $x = ۵۸ + ۲۲۷t$، $y = -۹۳ - ۳۶۴t$

(پ) $x = ۴۸ + ۵t$، $y = -۱۶۸ - ۱۸t$

(ت) $x = -۲۲ - ۵۷t$، $y = -۶۱ - ۱۵۸t$

بخش ۱۳ـ۴

۱. (الف) $\frac{۳+\sqrt{۱۵}}{۳}$ (ب) $\frac{-۴+\sqrt{۳۷}}{۳}$ (پ) $\frac{۵+\sqrt{۱۰}}{۳}$ (ت) $\frac{۱۹-\sqrt{۲۱}}{۱۰}$ (ث) $\frac{۳۱۴-\sqrt{۳۷}}{۲۳۳}$.

۲. $\frac{\sqrt{۵}-۱}{۲}$

۳. $\frac{۵-\sqrt{۵}}{۲}$، $\frac{۸۷+\sqrt{۵}}{۶۲}$

۴. (الف) $[۲; \overline{۴}]$. (ب) $[۲; \overline{۱, ۱, ۱, ۴}]$. (پ) $[۲; \overline{۳}]$. (ت) $[۲; \overline{۱, ۳}]$. (ث) $[۱; ۳, \overline{۱, ۲, ۱, ۴}]$

۵. (ب) $[۱; \overline{۲}]$، $[۱; \overline{۱, ۲}]$، $[۳; \overline{۱, ۶}]$، $[۶; \overline{۱۲}]$.

۶. $\frac{۱۶۷۷}{۴۳۳}$

۷. (الف) $\frac{۱۲۶۴}{۴۶۵}$

۹. (الف) $\frac{۳۴}{۲۷}$ (ب) $\frac{۳۰۱}{۲۳۹}$.

۱۱. ۳، $\frac{۳۵۵}{۱۱۳}$.

بخش ۱۳ـ۵

۲. (الف) $x = ۸$، $y = ۳$. (ب) $x = ۱۰$، $y = ۳$ (پ) $x = ۱۷$، $y = ۴$

(ت) $x = ۱۱$، $y = ۲$ (ث) $x = ۲۵$، $y = ۴$.

۳. (الف) $x = ۳$، $y = ۲$؛ $x = ۱۷$، $y = ۱۲$؛ $x = ۹۹$، $y = ۷۰$.

(ب) $x = ۲$، $y = ۱$؛ $x = ۷$، $y = ۴$؛ $x = ۲۶$، $y = ۱۵$؛ $x = ۹۷$، $y = ۵۶$؛

$x = ۳۶۲$، $y = ۲۰۹$.

(پ) $x = ۹$، $y = ۴$؛ $x = ۱۶۱$، $y = ۷۲$.

۴. ۴۸، ۱۶۸۰.

۵. (الف) $x = ۲۴$، $y = ۵$؛ $x = ۱۱۵۱$، $y = ۲۴۰$.

(ب) $x = ۵۱$، $y = ۱۰$؛ $x = ۵۲۰۱$، $y = ۱۰۲۰$.

(پ) $x = ۲۳$، $y = ۴$؛ $x = ۱۰۵۷$، $y = ۱۸۴$.

۶. (الف) $x = ۹۸۰۱$، $y = ۱۸۲۰$ (ب) $x = ۲۰۴۹$، $y = ۳۲۰$

(پ) $x = ۳۶۹۹$، $y = ۴۳۰$.

۷. (الف) $x = ۱۸$، $y = ۵$ (ب) $x = ۷۰$، $y = ۱۳$ (پ) $x = ۳۲$، $y = ۵$.

۱۲. $x = ۴۴۹$، $y = ۶۰$؛ $x = ۱۳۴۵۵$، $y = ۱۷۹۸$.

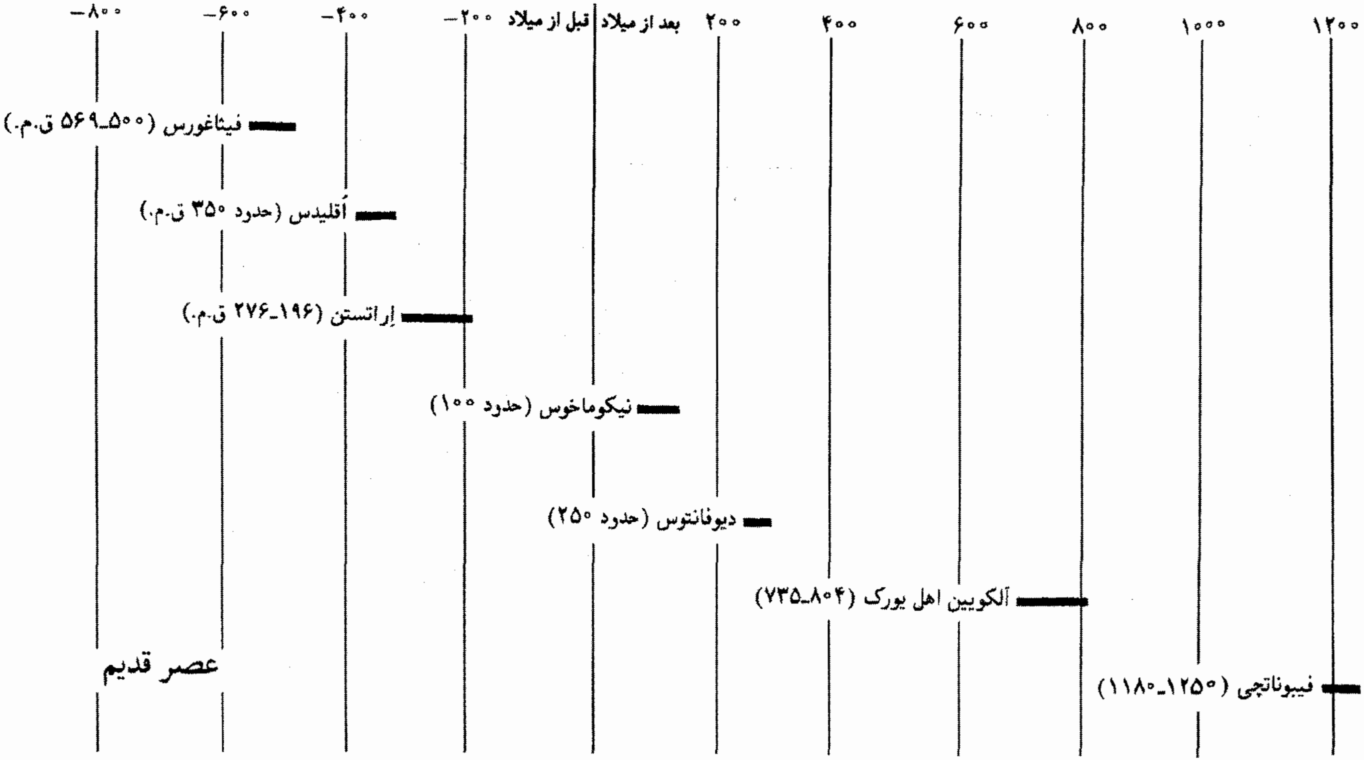
۱۳. (ب) $x = ۲۵۴$، $y = ۹۶$؛ $x = ۴۰۴۸$، $y = ۱۵۳۰$.

(پ) $x = ۲۱۳$، $y = ۳۶$؛ $x = ۲۵۳۸$، $y = ۴۲۹$.

نمایه

فهرست نمادها

دانشمندان برجستهٔ نظریهٔ اعداد در طول تاریخ



دانشمندان برجستهٔ نظریهٔ اعداد در طول تاریخ