وزارت علوم، تحقیقات و فناوری

مرکز نشر دانشگاهی

آشنایی با نظریهٔ اعداد

ویلیام دبلیو. آدامز، لری جوئل گولدشتین

ترجمهٔ آدینه محمد نارنجانی

آشنایی با نظریهٔ اعداد

ویلیام دبلیو. آدامز، لری جوئل گولدشتین

ترجمهٔ آدینه محمد نارنجانی

مرکز نشر دانشگاهی

فهرست

بسم الله الرحمن الرحیم

مقدمهٔ مترجم

تئوری مقدماتی اعداد بایدیکی ازمهمترین موضوعها برای‌تعلیم اولیه‌ی ریاضیات باشد. چندان اطلاع قبلی نمی‌خواهد ، موضوعش ملموس و مانوس است ، طریقه‌های‌استدلال‌که به‌کارمی‌گیرد ساده،کلی وتعدادشان کم است ، و از لحاظ تحریك کنجکاوی طبیعی آدمی در علوم ریاضی مانند ندارد. یك ماه تعلیم فهیمانه در تئوری اعداد دوبار آموزنده‌تر ، دوبار مفیدتر ، وحداقل ده‌بار سرگرم‌کننده‌تر ازهمان مدت تعلیم «حسابان برای مهندسین» میباشد.

هاردی[1]

کتابی که هم‌اکنون پیش روی شماست ، ترجمهٔ شش فصل اول از کتاب آشنایی با نظریهٔ‌اعداد تألیف و . و . آدامز و ل . ج . گولدشتین است. مواد این کتاب هم‌اکنون در بسیاری ازکشورها دردورهٔ‌کارشناسی ریاضی (لیسانس) تدریس می‌شود. علت اینکه ترجمهٔ این‌فصول جداگانه چاپ‌شده ، این‌است‌که این‌کتاب شامل دوقسمت‌کاملا مجزاست. قسمت اول ، نظریهٔ مقدماتی اعداد است که ترجمهٔ‌آن ازنظرتان می‌گذرد و قسمت دوم آن آشنایی با نظریهٔ جبری اعداد است‌که امید است آن نیز آمادهٔ چاپ‌گردد.

در ترجمهٔ این‌کتاب ، بنا به پیشنهادگروه ریاضی مرکز نشر دانشگاهی ، سعی شده که از اصطلاحات مورد قبول انجمن‌ریاضی استفاده‌شود ولی هروقت‌که اصطلاحی درآنجا یافت نشده ازکتاب با ارزش تئوری مقدماتی اعداد ، تألیف مرحوم غلامحسین مصاحب استفاده شده است .

---

۱ ــ غلامحسین مصاحب ، تئوری مقدماتی اعداد ، جلد اول ، (تهران،۱۳۵۵) صفحهٔ۲۰مقدمه

از دست اندرکاران مرکز نشر دانشگاهی، بویژه آقای دکتر نصرالله پورجوادی سرپرست این مرکز و آقای دکتر علی‌اکبر جعفریان سرپرست گروه ریاضی سپاسگزاری دارد. ازآقای دکتر محمدهادی شفیعیها که تلاش‌زیاد ایشان، هنگام ویرایش، سهم به‌سزایی در برطرف کردن‌نارسائیهای ترجمه داشته، نهایت تشکر حاصل است. ازکارکنان بخش تصحیح و تولید مرکز نشر دانشگاهی‌ونیز ازکارگران‌چاپخانهٔ مجتمع‌دانشگاهی‌ادبیات‌وعلوم انسانی که‌حروفچینی این‌کتاب را انجام داده‌اند صمیمانه تشکر می‌کنم. در خاتمه، از خوانندگان تقاضا دارد هرجا به غلطی برخورد می‌کنند منتی برمترجم گذاشته آن را یادآوری فرمایند.

آدینه محمد نارنجانی
گروه ریاضی ــ دانشگاه تربیت معلم
تیر ماه ۱۳۶۲

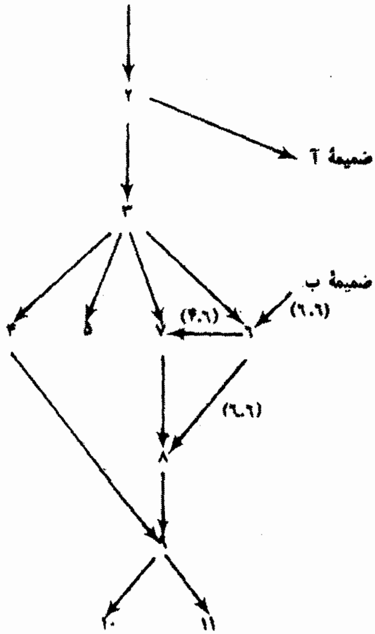
پیشگفتار مؤلفان

کتاب حاضر مقدمه‌ای است بر نظریهٔ اعداد که بیشتر بر نظریهٔ معادلات سیاله مبتنی می‌باشد. این کتاب، قبل‌ازهمه، به‌عنوان متنی برای درس استانده‌ای در نظریهٔ مقدماتی اعداد برای دانشجویان رشته‌های ریاضی وآموزش ریاضی تهیه‌شده است. بنابراین کوشیده‌ایم که درمراحل اولیهٔ این کتاب با گامهای آهسته پیش برویم، ومقدار نسبتاً زیادی بیشتر ازکتابهای معمول دراین سطح ، درباره نظریهٔ اعداد، ساختار و اهدافش «گفتگو» نموده‌ایم. سعی کرده‌ایم آن قسمت ازکتاب راکه مربوط به‌اولین درس یك ترمی درنظریهٔ اعداد است، تاآنجاکه ممکن است برای طیف بیشتری از دانشجویان، قابل استفاده سازیم، بی‌آنکه محتوای آن‌را پایین بیاوریم. برای‌این‌منظور، مثلا به‌مقدار زیادی ازمحاسبات عددی تن‌درداده‌ایم، وغالبأمتکی به‌هیچ‌اطلاعات قبلی غیراز جبردبیرستان نشده‌ایم. نظریهٔ معادلات سیاله موضوعی است عمومی که می‌توانیم مباحث خود را پیرامون‌آن تنظیم‌کنیم؛ این امرموجب می‌شود (امیدواریم) که‌نظریهٔ اعداد، به‌جای‌اینکه مجموعهٔ‌پراکنده‌ای ازموضوعات گوناگون جلوه کند، نظام سازمان یافته‌ای به‌نظر آیدکه اهدافی درپیش داردکه یکی ازآنها مطالعهٔ معادلات سیاله است.

فصول ۱ـ۶، همان‌گونه‌که ازجدول بستگی‌منطقی‌صفحهٔ‌بعدپیداست، درتنظیم‌یك درس یك‌ترمی درنظریهٔ اعداد تاحد زیادی‌آزادی عمل به‌ما می‌دهد.

درفصول ۷ تا ۱۱ مقدمه‌ای برنظریهٔ جبری اعداد، از راه‌مطالعهٔ معادلات سیالهٔ درجهٔ دوم، آورده می‌شودکه به‌مطالعهٔ میدانهای درجهٔ دوم‌منجر می‌شود. از ابتدای فصل هشتم، کتاب دریك‌سطح بالاتری‌نوشته شده است، وهمچنین اولین درس جبرمجرد در دورهٔ‌لیسانس ازپیش دانسته فرض می‌شود. درفصل هشتم، آلگوریتمی جهت حل معادلات سیالهٔ‌درجهٔ دوم به‌صورت $ax^2+bxy+cy^2=n$ ، نشان می‌دهیم. فصول هفتم و هشتم مقدمهٔ مختصری

است درباب میدانهای درجهٔ دوم. درفصل نهم، حساب مدولها دریك میدان عددی درجهٔ دوم را، ازبعضی جهات، گسترش می‌دهیم. وقضیهٔ یکتایی تجزیه به‌عوامل رابرای مدولها ثابت می‌کنیم. از فصل۹ به‌بعد، متعلم می‌تواند به‌یکی از فصول ۱۰ یا ۱۱ بپردازد. فصل ۱۰ به مطالعهٔ معادلات‌سیالهٔ مختلف، یعنی معادلهٔ باشه $y^2=x^3+k$، آخرین قضیهٔ فرما به‌ازای $n=3$، ومعادلاتی به‌صورت نرمال‌تخصیص داده‌شده است. فصل۱۱ به‌مطالعهٔ نمایش‌اعداد صحیح، به‌توسط صورتهای دوتایی درجهٔ دوم، اختصاص داده شده است.



بیش‌از هزار مسئله دراین کتاب گنجانیده‌ایم. ما براین عقیده‌ایم که نظریهٔ اعداد، هنگامی که با حادثه‌جویی ویافتن چیزهای تازه به‌آن نزدیك می‌شویم، بی‌اندازه سرگرم‌کننده است. ازاین‌رو، مسائل ما متضمن محاسبات عددی ساده، آزمایشهایی که به‌منظور هدایت دانشجو برای بازیابی حدسهای خود طرح شده‌اند، مسائلی که به نظریهٔ متن وسعت می‌بخشد ومسائلی که دانشجو را به‌مبارزه می‌طلبد. ما این نوع اخیر از مسائل را با ستاره مشخص کرده‌ایم.

ما دراین کتاب روش زیر را درمورد شماره‌گذاری به‌کار می‌بریم. هنگام ارجاع به‌بخشهایی غیرازآن بخش‌کتاب که مطالعه می‌کنید به‌طریق زیرعمل می‌کنیم: برای ارجاع به‌بخشهای دیگرفصل موردمطالعه، ازعدد یك‌رقمی‌استفاده خواهیم‌کرد. برای مثال، بخش۳، ارجاع به‌بخش۳ ازهمان فصل است. ازطرف دیگر، بخش۳.۱۱ ارجاع به‌بخش۳ ازفصل

۱۱ است. هنگام ارجاع به‌بندها (پاراگرافها)ی داخل بخشها، اعداد یك رقمی ارجاع به بندهای همان بخش‌است. بنابراین، به‌عنوان مثال، منظور از لم ۲ اشاره به لم ۲ی همان بخش است. اما لم ۲.۳ اشاره به لم ۲ از بخش سوم فصل مورد مطالعه است. اعـداد ۳رقمی را تنها زمانی به کار خواهیم برد که به‌ارجاع خـارج از فصل مورد مطالعه نیازباشد. درایـن حالت منظور از لم ۲.۳.۸ ارجاع به لم ۲ از بخش ۳ از فصل۸ می باشد. کلیهٔ لگاریتمها دراین کتاب لگاریتم طبیعی فرض‌شده وبانماد log نمایش داده می‌شوند.

مؤلفین‌میل‌دارندازبسیاری‌ازهمکاران‌خودکه گفتگوها وپیشنهادهایشان در بهبوداین کتاب مؤثر بوده‌است تشکر کنند. از دکتر آدام کلیپنر[1] ودکتر جیمز شیفر[2] به‌خاطر آزمایش‌دستنوشته‌ها درسر کلاس و از دکتر تـوماس‌آپوستول[3] . دکتر بـروس برنت[4] و دکتر رالف گرینبرگ[5] به‌خاطر خواندن دستنوشته‌ها و دادن پیشنهادهای زیاد و مؤثرشان تشکر مـی کنیم. تشکرات خاص‌خودرا به دکتر اتان‌بولکر[6] و دکتر امیل گراسوالد[7] تقدیم می‌داریم که مطالعه وانتقاد قاطع وبی‌امانشان از دستنوشته، مافوق وظیفه یادوستی‌آنان بوده است. ماشین‌نویسهای ما، دبی کوران[8] و پولا وردان[9] کار خود را درمورد ماشین‌کـردن دستنوشته، واقعاً عـالی انجام داده‌اند. وازبخش ریاضی‌دانشگاه مری‌لند[10] به‌خاطر دراختیار گذاشتن‌امکانات ماشین‌نویسی تشکرمی کنیم. از الیزابت آدامز[11] به‌خاطر صبر و حوصله‌ای که درخواندن براهین از خود نشان داده‌اند بسیار ممنونیم. بالاخـره مـی‌خواهیم مراتب قدردانی خـود را از کارمندان پرنتیس‌ـهال[12] ، خصوصاً پنی‌لینسکی[13] ، که بااستفاده از حرفه خـود درپدید آوردن این کتاب، مارا مورد حمایت خود قرار داده‌اند، ابراز داریم.

کالج پارك، مری‌لند

ویلیام دبلیو. آدامز
لری‌جوئل گولدشتین

---

1. Adam Kleppner 2. James Schafer 3. Thomas Apostol
4. Bruce Berndt 5. Ralph Greendberg 6. Ethan Bolker
7. Emil Grosswald 8. Debbie Curran 9. Paula Verdun
10. Maryland 11. Elizabeth Adams 12. Prentice-Hall
13. Penny Linskey

۱

مقدمه

۱.۱ نظریهٔ اعداد چیست؟

نظریهٔ اعداد امروزه آنچنان موضوع وسیعی است که بسهولت نمی‌توان گفت که کدامیك از شاخه‌های ریاضی بدان متعلق است و کدامیك بدان تعلق ندارد. بهرحال، اجازه دهید که باساده انگاری بیش‌ازحد، بگوییم نظریهٔ اعداد شاخه‌ای از ریاضیات است که با مطالعهٔ خواص اعداد صحیح

...، ۴، ۳، ۲، ۱، ۰، ۱—، ۲—، ۳—، ۴—، ...

سروکار دارد.

اعداد صحیح (یا حداقل اعداد صحیح مثبت) وقواعد حساب مربوط به‌آنها در زمرهٔ قدیمیترین وبنیادی‌ترین فرآورده‌ها درفرآیند تفکر بشر است. تمدنهای باستانی، یکی‌پس‌از دیگری، به‌ضرورت شمردن‌ــ برای دادوستد، برای تعیین وقت، برای گاه‌شماری، برای اندازه‌گیری طول وسطح وبرای‌بنای ساختمانهاــ پی‌بردند. ازاین‌نیاز به‌شمردن‌بود که‌مفهوم عدد وقواعد اساسی حساب پا به‌عرصهٔ وجودگذاشتند. بیش‌از پنجهزارسال قبل، مصریان و چینیان منظماً حساب را در زندگی‌روزانه مورد استفاده قرار می‌دادند.

درمحاسبه با اعداد صحیح، نمی‌شود به‌الگوها وخواص فراوانی که آنها ازخودنشان می‌دهند توجهی نکرد و حس کنجکاوی، انسان‌را به‌این وا می‌دارد که حیرت زده از خود بپرسد این الگوهایی که ملاحظه می‌شود برای اولین هزار (اولین‌میلیون) عددصحیح صدق می‌کنند، آیا به‌مثابهٔ الگوهای کلی، برای همهٔ اعدادصحیح پابرجا هستند؟ چنین‌سؤالاتی به حیطهٔ نظریهٔ اعداد متعلق است. این پرسشها قبلا توسط مصریان وچینیان دوران‌باستان مطرح

شده بودند. مع‌هذا، درمیان تمدنهای کهن، برای نخستین بار یونانیان، بویژه فیثاغورسیان بودندکه تکان اولیه‌را به نظریهٔ جدید اعداد دادند.

برای اینکه تصور دقیقتری ازنوع مسائلی که توسط صاحبنظران درنظریهٔ اعداد مورد مطالعه قرارمی گرفتند وهمچنین تصوری از روش این کتاب برای‌پرداختن به‌موضوع به‌دست آوریم، اجازه بدهید بعضی‌از مسائلی‌راکه یونانیان عهد باستان موردتوجه قرار می‌دادند دراینجا مطرح کنیم.

مسئلهٔ ۱ : کلیهٔ مثلثهای قائم‌الزاویه‌ای را بیابید که طول‌اضلاع آنها اعدادصحیح باشند.

اگراندازه‌های اضلاع چنین مثلثی‌را x ، y و z ، که z وترآن است بگیریم، آنگاه قضیهٔ فیثاغورس ایجاب می کندکه داشته‌باشیم

$$x^۲+y^۲=z^۲. \tag{۱}$$

بنابراین، می بینیم که مسئلهٔ ۱ معادل است باتعیین همهٔ سه‌تاییهای صحیح $(x ، y ، z)$ که در معادلهٔ (۱) صدق کنند. این‌گونه سه‌تاییها را سه‌تاییهای فیثاغورسی نامند. به‌عنوان مثال، (۳ ، ۴ ، ۵)و(۱۳ ، ۱۲ ، ۵) دوسه‌تایی فیثاغورسی هستند. بعلاوه، اگر a ، b ، c سه‌عدد صحیح دلخواه باشند واگر

$$x=\pm(a^۲-b^۲)c \quad ، \quad y=\pm ۲abc \quad ، \quad z=\pm(a^۲+b^۲)c$$

آنگاه $(x ، y ، z)$ یك سه‌تایی فیثاغورسی است . (عملیات را انجام دهید.) بعلاوه ، دیوفانتوس ریاضیدان یونانی ثابت‌کردکه به‌ازای مقادیرمناسبی از a ، b ، c هرسه‌تایی فیثاغورسی به‌صورت فوق است.

مسئلهٔ ۲ : نشان دهیدکه $\sqrt{۲}$ را نمی‌توان به‌صورت‌نسبت‌دوعدد صحیح نوشت (یعنی، $\sqrt{۲}$ عددی‌گنگ است).

حل مسئلهٔ ۲ یکی ازدقیقترین‌کارهایی است‌که ریاضیات یونان انجام داده است. حل آن‌چنین است: اگر $\frac{x}{y}=\sqrt{۲}$، که x ، y اعداد صحیح هستند، دراین‌صورت $\frac{x^۲}{y^۲}=۲$ یا

$$x^۲-۲y^۲=۰. \tag{۲}$$

می‌توانیم فرض کنیم کـه کسر x/y ساده شده است، به‌طوری‌کـه x، y هـردو همزمان زوج‌نباشند، اماچون $x^۲=۲y^۲$، x بایستی‌زوج‌باشد، مثلا. $x=۲t$. بنابراین، $۲y^۲=۴t^۲$ و $y^۲=۲t^۲$ ، پس y هم‌زوج است و این مغایر بااین فرض است‌که x و y همزمان زوج نیستند.

مسئلهٔ ۳: فرض کنیم a ، b ، c سه‌عددصحیح مفروض باشند. کلیهٔ اعدادصحیح x ، y را که درمعادلهٔ $ax+by=c$ صدق‌می‌کنند بیابید.

حل‌کامل مسئلهٔ۳ را درفصل ۲ خواهیم دید. برای اینکه ظرافت مسئله را دریابیم، دو مثال خاص راموردمطالعه قرار می‌دهیم. به‌عنوان‌اولین‌مثال، معادلهٔ زیررا درنظر می‌گیریم

$$۲x+۳y=۵. \qquad (۳)$$

به‌ازای هرمقدار x مقداری برای y ، جهت برقراری معادله، به‌دست می‌آید. به‌عبارت دیگر $y=(۵-۲x)/۳$. به‌هرحال، اگر x را عددی صحیح فرض کنیم لزومی نداردکه $y=(۵-۲x)/۳$ صحیح‌باشد. برای‌مثال، اگر $x=۲$، آنگاه $y=۱/۳$. از این‌رو، بیان راه‌حلهایی که x و y صحیح را بهما بدهند تاحدی نیاز به‌دقت دارد. مع‌هذا، یك استدلال مقدماتی‌ما را قادرمی‌سازدکه‌تمامی‌آنهارا بیان‌کنیم، زیرا اگراعداد صحیح x ، y درمعادلهٔ $۲x+۳y=۵$ صدق‌کنند، باید $۲x=۵-۳y$ عددی زوج‌باشدودراین‌صورت y بایستی فرد باشد. (درغیراین‌صورت $۳y$ زوج و $۵-۳y$ فرد خواهد شد.) فرض‌کنیم به‌ازای عدد صحیح t ، $y=۲t+۱$. دراین‌صورت

$$x=\frac{۱}{۲}(۵-۳y)=۱-۳t ،$$

بنابراین، هرجواب‌صحیح معادلهٔ(۳) به‌صورت زیراست

$$x=۱-۳t ، \qquad y=۲t+۱ ، \qquad t \text{ عددصحیح} . \qquad (۴)$$

بالعکس، اگر t عددی صحیح باشد و x ، y درمعادلات(۴) صدق‌کنند داریم

$$۲x+۳y=۲(۱-۳t)+۳(۲t+۱)=۵ .$$

بنابراین، $(x ، y)$ جوابی برای معادلهٔ (۳) است. پس، هرجواب‌صحیح معادلهٔ (۳) از روابط (۴) حاصل می‌شود. برای مثال، $t=۰ ، ۱ ، -۳$ متناظر با جوابهای $(x ، y)=(۱ ، ۱)$، $(-۲ ، ۳)$ ، $(۱۰ ، -۵)$ برای معادلهٔ (۳) خواهد بود.

به‌عنوان دومین مثال خاص از مسئلهٔ ۳ ، معادلهٔ $۳x+۶y=۷$ را درنظر می‌گیریم، این معادله هیچ جواب صحیح $(x ، y)$ ندارد، چون اگر x و y اعداد صحیحی باشند، $۳x+۶y=۳(x+۲y)$ عدد صحیحی است‌که بر ۳ بخشپذیر می‌باشد. اما ۷ بر ۳ بخشپذیرنیست. بنابراین $۳x+۶y=۷$ دارای جواب‌صحیح نیست.

توجه‌کنیدکه، گرچه علی‌الظاهر، مسائل ۱ــ۳ هیچ‌ارتباطی بایکدیگر ندارند، تمام آنها به تعیین همهٔ جوابهای صحیح معادلاتی مانند $x^۲+y^۲=z^۲$ ، $x^۲-۲y^۲=۰$ ، $۲x+۳y=۵$ و $۳x+۶y=۷$ ویا اثبات عدم وجود جواب‌منجر می‌شوند. مسئلهٔ کلی تعیین جوابهای صحیح معادلات، یکی ازموضوعات‌اصلی نظریهٔ اعداداست. درحقیقت، عدهٔ زیادی ازمسائل نظریهٔ اعداد را می‌توان به‌مثابهٔ مسائلی انگاشت که‌درآنها جوابهای‌صحیح معادلات‌موردنظرند. آنچه که‌نظریهٔ اعداد را جالب می‌سازد و بدان کیفیت وخصوصیت‌خاصی

می‌بخشد آن‌است که چنین مسائلی ظریف‌تر از تعیین کلیه‌جوابهای یک‌معادله هستند. درحقیقت همان‌طورکه قبلا نشان دادیم معادلهٔ $x^{2}-2y^{2}=0$ در حوزهٔ اعداد صحیح ناصفر دارای جواب نیست. باوجود این، این معادله جوابهای زیادی (مثل $y=1$ ، $x=\sqrt{2}$) دارد. همچنین به‌ازای هرمقدارکه به x و y داده شده باشد، یک‌جواب معادلهٔ $x^{2}+y^{2}=z^{2}$ را می‌توان از تساوی $z=\pm\sqrt{x^{2}+y^{2}}$ تعیین کرد. به‌هرحال، تعیین‌جوابهای‌صحیح (x,y,z) مستلزم بیان‌کاملا پیچیده‌ای است، خصوصاً وقتی‌که باسادگی معادله اصلی‌مقایسه شود.

تمام معادلاتی راکه دربالا مطالعه‌کردیم مثالهایی از معادلات سیاله هستند. بـه‌بیان دقیقتر، معادلهٔ سیاله، یک معادلهٔ بسجمله‌ای[1] است (برحسب هرتعدادی از مجهولات) کـه مقصود ما تعیین جوابهای صحیح‌آن است. چنین معادلاتی به‌نام ریاضیدان یونانی‌دیوفانتوس اسکندرانی[2] ، که اولین بار آنهارا مورد مطالعهٔ اصولی‌قرارداد، معادلات دیوفانتوسی نام‌گذاری شده‌اند. ولی‌ما، برای سهولت بیان، همه‌جا آنهارا معادلات سیاله نـامیده‌ایم. از زمانهای قدیم، معادلات سیاله‌یکی‌از موضوعات‌کانونی درتحقیقات نظریهٔ اعداد بوده است. درحقیقت، مقدار زیادی از دانش ما درمورد اعداد صحیح از تلاش درحل معادلات سیالـه ناشی شده است. بنابراین، موضوع اصلی این‌کتاب را به‌معادلات سیاله تخصیص داده‌ایم.

دراین‌کتاب، ماخواص گوناگون‌اعدادصحیح راپیداخواهیم‌کرد. اماکراراً به‌معادلات سیاله برخواهیم‌گشت تانشان دهیم‌که چگونه اطلاعاتی راکه از اعدادصحیح کسب‌کرده‌ایم می‌توانیم در عمل به‌کار بریم. اگرچه مطمئناً غیرممکن است‌که همهٔ نظریهٔ اعـداد را بتوان به‌کمک معادلات سیاله موردبحث قرارداد ولی اصول(روش عملی) لازم برای‌حل حتی‌دستهٔ محدودی از معادلات سیاله دامنهٔ پهناوری از روشهای نظریهٔ اعدادی را آشکار می‌سازند و ازاین‌رو، زمینهٔ مساعدی جهت مطالعهٔ نظریهٔ اعداد فراهم می‌آورند.

این‌کتاب را می‌توان به‌دوقسمت تقسیم کرد. فصول ۱ـ۷ فقط نیازمند آن حـداقل پیشنیازی است‌که مختصراً دربخش ۱.۲ شرح داده شده است و شامل‌چیزی است‌که معمولا نظریهٔ مقدماتی اعداد نامیده‌می‌شود. درفصول ۸ـ۱۱، سطح پیشرفته‌تری ازموضوعات‌درحد درس مقدماتی جبرمجرد دانسته فرض شده است. محتوای نیمهٔ دوم‌کتاب شامل مقدمه‌ای بر نظریهٔ جبری اعداد درحالت خاص میدانهای درجهٔ دوم می‌باشد. هدف ما استفاده ازمفاهیم جبری برای روشن ساختن نظریهٔ معادلات سیالهٔ درجهٔ دوم به‌صورت

$$ax^{2}+bxy+cy^{2}=m$$

است. از سده‌های پیش، نظریهٔ این‌گونه معادلات زمینه‌ای آزمایشی برای بسیاری از مفاهیم جدید نظریهٔ اعداد توسط بـزرگترین صاحبنظران نظریهٔ اعداد، ازجمله فرما[3] ، لژاندر[4] ،

---

۱. دانشمندان نظریهٔ اعداد اغلب حـالات کلیتر معادلات سیاله را درنظر می‌گیرند. به‌عنوان مثال $2^{x}+y^{2}=3$ ، اما ما دراین‌کتاب خودرا به‌معادلات بسجمله‌ای محدود می‌کنیم

2. Diophantus of Alexandria

3. Fermat 4. Legendre

لاگرانژ[۱] ، گاوس[۲] ، و دیریکله[۳] بوده است. هنوز هم مسائل متعدد حل نشده‌ای در این مورد باقی مانده‌اند ، و بنابراین موضوع مهیجی برای بحث در درسی از نظریهٔ اعداد درسطح لیسانس خواهند بود.

به‌عنوان مثالهای بیشتر از معادلات جالب سیاله دومثال می‌آوریم که توسط پیر فرما حقوقدان و ریاضیدان آماتور فرانسوی درقرن هفدهم مورد مطالعه قرار گرفتند.

مسئلهٔ ۴ : مطلوب است تعیین کلیهٔ اعداد صحیح مثبت a که به‌صورت مجموع دومربع کامل بیان می‌شوند . به عبارت دیگر، به ازای چه مقادیر a معادلهٔ سیالهٔ $a = x^{2} + y^{2}$ برحسب اعدادصحیح x ، y قابل حل می‌باشد.

ما درفصل ۶ به‌حل کامل مسئلهٔ ۴ خواهیم پرداخت. ولی فعلا خودرا فقط به‌حالتی که a عدد اول است، یعنی حالتی که a عواملی غیراز ۱ $\pm$ و $a\pm$ ندارد، محدود می‌کنیم. دراین‌حالت خاص، فرما ثابت کردکه فقط زمانی می‌توان معادلهٔ $a = x^{2} + y^{2}$ را درحوزهٔ اعداد صحیح حل کردکه $a-1$ بر ۴ بخشپذیر ویا a برابر ۲ باشد. بدین‌ترتیب، مثلا $x^{2} + y^{2} = ۷$ دارای جواب صحیح نیست (۶ = ۱ − ۷ بر ۴ بخشپذیر نیست) ، و حال آنکه $x^{2} + y^{2} = ۱۳$ درحوزهٔ اعداد صحیح دارای جواب است (۱۲ = ۱ − ۱۳ بر ۴ بخشپذیر است) . آموزنده خواهد بود اگر شما نتیجهٔ فرما را درمورد اولین ۲۰ مثال یا بیشتر آزمایش کنید.

فرما یك معادلهٔ سیالهٔ حل نشده (تاامروز) ازخود به‌جا گذاشته بودکه به‌آخرین‌قضیهٔ فرما شهرت یافته است. فرما قسمت اعظم آنچه راکه از نظریهٔ اعداد می‌دانست با خواندن ترجمهٔ لاتین کارهای دیوفانتوس فراگرفت. دریك‌بند کتاب، دیوفانتوس ازمعادلات‌فیثاغورسی (مسئلهٔ ۱) صحبت کرده است. فرما درحاشیه‌ای از این قسمت به‌عنوان تعمیمی برمعادلهٔ فیثاغورسی نوشته است:

مسئلهٔ ۵ : معادلهٔسیالهٔ $z^{n} = x^{n} + y^{n}$، به‌ازای $n \geqslant ۳$ ، جوابی برای x ، y ، z درحوزهٔ اعداد صحیح ندارد، به‌استثنای جوابهایی که ازصفر قرار دادن یکی از مقادیر x ، y ، z به‌دست می‌آیند.

بعلاوه، فرما درحاشیهٔ کتابی ادعا کرده است که دلیلی شگفت‌انگیز برای حکم‌مذکور داردکه دراین حاشیه نمی‌گنجد. ریاضیدانان به مدت سه‌قرن ونیم تحقیقات دامنه‌داری را برای این «برهان شگفت‌انگیز» فرما انجام داده‌اند. توافق کلی ریاضیدانان امروزه براین است که فرما فکر می‌کرده که برهانی دارد لیکن‌آن برهان غلط بوده است. درهرحال، مسئله‌ای که فرما مطرح کرده باقی است. آیا این حکم درست است یا غلط؟ ریاضیدانان

---

1. Lagrange 2. Gauss 3. Dirichlet

ثابت کرده‌اند که نظر فرما برای تعداد زیادی از مقادیر خاص n صائب است. به‌عنوان مثال، هم‌اکنون می‌دانیم که ادعای فرما، درحقیقت، به‌ازای کلیهٔ مقادیر n تا ۳۰۰۰۰ صحیح است[۱]. بعلاوه کامپیوترهایی که سرعت عمل خیلی زیاد دارند به‌کار گرفته شده‌اند تا مثالی پیدا کنند که حکم فرما را غلط ازآب درآورد ولی تاکنون هرگز چنین مثالی یافت نشده است. درفصول ۶ و ۱۰ بیشتر به‌بحث درمورد آخرین قضیهٔ فرما خواهیم پرداخت، و ثابت خواهیم کرد که قضیهٔ فرما برای $n = ۳ ، ۴$ درست است.

مثالهای فوق دربارهٔ مسائل نظریهٔ اعداد حداقل یك جنبهٔ مهم نظریهٔ اعداد را نشان می‌دهند. بسیاری ازمسائل نظریهٔ اعداد از مشاهده این یاآن خاصیت که اعداد صحیح آشکار می‌سازند آغاز می‌شود. دراغلب موارد، که خاصیتی از اعداد مورد تردید باشد، آن خاصیت برای موارد متعددی عملا موردآزمایش قرار می‌گیرد. البته، درحالت کلی انتظار نداریم این روش بتواند، هیچ‌نوع اثباتی رافراهم کند. ولی درخیلی جاها به‌دردمی‌خورد. اولا، دلیل تجربی می‌تواند مارا به‌حقیقت مورد تردیدی که درمعرض پژوهش قرار گرفته عقیده‌مند سازد. ثانیاً، دلیل تجربی می‌تواند باارائهٔ مثالهای نقض برای یك پدیده‌نشان‌دهد که این پدیده همواره روی نمی‌دهد. ثالثاً، دلیل تجربی می‌تواند مارا هدایت‌کند تا روش درست اثباتی را حدس‌بزنیم. روزگاری‌بود که اثبات نتایج مورد تردید از راه تجربه روند رایجی بود. ولی امروزه کامپیوترهایی که سرعت‌عمل خیلی زیاد دارند ابزار مهمی برای صاحبنظران معاصر درنظریهٔ اعداد هستند.

خواننده نبایستی تصورکند که نظریهٔ اعداد یك نظریهٔ تجربی محض است. آن قسمت از نظریهٔ اعداد که برمشاهده مبتنی است فقط آغازآن است. صاحبنظر درنظریهٔ اعداد، پس ازآن که حکمی دربارهٔ اعداد صحیح راکه باید مورد آزمایش قرارگیرد تنظیم نمود، آنگاه بامسئلهٔ اثبات یا رد حکم مواجه می‌شود. و تهیهٔ اثبات برای حقایقی که درستی آنها مورد تردید است اغلب کاری فوق‌العاده دشوار است. چه‌بسا که، حدسی به‌صورت ساده‌ای بیان شده وهمه‌جا دلیل تجربی‌آن‌را تأیید می‌کند ولی مع‌هذا نمی‌توان آن‌را اثبات ویا رد کرد. به‌عنوان مثال، گولدباخ[۲]، در ۱۷۴۲ میلادی، اعلام کرد که هرعدد صحیح زوج بزرگتر از ۲ مجموع دوعدد اول است. ولی تاکنون هیچ برهان صحیحی برای‌آن‌آورده نشده است.

جنبهٔ شگفت‌انگیز دیگر نظریهٔ اعداد آن است که وقتی امکان اثبات حدسی در بارهٔ نظریهٔ اعداد وجود دارد چه بسا اثبات شامل نظراتی است که به‌ظاهرخیلی از حدس اصلی دور شده‌اند. به‌عنوان مثال، بسیاری از اثباتهای قضایای مربوط به نظریهٔ اعداد متکی براصول هندسی، جبری، یاتحلیلی (یعنی حساب دیفرانسیل وانتگرال) هستند که اساساً دربیان قضایا اشاره‌ای به‌آنها نشده است وبالمآل به‌اعداد صحیح مربوط می‌شوند.

پیش‌ازاینکه هرگونه بحث اساسی‌درنظریهٔ‌اعداد را آغازکنیم، مناسب به‌نظر می‌رسد که این سؤال رامطرح کنیم که «چرا باید نظریهٔ اعداد را مطالعه‌کرد؟» دلایل زیادی دراین-

---

۱. به‌مقالهٔ Wells Johnson درمجلهٔ Math. Computation, Jan . 1975 رجوع‌کنید.

2. Goldbach

باره موجود است، ولی اجازه دهید به ذکر چندتایی اکتفا کنیم. اعداد صحیح درفعالیتهای روزمرهٔ افراد بشر پدید می‌آیند. وکنجکاوی انسان سؤالاتی را مطرح می‌کند، که صرفاً به‌علت‌اینکه مطرح شده‌اند، باید جواب داده شوند. این امر نظریهٔ اعداد را درهمان مقولهٔ علوم محض، که جویای جواب برای پدیده‌های طبیعی هستند، قرار می‌دهد، واین‌خود یك دلیل کافی برای دفاع ازمطالعهٔ نظریهٔ اعداد است. ولی، دلایل متقاعدکنندهٔ دیگری‌هم‌وجود دارند. نظریهٔ اعداد می‌تواند ازجنبهٔ هنری مورد مطالعه قرار گیرد، زیرا نتایج آن ممکن است از دیدگاه زیبائی‌شناسی بررسی شود. هنگامی‌که ازاین‌جهت بنگریم، نظریهٔ اعداد ارزش مطالعه پیدا می‌کند زیرا مطالعهٔ‌آن برای حس دریافت زیبائی ما خوشایند و مطبوع است. بالاخره، دلیل‌بسیارمهم دیگر برای مطالعهٔ‌نظریهٔ اعداد مرکزیتی است‌که نظریهٔ اعداد در ریاضیات دارد. به‌وسیلهٔ مطالعهٔ نظریهٔ اعداد، به‌دست آوردن دید وسیعتری نسبت به‌بیشتر قسمتهای ریاضیات معاصر ممکن می‌گردد زیرا تعداد معدودی از رشته‌های ریاضی هستندکه هیچ‌ارتباطی بانظریهٔ اعداد ندارند. همچنین، مطالعهٔ نظریهٔ اعداد اغلب مارا به‌تکوین همهٔ رشته‌های ریاضی راهنمایی می‌کند. به‌خاطر تمامی این دلایل است‌که گاوس نظریهٔ اعداد را ملکهٔ ریاضیات نامید.

۲.۱ پیشنیازها

ما مجموعهٔ اعداد صحیح، اعداد منطق، اعداد حقیقی، و اعداد مختلط رابترتیب به $\mathbf{Z}$ ، $\mathbf{Q}$ ، $\mathbf{R}$ و $\mathbf{C}$ نمایش خواهیم داد. برای سادگی بیان، قراردادهای زیر را می‌گذاریم:

درسراسر فصول ۱ـ۶ همهٔ حروف ریز خوابیده (مثل a ، b ، c ، m ، n ، x ، y ، z) را برای نمایش اعدادصحیح به‌کار خواهیم برد. درفصول ۷ تا ۱۱ این قرارداد را به‌اصطلاح کش می‌دهیم تا شامل اعداد منطق نیز بشود. .

اینك فهرستی ازپیشنیازهای لازم برای مطالعهٔ این‌کتاب را ذکرمی‌کنیم.

۱. فرض مابراین‌است‌که خواننده باعلائم وقراردادهای نظریهٔ مجموعه‌ها آشناست.

۲. فرض می‌کنیم خواننده باخواص جبری اعداد صحیح‌آشنایی دارد. یعنی فرض می‌کنیم باخواص جمع، تفریق، ضرب، وتقسیم‌آشنا باشد. همچنین فرض می‌کنیم خواننده بتواند نامساویهایی راکه اعدادصحیح درآنها دخالت دارند بامهارت دستکاری وساده‌کند. درمواقع لزوم این‌حقایق مفروض را بدون توضیح اضافی به‌کار خواهیم گرفت. به‌همین طریق، خواننده می‌تواند بااستفاده ازعملیات جبری درمورد اعداد صحیح، مثل‌عملیات جبر دبیرستانی‌که باآنها مأنوس است، تمرینات عرضه‌شده دراین‌کتاب راحل‌کند.

۳. ما دوخاصیت اعداد صحیح راکه نقطهٔ شروعی برای بسیاری از اثباتهای ماست دانسته فرض خواهیم‌کرد. اولین این خواص اصل استقراء ریاضی است‌که به‌احتمال زیاد قبلا خواننده باآن آشنایی داشته است. دومین خاصیت به اصل خوشترتیبی موسوم است.

اصل استقراء ریاضی : فرض‌کنیم به‌ازای هرعدد مثبت n یك گزارهٔ $P(n)$ داده شده باشد. بعلاوه، فرض‌کنیم $P(1)$ درست باشد وهرگاه‌که $P(n)$ درست است $P(n+1)$ نیز

درست باشد. دراین‌صورت $P(n)$ به‌ازای کلیهٔ اعداد صحیح مثبت n درست‌است.

اصل خوشترتیبی : فرض کنیم S گردایه‌ای ناتهی از اعدادصحیح مثبت‌باشد.دراین‌صورت S عضوی داردکه ازهمه کوچکتراست. به‌عبارت‌دیگر، S شامل عددصحیح مثبتی‌است‌مثل n که $n \leqslant x$ به‌ازای هر x در S .

اصل خوشترتیبی را اغلب به‌طریق زیر به‌کارخواهیم برد. فرض کنید می‌خواهیم ثابت کنیم کلیهٔ اعدادصحیح مثبت دارای خاصیت معینی هستند. مجموعه‌ای از اعداد صحیح مثبت درست می‌کنیم که این خاصیت را نداشته باشند وآن‌را S می‌نامیم، S عضوی مانند z دارد که ازهمه‌کوچکتر است. یعنی، z کوچکترین عدد صحیح مثبتی است‌که دارای خاصیت مفروض نیست. مطابق معمول این z دارای خاصیت شگفت‌انگیزی است که تناقض ایجاد می‌کند. بنابراین، S بایستی تهی باشد، یعنی خاصیت مفروض به‌ازای کلیهٔ اعداد صحیح مثبت n برقرار است. خواننده مثالهای متعددی ازاین طرز اثبات را درفصل ۲ خواهد دید.

۴. ازفصل ۸ به‌بعد، فرض‌خواهیم کرد خواننده درسی ازجبر مجرد راکه‌شامل تعاریف ومقدماتیترین حقایق درمورد گروهها، حلقه‌ها، و میدانهاست گذرانده باشد (به‌عنوان مثال، گروهها، زیر گروهها، گروههای‌خارج‌قسمتی، مرتبهٔ یك‌عضو، قضیهٔ‌لاگرانژ، روابط‌هم‌ارزی، حلقه‌ها، ایده‌آلها، نظریهٔ تجزیه، میدانها).

۳.۱ تمرینات

۱. بااستفاده از استقراء ریاضی دستور زیر را ثابت‌کنید

$$۱+۲+۳+\cdots+n=\frac{n(n+۱)}{۲}.$$

۲. بااستفاده از استقراء ریاضی دستور زیر را ثابت‌کنید

$$۱^۲+۲^۲+۳^۲+\cdots+n^۲=\frac{n(n+۱)(۲n+۱)}{۶}.$$

۳. ثابت‌کنید

$$۱^۳+۲^۳+۳^۳+\cdots+n^۳=(۱+۲+\cdots+n)^۲$$

۴. ثابت‌کنید

$$(x+y)^n=x^n+\binom{n}{۱}x^{n-۱}y+\binom{n}{۲}x^{n-۲}y^۲+\cdots+\binom{n}{n-۱}xy^{n-۱}+y^n,$$

که درآن

$$\binom{n}{k}=\frac{n(n-۱)\cdots(n-k+۱)}{k(k-۱)\cdots ۲\cdot۱}.$$

۵. اثبات زیر را برای همرنگ بودن کلیهٔ توپهای بیلیارد درنظرمی گیریم. از استقرا روی n ، تعداد توپهای بیلیارد، استفاده‌می کنیم. نتیجه به‌ازای $n=1$ روشن است. بنابراین فرض کنیم $n>1$. توپهای بیلیارد را دریك صف قرارمی‌دهیم. بنا براستقرا ، اولین $n-1$ توپ بیلیارد همه یك‌رنگ دارند. همچنین بنابراستقرا ، آخرین $n-1$ توپ‌هم یك رنگ دارند. بنابراین بایستی تمام آنها دارای یك‌رنگ باشند. مغالطهٔ این استدلال کجاست؟

۶. ثابت کنید که‌بیان دیگر اصل استقرا که درزیرآمده است با بیانی که در کتاب آورده شده معادل‌است. فرض کنیم به‌ازای هرعددصحیح مثبت n گزارهٔ $P(n)$ مفروض‌باشد. فرض کنیم $P(1)$ درست باشد. بعلاوه، فرض کنیم هرگاه $P(m)$ به‌ازای هرعدد صحیح مثبت $m\leqslant n$ درست است، آنگاه $P(n+1)$ درست باشد. دراین‌صورت $P(n)$ به‌ازای هرعدد صحیح مثبت n برقرار است.

۳.۱ چگونگی استفاده ازاین کتاب

این فصل را باذکرچندراهنمایی برای دانشجویان به‌پایان می‌رسانیم. امیدواریم که این‌راهنماییها استفاده ازکتاب راساده‌ترکند واین‌درس اول درنظریهٔ اعداد را لذت‌بخش‌تر بسازد.

اولا، دانشجویان بایستی تمرینات زیادی راحل کنند. تمرینات‌زیادی‌آورده‌شده‌است. بعضی‌ازآنهامحاسبات عادی هستند که‌روشنگرقضایامی باشند. بعضی دیگر، نظریه‌های‌موضوع متن را بسط‌می‌دهند. برخی‌دیگرمسائل‌مشکلی هستند که باهوش‌ترین خوانندگان‌را به‌مبارزه می‌طلبند. این‌دسته ازتمرینات معمولا بایك یاچندستاره مشخص‌خواهندشد.

برای‌روشن ساختن تعاریف وقضایا دانشجویان بایستی مثالهای عددی بسازند. اغلب بینشی که یك مثال عددی از یك‌بحث به‌دست می‌دهد به‌مراتب روشنتر از بینشی است که مطالعهٔ صرف استدلالهای منطقی فراهم‌می کند. همچنین، دریافت اثباتی از راه مثال عددی، اغلب، نحوهٔ ساختمان اثبات را با وضوح بیشتری درمعرض دید قرارمی‌دهد.

بالاخره، دانشجویان بایستی اعداد صحیح را بیازمایند ، محاسبه‌کنند، جداول را بسازند، خواصی از اعداد صحیح‌را حدس بزنند ودراثبات ویا رد این حدسیات سعی کنند. اگر به درستی حدسی مشکوك هستید، با کامپیوتر بسیار سریعی که در دسترس دارید آن را برای اولین هزار (یا میلیون) مورد از اعدادصحیح بیازمایید. به‌خاطرداشته باشید که‌استدلال تجربی ما درقضایای نظریهٔ اعداد است و با اجرای بعضی تجربه‌ها می‌توانید در زمرهٔ دانشمندان برجسته، حرفه‌ای وغیرحرفه‌ای، نظیرآنهایی که درپیشرفت نظریهٔ اعداد سهم بسزایی داشته‌اند، درآیید.

۲

بخشپذیری و اعداد اول

۱.۲ مقدمه

در این فصل، ما چگونگی تشکیل اعداد صحیح را از دیدگاه ضرب مورد بحث قرارمی‌دهیم. برای پی‌بردن به‌تصوری که ما در ذهن خود ازتشکیل اعداد داریم، ابتداتشکیل اعداد صحیح را از دیدگاه جمع در نظرمی‌گیریم. عدد ۱ عدد خیلی خاصی است. زیرا از ۱ با جمعهـای متوالی اعداد $۲=۱+۱$ ، $۳=۱+۱+۱$ ، $۴=۱+۱+۱+۱$ و غیره را به دست می‌آوریم. به عبارت دیگر، هرعدد صحیح مثبت از راه جمع کردن تعداد مناسبی ۱ به‌دست می‌آید. آیا اعداد صحیح همین کیفیتی راکه نسبت به جمع ارائه‌می‌دهند نسبت به ضرب هم ارائه می‌دهند؟ یعنی عدد صحیح یکتایی مانند n وجود دارد که هرعدد صحیح‌مثبت بزرگتراز ۱ را بتوان‌از ضرب کردن n به‌دفعات‌مناسبی درخودش به‌دست‌آورد؟ به سادگی دیده می‌شود که‌چنین عددصحیحی وجود ندارد. برای‌مثال، اگر $n=۲$ ، آنگاه در دنبالهٔ ۲ ، $۲^۲$ ، $۲^۳$ ، ... اعداد ۳ ، ۵ ، ... ، و در حقیقت، «بیشتر» اعداد صحیح، ظاهر نمی‌شوند. همین استدلال برای هرعدد n صادق است (تمرین). ولی، کیفیتی شبیه به‌کیفیت مربوط به جمع وجود دارد. عدد صحیح p را اول گوییم هرگاه $p>۱$ و تنها عوامل آن ±۱ و $\pm p$ باشند. در این فصل نشان خواهیم داد کـه هرعدد صحیح بزرگتر از ۱ را می‌توان به صورت حاصلضرب اعداد اول نوشت، به عنوان مثال

$$۴=۲\times۲ ،\quad ۵=۵ ،\quad ۶=۲\times۳ ،\quad ۱۲=۲\times۲\times۳ ،\quad ۱۰۰=۲\times۲\times۵\times۵ .$$

بنابراین به‌جای اینکه یك بلوك ساختمانی برای ساخت ضربی اعداد صحیح داشته باشیم، بلوکهای ساختمانی زیادی داریم وآنها اعداد اول هستند. (در حقیقت، دراین فصل ثـابت

خواهیم کرد که تعدادی نامتناهی از اعداد اول وجود دارد.)

مثال ۱: تجزیهٔ یك عدد صحیح به حاصلضرب اعداد اول برای یافتن مخرج مشترك در کسرها به‌کار می‌رود. برای مثال، $31/60 + 5/162$ را محاسبه می‌کنیم. چون $162 = 2 \times 3^4$ و $60 = 2^2 \times 3 \times 5$، کوچکترین مخرج مشترك دو کسر عبارت است از $1620 = 5 \times 3^4 \times 2^2$. بنابراین،

$$\frac{5}{162} + \frac{31}{60} = \frac{5}{162} \times \frac{2 \times 5}{2 \times 5} + \frac{31}{60} \times \frac{3^3}{3^3} = \frac{50}{1620} + \frac{837}{1620} = \frac{887}{1620}.$$

علاوه بر اینکه ثابت می‌کنیم هر عدد صحیح بزرگتر از ۱ را می‌توان به صورت حاصلضرب اعداد اول نوشت همچنین نشان خواهیم داد که چنین تجزیه‌ای، صرف‌نظر از ترتیب عاملها، منحصر بفرد است (یعنی 3×2 و 2×3 را تجزیه‌های متمایز ۶ به حساب نمی‌آوریم). یکتایی تجزیه به‌عوامل اول از اهمیت زیادی برخوردار است. در واقع، همچنانکه در این فصل خواهیم دید، یکتایی تجزیه در اعداد صحیح یکی از ظریفترین خواص اعداد صحیح و یکی از حقایق ابتدایی در پدیدآوردن نظریهٔ اعداد است.

مثال ۲: برای درك این حقیقت که یکتایی تجزیه دارای نتایج جالبی است، از آن برای یافتن کلیهٔ عوامل مثبت عدد صحیح $b = 4667544 = 2^3 \times 3^5 \times 7^4$ استفاده می‌کنیم. اگر a یك عامل b باشد، آنگاه به‌ازای عددی صحیح مانند c داریم $b = ac$. اگر $a = p_1 \cdots p_r$ و $c = q_1 \cdots q_s$ بترتیب تجزیه‌های a و c به‌عوامل اول باشند، آنگاه $b = ac = p_1 \cdots p_r q_1 \cdots q_s$ تجزیهٔ b به‌حاصلضرب اعداد اول است. بنابر یکتایی تجزیه، p_1، ...، p_r بایستی ازمیان تجزیهٔ $2^3 \times 3^5 \times 7^4$ گرفته شده باشند به‌این ترتیب که ۲ حداکثر ۳ بار ظاهر شود، ۳ حداکثر ۵ بار ظاهر شود و ۷ حداکثر ۴ بار ظاهر شود. بنابراین، عوامل مثبت b اعدادی هستند به صورت $2^k \times 3^l \times 7^m$ به ازای $0 \leqslant k \leqslant 3$، $0 \leqslant l \leqslant 5$، $0 \leqslant m \leqslant 4$.

قضیهٔ یکتایی تجزیه را (که به قضیهٔ بنیادی حساب معروف است) در بخش ۲.۴ ثابت خواهیم کرد. برای این کار، ابتدا لازم است حقایق معینی را درمورد بخشپذیری اعداد صحیح به‌اثبات برسانیم. این حقایق را فقط از به‌کاربردن اصل استقراء ریاضی و اصل خوشترتیبی نتیجه خواهیم گرفت.

نظریهٔ بخشپذیری که دراینجا آن را ارائه می‌کنیم به‌ما اجازه خواهد داد که اولین گامها را در حل معادلات سیاله برداریم. دلیل اساسی برای این امر چنین است: در حل معادلات معمولی ما عادت کرده‌ایم از اعمال جبری جمع، تفریق، ضرب، و تقسیم استفاده کنیم. ولی، اگرمنظور ما پیدا کردن جوابهای صحیح یك معادله باشد، معمولا نمی‌توانیم از تقسیم استفاده کنیم، زیرا که خارج‌قسمت دوعددصحیح لزوماً عددی‌صحیح نیست. بنابراین، مطالعهٔ خواص بخشپذیری اعداد صحیح برای حل معادلات سیاله ضروری به‌نظرمی‌آید. به

عنوان پی‌آمدی از قضایای این فصل ، می‌توانیم هرمعادلهٔ سیاله به صورت $ax+by=c$ را کاملا حل کنیم.

۲.۲ بخشپذیری

تعریف ۱[۱]**:** گوییم a ، b را عاد می‌کند و می‌نویسیم $a|b$ اگر، وفقط اگر ، عددی مانند c وجود داشته باشد چنانکه $b=ac$. دراین حالت a را یك عامل b نیز گوییم و یا گوییم b بر a بخشپذیر است و یا آنکه b مضرب a است.

برای مثال ، ۱۲|۳ ، ۲۴۵|۷ ، ۲۰۰۹|۴۱ و ۴۶۶۷۵۴۴|۵۸۸ .

اگرa، b را عادنکند، می‌نویسیم $a\nmid b$. برای‌مثال ۵∤۳، ۵∤۴، ۵∤۷، زیرا تنها اعداد صحیحی که ۵ را عاد می‌کنند ۱± و ۵± هستند.
ما بعضی خواص‌بدیهی نسبت بخشپذیری بین دوعدد صحیح را دراینجا خواهیم‌آورد.

قضیهٔ ۲ : (یکم) $a|b$ و $a|c$ ایجاب می‌کند که $a|bx+cy$.

(دوم) $a|b$ ایجاب می‌کند که $a|bc$.

(سوم) $a|b$ و $b|c$ ایجاب می‌کند که $a|c$.

(چهارم) فرض کنیم $a>0$ و $b>0$. دراین صورت $a|b$ ایجاب می‌کند که $a\leqslant b$.

(پنجم) $a|b$ و $b|a$ ایجاب می‌کند که $a=\pm b$.

برهان:

(یکم) اگر $a|b$ و $a|c$ ، آنگاه s و t ای موجودند چنانکه $b=as$ و $c=at$. اما دراین صورت $bx+cy=asx+aty=a(sx+ty)$ ، بنابراین $a|bx+cy$.

(دوم) این قسمت از قسمت (یکم) باجایگذاری $x=c$ ، $y=0$ نتیجه می‌شود.

(سوم) اگر $a|b$ و $b|c$ ، آنگاه بـه ازای مقادیری از s و t ، $b=as$ ، $c=bt$. بنابراین ، $c=ast$ و $a|c$.

(چهارم) برای‌اثبات این قسمت، می‌نویسیم $b=ac$ ، چون a و b مثبت‌اند، می‌بینیم که c هم مثبت است، وبنابراین $c\geqslant 1$. پس، $b=ac\geqslant a$.

(پنجم) اول توجه می‌کنیم که اگر $a|b$ ، داریم $|a|\,|\,|b|$ زیرا اگر $b=ac$ ،آنگاه $|b|=|a|\times|c|$. بنابراین ، اگـر $a|b$ و $b|a$ ، آنگاه $|a|\,|\,|b|$ و $|b|\,|\,|a|$ ، کـه با

---

۱. یادآوری می‌کنیم‌که قرارداد فصل ۱ در مورد نمایش اعداد صحیح توسط حـروف خوابیدهٔ کوچك، به‌قوت خود باقی است.

توجه به قسمت (چهارم[1]) ، $|b|\leqslant|a|$ و $|a|\leqslant|b|$. درنتیجه $|a|=|b|$ یعنی $a=\pm b$ و این همان چیزی است که می‌خواستیم اثبات کنیم[2]. ■

قسمت (یکم) قضیهٔ ۲ ، برای مثال ، ایجاب می کند که ، چون ۲|۴ و ۲|۶ ، بایستی داشته‌باشیم $(۷ \times ۶ + ۳ \times ۴)|۲$ و یا ۲|۵۴. ما اغلب گزارهٔ قسمت (یکم) را به‌صورت زیر به‌کار خواهیم برد:

(یکم′) فرض می‌کنیم $c=ax+by$ و $d|b$ اما $d\nmid c$. پس $d\nmid a$.

در واقع ، اگر d ، a را عاد کند، قسمت (یکم) قضیهٔ ۲ ایجاب می کند که $d|c$. بنابراین (یکم′) ثابت می‌شود.

توجه : حکم زیر همواره معتبر نیست: اگر $c=ax+by$ ، $d|b$ ، و $d\nmid a$ ، آنگاه $d\nmid c$. چرا معتبر نیست؟

یك طریق اینکه ببینیم آیا عدد صحیح مفروضی عدد صحیح‌دیگری را عاد می کند یا نه، استفاده ازعمل تقسیم‌طولانی است. برای مثال، برای‌تعیین این که آیا ۲۴۳۷|۵۱۳۲۹، از تقسیم استفاده می کنیم:

$$\begin{array}{r|l} & ۲۱ \\ ۲۴۳۷ & ۵۱۳۲۹ \\ & ۴۸۷۴ \\ \hline & ۲۵۸۹ \\ & ۲۴۳۷ \\ \hline & ۱۵۲ \end{array}$$

بنابراین، $۵۱۳۲۹/۲۴۳۷ = ۲۱ + (۱۵۲/۲۴۳۷)$ ویا معادل آن

$$۵۱۳۲۹ = ۲۱(۲۴۳۷) + ۱۵۲.$$

بالاخص، می بینیم که ۲۴۳۷∤۵۱۳۲۹ ، زیرا وقتی‌ما ۵۱۳۲۹ را بر ۲۴۳۷ تقسیم می کنیم باقیمانده‌ای مساوی ۱۵۲ حاصل می‌شود. آنچه راکه بعد می‌خواهیم نشان دهیم این است که برای به‌دست آوردن خارج قسمت و باقیمانده همواره می‌توانیم عمل تقسیم را انجام دهیم وبعلاوه خارج قسمت و باقیمانده منحصر بفردند. این قضیه به آلگوریتم تقسیم معروف است .

قضیهٔ ۳: فرض‌کنیم a و b دو عدد صحیح باشند و $a>0$. در این صورت اعداد صحیح

---

۱. توجه داشته باشیدکه بنابر شرط (چهارم) a و b بایستی ناصفر باشند . برمتعلم است که حالت‌صفررا جداگانه بررسی‌کند. همچنین‌توجه‌کنیدکه بنابرتعریف ۰|۰ ، زیرا $0 = 1\times 0$ (مترجم).

۲. نامساویهایی‌که دراین اثبات به‌کار رفته‌اند ازفرض صحیح بودن اعداد ناشی شده‌اند.

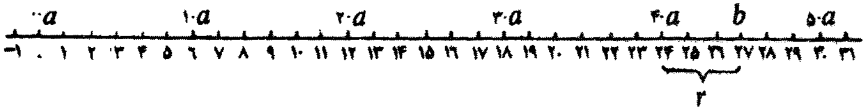
منحصر بفردی مانند q و r موجودندکه در رابطهٔ ذیل صدق می‌کنند[1]

$$b=qa+r \ ، \ ۰\leqslant r<a \ .$$

آلگوریتم تقسیم معادل با این حکم است که $\frac{b}{a}=q+\left(\frac{r}{a}\right)$، $۰\leqslant\frac{r}{a}<۱$. درمثال بالا ، $b=۵۱۳۲۹$ و $a=۲۴۳۷$ و $q=۲۱$ و $r=۱۵۲$.

بیدرنگ نتیجه می‌شود که $a|b$ اگر، وفقط اگر ، $r=۰$. به‌عبارت دیگر $a|b$ اگر، و فقط اگر، باقیماندهٔ تقسیم b بر a صفر باشد.

برای این کــه اثبات قضیهٔ ۳ را بفهمیم بهتر است از رسم خط حقیقی کمك بگیریم. اعداد صحیح na ($n=۰،\pm۱، ...$) توسط نقاط متساوی‌الفاصله، به‌فاصلهٔ a از یکدیگر، برخط مفروض نشان‌داده شده‌اند. هنگامی که n به‌اندازهٔ کافی بزرگ‌شود عدد na درطرف راست b قرارمی گیرد. عدد صحیح qa ، بلافاصله قبل از b ، معرف خارج قسمت b وفاصلهٔ بین qa و b معرف باقیماندهٔ r است. حالت $a=۶$ ، $b=۲۷$ در شکل ۱.۲ دیده می‌شود.



$$۲۷=۴\times۶+۳ \ ، \ q=۴ \ ، \ r=۳ .$$

شکل ۱.۲

برهان قضیهٔ ۳ : اول فرض می‌کنیم $b\geqslant۰$. واضح است که عددی طبیعی مانند n موجود است به‌طوری که $na>b$ (مثلا ، $n=b+۱$) . فرض‌کنیم $q+۱$ کوچکترین عدد با این شرط باشد (اصل خوشترتیبی). دراین صورت

$$(q+۱)a>b\geqslant qa \ .$$

فرض‌کنیم $r=b-qa$. دراین صورت $b\geqslant qa$ ایجاب می‌کند کــه $r=b-qa\geqslant۰$. بالاخره $(q+۱)a=qa+a>b$ ایجاب می‌کند که $r=b-qa<a$.

حالت $b<۰$ را به عنوان تمرین به متعلم واگذار می‌کنیم.

برای آن‌که نشان دهیم q و r منحصر بفردند، فرض می‌کنیم

$$b=qa+r=q_۱a+r_۱ \ ، \ ۰\leqslant r، r_۱<a \ .$$

یا $r_۱\geqslant r$ یا $r\geqslant r_۱$. برای سادگی استدلال ، فرض می‌کنیم $r\geqslant r_۱$. دراین صورت

$$۰\leqslant r-r_۱<a \ ، \qquad (*)$$

۱. آلگوریتم تقسیم‌برای هردو عددصحیح برقرار است وفقط بایدمقسوم‌علیه ناصفر باشد. اثبات درحالت $a<۰$ برمتعلم است (مترجم).

و

$$(q_1-q)a=r-r_1 \cdot$$

بنابراین، $a|r-r_1$. اگر $r-r_1>0$ ، آنگاه قضیهٔ ۲، (چهارم) ایجاب می‌کند $a\leqslant r-r_1$ که متناقض با (*) است. از این‌رو $r-r_1=0$ و $r=r_1$. بنابراین $(q_1-q)a=0$ و $q=q_1$. ■

۲.۲ تمرینات

۱. کدامیك از نسبتهای بخشپذیری زیردرست است؟

$$۲|۲\ ;\ ۲|۶\ ;\ ۳|۱۷\ ;\ -۷|۱۴\ ;\ ۸|۰\ ;\ ۱۷|۱۳۵\ ;$$

$$۱۰|(-۱۲۰)\ ;\ -۱۷|(-۶۸)\ ;\ -۲۳|(-۱۱۷)\ ;$$

$$۳۴۸۱|۴۳۷۲۸۹\ ;\ ۳۴۸۱|۴۳۵۱۲۵ \cdot$$

۲. کلیهٔ مقسوم‌علیه‌های ۱۲، ۱۳، ۷۲، و ۲۶۰ را پیدا کنید.

۳. در موارد زیر، b را بر a تقسیم کنید و خارج قسمت و باقیمانده را به‌دست‌آورید:

(آ) $a=۱۷$ ، $b=۲۳$.

(ب) $a=۱۷$ ، $b=-۲۳$.

(ج) $a=۱۴$ ، $b=۳۶۴$.

(د) $a=۳۷۶$ ، $b=۴۳۵۸۱$.

(ه) $a=۴۳۵۸۱$ ، $b=۳۷۶$.

۴. شکلی متناظر با شکل ۱.۲ برای موارد زیر رسم کنید.

(آ) $a=۱۷$ ، $b=۴۰$.

(ب) $a=۳$ ، $b=۴۰$.

(ج) $a=۵$ ، $b=۴۰$.

(د) $a=۷$ ، $b=-۴۰$.

۵. بین اعداد صحیح از ۱ تا ۱۰۰ چند عدد بر ۹ بخشپذیرند؟ بین اعداد صحیح از ۱ تا ۲۰۰۰ چند عدد بر ۹ بخشپذیرند؟ اگر a و n اعداد صحیح‌مثبتی باشند، بین اعدادصحیح از ۱ تا n چند عدد بر a بخشپذیرند؟

۶. بین‌اعداد صحیح از ۲۵ تا ۲۵۰ چندعدد بر ۱۱ بخشپذیرند؟ بین اعدادصحیح از ۲۵۰ تا ۲۵۰۰۰ چند عدد بر ۱۱ بخشپذیرند؟ اگر n ، m ، a اعداد صحیحی مثبت ، $n>m$ ، باشند ، بین اعداد صحیح از m تا n چند عدد بر a بخشپذیرند؟

۷. اگر a ، b ، c سه‌عدد صحیح ناصفر باشند ، ثابت کنید که $ac|bc$ اگر ، و فقط اگــر ، $a|b$[1] .

۸. گزارهٔ زیر را ثابت ویا رد کنید: اگر $d \neq 0$ و $c=ax+by$ و $d|c$ و $d|b$، آنگاه $d|a$.

۹. نشان دهید که به ازای هرعدد صحیح n ، n^2 نمی‌تواند به‌صورت $3k+2$ بــاشد ولی می‌تواند به صورت $3k$ یا $3k+1$ باشد. (یعنی، اگرعدد صحیح مربعی را بــر ۳ تقسیم کنیم ، باقیمانده نمی‌تواند ۲ باشد.)(راهنمایی : n را بر ۳ تقسیم کنید و جداگانه هــر سه حالت ممکن برای باقیمانده را در نظر بگیرید.)

۱۰. نشان‌دهید که به ازای هرعدد صحیح n ، $4 \nmid n^2+2$.

۱۱. نشان دهید که به ازای هرعدد صحیح n ، $2|n^2-n$ ، $6|n^3-n$.

۱۲. گزارهٔ زیر را ثابت ویا رد کنید: $a^2|b^3$ ایجاب می کند که $a|b$.

۱۳. (آ) نشان‌دهید که به‌ازای‌هرعدد صحیح n ، اعداد صحیح k و r موجودند به‌طوری که

$$n=3k+r \text{ و } r=-1, 0, 1 .$$

(ب) آیا می‌توانید این تمرین را تعمیم دهید؟[2]

۱۴. (آ) نشان دهید که به ازای هرعدد صحیح مفروض k عدد صحیحی مــانند n موجود است‌به‌طوری که $5|n^3+k$. (راهنمایی: بنویسید $k=5q+r$ ، که درآن $0 \leqslant r < 5$.)

(ب) اگر به‌جای ۵ ، ۷ بگذاریم آیا باز هم این گزاره درست است؟

۱۵. نشان دهید که آخرین رقم یك مربع کامل فقط می‌تواند ۰ ، ۱ ، ۴ ، ۵ ، ۶، یا ۹ باشد.

۱۶. نشان‌دهید که شرط لازم وکافی برای اینکه‌عدد صحیح مثبتی‌مربع کامل باشد، این‌است که تعداد مقسوم‌علیه‌های مثبتش عددی‌فردباشد. (راهنمایی: برای اینکه‌موضوع را درحالت کلی دریابید ، تاحدامکان مثالهای عددی زیادی را آزمایش‌کنید.)

۱۷. نشان دهید که به‌ازای هرعدد صحیح‌مثبت n ، $2|3^n-1$ ، $3|4^n-1$ ، $4|5^n-1$ ، الی‌آخر (راهنمایی: از اتحاد بسجمله‌ای

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots+x+1)$$

استفاده کنید.)

۱۸. از اتحاد بسجمله‌ای $x^n+1=(x+1)(x^{n-1}-x^{n-2}+\cdots+x^2-x+1)$ ، وقتی که n عدد صحیح مثبت فردی است، استفاده کنید، تا ثابت نمایید کــه هرگاه 2^n+1 دارای هیچ مقسوم‌علیه مثبتی غیر از خودش و ۱ نباشد (یعنی ، اول باشد)، آنگاه n بایستی توانی از ۲ باشد. (راهنمایی: اگر n فرد باشد، آنگاه $3|2^n+1$ ؛ اگر $n=2k$ و k فرد

---

۱. دراین مسأله‌کافی است c ناصفرباشد (مترجم).

۲. این قضیه موسوم به‌تقسیم با کوچکترین باقیماندهٔ مطلق است (مترجم).

باشد، آنگاه $۵ \mid ۲^{n}+۱$ والی‌آخر.) اعداد اول به‌صورت $۲^{n}+۱$ ، اعداد اول فرما نامیده می‌شوند.

۱۹. با مشاهدهٔ مسائل ۱۷ و ۱۸ ، آیا می‌توانید گزاره‌ای کلی در موردکاربرد اتحادهای بسجمله‌ای در مسائل مربوط به‌بخشپذیری بیان کنید؟

۲۰. نشان دهید که، به‌ازای هر $n \geqslant ۱$ ، $۱+۲+\cdots+n \mid ۳(۱^۲+۲^۲+\cdots+n^۲)$.

۲۱. فرض می‌کنیم m و n فرد باشند.

(آ) نشان دهید که $۸ \mid m^۲-n^۲$.

(ب) نشان دهید که $۸ \mid m^۴+n^۴-۲$.

۲۲. نشان دهید که ضرایب دوجمله‌ای

$$\binom{n}{k}=\frac{n!}{k!(n-k)!} \qquad (۰\leqslant k\leqslant n)$$

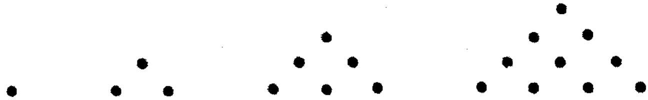
اعدادصحیح‌اند، که‌در آن $x!=۱\times ۲\times \cdots \times x$.

۲۳. فرض کنیم n ، $n_۱$ ، $n_۲$ ، … ، n_l اعداد صحیح مثبت باشند به طوری که $n=n_۱+\cdots+n_l$. نشان دهید که

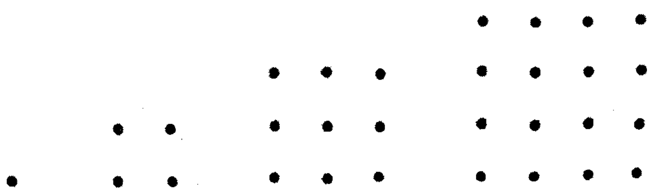
$$\frac{n!}{n_۱!\cdots n_l!}$$

عددی است صحیح .

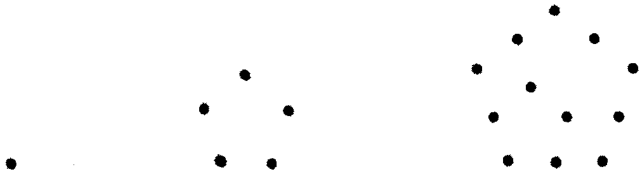
۲۴. اعداد به اصطلاح مصور که به توسط یونانیها مطالعه شده است چنین تعریف شده‌اند: nامین عدد مثلثی ، بنابر تعریف ، تعداد نقطه‌ها در مثلث nام در دنبالهٔ زیر است:



سپس n امین عدد مربعی، تعدادنقطه‌های مربع nام، در دنبالهٔ زیراست:



nامین عدد مخمسی تعداد نقطه‌ها در پنج ضلعی nام دردنبالهٔ زیر است:



و به‌همین طریق برای اعداد مسدسی ومسبعی وغیره :

(آ) نشان دهید که nامین عدد مثلثی $\frac{1}{2}(n^2+n)$ است .

(ب) نشان دهید که nامین عدد مربعی n^2 است.

(ج) نشان دهید که nامین عدد مخمسی $\frac{1}{2}(3n^2-n)$ است .

(د) دستوری کلی برای nامین عدد k- ضلعی بیابید.

(ه) نشان دهید که اعداد ۳ ، ۴ ، ۸ و ۹ نمی‌توانند آخرین رقم یك عدد مخمسی باشند .

۲۵. (آ) فرض کنیم n عدد صحیح مثبتی بزرگتر از ۱ باشد. نشان دهید که هرعددصحیح مثبت a می‌تواند به‌طور منحصر بفردی به صورت $a=a_0+a_1n+a_2n^2+\dots+a_kn^k$ نوشته‌شود، که $0\leqslant a_i\leqslant n-1$. به‌ازای $n=10$ ، رقمهای a_0 ، ... ، a_k معرف رقمهای نمایش اعشاری a هستند. حالت کلی حالتی است که نمایش a در مبنای n نامیده می‌شود.

(ب) نمایش $a=57$ ، $a=139$ ، و $a=199$ را درمبنای ۷ بیابید.

۳.۲ بزرگترین مقسوم‌علیه مشترك

در مبحث بخشپذیری‌مفهوم بزرگترین مقسوم‌علیه مشترك (پس از مفهوم عدد اول) شاید مهمترین مفهوم باشد.

تعریف ۱: فرض کنیم a و b دوعدد صحیح باشند. d را بزرگترین مقسوم علیه مشترك (بمم) a و b نامیم اگر ، وفقط اگر،

(یکم) $d>0$ ؛

(دوم) $d|a$ و $d|b$ (یعنی، d مقسوم‌علیه مشترکی از a و b باشد)؛

(سوم) هرگاه $e|a$ و $e|b$ ، آنگاه $e|d$.

بزرگترین مقسوم‌علیه مشترك دو عدد a و b را چنین می‌نویسیم $d=$ بمم$(a ، b)$. اگر

۱ = بمعم$(a ، b)$ ، آنگاه a و b را نسبت به هم اول[1] گوییم.

مثال ۲: اینك چند مثال از بزرگترین مقسوم‌علیه مشترك دو عدد ارائه می‌دهیم:

(یکم) $a=۲ ، \quad b=۳ ، \quad d=۱$.

(دوم) $a=۱۲ ، \quad b=۱۵ ، \quad d=۳$.

(سوم) $a=۲۵ ، \quad b=۸۵ ، \quad d=۵$.

(چهارم) $a=۱۰۰ ، b=۴۷۵ ، d=۲۵$.

به عنوان مثال قسمت (دوم) را ثابت می‌کنیم ، مقسوم‌علیه‌های ۱۲ عبارتند از ± ۱ ، ± ۲ ، ± ۳ ، ± ۴ ، ± ۶ ، و ± ۱۲ . مقسوم‌علیه‌های ۱۵ عبارت‌اند از ± ۱ ، ± ۳ ، ± ۵ ، ± ۱۵ . مقسوم‌علیه‌های‌مشترك ۱۲ و ۱۵ اعداد ± ۱ و ± ۳ هستند و ، در واقع ، ۳ تنها مقسوم‌علیه مشترك مثبتی است که همهٔ مقسوم‌علیه‌های مشترك آن را عاد می‌کنند. توجه به‌نقش دقیقی که یکتایی تجزیه درمحاسبهٔ بالا بـرای ۳ = بمعم(۱۵ ، ۱۲) بازی مـی کند بسیار آموزنده است.

حال تعریف بـزرگترین مقسوم‌علیه مشترك را تفسیر می‌کنیم. اولا شرط (یکم) حکم می‌کند بمعم$(a ، b)$ بایستی‌عددصحیح‌مثبتی باشد. شرط (دوم) حکم می‌کند که بمعم$(a ، b)$ هم‌مقسوم‌علیهی از a و هم مقسوم‌علیهی از b است، بالاخـره شرط (سوم) می‌گـوید کـه بمعم$(a ، b)$ دارای ایـن خاصیت استکـه همهٔ مقسوم علیه‌های مشترك a و b آن را عـاد می‌کنند.

به هیچ وجه واضح نیست که a و b بزرگترین مقسوم‌علیه مشترکی دارند یا نه. اثبات وجود بمعم یکی از وظایف عمدهٔ این قسمت خواهد بود.

تعریف ۱ ، گذشته ازآن‌که وجود بزرگترین مقسوم‌علیه مشترك a و b را قابل تردید می‌شمارد ، امکان وجود دو بـزرگترین مقسوم علیه مشترك برای a و b را نیز نفی نمی‌کند. اما عملا بسادگی می‌توان نشان داد که حداکثر یك بـزرگترین مقسوم‌علیه مشترك موجود است، زیرا اگر d_1 و d_2 درشرایط تعریف ۱ صدق‌کنند، آنگاه شرط (دوم) ایجاب‌می‌کند کـه $d_1|a$ و $d_1|b$ ، $d_2|a$ و $d_2|b$. از این‌رو ، وقتی شرط (سوم) را متناوبـاً به ازای $e=d_1$ ، $d=d_2$ ، و $e=d_2$ ، $d=d_1$ به‌کار بـریم ، می‌بینیم کـه $d_1|d_2$ و $d_2|d_1$. بنابراین، ازقضیهٔ ۲.۲ (پنجم) نتیجه‌می‌گیریم که $d_1=\pm d_2$. ولی،چون d_1وd_2هردومثبت‌اند می‌بینیم که $d_1=d_2$. بنابراین ، نشان داده‌ایم که b و a حداکثر یك بزرگترین مقسوم‌علیه مشترك دارند. این حقیقت در حکم قضیهٔ ۳ که در زیر می‌آید ذکر خواهد شد.

ازآن جایی که مفهوم بزرگترین مقسوم‌علیه مشترك ازاهمیت زیادی برخوردار است، برای اثبات وجودآن دو برهان ارائه خواهیم‌داد. بـرهان اول «شسته ورفته» بوده ولی‌فقط

---

۱. a و b را متباین نیز می‌خوانیم (مترجم).

وجود آن را نشان می‌دهد درحالی که دومین برهان جنبهٔ سازندگی دارد، بدین معنی که روش صریحی برای یافتن بزرگترین مقسوم علیه مشترك ارائه می‌دهد. هردو برهان ازلحاظ فهم تاحدی مشکل هستند. درواقع مسئلهٔ وجود یك بمم ظریفترین نکتهٔ این فصل است. هر برهانی دربارهٔ این وجود باید لااقل متضمن یك یا دو دید استادانه باشد. اما، قبلا شخص دیگری این دیدهای جالب را دریافته است، وکافی است که ما برجای خود بنشینیم و زیبایی آنها را تحسین کنیم.

نکتهٔ دیگری هم هست که می‌خواهیم قبل از پرداختن به برهان ذکر کنیم. یك چیز غیر مترقبه و حتی شگفت‌انگیز این است که، ماراه حل کامل معادلهٔ سیالهٔ $ax+by=c$ را به عنوان حاصل این براهین به‌دست می‌آوریم.

قضیهٔ ۳: فرض کنیم a و b اعداد صحیحی باشند که حداقل یکی از آنها ناصفر باشد[۱]. در این صورت بمم$(a ، b)=d$ موجود و منحصر بفرد است.

برهان اول: مجموعهٔ S متشکل ازهمهٔ اعداد صحیح بصورت $ax+by$ را، که در آن x و y کلیهٔ اعداد صحیح را اختیار می‌کنند، یعنی

$$S=\{ax+by| \text{ اعداد صحیح‌اند } y \text{ و } x\}$$

را درنظر می‌گیریم.

چون S شامل اعداد a و $-a$، b و $-b$ ($-a=a(-۱)+b\cdot ۰$ و $a=a\cdot ۱+b\cdot ۰$) است پس شامل یك عدد صحیح مثبت خواهد بود. فرض کنیم d کوچکترین عدد صحیح مثبت در S باشد. پس با تعریفی که از S کرده بودیم، به‌ازای اعداد صحیحی مانند $x_۰$ و $y_۰$ می‌توانیم بنویسیم $d=ax_۰+by_۰$. گوییم که این d بمم a و b است. (این نحوهٔ برداشت، تا آنجا که به ما مربوط می‌شود، خیلی زیرکانه است.) خوب، مطابق تعریف $d>۰$، وبنابراین شرط (یکم) تعریف ۱ برقراراست. اگر $e|a$ و $e|b$، آنگاه بنابرقضیهٔ ۲.۲ (یکم)، $e|d$. برای اینکه نشان دهیم d، a را عاد می‌کند ازآلگوریتم تقسیم (قضیهٔ ۳.۲) استفاده می‌کنیم و می‌نویسیم

$$a=qd+r \ , \ ۰\leqslant r<d \ ,$$

و نشان می‌دهیم که $r=۰$. این نتیجه حاصل می‌آید زیرا

$$\begin{aligned} r&=a-qd=a-q(ax_۰+by_۰)\\ &=a-aqx_۰-bqy_۰=a(۱-qx_۰)+b(-qy_۰) \end{aligned}$$

---

۱. البته بمم(۰ ، ۰) برابرصفر تعریف می‌شود. ولی، توجه داشته باشید که با این تعریف شرط یکم تعریف ۱ برقرارنمی‌باشد. همچنین ازنظر لغوی نیز ۰ بزرگترین مقسوم‌علیه مشترك ۰ و ۰ نیست زیرا که مثلا ۱ نیز مقسوم‌علیه مشترکی است ولی توجه‌کنید که ۱|۰ (مترجم).

بنابراین، r به S تعلق دارد ($r=ax+by$ با $x=1-qx_0$ و $y=-qy_0$). چون $0\leqslant r<d$ و d کوچکترین عدد صحیح مثبت در S است، پس نتیجه می‌شود که $r=0$، همان چیزی که مطلوب بود. بنابراین $d|a$. با استدلالی مشابه نشان می‌دهیم که $d|b$. پس شرط (دوم) تعریف ۱ برقرار است و بمعم$(a ، b)=d$. ■

تبصره: اثبات اینکه d، a را عاد می‌کند اثباتی است که به‌کرات پیش خواهد آمد، و شما بایستی با این اصل کاملا آشنا باشید که: وقتی عدد صحیح مفروضی به صورت کوچکترین عدد صحیحی که خاصیت مفروضی را دارد تعریف شده باشد و شما بخواهید نشان دهید که این عدد، عدد صحیح دیگری را عاد می‌کند، عمل تقسیم را انجام دهید و باقیمانده را به دست بیاورید. سپس نشان دهید که این باقیمانده همان خاصیت مفروض را دارد و بنابراین بایستی صفر باشد.

لطفاً به نتیجهٔ جالب زیر که از اثبات فوق نتیجه شده توجه کنید.

نتیجهٔ ۴: اگر بمعم$(a ، b)=d$، آنگاه اعداد صحیح x و y موجودند به طوری که

$$d=ax+by.$$ [1]

مثال ۵: (به مثال ۲ و نتیجهٔ ۴ مراجعه کنید.)

(یکم) $a=2$ ، $b=3$; $x=-1$ ، $y=1$; $1=2(-1)+3(1)$.

(دوم) $a=12$ ، $b=15$; $x=-1$ ، $y=1$; $3=12(-1)+15(1)$.

(سوم) $a=25$ ، $b=85$; $x=7$ ، $y=-2$; $5=25(7)+85(-2)$.

(چهارم) $a=100$ ، $b=475$; $x=5$ ، $y=-1$; $25=100(5)+475(-1)$.

هم اکنون، دومین برهان قضیهٔ ۳ را می‌آوریم. این برهان آلگوریتم اقلیدسی نامیده می‌شود (قضیهٔ ۲ از کتاب هفتم اصول اقلیدس[2]). این برهان روش روشنی برای محاسبهٔ بمعم دو عدد صحیح، پیش پای ما می‌گذارد.

برهان دوم قضیهٔ ۳: فرض می‌کنیم $a>0$. (اثبات حالت $a\leqslant 0$ به‌عهدهٔ متعلم واگذار می‌شود.) بنابر قضیهٔ ۳.۲ می‌توان نوشت

$$b=q_1a+r_1 \qquad 0<r_1<a$$

$$a=q_2r_1+r_2 \qquad 0<r_2<r_1$$

---

۱. یعنی بزرگترین مقسوم‌علیه مشترک دوعدد را همیشه می‌توان به‌صورت ترکیب خطی از آن دو عدد بیان‌کرد (مترجم).

2. Euclid, *Elements*, Book VII, Proposition 2.

$$r_1=q_3r_2+r_3 \qquad 0<r_3<r_2$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-2}=q_nr_{n-1}+r_n \qquad 0<r_n<r_{n-1}$$
$$r_{n-1}=q_{n+1}r_n \qquad \text{(بدون باقیمانده)}$$

چون باقیمانده‌ها کاهش می‌یابند و بزرگتر از صفر یا مساوی با آن هستند، سرانجام بایستی باقیمانده‌ای داشته باشیم که صفر است. البته همینکه باقیماندهٔصفر به‌دست‌آوردیم جریان‌عمل را متوقف می‌کنیم. دراینجا n می‌تواند یکی از اعداد ۰ ، ۱ ، ۲ ، ۳ ، ... باشد ، و r_0 را همان a تعریف می‌کنیم.

در این برهان ، می‌خواهیم نشان دهیم که بمعم$(a ، b)=r_n$. بنابرتعریف، $r_n>0$. پس شرط (یکم) از تعریف ۱ برقرار است. مطابق تعریف، $r_n|r_{n-1}$ بنابراین، با استفاده از معادلهٔ ماقبل آخر معادلات بالا ، $r_n|r_n$ و $r_n|r_{n-1}$ ایجاب می کنندکه $r_n|r_{n-2}$ (مجدداً قضیهٔ ۲.۲ شرط (یکم)). سپس $r_n|r_{n-1}$ و $r_n|r_{n-2}$ ایجاب‌می کنندکه $r_n|r_{n-3}$. این عمل را ادامه‌می‌دهیم وآن را درمورد مجموعهٔ معادلات فوق اعمال می کنیم تا سرانجام به $r_n|r_3$ و $r_n|r_2$ می‌رسیم که ایجاب می کنند داشته باشیم $r_n|r_1$ ، و لذا $r_n|a$ ؛ وهمین‌طور $r_n|b$. بنابراین، شرط (دوم) از تعریف ۱ نیزبرقرار است. بالاخره، اگر $e|a$ و $e|b$ ، آنگاه مثل قبل $e|r_1$ وهمچنین $e|r_2$ ، الی‌آخر.وقتی که رشتهٔ معادلات را تا پایین ادامه دهیم، سرانجام به $e|r_n$ می‌رسیم، و بنابراین ، شرط (سوم) ازتعریف ۱ نیز برقرار می‌شود. ■

به وسیلهٔ این روش شما می‌توانید d را برای امثله‌ای‌که درمثال ۲ آمده‌اند محاسبه کنید. ما بمعم(۲۴۳۷ ، ۵۱۳۲۹) را پیدا می کنیم. قبلا اولین تقسیم را دربخش ۲ انجام داده‌ایم .

$$۵۱۳۲۹=۲۱\times۲۴۳۷+۱۵۲$$
$$۲۴۳۷=۱۶\times۱۵۲+۵$$
$$۱۵۲=۳۰\times۵+۲$$
$$۵=۲\times۲+۱$$
$$۲=۲\times۱+۰ .$$

بنابراین، بمعم(۵۱۳۲۹ و ۲۴۳۷) = ۱ . پس ۲۴۳۷ و ۵۱۳۲۹ نسبت به‌هم اول‌اند.

توجه می کنیم که این برهان، برهان سازنده‌ای ازنتیجهٔ ۴ را نیز به‌دست‌می‌دهد. یعنی $d=r_n$ و بنابراین

$$\begin{aligned} d&=r_{n-2}-q_nr_{n-1}\\ &=r_{n-2}-q_n(r_{n-3}-q_{n-1}r_{n-2})\\ &=r_{n-2}(1+q_nq_{n-1})-r_{n-3}q_n . \end{aligned}$$

حال به جای r_{n-2} و r_{n-3} و ... بترتیب مساوی آنها $r_{n-4}-q_{n-2}r_{n-3}$ و $r_{n-5}-q_{n-3}r_{n-4}$ و ... را قرار می‌دهیم، تا سرانجام d را به‌صورت $ax+by$ به دست آوریم.[1]

شما باید این روش را برای امثلهٔ مثال ۵ انجام دهید (توجه: ممکن است شما همان جوابهای مثال ۵ را به دست نیاورید) . ما این روش را با یافتن x و y به‌طوری که

$$۲۴۳۷x+۵۱۳۲۹y=۱ \qquad (۱)$$

روشن می کنیم.

$$
\begin{aligned}
۱&=۵-۲\times۲\\
&=۵-۲(۱۵۲-۳۰\times۵)=-۲\times۱۵۲+۶۱\times۵\\
&=-۲\times۱۵۲+۶۱(۲۴۳۷-۱۶\times۱۵۲)\\
&=۶۱\times۲۴۳۷-۹۷۸\times۱۵۲\\
&=۶۱\times۲۴۳۷-۹۷۸(۵۱۳۲۹-۲۱\times۲۴۳۷)\\
&=-۹۷۸\times۵۱۳۲۹+۲۰۵۹۹\times۲۴۳۷
\end{aligned}
$$

بنابراین، $x=۲۰۵۹۹$ ، $y=-۹۷۸$.

ممکن است این روش پرمحاسبه به نظر آید، اما اگر به‌اندازهٔ جواب آن نگاه کنیدو اگر درفکر پیدا کردن x و y صحیح برای معادلهٔ (۱) باشید، خواهید دید که این روش به راستی خیلی مؤثر است.

اینك ما به ذکر چند حقیقت دیگر دربارهٔ بمعم می‌پردازیم.

قضیهٔ ۶ : فرض کنیم بمعم$(a ، b)=d$.

(یکم) $d=۱$ اگر، وفقط اگر، اعداد صحیح x و y موجود باشند به طوری که $ax+by=۱$.

(دوم) بمعم$(a/d ، b/d)=۱$.

(سوم) $a|bc$ و $d=۱$ ایجاب می کنند که $a|c$.

(چهارم) $a|bc$ ایجاب می کند که $(a/d)|c$.

(پنجم) بمعم$(ma ، mb)=md$ ، به شرط آنکه $m>۰$.[2]

---

۱. اثبات دقیق‌کلیهٔ این مطالب به‌استقراء ریاضی می‌باشد و برمتعلم است آنها را توسط استقراء ثابت‌کند (مترجم).

۲. اگر $m<۰$ ، رابطهٔ بمعم$(am ، bm)=|m|d$ برقرار است. همچنین با توجه به تعریف پاورقی صفحهٔ ۲۱ ، رابطهٔ فوق به‌ازای $m=۰$ نیز برقرار است. اثبات برمتعلم است (مترجم).

اینها همه حقایق بسیار مهمی هستند، ولی (سوم) بنیادیترین آنهاست. ترتیب فوق برای سهولت دراثبات آنها اتخاذ شده است.

برهان:

(یکم) نتیجهٔ ۴ دقیقاً بیانگر این حکم است که $d=1$ وجود x و y را ایجاب می‌کند. بالعکس، اگر $ax+by=1$ و $d|a$ و $d|b$، می‌بینیم که $d|1$ و بنابراین $d=\pm 1$. پس، چون $d>0$، داریم $d=1$.

(دوم) مجدداً بنابر نتیجهٔ ۴، اعداد صحیح x و y وجود دارند به‌طوری که

$$ax+by=d ,$$

و بنابراین

$$\frac{a}{d}x+\frac{b}{d}y=1 .$$

یادآوری می‌کنیم که a/d و b/d اعداد صحیح هستند، پس بنابر قسمت (یکم) بمعم$(a/d , b/d)=1$ یعنی همان که می‌خواستیم.

(سوم) چون $d=1$، اعدادصحیح x و y وجود دارندبه‌طوری که $ax+by=1$. ازضرب طرفین معادله در c نتیجه می‌شود

$$c=acx+bcy .$$

بنابراین، $a|a$ و $a|bc$ ایجاب می‌کندکه $a|c$، یعنی همانکه می‌خواستیم.

(چهارم) بدیهی است که $a|bc$ ایجاب می‌کند $(a/d)|(b/d)c$. اکنون فقط از قسمتهای (دوم) و (سوم) استفاده کنید.

(پنجم) واضح‌است که $md|ma$ و $md|mb$. فرض کنیم $e|ma$ و $e|mb$. بایستی نشان دهیم که $e|md$. فرض می‌کنیم

$$d=ax+by .$$

پس

$$md=max+mby ,$$

و لذا واضح است که $e|md$. بنابراین، با توجه به تعریف ۱، بمعم$(ma , mb)=md$.

تبصره: در برهان قسمت (سوم) یك اصل بنیادی دیگری برای اثباتهای نظریهٔ اعداد را دیده‌اید وامیدواریم آن را خوب فهمیده باشید. (در تبصرهٔ مشابهی درصفحهٔ ۲۲ اولین‌اصل بنیادی‌آورده شده بود.) اگر بخواهیدمطلبی را درموردa وb ثابت کنیدواگر بمعم$(a,b)=1$، بنویسید $ax+by=1$ و ببینید که آیا کمکی می‌کند؟ اغلب اوقات چنین است.

اینك، همچنانکه قول داده بودیم ، می‌توانیم شرح کاملی دربارهٔ جوابهای معادلهٔ $ax+by=c$ بدهیم .

قضیهٔ ۷ : اگر a ، b ، c اعداد صحیحی باشند وحداقل یکی از a و b ناصفر باشد ، قرار می‌دهیم $d=$ بمم$(a \text{ ، } b)$. آنگاه معادلهٔ سیالهٔ

$$ax+by=c \qquad (۲)$$

را فقط وفقط وقتی می‌توانیم برحسب اعداد صحیح x و y حل کنیم که $d|c$. دراین‌حالت، فرض کنیم $x=x_\circ$ و $y=y_\circ$ یکی ازجوابها باشد. سپس‌جواب‌عمومی(۲) عبارت‌است‌از

$$x=x_\circ+\frac{b}{d}k \text{ ، } \quad y=y_\circ-\frac{a}{d}k \text{ ، } \quad k=\circ \text{ ، } \pm ۱ \text{ ، } \pm ۲ \text{ ، } \ldots$$

برهان: اگر اعداد صحیح x و y وجود داشته باشند به طوری که $ax+by=c$ ، آنگاه مطابق معمول ، $d|a$ و $d|b$ ایجاب می‌کنند که $d|c$. بالعکس ، فرض کنیم $d|c$. بنا بر نتیجهٔ ۴ اعداد صحیح x' و y' وجود دارند به‌طوری‌که

$$ax'+by'=d \text{ .}$$

پس‌ازضرب‌طرفین در c/d، می‌بینیم که $x=(c/d)x'$ و $y=(c/d)y'$ جوابی برای معادلهٔ اصلی (۲) است . (فرض $d|c$ برای آن است که $x=(c/d)x'$ و $y=(c/d)y'$ اعداد صحیح باشند.)

برای قسمت‌دوم قضیه ، بایك جواب $x_\circ$ و $y_\circ$ معادلهٔ (۲) شروع می‌کنیم . اگر در (۲) به‌جای x و y مستقیماًمقادیرآنها : $x=x_\circ+(b/d)k$ ، $y=y_\circ-(a/d)k$ راقرار دهیم می‌بینیم که x و y یك جواب (۲) است. بالعکس، فرض کنیم x و y یك جواب غیر مشخص (۲) باشد. فرض می‌کنیم $a\neq\circ$. (اگر $a=\circ$ ، آنگاه بنابرفرض $b\neq\circ$ و باز همین‌گونه عمل می‌کنیم.) بنابراین

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

$$a(x-x_\circ)=b(y_\circ-y) \text{ .}$$

بدین ترتیب ،

$b|a(x-x_\circ)$ وبنابراین، بنابرقضیهٔ۶ (چهارم)، $\frac{b}{d}\Big|(x-x_\circ)$ پس، عدد صحیحی مانند k وجود دارد به طوری که $x-x_\circ=(b/d)k$ ؛ یعنی

$$x=x_\circ+\frac{b}{d}k \text{ .}$$

اگر در (۲) به‌جای x مقدارش را بگذاریم ومعادله را نسبت به y حل کنیم خواهیم‌داشت

$$a(x_\circ+\frac{b}{d}k)+by=c,$$

بنابراین

$$by=c-ax_\circ-a\frac{b}{d}k$$

$$=by_\circ-b\frac{a}{d}k,$$

پس

$$y=y_\circ-\frac{a}{d}k,$$

و این‌همان چیزی است که می‌خواستیم .

به‌عنوان مثال ، درصفحهٔ ۲۴ نتیجه گرفتیم که یك جواب معادلهٔ

$$۲۴۳۷x+۵۱۳۲۹y=۱$$

عبارت است از $x_\circ=۲۰۵۹۹$ و $y_\circ=-۹۷۸$. چون دراینجا $d=۱$ جواب عمومی این معادله به‌صورت زیراست

$$x=۲۰۵۹۹+۵۱۳۲۹\,k$$

$$y=-۹۷۸-۲۴۳۷\,k$$

به ازای $k=۰$ ، ±۱ ، ±۲ ، ... ، بنابراین، مثلا به‌ازای $k=-۱$ جواب زیرحاصل می‌شود

$$x=-۳۰۷۳۰ \text{ و } y=۱۴۵۹ .$$

۳.۲ تمرینات

۱. بمعم زوجهای زیر از اعداد را بیابید و با استفاده ازتعریف بمعم ثابت‌کنید که جوابهای شما درست‌اند :

(آ) $a=۱۵$ ، $b=۲۰$.

(ب) $a=۲۱$ ، $b=۳۱۵$.

(ج) $a=۵۴$ ، $b=۸$.

(د) $a=۲۴$ ، $b=۴۹$.

۲. با استفاده از آلگوریتم اقلیدسی بمعم اعداد زیر را بیابید :

(آ) $a=10587$ ، $b=534$.

(ب) $a=9800$ ، $b=180$.

(ج) $a=1587645$ ، $b=6755$.

۳. برای هرقسمت از تمرینات ۱ و ۲ ، بمعم$(a، b)$ را به‌صورت $ax+by$ بنویسید.

۴. معادلات سیالهٔ خطی زیر را حل کنید :

(آ) $8x+3y=27$.

(ب) $2x+11y=34$.

(ج) $3x+83y=-4$.

۵. ثابت کنید که به ازای کلیهٔ مقادیر n ، ۱ $=$ بمعم$(n، n+1)$.

۶. فرض کنیم عدد k این خاصیت را دارد که به ازای هر عدد صحیح مثبت n، ۱ $=$ بمعم$(n، n+k)$. ثابت کنید که $k=1$ یا $k=-1$.

۷. به‌ازای چه مقادیری از k، برای هر عدد صحیح مثبت n، تساوی ۲ $=$ بمعم$(n، n+k)$ برقرار است ؟

۸. ثابت کنید که به ازای کلیهٔ مقادیر k ، بمعم$(a، b)$ $=$ بمعم$(a+kb، b)$.

۹. ثابت کنید که هرگاه $a|c$ و $b|c$ و ۱ $=$ بمعم $(a، b)$ ، آنگاه $ab|c$. (راهنمایی : از تبصرهٔ متن درباب اعداد صحیحی که نسبت به‌هم اول‌اند، نتیجه‌گیری کنید.)

۱۰. دو کسر چنان بیابید که مخرجهای آنها بترتیب ۱۱ و ۱۳ بوده ومجموعشان $\frac{67}{143}$ باشد.

۱۱. خانوادهٔ اسمیت رستورانی را اداره می‌کنند که بهای ثابت هر وعده غذا ۱۱ دلار برای بزرگسالان و ۷ دلار برای خردسالان است (تورم!). درپایان یك روز، کل موجودی صندوق ۶۵۷ دلار است. کمترین تعداد افرادی که می‌توانسته‌اند آن روز غذا خورده باشند چند نفر بوده است؟

۱۲. مطلوب است کلیهٔ اعداد صحیح x را که خاصیت زیر را دارند: باقیماندهٔ x در تقسیم بر ۱۱ برابر ۶ ، ودرتقسیم بر ۷ برابر ۳ است.

۱۳. (آ) نشان دهید که معادلهٔ سیالهٔ $ax+by=c$ ، که $a>0$، $b>0$ ، $c>0$ فقط تعداد متناهی جواب مثبت دارد .

(ب) تعداد جوابهای مثبت معادلهٔ $16x+27y=390$ را بیابید.

۱۴. فرض کنیم a و b اعداد صحیح مثبت باشند. منظور ما ازکوچکترین مضرب مشترك a و b، که به کمم$(a، b)$ نمایش می‌دهیم، عددصحیحی است مانند m که (یکم) $m>0$ ، (دوم)

$a|m$ و $b|m$، و (سوم) هرگاه n به قسمی باشد که $a|n$ و $b|n$، آنگاه $m|n$.

(آ) فرض کنیم $a=5$، $b=3$. نشان دهید که ۱۵ کوچکترین مضرب مشترک a و b است.

(ب) فرض کنیم $a=16$، $b=24$. کمم(a, b) را بیابید. جواب همین سؤال را در مورد $a=12$، $b=15$ پیدا کنید.

(ج) ثابت کنید که a و b حداکثر یك کوچکترین مضرب مشترك دارند.

(د) ثابت کنید که a و b یك کوچکترین مضرب مشترك دارند. درحقیقت ثابت کنید که $ab/($بمعم$(a, b))$ یك کوچکترین مضرب مشترك a و b است، بنابراین

$$ab = \text{بمعم}(a, b)\,\text{کمم}(a, b)$$

(راهنمایی: از تمرین ۹ استفاده کنید.)

۱۵. فرض کنید بمعم$(a, 4)=2$ و بمعم$(b, 4)=2$. ثابت کنید که بمعم$(a+b, 4)=4$.

۱۶. فرض کنیم a، b، c اعداد صحیح باشند.

(آ) تعریفی برای بزرگترین مقسوم علیه مشترك a، b، c پیدا کنید.

(ب) ثابت کنید که اگر a، b، c توأماً صفر نباشند، آنگاه یك، وفقط یك، بزرگترین مقسوم‌علیه مشترك دارند (که با بمعم(a, b, c) نمایش داده می‌شود).

(ج) نشان دهید که بمعم (بمعم(a, b)، c) = بمعم (a, b, c).

(د) نشان‌دهید که بمعم(a, b, c) می‌تواند به صورت $ax+by+cz$ نوشته‌شود.

۱۷. تمامی نتایج مسئلهٔ ۱۶ را برای n عدد صحیح a_1، a_2، ...، a_n تعمیم دهید.

۱۸. کلیهٔ جوابهای معادلهٔ سیالهٔ $3x+5y+4z=6$ را بیابید.

۱۹. دستگاه معادلات سیالهٔ

$$x+2y+3z=4$$
$$2x-z=-1$$

را حل کنید.

۲۰. ثابت کنید که دستگاه معادلات سیالهٔ

$$3x+6y+z=2$$
$$4x+10y+2z=3$$

دارای جواب نیست.

۲۱. (آ) فرض کنیم a، b، c، d اعداد صحیحی باشند. نشان دهید که معادلهٔ سیالهٔ

$$ax+by+cz=d$$

حل‌پذیر است اگر، وفقط اگر، $d|$ بمعم$(a \text{ ، } b \text{ ، } c)$.

(ب) فرض کنیم معادلهٔ قسمت (آ) حل پذیر و $(x_\circ \text{ ، } y_\circ \text{ ، } z_\circ)$ یك جواب آن باشد، کلیهٔ جوابها را معین کنید.

۲۲. دراین تمرین، یك کران بالا جهت تعداد مراحل درآلگوریتم اقلیدسی تعیین خواهیم کرد. فرض کنیم $b \geqslant a > \circ$ و

$$b=q_\text{۱}a+r_\text{۱} \text{ ،} \qquad \circ<r_\text{۱}<a$$

$$a=q_\text{۲}r_\text{۱}+r_\text{۲} \text{ ،} \qquad \circ<r_\text{۲}<r_\text{۱}$$

$$\vdots \qquad\qquad \vdots$$

$$r_k=q_{k+\text{۲}}r_{k+\text{۱}}+r_{k+\text{۲}} \text{ ،} \quad \circ<r_{k+\text{۲}}<r_{k+\text{۱}}$$

$$\vdots \qquad\qquad \vdots$$

$$r_{n-\text{۱}}=q_{n+\text{۱}}r_n .$$

دراین صورت $r_\text{۱}>r_\text{۲}>\dots>r_n$.

(آ) نشان دهید که $b \geqslant \text{۲}r_\text{۱}$ $a \geqslant \text{۲}r_\text{۲}$.

(ب) نشان دهید که به‌ازای $k \geqslant \text{۱}$ ، داریم $r_k \geqslant \text{۲}r_{k+\text{۲}}$.

(ج) نشان دهید که $b \geqslant \text{۲}^{n/\text{۲}}$ وبنابراین $n \leqslant \text{۲}(\log b/\log \text{۲})$

(د) نشان دهید که به‌ازای $b \leqslant \text{۱۰۰۰۰}$ ، آلگوریتم اقلیدسی باید حداکثر در ۲۸ مرحله خاتمه پیدا کند.

۲۳. یك برنامهٔ کامپیوتری برای محاسبهٔ بزرگترین مقسوم‌علیه مشترك a و b بنویسید. برای یافتن تعداد دفعاتی که ممکن است آلگوریتم تقسیم را دربرنامهٔ خود تکرار کنید، می‌توانید از تمرین ۲۲ استفاده کنید.

۲۴. فرض کنیم $a_\text{۱}$ ، $a_\text{۲}$ ، ... ، a_n اعداد ناصفر باشند. m را یك کوچکترین مضرب مشترك $a_\text{۱}$ ، ... ، a_n گوییم به‌شرط آنکه (یکم) $m>\circ$، (دوم) به‌ازای $i=\text{۱} \text{ ، } \text{۲} \text{ ، } \dots \text{ ، } n$، $a_i|m$ و (سوم) هرگاه به‌ازای $i=\text{۱} \text{ ، } \dots \text{ ، } n$ داشته باشیم $a_i|m_\text{۱}$ ، آنگاه $m|m_\text{۱}$.

(آ) ثابت کنید که $a_\text{۱}$ ، ... ، a_n فقط‌وفقط یك کوچکترین‌مضرب مشترك دارند، که به کمم$(a_\text{۱} \text{ ، } \dots \text{ ، } a_n)$ نمایش داده می‌شود.

(ب) باآوردن مثال عددی مسئله را برای مقادیر مختلف $a_\text{۱}$ ، ... ، a_n تجربه کنید و درهرحالت کمم$(a_\text{۱} \text{ ، } \dots \text{ ، } a_n)$ را محاسبه کنید.

(ج) بااستفاده از تجربهٔ خود، نشان دهید که اگر همهٔ a_iها مثبت باشند، تساوی زیر همواره برقرار نیست

$$(a_1 , \dots , a_n)\text{بمعم} .(a_1 , \dots , a_n)\text{کمم} = a_1 \dots a_n$$

آیا می‌توانید تعمیمی از تمرین ۱۴(د) به‌دست دهید که برای بیش‌از دوعدد برقرار باشد؟

*۲۵. دنبالهٔ فری[1] مرتبهٔ n را به عنوان مجموعهٔ تمامی کسرهای تحویل‌ناپذیر a/b، $0 \leqslant a/b \leqslant 1$، $1 \leqslant b \leqslant n$، تعریف‌می‌کنیم. مثلاً، اولین‌سه‌دنبالهٔ فری‌عبارت‌اند از

$$\frac{1}{1} , \frac{0}{1} ; \frac{1}{1} , \frac{1}{2} , \frac{0}{1} ; \text{و} \quad \frac{1}{1} , \frac{2}{3} , \frac{1}{2} , \frac{1}{3} , \frac{0}{1} .$$

ثابت کنید:

(آ) اگر a_1/b_1 ، a_2/b_2 کسرهای مجاور یکدیگر دریك دنبالهٔ فری باشند، آنگاه $a_2b_1 - a_1b_2 = 1$.

(ب) اگر دریك‌دنبالهٔ‌فری کسرهای a_1/b_1 ، a_2/b_2 ، a_3/b_3 مجاورهم باشند، آنگاه $b_2 = b_1 + b_3$ و $a_2 = a_1 + a_3$.

۲۶. فرض کنیم m و n اعداد صحیحی باشند به‌طوری که $1 = (m , n)\text{بمعم}$.

(آ) چه وقت تساوی $\text{بمعم}(m-n , m+n) = \text{بمعم}(m , n)$ برقرار است؟

(ب) فرض کنیم a ، b ، c ، d ، m و n اعداد صحیحی باشند به‌طوری که $ad - bc = 1$، $mn \neq 0$. نشان دهید که $\text{بمعم}(m , n) = \text{بمعم}(am+bn , cm+dn)$.

*۲۷. فرض کنیم $a \geqslant 1$ و m ، n اعداد صحیح مثبت متمایز باشند. نشان دهید که

$$\text{بمعم}\left(a^{2^m}+1 , a^{2^n}+1\right) = \begin{cases} 1 & \text{اگر } a \text{ زوج باشد،} \\ 2 & \text{اگر } a \text{ فرد باشد.} \end{cases}$$

۲۸. دنبالهٔ اعدادصحیح فیبوناتچی[2] را به‌صورت زیر تعریف می کنیم: $F_0 = 1$ ، $F_1 = 1$ ، $F_2 = 1+1 = 2$ ، $F_3 = 1+2 = 3$ ، $F_4 = 2+3 = 5$ ، $F_5 = 3+5 = 8$ ، ... ، $F_{n+2} = F_{n+1} + F_n$. این‌دنباله درقرون وسطی توسط فیبوناتچی ریاضیدان ایتالیایی معرفی شده بود.

(آ) نشان دهید که هردوجملهٔ متوالی در دنبالهٔ فیبوناتچی نسبت به‌هم اول‌اند.

(ب) نشان دهید که $F_{n-1} = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \dots$.

(پس‌از مرحله‌ای، جمله‌ها صفر اند.)

1. Farey 2. Fibonacci

۲۹. بزرگترین‌مقسوم‌علیه مشترک ضرایب دوجمله‌ای $\binom{n}{۱}$ ، $\binom{n}{۲}$ ، ... ، $\binom{n}{n-۱}$ چیست؟ (به‌تمرین ۱۷ مراجعه کنید).

۳۰. فرض کنیم a و b اعداد صحیح متمایزی باشند. نشان دهید که تعداد نامتناهی عدد صحیح مانند x وجود دارد به‌طوری‌که ۱ = بمعم$(a+x \text{ ، } b+x)$.

۳۱. فرض کنیم a ، b ، c ، d اعدادی صحیح باشند به‌قسمی که $b\neq d$ ، و ۱ = بمعم$(c \text{ ، } d)$ = بمعم$(a \text{ ، } b)$. نشان‌دهید که $a/b+c/b$ عدد صحیح نیست.

۳۲. فرض کنیم a ، b اعداد صحیح باشند ، و $b\neq ۰$. فرض کنیم آلگوریتم تقسیم را به‌کار ببریم

$$a=bq_۱+r_۱$$
$$b=r_۱q_۲+r_۲$$
$$r_۱=r_۲q_۳+r_۳$$
$$\vdots$$

نشان دهید که کسر مسلسل زیر را برای $\frac{a}{b}$ داریم

$$\frac{a}{b}=q_۱+\cfrac{۱}{q_۲+\cfrac{۱}{q_۳+\cdots}}$$

۳۳. نشان دهید که هرعدد صحیح زوج می‌تواند به‌صورت $a-b$ نوشته شود به‌طوری که بمعم$(a \text{ ، } n)$ = بمعم$(b \text{ ، } n)$ = ۱.

*۳۴. فرض‌کنیم m و n اعداد صحیح مثبت باشند، و بمعم$(m \text{ ، } n)$ $=d$. نشان دهید که ۱ − ۲^d = بمعم$(۲^m-۱ \text{ ، } ۲^n-۱)$.

۴.۲ یکتایی تجزیه به‌عوامل اول

سرانجام آماده شده‌ایم تا نتیجهٔ اصلی این فصل‌را، که یکتایی تجزیهٔ اعدادصحیح به عوامل اول است، ثابت‌کنیم. ابتدا «بلوکهای ساختمانی» را تعریف‌می‌کنیم.

تعریف ۱ : عدد اول (یا به‌طورخلاصه اول) عددصحیحی مانند p است به‌طوری‌که

(یکم) $p>۱$ ؛

(دوم) اگر $a|p$ ، آنگاه $a=\pm ۱$ یا $a=\pm p$.

برای‌مثال، ... ، ۱۱ ، ۷ ، ۵ ، ۳ ، ۲ $=p$ اول‌هستند. چندقضیهٔ مقدماتی‌رابه‌صورت لم بیان می‌کنیم.

لم۲: اگر $n>1$ آنگاه n حاصلضرب چند عدد اول است.

باید تأکید شودکه یك عدد اول، خود حاصلضرب اعداد اول تلقی مـی‌شود ، یعنی حاصلضرب یك عدد اول.

برهان‌لم۲: اگراعدادصحیح بزرگتراز یكmوجود داشته باشند که‌حاصلضرب‌اعداد اول‌نباشند، آنگاه بنا به‌اصل خوشترتیبی، کوچکترین‌عددی ازاین‌گونه موجود است که آن‌راmمی‌نامیم. دراین‌صورت m نمی‌تواند اول باشد، ولـذا، بنابرتعریف عدد اول، برای m مقسوم‌علیهی مانند a وجود دارد $(a|m)$ به‌طوری‌کـه $a\neq\pm 1$ و $a\neq\pm m$. مـی‌توانیم a را مثبت فرض کنیم.می‌نویسیم $m=ab$. دراین‌صورت $1<a, b<m$ (قضیهٔ۲.۲ قسمت (چهارم)). چون m کوچکترین عدد صحیح بزرگتراز ۱ است‌کـه به‌صورت حاصلضرب اعـداد اول نیست، a و b بایستی به‌صورت حـاصلضرب اعـداد اول باشند، مثلاً، $a=p_1p_2\cdots p_r$ و $b=q_1q_2\cdots q_s$ ، دراینجا p_1 ، ... ، p_r و q_1 ، ... ، q_s معرف اعداد اول‌اند. پس

$$m=ab=p_1\cdots p_rq_1\cdots q_s$$

بصورت حاصلضربی از اعداد اول است. این متناقض باانتخاب m است ولذا لم۲ اثبات می‌شود. ■

لم۳: (لم‌اقلیدس) فرض‌کنیم p عددی اول باشد. دراین صورت $p|ab$ ایجاب می‌کندکـه $p|a$ یا $p|b$.

برهان: این نتیجهٔ بلافصل قسمت (سوم) ازقضیهٔ ۶.۳ می‌باشد، زیرا $p\nmid a$ ایجاب می‌کند که ۱ = بمعم(a و p) ، وبنابراین $p|b$. ■

نتیجهٔ ۴: فرض‌کنیمp عددی اول باشد. دراین‌صورت $p|a_1a_2\cdots a_r$ ایجاب می‌کندکـه به‌ازای i ای $1\leqslant i\leqslant r$ ، $p|a_i$.

برهان: تمرین. از استقرا استفاده کنید. ■

قضیهٔ۵: (یکتایی تجزیه به‌عوامل‌اول). فرض‌کنیم $n>1$ عددصحیحی باشد. دراین‌صورت

$$n=p_1p_2\cdots p_r$$

حاصلضربی از اعداد اول است واین تجزیه یکتاست. منظور ازیکتایی این است که اگر

$$n = p_1 \cdots p_r = q_1 \cdots q_s ،$$

کـه p_1 ، … ، p_r و q_1 ، … ، q_s اعـداد اول هستند، آنگاه $r = s$ و بعداز مرتب کـردن دوبارهٔ q_1 ، … ، q_s داشته باشیم $p_1 = q_1$ ، … ، $p_r = q_r$.

واضح است که ما بایستی اجازهٔ مرتب کردن مجدد را به q_iها بدهیم تاعوامل متناظر مساوی باشند، زیرا، برای‌مثال،

$$۱۲ = ۲ \times ۲ \times ۳ = ۲ \times ۳ \times ۲ = ۳ \times ۲ \times ۲$$

برهان قضیهٔ ۵: باتوجه به لم ۲ می‌دانیم که هرعددصحیح n بـزرگتر از ۱ را می‌توان بـه حاصلضرب عوامل اول تجزیه کرد. اگر اعداد صحیحی چون $n > ۱$ وجود داشته باشند که تجزیهٔ‌آنها به‌عوامل اول یکتا نباشد، آنگاه کوچکترین‌عددی ازاین‌گونه موجود خواهدبود (اصل خوشترتیبی)؛ آن‌را m می‌نامیم. فرض کنیم

$$m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

دراین‌صورت $p_1 | q_1 q_2 \cdots q_s$ ولذا بنابرنتیجهٔ ۴ ، به‌ازای مقداری از i ، $p_1 | q_i$. بامرتب کردن مجدد q_jها می‌توانیم فرض کنیم $i = ۱$. بنابراین $p_1 | q_1$. چون q_1 اول است، داریم $p_1 = \pm ۱$ یا $p_1 = \pm q_1$. چون $p_1 > ۱$ ، داریم $p_1 = q_1$. پس می‌توانیم $p_1 = q_1$ را دربسط m حذف کنیم وبه‌دست‌آوریم

$$m_1 = p_2 \cdots p_r = q_2 \cdots q_s \cdot$$

اما $m > m_1$ (قضیهٔ ۲.۲ (چهارم)). بنابراین، چون m کوچکترین عدد صحیح بزرگتراز ۱ بدون تجزیهٔ یکتا بـود، داریـم $r - ۱ = s - ۱$ ، و بعداز مـرتب کـردن مجـدد q_iها ، $p_2 = q_2$ ، … ، $p_r = q_s$. پس $r = s$ و $p_1 = q_1$ ، … ، $p_r = q_r$. بنابراین، بالاخره تجزیهٔ m به‌عوامل اول بایستی یکتا باشد. این تناقض قضیهٔ ۵ را اثبات می‌کند. ■

نتیجهٔ ۶: اگر $n < -۱$ ، آنگاه اعداد اول p_1 ، … ، p_r موجودند به‌طوری که

$$n = -p_1 \cdots p_r$$

واین تجزیه به‌عوامل اول یکتاست.

برهان: درواقع، $-n$ درفرض قضیهٔ ۵ صدق می‌کند. ■

دراینجا، باید به‌نکته‌ای اشاره کنیم که ممکن است دانشجویان را سردرگم سازد. در تعریف ۱، چرا ما ۱ را از اول بودن مستثنا کردیم؟ البته، در ریاضیات برای نامی که به‌اشیاء می‌دهیم هیچ‌گونه تقدسی وجود ندارد. ولی، این نامها به‌دقت انتخاب مـی‌شوند تا ایـن

مفاهیم‌را، تاآنجا که میسراست، روشن سازند. دراین مورد، اگر ما اجازه داده بودیم که ۱ عددی اول باشد، آنگاه قضیهٔ ۵ غلط می بود. مثلا ،

$$۶ = ۲ \times ۳ = ۲ \times ۳ \times ۱ = ۱ \times ۲ \times ۳ \times ۱ = ۱ \times ۲ \times ۳ \times ۱ \times ۱$$

وغیره. بنابراین، اگرما ۱ را عدد اول بنامیم یکتایی تجزیه ازمیان می‌رود.

یك تذکرهم دربارهٔ اثبات قضیهٔ ۵ بجاست. اگرشما به‌این اثبات که همواره تجزیه به‌اعداد اول ممکن است (لم۲) واثبات اینکه تجزیه یکتاست نگاه کنید، ممکن‌است‌اشتباهاً معتقد شوید که اثباتها تقریباً از دشواری مساوی‌برخوردارند. ولی چنین نیست، و همچنانکه قبلا متذکرشده‌ایم، یکتایی نتیجهٔ به‌مراتب عمیقتری است. اگرشما هردو اثبات را بدقت بررسی کنید، خواهید دید که اثبات وجودی ازچیزی جزاصل خوشترتیبی وحقایق پیش‌پا‌افتاده درمورد بخشپذیری استفاده نمی کند. از سوی دیگر ، دراثبات یکتایی جان‌کلام را این‌حکم تشکیل می‌دهد که $q_s \cdots q_1$ | p_1 ایجاب می کند که به‌ازای بعضی مقادیر i ، $p_1 | q_i$. این اصلا همان لم۳، یعنی، قضیهٔ ۶.۳ (سوم) است ونتیجهٔ اخیر برموضوع نسبتاً غیرپیش‌پا‌افتاده‌ای درباب بزرگترین مقسوم‌علیه مشترك دربخش۳ استوار شده بود.

این بخش را باگردآوری مطالب‌بیشتری درمورد اعداد اول وتجزیه اعداد به عوامل اول به‌پایان می‌رسانیم. مطالب اولیه‌خود به‌این‌سؤال مربوط می‌شوند که چه‌تعداد عدد اول موجود است و چگونه (درمیان اعداد صحیح) توزیع شده‌اند . این پرسشها به‌زیباترین و ریشه‌دارترین‌نتایج درنظریهٔ اعداد که هنوزهم‌موضوع‌پژوهش زیادی هستند، منجرمی‌شوند. مابه‌نتایج ۷و۸ زیرا اکتفا می کنیم. علاقه‌مندان می توانند به‌ضمیمهٔ آ، که شامل اثبات دیگری ازنتیجهٔ ۷ و بهتراز آن است مراجعه‌کنند. اثباتها برحساب دیفرانسیل و انتگرال تکیه دارند وبه‌خواننده دید مختصری از موضوع دلپذیر وعمیق‌کاربردهای حساب دیفرانسیل و انتگرال درنظریهٔ اعداد (به‌نام نظریهٔ تحلیلی اعداد) می‌دهد.

نتیجهٔ ۷ : (اقلیدس). بینهایت عدد اول وجود دارد.

برهان: اگرچنین نباشد، آنگاه تعدادی متناهی، مثلا k ، عدد اول وجود خواهد داشت که آنهارا با p_1 ، ... ، p_k نمایش‌می‌دهیم. قرارمی‌دهیم

$$n = p_1 p_2 \cdots p_k + 1 .$$

می‌دانیم (لم۲ یا قضیهٔ۵) که عدد اولی مانند p موجود است به‌طوری که $p|n$. چون‌pاول و p_1 ، ... ، p_k کلیهٔ‌اعداد اول می‌باشند، بایستی iی باشد به‌طوری که $p = p_i$. بنابراین، $p | p_1 \cdots p_k$. این‌حقیقت، به‌انضمام $p|n$، ایجاب‌می کند که $p|1$. این تناقض نتیجه‌را‌ثابت می کند. ■

نتیجهٔ ۸ : مابین اعداد اول متوالی، شکافهای به‌دلخواه بزرگی وجود دارند[۱] .

برهان: حکم قضیه این است که به‌ازای هرعددصحیح مثبتn ، دنباله‌ای از n عـدد صحیح متوالی‌وجود دارد که‌هیچیك اول‌نیستند. در واقع، اگرحاصلضرب $n\times\dots\times ۳\times ۲\times ۱$ را به $n!$ نمایش دهیم آنگاه

$$(n+۱)!+۲ \text{ ، } (n+۱)!+۳ \text{ ، } \dots \text{ ، } (n+۱)!+(n+۱)$$

دنبالـه‌ای از n عـدد صحیح است. اول نبودن هیچیك از آنها واضح است، زیرا بـه‌ازای $۲\leqslant k\leqslant n+۱$

$$k\,|\,(n+۱)!+k$$

و $۲\leqslant k<(n+۱)!+k$. بنابراین، $(n+۱)!+k$ مقسوم‌علیهی غیراز ± ۱ و خودش دارد ولذا اول‌نیست. ■

بالاخره روشی برای تجزیهٔ اعداد صحیح به عوامل اول و تولید اعـداد اول ارائه می‌کنیم. روش تولید اعداد اول، غربال اراتستن[۲] نامیده مـی‌شود. ازایـن‌رو غربال نامیده می‌شود که روش‌آن شبیه‌به گرفتن غربالی است‌پر از اعداد صحیح و بیرون ریختن بیشتراعداد صحیح ازسوراخهای‌آن، به‌طوری‌که درخاتمهٔ عمل فقط اعداد اول درغربال‌باقی‌می‌مانند. با قضیهٔ زیرشروع می‌کنیم:

قضیهٔ ۹ : اگر $n>۱$ عددصحیح غیراولی باشد، آنگاه عـددی اول مانند p وجـود دارد چنان‌که

$$p|n \text{ و } p\leqslant\sqrt{n} \text{ .}$$

برهان: چون n اول نیست، اعداد صحیح a و b وجود دارندچنان‌که

$$n=ab \text{ و } ۲\leqslant a\leqslant b<n\text{ .}$$

پس $n=ab\geqslant a^۲$ یـا $a\leqslant\sqrt{n}$. فرض‌کنیم p عـدد اولی باشد چنان‌که $p|a$. درایـن صورت $p|n$ و $p\leqslant a\leqslant\sqrt{n}$. ■

---

۱. ازطرف دیگر، درمسئله‌ای حل نشده عنوان شده استکـه‌آیا تعدادی نامتناهی از زوجهای اعداد اول $(p\text{ ، }p+۲)$ ، که p و $p+۲$ عدد اول‌اند مـوجود است (دراینجا فاصله۲است). (گاهی‌اوقات‌آنهارا اعداد اول دوقلو نامند(مترجم)). امثله‌عبارت‌اند از $(۳\text{ ، }۵)$ ، $(۵\text{ ، }۷)$ ، $(۱۱\text{ ، }۱۳)$ ، $(۱۷\text{ ، }۱۹)$ ، و $(۲۹\text{ ، }۳۱)$.

2. Eratosthenes

برای مثال، ۱۸ اول نیست، و $۲ | ۱۸$ و $\sqrt{۱۸} \geqslant ۲$. همچنین ۲۵ اول نیست، و $۵ | ۲۵$ و $\sqrt{۲۵} \geqslant ۵$.

لذا، برای تحقیق اینکه عدد صحیح مفروض بزرگتر از یك n اول است یا نه کافی است تحقیق کنیم که n بر عدد اول $p \leqslant \sqrt{n}$ بخشپذیر است یا نه. اگر چنین نباشد، n اول است. درحالت کلی این روش مقدار زیادی از کار ما را کم می کند.

به‌عنوان مثال، آیا $n = ۲۷۱$ اول است؟ $۱۷ > \sqrt{۲۷۱} > ۱۶$، و بنابراین یا ۲۷۱ اول است یا عدد اولی چون $p \leqslant ۱۶$ موجود است به‌طوری که $p | ۲۷۱$. اعداد اول نابیشتر از ۱۶ عبارت‌اند از ۲، ۳، ۵، ۷، ۱۱، و ۱۳. اینك ما باید عملیات اندکی انجام دهیم و ببینیم آیا یکی از این اعداد ۲۷۱ را عاد می کند. هیچکدام از آنها ۲۷۱ را عاد نمی کند (عمل تقسیم را انجام دهید). بنابراین، ۲۷۱ اول است.

فکر فوق را می‌توان برای تولید اعداد اول به‌کار گرفت. روشی که به‌دست می‌آید غربال اراتستن است. فرض کنیم می‌خواهیم همهٔ اعداد اول نابیشتر از n را بیابیم. می‌دانیم، هر عدد غیر اول بر عدد اولی نابیشتر از $\sqrt{n}$ بخشپذیر است. بنابراین اعداد صحیح از ۲ تا n و خود n را فهرست می کنیم. همهٔ مضارب ۲ غیر از خود ۲ را خط می‌زنیم. عدد صحیح بعدی در فهرست، عدد اول ۳ است. کلیهٔ مضارب ۳ غیر از خود ۳ را خط می‌زنیم. عدد صحیح بعدی در فهرست که خط نخورده است عدد اول ۵ است (۴ خط خورده است زیرا مضرب ۲ بوده است). کلیهٔ مضارب ۵ غیر از خود ۵ را خط می‌زنیم. این روش را ادامه می‌دهیم. فرض کنیم همهٔ مضارب p غیر از p را خط زده‌ایم. عدد صحیح بعدی مانده در فهرست عدد اول بعد از p خواهد بود؛ آن را q می‌نامیم. این روش را تا جایی که $q > \sqrt{n}$ ادامه می‌دهیم، و سپس از ادامهٔ عمل دست می کشیم. کلیهٔ اعداد باقیمانده اعداد اول ما بین ۲ و n هستند، همچنانکه کلیهٔ اعداد صحیح دیگر که خط خورده‌اند مضارب اعداد اول نابیشتر از $\sqrt{n}$ هستند.

مثال ۱۰: $n = ۳۰$. چون $۶ > \sqrt{۳۰} > ۵$، بایستی کلیهٔ مضارب ۲، ۳، و ۵ را خط بزنیم

۲	۳	~~۴~~	۵	~~۶~~	۷	~~۸~~	~~۹~~	~~۱۰~~	
۱۱	~~۱۲~~	۱۳	~~۱۴~~	~~۱۵~~	~~۱۶~~	۱۷	~~۱۸~~	۱۹	~~۲۰~~
~~۲۱~~	~~۲۲~~	۲۳	~~۲۴~~	~~۲۵~~	~~۲۶~~	~~۲۷~~	~~۲۸~~	۲۹	~~۳۰~~

بنابراین، فهرست اعداد اول نابیشتر از ۳۰ عبارت است از ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳، و ۲۹.

توجه داشته باشید که برای تعیین کلیهٔ اعداد اول تا ۱۰۰، بایستی فقط مضارب یك عدد اول دیگر، یعنی ۷، را خط بزنیم. پس این روش فوق‌العاده مؤثر است.

۴.۲ تمرینات

۱. اعداد صحیح زیر را به‌صورت حاصلضرب عوامل اول بنویسید: ۱۳ ، ۱۶ ، ۲۸ ، ۱۴۴ ، ۱۶۹ ، ۴۴ ، ۱۰۰ .

۲. به‌کمك غربال اراتستن کلیهٔ اعداد اول نابیشتر از ۱۰۰ را تعیین کنید. (یافتن کلیهٔ اعداد اول نابیشتر از ۵۰۰ ، بااستفاده از غربال، نبایستی بیشتر از یك ساعت از وقت شمارا بگیرد وبنابراین جدول ۱ آخر کتاب رامقابله کنید. این تاحد زیادی بستگی دارد به‌اینکه شما تاچه اندازه از اشتباه براثر خستگی درامان مانده باشید.)

۳. یك برنامهٔ کامپیوتری برای تعیین کلیهٔ اعداد اول $p \leqslant n$ با استفاده از غربال اراتستن بنویسید. اگر کامپیوتری دراختیار دارید، فهرستی از کلیهٔ اعداد اول نابیشتر از ۱۰۰۰ تهیه کنید.

۴. عدد صحیح ناصفر n مفروض است، A_n رامساوی مجموعهٔ اعداد اول $p|n$ قرارمی‌دهیم. بنابراین $A_1 = \varnothing$ ، $A_2 = \{2\}$ ، $A_6 = \{2 , 3\}$ ، و $A_{12} = \{2 , 3\}$. احکام مفید زیر را ثابت کنید:

(آ) $1 =$ بمعم(m , n) اگر، وفقط اگر، $A_n \cap A_m = \varnothing$.

(ب) $n|m$ ایجاب می‌کند که $A_n \subseteq A_m$ (و بنابراین $A_n \nsubseteq A_m$ ایجاب می‌کند که $n \nmid m$).

(ج) اگر $d = nx + my$ ، آنگاه $A_d \supseteq A_m \cap A_n$.

(د) اگر $d = mn$ ، آنگاه $A_d = A_n \cup A_m$.

(ه) اگر بمعم$(m , n) = d$ ، آنگاه $A_d = A_n \cap A_m$.

۵. به‌ازای هرزوج عددصحیح مفروض بزرگتراز ۱ مانند m و n ، نشان دهید که می‌توان آنهارا به‌صورت

$$m = p_1^{a_1} \dots p_k^{a_k}$$
$$n = p_1^{b_1} \dots p_k^{b_k} ,$$

نوشت که درآن p_1 ، ... ، p_k اعداد اول متمایز، و a_1 ، ... ، a_k ، b_1 ، ... ، b_k اعداد صحیح نامنفی هستند (مثل $12 = 2^2 \times 3 \times 5^0$ و $15 = 2^0 \times 3 \times 5$).[1]

۶. بااستفاده ازعبارات تمرین ۵، نشان دهید که

(آ) $m|n$ اگر، وفقط اگر، $a_1 \leqslant b_1$ ، ... ، $a_k \leqslant b_k$.

---

۱. درواقع، هرعددصحیح ناصفر m رامی‌توان به‌صورت $\pm \prod_p p^{\alpha_p}$ نوشت که در آن $\alpha_p \geqslant 0$ و فقط تعدادی متناهی α_p ناصفراست، حاصلضرب روی‌کلیه‌ی اعداد اول می‌باشد (مترجم).

(د) بمعم$(m ، n)=p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}$ ، که مینیموم $(a_i ، b_i)=c_i(1\leqslant i\leqslant k)$.

(ج) کمم$(m ، n)=p_1^{d_1}p_2^{d_2}\dots p_k^{d_k}$ ، که ماکزیموم $(a_i ، b_i)=d_i(1\leqslant i\leqslant k)$.

(کمم در تمرین ۱۴ بخش ۳.۲ تعریف شده است.)

۷. از تمرین ۶ استفاده کنید تا نشان دهید که

$$nm=(\text{بمعم}(m ، n))(\text{کمم}(m ، n))،$$

و بنابراین اثبات دیگری از تمرین ۱۴ (د) بخش ۳.۲ ارائه دهید.

۸. ثابت کنید که به‌ازای اعداد صحیح مثبت m و n گزارهٔ

اگر $a^m|b^n$ ، آنگاه $a|b$

راست است اگر، و فقط اگر، $m\geqslant n$.

۹. فرض کنیم ۲ $a\geqslant$ ، ۲ $n\geqslant$. نشان دهید که اگر a^n-1 عددی اول باشد، آنگاه $a=2$ و n عددی است اول. (راهنمایی: به‌تمرین ۱۷ بخش ۲.۲ مراجعه کنید.) اعداد اول به‌این صورت، اعداد اول مرسن[1] نامیده می‌شوند.

۱۰. (این تمرین برای آنهایی است که دسترسی به‌کامپیوتر دارند.) فرض کنیم $\pi(x)$ تعداد اعداد اول تا بیشتر از x باشد. برنامه‌ای را که برای تمرین ۳ نوشتید برای محاسبهٔ (آ) $\pi(x)-(x/\log x)$ و (ب) $\pi(x)/(x/\log x)$ به‌ازای مقادیر ۱۰۰، ۲۰۰، ۳۰۰، ۴۰۰، ...، ۱۰۰۰۰ برای x به‌کار برید. برمبنای داده‌های عددی به‌دست آمده، آیا می‌توانید حدسی بزنید؟ (همین محاسبات توسط گاوس انجام شده بودند.) توجه: $\log x$ به‌معنی لگاریتم طبیعی x است.

۱۱. فرض کنیم $f(x)=a_0x^n+\dots+a_n$ بسجمله‌ای ناصفر[2] باضرایب صحیح باشد. نشان دهید که $f(k)$ ، به‌ازای تعداد نامتناهی عدد صحیح k ، عدد مرکب است. (راهنمایی: مسئله را به‌حالتی که $|a_n|>1$ تبدیل کنید.)

۱۲*. نشان دهید که به‌ازای $n>1$ ، عدد $1+\frac{1}{2}+\dots+\frac{1}{n}$ عدد صحیح نیست.

۱۳*. نشان دهید که به‌ازای $n\geqslant 1$ ، عدد $1+\frac{1}{3}+\dots+\frac{1}{(2n+1)}$ عدد صحیح نیست.

۱۴. فرض کنیم $\frac{a}{b}$ کسری تحویل‌ناپذیر (یعنی، ۱ = بمعم$(a ، b)$) باشد. فرض کنیم $\frac{a}{b}$

---

1. Mersenne

۲. به‌جای ناصفر باید ناثابت باشد، زیرا اگر $f(x)=p$ عددی اول باشد، آنگاه به‌ازای هیچ kای مرکب نیست، چراکه همواره مقدارش عدد اول p است (مترجم).

صفری[1] از بسجملهٔ $a_0x^n+\dots+a_n$ که a_0، …، a_n اعداد صحیح‌هستند و $a_0\neq 0$، باشد. نشان‌دهید که $a|a_n$، $b|a_0$.

۱۵. فرض کنیم p عددی اول و a عدد صحیحی باشد چنان‌که $1<a<p$. نشان دهید که $\binom{p}{a}$ بر p بخشپذیر است.

۱۶. فرض‌می‌کنیم p عددی اول، و a و b اعداد صحیح باشند. نشان دهید که a^p-b^p یا نسبت به p اول است یا $p^2|a^p-b^p$. (راهنمایی: از تمرین ۱۵ استفاده کنید.)

۱۷. ثابت‌کنید که به‌ازای هر n، $n^{34}-9$ هیچگاه اول نیست.

۱۸. (هیلبرت[2]) فرض کنیم R معرف گردایهٔ کلیهٔ اعداد صحیح‌مثبت به‌صورت $4k+1$، k عددی صحیح باشد.

(آ) نشان دهید که حاصلضرب هردوعضو R باز عضوی از R است.

(ب) عضو m از R را عضو اول گوییم هرگاه تنها اعضای R که m را عاد می‌کنند ۱ و m باشند. کلیهٔ اعضای اول نابیشتراز ۱۰۰ را بیابید.

(ج) نشان دهید که هرعددصحیح از R می‌تواند به‌صورت حاصلضربی از اعضای‌اول نوشته شود.

(د) نشان دهید که تجزیهٔ قسمت (ج) لزوماً یکتا نیست.

۱۹. فرض کنیم P_n معرف nامین عدد اول باشد.

(آ) نشان دهید که به‌ازای $n\geqslant 4$، $p_{n+1}^2<p_1p_2\cdots p_n$.

(ب) نشان دهید که $p_n<2^{2^n}$.

۲۰. قضیهٔ مشهوری به‌نام‌اصل موضوع برتراند[3] حکم می‌کند که به‌ازای هر $n\geqslant 1$ عدد اولی مانند p موجود است به‌طوری که $n\leqslant p\leqslant 2n$.

(آ) اصل برتراند را به‌ازای $n\leqslant 100$ تحقیق کنید.

(ب) اصل برتراند را فرض کنیدو تحقیق کنید که $p_n\leqslant 2^n$، که دراینجا p_n معرف nامین عدد اول است.

---

۱. ریشه‌های معادلهٔ $f(x)=0$ را معمولا صفرهای $f(x)$ می‌خوانند (مترجم).

2. Hilbert

3. Bertrand

*۲۱. نشان دهید که تنها اعداد صحیح مثبت ممکنی که مجموع اعداد صحیح مثبت[1] متوالی نیستند توانهای ۲ هستند.

۲۲. فرض کنیم $d_1(n)$ نمایش تعداد مقسوم‌علیه‌های n به‌صورت $4k+1$ و $d_3(n)$ نمایش تعداد مقسوم‌علیه‌های n به‌صورت $4k+3$ باشد. نشان‌دهید که $d_1(n) \geqslant d_3(n)$.

۲۳. (آ) نشان دهید که $\sqrt{5}$، $\sqrt[3]{3}$ و $\sqrt[7]{2}$ اعداد گویا نیستند.

(ب) فرض کنیم a عدد صحیح مثبتی باشد و $a = p_1^{e_1} \dots p_t^{e_t}$ تجزیهٔ a به حاصلضرب توانهای اعداد اول متمایز p_1، ...، p_t باشد. نشان‌دهید که $\sqrt[m]{a}$ عددی گویاست اگر، و فقط اگر، $m|e_1$، $m|e_2$، ...، و $m|e_t$.

---

۱. درمتن انگلیسی کتاب کلمهٔ مثبت نیامده است. به‌نظر مترجم این فرض ضروریست (مترجم).

ضمیمهٔ آ

برهان اویلر برای نامتناهی بودن تعداد اعداد اول

در این ضمیمه، برهان دیگری جهت اثبات نامتناهی بودن تعداد اعداد اول ارائه می‌دهیم. برهانی که در اینجا ارائه می‌شود متعلق به لئونهارد اویلر[1] ریاضیدان قرن هیجدهم سویسی است. تازگی این روش در این است که فکر حساب دیفرانسیل و انتگرال را با حساب اعداد صحیح مرتبط می‌کند. تابع ζ از متغیر s را با ضابطهٔ

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

درنظر می‌گیریم . این تابع، به احترام غول ریاضیات آلمان برنهارد ریمان[2] که در ۱۸۵۹ میلادی، به‌طور اصولی و منظم خواص کامل این تابع را موردمطالعه قرارداد، تابع زتای ریمان نامیده شده است. در واقع، سری نامتناهی $\zeta(s)$ اولین‌بار توسط اویلر ، تقریباً صدسال قبل ازآنکه ریمان به‌این تابع بپردازد، معرفی شده بود.

از روی آزمون انتگرال، سری $\zeta(s)$ به‌ازای $s>1$ همگراست و بنابراین ، به‌ازای $s>1$ ، تابعی از s تعریف می‌کند. بعلاوه ، چون

$$\frac{1}{n^s}\geqslant\int_n^{n+1}\frac{dx}{x^s},$$

می‌بینیم که

$$\sum_{n=1}^{\infty}\frac{1}{n^s}\geqslant\int_1^{\infty}\frac{dx}{x^s}=\frac{1}{s-1}\,.$$

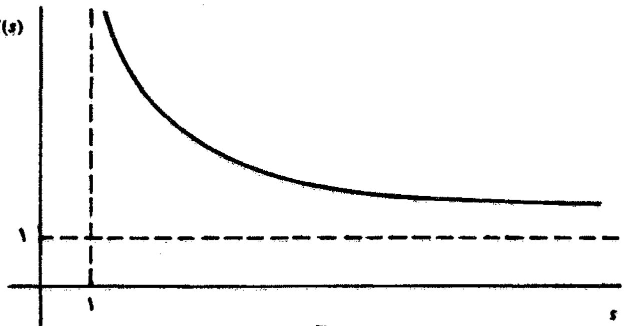
---

1. Leonhard Euler 2. Bernhard Riemann

بنابراین، می‌بینیم که

$$\lim_{s\to 1+}\zeta(s)=\infty \cdot$$

نمودار $\zeta(s)$، همچنانکه شما به‌سادگی می‌توانید بررسی کنید، به‌گونه‌ای است که درشکل آ.۱ داده شده است.



شکل آ.۱

ما به مفهوم حاصلضرب نامتناهی احتیاج خواهیم‌داشت. تعریف‌آن ساده و به مجموع نامتناهی خیلی شبیه می‌باشد. یعنی اگر $a_۱$ ، $a_۲$ ، $a_۳$ ، ... دنباله‌ای از اعداد حقیقی باشد تعریف می‌کنیم[۱].

$$\prod_{n=۱}^{\infty} a_n=\lim_{N\to\infty}\prod_{n=۱}^{N}a_n=\lim_{N\to\infty} a_۱a_۲\cdots a_N \cdot$$

ارتباط $\zeta(s)$ با اعداد اول درقضیهٔ زیرآمده است.

قضیهٔ ۱ : (دستور حاصلضرب)

$$\zeta(s)=\prod_p\left(۱-\frac{۱}{p^s}\right)^{-۱} \qquad \text{به‌ازای } s>۱$$

باید علامت‌گذاری قضیهٔ ۱ را تفسیر کنیم. منظور ازنماد $\prod_p$ حاصلضرب روی کلیهٔ اعداد اول p است. بنابراین، اگر $p_۱<p_۲<p_۳<\dots$ نمایش کلیهٔ اعداد اول که بترتیب فهرست شده‌اند باشد، آنگاه قضیهٔ ۱ بیان می‌کند که اگرتعدادی نامتناهی عدد اول موجود باشند. آنگاه

$$\zeta(s)=\prod_{m=۱}^{\infty}\left(۱-\frac{۱}{p_m^s}\right)^{-۱}=\lim_{N\to\infty}\prod_{m=۱}^{N}\left(۱-\frac{۱}{p_m^s}\right)^{-۱},$$

۱. این تعریف حاصلضرب نامتناهی مغایر با تعریف معمولی‌آن است‌که درکتابهای آنالیز داده می‌شود. به‌دلایل‌فنی، معمولا نیاز به‌این‌است‌که حد ناصفرباشد. ولی، تعریف ما برای‌مقصودمان کفایت می‌کند.

یا ، اگر درست M عدد اول موجود باشد

$$\zeta(s)=\prod_{m=1}^{M}\left(1-\frac{1}{p_m^s}\right)^{-1}$$

برهان قضیهٔ ۱: چون $1>\frac{1}{p_m^s}>0$ ، دستور سری‌هندسی

$$\frac{1}{1-\frac{1}{p_m^s}}=1+\frac{1}{p_m^s}+\frac{1}{p_m^{2s}}+\frac{1}{p_m^{3s}}+\cdots \qquad (*)$$

را داریم. این مجموع شامل فقط عده‌ای از جملات سری

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

است، یعنی آن جمله‌هایی که $n=p_m^k$ یعنی توانهای p_m است. می‌خواهیم ببینیم وقتی که اولین دو سری (*) را درهم ضرب کنیم ($p_1=2$ ، $p_2=3$) چه پیش می‌آید[1] .

$$\left(1-\frac{1}{2^s}\right)^{-1}\left(1-\frac{1}{3^s}\right)^{-1}=\left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\cdots\right)\left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\cdots\right)$$
$$=\sum\frac{1}{n^s},$$

که دراینجا مجموع روی کلیهٔ n هایی است که عوامل آنها فقط ۲ و ۳ هستند.

به همین طریق

$$\left(1-\frac{1}{2^s}\right)^{-1}\left(1-\frac{1}{3^s}\right)^{-1}\left(1-\frac{1}{5^s}\right)^{-1}=\sum\frac{1}{n^s}, \qquad (1)$$

که مجموع روی کلیهٔ n هایی است که عوامل آنها فقط ۲ ، ۳ و ۵ هستند. و در حالت کلی

$$\prod_{m=1}^{N}\left(1-\frac{1}{p_m^s}\right)^{-1}=\sum\frac{1}{n^s}, \qquad (2)$$

که مجموع روی کلیهٔ n هایی است که عوامل آنها فقط p_1 ، p_2 ، ... ، p_N هستند. نکتهٔ مهمی را ندیده گرفته‌ایم. مثلا ، یکبار دیگر معادلهٔ (۱) را از نظر بگذرانیم. از کجا می‌دانیم که هرعدد صحیح n که فقط عوامل اول ۲ و ۳ و ۵ دارد فقط وفقط یکبار ظاهر می‌شود. این امر که $n=2^a3^b5^c$ در بسط ظاهر می‌شود بدیهی است؛ تنها راه برای آنکه یك عدد n دوبار یا بیشتر ظاهرشود آن است که برای n بسط دیگری به‌صورت $2^{a'}3^{b'}5^{c'}$ داشته

---

۱. فرض می‌کنیم‌که متعلم با قضیهٔ زیر در مورد سریهای نامتناهی آشناست . اگر Σa_n و Σb_m سریهای همگرا باجملات مثبت باشند، آنگاه $\sum_{m,n}a_nb_m$ همگرا ومساوی $(\Sigma a_n)(\Sigma b_m)$ می‌باشد.

باشیم، که می‌دانیم چنین‌چیزی بنابر یکتایی تجزیه به‌عوامل اول امکان‌ندارد. همین‌ملاحظات برای معادلهٔ (۲) صادق است. در واقع، می‌تـوان قضیهٔ ۱ را یك بیان تحلیلیِ از قضیهٔ یکتایی تجزیه گرفت.

اگر فقط تعداد متناهی عدد اول موجود باشد، مثلا M عدد اول‌آنگاه، معادلهٔ (۲) به ازایِ $N=M$ اثبات قضیه را به‌پایان می‌رسانـد. در غیراین‌صورت، تعدادی نامتناهی عدد اول موجود است و $p_N \to \infty$ وقتی‌که $N \to \infty$. برای تمام‌کردن اثبات بایدنشان دهیم که

$$\lim_{N\to\infty}\left|\zeta(s)-\prod_{m=1}^{N}\left(1-\frac{1}{p_m^s}\right)^{-1}\right|=0. \qquad (۳)$$

بنابر(۲)،

$$\left|\zeta(s)-\prod_{m=1}^{N}\left(1-\frac{1}{p_m^s}\right)^{-1}\right|=\sum\frac{1}{n^s}$$
$$\leqslant\sum_{n=p_N+1}^{\infty}\frac{1}{n^s},$$

که اولین جمع روی‌کلیهٔ nهایی است‌که حداقل یك عامل اول $p>p_N$ دارند. درحساب دیفرانسیل وانتگرال، مطلب متعارفی‌است‌که بایستی «ماندهٔ» یك سری نامتناهی همگرا، به صفرمیل‌کند، و بنابراین

$$\lim_{N\to\infty}\sum_{n=p_N+1}^{\infty}\frac{1}{n^s}=0$$

این تساوی، تساوی (۳) را ایجاب می‌کند وبنابراین قضیهٔ ۱ ثابت شده است. ■

قضیهٔ ۱ برای نشان دادن نامتناهی بودن تعداد اعداد اول کافی است.

نتیجهٔ ۲: (اقلیدس). بینهایت عدد اول موجود است.

برهان (اویلر): اگرچنین نباشد، فرض می‌کنیم p_1، ...، p_M کلیهٔ اعداد اول باشند. در این صورت بنابرقضیهٔ ۱،

$$\zeta(s)=\prod_{m=1}^{M}\left(1-\frac{1}{p_m^s}\right)^{-1},$$

یك حاصلضرب متناهی است. بنابراین، واضح است‌که طرف راست به ازای هرعددحقیقی $s>0$ معنی دارد ومعرف یك تابع پیوسته است. ولی قبلا مشاهده‌کردیم‌که

$$\lim_{s\to 1+}\zeta(s)=\infty,$$

که باحکم

$$\lim_{s\to 1+}\prod_{m=1}^{M}\left(1-\frac{1}{p_m^s}\right)^{-1}=\prod_{m=1}^{M}\left(1-\frac{1}{p_m}\right)^{-1}<\infty$$

متناقض است. ∎

هدف ما اثبات شرح دقیقتری از نتیجهٔ ۲ می‌باشد، یعنی

$$\sum_p \frac{1}{p}=\infty\,.$$

توجه‌داشته باشید که این‌معادله چیزی بیش‌ازنامتناهی‌بودن‌تعداد اعداد اول‌را تصدیق می‌کند. به عنوان مثال، تعداد اعداد مربع‌کامل به‌صورت n^2 هم‌نامتناهی است، ولی

$$\sum_{n=1}^{\infty}\frac{1}{n^2}<\infty\,.$$

بنا براین، به‌تعبیری، «تعداد اعداد اول از تعداد اعداد مربع بیشتراست». دقیقتر‌این‌که، در مجموعهٔ کلیهٔ اعداد صحیح، اعداد اول متراکمتر(چگالتر) از مربعهای کامل هستند.

قضیهٔ ۳ : (اویلر). $\sum_p \frac{1}{p}=\infty$.

برهان: به‌ازای $s>1$، $\log\zeta(s)$ را درنظر می‌گیریم، چون به ازای $s>1$، $\zeta(s)>0$، پس $\log\zeta(s)$ تعریف شده است؛ و چون $\lim_{s\to 1+}\zeta(s)=\infty$، بایستی داشته باشیم

$$\lim_{s\to 1+}\log\zeta(s)=\infty\,. \qquad (4)$$

بنا بر قضیهٔ ۱،

$$\log\zeta(s)=\log\left(\lim_{N\to\infty}\prod_{k=1}^{N}\left(1-\frac{1}{p_k^s}\right)^{-1}\right)$$
$$=\lim_{N\to\infty}\left(\log\prod_{k=1}^{N}\left(1-\frac{1}{p_k^s}\right)^{-1}\right)\,.$$

(چون $\log x$ تابعی پیوسته است، این‌حقیقت که $a_N\to a$، وقتی $N\to\infty$ ایجاب‌می‌کند که $\log a_N\to\log a$ وقتی $N\to\infty$.) بنا براین،

$$\log\zeta(s)=\lim_{N\to\infty}\sum_{k=1}^{N}\left(-\log\left(1-\frac{1}{p_k^s}\right)\right)\,.$$

سری نامتناهی $\log(1-x)$ را یادآوری می‌کنیم: به ازای $|x|<1$،

$$-\log(1-x)=x+\frac{x^2}{2}+\frac{x^3}{3}+\dots=\sum_{m=1}^{\infty}\frac{x^m}{m}\,.$$

چون به‌ازای $s>1$ ، $0<\frac{1}{p_k^s}<1$ ،

$$-\log\left(1-\frac{1}{p_k^s}\right)=\sum_{m=1}^{\infty}\frac{1}{mp_k^{ms}}=\frac{1}{p_k^s}+\sum_{m=2}^{\infty}\frac{1}{mp_k^{ms}}$$

$$<\frac{1}{p_k^s}+\sum_{m=2}^{\infty}\frac{1}{p_k^m}$$

$$=\frac{1}{p_k^s}+\frac{1}{p_k^2}\sum_{m=0}^{\infty}\frac{1}{p_k^m}$$

(بنا بردستورسری هندسی، به ازای $|r|<1$ ، $\sum_{m=0}^{\infty}r^m=\frac{1}{1-r}$.)

$$=\frac{1}{p_k^s}+\frac{1}{p_k^2}\times\frac{1}{1-\frac{1}{p_k}}$$

$$=\frac{1}{p_k^s}+\frac{1}{p_k(p_k-1)}.$$

بنابراین ،

$$\log\zeta(s)\leqslant\lim_{N\to\infty}\sum_{k=1}^{N}\left(\frac{1}{p_k^s}+\frac{1}{p_k(p_k-1)}\right).$$

توجه می‌کنیم که

$$\sum_{k=1}^{\infty}\frac{1}{p_k(p_k-1)}\leqslant\sum_{n=2}^{\infty}\frac{1}{n(n-1)}<\infty,$$

و به ازای $s>1$ ،

$$\sum_{k=1}^{\infty}\frac{1}{p_k^s}\leqslant\sum_{n=1}^{\infty}\frac{1}{n^s}<\infty.$$

لذا

$$\sum_{k=1}^{\infty}\frac{1}{p_k^s} \text{ و } \sum_{n=1}^{\infty}\frac{1}{p_k(p_k-1)}$$

بنا برآزمون مقایسه همگرایند. قرارمی‌دهیم

$$\alpha=\sum_{k=1}^{\infty}\frac{1}{p_k(p_k-1)},$$

که عددی ثابت ومستقل از s است. دراین صورت

$$\log\zeta(s)\leqslant\sum_{k=1}^{\infty}\frac{1}{p_k^s}+\alpha.$$

بلافاصله از معادلهٔ (۴) بدست می‌آید که

$$\lim_{s\to 1+}\sum_{k=1}^{\infty}\frac{1}{p_k^s}=\infty . \qquad (۵)$$

بعلاوه، چون به‌ازای کلیهٔ مقادیر $s>1$ ، $\frac{1}{p_k}>\frac{1}{p_k^s}$. می بینیم که

$$\sum_{k=1}^{N}\frac{1}{p_k}>\sum_{k=1}^{N}\frac{1}{p_k^s} ,$$

و بنا براین به ازای کلیهٔ مقادیر $s>1$ ،

$$\sum_{k=1}^{\infty}\frac{1}{p_k}>\sum_{k=1}^{\infty}\frac{1}{p_k^s} .$$

پس بالاخره، ازمعادلهٔ (۵) نتیجه‌می گیریم که

$$\sum_{k=1}^{\infty}\frac{1}{p_k}=\infty ,$$

واین همان چیزی است که می‌خواستیم. ■

۳

همنهشتیها

۱.۳ مقدمه

دراین فصل به‌معرفی یکی دیگر از مفاهیم بنیادی نظریهٔ اعداد، مفهوم همنهشتی، خواهیم پرداخت. برای اینکه شما را متوجه مفهوم همنهشتی سازیم، فرآیند اندازه‌گیری زمان از روی ساعت را درنظر می‌گیریم. به‌لحاظ سادگی، فرض می‌کنیم می‌خواهیم ساعت صحیح (ونه‌دقیقه‌های گذشته ازساعت) را بیان کنیم. دراین‌صورت فرآیند اندازه‌گیری‌زمان که در زندگی روزانه به‌کار می‌گیریم به‌قرار زیر است: به‌هرساعت عددی را، که معرف تعداد ساعاتی‌است که ازآخرین ظهر ویا ازآخرین نیمه شب گذشته است، تخصیص‌می‌دهیم. پس‌از گذشت ۱۲ ساعت، مجدداً ازنو شروع به‌شمارش می‌کنیم. بدین‌ترتیب، تنها زمانهایی درنظر گرفته می‌شوند که توسط اعداد ۱ تا ۱۲ داده شده باشند، و به دو زمان که اختلافشان مضربی از ۱۲ ساعت‌باشد یك‌عدد تخصیص داده می‌شود. بدین‌ترتیب ما زمان را با«نادیده گرفتن مضارب ۱۲ ساعت» اندازه‌گیری می‌کنیم. پدیدهٔ مشابهی را درکیلومترشمار ماشین مشاهده می‌کنیم. اکثرکیلومترشمارها مسافت را فقط تا ۹۹۹۹۹ کیلومتر ثبت می‌کنند. درکیلومتر ۱۰۰۰۰۰، کیلومترشمار صفر را نشان می‌دهد و دوباره شروع به‌ثبت اعداد مابین ۰ و ۹۹۹۹۹ می‌کند. بنابراین، اگرمسافت بین دونقطه مضربی از ۱۰۰۰۰۰ باشد، کیلومترشمار این دونقطه را یکی می‌شمارد.

مثالهای مربوط به ساعت و کیلومترشمار را می‌توانیم به‌صورت زیر تعمیم دهیم. فرض کنید که‌یك‌صفحهٔ‌شماره‌گیر داریم که روی‌آن اعداد ۰، ۱، ...، $n-1$ ثبت‌شده‌اند، وتصور کنید که صفحهٔ شماره‌گیر به‌اسبابی، که برای شمردن چیزی (ساعت، کیلومتر، مردم،

وغیره) تعبیه شده متصل شده است. برای هرمورد از پدیدهٔ موردنظر شمارگر یك شماره به‌پیش می‌رود. دراین صورت به‌آسانی می‌بینیم که شمارگر شمارش را با نادیده گرفتن مضارب n انجام می‌دهد. بنابراین، وقتی که شمارش واقعی ۱ ، $n+۱$ ، $۲n+۱$ ، $۳n+۱$ ، ... است صفحهٔ شماره‌گیر ۱ را نشان خواهد داد؛ وقتی که شمارش واقعی ۲ ، $n+۲$ ، $۲n+۲$ ، $۳n+۲$ ، ... است صفحهٔ شماره‌گیر ۲ را نشان خواهد داد و هکذا الی آخر. یا، درحالت کلی، صفحهٔ شماره‌گیر برای شمارشهای x و y یك عدد را نشان‌خواهد داد، به‌شرط‌آنکه $y-x$ بر n بخشپذیر باشد. این «کیلومترشمار» خیالی کاملا مفهوم مجرد همنهشتی را روشن می‌کند.

تعریف ۱: فرض کنیم n عددصحیح مثبتی باشد. گوییم x و y همنهشت‌به‌هنگ n هستند، و به $x \equiv y$ (هنگ n) نشان داده می‌شوند، به‌شرط‌آنکه $y-x$ بر n بخشپذیر باشد. اگر x همنهشت y به هنگ n نباشد، می‌نویسیم $x \not\equiv y$ (هنگ n) .

بدین‌ترتیب، مثلا، $۳ \equiv ۸$ (هنگ ۵) ، $۲ \equiv ۴$ (هنگ ۲) ، $۴۳ \equiv ۵۷$ (هنگ ۷). در مثالی که درباب ساعت دربالا آوردیم، ساعت دقیقاً وقتی دو زمان رایکی نشان می‌دهد که زمانهاهمنهشت به‌هنگ ۱۲ باشند. کیلومترشمار ما دومسافتی راکه بایکدیگرهمنهشت‌به‌هنگ ۱۰۰۰۰۰ هستند یکی نشان‌می‌دهد. وکیلومترشمار خیالی ما اعدادی رایکی نشان می‌دهد که همنهشت به‌هنگ n باشند. اگرما به‌زبان کیلومترشمار خیالیمان صحبت کنیم وکلیهٔ اعداد صحیحی راکه کیلومترشمار یکی نشان می‌دهد طبقه‌بندی کنیم، می‌بینیم که اعداد صحیح در طبقه‌هایی به‌صورت زیر قرار می‌گیرند[1]:

شمارهٔ کیلومترشمار

۰ ... ، $۴n$ ، $۳n$ ، $۲n$ ، n ، ۰ ، $-n$ ، $-۲n$ ، ...

۱ ... ، $۴n+۱$ ، $۳n+۱$ ، $۲n+۱$ ، $n+۱$ ، ۱ ، $-n+۱$ ، $-۲n+۱$ ، ...

۲ ... ، $۴n+۲$ ، $۳n+۲$ ، $۲n+۲$ ، $n+۲$ ، ۲ ، $-n+۲$ ، $-۲n+۲$ ، ...

⋮ ⋮

$n-۱$ ... ، $۵n-۱$ ، $۴n-۱$ ، $۳n-۱$ ، $۲n-۱$ ، $n-۱$ ، -۱ ، $-n-۱$ ، ...

مثلا، هرگاه $n=۲$ ، آنگاه دوطبقه وجود خواهد داشت

... ، ۴ ، ۲ ، ۰ ، -۲ ، -۴ ، ... که‌همنهشت ۰ به‌هنگ ۲ هستند، و

... ، ۵ ، ۳ ، ۱ ، -۱ ، -۳ ، ... که همنهشت ۱ به‌هنگ ۲ هستند،

---

۱. باکیلومتر شمار ما اعداد منفی نیز خوانده می‌شوند، بدین‌شکل‌که عقربهٔ شماره‌گیر را وارونه بچرخانیم.

بنابراین همنهشتی به‌هنگ ۲ به‌ما اجازه می‌دهد که اعداد زوج و فرد را ازهم جدا کنیم. اگر $n=3$، آنگاه سه‌طبقه وجود خواهد داشت، یعنی

... ، ۶ ، ۳ ، ۰ ، ۳− ، ۶− ، ... که همنهشت ۰ به‌هنگ ۳ هستند،

... ، ۷ ، ۴ ، ۱ ، ۲− ، ۵− ، ... که همنهشت ۱ به‌هنگ ۳ هستند، و

... ، ۸ ، ۵ ، ۲ ، ۱− ، ۴− ، ... که همنهشت ۲ به‌هنگ ۳ هستند.

حال که مفهوم همنهشتی را توضیح دادیم، به‌ذکر اهمیت آن در نظریهٔ اعداد می‌پردازیم. اول مشاهده می‌کنیم که $n|a$ اگر، وفقط اگر، $a\equiv 0$ (هنگ n). (زیرا، $n|a$ اگر، وفقط اگر، به‌ازای مقداری از k ، $a-0=kn$.) بدین‌ترتیب، مفهوم بخشپذیری می‌تواند به‌زبان همنهشتیها تعبیر شود. در واقع، همنهشتیها به‌هنگ n کاری خیلی بیشتر از تعیین بخشپذیری بر n انجام می‌دهند. همنهشتیها به‌هنگ n ما را همواره در جریان باقیمانده‌هایی که هنگام تقسیم بر n ظاهر می‌شوند قرار می‌دهند. از این‌رو به‌نظریهٔ همنهشتیها می‌توان به‌عنوان پالایشی برای نظریهٔ بخشپذیری نگریست. اما چه لزومی به‌این پالایش هست؟ یك دلیل آن این است که همنهشتیها می‌توانند خیلی شبیه به‌معادلات مورد بحث قرار گیرند. بدین‌ترتیب، مثلاً، پیدا کردن جوابهای x از همنهشتیهای

$$3x\equiv 2 \ (\text{هنگ } 5)$$

$$5x^2+3x+8\equiv 0 \ (\text{هنگ } 17)$$

معنی دارد. در بخش بعدی خواهیم دید که تقریباً کلیهٔ جبر دبیرستانی را می‌توان روی همنهشتیها انجام داد. بنابراین، ممکن است به همنهشتیها به‌عنوان ماشینی جبری نگاه کنیم که برای مطالعهٔ بخشپذیری در اختیار ما گذاشته شده‌است.

نظریهٔ همنهشتیها که در این فصل بسط داده شده است در معادلات سیاله کاربردهایی دارد. برای این که به‌اصلی کلی که در پشت‌سر چنین کاربردهایی قرار دارد پی‌ببریم، برای سادگی، مورد یك معادلهٔ سیالهٔ

$$f(x, y)=0, \qquad (1)$$

برحسب دومجهول x و y را درنظر می‌گیریم. دراینجا $f(x, y)$ بسجمله‌ای است از دو متغیر با ضرایب صحیح. اگر (x, y) یك‌جواب معادلهٔ سیالهٔ(۱) باشد آنگاه چون به‌ازای هرعدد صحیح n ، $n|0$ می‌بینیم که به‌ازای هر n ، $n|f(x, y)$، بنابراین

$$f(x, y)\equiv 0 \ (\text{هنگ } n).$$

پس، اگر (x, y) یك جواب معادلهٔ (۱) باشد، آنگاه، به‌ازای کلیهٔ مقادیر n ، (x, y) یك جواب همنهشتی

$$f(x, y)\equiv 0 \ (\text{هنگ } n) \qquad (2)$$

نیز خواهد بود. بالاخص، قضیهٔ زیر را داریم:

قضیهٔ ۲: اگر معادلهٔ سیالهٔ

$$f(x, y) = 0$$

جوابی داشته باشد، همنهشتیهای

$$f(x, y) \equiv 0 \pmod{n}$$

به‌ازای کلیهٔ مقادیر n دارای جواب هستند.

می‌توانیم، برای اثبات جواب نداشتن بعضی از معادلات سیاله، از بیان قضیهٔ ۲ به‌صورت زیر استفاده کنیم:

قضیهٔ ′۲: فرض کنیم به‌ازای یک مقدار صحیح n همنهشتی

$$f(x, y) \equiv 0 \pmod{n}$$

جواب نداشته باشد. دراین صورت معادلهٔ سیالهٔ

$$f(x, y) = 0$$

جواب ندارد.

این اصل که به‌نظر ساده می‌آید بسیار تواناست. به‌عنوان مثال، معادلهٔ سیالهٔ

$$x^2 - 4y^2 = 2 \tag{3}$$

را درنظر می‌گیریم. دراین مورد، می‌توانیم چنین بنویسیم: $f(x, y) = x^2 - 4y^2 - 2$. با گرفتن $n = 4$ ونشان دادن این امر که همنهشتی

$$x^2 - 4y^2 - 2 \equiv 0 \pmod{4} \tag{4}$$

جواب ندارد، می‌خواهیم نشان دهیم که این معادلهٔ سیاله جواب ندارد. زیرا، اگر اعداد صحیح x و y درمعادلهٔ (۴) صدق کنند، همنهشتی بالا به‌حکم معادل آن یعنی $4 | x^2 - 4y^2 - 2$ بدل می‌شود. اما، چون $4 | 4y^2$، داریم $4 | x^2 - 4y^2 - 2 + 4y^2$ (قضیهٔ ۲.۲.۲) و بنابراین $4 | x^2 - 2$. اما آیا $x^2 - 2$ می‌تواند بر ۴ بخشپذیر باشد؟ اینک با درنظر گرفتن دوحالت جداگانهٔ زوج و فرد برای x نشان خواهیم داد که این بخشپذیری ممکن نیست. اگر x زوج، مثلا $x = 2t$، باشد. دراین‌صورت $x^2 - 2 = 4t^2 - 2$، بنابراین $4 | x^2 - 2$ ایجاب می‌کند که $4 | (4t^2 - 2) - 4t^2$، و ازآنجا $4 | -2$ که مهمل است. اگر x فرد، مثلا $x = 2t + 1$، باشد. دراین‌صورت $x^2 - 2 = 4t^2 + 4t - 1$، بنابراین $4 | x^2 - 2$ ایجاب می‌کند که $4 | (4t^2 + 4t - 1) - (4t^2 + 4t)$، وازآنجا $4 | -1$، که بازهم مهمل است. بنابراین، همنهشتی (۴) جواب ندارد و بالنتیجه معادلهٔ سیالهٔ متناظر آن (۳)، نیز جواب نخواهد داشت.

بنابراین، می بینیم که اگر بتوانیم ثابت کنیم که همنهشتیها جواب ندارند، مـی توانیم احکام متناظرآنها درمورد معادلات سیاله را نفی کنیم. حتی اگریك همنهشتی جوابهایی داشته باشد، اغلب این جوابها می‌توانند اطلاعات مهمی درمورد ماهیت جوابهای (اگـر جوابی موجود باشد) معادلات سیالهٔ متناظرشان بدهند. ایـن موضوع را بعداً درایـن فصل دنبال خواهیم کرد. همچنین نحوهٔ کارکردن باهمنهشتیها را فرا خواهیم گرفت تا بتوانیم بحث دربارهٔ همنهشتی(۴) را دریك سطر ارائه دهیم.

۱.۳ تمرینات

۱. دربارهٔ درستی یا نادرستی احکام زیراظهار نظر کنید.

(آ) (هنگ۲)۴ $\equiv$ ۲. (ب) (هنگ۵)۶ $\equiv$ ۱۱.

(ج) (هنگ۱۱)۱۸ $\equiv$ ۳۳. (د) (هنگ۶)۲۱ $\equiv$ ۵۷.

(ه) $k>0$ ، (هنگ k) $k^2\equiv k$. (و) (هنگ۱۷) ۱۴ $\equiv$ $-$۱۱.

۲. (آ) نشان دهید که هرعدد صحیح دقیقاً مـی‌تواند به‌یکی ازصورتهای $4k$ ، $4k+1$ ، $4k+2$ ، $4k+3$ ، که‌درآن k عددی است صحیح، نوشته شود.

(ب) نشان دهید که هرعددصحیح درست بایکی از اعداد ۰ ، ۱ ، ۲ ویا ۳ همنهشت به‌هنگ۴ است.

(ج) نشان دهید که همنهشتی (هنگ۴) $0\equiv 2-x^2-y^2$ جواب ندارد وبنابراین معادلهٔ سیالهٔ $y^2=x^2+2$ نیز جواب‌ندارد. (راهنمایی: ازقسمت(آ)استفاده کنید.)

۳. نشان دهید که اگر معادلهٔ سیالهٔ $y^2=x^3+2$ جوابی داشته باشد، x و y بایستی هردو فرد باشند. (راهنمایی: همنهشتیهای به‌هنگ۴ را درنظر بگیریـد و از تمرین۲ (آ) استفاده کنید.)

۴. فرض‌کنیم x ، y و z اعدادی صحیح باشند. احکام‌زیر را ثابت‌کنید:

(آ) (هنگ n) $x\equiv x$.

(ب) اگر (هنگ n) $x\equiv y$ ، آنگاه (هنگ n) $y\equiv x$.

(ج) اگر (هنگ n) $x\equiv y$ و (هنگ n) $y\equiv z$ ، آنگاه (هنگ n) $x\equiv z$.

۲.۳ خواص اساسی همنهشتیها

دراین بخش، بعضی‌حقایق اساسی دربارهٔ همنهشتیها رابسط خواهیم داد. مطلب‌اصلی ما این خواهد بود که‌همنهشتی نوعی«تساوی» است‌وهمنهشتی (هنگ n) $a\equiv b$ ، دربسیاری از موارد می‌توانند به‌مثابهٔ معادلهٔ $a=b$ درنظر گرفته شود. منظور اصلی ما دراین‌بخش این است که ببینیم این شباهت را تابه‌کجا می‌توان تعمیم داد. به‌طور دقیقتراینکه، مـی‌خواهیم تعیین‌کنیم که کدامیك از اعمال مجاز ـمثل جمع، تفریق، ضرب‌ـ درمورد معادلات، درمورد

همنهشتیها هم مجازند. درسرتاسر این فصل، n نمایش عددصحیح مثبتی خواهدبود. تنهاحقیقتی راکه ما از بخش قبل می‌پذیریم تعریف همنهشتی به‌هنگ n می باشد.

پیش‌ازاین‌که جلوتر برویم، می‌خواهیم دونتیجهٔ ساده و پیش‌پاافتاده دربارهٔ همنهشتی به‌هنگ n را ثابت کنیم.

قضیهٔ ۱: فرض کنیم a ، b و c اعداد صحیح باشند. دراین‌صورت

(یکم) $a \equiv a$ (هنگ n).

(دوم) اگر $a \equiv b$ (هنگ n) ، آنگاه $b \equiv a$ (هنگ n) .

(سوم) اگر $a \equiv b$ (هنگ n) و $b \equiv c$ (هنگ n) ، آنگاه $a \equiv c$ (هنگ n).

برهان:

(یکم) $n|a-a$.

(دوم) اگر $n|a-b$ ، آنگاه $n|b-a$.

(سوم) اگر $n|a-b$ و $n|b-c$ ، آنگاه $n|(a-b)+(b-c)$ ، بنابراین $n|a-c$. ∎

نتیجهٔ عملی قضیهٔ ۱ این است که به‌ما اجازه می‌دهد ترتیب همنهشتیها راعکس کنیم و همنهشتیهای به‌هنگ n را باهم ترکیب کنیم. ازاین به‌بعد، مااین اعمال را بدون هیچ گونه توضیحی انجام خواهیم داد[1].

قضیهٔ ۲: فرض کنیم $a \equiv b$ (هنگ n) و $c \equiv d$ (هنگ n). دراین‌صورت

(یکم) $a+c \equiv b+d$ (هنگ n) .

(دوم) $a-c \equiv b-d$ (هنگ n) .

(سوم) $ac \equiv bd$ (هنگ n) .

برهان: بنابرفرض، $n|a-b$ و $n|c-d$. بنابراین، $n|(a-b)+(c-d)$ ایجاب‌می کند که $n|(a+c)-(b+d)$ ، که ایجاب می کند $a+c \equiv b+d$ (هنگ n)، کـه قسمت (یکم) را ثابت می کند. قسمت (دوم) را به‌عنوان تمرین واگذار می‌کنیم. بـرای اثبات (سوم)، مشاهده می کنیم که چون $n|a-b$ ، داریم $n|c(a-b)$ ، بنابراین $n|ac-bc$ ولذا $ac \equiv bc$ (هنگ n). به‌همین‌طریق، چون $n|c-d$، داریم $bc \equiv bd$ (هنگ n). بنابراین

---

۱. ما $a \equiv b$ (هنگ n) ، $b \equiv c$ (هنگ n) رابه‌صورت $a \equiv b \equiv c$ (هنگ n) خلاصه مـی‌کنیم وبه‌همین‌طریق ردیفهای بیشتری از همنهشتیها را خلاصه خواهیم‌کرد.

$ac\equiv bc\equiv bd$ (هنگ n)، بدین ترتیب، قسمت (سوم) هم ثابت می‌شود. ■

یك استدلال استقرائی مقدماتی به‌ما اجازه می‌دهد قضیهٔ ۲ را به‌صورت زیر تعمیم‌دهیم:

نتیجهٔ ۳ : فرض کنیم $a_1\equiv b_1$ (هنگ n)، $a_2\equiv b_2$ (هنگ n)، …، $a_m\equiv b_m$ (هنگ n). دراین‌صورت

$$a_1+\dots+a_m\equiv b_1+\dots+b_m\ (\text{هنگ}\ n)$$

و

$$a_1\dots a_m\equiv b_1\dots b_m\ (\text{هنگ}\ n)$$

ازقضیهٔ ۲ ونتیجهٔ ۳، می‌بینیم که می‌توانیم جملات متناظر درهمنهشتیها به‌هنگ n راباهم جمع، تفریق، و دریکدیگر ضرب کنیم، وبنابراین می‌توانیم باهمنهشتیها بسیار شبیه معادلات رفتار کنیم.

قضیهٔ ۲ (یا بهتر ازآن نتیجهٔ ۳) نتیجهٔ‌عملی زیررا دارد. فرض کنیم $f(x)$ یك بسجمله باضرایب صحیح باشد و $a\equiv b$ (هنگ n). دراین‌صورت

$$f(a)\equiv f(b)\ (\text{هنگ}\ n)\,. \qquad (۱)$$

زیرا، اگر $f(x)=a_0+a_1x+\dots+a_mx^m$، آنگاه‌معادلهٔ (۱) فقط به‌این‌معنی‌است که

$$a_0+a_1a+\dots+a_ma^m\equiv a_0+a_1b+\dots+a_mb^m\ (\text{هنگ}\ n)\,,$$

که باچندین‌بار استفاده ازنتیجهٔ ۳ به‌آسانی اثبات می‌شود.

برای‌اینکه‌ارزش‌عملی‌معادلهٔ (۱) راببینیم،فرض‌کنیم $f(x)=x^3+4x^2+5x-1$، $n=3$. دراین‌صورت، چون $13\equiv 1$ (هنگ ۳)، همنهشتی (۱) بیان می‌کند که

$$13^3+4\times 13^2+5\times 13-1\equiv 1^3+4\times 1^2+5\times 1-1\ (\text{هنگ}\ 3) \qquad (۲)$$

$$\equiv 1+4+5-1\ (\text{هنگ}\ 3)$$

$$\equiv 9\ (\text{هنگ}\ 3)$$

$$\equiv 0\ (\text{هنگ}\ 3)$$

توجه کنید که طرف‌راست معادلهٔ (۲) چقدر ساده‌تر ازطرف چپ محاسبه شد.

قبلا دربخش ۱ اشاره کردیم که یکی‌از اهداف‌اصلی نظریهٔ همنهشتیها تعیین (درصورت وجود) جوابهای همنهشتی

$$f(x)\equiv 0\ \ (\text{هنگ}\ n) \qquad (۳)$$

است، که دراینجا $f(x)$ یك بسجمله با ضرایب صحیح است. ازمعادلهٔ (۱) دیده می‌شود که، برای اینکه معلوم کنیم x یك جواب معادلهٔ فوق‌هست یانه، کافی‌است تحقیق‌کنیم که عددی مثل x' که همنهشت x به‌هنگ n است، جواب آن‌است یانه. آیاهمواره می‌شود x'ی‌انتخاب

کرد که این تحقیق متضمن محاسبهٔ زیاد نباشد؟ البته که ممکن است، همان‌طور که قضیهٔ زیر نشان می‌دهد:

قضیهٔ ۴ : هرعدد صحیح x با یك و تنها یکی از اعدادصحیح ۰ ، ۱ ، ۲ ،... ، $n-1$ همنهشت به‌هنگ n است.

برهان: این حکم دراصل بیان دیگری از آلگوریتم تقسیم است (قضیهٔ ۳.۲.۲). زیرا مطابق آلگوریتم تقسیم، می‌توانیم x را به‌صورت $x=qn+r$ ، $0\leqslant r\leqslant n-1$ ، بنویسیم. و بنا بر تعریف همنهشتی، داریم $x\equiv r$ (هنگ n) ، همچنین اگر داشته باشیم $x\equiv r'$ (هنگ n) ، $0\leqslant r'\leqslant n-1$ ، آنگاه عددی مانند q' وجود دارد به‌طوری که $x-r'=q'n$ ، بنابراین $x=q'n+r'=qn+r$. پس، بنا برحکم یکتایی آلگوریتم تقسیم، داریم $r=r'$. ■

اگر $n=2$ ، آنگاه قضیهٔ۴ حکم می کند که هرعددصحیح فقط با یکی از اعداد ۰ یا ۱ همنهشت به‌هنگ۲ است. این، همان‌حقیقت‌ساده و بدیهی است که هرعدد صحیح یا زوج است یا فرد، ولی هردو نیست. اگر $n=3$، آنگاه قضیهٔ۴ حکم می کند که هرعدد صحیح فقط با یکی از اعداد ۰ ، ۱ و یا ۲ همنهشت به‌هنگ۳ است.

دربارهٔ چگونگی پرداختن به‌حل همنهشتی(۳) مطالب زیادی باید بگوییم، ولی اجازه بدهید که فعلا این بحث را رها کنیم و به‌نتایج دیگری که قضیهٔ۴ عرضه می کند بپردازیم.

قضیهٔ۴ حکم می کند که مجموعهٔ اعداد صحیح ۰ ، ۱ ، ۲ ، ... ، $n-1$ ، دارای این خصوصیت است که هرعددصحیح با یك وفقط یکی از اعضای این مجموعه همنهشت به‌هنگ n است. این خصوصیت، همان خصوصیتی است که موجب می‌شود مجموعهٔ مذکور درحل همنهشتی(۳) مفید واقع‌شود. ولی‌مجموعهٔ ۰ ، ۱ ، ۲ ، ... ، $n-1$ تنها مجموعه‌ای نیست که این خصوصیت را دارد، و این واقعیت گویای تعریف زیراست:

تعریف ۵ : یك دستگاه‌کامل مانده‌ها به‌هنگ n مجموعه‌ای‌است از n عددصحیح r_1 ، ... ، r_n به‌طوری که هرعددصحیح x با یك وتنها یکی‌از اعداد r_1 ، ... ، r_n همنهشت باشد.

مثال ۶ :

(یکم) قضیهٔ۴ حکم می کند که ۰ ، ۱ ، ... ، $n-1$ دستگاه کاملی از مانده‌ها به هنگ n است.

(دوم) هردسته از اعداد زیردستگاه کاملی ازمانده‌ها به‌هنگ ۵ است:

۰ ، ۱ ، ۲ ، ۳ ، ۴ ;

۲− ، ۱− ، ۰ ، ۱ ، ۲ ;

۲۵ ، ۲۶ ، ۲۷ ، ۲۸ ، ۲۹ ;

−۳۰ ، −۲۹ ، −۲۸ ، −۲۷ ، −۲۶ ؛

۴۳۵۵ ، ۲۳۱۱ ، ۱۱۷ ، ۱۳ ، −۱۹۶ .

اکنون برهانی برای مجموعهٔ دوم ذکر می‌کنیم. توجه کنید که

(هنگ ۵) ۰ ≡ ۰ ، (هنگ ۵) ۴ ≡ −۱ ، (هنگ ۵) ۳ ≡ −۲ ،

(هنگ ۵) ۲ ≡ ۲ ، (هنگ ۵) ۱ ≡ ۱ .

اگر x عدد صحیح دلخواهی باشد، آنگاه بنا بر قضیهٔ ۴ ، x با یك و تنها یکی از اعداد صحیح ۰ ، ۱ ، ۲ ، ۳ ، ۴ همنهشت است. و بنا بر محاسبهٔ فوق، اگر (هنگ ۵) $x \equiv r$ ، $0 \leqslant r \leqslant 4$ ، آنگاه r با یك و تنها یکی از اعداد صحیح −۲ ، −۱ ، ۰ ، ۱ ، ۲ همنهشت است، بنا بر این x با یك و تنها یکی از اعداد صحیح −۲ ، −۱ ، ۰ ، ۱ ، ۲ همنهشت است. اثبات این که کلیهٔ مجموعه‌های دیگر فوق دستگاه کاملی از مانده‌ها به‌هنگ ۵ می‌باشند نیز به‌همین طریق است. تنها نکته این است که درهر مجموعه یك و تنها یك عدد صحیح همنهشت باهریك از اعداد ۰ ، ۱ ، ۲ ، ۳ ، ۴ موجود است.

دستگاههای کامل مانده‌ها به‌هنگ n به‌ما اجازه خواهند داد تا محاسبات واضحی را با همنهشتیها به‌هنگ n انجام دهیم. برای اثبات همنهشتیهای فرما، اویلر و ویلسن[1] در بخش ۳، ما به‌مفهوم کلی همنهشتی احتیاج خواهیم داشت. ولی، برای محاسبهٔ کلی، ما به‌دستگاه کامل مانده‌های ۰ ، ۱ ، … ، $n-1$ که به‌خاطر سپردن آن بسیار ساده است، متوسل خواهیم شد. یا از دستگاهی نظیر دستگاه کامل مانده‌های ۲ ، ۱ ، ۰ ، −۱ ، −۲ به‌هنگ ۵ استفاده خواهیم کرد که این برتری را دارد که اعداد آن از اعداد دستگاه عادی کامل مانده‌های ۰، ۱، ۲، ۳، ۴ کوچکترند و بدین‌ترتیب محاسبات را ساده‌تر می‌سازند. متعلم ممکن است از این صرفه‌جویی که براثر چنین تغییر جزئی فراهم آمده استقبال نکند. ولی مثال زیر را درنظر بگیرید:

مثال ۶′ : می‌خواهیم باقیماندهٔ تقسیم 6^{48} بر ۱۳ را محاسبه کنیم. البته، ممکن است مستقیما مقدار 6^{48} را محاسبه کنیم و با تقسیم کردن بر ۱۳ ببینیم که باقیماندهٔ آن چقدر است. ولی حجم محاسبه بقدری است که تنها عدهٔ معدودی علاقمند به محاسبه به‌آن تن درخواهند داد. خوشبختانه، محاسبهٔ باقیمانده با استفاده از همنهشتیها به‌هنگ ۱۳ ساده است. از دستگاه کامل مانده‌ها به‌هنگ ۱۳ که درزیر آمده استفاده می‌کنیم:

−۶ ، −۵ ، −۴ ، −۳ ، −۲ ، −۱ ، ۰ ، ۱ ، ۲ ، ۳ ، ۴ ، ۵ ، ۶ .

می‌توانیم محاسبات خود را به‌صورت زیر مرتب کنیم:

$6^2 = 36 \equiv -3$ (هنگ ۱۳)

$6^4 = (6^2)^2 \equiv (-3)^2 = 9 \equiv -4$ (هنگ ۱۳)

$6^8 = (6^4)^2 \equiv (-4)^2 = 16 \equiv 3$ (هنگ ۱۳)

---

1. Wilson

$$6^{16} = (6^8)^2 \equiv 3^2 = 9 \equiv -4 \pmod{13}$$

$$6^{32} = (6^{16})^2 \equiv (-4)^2 = 16 \equiv 3 \pmod{13}$$

$$6^{48} = 6^{32} \times 6^{16} \equiv 3 \times (-4) = -12 \equiv 1 \pmod{13} .$$

یعنی، $6^{48} \equiv 1 \pmod{13}$، یاوقتی 6^{48} بر ۱۳ تقسیم‌شود باقیمانده مساوی ۱ می‌شود. متعلم باید سعی کند این‌مثال‌را، بااستفاده از دستگاه کامل مانده‌های ۰ ، ۱ ، ۲ ، ... ، ۱۲، (به‌جای دستگاه قبلی)، به‌انجام برساند. البته محاسبات خسته‌کننده‌تر اند.

درقضیهٔ ۲، دیدیم که طرفین همنهشتیهارا، مانند معادلات جبری، می‌توانیم نظیر به‌نظیر باهم‌جمع، ازهم‌تفریق و درهم ضرب کنیم. حال به‌مسئلهٔ تقسیم طرفین یك همنهشتی بریك‌عدد برمی‌گردیم.

مشکل تقسیم طرفین یك همنهشتی بریك عدد آن است که خواستارآنیم که کلیهٔ اعداد یك همنهشتی اعداد صحیح باشند. برای اینکه تصوری ازمشکل موجود به‌دست آوریم، همنهشتی زیر را درنظر می‌گیریم:

$$2x \equiv 3 \pmod{4}$$

اگر رابطه‌فوق‌معادله‌بود، می‌توانستیم‌طرفین آن را در $1/2$ ضرب‌کنیم‌و $x = 3/2$ را به‌دست آوریم. آیاعدد صحیحی موجوداست که بتواند نقش $1/2$ را درحل این‌همنهشتی بازی‌کند؟ متأسفانه چنین عددی وجود ندارد، زیرا همنهشتی فوق جواب ندارد. در واقع، بیاییم از دستگاه‌کامل مانده‌های ۰ ، ۱ ، ۲ ، ۳ به‌هنگ ۴ استفاده‌کنیم. اگر $x \equiv 0 \pmod{4}$ ، آنگاه $2x \equiv 0 \pmod{4}$ ؛ اگر $x \equiv 1 \pmod{4}$ ، آنگاه $2x \equiv 2 \pmod{4}$ ؛ اگر $x \equiv 2 \pmod{4}$ ، آنگاه $2x \equiv 2 \times 2 \equiv 0 \pmod{4}$ ؛ اگر $x \equiv 3 \pmod{4}$ ، آنگاه $2x \equiv 2 \times 3 \equiv 2 \pmod{4}$ ، درهرحالت، $2x \equiv 0$ یا $2 \pmod{4}$ و بنابراین $2x \not\equiv 3 \pmod{4}$ وهمنهشتی فوق‌جواب ندارد.

بدین‌ترتیب درحالت کلی، نمی‌توانیم طرفین یك همنهشتی را بریك عددصحیح تقسیم کنیم. یا، به‌عبارت دیگر، همیشه نمی‌توانیم عدد صحیحی بیابیم که «نقش وارون یك عدد صحیح را بازی‌کند». اجازه دهیدکه منظور خود را تااندازه‌ای دقیقتر تعریف کنیم.

تعریف ۷: فرض کنیم a عددصحیحی باشد. منظورما از عکس‌حسابی a به‌هنگ n عددصحیحی است مانند a^* به‌طوری که $aa^* \equiv 1 \pmod{n}$.

عکس‌حسابی a دقیقا نظیر $1/a$ درنظریهٔ‌اعداد است. زیرا،همنهشتی $aa^* \equiv 1 \pmod{n}$ نظیر معادلهٔ $a \times (1/a) = 1$ است. چنین نیست که هرعدد صحیح عکس حسابی به هنگ n داشته باشد. به‌عنوان مثال، ۲ عکس‌حسابی به‌هنگ ۴ ندارد (تمرین). ازطرف‌دیگر نتیجهٔ زیر را داریم:

قضیهٔ ۸: هرگاه ۱ = بمعم(a , n)، آنگاه a یک‌عکس حسابی a^* به‌هنگ n دارد.

برهان: چون ۱ = بمعم(a , n)، xی و yی موجودند به‌طوری که ۱ = $ax+ny$. پس $ax \equiv 1$ (هنگ n) و می‌توانیم a^* را مساوی x بگیریم. ■

توجه‌داشته باشید که اثبات قضیهٔ ۸ نشان می‌دهد که می‌توانیم از آلگوریتم اقلیدسی برای محاسبهٔ عکس‌حسابی a استفاده کنیم.

در تمرینات نشان‌خواهیم داد که کلیهٔ عکسهای حسابی a به‌هنگ n، به‌هنگ n همنهشت یکدیگرند؛ یعنی همه به‌هنگ n «یکی» هستند.

مثال ۹:

(یکم) فرض کنیم ۳ = n ، ۲ = a. دراین‌صورت می‌توانیم a^* را مساوی ۲ بگیریم زیرا (هنگ ۳) $2 \times 2 \equiv 1$.

(دوم) فرض کنیم ۵ = n ، ۳ = a. دراین‌صورت می‌توانیم a^* را مساوی ۲ بگیریم زیرا (هنگ ۵) $3 \times 2 \equiv 1$.

همچنانکه گفته‌ایم، a^* یعنی عکس حسابی a، درصورت‌وجود، نقش وارون a را بازی می‌کند. برای مثال، بااستفاده از مفهوم عکس‌حسابی، می‌توانیم قانون حذف زیر را برای همنهشتیها ثابت کنیم:

قضیهٔ ۱۰: هرگاه ۱ = بمعم(a , n) و

$$ax \equiv ay \ (\text{هنگ } n)$$

آنگاه

$$x \equiv y \ (\text{هنگ } n).$$

برهان: فرض کنیم a^* عکس‌حسابی a به‌هنگ n باشد، که بنابرقضیهٔ ۸ وجود دارد زیرا که فرض کرده‌ایم ۱ = بمعم(a , n). دراین‌صورت داریم

$$x \equiv 1 \times x \equiv (a^*a)x \equiv a^*(ax) \equiv a^*(ay) \equiv (a^*a)y \equiv 1 \times y \equiv y \ (\text{هنگ } n),$$

زیراکه $a^*a \equiv 1$ (هنگ n). ■

درمورد قضیهٔ ۱۰، اگر بمعم(a , n) بزرگتر از ۱ باشد، حذف a همواره‌ممکن نیست. مثلاً، (هنگ ۴) $2 \times 3 \equiv 2 \times 1$، ولی (هنگ ۴) $3 \not\equiv 1$. اما، می‌توانیم قضیهٔ ۱۰ را به‌صورت کلیتر زیر بنویسیم:

قضیهٔ ۱۱: هرگاه d = بمعم(a , n) و

$$ax \equiv ay \ (\text{هنگ } n).$$

آنگاه

$$x \equiv y\left(\frac{n}{d} \text{ هنگ }\right) .$$

برهان: توجه کنید که چون $ax \equiv ay$ (n هنگ)، داریم $n|ax-ay$، لذا $(n/d)|(a/d)(x-y)$، و بنابراین

$$\frac{a}{d}x \equiv \frac{a}{d}y \left(\frac{n}{d} \text{ هنگ }\right) .$$

بعلاوه، ۱ = بمعم$(a/d \text{ ، } n/d)$ (قضیهٔ ۶.۳.۲ (دوم))، پس بنابر قضیهٔ ۱۰ داریم

$$x \equiv y\left(\frac{n}{d} \text{ هنگ }\right) . \qquad \blacksquare$$

توجه کنید که قضیهٔ ۱۰ درست همان قضیهٔ ۱۱ درحالت خاص $d = 1$ است. همچنین توجه داشته باشید که قضیهٔ ۱۱، درست همان بیان دیگر قسمت چهارم قضیهٔ ۶.۳.۲ به‌زبان همنهشتیها است.

مثال ۱۲:

(یکم) چون (هنگ ۱۴) ۱۶ × ۳ ≡ ۲ × ۳ و ۱ = بمعم(۱۴ ، ۳) ، داریم (هنگ ۱۴) ۱۶ ≡ ۲.

(دوم) چون (هنگ ۲۶)۱۸ × ۶ ≡ ۵ × ۶ و ۲ = بمعم(۲۶ ، ۶) ، داریم (هنگ۱۳)۱۸ ≡ ۵. توجه داشته باشید که (هنگ ۲۶)۱۸ ≡ ۵ درست نیست.

ما اکنون وسیلهٔ کافی دراختیار داریم تا بررسی یکی از مسائل بنیادی مورد بحث دراین کتاب، یعنی حل همنهشتیهای بسجمله‌ای، راشروع کنیم. فرض کنیم $f(x)$ یك بسجمله‌ای باضرایب‌صحیح باشد. سؤالی که ما درجستجوی جواب آن‌هستیم این است که به‌ازای‌چه‌مقادیر x همنهشتی

$$f(x) \equiv 0 (n \text{ هنگ }) \tag{۴}$$

برقرار است؟ دربخش پیش، رابطهٔ بین جواب این معادله ومسئلهٔ تعیین جوابهای معادلهٔ سیالهٔ $f(x) = 0$ را دیده‌ایم. درحالت کلی، ممکن‌است همنهشتی(۴) ، همان‌گونه که از مثال زیر دیده می‌شود، جواب نداشته باشد:

مثال ۱۳: همنهشتی (هنگ۸)$0 \equiv 1 + x^2$ جواب ندارد. زیرا اگر x یك جواب آن‌باشد، آنگاه(هنگ۸)۷ ≡ ۱ − ≡ x^2. اما، بااستفاده از دستگاه کامل‌مانده‌های ۰ ، ±۱ ، ±۲ ، ±۳ ، ±۴ [1] به‌هنگ۸ ، می‌بینیم که درپنج حالت، x^2 بترتیب با ۰ ، ۱ ، ۴ ، ۱ ، ۰

---

۱. چون (هنگ ۸) ۴ ≡ ۴− فقط یکی‌از آنها (۴ یا ۴−) کافی است (مترجم).

همنهشت به‌هنگ ۸ است (محاسبات را بررسی کنید). بالاخص، درهرحالت، (هنگ ۸) $x^2 \not\equiv 7$، بنابراین همنهشتی (هنگ ۸) $x^2+1\equiv 0$ جواب ندارد. به‌عنوان نتیجه‌ای ازمحاسبات‌خود، نکتهٔ جالب زیر را ارائه می‌کنیم:

یك مربع‌کامل با ۰ ، ۱ یا ۴ همنهشت به‌هنگ ۸ است. بالاخص یك مربع کامل فرد همنهشت ۱ است به‌هنگ ۸.

ممکن‌است چندتوضیح کلی درمورد همنهشتی(۴)داده‌شود. اگر x یك جواب‌باشدو (هنگ $x\equiv x'(n$ ، آنگاه درمعادلهٔ(۱) ، قبلا مشاهده کرده‌ایم که x' نیز یك جواب است. بنابراین، می‌توانیم از مفهوم دستگاه کامل مانده‌ها به هنگ n برای ارائهٔ روش سادهٔ زیر جهت یافتن کلیهٔ جوابهای(۴) استفاده کنیم. یك دستگاه کامل مانده‌ها به‌هنگ n مثل r_1 ، ... ، r_n انتخاب می کنیم. هریك ازکمیات r_1 ، ... ، r_n را می‌آزماییم تاببینیم کدامیك می‌توانند جواب(۴) باشند. فرض کنیم a_1 ، ... ، a_t جوابهای(۴) باشند. اگر x یك‌جواب (۴) باشد، آنگاه (هنگ n) $f(x)\equiv 0$. ولی، بنابرتعریف دستگاه کامل مانده‌ها، به‌ازای مقداری‌از i ، $x\equiv r_i$. اما دراین‌صورت‌بنابر(۱) داریم (هنگ $f(x)\equiv f(r_i)(n$، بنابراین (هنگ $f(r_i)\equiv 0\ (n$ و r_i یك جواب (۴) است. به‌عبارت دیگر ، r_i یکی از مقادیر a_1 ، ... ، a_t است. ازاین‌رو می‌بینیم که اگر x یك جواب(۴) باشد، آنگاه به‌ازای‌مقداری از j ، $1\leqslant j\leqslant t$ ، (هنگ $x\equiv a_j\ (n$. بنابراین‌کافی است دستگاه کامل مانده‌های ثابت دلخواهی به‌هنگ n را برای جوابهای(۴) بیازماییم. این‌روشی بودکه اساساً درمثال ۱۳ به‌کار بردیم. این روش درواقع درست همان روش آزمون وخطاست. ولی، ما درجستجوی روشی بهتر ازاین هستیم.

حال، از بحث حاضر، به‌این نتیجه می‌رسیم که xهایی که درمعادلهٔ(۴) صدق می کنند همان xهایی هستندکه دریکی از همنهشتیهای زیرصدق می کنند

$$x\equiv a_1(n \text{ هنگ})،\ \text{یا}\ x\equiv a_2(n \text{ هنگ})،\ \ldots،\ \text{یا}\ x\equiv a_t(n \text{ هنگ}).$$

چون a_iها از دستگاه کامل مانده‌ها به‌هنگ n گرفته‌شده‌اند، می‌بینیم که‌هیچ‌دو a_jای همنهشت بایکدیگر به‌هنگ n نیستند، و xهایی که توسط هریك از همنهشتیهای‌فوق تعیین‌می‌شوندتماماً از یکدیگر متمایزند. دراینجا، می‌توانیم بگوییم که همنهشتی(۴) t جواب متمایز دارد. (البته، اگر دقیق بگوییم تعدادی نامتناهی جواب خواهیم داشت، ولی ما فقط آن‌جوابهایی را متمایز می‌شماریم که ناهمنهشت به‌هنگ n هستند). هرچندکه درحالت کلی(۴) کاملا پیچیده است، درحالتی که $f(x)$ بسجمله‌ای خطی باشد، مفهوم عکس حسابی به‌ما اجازه خواهد داد تامطلب را دراختیار خود درآوریم. بنابراین اینك به‌مطالعهٔ همنهشتی خطی

$$ax\equiv b\ (n \text{ هنگ}) \qquad (5)$$

می‌پردازیم. حتی یك چنین معادلهٔ ساده‌ای هم ممکن است جواب نداشته باشد، همچنانکه، وقتی‌ما معادلهٔ (هنگ ۴) $2x\equiv 3$ را درنظرگرفتیم، به‌این امر برخوردیم.

فرض کنیم معادلهٔ(۵) یك جواب x دارد، وفرض کنیم s یك‌عامل مشترك a و n باشد.

چون $n|(ax-b)$ به‌ازای مقداری از k خواهیم داشت $b=ax-kn$، وبنا براین s عاملی از b است. بویژه، اگر بمعم$(a ، n)$ را s بگیریم می بینیم که برای اینکه(۵) جوابی داشته باشد، بایستی داشته باشیم $b|$ بمعم$(a ، n)$. این مطلب را به‌صورت یك لم بیان‌می کنیم.

لم ۱۴: اگر همنهشتی $ax\equiv b(n$ هنگ$)$ جوابی داشته باشد، آنگاه $b|$ بمعم$(a ، n)$.

قضیهٔ ۱۵: فرض کنیم ۱ = بمعم$(a ، n)$. فرض کنیم a^* یك‌عکس حسابی a به‌هنگ n باشد. دراین‌صورت x در $ax\equiv b$ (هنگ n) صدق می کند اگر، وفقط اگر، $x\equiv a^*b$ (هنگ n) .

برهان: اگر $ax\equiv b$ (هنگ n)، آنگاه $aa^*x\equiv a^*b$ (هنگ n)، اماچون $aa^*\equiv 1$ (هنگ n)، داریم $x\equiv a^*b$ (هنگ n). اگر $x\equiv a^*b$ (هنگ n) ، آنگاه

$$ax\equiv aa^*b\equiv 1\times b\equiv b(n \text{ هنگ}) . \quad \blacksquare$$

مثال ۱۶:

(یکم)می‌خواهیم معادلهٔ $2x\equiv 5$ (هنگ ۳) راحل کنیم. چون $2^*=2$، جوابها به‌صورت $x\equiv 2\times 5\equiv 1$ (هنگ ۳) می‌باشند. بنابراین، جوابهای معادله کلیهٔ اعدادصحیح به‌صورت $3t+1$ می‌باشند.

(دوم) می‌خواهیم معادلهٔ $3x\equiv 7$ (هنگ ۵) را حل کنیم. دراین حالت، $3^*=2$، و بنابراین $x\equiv 2\times 7\equiv 4$ (هنگ ۵). پس، جوابهای معادله کلیهٔ اعداد صحیح به‌صورت $5t+4$ می‌باشند.

درمثالهای فوق، عکس حسابی a^* را از راه تجسس تعیین کردیم. ولی این روش برای مقادیر کوچك a عملی است. درحالت کلی، a^* رامی‌توان بااستفاده ازروشهای فصل ۲ تعیین کرد، زیرا a^* عکس حسابی a به‌هنگ n است اگر و فقط اگر به‌ازای مقداری از k ، $aa^*-1=kn$؛ یعنی a^* می‌تواند به‌عنوان اولین مؤلفهٔ یك جواب $(x ، y)$ ازمعادلهٔ سیالهٔ $ax+ny=1$ به‌دست‌آورده شود، معادله‌ای که ما به‌طور جامع درفصل ۲ دربارهٔ آن بحث کردیم. بنابراین، a^* به‌روش نسبتاً ساده‌ای تعیین می‌شود.

اینك به‌مطالعهٔ همنهشتی خطی $ax\equiv b(n$ هنگ$)$ درحالت کلی برمی گردیم. فرض کنیم $d=$ بمعم$(a ، n)$. بنابر لم ۱۴، همچنین، می‌توانیم فرض کنیم $d|b$ ، زیرا درغیر این صورت جوابی موجود نیست. پس $b=db_1$. بعلاوه چون $d|a$ و $d|n$، می‌توانیم بنویسیم $a=da_1$ ، $n=dn_1$ وهمنهشتی می‌تواند چنین نوشته شود

$$a_1dx\equiv b_1d(n_1d \text{ هنگ}) .$$

چون $d=$ بمعم$(a ، n)$، مطابق قضیهٔ ۱۱ می‌توانیم بگوییم که x یك‌جواب آخرین همنهشتی است اگر و فقط اگر

$$a_1x\equiv b_1(n_1 \text{ هنگ}) .$$

بعلاوه، چون $d=$ بمعم$(a \text{،} n)$ بنا بر قضیهٔ ۶.۳.۲ (دوم) می‌دانیم که ۱ $=$ بمعم$(a_1 \text{،} n_1)$. بنا براین، جوابهای (هنگ $a_1x \equiv b_1(n_1$ همان جوابهای (هنگ $ax \equiv b(n$ هستند. و بنا بر قضیهٔ ۱۵، جوابهای همنهشتی آخری به‌صورت

$$x \equiv a_1^* b_1 (n_1 \text{ هنگ})$$

هستند که دراینجا a_1^* عکس‌حسابی a_1 به‌هنگ n_1 می‌باشد. بنا براین، سرانجام، می‌توانیم بگوییم:

قضیهٔ ۱۷: فرض کنیم $d=$ بمعم$(a \text{،} n)$. همنهشتی (هنگ $ax \equiv b(n$ حلپذیر است اگر و فقط اگر $d|b$. اگر $d|b$، آنگاه جوابها عبارت‌اند از کلیهٔ xهایی که

$$x \equiv a_1^* \frac{b}{d}\left(\frac{n}{d} \text{ هنگ}\right)$$

که‌دراینجا a_1^* عکس‌حسابی a/d به‌هنگ n/d است. بنا براین جوابهای متمایز به‌هنگ n توسط $x = a_1^*(b/d) + k(n/d)$، $0 \leqslant k \leqslant d-1$ داده می‌شوند.

مثال ۱۸: همنهشتی (هنگ ۱۵)$27x \equiv 3$ را درنظر می‌گیریم. دراینجا

$$3 = \text{بمعم}(27 \text{،} 15) = d \text{ و } 3|3\text{،}$$

پس همنهشتی جواب‌دارد. دراینجا $a/d = 9$، $b/d = 1$، $n/d = 5$، و ۴ یك‌عکس‌حسابی a/d به‌هنگ n/d است. بنا براین‌جوابهای همنهشتی‌عبارت‌اند از (هنگ۵) $x \equiv 4 \times 1 \equiv 4$. برحسب‌همنهشتی به‌هنگ۱۵، جوابهامی‌توانندچنین‌نوشته‌شوند(هنگ۱۵) $x \equiv 4 \text{،} 9$ یا ۱۴. از این قرار، می‌بینیم که بنا بر بحث کلی‌خودمان، این همنهشتی سه جواب متمایز دارد. ولی، توجه کنید که اگر ۱ $=$ بمعم$(a \text{،} n)$، آنگاه بنا بر قضیهٔ ۱۵ فقط یك جواب موجود است[1].

اشاره به‌این‌نکته بی‌فایده نیست که بحث فوق باحل معادلهٔ سیالهٔ خطی دومتغیرهٔ

$$ax + by = c \qquad (۶)$$

ارتباط پیدا می‌کند. دراینجا a و b اعداد صحیح ناصفرند. اگر $b<0$، می‌توانیم معادلهٔ $-ax-by=-c$ را حل کنیم وهمان جوابهای معادلهٔ(۶) را به‌دست‌آوریم، پس فرض می‌کنیم $b>0$. دراین‌صورت(۶) با

$$ax \equiv c(b \text{ هنگ}) \qquad (۷)$$

معادل است. واین مسئله کاملا دربالا مورد بحث قرار گرفت.

---

۱. درحالت‌کلی‌که $d=$ بمعم$(a \text{،} n)$، بنا برقضیهٔ۱۷، d جواب‌متمایز به‌هنگ n موجود است (مترجم).

به‌عنوان مثال، می‌خواهیم

$$۷x+۵y=۳ \qquad (۸)$$

را حل کنیم. این معادله درحکم همنهشتی $۷x\equiv۳$(هنگ ۵) یا $۲x\equiv۳$(هنگ ۵) است. دراینجا $۳\equiv ۲^*$ (هنگ ۵)، و لذا $x\equiv ۳\times۳\equiv۹\equiv -۱$ (هنگ ۵). بنابراین، $x=-۱+۵k$. اگر این نتیجه را درمعادلهٔ(۸) بگذاریم بیدرنگ $y=۲-۷k$ حاصل می‌آید، وبدین طریق معادله حل می‌شود.

باتمام‌وضوحی که این‌روش‌دارد، بایستی‌خاطرنشان‌شودکه بحث فوق‌به دورمی‌انجامد. یعنی‌حل‌معادلهٔ(۷)متضمن‌تعیین a^*،وتنهاروش کلی برای‌تعیینa^*همان‌حل‌معادلهٔ $ax+by=۱$ است. باوجوداین، روش‌همنهشتی‌اغلب راحت‌ترین روش برای‌حل(۶)است، خصوصاً وقتی که a^* را بتوان از راه تجسس تعیین کرد. همچنین‌دستوری برای a^* دربخش۳ داده خواهدشد.

درقضیهٔ۸دیدیم که a یك‌عکس حسابی به‌هنگ n دارد به‌شرط آنکه۱ = بمعم$(a ، n)$.

اینك اجازه دهید عکس این سؤال را عنوان کنیم. کدام اعداد صحیح a یك عکس حسابی a^* دارند؟ این سؤال بااین‌سؤال معادل است که به‌ازای چه‌مقادیری از a همنهشتی

$$aa^*\equiv۱\ (\text{هنگ } n)$$

برحسب a^* حلپذیراست؟ فرض‌کنیم بمعم$(a ، n)=d$. بنابر قضیهٔ ۱۷، a^* موجود است اگروفقطاگر $d|۱$، یعنی $d=۱$. بنابراین،می‌بینیم که aهایی که یك‌عکس حسابی به‌هنگn دارند دقیقاً آنهایی هستندکه برای‌آنها داریم ۱ = بمعم$(a ، n)$. اجازه دهید سعی‌کنیم‌این اعداد را بهتر تشریح‌کنیم. برای انجام این‌امر، به‌لم زیراحتیاج داریم.

لم ۱۹: فرض‌کنیم ۱ = بمعم$(a ، n)$ و$a\equiv a'$(هنگ n). دراین‌صورت۱ = بمعم$(a' ، n)$.[1]

برهان: چون $a\equiv a'$(هنگ n)، عددی‌مانند k وجود دارد به‌طوری که $a=a'+kn$. فرض کنیم بمعم$(a' ، n)$بزرگتراست‌از۱ دراین‌صورت‌عدد اولی‌مانندp موجود است به‌طوری که بمعم$p|(a' ، n)$. پس، بنابرتعریف بمعم، $p|a'$ و $p|n$. اما دراین‌صورت $p|a'+kn$، وبنابراین $p|a$. این مستلزم آن‌است که بمعم$p|(a ، n)$، پس ۱ < بمعم$(a ، n)$، واین یك تناقض است. ■

از لم قبلی، به‌سادگی می‌توانیم اعداد صحیح را با عکسهای حسابی تشریح‌کنیم. دستگاه‌کامل مانده‌ها به‌هنگ n راکه توسط ۰ ، ۱ ، ۲ ، ... ، $n-۱$ مشخص شده‌اند درنظر می‌گیریم. هرعدد صحیحx دقیقاً بایکی‌از اعداد ۰ ، ۱ ، ... ، $n-۱$ همنهشت‌است. فرض کنیمxیك‌عکس‌حسابی به‌هنگ n دارد و$x\equiv a$(هنگ n) ، $۰\leqslant a\leqslant n-۱$. دراین‌صورت بنابر بحث‌فوق، ۱ = بمعم$(x ، n)$ وبنابراین‌ازلم ۱۹می‌بینیم که ۱ = بمعم$(a ، n)$. بالعکس، اگر x عدد صحیح غیر مشخصی باشد به‌طوری که $x\equiv a$(هنگ n)$(۰\leqslant a\leqslant n-۱)$، و

---

۱. به‌مسئلهٔ ۳۲ مراجعه‌کنید(مترجم).

۱ = بمعم$(a ، n)$، آنگاه x یك‌عکس‌حسابی به‌هنگ n دارد. زیرا، چون ۱ = بمعم$(a ، n)$، a یك‌عکس‌حسابی a^* دارد، و a^* یك عکس حسابی برای x است زیرا

$$xa^* \equiv aa^* \equiv 1 \ (\text{هنگ } n) \ .$$

بنابراین، قضیهٔ زیر را کاملا ثابت‌کرده‌ایم:

قضیهٔ ۲۰: در دستگاه‌کامل مانده‌های ۰ ، ۱ ، ... ، $n-1$ فرض‌کنیم تمامی اعداد a که درشرط ۱ = بمعم$(a ، n)$ صدق‌می‌کنند توسط دنبالهٔ a_1 ، a_2 ، ... ، a_t مشخص‌شده‌باشند. دراین‌صورت عددصحیح x عکس‌حسابی به‌هنگ n دارد اگروفقط‌اگر به‌ازای مقداری از i

$$x \equiv a_i \ (\text{هنگ } n) \ .$$

مثال ۲۱:

(یکم) هرگاه $n = 3$، آنگاه اعداد صحیح a ازمیان اعداد ۰ ، ۱ ، ۲ به‌طوری‌که ۱ = بمعم$(a ، 3)$ باشد، ۱ و ۲ هستند، بنابراین $t = 2$ و x یك‌عکس‌حسابی به‌هنگ ۳ دارد اگروفقط‌اگر (هنگ ۳) ۲ یا ۱ $\equiv x$.

(دوم) هرگاه $n = 12$ آنگاه اعداد صحیح a از میان اعداد ۰ ، ۱ ، ۲ ، ... ، ۱۱ به‌طوری‌که ۱ = بمعم$(a ، 12)$ ، عبارت‌اند از ۱ ، ۵ ، ۷ ، ۱۱ ، بنابراین $t = 4$ و x یك عکس حسابی به‌هنگ ۱۲ دارد اگروفقط‌اگر (هنگ ۱۲) ۱۱ یا ، ۷ ، ۵ ، ۱ $\equiv x$.

(سوم) هرگاه $n = p$، یك‌عدد اول‌باشد. اعدادصحیح a از میان‌اعداد ۰، ۱، ...، $p-1$ به‌طوری‌که ۱ = بمعم$(a ، p)$، عبارت‌اند از ۱ ، ۲ ، ... ، $p-1$، زیرا p عددی است‌اول. بنابراین، x به‌هنگ عدد اول p یك عکس حسابی دارد اگر وفقط اگر

$$x \equiv 1 ، 2 ، 3 ، \ldots ، p-1 \ (\text{هنگ } p) .$$

درقضیهٔ ۲۰ از دستگاه کامل مانده‌های ۰ ، ۱ ، ۲ ، ... ، $n-1$ به‌هنگ n استفاده شده است. ولی برمتعلم است که تحقیق‌کند درقضیهٔ ۲۰ به‌جای ۰ ، ۱ ، ... ، $n-1$ هردستگاه کاملی از مانده‌ها به‌هنگ n می‌تواند به‌کار برده شود وبازهم قضیه برقرار بماند. با همین مقدار بررسی، متعلم توجه خواهد داشت‌که اعضای a ازیك دستگاه‌کامل مانده‌ها به‌هنگ n که نسبت به n اول هستند خیلی خاص می‌باشند. این امر تعریف زیر را موجب‌می‌شود:

تعریف ۲۲: یك دستگاه مخفف مانده‌ها به هنگ n مجموعه‌ای است از اعداد صحیح a_1 ، ... ، a_t باخصوصیت زیر: هرعددصحیح x که ۱ = بمعم$(x ، n)$ بایك و تنها یکی از اعداد a_1 ، ... ، a_t همنهشت است.

ساده‌ترین راه برای به‌دست‌آوردن یك دستگاه مخفف مانده‌ها به‌هنگ n این‌است‌که تعیین‌کنیم کدامیك از اعدادصحیح a ازیك دستگاه کامل مانده‌های مفروض به‌هنگ n نسبت به n اول‌هستند. مجموعهٔ چنین اعداد صحیحی یك دستگاه مخفف مانده‌ها به‌هنگ n است.

زیرا فرض کنیم r_1 ، ... ، r_n دستگاه کاملی از مانــدهها بههنگ n باشد و از میان اعــداد r_1 ، ... ، r_n اعداد صحیحی که نسبت به n اول هستند a_1 ، ... ، a_t باشند. دراین‌صورت اگر x عــدد صحیحی باشد چنان‌که ۱ = بمعم$(x ، n)$، مطمئناً به‌ازای مقداری از i داریـم $x \equiv r_i$ (هنگ n) (چون r_1 ، ... ، r_n تشکیل دستگاه کاملی از ماندهها بههنگn می‌دهند). بعلاوه، چون ۱ = بمعم$(x ، n)$ بنابر لم۱۹ داریم ۱ = بمعم$(r_i ، n)$. بنابـراین، r_i یکی‌از اعـداد a_1 ، ... ، a_t است ، و درایــن‌صورت بــه‌ازای مقداری از j ، $x \equiv a_j$ (هنگ n). بالاخره، x فقط بایکی از اعداد a_1 ، ... ، a_t همنهشت است، چــون‌که a_jها قسمتی از یك دستگاه کامل ماندهها بههنگ n می‌باشند. پس، a_1 ، ... ، a_t یك دستگاه مخفف ماندهها به هنگ n است.

مثال ۲۳:

(یکم) هرگاه ۳ = n ، آنگاه ۱ ، ۲ دستگاه مخففی ازماندهها بههنگ۳ است.

(دوم) اگر ۱۲ = n، آنگاه ۱ ، ۵ ، ۷ ، ۱۱ دستگاه مخففی ازماندهها بههنگ۱۲ است. ۱$\pm$ ، ۵$\pm$ یك دستگاه دیگر می‌باشد.

(سوم) ۱ ، ۲ ، ... ، $p-1$ دستگاه مخففی از ماندهها بههنگ $n=p$ است، کــه درآن p عددی است اول.

(چهارم) دستگاه مخفف ماندهها که از دستگاه‌کامل ماندههای ۲۵ ، ۲۶ ، ۲۷ ، ۲۸، ۲۹ بههنگ۵ به‌دست می‌آید، درست ۲۶ ، ۲۷ ، ۲۸ ، ۲۹ است.

اگر a_1 ، ... ، a_t و b_1 ، ... ، b_s دو دستگاه مخفف‌ماندهها بههنگ n باشند، آنگاه هر a_i دقیقاً بایك b_j بههنگnهمنهشت است وهیچ‌دو a_iای‌بایك b_j همنهشت نیستند. بعلاوه، هر b_j دقیقاً بایك a_i همنهشت‌است‌وهیچ‌دو b_jای بایك a_i همنهشت‌نیستند. بنابراین، $s=t$، وتعداد اعضای هر دو دستگاه مخفف ماندهها بههنگn مساوی هستند. با استفاده از دستگاه مخفف ماندهها که از دستگاه کامل ماندههای ۰ ، ۱ ، ... ، $n-1$ به‌دست می‌آید، می‌بینیم که‌تعداد اعداد یك دستگاه مخفف ماندهها بههنگn برابر است باتعداد اعداد صحیح‌مابین ۰ و $n-1$ که نسبت به n اول هستند[1].

تعریف۲۴: فرض کنیم $\varphi(n)$ معرف تعداد اعدادصحیح مابین ۰ و $n-1$ باشد که نسبت به n اول‌اند. $\varphi(n)$، به‌یاد ریاضیدان سویسی لئونهارد اویلر، که اول‌بار خواص‌آن را مطالعه کرد، **تابع فی اویلر** نامیده می‌شود[2].

---

۱. چون $n \equiv$ ۰ (هنگ n) به‌جای ۰ ، ۱ ، ... ، $n-1$ دستگاه‌کامل‌ماندههای ۱ ، ۲ ، ... ، n رادرنظرگرفته‌ودرنتیجه تعداد اعضای‌یك دستگاه مخفف‌ماندهها برابراست باتعداد اعدادطبیعی نابیشتر از nکه نسبت به n اول هستند (مترجم).

۲. توجه داشته باشیدکه درتعریف داریم $\varphi(1)=1$.

جدولی (جدول ۱) از مقادیر $\varphi(n)$ به‌ازای $n \leqslant ۲۰۰$ درآخر کتاب آورده‌ایم[۱].

از بحث فوق، به‌نتیجهٔ زیر می‌رسیم:

قضیهٔ ۲۵: تعداد اعدادصحیح درهر دستگاه مخفف مانده‌ها به‌هنگ n یکی و دقیقاً مساوی $\varphi(n)$ است.

مثال ۲۶: از مثال ۲۳، می‌بینیم که $\varphi(۳) = ۲$ ، $\varphi(۱۲) = ۴$ ، $\varphi(p) = p - ۱$ به‌ازای عدد اول p ، $\varphi(۵) = ۴$. توجه داشته‌باشید که درحالت کلی $\varphi(n) = n - ۱$ درست نیست، به‌عنوان‌مثال $\varphi(۱۲) = ۴ \neq ۱۲ - ۲$.

ماهم به‌مفهوم دستگاه مخفف‌مانده‌ها به‌هنگn وهم به‌مفهوم تابع اویلر، فی ، بعداً دراین فصل و همچنین درفصلهای دیگر کتاب برخورد خواهیم کرد، و بنابراین از بحث بیشتر دراینجا خودداری می‌کنیم.

پیش‌ازاینکه این بخش را به‌پایان برسانیم از روش همنهشتیها برای مطالعهٔ یك معادلهٔ سیالهٔ خاص استفاده می‌کنیم. معادلهٔ

$$x^۳ + y^۳ = z^۳$$

راکه حالت خاصی از معادلهٔ معروف فرما است درنظر می‌گیریم. نشان خواهیم دادکه

اگر (x , y , z) یك جواب معادلهٔ $x^۳ + y^۳ = z^۳$ باشد، آنگاه لااقل یکی از اعداد x ، y ، z بر ۳ بخشپذیر است.

اثبات: در واقع، نشان خواهیم دادکه همنهشتی

$$x^۳ + y^۳ \equiv z^۳ \ (\text{هنگ } ۹) \qquad (۹)$$

مارا دراستخراج نتیجه یاری خواهدکرد.

ابتدا مشاهده می‌کنیم که اگر w عددی صحیح باشد، آنگاه

$$w^۳ \equiv w \ (\text{هنگ } ۳)$$

زیرا ۱ — ، ۰ ، ۱ دستگاه کاملی از مانده‌ها به‌هنگ ۳ است و صدق کردن هرسهٔ آنهارا یك‌بیك بسهولت‌می‌توان بررسی کرد. ازآنجایی که هر همنهشتی به‌هنگ۹ یك‌همنهشتی به هنگ ۳ نیز هست، همنهشتی(۹) می‌گویدکه

$$x + y \equiv z (\text{هنگ } ۳) \ , \qquad (۱۰)$$

بنابراین به‌ازای مقداری مانند a داریم

$$z = x + y + ۳a \ .$$

اگر این مقدار را درمعادلهٔ(۹) قرار دهیم نتیجه خواهد شد

---

۱. جدول آخرکتاب مقادیر $\varphi(n)$ را بازاء $n \leqslant ۱۰۰$ دارد (مترجم).

$$\begin{aligned} x^{۳}+y^{۳}\equiv z^{۳} &= (x+y+۳a)^{۳} \\ &= x^{۳}+y^{۳}+۳x^{۲}y+۳y^{۲}x+۹x^{۲}a+۹y^{۲}a \\ &\quad +۲۷a^{۲}x+۲۷a^{۲}y+۲۷a^{۳}+۱۸xya \\ &\equiv x^{۳}+y^{۳}+۳x^{۲}y+۳y^{۲}x \ (\text{هنگ } ۹)\,. \end{aligned}$$

پس از حذف $x^{۳}+y^{۳}$ ازطرفین همنهشتی نتیجه می‌شود

$$۳xy(x+y)\equiv ۰ \ (\text{هنگ } ۹)\,,$$

یا از قضیهٔ ۱۱

$$xy(x+y)\equiv ۰ \ (\text{هنگ } ۳)\,.$$

استفادهٔ مجدد از (۱۰) نشان می‌دهد که

$$xyz\equiv ۰ \ (\text{هنگ } ۳)\,.$$

یعنی، $۳|xyz$، بنابراین x ، y ، یا z بر ۳ بخشپذیر است. ■

۲.۳ تمرینات

۱. فرض کنیم $f(x)=۱۱x^{۳}+۱۵x^{۲}+۹x-۲$.

(آ) باقیماندهٔ تقسیم $f(۲)$ بر ۷ را بیابید.

(ب) باقیماندهٔ تقسیم $f(۶)$ بر ۷ را بیابید.

(ج) باقیماندهٔ تقسیم $f(۹۷)$ بر ۱۱ را بیابید.

۲. نشان دهید که هریك از دسته عددهای زیر، دستگاه کامل مانده‌ها به‌هنگ ۱۱ است:

(آ) -۵ ، -۴ ، -۳ ، -۲ ، -۱ ، ۰ ، ۱ ، ۲ ، ۳ ، ۴ ، ۵.

(ب) ۰ ، ۱۲ ، ۲۴ ، ۳۶ ، ... ، ۱۲۰.

(ج) ۲۰ ، ۲۱ ، ۲۲ ، ۲۳ ، ... ، ۳۰.

(د) هر ۱۱ عدد متوالی.

۳. اگر n عدد صحیح مثبتی باشد، $n!$ (فاکتوریل n) را با $n!=n(n-۱)\dots ۱$ تعریف می‌کنیم.

(آ) ازمیان دستگاه کامل مانده‌های ۰ ، ۱ ، ... ، $n-۱$ ، به‌ازای $n\leqslant ۲۴$، کدامیك همنهشت $(n-۱)!$ به‌هنگ n است؟

(ب) برمبنای قسمت(آ) آیا می‌توانید حدسی کلی بزنید؟

۴. دستگاه مخفف مانده‌های مربوط به‌دستگاه کامل مانده‌های ۰ ، ۱ ، ... ، $n-۱$ را به‌ازای

(آ) $n=9$، (ب) $n=15$، (ج) $n=24$،

بیابید.

۵. برمبنای تمرین۴، $\varphi(9)$، $\varphi(15)$، $\varphi(24)$ را محاسبه کنید.

۶. ثابت کنید که $\varphi(p^r)=p^r-p^{r-1}$، p عددی است اول.

۷. کلیهٔ جوابهای همنهشتیهای زیر را بیابید.

(آ) $3x\equiv 1$ (هنگ 5). (ب) $x^2+1\equiv 0$ (هنگ 4).

(ج) $x^3+2x+1\equiv 0$ (هنگ 7).

(د) $x^5+x^4+x^3+x+1\equiv 0$ (هنگ 5).

۸. باقیماندهٔ تقسیم 11^{p-1} بر p را بیابید، وقتی که

(آ) $p=2$. (ب) $p=3$. (ج) $p=5$. (د) $p=7$. (ه) $p=11$.

(و) $p=13$.

(ز) درقسمتهای (آ) تا (و) به‌جای ۱۱ عدد ۵ بگذارید و آنهارا حل کنید.

۹. باقیماندهٔ تقسیم $3^{\varphi(n)}$ بر n را محاسبه کنید، که در آن

(آ) $n=1$. (ب) $n=2$. (ج) $n=3$. (د) $n=4$. (ه) $n=5$. (و) $n=6$.

(ز) $n=7$.

(ح) درقسمتهای (آ) تا (ز) به‌جای ۳ عدد ۵ بگذارید و آنها را حل کنید.

(ط) آیا می‌توانید براساس قسمتهای (آ) تا (ح) حدسی بزنید؟

۱۰. همنهشتیهای زیر را حل کنید:

(آ) $3x\equiv 9$ (هنگ 5). (ب) $3x\equiv 9$ (هنگ 24). (ج) $5x\equiv 15$ (هنگ 12).

۱۱. عکسهای حسابی عددهای ۱، ۲، ۳، ۷، ۹، ۱۰ را به‌هنگ ۱۱ بیابید.

۱۲. (آ) اعداد صحیحی که به هنگ ۱۸ عکس حسابی دارند، کدام‌اند؟

(ب) عکس حسابی به‌هنگ ۱۸ کلیهٔ اعداد صحیحی را که عکس دارند بیابید.

۱۳. فرض کنیم a^* و b^* عکسهای‌حسابی a به‌هنگ n باشند. ثابت کنید که $a^*\equiv b^*$ (هنگ n).

۱۴. همنهشتیهای خطی زیر را حل کنید:

(آ) $2x\equiv 5$ (هنگ 7). (ب) $19x\equiv 15$ (هنگ 8).

(ج) $6x\equiv 12$ (هنگ 14). (د) $13x\equiv 27$ (هنگ 52).

۱۵. (آ) نشان دهید که ۱۱۴۳ یك عکس حسابی به‌هنگ ۱۹۵۷ دارد.

(ب) عکس حسابی درقسمت (آ) را بیابید.

۱۶. نشان دهید که هر مکعب کامل با ۰ ، ۱ یا ۱ − همنهشت به‌هنگ ۹ است.

۱۷. نشان دهید که قوهٔ چهارم هر عدد همنهشت ۰ یا ۱ به‌هنگ ۵ است.

۱۸. فرض کنیم r_1 ، ... ، r_n دستگاه کاملی از مانده‌ها به‌هنگ n باشد.

(آ) نشان‌دهید که اگر a عددی صحیح باشد، آنگاه r_1+a ، ... ، r_n+a یك دستگاه کامل مانده‌ها به‌هنگ n است.

(ب) نشان دهید که اگر ۱ = بمعم$(a ، n)$ ، آنگاه ar_1 ، ... ، ar_n یك دستگاه کامل مانده‌ها به‌هنگ n است[1].

۱۹. فرض کنیم s_1 ، ... ، $s_{\varphi(n)}$ یك دستگاه مخفف مانده‌ها به‌هنگ n باشد.

(آ) نشان دهید که اگر ۱ = بمعم$(a ، n)$ ، آنگاه as_1 ، ... ، $as_{\varphi(n)}$ یك دستگاه مخفف مانده‌ها به‌هنگ n است.

(ب) آیا این‌درست‌است که به‌ازای کلیهٔ‌اعداد صحیح a، اعداد s_1+a ،... ، $s_{\varphi(n)}+a$ یك دستگاه مخفف مانده‌ها به‌هنگ n است[2]؟

۲۰. فرض کنیم p عددی اول و r عدد صحیح مثبتی باشد. فرض کنیم a عکس حسابی به هنگ p^r نداشته باشد. دراین‌صورت‌نشان‌دهید که توانی از a همنهشت ۰ به‌هنگ p^r است.

۲۱. فرض کنیم a عدد صحیحی باشد. یك‌برنامه برای کامپیوتر بنویسید تا تعیین کند کدامیك از اعداد ۰ ، ۱ ، ... ، $n-1$ ، همنهشت a به‌هنگ n است.

۲۲. فرض کنیم $f(x)$ یك بسجملهٔ باضرایب صحیح باشد. یك برنامه برای کامپیوتر بنویسید تا تعیین کند که کدامیك از اعداد صحیح ۰ ، ۱ ، ... ، $n-1$ همنهشت $f(x)$ به‌هنگ n است. سعی کنید محاسباتتان تا سرحدامکان کارآمد باشد، درنظر داشته باشید که یك محاسبهٔ ساده چیست. اصولا محاسبات شماممکن است اعدادی بدهند که برای کامپیوتر خیلی بزرگ باشند.

۲۳. کلیهٔ جوابهای همنهشتی $2x+3y\equiv 5$ (هنگ ۷) را بیابید.

۲۴. کلیهٔ جوابهای همنهشتی $x^2+y^2-5y-2\equiv 0$ (هنگ ۹) را بیابید.

*۲۵. چه وقت ممکن است همنهشتی $a_1x_1+\dots+a_mx_m\equiv b$ (هنگ n) برحسب x_1 ، ... ، x_m حل بشود؟ اگرحل آن ممکن‌باشد، جوابها چه خواهند بود؟

۱. (ج) از (آ) و (ب) نتیجه بگیریدکه اگر ۱ = بمعم$(a،n)$، آنگاه ar_1+b ،... ، ar_n+b یك دستگاه کامل مانده‌ها به‌هنگ n است. یا ابتدا (ج) را ثابت‌کنید وسپس (آ) و (ب) را به‌عنوان حالت خاص از آن نتیجه بگیرید (مترجم).

۲. (ج) آیا می‌توانید aهایی راتعیین‌کنیدکه به‌ازای آنها s_1+a ، ... ، $s_{\varphi(n)}+a$ دستگاه مخففی از مانده‌ها به‌هنگ n باشد (مترجم).

۲۶. (نُه، نُه کنار گذاشتن) فرض کنیم عددصحیح زیر به‌ما داده شده است

$$x = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0 \text{،}$$

a_iها یکی از اعداد ۰، ۱، …، ۹ هستند. دراین‌صورت $a_n \ldots a_0$ نمایش اعشاری عدد صحیح x است.

(آ) نشان دهید که

$$x \equiv a_n + a_{n-1} + \cdots + a_0 \ (\text{هنگ } 9) \ .$$

(ب) آیا ۵۷۸۵۶۸۴ بر ۹ بخشپذیر است؟

۲۷. قسمت (دوم) قضیهٔ۲ را ثابت کنید.

۲۸. (آ) نشان دهید که ۲ عکس حسابی به‌هنگ ۴ ندارد.

(ب) عدد ۲ به‌هنگ چه‌اعدادی عکس حسابی دارد؟ این عکس چیست؟

۲۹. یك اثبات مستقیم برای قضیهٔ ۱۰ بدون استفاده ازقضیهٔ ۸ ارائه دهید.

۳۰. فرض کنیم r_1، …، r_n یك دستگاه‌کامل مانده‌ها به‌هنگ n باشد، و فرض کنیم که ازمیان اعداد r_1، …، r_n آنهایی که با n اول هستند a_1، a_2، …، a_t باشند، یعنی به‌ازای $i = 1$، …، t تساوی ۱ = بمعم$(a_i ، n)$ برقرار باشد. دراین‌صورت x یك عکس حسابی به‌هنگ n دارد اگر، وفقط اگر، به‌ازای مقداری‌از i، $x \equiv a_i$ (هنگ n).

۳۱. فرض کنیم ۱ = بمعم$(a ، n)$. با استفاده ازاین واقعیت که x و yیی موجودندبه‌طوری که $ax + ny = 1$ ثابت کنید که همنهشتی $ax \equiv b$ (هنگ n) یك جواب دارد.

۳۲. ثابت کنید که اگر $a \equiv a'$ (هنگ n)، آنگاه بمعم$(a ، n)$ = بمعم$(a' ، n)$. (این تعمیم لم ۱۹ است.)

۳۳. فرض‌کنیم n عددصحیح مفروضی باشد.

(آ) نشان‌دهید که $x^2 - y^2 = n$ برحسب‌اعداد صحیح حلپذیر است اگر، وفقط اگر، n فرد باشد یا $4 | n$.

(ب) اگر $x^2 - y^2 = n$ برحسب اعدادصحیح حلپذیر باشد، کلیهٔ جوابهای آن را تعیین کنید.

۳۴. نشان‌دهید که‌تعداد کسورتحویلناپذیر a/b، $0 < a/b \leqslant 1$، $1 \leqslant b \leqslant n$ درست برابر با $\varphi(1) + \varphi(2) + \cdots + \varphi(n)$ است.

۳۵. فرض کنیم n عددی فرد و r_1، …، r_k یك دستگاه مخفف مانده‌ها به‌هنگ n باشد. نشان دهید که

$$r_1 + r_2 + \cdots + r_k \equiv 0 \ (\text{هنگ } n) \ .$$

*۳۶. (اویلر) نشان دهید که $2^{2^5}+1$ بر ۶۴۱ بخشپذیر است.
(راهنمایی: $2^{32}=2^4\times 2^{28}=(641-5^4)\times 2^{28}$.)

۳۷. ثابت کنید که وقتی k فرد است $11^{2k}+19^{2k}$ بر ۲۴۱ بخشپذیر است.

۳۸. (آ) به‌ازای $n=2, 3, 4, 6, 8, 12, 18, 24, 30$، نشان‌دهید که اعداد صحیح بین ۱ و n که نسبت به n اول‌اند (یعنی، دستگاه استانده مخفف مانده‌ها به هنگ n) شامل ۱ و اعداد اول است.

*(ب) نشان دهید که به‌ازای $n>30$، دستگاه استانده مخفف مانده‌ها به هنگ n همواره شامل یك عدد مرکب است.

۳۹. دستگاه همنهشتیهای

$$2x+7y\equiv 2 \text{ (هنگ ۵)}$$

$$3x-y\equiv 11 \text{ (هنگ ۵)}$$

راحل کنید.

۳.۳ چند همنهشتی خاص

دراین بخش، دو همنهشتی خاص را که هم ازلحاظ تاریخی وهم از لحاظ فنی در نظریهٔ اعداد مهم هستند اثبات خواهیم کرد. همنهشتی اول از اویلر است و تعمیمی از یك قضیهٔ فرما می‌باشد. دومی قضیهٔ کوچك فرما (برای تمایز آن از آخرین قضیهٔ فرما) نامیده می‌شود. دومین قضیه، قضیهٔ ویلسن نامیده می‌شود. ما این دو قضیه را اثبات خواهیم کرد و بعضی ازکاربردهای آنها را نیز نشان خواهیم‌داد.

اصولا، همواره می‌توان‌آزمایش کرد که آیا دوعدد صحیح x و y به‌هنگ n همنهشت هستند یا نه. کافی‌است که فقط $x-y$ را محاسبه وبر n تقسیم کنیم. اما اگر $x-y$ بزرگ باشد، انجام تقسیم‌کار طاقت فرسایی است. هم قضیهٔ اویلر وهم قضیهٔ ویلسن به ما اجازه می‌دهند، که بعضی همنهشتیها را که درآنها x و y بسیار بزرگ هستند حل کنیم. بعلاوه، مزیت‌آنها این است که آنها همنهشتیهای «کلی» هستند.

ابتدا قضیهٔ فرما را بیان‌می‌کنیم.

قضیهٔ ۱: (قضیهٔ کوچك فرما) : هرگاه p عددی اول باشد و $p\nmid a$، آنگاه

$$a^{p-1}\equiv 1 \text{ (هنگ } p\text{)}\,.$$

قبل از اثبات قضیهٔ فرما چند مثال می‌آوریم. داریم $2^{10}\equiv 1$ (هنگ ۱۱) و $99^{820}\equiv 1$ (هنگ ۸۲۱). (۸۲۱ عددی است اول). بعلاوه، محاسبات مثال ۶′.۲ باتوجه به‌قضیهٔ فرما بدیهی است. ماکاربرد دیگری ارائه خواهیم داد که درنوع خود برجسته‌است.

می‌خواهیم باقیماندهٔ تقسیم $۲^{۱۱۳۷}$ بر ۱۷ را تعیین کنیم چون ۱۷ عددی اول است و ۱۷∤۲ قضیهٔ فرما ایجاب می کند که

$$۲^{۱۶} \equiv ۱ \ (\text{هنگ } ۱۷) \, .$$

داریم

$$۱۱۳۷ = ۱۶ \times ۷۱ + ۱ \, .$$

بنابراین،

$$۲^{۱۱۳۷} = (۲^{۱۶})^{۷۱} \times ۲^{۱} \equiv ۱^{۷۱} \times ۲ = ۲ \ (\text{هنگ } ۱۷) \, .$$

لذا، باقیماندهٔ تقسیم $۲^{۱۱۳۷}$ بر ۱۷ برابر ۲ است. توجه کنید که $۲^{۱۱۳۷}$ عدد بسیار بزرگی است که واقعاً تقسیم آن بر ۱۷ غیرعملی خواهد بود.

با توجه به‌مثال ۲۶.۲، اگر $n = p$ عددی اول باشد، آنگاه $\varphi(n) = p - ۱$، و می بینیم که قضیهٔ فرما حالت خاصی است ازقضیهٔ زیر که منسوب به اویلر است:

قضیهٔ ۴ (اویلر): اگر $(a \text{ ، } n)$بمعم $= ۱$، آنگاه

$$a^{\varphi(n)} \equiv ۱ \ (\text{هنگ } n) \, ,$$

که دراینجا $\varphi(n)$ معرف تابع فی‌اویلر است.

برهان: فرض کنیم $r_۱$ ، … ، $r_{\varphi(n)}$ دستگاه‌مخففی‌ازمانده‌ها به‌هنگ n باشد. (تعریف ۲۲.۲ و بحث بعد ازآن را ببینید.) چون $(a \text{ ، } n)$بمعم $= ۱$ و $(r_i \text{ ، } n)$بمعم $= ۱$، می بینیم که به ازای جمیع‌مقادیر i ، $(ar_i \text{ ، } n)$بمعم $= ۱$. بنابراین، مطابق‌تعریف دستگاه مخفف‌مانده‌ها، هر ar_i با یکی از اعداد صحیح $r_۱$ ، … ، $r_{\varphi(n)}$ همنهشت است. بعلاوه، هیچ دو ar_iای همنهشت یك r_j نیستند، زیراکه اگر $ar_i \equiv r_j$ (هنگ n) و $ar_{i'} \equiv r_j$ (هنگ n)، آنگاه

$$ar_i \equiv ar_{i'} \ (\text{هنگ } n)$$

بنابراین $r_i \equiv r_{i'}$ (هنگ n) (قضیهٔ ۲ . ۱۰)، که چون هیچ دوعددی‌از دنبالهٔ $r_۱$ ، … ، $r_{\varphi(n)}$ به‌هنگ n باهم‌همنهشت‌نیستندلازم می‌آید $r_i = r_{i'}$. پس، می بینیم که $ar_۱$ ، … ، $ar_{\varphi(n)}$ با $\varphi(n)$ عدد صحیح متمایز $r_۱$ ، … ، $r_{\varphi(n)}$ همنهشت هستند. یعنی $ar_۱$ ، … ، $ar_{\varphi(n)}$ بـه ترتیبی با $r_۱$ ، … ، $r_{\varphi(n)}$ همنهشت به‌هنگ n هستند.

بنابراین،

$$(ar_۱)(ar_۲) \cdots (ar_{\varphi(n)}) \equiv r_۱ r_۲ \cdots r_{\varphi(n)} \ (\text{هنگ } n)$$

ازآنجا

$$r_۱ r_۲ \cdots r_{\varphi(n)} a^{\varphi(n)} \equiv r_۱ r_۲ \cdots r_{\varphi(n)} \ (\text{هنگ } n)$$

چون $(r_۱ \cdots r_{\varphi(n)} \text{ ، } n)$بمعم $= ۱$ ، مجدداً قضیهٔ ۲ . ۱۰ ایجاب می کند که

$$a^{\varphi(n)} \equiv 1 \ (\text{هنگ}\ n) .$$

و این اثبات قضیهٔ اویلر را تکمیل می‌کند. ■

یکی از کاربردهای جالب قضیهٔ اویلر این است که به‌ما اجازه می‌دهد تا به‌طورصریح عکس حسابی اعداد صحیح به هنگ n را نشان دهیم. فرض کنیم ۱ = بمعم(a , n). در این صورت می‌بینیم که $a^* = a^{\varphi(n)-1}$ یك‌عکس حسابی a به هنگ n است، زیرا بنا بر قضیهٔ اویلر ملاحظه می‌کنیم که

$$aa^* = a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 \ (\text{هنگ}\ n)$$

بنابراین، $a^{\varphi(n)-1}$ یك عکس حسابی a به هنگ n است.

اکنون به قضیهٔ ویلسن برمی‌گردیم.

قضیهٔ ۳ (ویلسن): هرگاه p عددی اول باشد، آنگاه

$$(p-1)! \equiv -1 \ (\text{هنگ}\ p) .$$

برهان: اگر ۳ یا ۲ $= p$ قضیه می‌تواند مستقیماً بررسی شود چون

$$1 \equiv -1 \ (\text{هنگ}\ 2)$$

$$1 \times 2 \equiv -1 \ (\text{هنگ}\ 3) .$$

پس می‌توانیم فرض کنیم $p > 3$.

روش اثبات این است که اعداد صحیح ۲ ، ۳ ، ... ، $p-2$ را به‌زوجهایی از اعداد صحیح چنان قسمت کنیم، که حاصلضرب هرزوج همنهشت ۱ باشد. پس فقط ۱ و $p-1$ در حاصلضرب $(p-1)!$ باقی می‌مانند که ازآن نتیجه روشن است.

به ازای هرعدد صحیح r ، $1 \leqslant r \leqslant p-1$ ، فرض کنیم r^* عکس حسابی آن به هنگ p باشد که دربازهٔ $1 \leqslant r^* \leqslant p-1$ قراردارد. (چون $p \nmid r$ ، عکس حسابی r وجود دارد؛ مطمئناً می‌توانیم r^* را طوری انتخاب کنیم که $0 \leqslant r^* \leqslant p-1$ زیرا که ۰ ، ۱ ، ... ، $p-1$ دستگاه کاملی ازمانده‌ها به‌هنگ p است؛ بالاخره، $r^* = 0$ ایجاب می‌کند که $1 \equiv rr^* = 0 \ (\text{هنگ}\ p)$ ، که بی‌معنی است.) به هر عدد صحیح r عکس حسابیش را تخصیص می‌دهیم. به‌خصوص، r^* به‌عکس حسابی خودش تخصیص‌داده شده‌است، که آنرا با r^{**} نشان می‌دهیم. اما

$$r^* r^{**} \equiv 1 \ (\text{هنگ}\ p)$$

و

$$r^* r \equiv 1 \ (\text{هنگ}\ p)$$

ایجاب می‌کند که $r^* r \equiv r^* r^{**} \ (\text{هنگ}\ p)$ و بنابراین بنابر قضیهٔ ۲ . ۱۰ داریم

$r^{**}\equiv r$ (هنگ p) . چون‌هر‌دوعدد صحیح r و r^{**} ما بین ۱ و $p-۱$ قراردارند،می‌بینیم که $r=r^{**}$. پس، به‌عدد صحیح r^* عدد r را تخصیص داده‌ایم. به‌این ترتیب ، اعداد صحیح ۱ ، ۲ ، ... ، $p-۱$ را به‌زوجهایی از اعداد صحیح (r , r^*) قسمت کرده‌ایم مگر اینکه $r=r^*$. اما $r=r^*$ ایجاب‌می کند که $r\equiv r^*$ (هنگ p)، و بنا براین $r^۲\equiv rr^*\equiv ۱$ (هنگ p)؛ دراین‌صورت داریم $p|r^۲-۱=(r-۱)(r+۱)$ وبنا براین $p|r-۱$ یا $p|r+۱$. پس $r\equiv ۱$ (هنگ p) یا $r\equiv -۱\equiv p-۱$ (هنگ p) . بنا براین اگر دو عدد ۱ و $p-۱$ را از فهرست ۱ ، ۲ ، ... ، $p-۱$ خارج کنیم، $p-۳$ عدد صحیح ۲ ، ۳ ، ... ، $p-۲$ را به $s=\frac{p-۳}{۲}$ زوج تقسیم کرده‌ایم که هیچ عضومشترك ندارند. حال‌این زوجها را فهرست می کنیم :

$$(r_۱ , r_۱^*) , \ldots , (r_s , r_s^*) .$$

پس

$$\begin{aligned} ۲\times ۳\times \cdots \times (p-۲) &= r_۱r_۱^*r_۲r_۲^* \cdots r_sr_s^* \\ &\equiv ۱\times ۱\times \cdots \times ۱ \ (\text{هنگ } p) \quad (\text{چون } r_ir_i^*\equiv ۱ \ (\text{هنگ } p)) \\ &\equiv ۱ \ (\text{هنگ } p) . \end{aligned}$$

بنا براین ،

$$\begin{aligned} ۱\times ۲\times ۳\times \cdots \times (p-۱) &\equiv (p-۱) \ (\text{هنگ } p) \\ &\equiv -۱ \ (\text{هنگ } p) \end{aligned}$$

که همان قضیهٔ ویلسن است. ■

مثال ۴ : اگر $p=۷$ ، $(p-۱)!=۷۲۰=۷\times ۱۰۲+۶\equiv -۱$ (هنگ ۷) . توجه کنید که زوجهای بحث شده در اثبات قضیهٔ ویلسن در حالت $p=۷$ ، (۲ ، ۴) و (۳ ، ۵) می باشند .

اینك به ذکر چند کاربرد کاملا شگفت‌انگیز از قضیهٔ ویلسن و قضیهٔ فرما می‌پردازیم.

قضیهٔ ۵ : هر گاه p عدد اول فردی باشد، آنگاه همنهشتی

$$x^۲\equiv -۱ \ (\text{هنگ } p)$$

دارای جواب است اگر و فقط اگـر $p\equiv ۱$ (هنگ ۴) . وقتی $p\equiv ۱$ (هنگ ۴) ، آنگاه $x=((p-۱)/۲)!$ یك جواب است.

بدین ترتیب، همهٔ اعداد اول p کـه به ازای آنها ۱ ــ به هنگ p جذر دارد کاملا مشخص می‌شونـد . بـرای مثال $x^۲\equiv -۱$ (هنگ ۷) جواب نـدارد ، در حالی کـه $x^۲\equiv -۱$ (هنگ ۵) جواب دارد. (دستگاه کامل مانده‌ها به‌هنگ ۷ و ۵ را بترتیب بررسی

کنید.)

برهان قضیهٔ ۵ : ابتدا فرض کنیم به ازای یک مقدار x ، (هنگ p)$x^۲ \equiv -۱$. دراین صورت

$$x^{p-۱} \equiv (x^۲)^{\frac{p-۱}{۲}} \equiv (-۱)^{\frac{p-۱}{۲}} (\text{هنگ } p) .$$

از طرف دیگر ، بنابرقضیهٔ فرما

$$x^{p-۱} \equiv ۱ (\text{هنگ } p) .$$

بنابراین ، (هنگ p)$(-۱)^{(p-۱)/۲} \equiv ۱$ ، پس $p | ۱-(-۱)^{(p-۱)/۲}$. اگر $۰ \neq ۱-(-۱)^{(p-۱)/۲}$ ، آنگاه $۲ = ۱-(-۱)^{(p-۱)/۲}$ که متناقض با فرض فردبودن p است. بنابراین، $۱ = (-۱)^{(p-۱)/۲}$ پس $(p-۱)/۲$ زوج است؛ یعنی (هنگ ۴)$p \equiv ۱$.
بالعکس، فرض کنیم (هنگ ۴)$p \equiv ۱$. آنگاه

$$(p-۱)! = ۱ \times ۲ \dots \frac{p-۱}{۲}(p-۱)(p-۲) \dots \left(p-\frac{p-۱}{۲}\right)$$

$$\equiv ۱ \times ۲ \dots \frac{p-۱}{۲}(-۱)(-۲) \dots \left(-\frac{p-۱}{۲}\right) (\text{هنگ } p)$$

$$= (-۱)^{(p-۱)/۲} \times ۱^۲ \times ۲^۲ \dots \left(\frac{p-۱}{۲}\right)^۲ \equiv \left(۱ \times ۲ \dots \frac{p-۱}{۲}\right)^۲ (\text{هنگ } p)$$

(چون (هنگ ۴)$p \equiv ۱$) .

ازطرف دیگر ، بنابرقضیهٔ ویلسن ،

$$(p-۱)! \equiv -۱ (\text{هنگ } p)$$

بنابراین اگرقرار دهیم $x = ۱ \times ۲ \dots [(p-۱)/۲]$ ، داریم

$$x^۲ \equiv -۱ (\text{هنگ } p) . \qquad ■$$

قضیهٔ‌قبل به‌حل یک‌همنهشتی‌درجهٔ دوم‌خاص‌مربوط می‌شود. ما درفصل بعد، همنهشتیهای درجهٔ دوم را به‌تفصیل مطالعه خواهیم کرد، و بنابراین، فعلا از پرداختن به‌قضیهٔ ۵ آن چنان‌که شایستهٔ آن است خودداری می‌کنیم . اما ، اجازه دهید چند نتیجهٔ مقدماتی ولی شگفت‌انگیز ازقضیهٔ ۵ استخراج کنیم.

نتیجهٔ ۶ : هرگاه x عددی صحیح و p عدد اول فردی باشد که $x^۲+۱$ را عاد کند، آنگاه (هنگ ۴)$p \equiv ۱$.

برهان: اگر $p \mid x^2+1$، آنگاه $x^2 \equiv -1 \ (\text{هنگ } p)$. بنابراین بنابر قضیهٔ ۵ نتیجه حاصل شده است. ■

مثال ۷: اگر $x=6$، آنگاه $x^2+1=37\equiv 1 \ (\text{هنگ } 4)$. اگر $x=8$، آنگاه $x^2+1=65=5\times 13$، که هم ۵ و هم ۱۳ همنهشت ۱ به‌هنگ ۴ هستند.

مثال ۸: ازقضیهٔ ۵ برای مطالعهٔ معادلهٔ سیالهٔ

$$y^2 = x^3 + 23 \qquad (1)$$

استفاده می‌کنیم. ما نشان خواهیم دادکه این معادله جواب ندارد. این معادله حالت خاص معادلهٔ باشه[1] $y^2=x^3+k$ است، که در ۱۶۲۱ میلادی‌توسط باشه[2] بحث شد. متعلم باید توجه داشته باشد کــه در مطالعهٔ معادلهٔ (۱) فقط ازقضیهٔ ۵ ومطالب مقدماتی مــربوط به همنهشتیها استفاده می‌شود. ولی این‌کار را نمی‌توان برای kی دلخواه انجام داد. دراثبات (۱) ازخصوصیات ویژهٔ عدد ۲۳ استفاده می‌شود.

اینك نشان خواهیم دادکه (۱) جوابی ندارد. ما این‌کار را با درنظرگرفتن تك‌تك چهار حالت ممکن به‌هنگ ۴ وکنارگذاردن هریك به انجام خواهیم رساند؛ یعنی x بایستی بــا یکی از اعداد ۰، ۱، ۲، ۳ همنهشت بــه هنگ ۴ باشد. ابتدا می‌بینیم کــه اگــر $x\equiv 0$ یا $2 \ (\text{هنگ } 4)$، آنگاه $x^3\equiv 0 \ (\text{هنگ } 4)$ وبنابراین

$$y^2 = x^3+23\equiv 23\equiv 3 \ (\text{هنگ } 4)\,.$$

ولی مربع یك عدد می‌تواند فقط همنهشت ۰ یا ۱ به هنگ ۴ باشد، بنابــراین x نمی‌تواند همنهشت ۰ یا ۲ به هنگ ۴ باشد. بعدفرض‌کنیم $x\equiv 3\equiv -1 \ (\text{هنگ } 4)$. دراین صورت

$$y^2 = x^3+23\equiv (-1)^3+23 = 22\equiv 2 \ (\text{هنگ } 4)$$

باز مربع یك عدد می‌تواند فقط همنهشت ۰ یا ۱ به‌هنگ ۴ باشد، وبنابراین x نمی‌تواند همنهشت ۳ به هنگ ۴ باشد.

اینك تنهاحالت‌ممکن $x\equiv 1 \ (\text{هنگ } 4)$ برای‌مطالعه باقی می‌ماند. این‌حالت‌دشوارتر

---

۱. دربارهٔ معادلهٔ باشه به حد باورنکردنی مطلب نوشته شده است. حالت خاص آن توسط تعداد زیادی از ریاضیدانان سده‌های هیجدهم و نوزدهم مورد بحث قرارگــرفته است. در اوایــل سدهٔ اخیر توسط ل. ج. موردل **L. J. Mordell** ثابت شدکه معادلهٔ سیالهٔ $y^2=x^3+k$ (k مفروض) فقط تعدادی متناهی جواب دارد. در ۱۹۶۶ آ. بیکــر **A. Baker** ازکمبریج اولین روش متناهی را جهت تعیین جوابها ارائه داد، هرچندکه تا زمان نوشتن این‌کتاب، این نظریه کاملا در مرحله‌ای نبودکه بتوان آن را به‌کامپیوتر داد. از نظر تاریخی معادلهٔ باشه معادلهٔ سیالهٔ‌مهمی است، و ما درسراسر این‌کتاب به‌حالتهای خاص‌آن برخواهیم‌گشت تابرتری قضایای مختلفی را که اثبات خواهیم‌کرد روشن‌کنیم.

2. Bachet

ومستلزم فکری استادانه است. ما (۱) را به‌صورت

$$y^{۲}+۴=x^{۳}+۳^{۳}=(x+۳)(x^{۲}-۳x+۹) \qquad (۲)$$

می‌نویسیم. دراین صورت $x\equiv ۱$ (هنگ ۴) ایجاب می‌کند که

$$x^{۲}-۳x+۹\equiv ۱-۳+۹=۷\equiv -۱ \text{ (هنگ ۴)} \qquad (۳)$$

پس‌عدد اولی مانند p وجود دارد به‌طوری که $p\equiv -۱$ (هنگ۴) و $p|x^{۲}-۳x+۹$. این مطلب درست است ، زیرا بسهولت دیده می‌شود که به ازای کلیهٔ اعداد صحیح x ، $x^{۲}-۳x+۹\geqslant ۲$ ، وبنابراین می‌توانیم آن را به‌صورت حاصلضرب اعداد اول بنویسیم

$$x^{۲}-۳x+۹=p_{۱}p_{۲}\cdots p_{t} \cdot$$

اگر هر $p_i\equiv ۱$ (هنگ ۴) $(۱\leqslant i\leqslant t)$ ، آنگاه

$$x^{۲}-۳x+۹=p_{۱}p_{۲}\cdots p_{t}\equiv ۱\times ۱ \cdots ۱\equiv ۱ \text{ (هنگ ۴)} ,$$

که متناقض بامعادلهٔ (۳) است. بنابراین مقداری از p_i ، مثل p داریم، که $x^{۲}-۳x+۹$ را عاد می‌کند و $p\equiv -۱$ (هنگ ۴) . در این صورت ، بالاخص ، معادلهٔ (۲) ایجاب می‌کند که

$$y^{۲}\equiv -۴=(-۱)۲^{۲} \text{ (هنگ } p) . \qquad (۴)$$

چون $p\equiv -۱$ (هنگ ۴) ، p عددی است اول و فرد، و بنابراین ۲ یك عکس حسابی ۲^* به‌هنگ p دارد. پس، (۴) ایجاب می‌کند که

$$(۲^{*}y)^{۲}\equiv -۱ \text{ (هنگ } p) .$$

بنابراین ، ۲^*y یك جواب همنهشتی $z^{۲}\equiv -۱$ (هنگ p) خواهد شد، که متناقض قضیهٔ۵ است زیرا که $p\equiv -۱$ (هنگ ۴) .

بدین ترتیب ثابت شد که معادلهٔ (۱) جواب ندارد.

۳.۳ تمرینات

۱. a^k به هنگ ۷ را به ازای $k=۰ ، ۱ ، ۲ ، ۳ ، ۴ ، ۵ ، ۶$ و

(آ) $a=۱$ ، (ب) $a=۲$ ، (ج) $a=۳$ ، (د) $a=۴$ ، (ه) $a=۵$ ، (و) $a=۶$،

بیابید. درهرحالت باید از دستگاه کامل مانده‌های ۰ ، ۱ ، ۲ ، ... ، ۶ استفاده کنید.

۲. تمرین ۱ را ادامه می‌دهیم.

(آ) a^k به هنگ ۷ را به‌ازای $a=۱ ، ۲ ، ۳ ، ۴ ، ۵ ، ۶$ برای هر k ی دلخواه محاسبه کنید .

(ب) آیا می‌توانید درمورد قوای a^k به‌هنگ ۷ حدسی بزنید؟

(ج) آیا می‌توانید درمورد کوچکترین مقدار $k>0$ به طوری که $a^k\equiv 1$ (هنگ ۷) حدسی بزنید؟

(د) حدسهایی راکه درقسمتهای (ب) و (ج) زده‌اید باحل کردن تمرینهای ۱ و ۲ برای قوای اعداد صحیح به‌هنگ ۱۱ و ۱۳ بیازمایید.

۳. نشان دهیدکه اگر p عددی اول باشد، آنگاه $a^p\equiv a$ (هنگ p).

۴. اثبات قضیهٔ ویلسن را به‌طور عددی درحالت ۱۱ ، ۷ ، ۵ $=p$ انجام دهید.

۵. (آ) آیاهمنهشتی $x^2\equiv -1$ (هنگ ۱۷) جواب دارد؟ اگرجواب دارد، آن‌رابیابید.

(ب) قسمت (آ) را برای همنهشتی $x^2\equiv -1$ (هنگ ۴۳) تکرار کنید.

۶. آیا همنهشتی $x^2\equiv -1$ (هنگ ۹۱) جواب دارد؟

۷. آیا $x^2\equiv -1$ (هنگ ۶۵) جواب دارد؟

۸. ثابت کنیدکه اگر $a^{m-1}\equiv 1$ (هنگ m) و $a^r\not\equiv 1$ (هنگ m)، به‌ازای هر $r|m-1$ و $r<m-1$، آنگاه m عددی اول است.

۹. عکس قضیهٔ ویلسن را ثابت کنید: نشان دهیدکه اگر m عددی صحیح باشد به‌طوری که $(m-1)!\equiv -1$ (هنگ m) آنگاه m عددی‌اول است. درحقیقت نشان‌دهیدکه‌اگر m اول و ۴ نباشد، آنگاه $(m-1)!\equiv 0$ (هنگ m).

۱۰. نشان دهیدکه معادلهٔ سیالهٔ $x^2+1=23y$ جواب ندارد.

۱۱. فرض کنیم a عدد صحیح فردی باشد. نشان دهیدکه اگر $k\geqslant 3$، آنگاه

$$a^{2^{k-2}}\equiv 1\ (\text{هنگ } 2^k).$$

(راهنمایی: از استقرا روی k استفاده کنید. در بخش ۲.۳ آن را به ازای $k=3$، بررسی کردیم.)

۱۲. نشان دهیدکه $y^2=x^3-73$ درمجموعهٔ اعداد صحیح جوابی ندارد.

۱۳. فرض کنیم m عدد صحیحی باشد به‌طوری‌که عامل اولی همنهشت ۳ به هنگ ۴ نداشته باشد و n عدد صحیح دلخواهی باشد. نشان دهیدکه معادلهٔ سیالهٔ

$$y^2+4m^2=x^3+(4n-1)^3$$

جواب ندارد.

۱۴. یك برنامهٔ کارآمدکامپیوتری برای محاسبهٔ a^*، عکس حسابی a به هنگ n، بنویسید. (برنامهٔ شما بایستی متضمن‌آزمایشی باشدکه تعیین کندآیا a چنین عکسی دارد یانه.)

۱۵. فرض کنیم p عدد اولی بزرگتر از ۲ باشد و $0<a<p-1$. نشان دهید که

$$\binom{p-1}{a}\equiv(-1)^a (\text{هنگ } p) .$$

۱۶*. نشان دادیم که به ازای $p\equiv 1$ (هنگ ۴)، داریم

$$\left(\frac{p-1}{2}\right)!^2\equiv -1 (\text{هنگ } p) .$$

نشان دهید که به ازای $p\equiv 1$ (هنگ ۴)، داریم

$$\left(\frac{p-1}{2}\right)!^2\not\equiv -1 (\text{هنگ } p^2) .$$

۱۷. فرض کنیم p عددی اول باشد به طوری که $n<p<2n$. در این صورت ثابت کنید

(آ) $\binom{2n}{n}\equiv 0 (\text{هنگ } p)$.

(ب) $\binom{2n}{n}\not\equiv 0 (\text{هنگ } p^2)$.

۱۸. فرض کنیم p عددی اول و a و b اعداد صحیحی باشند به طوری که $p\nmid ab$. نشان دهید که $(a+b)^p\equiv a^p+b^p (\text{هنگ } p)$.

۱۹**. (قضیهٔ هوستن هولم[1]) فرض کنیم p عدد اولی بزرگتر از ۳ باشد. نشان‌دهید که صورت کسر $1+1/2+1/3+\dots+1/(p-1)$ بر p^2 بخشپذیر است. (راهنمایی: توجه کنید که $(p-1)!$ جملهٔ ثابت بسجملهٔ $(x-1)\dots(x-(p-1))$ است. x را مساوی p قراردهید و بخشپذیری ضرایب بر p را مطالعه کنید و ضریب x را درنظر بگیرید.)

۲۰. بنابر قضیهٔ ویلسن عددی مانند k وجود دارد که، $kp=1+(p-1)!$.

(آ) چه وقت می‌تواند $k=1$ ؟

(ب) چه وقت می‌تواند $k=p$ ؟

۲۱. فرض کنیم p عدد اول فردی باشد.

(آ) نشان‌دهید که $2^2\times 4^2\times 6^2\dots(p-1)^2\equiv(-1)^{(p+1)/2} (\text{هنگ } p)$

(ب) نشان‌دهید که $1^2\times 3^2\dots(p-2)^2\equiv 2^2\times 4^2\dots(p-1)^2 (\text{هنگ } p)$

---

1. Wohlstenholme

۴.۳ حل همنهشتیهای بسجمله‌ای، ۱

فرض کنیم $f(x)$ بسجملهٔ ناصفری باضرایب صحیح، و n عددی صحیح ومثبت باشد. دراین بخش، مسئلهٔ تعیین جوابهای همنهشتی

$$f(x) \equiv 0 \ (\text{هنگ } n) \qquad (1)$$

را دنبال خواهیم کرد. قبلا تعدادی ازحالات خاص این مسئله را بررسی کرده‌ایم. به‌عنوان مثال، همنهشتی خطی $ax \equiv b \ (\text{هنگ } n)$ را که متناظر با $f(x) = ax - b$ است، بررسی کردیم. بعلاوه،همنهشتی $x^2 \equiv -1 \ (\text{هنگ } n)$ را،که متناظربا بسجملهٔ $f(x) = x^2 + 1$ است،مورد توجه قراردادیم. ازمطالعهٔ این دوحالت خاص، می‌بینیم که پیدا کردن جوابهای همنهشتیهای بسجمله‌ای می‌تواند کار دشواری باشد. زیرا ریاضیدانان به هیچ وجه داستان کامل حل همنهشتیهای بسجمله‌ای را در اختیار ندارند، آنچه که ما دراین موضوع باید بگوییم تنها اشاره‌ای جزئی به‌آن‌خواهدبود.

قبلا دیده‌ایم که اگر x یك جواب همنهشتی (۱) باشد، آنگاه هر y ی به صورت $x \equiv y \ (\text{هنگ } n)$ نیز یك جواب است. بنابراین، برای ردیابی جوابهای (۱)، دو جواب x و y را زمانی «متمایز» می‌شماریم که $x \not\equiv y \ (\text{هنگ } n)$. پس، (۱) می‌تواند حداکثر n جواب‌متمایزداشته‌باشد، زیراکه‌دقیقاً امکان وجود n عدد صحیح ناهمنهشت به‌هنگ n هست. برای یافتن جوابهای (۱) کافی است که n عدد صحیح ازیك دستگاه کامل وثابت مانده‌ها (مثلا $0, 1, 2, \ldots, n-1$) را بیازماییم. فرض کنیم اعضای دستگاه کامل مانده‌ها که جوابهای (۱) هستند، عبارت باشند از $a_1, \ldots, a_s$. در این صورت x فقط وفقط وقتی جواب (۱) است که

$$x \equiv a_1 \ (\text{هنگ } n) \text{، یا } x \equiv a_2 \ (\text{هنگ } n) \text{، ... ، یا } x \equiv a_s \ (\text{هنگ } n).$$

دوباره تأکید می‌کنیم که $0, 1, \ldots, n-1$ اغلب مناسبترین دستگاه کامل مانده‌ها برای محاسبات نیست. اگر n فرد باشد، آنگاه دستگاه کامل مانده‌های

$$-\frac{n-1}{2}, -\frac{n-1}{2}+1, \ldots, -1, 0, 1, 2, \ldots, \frac{n-1}{2}$$

اعدادی هستند که از لحاظ قدر مطلق از دستگاه اول کوچکترند و بنابراین محاسبه با آنها ساده‌تر است. برای مثال، اگر می‌خواستیم همنهشتی

$$x^5 \equiv 2 \ (\text{هنگ } 24)$$

را حل کنیم ویا اگر می‌خواستیم تعیین کنیم که آیا $x \equiv 23 \ (\text{هنگ } 24)$ یك جواب معادلهٔ فوق هست یا نه، غیرعاقلانه خواهد بود اگر ازعدد ۲۳ استفاده کنیم، زیرا درآن صورت بایستی ۲۳ را به قوهٔ پنجم برسانیم وببینیم که آیا ۲۴ عدد $23^5 - 2$ را عاد می‌کند یا نه. چون $23 \equiv -1 \ (\text{هنگ } 24)$، محاسبه کردن $(-1)^5 = -1$ خیلی ساده‌تر است که از آنجا بلافاصله دیده می‌شود که $23^5 \not\equiv 2 \ (\text{هنگ } 24)$.

اکنون حل همنهشتی (۱) را دنبال می‌کنیم. فرض کنیم

$$n = p_1^{a_1} \cdots p_t^{a_t}$$

که در آن p_1 ، ... ، p_t اعداد اول متمایز هستند . در این صورت اگر x یك جواب $f(x) \equiv 0 \pmod{n}$ باشد x یك جواب کلیهٔ همنهشتیهای

$$(۲)\qquad \begin{aligned} f(x) &\equiv 0 \pmod{p_1^{a_1}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{a_r}} \end{aligned}$$

نیزخواهد بود . بالعکس ، فرض کنیم x یك جواب همزمان کلیهٔ همنهشتیهای (۲) باشد، در این‌صورت $f(x)$ بر $p_1^{a_1}$ ، بر $p_2^{a_2}$ ، ... ، بر $p_t^{a_t}$ بخشپذیر می‌باشد. چون کلیهٔ $p_i^{a_i}$ ها هیچ عامل مشترکی ندارند، $f(x)$ بر $n = p_1^{a_1} \cdots p_t^{a_t}$ بخشپذیر است، وبنابراین x یك‌جواب همنهشتی $f(x) \equiv 0 \pmod{n}$ است. بدین‌ترتیب، دیده‌ایم که جوابهای‌همنهشتی (۱)همان جوابهای همزمان کلیهٔ همنهشتیهای (۲) هستند.

بنابراین، برای دستیابی به‌حل کامل همنهشتی $f(x) \equiv 0 \pmod{n}$ ، می‌توانیم در دو مرحله اقدام کنیم:

۱. هریك از همنهشتیهای

$$f(x) \equiv 0 \pmod{p_i^{a_i}} \qquad (i = 1, \ldots, t)$$

را جداگانه حل کنیم.

۲. تعیین‌کنیم که کدام جوابها جوابهای مشترك کلیهٔ همنهشتیهای (۲) هستند.

برای اینکه به محتوای مرحلهٔ دوم بهتر پی‌ببریم، فرض‌می کنیم قسمت ۱ کاملا انجام شده باشد وجوابهای همنهشتیهای

$$(۳)\qquad f(x) \equiv 0 \pmod{p_i^{a_i}} \qquad (i = 1, \ldots, t)$$

(به نحوی) تعیین شده وعبارت باشند از

$$(۴)\qquad x \equiv b_{i1} \pmod{p_i^{a_i}},\ x \equiv b_{i2} \pmod{p_i^{a_i}},\ \ldots$$

برای اینکه عدد مفروض x یك جواب همنهشتی $f(x) \equiv 0 \pmod{n}$ باشد ، دیده‌ایم که لازم و کافی است که x در هریك ازهمنهشتیهای (۳) صدق کند. بنابراین، چون جوابهای (۳) به توسط (۴) داده شده‌اند، x یك‌جواب $f(x) \equiv 0 \pmod{n}$ است اگر، وفقط اگر، x همنهشت یکی از اعداد b_{11} ، b_{12} ، ... $\pmod{p_1^{a_1}}$ ، همنهشت یکی از اعداد b_{21} ، b_{22} ، ... $\pmod{p_2^{a_2}}$ وغیره باشد. پس، ما به‌نتیجهٔ زیرمی‌رسیم :

قضیهٔ ۱ : عدد صحیح x یك جواب همنهشتی $f(x) \equiv 0 \pmod{n}$ است اگر، وفقط اگر، x در دستگاهی از همنهشتیهای

$$x \equiv b_1 (p_1^{a_1} \text{ هنگ})$$
$$\vdots$$
$$x \equiv b_t (p_t^{a_t} \text{ هنگ})$$

صدق کند، که در آن b_i یك جواب همنهشتی

$$f(x) \equiv 0 (p_i^{a_i} \text{ هنگ}) \quad (i = 1, \ldots, t)$$

می باشد.

ازقضیهٔ ۱، درمی یابیم که، به‌شرط آنکه‌قسمت اول حل‌شده باشد، قسمت دوم‌می‌تواند حل شود مشروط براینکه بتوانیم دستگاه همنهشتیهای به‌صورت

$$x \equiv b_1 (p_1^{a_1} \text{ هنگ})$$
$$\vdots$$
$$x \equiv b_t (p_t^{a_t} \text{ هنگ})$$

را حل کنیم. یعنی xی بیابیم که به طور همزمان در کلیهٔ این همنهشتیها صدق کند. اینك به‌مسئلهٔ فوق خواهیم پرداخت و آن را کاملا حل خواهیم کرد. یعنی قضیهٔ زیر را ثابت خواهیم کرد:

قضیهٔ ۲ : (قضیهٔ باقیماندهٔ چینی): فرض‌کنیم اعدادصحیح مثبت m_1، m_2، ...، m_t دو به‌دو نسبت به هم اول باشند؛ یعنی، $1 = (m_i, m_j)$ بمعم اگر $i \neq j$ و $1 \leqslant i, j \leqslant t$. بعلاوه، فرض‌کنیم b_1، b_2، ...، b_t اعدادصحیح‌دلخواهی‌باشند. دراین‌صورت‌همنهشتیهای

$$x \equiv b_1 (m_1 \text{ هنگ})$$
$$\vdots$$
$$x \equiv b_t (m_t \text{ هنگ})$$

یك جواب همزمان دارند. بعلاوه، این جواب همزمان به‌هنگ $m_1 \ldots m_t$ منحصر بفرد است. یعنی، اگر y جواب دیگری باشد، آنگاه $x \equiv y (m_1 \ldots m_t \text{ هنگ})$.

قبل ازاینکه قضیهٔ ۲ را ثابت‌کنیم به‌ذکر چندتبصره می‌پردازیم.

تبصرهٔ ۱: چون در بحث قبلی، اعداد صحیح $p_1^{a_1}$، ...، $p_t^{a_t}$ دو بــه‌دو نسبت به‌هم اول

هستند (اعداد اول p_1 ، ... ، p_t همه متمایزند)، دستگاه همنهشتیهای قضیهٔ ۱ همواره جواب دارد، و این جواب به هنگ $n = p_1^{a_1} \cdots p_t^{a_t}$ منحصر بفرد است. ما از این تبصره بعداً در این بخش، برای مسئلهٔ اصلی خود دربارهٔ حل همنهشتیهای بسجمله‌ای استفاده خواهیم کرد.

تبصرهٔ ۲ : اثبات ما برای قضیهٔ ۲ سازنده خواهد بود، بدین معنی که یك روش محاسباتی برای ما فراهم خواهد کرد که به وسیلهٔ آن جوابهای دستگاه همنهشتیها را می‌توان در تعدادی متناهی مرحله محاسبه نمود.

تبصرهٔ ۳ : دلیل اینکه قضیهٔ ۲ قضیهٔ باقیماندهٔ چینی نامیده شده است این است که صورتهای بدوی آن به چینیان باستان برمی‌گردد.

برهان قضیهٔ ۲ : روش اثبات این است که x را به‌صورت

$$x = y_1 b_1 + \cdots + y_t b_t$$

بنویسیم، که در آن $y_1 \equiv 1$ (هنگ m_1) و $y_1 \equiv 0$ (هنگ m_i) $(2 \leqslant i \leqslant t)$، $y_2 \equiv 1$ (هنگ m_2) و $y_2 \equiv 0$ (هنگ m_i) $(i = 1, 3, 4, \ldots, t)$، و به همین طریق برای y_3 ، ... ، y_t . برای اینکه داشته باشیم $y_1 \equiv 0$ (هنگ m_i) $(2 \leqslant i \leqslant t)$ بایستی داشته باشیم $m_2 \cdots m_t | y_1$ زیرا m_i ها دوبدو نسبت به‌هم اول هستند. بنابراین، در حالت کلی، می‌گیریم

$$m'_i = \frac{m_1 m_2 \cdots m_t}{m_i} .$$

در این صورت $1 = (m_i , m'_i)$ بمعم زیرا m_1 ، ... ، m_t دو بدو نسبت به هم اول هستند (تمرین). بنابراین، m'_i دارای یك عکس‌حسابی m'^*_i به هنگ m_i است:

$$m'^*_i m'_i \equiv 1 \ (\text{هنگ } m_i)$$

قرار می‌دهیم $y_i = m'^*_i m'_i$ ، ومعادلهٔ متناظر آن خواهد شد

$$x = m'^*_1 m'_1 b_1 + \cdots + m'^*_t m'_t b_t .$$

حال نشان می‌دهیم که $x \equiv b_1$ (هنگ m_1) . در واقع، به ازای $2 \leqslant i \leqslant t$، داریم

$$m_1 | m'_i ,$$

بنابراین، به‌ازای $2 \leqslant i \leqslant t$، $m'^*_i m'_i b_i \equiv 0$ (هنگ m_1)؛ همچنین $m'^*_1 m'_1 \equiv 1$ (هنگ m_1)، پس $m'^*_1 m'_1 b_1 \equiv b_1$ (هنگ m_1). بنابراین،

$$x \equiv b_1 + 0 + \cdots + 0 \equiv b_1 \ (\text{هنگ } m_1)$$

به همین طریق نتیجه می‌شود که به ازای کلیهٔ i ها، $1 \leqslant i \leqslant t$، $x \equiv b_i$ (هنگ m_i) .

برای یکتایی جواب، فرض کنیم x' جواب همزمان دیگری باشد. در این‌صورت، به ازای $i = ۱ ، ۲ ، \ldots ، t$ ، $x \equiv x'$ (هنگ m_i) . بنابراین، چون $m_۱$ ، $m_۲$ ، ... ، m_t دوبدو نسبت به‌هم اول هستند وچون $x - x'$ بر $m_۱$ ، $m_۲$ ، ... ، m_t بخشپذیر است، داریم $m_۱ m_۲ \cdots m_t | x - x'$. پس،

$$x \equiv x' (\text{هنگ } m_۱ m_۲ \cdots m_t) \qquad \blacksquare$$

روش فوق برای اثبات، کاملا سازنده است، بدین معنی که روش خاصی برای‌محاسبهٔ جواب x به ما می‌دهد. اجازه دهید ابتدا مثال ساده‌ای بیاوریم. x هایی را بیابید که در همنهشتیهای

$$x \equiv ۱ (\text{هنگ } ۳)$$
$$x \equiv ۴ (\text{هنگ } ۵)$$

صدق می‌کنند. در اینجا $m_۱ = ۳$ ، $m_۲ = ۵$ ، $b_۱ = ۱$ ، $b_۲ = ۴$. بنابراین، $m'_۱ = (۵ \times ۳)/۳ = ۵$ و $m'_۲ = ۳$. در این‌صورت چون $m'^*_۱$ یک عکس حسابی $m'_۱$ (هنگ $m_۱$) است، $m'^*_۱$ بایستی در

$$۵ m'^*_۱ \equiv ۱ (\text{هنگ } ۳)$$

صدق کند، بنابراین $m'^*_۱ \equiv ۲ (\text{هنگ } ۳)$. همچنین $۳ m'^*_۲ \equiv ۱ (\text{هنگ } ۵)$ نتیجه می‌دهد که $m'^*_۲ \equiv ۲ (\text{هنگ } ۵)$. پس،

$$x = ۲ \times ۵ \times ۱ + ۲ \times ۳ \times ۴ = ۳۴ \equiv ۴ (\text{هنگ } ۱۵).$$

به عنوان مثالی مشکلتر جوابهای همزمان‌همنهشتیهای

$$x \equiv ۷ (\text{هنگ } ۸)$$
$$x \equiv ۲ (\text{هنگ } ۹)$$
$$x \equiv -۱ (\text{هنگ } ۵)$$

را می‌یابیم. در اینجا

$$b_۱ = ۷ ، b_۲ = ۲ ، b_۳ = -۱$$

و

$$m_۱ = ۸ ، m_۲ = ۹ ، m_۳ = ۵$$

و از این‌رو

$$m'_۱ = ۹ \times ۵ = ۴۵ ، m'_۲ = ۸ \times ۵ = ۴۰ ، m'_۳ = ۸ \times ۹ = ۷۲ .$$

$$۴۵m'_۱ \equiv ۱(\text{هنگ } ۸)\ ,\ ۴۰m'_۲ \equiv ۱(\text{هنگ } ۹)\ ,\ ۷۲m'_۳ \equiv ۱(\text{هنگ } ۵)\ .$$

بنابراین

$$m'_۱ \equiv ۵(\text{هنگ } ۸)\ ,\ m'_۲ \equiv -۲(\text{هنگ } ۹)\ ,\ m'_۳ \equiv ۳(\text{هنگ } ۵)\ .$$

بنابراین قرارمی‌دهیم

$$x = ۵ \times ۴۵ \times ۷ + (-۲) \times ۴۰ \times ۲ + ۳ \times ۷۲(-۱) = ۱۱۹۹$$

$$\equiv ۱۱۹(\text{هنگ } ۳۶۰)$$

(ن $\times ۹ \times ۸ = ۳۶۰$). بسهولت‌می‌توان‌تحقیق‌کرد که $x = ۱۱۹$ درهمنهشتیهای اولیه‌صدق می‌کند.

از ترکیب قضایای ۱ و ۲ ، ملاحظه می‌کنیم که مسئلهٔ حل همنهشتیهای بسجمله‌ای کاملا به مسئلهٔ حل همنهشتیهای بسجمله‌ای به صورت

$$f(x) \equiv ۰(\text{هنگ } p^a)\ ,$$

که درآن p عددی اول‌است، تبدیل می‌شود. این‌مطلب ممکن‌است چیزساده‌ای به نظربرسد، ولی لااقل به دو دلیل حائزاهمیت است. اگر n برتعداد زیادی ازاعداد اول‌که به توانهای کوچکی رسیده‌اند بخشپذیر باشد، آنگاه همنهشتی‌ای راکه هنگ آن توانهای اعداد اول است می‌توان با آزمون کلیهٔ حالات ممکن حل نمود. این راه متضمن‌کاری خیلی‌کمتر از آزمون همهٔ حالات به هنگ n می‌باشد. به‌عنوان مثال، اگر $n = ۴۸ = ۳ \times ۲^۴$ ، آنگاه تعداد اعضای دستگاه کامل مانده‌ها به هنگ n ، ۴۸ است ، و حال آنکه این تعداد به‌هنگهای ۳ و $۲^۴$ جمعاً $۱۹ = ۱۶ + ۳$ می‌باشد. اما حتی یك دلیل اجباری‌تر برای تبدیل مسئلهٔ حل همنهشتیهای بسجمله‌ای به حالت همنهشتیهایی به‌هنگ قوه‌ای از یك عدد اول،آن است‌که بسیاری ازنتایج نظری‌که نمی‌توانند در حالت‌کلی ثابت شوند می‌توانند بوسیلهٔ همنهشتیها به‌هنگ قوای اول اثبات شوند.

اما، قبل ازاینکه جلوتر برویم، اجازه دهید مطالبی راکه تاکنون عنوان‌کرده‌ایم‌توسط مثال عددی $x^۲ \equiv ۱(\text{هنگ } ۵۶)$ روشن کنیم . چون این همنهشتی معادل با همنهشتی $x^۲ - ۱ \equiv ۰(\text{هنگ } ۵۶)$ است، می‌توانیم‌قرار دهیم $f(x) = x^۲ - ۱$. علاوه براین، چون $۵۶ = ۲^۳ \times ۷$ ، همنهشتی اولیه با دو همنهشتی

$$x^۲ - ۱ \equiv ۰(\text{هنگ } ۲^۳)$$

$$x^۲ - ۱ \equiv ۰(\text{هنگ } ۷)$$

معادل است. همنهشتی اول جوابهای $x \equiv ۱ , ۳ , ۵ , ۷(\text{هنگ } ۲^۳)$ را دارد. (فعلا ، ما جوابها را فقط بوسیلهٔ آزمودن‌کلیهٔ اعضای‌یك دستگاه‌کامل مانده‌ها، که دراین حالت‌به‌هنگ ۸ است، به‌دست‌می‌آوریم.) به همین طریق ، همنهشتی دوم جوابهای $x \equiv ۱ , ۶(\text{هنگ } ۷)$ را دارد. بنابراین،همنهشتی $x^۲ \equiv ۱(\text{هنگ } ۵۶)$ هشت‌جواب به‌هنگ‌۵۶ دارد، که‌جوابهای

هشت زوج همنهشتی زیر هستند:

$$\begin{cases} x\equiv ۳\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۶\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۳\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۱\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۱\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۶\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۱\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۱\ (\text{هنگ}\ ۷) \end{cases}$$

$$\begin{cases} x\equiv ۷\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۶\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۷\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۱\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۵\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۶\ (\text{هنگ}\ ۷) \end{cases},\quad \begin{cases} x\equiv ۵\ (\text{هنگ}\ ۲^{۳}) \\ x\equiv ۱\ (\text{هنگ}\ ۷) \end{cases}.$$

جوابهای این‌زوجهای‌همنهشتی، جوابهای‌همنهشتی اولیه را می‌دهند. وجوابهای این‌زوجهای همنهشتی را می‌توان با به‌کاربردن قضیهٔ باقیماندهٔ چینی پیداکرد. این جوابها عبارتند از.

$$x\equiv ۲۷\ (\text{هنگ}\ ۵۶),\quad x\equiv ۴۳\ (\text{هنگ}\ ۵۶),\quad x\equiv ۴۱\ (\text{هنگ}\ ۵۶),\quad x\equiv ۱\ (\text{هنگ}\ ۵۶)$$

$$x\equiv ۵۵\ (\text{هنگ}\ ۵۶),\quad x\equiv ۱۵\ (\text{هنگ}\ ۵۶),\quad x\equiv ۱۳\ (\text{هنگ}\ ۵۶),\quad x\equiv ۲۹\ (\text{هنگ}\ ۵۶).$$

اینك چند تذکر درمورد همنهشتیهایی به‌صورت

$$f(x)\equiv ۰\ (\text{هنگ}\ p^{a}),$$

که در آن p عددی اول است، می‌دهیم . اولین هدف ما این خواهد بودکه نشان دهیم کـه برای حل یك چنین همنهشتی، عملا کافی است که همنهشتی ساده‌تر

$$f(x)\equiv ۰\ (\text{هنگ}\ p)$$

را حل کنیم . در واقع ، کاری کـه می‌خواهیم بکنیم تجویز روشی است بـرای محاسبهٔ جوابهای‌همنهشتی

$$f(x)\equiv ۰\ (\text{هنگ}\ p^{a+۱})$$

از روی جوابهای همنهشتی

$$f(x)\equiv ۰\ (\text{هنگ}\ p^{a})$$

بنابراین، اگر از جوابهای همنهشتی به هنگ p شروع کنیم، روش ما اجازه خواهد دادکه متوالیاً جوابهای همان همنهشتی به‌هنگهای $p^{۲}$ ، $p^{۳}$ ، وغیره را محاسبه کنیم.

فرض می‌کنیم $a\geqslant ۱$ و جوابهای همنهشتی

$$f(x)\equiv ۰\ (\text{هنگ}\ p^{a})$$

به توسط

$$x\equiv b_{۱}\ (\text{هنگ}\ p^{a}),\ \ldots,\ x\equiv b_{r}\ (\text{هنگ}\ p^{a})$$

داده شده باشند. منظور ما تعیین جوابهای

$$f(x)\equiv ۰\ (\text{هنگ}\ p^{a+۱})$$

است.

اما ، ابتدا به یك نتیجهٔ مقدماتی در مورد بسجمله‌ها احتیاج داریم. اگر

$$f(x)=a_0+a_1x+\cdots+a_mx^m$$

آنگاه مشتق صوری آن‌که به f' نمایش داده می‌شود توسط دستور معمولی

$$f'(x)=a_1+2a_2x+\cdots+ma_mx^{m-1}$$

داده می‌شود . قواعد معمولی مشتقگیری را برای‌مشتق صوری به‌کار می‌بریم ، یعنی به ازای بسجمله‌های f و g داریم

$$(f+g)'=f'+g' \qquad (5)$$

$$(af)'=af' \qquad \text{به‌ازای عددصحیح } a \qquad (6)$$

مشتق دوم f (یعنی، مشتق f') را به f'' نمایش خواهیم داد. به طورکلی، iمین مشتق f را به $f^{(i)}$ نمایش خواهیم داد. درآنچه‌که در زیرخواهد آمد، ما به‌حالت خاصی که درحساب دیفرانسیل وانتگرال دستور تیلر[1] نامیده می‌شود احتیاج خواهیم داشت.

لم ۳ : فرض‌کنیم $f(x)$ یك بسجملهٔ دلخواه از درجهٔ m باشد. دراین صورت

$$f(x+y)=f(x)+\frac{f'(x)}{1}y+\frac{f''(x)}{1\times 2}y^2+\cdots+\frac{f^{(m)}(x)}{1\times 2\cdots m}y^m.$$

بعلاوه، اگر f دارای ضرایب صحیح باشد ، کلیهٔ بسجمله‌های

$$\frac{f'(x)}{1},\ \frac{f''(x)}{1\times 2},\ \ldots,\ \frac{f^{(m)}(x)}{1\times 2\cdots m}$$

نیز ضرایب صحیح خواهند داشت.

برهان: بنابر خواص (۵) و (۶) مشتق، کافی است لم را برای بسجملهٔ $f(x)=x^m$ ثابت کنیم. دراین حالت، $f(x+y)=(x+y)^m$ به توسط قضیهٔ دو جمله‌ای داده می‌شود:

$$f(x+y)=x^m+\frac{m}{1}x^{m-1}y+\frac{m(m-1)}{1\times 2}x^{m-2}y^2+\cdots+y^m$$

که در آن کلیهٔ ضرایب (که ضرایب دو جمله‌ای نامیده می‌شوند) اعداد صحیح‌انـد . در این صورت

$$\frac{f'(x)}{1}=\frac{m}{1}x^{m-1},\quad \frac{f''(x)}{1\times 2}=\frac{m(m-1)}{1\times 2}x^{m-2},$$

---

1. Taylor

و الی‌آخر. بنابراین،

$$f(x+y)=f(x)+\frac{f'(x)}{1}y+\frac{f''(x)}{1\times 2}y^2+\cdots+y^m,$$

و لم ثابت شده است. ■

اینك به همنهشتی $f(x)\equiv 0\,(p^{a+1}$ هنگ$)$ برمی گردیم. اگر x یك جواب آن باشد، آنگاه x یك جواب $f(x)\equiv 0\,(p^a$ هنگ$)$ نیز خواهد بود، و بنابراین $x\equiv b\,(p^a$ هنگ$)$، که b یکی از مقادیر b_1، b_2، ...، b_r است. بنابراین به ازای عددی چون k می‌توانیم بنویسیم $x=b+kp^a$. حال شرطی را تعیین می کنیم که بایستی k درآن صدق کند تا x یك جواب $f(x)\equiv 0\,(p^{a+1}$ هنگ$)$ باشد. بنابر لم ۳، با فرض $x=b$، $y=kp^a$، خواهیم داشت:

$$f(x)=f(b+kp^a)$$
$$=f(b)+\frac{f'(b)}{1}kp^a+\frac{f''(b)}{1\times 2}(kp^a)^2+\cdots+\frac{f^{(m)}(b)}{1\times 2\cdots m}(kp^a)^m.$$

بنابر لم ۳، بسجمله‌های

$$\frac{f'(x)}{1},\ \frac{f''(x)}{1\times 2},\ \ldots,\ \frac{f^{(m)}(x)}{1\times 2\cdots m}$$

دارای ضرایب صحیح هستند، بنابراین

$$\frac{f'(b)}{1},\ \frac{f''(b)}{1\times 2},\ \ldots,\ \frac{f^{(m)}(b)}{1\times 2\cdots m}$$

همه اعداد صحیح هستند. بعلاوه، چون $a\geqslant 1$، داریم $2a\geqslant a+1$، بنابراین p^{2a}، p^{3a}، ...، p^{ma} همه همنهشت صفر به هنگ p^{a+1} می‌باشند. پس،

$$f(x)\equiv f(b)+\frac{f'(b)}{1}kp^a\,(p^{a+1}\ \text{هنگ}).$$

چون $f(b)\equiv 0\,(p^a$ هنگ$)$، می‌توانیم به ازای عددی چون t، قرار دهیم $f(b)=tp^a$. بنابراین،

$$f(x)\equiv p^a(t+f'(b)k)\,(p^{a+1}\ \text{هنگ}).$$

پس، به ازای $x=b+kp^a$ فقط و فقط وقتی $f(x)\equiv 0\,(p^{a+1}$ هنگ$)$ که

$$p^a(t+f'(b)k)\equiv 0\,(p^{a+1}\ \text{هنگ}),$$

که معادل است با

$$t+f'(b)k\equiv 0 \ (\text{هنگ } p) \qquad (\text{قضیهٔ } 11.2) \ .$$

بنابـراین شرطی را کـه بایستی k در آن صدق کند تا $x=b+kp^a$ یك جواب $f(x)\equiv 0 \ (\text{هنگ } p^{a+1})$ باشد استخراج کرده‌ایم، یعنی

$$\boxed{f'(b)k\equiv -\frac{f(b)}{p^a} \ (\text{هنگ } p) \ .} \qquad (7)$$

(یادآوری می‌کنیم که بنا برفرض $f(b)\equiv 0 \ (\text{هنگ } p^a)$، و بنابراین $f(b)/p^a$ عددی صحیح است.) از این‌رو برای تعیین جوابهای $f(x)\equiv 0 \ (\text{هنگ } p^{a+1})$ در صورتی که جوابهای $f(x)\equiv 0 \ (\text{هنگ } p^a)$ را بدانیم، کافی است که همنهشتی خطی (۷) را به‌ازای k، به‌هنگ عدد اول p حل کنیم. مادربارهٔ این موضوع به طور همه جانبه در بخش ۲ بحث کردیم. با وجود این، در وضع فعلی ما صریحاً جواب را پیدا می‌کنیم. دوحالت وجود دارد که درنظر می‌گیریم.

حالت ۱ : $f'(b)\equiv 0 \ (\text{هنگ } p)$. دراین حالت همنهشتی (۷) فقط موقعی می‌تواند برقرار باشد که

$$\frac{f(b)}{p^a}\equiv 0 \ (\text{هنگ } p) \ ,$$

که معادل است با

$$f(b)\equiv 0 \ (\text{هنگ } p^{a+1})$$

بنابراین، دوامکان وجود دارد. یا $f(b)\equiv 0 \ (\text{هنگ } p^{a+1})$، که دراین حالت به ازای هر مقـدار k، $x=b+kp^a$ یك جـواب همنهشتی $f(x)\equiv 0 \ (\text{هنگ } p^{a+1})$ است. یـا $f(b)\not\equiv 0 \ (\text{هنگ } p^{a+1})$، که در این حالت به ازای هیچ k ای، $x=b+kp^a$ جوابی برای همنهشتی $f(x)\equiv 0 \ (\text{هنگ } p^{a+1})$ نیست.

حالت ۲ : $f'(b)\not\equiv 0 \ (\text{هنگ } p)$. دراین‌حالت همنهشتی (۷) دقیقاً یك‌جواب خواهدداشت. یعنی،

$$k\equiv -f'(b)^*\frac{f(b)}{p^a} \ (\text{هنگ } p) \ ,$$

که‌درآن $f'(b)^*$ یك عکس حسابی $f'(b)$ (هنگ p) است. بنابراین، درحالت۲، تنهاجواب منحصر بفرد همنهشتی $f(x)\equiv 0 \ (\text{هنگ } p^{a+1})$ بـه‌صورت $x\equiv b+kp^a \ (\text{هنگ } p^{a+1}$

خواهد بود، یعنی،

$$x \equiv b - f'(b)\cdot \frac{f(b)}{p^a} p^a (\text{هنگ } p^{a+1}) .$$

بنابراین، ملاحظه شد که در کلیهٔ حالات وقتی کــه جوابهای به‌هنگ p^a را بــدانیم می‌توانیم جوابهای به هنگ p^{a+1} را تعیین کنیم. این قسمت را با ذکــر چند مثال خاتمه می‌دهیم.

مثال ۴ : کلیهٔ جوابهای همنهشتی

$$f(x) = x^۳ - ۲x + ۱ \equiv ۰ (\text{هنگ } ۳^۲)$$

را بیابید. حل مسئله را با تعیین کلیهٔ جوابهای $f(x) \equiv ۰ (\text{هنگ } ۳)$ از راه تجسس شروع می‌کنیم. فقط سه امکان وجود دارد، یعنی $x \equiv ۰ ، \pm ۱ (\text{هنگ } ۳)$. بسهولت تحقیق می‌کنیم که $x \equiv ۱ (\text{هنگ} ۳)$ تنها جواب مسئله می‌باشد.

ابتدا $f(x) \equiv ۰ (\text{هنگ } ۳^۲)$ را حل می‌کنیم. یك جواب بــه هنگ ۳ وجود دارد، بنابراین $b = b_۱ = ۱$. همچنین، $f(۱) = ۰$ و $f'(x) = ۳x^۲ - ۲$، بنابراین $f'(۱) = ۱$. پس، بنابر (۷)، بایستی همنهشتی

$$۱ \times k \equiv \frac{۰}{۳} (\text{هنگ } ۳)$$

را حل کنیم، که دارای جواب منحصر بفرد $k \equiv ۰ (\text{هنگ } ۳)$ است. بنابراین،

$$x \equiv b + k \times ۳ \equiv ۱ (\text{هنگ } ۹)$$

تنها جواب به هنگ ۹ می‌باشد. (دراین حالت زیاد مشکل نخواهد بود کــه این نتیجه را مستقیماً با بررسی تمام نه حالت ممکن به هنگ ۹ تحقیق کنیم.)

مثال۵: می‌خواهیم کلیهٔ جوابهای همنهشتی

$$f(x) = x^۲ + x + ۱ \equiv ۰ (\text{هنگ } ۴۹)$$

راپیدا کنیم. کار را بایستی مجدداً باحل همنهشتی $f(x) \equiv ۰ (\text{هنگ } ۷)$ شروع کنیم. با بررسی مستقیم هفت حالت ممکن می‌بینیم که $f(x) \equiv ۰ (\text{هنگ } ۷)$ اگر، وفقط اگر،

$$x \equiv ۲ \text{ یا } -۳ (\text{هنگ } ۷) .$$

اینك $f(x) \equiv ۰ (\text{هنگ } ۷^۲)$ راحل می‌کنیم. دراینجا $b_۱ = ۲$ و $b_۲ = -۳$. بامحاسبه معلوم می‌شود

$$f(۲) = ۷ \text{ و } f(-۳) = ۷ .$$

همچنین $f'(x) = ۲x + ۱$، و بنابراین

$$f'(۲) = ۵ \quad \text{و} \quad f'(-۳) = -۵ .$$

برای یافتن جوابهایی به‌صورت $x = ۲ + ۷k$ بایستی (۷) را حل کنیم، دراین حالت

$$۵k \equiv -\frac{۷}{۷} \; (\text{هنگ } ۷) \; ،$$

بنابراین $k \equiv -۳$ (هنگ ۷) و $x \equiv -۱۹$ (هنگ ۴۹). به‌همین‌طریق، اگر $x = -۳ + ۷k$، بایستی

$$-۵k \equiv -\frac{۷}{۷} \; (\text{هنگ } ۷)$$

راحل کنیم، لذا $k \equiv ۳$ (هنگ ۷) و $x \equiv ۱۸$ (هنگ ۴۹). پس، جوابهای $f(x) \equiv ۰$ (هنگ ۴۹) چنین خواهند شد $x \equiv ۳۰ \; ، \; ۱۸$ (هنگ ۴۹) .

مثالهای (۴) و (۵) هردو جزء حالت۲ مذکور درفوق قرار می گیرند. اکنون مثالی از حالت۱ ارائه‌می کنیم

مثال ۶: کلیهٔ جوابهای

$$f(x) = x^۲ + x + ۷ \equiv ۰ \; (\text{هنگ } ۲۷)$$

را بیابید.

می بینیم که $x \equiv ۱$ (هنگ ۳) تنها جواب $f(x) \equiv ۰$ (هنگ ۳) است . اینك $f(x) \equiv ۰$ (هنگ $۳^۲$) راحل می کنیم. دراینجا $b_۱ = ۱$، $f(۱) = ۹$. چون $f'(x) = ۲x + ۱$، داریم $f'(۱) = ۳$. بنابراین، جوابها به‌صورت $x = ۱ + ۳k$ هستند، که k در

$$۳k \equiv -\frac{۹}{۳} \; (\text{هنگ } ۳)$$

یا

$$۳k \equiv -۳ \; (\text{هنگ } ۳)$$

صدق‌می کند. واضح‌است که‌جمیع مقادیر k دراین همنهشتی صدق می کنند، بنابراین‌جوابهای $x = ۱ + ۳k$ به‌ازای $k \equiv ۰ \; ، \; ۱ \; ، \; ۲$ (هنگ ۳) حاصل می‌شوند و درنتیجه

$$x \equiv ۱ \; ، \; ۴ \; ، \; \text{یا } ۷ \; (\text{هنگ } ۹)$$

جوابهای $f(x) \equiv ۰$ (هنگ ۹) هستند.

بالاخره، $f(x) \equiv ۰$ (هنگ $۳^۳$) راحل می کنیم. دراینجا $b_۱ = ۱$ ، $b_۲ = ۴$ ، $b_۳ = ۷$. پس،

$$f(۱) = ۹ \quad ، \quad f(۴) = ۲۷ \quad ، \quad f(۷) = ۶۳$$

و

$$f'(۱)=۳ \text{ ، } f'(۴)=۹ \text{ ، } f'(۷)=۱۵ \text{ .}$$

جوابها به‌صورت $x=b_i+۹k$ ، به‌ازای $i=۱ ، ۲ ، ۳$ هستند. به‌ازای $i=۱$ ، k بایستی درهمنهشتی

$$۳k\equiv -\frac{۹}{۹}(\text{هنگ } ۳)$$

صدق کند و واضح است که جوابی وجود ندارد. به‌ازای $i=۲$ ، k بایستی در

$$۹k\equiv -\frac{۲۷}{۹}(\text{هنگ } ۳)$$

صدق کند و از آنجا که هر k در همنهشتی فوق صدق می‌کند جوابهای

$$x\equiv ۴+۹\times ۰\equiv ۴(\text{هنگ } ۲۷) \text{ ، } x\equiv ۴+۹\times ۱\equiv ۱۳(\text{هنگ } ۲۷) \text{ ، } x\equiv ۴+۹\times ۲\equiv ۲۲(\text{هنگ } ۲۷)$$

به‌دست‌می‌آیند. به‌ازای $i=۳$ ، k بایستی در

$$۱۵k\equiv -\frac{۶۳}{۹}\equiv -۷ \ (\text{هنگ } ۳)$$

صدق کند، وبنابراین جوابی وجود ندارد. پس $f(x)\equiv ۰(\text{هنگ } ۲۷)$ اگر، وفقط اگر،

$$x\equiv ۴ ، ۱۳ ، \text{ یا } ۲۲ \ (\text{هنگ } ۲۷).$$

۴.۳ تمرینات

۱. کلیهٔ جوابهای همزمان همنهشتیهای زیر را بیابید:

(آ) $x\equiv ۳(\text{هنگ } ۷)$ ، $x\equiv ۲(\text{هنگ } ۶)$.

(ب) $x\equiv ۵(\text{هنگ } ۲)$ ، $x\equiv ۱(\text{هنگ } ۳)$ ، و $x\equiv ۲(\text{هنگ } ۵)$.

(ج) $x\equiv ۱(\text{هنگ } ۹)$ ، $x\equiv ۵(\text{هنگ } ۷)$ ، و $x\equiv ۳(\text{هنگ } ۵)$.

۲. کلیهٔ اعدادصحیح n را که درتقسیم بر ۸ باقیماندهٔ ۴ و درتقسیم بر ۷ باقیماندهٔ ۶ ودرتقسیم بر ۵ باقیماندهٔ ۱ داشته‌باشند، بیابید.

۳. نشان دهید که به‌ازای هرعدد صحیح $k\geqslant ۱$ ، k عددصحیح متوالی وجود دارند که بر مربعهای اعدادی بزرگتراز ۱ بخشپذیرند (راهنمایی: ازقضیهٔ باقیماندهٔ چینی استفاده کنید.)

۴. با استفاده ازقضیهٔ باقیماندهٔ چینی همنهشتیهای زیر را حل کنید:

(آ) $x^۲+۱\equiv ۰(\text{هنگ } ۶۵)$.

(ب) $۵x^۲+۷x-۳\equiv ۰(\text{هنگ } ۳۵)$.

(ج) $11x+1\equiv 0$ (هنگ 210) .

۵. معلوم کنید که آیا مجموعه‌های همنهشتیهای همزمان زیر دارای جواب هستند؟ اگر جواب دارند کلیهٔ آنها را بیابید.

(آ) $x\equiv 5$ (هنگ 6) و $x\equiv 7$ (هنگ 10) .

(ب) $x\equiv 1$ (هنگ 6) و $x\equiv 8$ (هنگ 15) .

*۶. فرض کنیم m و n اعداد صحیح مثبت باشند. فرض کنیم بمعم$(m, n)=d$. ثابت کنید که همنهشتیهای همزمان

$x\equiv a$ (هنگ m) و $x\equiv b$ (هنگ n)

حلپذیرند اگر، وفقط اگر، $a\equiv b$ (هنگ d) .

۷. کلیهٔ جوابهای همزمان همنهشتیهای زیر را بیابید:

(آ) $3x\equiv 1$ (هنگ 10) و $4x\equiv 2$ (هنگ 7) .

(ب) $3x\equiv 2$ (هنگ 4) ، $2x\equiv 7$ (هنگ 15) ، و $4x\equiv -1$ (هنگ 7) .

۸. فرض کنیم m_1 ، m_2 ، … ، m_k اعداد صحیح مثبت دوبدو نسبت به‌هم اول باشند. فرض کنیم b_1 ، b_2 ، … ، b_k و a_1 ، a_2 ، … ، a_k اعداد صحیح مفروض باشند، به‌طوری که به‌ازای $i=1, 2, \ldots, k$ ، $1=$ بمعم(b_i, m_i). ثابت کنید که همنهشتیهای همزمان

$b_1x\equiv a_1$ (هنگ m_1)

$b_2x\equiv a_2$ (هنگ m_2)

$\vdots$

$b_kx\equiv a_k$ (هنگ m_k)

همواره حلپذیرند. دستوری شبیه قضیهٔ باقیماندهٔ چینی برای تعیین x دراین حالت ارائه دهید.

۹. با استفاده از روشی که دراین بخش بسط داده شده همنهشتیهای زیر را حل کنید:

(آ) $x^4+2x+4\equiv 0$ (هنگ 27) .

(ب) $x^2\equiv -1$ (هنگ 125) .

(ج) $x^2+3x-3\equiv 0$ (هنگ 49) .

(د) $x^2+3x-10\equiv 0$ (هنگ 49) .

۱۰. کلیهٔ جوابهای همنهشتی زیر را بیابید:

$4x^4+9x^3-5x^2-21x+61\equiv 0$ (هنگ 1125) .

(توجه: این مسئله برای روشن کردن کلیهٔ مفاهیم وحالاتی که دراین بخش مورد بحث قرار گرفته طرح شده است. جوابها $x\equiv 323, -52, -427$ (هنگ 1125) می‌باشند.)

۱۱. فرض کنیم p عدد اولی بزرگتر از ۲ باشد و فرض کنیم $p\nmid a$. فرض کنیم $x^{2}-a\equiv 0\,(p$ هنگ$)$ حلپذیر باشد. نشان دهید که به‌ازای کلیهٔ مقادیر $n\geqslant 1$، همنهشتی

$$x^{2}-a\equiv 0\,(p^{n}\ \text{هنگ})$$

درست دوجواب دارد.

*۱۲. فرض کنیم $p>2$ عددی اول باشد. به‌ازای کلیهٔ مقادیر $n\geqslant 1$، وقتی $p|a$ حلپذیری $x^{2}+a\equiv 0\,(p^{n})$ را تحلیل کنید. (حالات متعددی وجود خواهند داشت که به بزرگترین توان m به‌طوری که $p^{m}|a$ و به‌نتیجهٔ خارج‌قسمت a/p^{m} بستگی‌دارند.)

۱۳. فرض کنیم m و n اعدادصحیح مثبتی باشند به‌طوری که $1=(m\,،\,n)$بمعم. فرض کنیم r_{1} ، ... ، $r_{\varphi(m)}$ دستگاه‌مخففی‌ازمانده‌ها به‌هنگ m و s_{1} ، ... ، $s_{\varphi(n)}$ دستگاه مخففی از مانده‌ها به‌هنگ n باشند.

(آ) نشان دهید که اگر $1=(x\,،\,mn)$بمعم، آنگاه زوج منحصر به‌فرد $(i\,،\,j)$ با شرط $1\leqslant i\leqslant\varphi(m)$ و $1\leqslant j\leqslant\varphi(n)$ موجوداست‌به‌طوری که $x\equiv r_{i}(m$ هنگ$)$ و $x\equiv s_{j}(n$ هنگ$)$.

(ب) بالعکس، نشان‌دهید که به‌ازای‌هرزوج‌مفروض $(i\,،\,j)$، x منحصر بفردی به‌هنگ mn موجود است به‌طوری که $x\equiv r_{i}(m$ هنگ$)$ و $x\equiv s_{j}(n$ هنگ$)$ و $1=(x\,،\,mn)$بمعم.

۱۴. با استفاده از تمرین ۱۳ ثابت کنید که اگر $1=(m\,،\,n)$بمعم، آنگاه $\varphi(mn)=\varphi(m)\varphi(n)$.

۱۵. ثابت کنید که اگر $n=p_{1}^{k_{1}}p_{2}^{k_{2}}\ldots p_{r}^{k_{r}}$ تجزیهٔ استاندهٔ n به حاصلضرب اعداد اول باشد، آنگاه

$$\varphi(n)=p_{1}^{k_{1}-1}(p_{1}-1)\,p_{2}^{k_{2}-1}(p_{2}-1)\ldots p_{r}^{k_{r}-1}(p_{r}-1)\,.$$

(ازتمرین ۱۴ فوق وتمرین ۶ بخش ۲.۳ استفاده کنید.)

۱۶. از روی تعریف مشتق صوری یک بسجمله که درمتن‌آورده شده، مستقیماً ثابت‌کنید که برای بسجمله‌های f و g و عددصحیح a داریم

(آ) $(af)'=af'$. (ب) $(f+g)'=f'+g'$. (ج) $(fg)'=f'g+fg'$.

۵.۳ حل همنهشتیهای بسجمله‌ای، ۲

دراین بخش، نظریهٔ همنهشتیهای بسجمله‌ای $f(x)\equiv 0\,(n$ هنگ$)$ را بیشتر گسترش خواهیم‌داد. هدف اولیهٔ مامطالعهٔ همنهشتی $f(x)\equiv 0\,(p$ هنگ$)$، به‌ازای عدد اول p است. کوشش‌اصلی بخش‌قبلی‌این بود که نشان‌دهیم اگر بتوانیم همنهشتیهای بسجمله‌ای به‌هنگ‌اعداد اول‌راحل کنیم، آنگاه‌می‌توانیم به‌طورنسبتاً عادی‌آن‌را به‌همنهشتیهای کلی به‌هنگ n منتقل‌سازیم. بنابراین، کلیهٔ مشکلات ما قبلاً بایستی درمورد اعداد اول‌پیش‌بیایند. متأسفانه‌تنهاکاری که ما دراین بخش انجام خواهیم داد اثبات بعضی حقایق کلی درمورد همنهشتیهای بسجمله‌ای

به‌هنگ اعداد اول است. ما برای حل عملی آنها یا حتی برای تعیین اینکه آنها چه‌وقت دارای جواب‌اند روشی ارائه نخواهیم داد. زیرا چنین روشی بر کسی معلوم نیست. بعلاوه، تمامی فصل ۴ به‌حل این مسئله فقط درمورد بسجمله‌های درجهٔ دوم اختصاص دارد.

مطلب را با بیان کلیاتی دراین زمینه‌شروع می‌کنیم. چون کوشش ما برای‌حل همنهشتی

$$f(x)\equiv 0\ (\text{هنگ}\ n)\ , \qquad (۱)$$

به‌ازای بسجملهٔ $f(x)=a_mx^m+\dots+a_1x+a_0$، باضرایب صحیح است، مطمئناً اگر مایك (یاچند) a_i راباعدد صحیح دیگری همنهشت‌آن به‌هنگ n عوض کنیم تفاوتی نمی‌کند و دقیقاً همان جوابها را به‌دست خواهیم‌آورد. در واقع، اگـر درهنگ n عمل کنیم، خیلی طبیعی است که دو بسجمله راکه اختلاف ضرایب آنها مضربی از n است، به‌هنگ n «یکی» بشماریم. بدین‌ترتیب، به‌ارائهٔ تعریف زیر برانگیخته می‌شویم:

تعریف ۱: فرض‌کنیم $f(x)=a_0+a_1x+\cdots$ و $g(x)=b_0+b_1x+\cdots$[1] بسجمله‌های با ضرایب صحیح باشند. گـوییم $f(x)$ با $g(x)$ همنهشت به هنگ n است و می‌نویسیم

$$f(x)\equiv_x g(x)\ (\text{هنگ}\ n)$$

به‌شرط‌آنکه، به‌ازای جمیع مقادیر i، $a_i\equiv b_i$ (هنگ n).

مثال ۲:

(یکم) $x^3+x+1\equiv_x x^3+x-2$ (هنگ ۳).

(دوم) $x^3+x+1\equiv_x 4x^3+x+7$ (هنگ ۳).

(سوم) $x^3+x+1\equiv_x 3x^7+x^3+x+1$ (هنگ ۳).

(چهارم) $58x^7+89x^5+18\equiv_x 3x^7+4x^5+3$ (هنگ ۵).

واضح است که، درحالت کلی می‌توانیم یك همنهشتی رابه‌جای همنهشتی (۱) بگذاریم که درآن همهٔ ضرایب بسجمله بین ۰ و $n-1$ (یاهردستگاه کامل مانده‌ها) باشند. این امـر به‌طور قابل ملاحظه‌ای درمحاسبات به‌ما کمك‌می‌کند.

حال اگر $f(x)\equiv_x g(x)$ (هنگ n) مفروض‌باشد، یك بسجمله مانند $t(x)$ باضرایب صحیح‌موجود است به‌طوری که

$$f(x)-g(x)=nt(x)$$

---

۱. این طریق نمایش f و g بیانگر آنستکـه f و g سریهای‌صحیح هستند، زیرا بسجمله‌ها تعدادی متناهی جمله دارند (مترجم).

(زیرا ضرایب $f(x)-g(x)$ همان a_i-b_i ، درتعریف ۱ هستند) . بنابراین ، اگر $f(a)\equiv 0$ (n هنگ) ، می بینیم که

$$g(a)=f(a)-nt(a)\equiv 0 \,(\text{هنگ } n)\,.$$

یعنی، همنهشتی (۱) دقیقاً همان جوابهای همنهشتی $g(x)\equiv 0$ (n هنگ) را دارد. پس نتیجهٔ زیر را ثابت کرده‌ایم:

قضیهٔ ۳: فرض کنیم $f(x)\equiv_n g(x)$ (n هنگ) . دراین صورت جوابهای همنهشتی $f(x)\equiv 0$ (n هنگ) دقیقاً همان جوابهای همنهشتی $g(x)\equiv 0$ (n هنگ) می باشند. بعلاوه، همواره کافی است همنهشتیهای بسجمله‌ای را به گونه‌ای درنظر بگیریم که بسجمله‌های آنها دارای ضرایبی، بین ۰ و $n-1$ باشند.

حال به‌روش قسمت (سوم) مثال ۲ برمی گردیم. درمعادلهٔ (۱) کلیهٔ ضرایب $f(x)$ که بر n بخشپذیرند می‌توانند با ۰ تعویض شوند. بالاخص، ممکن است بتوانیم درجهٔ $f(x)$ را کمتر کنیم. این امر موجب تعریف زیر می‌شود:

تعریف ۴: فرض کنیم $f(x)=a_0+a_1x+\dots+a_mx^m$ یك بسجمله با ضرایب صحیح باشد. فرض کنیم چنین نباشد که کلیهٔ a_iها بر n بخشپذیر باشند. دراین‌صورت، درجهٔ f به‌هنگ n، که به‌صورت $\deg_n f$ نوشته می‌شود ، به‌معنی بزرگترین عدد صحیح i است به‌طوری که $a_i\not\equiv 0$ (n هنگ).

ازاین‌رو، به‌عنوان‌مثال، اگر $f(x)=12x^4+3x^2+x+1$، آنگاه

$$\deg_5 f=4\ ،\ \deg_{12} f=2\ ،\ \deg_4 f=2\ ،\ \deg_3 f=1\,.$$

حال نظریهٔ خود را دربارهٔ جوابهای واقعی معادلهٔ (۱) شروع می کنیم. فرض کنیم $f(x)$ و $g(x)$ بسجمله‌هایی باشند و $g(x)\neq 0$. دراین‌صورت، عمل تقسیم طولانی بسجمله‌ها که شما آن‌را در دبیرستان آموخته‌اید دوبسجملهٔ $q(x)$ ، خارج‌قسمت ، و $r(x)$ ، باقیمانده، را پدید می‌آورد، به‌طوری که

$$\frac{f(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)}$$

یا

$$f(x)=g(x)q(x)+r(x) \qquad (*)$$

که درآن درجهٔ[1] $r(x)$ کمتراز درجهٔ $g(x)$ است. درحالت کلی، درست نیست که بگوییم ضرایب $q(x)$ و $r(x)$ اعداد صحیح هستند، حتی اگر $f(x)$ و $g(x)$ هردو دارای ضرایب صحیح باشند.

ما به‌این حالت کلی احتیاج نخواهیم داشت. فقط درحالتی که $g(x)=x-a$ ،

---

۱. به‌شرط آنکه $r(x)$ صفر نباشد (مترجم).

احتیاج به‌تقسیم طولانی داریم. قضیهٔ(*) دابرای این‌حالت خاص به‌طور کامل ثابت‌خواهیم کرد. برهان متضمن یك کاربرد سادهٔ استقرا خواهد بود. ولی، اگر شما مستقیماً دست‌به کار شوید وعمل تقسیم‌طولانی $f(x)=a_mx^m+\dots+a_0$ بر $x-a$ را انجام دهید، خواهید دیدکه استقرا چیزی نیست جز راهی برای گفتن «وغیره» درکار تقسیم طولانی زیر:

$$\begin{array}{r|l} & a_mx^{m-1}+\dots \\ \hline x-a & a_mx^m+a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\dots+a_0 \\ & a_mx^m-aa_mx^{m-1} \\ \cline{2-2} & (a_{m-1}+aa_m)x^{m-1}+a_{m-2}x^{m-2}+\dots+a_0 \end{array}$$

لم ۵: فرض کنیم $f(x)=a_mx^m+\dots+a_0$ بسجمله‌ای باضرایب‌صحیح و a عددصحیحی باشد، دراین‌صورت یك بسجملهٔ $q(x)$ باضرایب صحیح وجود دارد به‌طوری که

$$f(x)=(x-a)q(x)+f(a)\ .$$

برهان: این نتیجه را با استقرا نسبت به درجهٔ $f(x)$ ثابت خواهیم‌کرد. اگر $f(x)$ بسجملهٔ ثابت $f(x)=a_0$ باشد، آنگاه‌می‌توانیم قرار دهیم $q(x)=0$، این‌مطلبی است که‌بسهولت می‌توانیم آن‌را بررسی کنیم. بدین‌ترتیب حالتی راکه درجهٔ $f(x)$ صفر است‌ثابت‌کردیم.
سپس،می‌توانیم‌درستی لم۵را برای کلیهٔ بسجمله‌های‌از درجهٔ نابیشتراز $m-1$ بپذیریم. قرار می‌دهیم

$$\begin{aligned} f_1(x)&=f(x)-a_mx^{m-1}(x-a)\\ &=(a_{m-1}+aa_m)x^{m-1}+a_{m-2}x^{m-2}+\dots+a_0 \end{aligned}$$

درجهٔ $f_1(x)$ نابیشتراز $m-1$ است، و مـی‌توانیم از فـرض استقرا استفاده‌کنیم. بدین‌ترتیب، یك‌بسجملهٔ $q_1(x)$ باضرایب صحیح موجود است به‌قسمی که

$$f_1(x)=(x-a)q_1(x)+f_1(a).$$

پس،

$$\begin{aligned} f(x)&=f_1(x)+a_mx^{m-1}(x-a)\\ &=(x-a)(q_1(x)+a_mx^{m-1})+f_1(a). \end{aligned}$$

فرض کنیم $q(x)=q_1(x)+a_mx^{m-1}$. دراین‌صورت $q(x)$ دارای‌ضرایب صحیح است، و

$$f(x)=(x-a)q(x)+f_1(a)\ .$$

بالاخره، $x=a$ را درنتیجهٔ‌آخری‌قرار می‌دهیم ومی‌بینیم که $f(a)=f_1(a)$. بنابراین‌لم۵ کاملا ثابت شده است. ■

از لم ۵ مستقیماً به‌دست‌می‌آید که اگر a یك جواب (۱) باشد آنگاه می‌توانیم ازعامل $x-a$ به هنگ n «فاکتور بگیریم». یعنی،

قضیهٔ ۶: فرض کنیم $f(x)$ یك بسجمله باضرایب صحیح و a عـدد صحیحی باشد. دراین صورت $f(a)\equiv \circ (n$ هنگ$)$ اگر، وفقط اگر، یك بسجملهٔ $q(x)$ باضرایب صحیح وجـود داشته باشد به‌قسمی که

$$f(x)\equiv_x (x-a)q(x)(n \text{ هنگ}) . \qquad (۲)$$

(معادلهٔ (۲) یك همنهشتی بسجمله‌هاست، همان‌گونه که در تعریف ۱ آمده است.)

برهان: اگر $f(a)\equiv \circ (n$ هنگ$)$، از لم ۵ به‌دست می‌آوریم که

$$f(x)=(x-a)q(x)+f(a)،$$

که‌درآن $n|f(a)$. مثلا، اگر $q(x)$ رامانند لم ۵ اختیار کنیم، در واقع (۲) به‌دست خواهد آمد. بالعکس، هـرگاه ازقضیهٔ ۳ استفاده کنیم، می‌بینیم کـه چـون a یك جواب همنهشتی $(x-a)q(x)\equiv \circ (n$ هنگ$)$است، بایستی‌یك جواب $f(x)\equiv \circ (n$ هنگ$)$ هم‌باشد. ■

نتیجهٔ ۷: بسجملهٔ $q(x)$ درقضیهٔ ۶ همواره می‌توانـد طوری انتخاب شود کـه درجه‌اش حداکثر مساوی $\deg(f(x))-۱$ باشد.

برهان: $q(x)$ درقضیهٔ ۶ مستقیماً از لم ۵ حاصل می‌آید. برهان لـم ۵ را امتحان می‌کنیم. می‌بینیم که

$$q(x)=a_m x^{m-۱}+(a_{m-۱}+aa_m)x^{m-۲}+\dots ,$$

و لذا نتیجه روشن است. ■

اینك باید خود را به‌حل حالت

$$f(x)\equiv \circ (p \text{ هنگ}) ,$$

که درآن $n=p$ عددی اول است، محدودکنیم. دراین حالت می‌توانیم تعداد جـوابها را توسط درجهٔ معادله محدودکنیم. ابتدا ثابت‌می‌کنیم:

قضیهٔ ۸: فرض کنیم $f(x)$ بسجمله‌ای‌باضرایب‌صحیح‌باشد. فرض کنیم $b_۱$، $b_۲$، ...، b_t، t جواب ناهمنهشت $f(x)\equiv \circ (p$ هنگ$)$ باشند. دراین‌صورت یك بسجملهٔ $q(x)$ با ضرایب صحیح وجود دارد به‌قسمی که

$$f(x)\equiv_x (x-b_۱)(x-b_۲)\dots(x-b_t)q(x)(p \text{ هنگ}) .$$

بعلاوه، $\deg_p q(x)\leqslant \deg_p f(x)-t$.

برهان: اگر به‌جای $f(x)$ بسجمله‌ای همنهشت با آن به‌هنگ p بگذاریم می‌توانیم فرض کنیم $f(x)=a_m x^m+\dots+a_0$، که‌در آن $a_m \not\equiv 0$ (هنگ p). یعنی، $\deg_p f(x)=m$. بنا بر قضیهٔ۶ و نتیجهٔ۷ یك بسجملهٔ $q_1(x)$ وجود دارد به‌قسمی که

$$f(x)\equiv_x (x-b_1)q_1(x) \pmod{p}$$

با این شرط که $\deg_p q_1(x)\leqslant m-1=\deg_p f(x)-1$.

درنتیجهٔ اخیر b_2 را جایگزین x می‌کنیم، و به‌دست می‌آوریم

$$f(b_2)\equiv (b_2-b_1)q_1(b_2) \pmod{p}.$$

اما $f(b_2)\equiv 0 \pmod{p}$ ایجاب می‌کند که $p|(b_2-b_1)q_1(b_2)$ ، ولذا (بنا بر لم۲.۴.۰۳) $p|b_2-b_1$ یا $p|q_1(b_2)$. بنا بر فرض، $b_2\not\equiv b_1 \pmod{p}$ وبدین‌ترتیب $p|q_1(b_2)$، پس $q_1(b_2)\equiv 0 \pmod{p}$. مجدداً قضیهٔ ۶ ونتیجهٔ ۷ را به کار می‌بریم، می‌بینیم که بسجمله‌ای مانند $q_2(x)$ وجود دارد به‌قسمی که

$$q_1(x)\equiv_x (x-b_2)q_2(x) \pmod{p}$$

با $\deg_p q_2(x)\leqslant \deg_p q_1(x)-1$. بنابراین، یك مراجعهٔ فوری به تعاریف ایجاب می‌کند که

$$f(x)\equiv_x (x-b_1)(x-b_2)q_2(x) \pmod{p}.$$

با این‌شرط که

$$\deg_p q_2(x)\leqslant \deg_p q_1(x)-1\leqslant \deg_p f(x)-1-1=\deg_p f(x)-2.$$

اینك $x=b_3$ را درآخرین نتیجه قرار می‌دهیم. به‌همین‌طریق عمل می‌کنیم و به‌دست می‌آوریم

$$f(x)\equiv_x (x-b_1)(x-b_2)(x-b_3)q_3(x) \pmod{p}$$

با این‌شرط که $\deg_p q_3(x)\leqslant \deg_p f(x)-3$.

اگرعمل‌را به‌همین‌ترتیب ادامه دهیم، قضیهٔ۸ به‌دست می‌آید. ■

نتیجهٔ ۹: فرض کنیم $f(x)$ بسجمله‌ای باضرایب صحیح باشد وچنین نباشد که همهٔ‌ضرایب بر p بخشپذیر باشند. دراین‌صورت تعداد جوابهای ناهمنهشت $f(x)\equiv 0 \pmod{p}$ حداکثر برابر درجهٔ $f(x)$ به‌هنگ p است.

برهان: اگر b_1 ، … ، b_t ، t جواب ناهمنهشت باشند، آنگاه طبق قضیهٔ۸ داریم

$$f(x)\equiv_x (x-b_1)\dots(x-b_t)q(x) \pmod{p}$$

دراینجا $\deg_p q(x)\leqslant \deg_p f(x)-t$. ولی $q(x)$ بایستی دارای ضریبی باشد که بر p

بخشپذیر نباشد، زیرا درغیراین‌صورت کلیهٔ ضرایب $f(x)$ بر p بخشپذیر خواهند بود. بنابراین

$$0 \leqslant \deg_p q(x) \leqslant \deg_p f(x) - t$$

یا $t \leqslant \deg_p f(x)$، چنان‌که ادعا شده بود. ■

مثال ۱۰: اگر هنگ ما عددی اول نباشد، حکم نتیجهٔ ۹ غلط خواهد شد[1]. به‌عنوان مثال،

$$x^2 - 1 \equiv 0 \ (\text{هنگ } 8)$$

۴جواب $x \equiv 1, 3, 5, 7$ (هنگ ۸) دارد، درحالی‌که $\deg_8(x^2 - 1) = 2$.

ولی البته، $x^2 - 1 \equiv 0$ (هنگ p)، که p عددی اول است، فقط جوابهای $x \equiv \pm 1$ (هنگ p) دارد. زیرا مطابق نتیجهٔ ۹ می‌دانیم که حداکثر دوجواب موجوداست، وبوضوح $x \equiv \pm 1$ (هنگ p) جواب‌اند.

مثال ۱۱: بنابرقضیهٔ فرما (قضیهٔ ۱.۳) داریم اگر $p \nmid a$، آنگاه $a^{p-1} \equiv 1$ (هنگ p)، و بنابراین $a^p \equiv a$ (هنگ p). پس، a یك جواب

$$x^p - x \equiv 0 \ (\text{هنگ } p) \tag{۳}$$

است. روشن است که $x \equiv 0$ هم دراین همنهشتی صدق می‌کند. بنابراین هرعدد صحیح درهمنهشتی (۳) صدق می‌کند. اگر قضیهٔ ۸ را درمورد(۳) با جوابهای $0, 1, \ldots, p-1$ به‌کار بریم، می‌بینیم که

$$x^p - x \equiv_x x(x-1)\cdots(x-(p-1))q(x) \ (\text{هنگ } p), \tag{۴}$$

که درآن $\deg_p q(x) \leqslant p - p = 0$. بنابراین، $q(x)$ بسجمله‌ای است ثابت، مثلاً، $q(x) = b$، که b عددی است صحیح. پس ضریب x^p درطرف چپ (۴) برابر ۱ است و درطرف راست آن b است. بنابراین $b \equiv 1$ (هنگ p)، و

$$x^p - x \equiv_x x(x-1)(x-2)\cdots(x-(p-1)) \ (\text{هنگ } p).$$

به‌عنوان مثال، $x^3 - x \equiv_x x(x-1)(x-2)$ (هنگ ۳). (مستقیماً ضرب کنید ونتیجه را بررسی کنید.)

ممکن است‌درجهٔ بسجمله را دریك همنهشتی به‌هنگ یك عدد اول، بااستفاده ازنتایج مثال۱۱، بیشترتقلیل داد. چون $x^p \equiv x$ (هنگ p) به‌ازای هرمقدار x صادق است، می‌توانیم دریك بسجمله‌x را جایگزین x^p کنیم بی‌آنکه تغییری درمجموعهٔ جوابها داده شود. برای مثال، جوابهای

---

۱. بامراجعه به‌برهان نتیجهٔ ۹ (وقضیهٔ ۸) دریابیدکه اگرهنگ اول نباشدکدام‌قسمت ازاعتبار می‌افتد (مترجم).

$$x^{7}+x^{2}+5\equiv 0 \pmod{7}$$

دقیقاً همان جوابهای

$$x+x^{2}+5\equiv 0 \pmod{7}$$

هستند. زیرا، به‌ازای هرمقدار x ، $x^{7}\equiv x \pmod{7}$. اگرچه،

$$x^{7}+x^{2}+5\not\equiv_{x} x+x^{2}+5 \pmod{7}.$$

به‌عنوان مثالی که مستلزم کار بیشتری است،

$$x^{35}-x^{10}+x-3\equiv 0 \pmod{5} \qquad (5)$$

را درنظر می‌گیریم. چون $x^{35}=(x^{5})^{7}$ ، به‌ازای کلیهٔ مقادیر x داریم

$$x^{35}\equiv x^{7} \pmod{5}$$

چون $x^{7}=x^{5}x^{2}$ ، به‌ازای کلیهٔ xها داریم

$$x^{7}\equiv x\cdot x^{2}=x^{3} \pmod{5}$$

یا، به‌ازای هرعدد صحیح x ، $x^{35}\equiv x^{3} \pmod{5}$. به‌همین‌طریق، به‌ازای کلیهٔ مقادیر x،

$$x^{10}\equiv x^{2} \pmod{5}.$$

بدین‌ترتیب، جوابهای همنهشتی(۵) دقیقاً همان جوابهای‌همنهشتی زیراست

$$x^{3}-x^{2}+x-3\equiv 0 \pmod{5}.$$

ما بایك بسجمله از درجهٔ ۳۵ شروع کردیم و برای‌حل آن، کافی دانستیم که یك بسجملهٔ‌درجهٔ ۳ را حل کنیم.

باید توجه داشت که اگر دریك همنهشتی x را به‌جای x^{p} بگذاریم، محتملا، باتکرار این‌عمل به‌دفعات زیاد، همواره می‌توانیم به‌بسجمله‌ای از درجهٔ نابیشتراز $p-1$ برسیم. این مطلب را چنین بیان می‌کنیم:

قضیهٔ ۱۲: فرض کنیم p عددی اول باشد. دراین‌صورت

$$f(x)\equiv 0 \pmod{p}$$

می‌تواند به‌همنهشتی

$$g(x)\equiv 0 \pmod{p}$$

که دقیقاً دارای همان جوابهاست تبدیل شود، که درآن یادرجهٔ $g(x)$ حداکثر $p-1$ است ویا $g(x)$ بسجملهٔ‌صفر می‌باشد.

مثلاً، هنگامی که هنگ ۵ باشد، هرگز احتیاج نداریم بسجمله‌هایی از درجهٔ‌بزرگتر از ۴ را درنظر بگیریم.

۵.۳ تمرینات

۱. بررسی کنید که آیا زوجهای زیر از بسجمله‌ها به هنگ ۷ همنهشت هستند :

(آ) $x^۲+۲x+۱$ و $۸x^۳-۵x+۱$.

(ب) $۸x^۳-۶x+۱$ و $x^۲+۲x+۱$.

(ج) $۳x^۵+۲x^۲+x$ و $۱۰x^۵-۱۲x^۲+x+۷$.

(د) $۷x^۲+۲$ و $۷x+۲$.

۲. فرض کنیم $f(x)=۳۵x^۴+۷x^۲+۲x+۱$. مطلوب است $\deg_۲ f$ ، $\deg_۳ f$ ، $\deg_۵ f$ ، $\deg_۷ f$ و $\deg_{۱۱} f$.

۳. فرض کنیم f یك بسجمله باشد . نشان دهید که به ازای کلیهٔ اعداد اول p ، $\deg_p f\leqslant \deg f$ و فقط تعدادی متناهی از اعداد اول p وجود دارند به طوری که $\deg_p f<\deg f$.

۴. به‌ازای بسجمله‌های $f(x)$ درزیر واعداد صحیح a تحقیق کنید که $f(a)\equiv ۰$ (هنگ ۱۱). در هریك از این حالات ، بسجمله‌ای مانند $g(x)$ بیابید به قسمی که

$$f(x)\equiv_x (x-a)g(x)\ (\text{هنگ } ۱۱)\,.$$

(آ) $f(x)=x^۲+۱۰x+۳$ ، $a=۶$.

(ب) $f(x)=x^۳-x^۲+x+۱۰$ ، $a=۱$.

(ج) $f(x)=x^۳-۶x^۲-۲x+۲۰$ ، $a=-۳$.

۵. $x\equiv \pm ۱$ (هنگ ۱۳) جوابهای همنهشتی $f(x)\equiv ۰$ (هنگ ۱۳) می‌باشند، که در آن $f(x)=x^۴-۶x^۳-۳x^۲-۷x+۲$. بسجملهٔ $g(x)$ را بیابید به‌قسمی که

$$f(x)\equiv_x (x-۱)(x+۱)g(x)\ (\text{هنگ } ۱۳)\,.$$

۶. نشان دهید که بسجملهٔ $f(x)=x^۳+۳x^۲+۲x+۲$ به‌هنگ ۵ نمی‌تواند تجزیه‌شود (یعنی ، نمی‌توانیم بسجمله‌های $g(x)$ و $h(x)$ را بیابیم به قسمی که $\deg_۵ g(x)<۳$ ، $\deg_۵ h(x)<۳$ و $f(x)\equiv_x h(x)g(x)$ (هنگ ۵) .)

۷. همنهشتیهای بسجمله‌ای زیر را به همنهشتیهایی با همان جوابها که درجه‌ای کمتر از ۵ داشته باشند تبدیل کنید:

(آ) $۲x^{۱۷}+۳x^۲+۱\equiv ۰$ (هنگ ۵) .

(ب) $x^{۱۰}+۲x^۵+۱\equiv ۰$ (هنگ ۵) .

(ج) $۳x^{۲۳}+۲x^{۲۰}+۴x^{۱۷}-x^۶+x^۵-۳x^۳+۲x+۱\equiv ۰$ (هنگ ۵) .

۸. فرض کنیم p عددی اول و $f(x)=a_n x^n+\dots+a_۱ x+a_۰$ یك بسجمله باشد. فرض

کنیم $a_0 \not\equiv 0 \pmod p$ (هنگ p). نشان دهید که می‌توان یك بسجمله مانند $g(x)$ از درجهٔ نابیشتر از $p-2$ پیدا کرد به طوری‌که همنهشتیهای $f(x)\equiv 0$ (هنگ p) و $g(x)\equiv 0$ (هنگ p) جوابهای ناصفر واحدی داشته باشند.

۹. کلیهٔ جوابهای همنهشتیهای تمرین ۷ را بیابید.

۱۰. فرض کنیم p عددی اول باشد. اگر a و b اعداد صحیحی باشند به‌طوری که $a \geqslant 1$. کلیهٔ جوابهای همنهشتی

$$x^{p^a}\equiv b \ (\text{هنگ } p)$$

را بیابید.

۱۱. به ازای اعداد اول p، همنهشتیهای بسجمله‌ای زیر را ثابت کنید:

(آ) $x^{p-1}-1\equiv_x (x-1)(x-2)\cdots(x-(p-1))$ (هنگ p).

(ب) $x^{p-2}+x^{p-3}+\cdots+x+1\equiv_x (x-2)\cdots(x-(p-1))$ (هنگ p).

۱۲. با مقایسهٔ ضرایب دوطرف همنهشتی بسجمله‌ای تمرین ۱۱ (آ)، به ازای اعداد اول p همنهشتیهای زیر را ثابت کنید:

(آ) قضیهٔ ویلسن (ضریب ثابت را درنظر بگیرید).

(ب) به‌ازای $p\geqslant 3$، $1+2+\cdots+(p-1)\equiv 0$ (هنگ p).

(ج) به‌ازای $p\geqslant 5$،

$$1\times 2+1\times 3+\cdots+1(p-1)+2\times 3+\cdots+2(p-1)$$
$$+3\times 4+\cdots+3(p-1)+\cdots+(p-2)(p-1)\equiv 0 \ (\text{هنگ } p).$$

(د) به ازای $p\geqslant 5$،

$$1\times 2\cdots(p-2)+1\times 2\cdots(p-3)(p-1)+1\times 2\cdots(p-4)(p-2)$$
$$(p-1)+\cdots+1\times 3\cdots(p-1)+2\times 3\cdots(p-1)\equiv 0 \ (\text{هنگ } p).$$

۱۳**. فرض کنیم p عددی‌اول و $a\geqslant 1$ عددی صحیح باشد. فرض کنیم، r_1، ...، $r_{\varphi(p^a)}$ یك دستگاه مخفف مانده‌ها به هنگ p^a باشد. همنهشتی بسجمله‌ای زیر را ثابت کنید:

$$(x^{p-1}-1)^{p^{a-1}}\equiv_x (x-r_1)(x-r_2)\cdots(x-r_{\varphi(p^a)}) \ (\text{هنگ } p^a).$$

۶.۳ ریشه‌های اولیه

در این بخش کاربرد بینهایت مفیدی از نظریهٔ همنهشتیهای بسجمله‌ای به هنگ عدد اول p را ارائه می‌دهیم. ما خواص همنهشتی قوای گوناگون یك عدد صحیح a به هنگ p را پیدا خواهیم کرد.

مسئله را با آزمایشی شروع می کنیم. فرض کنیم $p=7$. درجدول ۳-۱ قوای a^k به هنگ ۷ را به ازای $a=0, 1, 2, \dots, 6$ (یک دستگاه کامل مانده‌ها) و $k=0, 1, 2, \dots, 6$، نسبت به‌دستگاه کامل‌مانده‌های ۰، ۱، ۲، ...، ۶ به‌هنگ ۷ فهرست کرده‌ایم.

چرا از $k=6$ جلوتر نرفتیم؟ به‌این دلیل که بنابر قضیهٔ کوچك فرما (قضیهٔ ۳.۱) می‌دانیم که اگر $7 \nmid a$، آنگاه $a^6 \equiv 1$ (هنگ ۷)، و بنابراین $a \equiv a$ (هنگ ۷) $a^7 = a^6$، $a^8 = a^6 \times a^2 \equiv a^2$ (هنگ ۷)، $a^9 = a^6 \times a^3 \equiv a^3$ (هنگ ۷)، والی آخر. بنابراین، وقتی که نماها به‌هنگ ۶، تغییرمی کنند، قوا خود به‌خود تکرار می‌شوند.

مطالعهٔ قوای یك عدد صحیح a درجدول، ما را به چه چیزی متوجه می‌سازد (اعداد جدول را در امتداد سطرها بخوانید)؟ در میان این اعداد دو عدد صحیح $a=3$، ۵، وجود دارند که همهٔ اعداد صحیح ۱، ۲، ۳، ۴، ۵، ۶ (یعنی، اعداد از ۱ تا $p-1$) را به عنوان قوهٔ خود می‌پذیرند. به عبارت دیگر، هر عدد صحیح b به قسمی که $b \not\equiv 0$ (هنگ p)، با قوه‌ای از ۳ (یا ۵) همنهشت به هنگ ۷ است. آیا این پدیده به‌ازای کلیهٔ اعداد اول p پیش می‌آید؟ اگر چنین باشد، ما می‌توانیم بررسی حساب به‌هنگ p را به بررسی قوای تنها یك عضو (همراه باصفر) تبدیل کنیم. در واقع، این موضوع درست است که به ازای هرعدد اول p چنین اعداد صحیحی وجود دارند، وآنها را ریشهٔ اولیه

جدول ۳ـ۱

قوای a^k از a (به هنگ ۷)

a \ k	۰	۱	۲	۳	۴	۵	۶
۰	۰	۰	۰	۰	۰	۰	۰
۱	۱	۱	۱	۱	۱	۱	۱
۲	۱	۲	۴	۱	۲	۴	۱
۳	۱	۳	۲	۶	۴	۸	۱
۴	۱	۴	۲	۱	۴	۲	۱
۵	۱	۵	۴	۶	۲	۳	۱
۶	۱	۶	۱	۶	۱	۶	۱

می‌نامند. دلیل وجود وفایدهٔ آنها موضوع بحث این بخش است. اینك ریشهٔ اولیه را رسماً تعریف می کنیم.

تعریف ۱ : فرض کنیم p عددی اول باشد. منظور از یك ریشهٔ اولیهٔ به هنگ p عددی‌است صحیح مانند g به طوری که اعداد

$$g^{\circ}=۱ ، g ، g^{۲} ، \dots ، g^{p-۲} \qquad (۱)$$

یك دستگاه مخفف مانده‌ها به هنگ p باشد. یعنی ، اعداد صحیح (۱) ، ترتیبی از اعداد ۱ ، ۲ ، ... ، $p-۱$ ، به‌هنگ p باشند.

هرچند که تعریف ۱ آنچه را که درباب ریشه‌های اولیه مورد نیاز است به ما می‌گوید، اما تعیین آنها آسان نیست ، وبنابراین به جدول ۳-۱ برمی‌گردیم تا ببینیم دیگر چه چیزی می‌توانیم پیدا کنیم. به سطرهای متناظر به اعداد غیر از ۳ و ۵ (و البته بجز $a\equiv ۰$) که درآنها درایه‌ها تکرارمی‌شوند، توجه می‌کنیم. به‌عنوان مثال، به ازای $a\equiv ۲$، می‌بینیم که ۱ ، ۲ ، ۴ تکرارشده‌اند. این‌بدان جهت‌است که $۲^{۳}\equiv ۱$ (هنگ ۷) ، وبنابراین $۲^{۴}=۲^{۳}\times ۲\equiv ۲$ (هنگ ۷) ، $۲^{۵}=۲^{۳}\times ۲^{۲}\equiv ۴$ (هنگ ۷) و الی آخر. یعنی ، اگر $a^{k}\equiv ۱$ (هنگ ۷) آنگاه $a^{k+۱}=a^{k}\,a\equiv a$ (هنگ ۷) ، و غیره . بنابراین می‌بینیم که نکتهٔ مهم این است که کوچکترین توانی برای a وجود دارد که حاصلش ، ۱ به هنگ ۷ می‌شود. ازاین به بعد قوای a خود به خود تکرار می‌شوند. بالاخص ، a به هنگ ۷ یك ریشهٔ اولیه است اگر، و فقط اگر، اولین قوه‌ای از a که برابر ۱ (به‌هنگ ۷) است ۶ باشد. (این قوه بنابر قضیهٔ کوچك فرما نمی‌تواند از ۶ بزرگتر باشد.) بدین ترتیب ما به تعریف زیر می‌رسیم :

تعریف ۲ : فرض کنیم p عددی‌اول باشد و a عددی صحیح به طوری که $a\not\equiv ۰$ (هنگ p). منظور از مرتبهٔ a به هنگ p کوچکترین عدد صحیح $k(\geqslant ۱)$ است به طوری که

$$a^{k}\equiv ۱ \ (\text{هنگ } p) .$$

این عدد را با $\mathrm{ord}_p a$ نمایش می‌دهیم .

مثلاً، $\mathrm{ord}_۷ ۲=۳$ ، $\mathrm{ord}_۷ ۳=۶$ ، $\mathrm{ord}_۷ ۴=۳$ ، $\mathrm{ord}_۷ ۵=۶$ ، و $\mathrm{ord}_۷ ۶=۲$.

بنابر قضیهٔ کوچك فرما ، می‌بینیم که $\mathrm{ord}_p a$ عددی است صحیح به طوری‌که

$$۱\leqslant \mathrm{ord}_p a\leqslant p-۱ .$$

همچنین از بحث فوق به قضیهٔ زیر می‌رسیم .

قضیهٔ ۳ : فرض‌کنیم p عددی اول و g عدد صحیحی باشد به طوری‌که $g\not\equiv ۰$ (هنگ p). در این صورت g یك ریشهٔ اولیه به هنگ p است اگر وفقط اگر $\mathrm{ord}_p g=p-۱$.

برهان: ابتدا فرض‌می‌کنیم g یك‌ریشهٔ اولیه به‌هنگ p باشد. دراین‌صورت، بنابرتعریف ۱ ، g° ، $g^{۱}$ ، ... ، $g^{p-۲}$ یك‌دستگاه مخفف مانده‌ها به هنگ p است. بالاخص، هیچ دوعددی

ازاین اعداد همنهشت نیستند. چون $g^{\circ}=1$، به ازای $1\leqslant k\leqslant p-2$ داریم $g^k\not\equiv 1\ (p$ هنگ$)$. چون $g^{p-1}\equiv 1\ (p$ هنگ$)$ (مجدداً قضیهٔ فرما)، بلافاصله از تعریف $\operatorname{ord}_p g$ داریم $\operatorname{ord}_p g=p-1$.

بالعکس، فرض کنیم $\operatorname{ord}_p g=p-1$. ازآنجا که $p-1$ عدد g°، ...، g^{p-2} وجود دارند که به ازای هر k، $p\nmid g^k$، برای اینکه نشان دهیم g یك ریشهٔ اولیه است، کافی است نشان دهیم که هیچ دوعددی ازاین اعداد همنهشت به هنگ p نیستند.

فرض کنیم این حکم غلط باشد. دراین صورت می‌توانیم دوعدد i و j بیابیم به‌قسمی که $0\leqslant i<j\leqslant p-2$ و

$$g^i\equiv g^j(p \text{ هنگ}) .$$

چون $g^j=g^ig^{j-i}$ و $p\nmid g^i$، می‌توانیم g^i را از طرفین حذف کنیم (قضیهٔ ۱۰۰۲) و به دست آوریم

$$1\equiv g^{j-i}(p \text{ هنگ}) .$$

چون $1\leqslant j-i<p-1$، پس فرض $\operatorname{ord}_p g=p-1$ را نقض کرده‌ایم. ■

اکنون ازقضیهٔ ۳ روشن می‌شود که $\operatorname{ord}_p a$ را باید به‌طور دقیق مطالعه کرد. ما نتایج را در قضیهٔ زیر جمع‌بندی خواهیم کرد.

قضیهٔ ۴ : فرض کنیم p عددی اول باشد و a عددی صحیح به طوری که $p\nmid a$. آنگاه

(یکم) $\operatorname{ord}_p a$، $p-1$ را عاد می‌کند.

(دوم) اگر $a^v\equiv 1\ (p$ هنگ$)$، آنگاه $\operatorname{ord}_p a$، v را عاد می‌کند.

(سوم)
$$\operatorname{ord}_p(a^u)=\frac{\operatorname{ord}_p a}{(u, \operatorname{ord}_p a)_{\text{بمعم}}} .$$

برهان : چون، بنابر قضیهٔ کوچك فرما داریم $a^{p-1}\equiv 1\ (p$ هنگ$)$، می‌بینیم که قسمت (یکم) مستقیماً از قسمت (دوم) نتیجه می‌شود.

قسمت (دوم) یك کاربرد مستقیم اصل کلی زیر برهان ۲.۳.۳ است که بدان توجه کردیم. یعنی، (برای خلاصه نویسی) می‌نویسیم $k=\operatorname{ord}_p a$، می‌توانیم مقادیری مانند q و r بیابیم به‌قسمی که

$$v=kq+r ,\ 0\leqslant r<k .$$

دراین صورت

$$1\equiv a^v=a^{kq+r}=(a^k)^q a^r\equiv 1^q a^r=a^r(p \text{ هنگ}) .$$

ولی k کوچکترین عدد صحیح $t(\geqslant ۱)$ است به طوری که $a^t \equiv ۱ \ (p$ هنگ$)$ و از این‌رو $a^r \equiv ۱ \ (p$ هنگ$)$ و $۰ \leqslant r < k$ ایجاب می‌کنند که $r = ۰$. پس، $k|v$، همچنانکه گفته شده بود.

برای قسمت (سوم) مجدداً می‌نویسیم $k = \text{ord}_p a$، همچنین می‌نویسیم

$$m = (u \text{ ، } \text{ord}_p a)_{\text{بمعم}} = (u \text{ ، } k)_{\text{بمعم}} .$$

ازآنجا، بنابر قسمت (دوم)، داریم

$$(a^u)^t = a^{ut} \equiv ۱ \ (p \text{ هنگ})$$

اگر، وفقط اگر، $k|ut$. ولی این معادل است با اینکه بگوییم

$$\frac{k}{m} \Big| \frac{ut}{m} .$$

چون $(k/m \text{ ، } u/m)_{\text{بمعم}} = ۱$ (قضیهٔ ۶.۳.۲) حکم اخیر با شرط

$$\frac{k}{m} \Big| t$$

معادل است (قضیهٔ ۶.۳.۲).

بنابراین، نشان داده‌ایم که $(a^u)^t \equiv ۱ \ (p$ هنگ$)$ اگر، وفقط اگر $(k/m)|t$. پس، k/m کوچکترین عدد صحیح t است که $(a^u)^t \equiv ۱ \ (p$ هنگ$)$، و بنابراین، همچنانکه می‌خواستیم ثابت کنیم $\text{ord}_p(a^u) = k/m$. ■

قبل ازاینکه بتوانیم وجود ریشه‌های اولیه را ثابت کنیم به یك قضیهٔ دیگر احتیاج داریم.

قضیهٔ ۵: فرض کنیم p عددی اول باشد و اعداد صحیح $a_۱$ و $a_۲$ به قسمی باشند که $p \nmid a_۱$ و $p \nmid a_۲$. بعلاوه فرض کنیم $\text{ord}_p a_۱ = k_۱$، $\text{ord}_p a_۲ = k_۲$ با این شرط که $(k_۱ \text{ ، } k_۲)_{\text{بمعم}} = ۱$، دراین صورت $\text{ord}_p(a_۱ a_۲) = k_۱ k_۲$.

برهان: چون

$$(a_۱ a_۲)^{k_۱ k_۲} = (a_۱^{k_۱})^{k_۲} (a_۲^{k_۲})^{k_۱} \equiv ۱^{k_۲} \times ۱^{k_۱} = ۱ \ (p \text{ هنگ}) ،$$

بنابر قضیهٔ ۴، قسمت (دوم)، $\text{ord}_p(a_۱ a_۲)$ عدد $k_۱ k_۲$ را عاد می‌کند.

حال فرض کنیم

$$(a_۱ a_۲)^t \equiv ۱ \ (p \text{ هنگ}) .$$

دراین صورت $a_1^t a_2^t \equiv 1 \pmod{p}$ و a_2^t عکس حسابی a_1^t می‌باشد.

بنابراین لم زیر مناسب است:

لم ۶: اگر $p \nmid a$ و a^* عکس حسابی a باشد، آنگاه $\mathrm{ord}_p a = \mathrm{ord}_p a^*$.

برهان : فرض کنیم $k = \mathrm{ord}_p a$. چون $a^k \equiv 1 \pmod{p}$ ، می‌بینیم که

$$a^{*k} = 1 \times a^{*k} \equiv a^k a^{*k} = (aa^*)^k \equiv 1^k = 1 \pmod{p},$$

وبنابراین، بنابر قضیهٔ ۴ ، قسمت (دوم) ، $\mathrm{ord}_p a^*$ عدد k را عاد می‌کند. حال فرض کنیم $\mathrm{ord}_p a^* = v$. دراین صورت، عیناً مانند فوق،

$$a^v \equiv a^{*v} a^v \equiv 1^v = 1 \pmod{p},$$

و بنابراین $\mathrm{ord}_p a = k$ عدد $v = \mathrm{ord}_p a^*$ را عاد می‌کند. یعنی ، $k|v$ و $v|k$ ، و بنابراین $v = k$. ■

دنبالهٔ برهان قضیهٔ ۵ : با توجه به‌آنچه که قبلا داشتیم، فوراً از لم ۶ نتیجه می‌گیریم که

$$\mathrm{ord}_p a_1^t = \mathrm{ord}_p a_2^t .$$

بنابراین، ازقضیهٔ ۴ ، قسمت (سوم)، نتیجه می‌شود که

$$\frac{k_1}{\text{بمعم}(t , k_1)} = \frac{k_2}{\text{بمعم}(t , k_2)}$$

چون $\text{بمعم}(k_1 , k_2) = 1$ ، k_1 ، k_2 هیچ عامل مشترکی بزرگتر از ۱ ندارنـد ؛ رابطهٔ اخیر ایجاب می‌کند که

$$\frac{k_1}{\text{بمعم}(t , k_1)} = \frac{k_2}{\text{بمعم}(t , k_2)} = 1$$

پس $k_1 = \text{بمعم}(t , k_1)$ ایجاب می‌کند $k_1|t$. به همین طـریق ، $k_2|t$. مجـدداً ، چون $\text{بمعم}(k_1 , k_2) = 1$ می‌توانیم نتیجه بگیریم که $k_1 k_2 | t$.

بالاخص ، تمام اینها نشان می‌دهند که $k_1 k_2 | \mathrm{ord}_p(a_1 a_2)$. همچنین ازآنجاکه $\mathrm{ord}_p(a_1 a_2) | k_1 k_2$ ، داریم $k_1 k_2 = \mathrm{ord}_p(a_1 a_2)$. ■

نتیجهٔ ۷ : فرض کنیم p عددی اول باشد و فرض کنیم a_1 ، ... ، a_r اعداد صحیحی باشند به قسمی که $p \nmid a_1 a_2 \dots a_r$. فرض کنیم $\mathrm{ord}_p a_i = k_i$ و k_iها دوبدو نسبت به‌هم اول‌اند. دراین صورت

$$\mathrm{ord}_p(a_1 a_2 \cdots a_r) = k_1 k_2 \cdots k_r .$$

برهان : تمرین (تمرین ۶) . ■

حال به اثبات قضیهٔ بنیادی این بخش می‌پردازیم .

قضیهٔ ۸ : اگر p عددی اول باشد، آنگاه ریشهٔ اولیه‌ای به‌هنگ p وجود دارد.

برهان : اگر $p=2$ ، آنگاه هرعدد فردی ریشهٔ اولیه خواهد بود، لذا فرض کنیم p فرد باشد. دراین صورت $p-1>1$ ، وبنابراین می‌توانیم بنویسیم

$$p-1=p_1^{a_1}p_2^{a_2}\dots p_r^{a_r},$$

که‌درآن p_1 ، p_2 ، ... ، p_r اعداد اول متمایزند.کافی‌است اعداد صحیح g_1 ، g_2 ، ... ، g_r را طوری‌بیابیم که

$$(*)\qquad \operatorname{ord}_p g_i=p_i^{a_i}\quad (1\leqslant i\leqslant r),$$

ازاین به بعد ، بنابر نتیجهٔ ۷ ، اگر قراردهیم $g=g_1g_2\dots g_r$ ، خواهیم داشت

$$\operatorname{ord}_p g=p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}=p-1,$$

و بنابراین ، بنابرقضیهٔ ۳ ، g یك ریشهٔ اولیه به هنگ p خواهد بود.

برهان وجود g_i براساس لم زیر بنا شده است.

لم ۹ : اگر $k|p-1$ ، آنگاه همنهشتی $x^k-1\equiv 0$ (هنگ p) درست k جواب دارد.

برهان : می‌نویسیم $p-1=kt$. از اتحاد بسجمله‌ای زیر که از دبیرستان باآن آشناهستیم استفاده می کنیم :

$$x^{p-1}-1=(x^k-1)(x^{k(t-1)}+x^{k(t-2)}+\dots+1).$$

فرض کنیم x یکی ازاعدادصحیح ۱ ، ۲ ، ... ، $p-1$ باشد.چون $x^{p-1}-1\equiv 0$ (هنگ p) (قضیهٔ کوچك فرما) ، داریم

$$(x^k-1)(x^{k(t-1)}+x^{k(t-2)}+\dots+1)\equiv 0 \ (\text{هنگ } p).$$

بنابراین ، $p|(x^k-1)(x^{k(t-1)}+\dots+1)$ ، و لـذا بنابـر لم اقلیدس (لم ۲.۴.۳) می‌بینیم که

$$p|x^k-1 \quad \text{یا} \quad p|x^{k(t-1)}+\dots+1.$$

به عبارت دیگر ، هر x که از میان اعداد ۱ ، ۲ ، ... ، $p-1$ اختیار شود جواب‌یکی از همنهشتیهای

$$x^{k}-۱\equiv ۰\ (\text{هنگ}\ p) \tag{۲}$$

یا

$$x^{k(t-۱)}+\dots+۱\equiv ۰\ (\text{هنگ}\ p) \tag{۳}$$

می‌باشد. چون $x\equiv ۰$ نه در همنهشتی (۲) و نه در همنهشتی (۳) صدق می‌کند، زوج همنهشتیهای (۲) و (۳) کلاً $p-۱$ جواب دارند. بنابر نتیجه ۹.۵ اولی، بایستی نابیشتر از k، و دومی بایستی نابیشتر از $k(t-۱)$ جواب داشته باشد. بنابراین، هردوی آنها روی هم رفته بایستی نابیشتر از $k+k(t-۱)=kt=p-۱$ جواب داشته باشند. تنها راه وقوع این امر این است که (۲) دارای k جواب باشد و (۳) دارای $k(t-۱)$ جواب. ادعایی که درمورد (۲) کردیم همان حکم لم ۹ می‌باشد. ■

دنبالهٔ برهان قضیهٔ ۸ : بنابر (*) می‌بینیم که کافی است نشان دهیم که عددی چون $g_۱$ وجود دارد به طوری که $\operatorname{ord}_p g_۱=p_۱^{a_۱}$. شرایطی که بایستی $g_۱$ درآنها صدق کند کدام‌اند؟ اولا،

$$g_۱^{p_۱^{a_۱}}\equiv ۱\ (\text{هنگ}\ p)\,. \tag{۴}$$

یعنی، $g_۱$ بایستی یك جواب همنهشتی

$$x^{p_۱^{a_۱}}-۱\equiv ۰\ (\text{هنگ}\ p) \tag{۵}$$

باشد. اکنون فرض می‌کنیم جوابی مانند $g_۱$ از (۵) را داریم. چه شرط دیگری باید $g_۱$ دارا باشد تا شرط $\operatorname{ord}_p g_۱=p_۱^{a_۱}$ را تضمین کند؟ فرض کنیم $b=\operatorname{ord}_p g_۱$. در این صورت، چون $g_۱$ در (۴) صدق می‌کند، می‌بینیم که $b\,|\,p_۱^{a_۱}$، لذا به ازای مقداری از v به طوری که $v\leqslant a_۱$، داریم $b=p_۱^{v}$. اما $\operatorname{ord}_p g_۱\neq p_۱^{a_۱}$ اگر، و فقط اگر، $b\neq p_۱^{a_۱}$، که معادل است با اینکه بگوییم $v\leqslant a_۱-۱$. اما اگر $v\leqslant a_۱-۱$، داریم

$$g_۱^{p_۱^{a_۱-۱}}=(g_۱^{b})^{p_۱^{a_۱-۱-v}}\equiv ۱\ (\text{هنگ}\ p)\,,$$

و بنابراین $g_۱$ درهمنهشتی

$$x^{p_۱^{a_۱-۱}}-۱\equiv ۰\ (\text{هنگ}\ p) \tag{۶}$$

صدق می‌کند. بالعکس، اگر $g_۱$ در (۶) صدق کند، آنگاه $\operatorname{ord}_p g_۱\,|\,p_۱^{a_۱-۱}$، و لذا $v\leqslant a_۱-۱$. پس، می‌بینیم که $\operatorname{ord}_p g_۱\neq p_۱^{a_۱}$ اگر، وفقط اگر، $g_۱$ درهمنهشتی (۶) صدق کند. بنابراین، $\operatorname{ord}_p g_۱=p_۱^{a_۱}$ اگر، وفقط اگر، $g_۱$ در (۵) صدق کند ولی در (۶) صدق نکند. بنابر لم ۹، همنهشتی (۵) $p_۱^{a_۱}$ جواب دارد وهمنهشتی (۶) $p_۱^{a_۱-۱}$ جواب. چون $p_۱^{a_۱-۱}<p_۱^{a_۱}$، می‌توانیم یك جواب (۵) را بیابیم که جواب (۶) نباشد. بنابراین، وجود $g_۱$ را ثابت کرده‌ایم.

به‌طریقی مشابه، می‌توانیم وجود g_2 ، ... ، g_r را نیز ثابت کنیم. ■

به‌نظر می‌رسد که اثبات فوق برای وجود ریشه‌های اولیه سازنده باشد، یعنی، روشی برای یافتن ریشه‌های اولیه به‌ما می‌دهد. ولی ارزش عملی آن کم است. زیرا باعلائم برهان قضیهٔ۸ ، بایستی جوابی از (۵) را بیابیم که جواب (۶) نباشد. ما برای‌حل (۵) روشی جزاینکه به‌جای x مقادیرخاص صحیحی بگذاریم وامتحان‌کنیم که آیا جواب هستند یا نه، نداریم. این روش از روش تعیین مستقیم مرتبهٔ اعداد صحیح خاص، از راه محاسبهٔ قوای آنها و تعیین اولین قوه‌ای که همنهشت با ۱ به‌هنگ p باشد، بهتر نیست. مع‌هذا، بایستی توجه‌کردکه روشی‌که دربرهان قضیهٔ۸ به‌کار رفته ونتایجی‌که از قضیهٔ ۴ ونتیجهٔ۷ به‌دست آمده‌اند، اغلب می‌توانند عمل را ساده‌کنند. اینك مثالی می‌آوریم.

مثال ۱۰: فرض‌کنیم $p=۲۳$. پس $p-۱=۲۲=۲\times۱۱$. بنابراین، به‌ازای اعداد صحیح a که $۲۳\nmid a$، داریم، $\operatorname{ord}_{۲۳}a=۱$ ، ۲ ، ۱۱ ، یا ۲۲ (قضیهٔ ۴(یکم)). مطلب را با محاسبهٔ $\operatorname{ord}_{۲۳}۲$ شروع می‌کنیم. بامحاسبه‌ای ساده می‌بینیم که $۲^۲\not\equiv۱$ (هنگ ۲۳) و $۲^{۱۱}\equiv۱$ (هنگ ۲۳)، بنابراین $\operatorname{ord}_{۲۳}۲=۱۱$. امامِلاحظه‌می‌کنیم که $\operatorname{ord}_{۲۳}(-۱)=۲$. بنابراین ما با استفاده از نتیجهٔ ۷ ، می‌بینیم که $\operatorname{ord}_{۲۳}(-۲)=۲\times۱۱=۲۲$. یعنی، -۲ یك ریشهٔ‌اولیه به‌هنگ ۲۳ است.

حال ببینیم که چگونه این مثال با طرح برهان قضیهٔ ۸ مطابقت می‌کند . چون $p-۱=۲\times۱۱$ ، می‌خواستیم‌جوابی برای همنهشتی $x^۲-۱\equiv۰$ (هنگ ۲۳) بیابیم که جواب $x-۱\equiv۰$ (۲۳) نباشد و جوابی برای $x^{۱۱}-۱\equiv۰$ (۲۳) بیابیم که جواب $x-۱\equiv۰$ (۲۳) نباشد. نشان دادیم که ۲ درشرط آخری صدق می‌کند وملاحظه‌کردیم که -۱ دراولین شرط صدق می‌کند ونتیجه‌گرفتیم که $(-۱)۲=-۲$ یك ریشهٔ اولیه بوده است.

حال درمورد چگونگی استفاده از ریشه‌های اولیه مفصلتر صحبت می‌کنیم. فرض‌کنیم g یك ریشه اولیه به‌هنگ عدد اول p باشد. درایـن‌صورت $g^۰$ ، $g^۱$ ، ... ، $g^{p-۲}$ دستگاه مخففی ازمانده‌ها به‌هنگ p است، وبنابراین هیچ‌دوتایی ازآنهانمی‌توانند همنهشت به‌هنگ p باشند. درحالت‌کلی، چه‌وقت g^i و g^j می‌توانند به‌هنگ p یکی باشند؟ اگر $i<j$ و

$$g^i\equiv g^j\ (p \text{ هنگ}) ,$$

آنگاه‌داریم $g^{j-i}\equiv۱$ (هنگ p). پس، $\operatorname{ord}_p g=p-۱$ ایجاب می‌کند که $p-۱\mid j-i$ (قضیهٔ۴ قسمت(دوم)) . بالعکس، اگر $p-۱\mid j-i$، آنگاه $j=i+k(p-۱)$ ، و بنابراین

$$g^j=g^{i+k(p-۱)}=g^i(g^{p-۱})^k\equiv g^i۱^k=g^i\ (p \text{ هنگ}) .$$

یعنی قضیهٔ زیر را ثابت‌کرده‌ایم.

قضیهٔ ۱۱: فرض کنیم g ریشهٔ اولیه‌ای به‌هنگ p باشد. دراین‌صورت $g^i \equiv g^j$ (هنگ p) اگر، وفقط اگر، $i \equiv j$ (هنگ $p-1$).

ازاین طریق، مسائل ضربی به‌هنگ p می‌توانند به‌مسائل‌جمعی به‌هنگ $p-1$ تبدیل شوند. (به‌تشابه این‌امر بالگاریتمها توجه کنید.) مااین مطلب را بابررسی مثال‌زیرباجزئیات بیشتری روشن خواهیم کرد. می‌خواهیم همنهشتی

$$x^n \equiv a \ (\text{هنگ } p) \qquad (۷)$$

راکه درآن $n>0$ و a عددصحیح مفروضی است حل کنیم. اعدادصحیح a که به‌ازای‌آنها همنهشتی(۷) یك جواب x داشته باشد مانده‌های قوهٔ nم به‌هنگ p نامیده می‌شوند.

اگر $p|a$ ، آنگاه پیداکردن‌جواب‌آسان است، زیرا دراین‌صورت $a \equiv 0$ (هنگ p)، وبنابراین همنهشتی(۷) همان $x^n \equiv 0$ (هنگ p) است. اگر x یك جواب آن باشد، آنگاه $p|x^n$. اما دراین‌صورت بنابر لم اقلیدس (لم ۳.۴.۲) $p|x$ وبنابراین $x \equiv 0$ (هنگ p). بالعکس، واضح‌است‌که $x \equiv 0$ (هنگ p) یك‌جواب می‌باشد. بنابراین، وقتی $p|a$، جوابها درست همان xهایی هستند که $x \equiv 0$ (هنگ p). ازاین به‌بعد، می‌توانیم فرض کنیم $p \nmid a$. دراین‌حالت، می‌بینیم که $x \equiv 0$ (هنگ p) نمی‌توانند جواب‌باشد.

همنهشتی(۷) لزومی نداردکه دارای جواب باشد. مثلا

$$x^2 \equiv 2 \ (\text{هنگ } 5)$$

جوابی ندارد. این امر را بسادگی از بررسی چهار حالت ممکن $x \equiv 1, 2, 3, 4$ (هنگ ۵) می‌بینیم، که بترتیب، به‌دست می‌آوریم $x^2 \equiv 1 ، 4 ، 4 ، 1$ (هنگ ۵). درواقع، (۷) همنهشتی‌کاملا دقیقی است، نظریهٔ آن بسیار پیچیده و مسائل حل نشدهٔ زیادی درآن مانده است. اکنون‌تلاش اولیه‌ای برای پیداکردن محکی‌برای‌حلپذیربودن(۷) رابه‌عمل‌می‌آوریم.

فرض‌کنید یك ریشهٔ اولیهٔ g به‌هنگ p را ثابت بگیریم. دراین‌صورت $1 = g^0$ ، g ، g^2 ، ... ، g^{p-2} یك‌دستگاه‌مخفف مانده‌ها به‌هنگ p است. چون $p \nmid a$، بایستی‌عددی صحیح مانند b وجود داشته باشد به‌طوری که

$$a \equiv g^b \ (\text{هنگ } p) \ .$$

علاوه براین، هیچ‌جواب x ازهمنهشتی(۷) نمی‌تواند بر p بخشپذیرباشد و بنابراین بایستی به‌صورت $x \equiv g^y$ (هنگ p) باشد. دراین‌صورت همنهشتی(۷) همان‌همنهشتی

$$g^{ny} \equiv g^b \ (\text{هنگ } p) \qquad (۸)$$

می‌باشد، وما باید جوابهای y را بیابیم. بنابرقضیهٔ ۱۱، (۸) باهمنهشتی خطی یك متغیرهٔ

$$ny \equiv b \ (\text{هنگ } p-1) \qquad (۹)$$

معادل است. می‌دانیم که (۹) برحسب y حلپذیر است اگر، وفقط اگر، بمعم$(n, p-1) \mid b$.

بنابراین ثابت‌کرده‌ایم که

قضیهٔ ۱۲: فرض کنیم p عددی اول و a عددی صحیح باشد به‌طوری که $p \nmid a$. فرض کنیم g ریشهٔ اولیه‌ای به‌هنگ p باشد و $a \equiv g^b$ (هنگ p). در این صورت همنهشتی $x^n \equiv a$ (هنگ p) حلپذیر است اگر، و فقط اگر، $b \mid$ بمعم($p-۱$ ، n).

مثال ۱۳: فرض کنید حالتی را درنظر بگیریم که $p = ۲۳$. درمثال ۱۰ ملاحظه کردیم که $g = -۲ \equiv ۲۱$ (هنگ ۲۳) یك ریشهٔ اولیه به‌هنگ ۲۳ است. بعلاوه، با توجه به‌قضیهٔ ۱۲ می‌دانیم که اگر $a \equiv (-۲)^b$ (هنگ ۲۳) آنگاه $x^n \equiv a$ (هنگ ۲۳) حلپذیر است اگر، و فقط اگر، $b \mid$ بمعم(۲۲ ، n). ازاین‌رو، مثلا اگر $n = ۲$ ، آنگاه b باید زوج باشد. اگر $n = ۱۱$، آنگاه b باید بر ۱۱ بخشپذیر باشد. همچنین اگر $۲ \nmid n$ و $۱۱ \nmid n$، b هرعدد دلخواهی می‌تواند باشد، وبنابراین به‌ازای هر a جوابی موجود است.

عملاً جوابها را چگونه محاسبه کنیم؟ برای انجام این امر، درواقع بایدهمنهشتی(۹) را حل کرد. اما قبل‌ازاینکه بتوانیم این کار را انجام دهیم باید بدانیم که b چیست. اما b به‌توسط شرط $a \equiv g^b$ (هنگ p) تعیین می‌شود، درحالی که a ازقبل به‌ما داده شده است. برای انجام این امر، به‌ازای مقادیر صریح a باید قوای g رافهرست کنیم. با استفاده از ریشهٔ اولیهٔ $g = -۲$ ی مثال ۱۰ ، قوای g^b را به‌ازای $۰ \leqslant b \leqslant p-۲ = ۲۱$ درجدول ۳-۲ فهرست می‌کنیم، وبرای این امر از دستگاه مخفف مانده‌های ۱ ، ۲ ، ... ، $p-۱$ استفاده می‌کنیم.

با استفاده از جدول ۳ـ۲ حل معادلاتی به‌صورت $x^n \equiv a$ (هنگ ۲۳) بسیار سهل است.

جدول ۳-۲

قوای ریشهٔ اولیهٔ ۲ــ به‌هنگ ۲۳

b	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱
g^b	۱	۲۱	۴	۱۵	۱۶	۱۴	۱۸	۱۰	۳	۱۷	۱۲	۲۲	۲	۱۹	۸	۷	۹	۵	۱۳	۲۰	۶	۱۱

به‌عنوان مثال،

$$x^{۷} \equiv ۱۷ \text{ (هنگ ۲۳)}$$

را حل می‌کنیم. بامراجعه به‌جدول ۳-۲، می‌بینیم که $۱۷ \equiv (-۲)^{۹}$ (هنگ ۲۳). می‌نویسیم $x \equiv (-۲)^{y}$ (هنگ ۲۳). دراین‌صورت، معادلهٔ $x^{۷} \equiv ۱۷$ (هنگ ۲۳) همان‌معادلهٔ

$$(-۲)^{۷y} \equiv (-۲)^{۹} \text{ (هنگ ۲۳)}$$

یا

$$۷y \equiv ۹ \text{ (هنگ ۲۲)}$$

می‌باشد. بسادگی تحقیق می‌کنیم که $\text{(هنگ ۲۲)}\ ۱۹ \equiv ۷^*$ (باتوجه به‌اینکه $\text{(هنگ ۲۲)}\ ۱ - \equiv ۷ \times ۳$)، ولذا

$$y \equiv ۱۹ \times ۹ \equiv -۲۷ \equiv ۱۷ \text{(هنگ ۲۲)}\ .$$

بنابراین $x \equiv (-۲)^{۱۷}$ (هنگ ۲۳) جوابی برای همنهشتی اولیه است. مجدداً بااستفاده از جدول ۳-۲ می‌بینیم که $x \equiv ۵$ (هنگ ۲۳) یك جـواب است. ایـن تنها جواب می‌باشد. (چرا؟)

نقص قضیهٔ ۱۲ این است که برای محاسبهٔ b ابتدا باید یك ریشهٔ اولیهٔ g به‌هنگ p را یافت. ولی می‌توانیم ازقضیهٔ ۱۲ محك سادهٔ زیر را که این نقص را ندارد استنتاج کنیم.

قضیهٔ ۱۴ (محك اویلر): فرض کنیم p عددی اول و a عددی صحیح باشد به‌طوری که $p \nmid a$ وفرض کنیم n مثبت باشد. هرگاه $s = (n \text{ ، } p-۱)$ بمعم، آنگاه همنهشتی $x^n \equiv a$ (هنگ p) حلپذیر است اگر، وفقط اگر، $a^{(p-۱)/s} \equiv ۱$ (هنگ p).

برهان: فرض کنیم g ریشهٔ اولیه‌ای به‌هنگ p باشد ومی‌نویسیم $a \equiv g^b$ (هنگ p).
ابتدا فرض کنیم $x^n \equiv a$ (هنگ p) دارای جواب باشد. دراین‌صورت

$$a^{(p-۱)/s} \equiv (x^n)^{(p-۱)/s} = (x^{p-۱})^{n/s} \text{(هنگ } p\text{)}$$

(یادآوری می‌کنیم که $s|n$ ، بنابراین n/s عـددی است صحیح.) بنابرقضیهٔ کـوچك فرما، $x^{p-۱} \equiv ۱$ (هنگ p)، وبنابراین

$$a^{(p-۱)/s} \equiv ۱^{n/s} = ۱ \text{(هنگ } p\text{)}.$$

بالعکس، فرض می‌کنیم $a^{(p-۱)/s} \equiv ۱$ (هنگ p). دراین‌صورت $a \equiv g^b$ (هنگ p) نتیجه می‌دهد که

$$۱ \equiv a^{(p-۱)/s} \equiv g^{b((p-۱)/s)} \text{(هنگ } p\text{)}\ .$$

بنابراین، چون $\mathrm{ord}_p g = p - ۱$ (قضیهٔ ۳)، ازقضیهٔ ۴ قسمت (دوم) نتیجه می‌گیریم که

$$p - ۱ | b\frac{p-۱}{s}\ ,$$

وبنابراین b/s عددی است صحیح. یعنی $s|b$ ، ولذا، بنابـر قضیهٔ ۱۲، $x^n \equiv a$ (هنگ p) حلپذیر می‌باشد. ■

اینك قضیهٔ ۱۴ را به‌حالت $n = ۳$ تخصیص می‌دهیم. اگـر $p \equiv ۲$ (هنگ ۳)، آنگاه $p - ۱ \equiv ۱$ (هنگ ۳)، بنابراین $۱ = (۳ \text{،} p - ۱)$ بمعم و $p - ۱ + ۳$ ... . اگر $p \equiv ۱$ (هنگ ۳)،

آنگاه $۳|p-۱$ ، پس $۳=$ بمعم$(p-۱ ، ۳)$. بنابراین به‌نتیجهٔ زیر می‌رسیم:

نتیجهٔ ۱۵: فرض کنیم p عدد اول فردی باشد و $p\neq ۳$ ، وفرض کنیم $۳\nmid a$. دراین‌صورت همنهشتی

$$x^{۳}\equiv a(\text{هنگ } p)$$

همواره حلپذیر است اگر $p\equiv ۲(\text{هنگ } ۳)$. اگر $p\equiv ۱(\text{هنگ } ۳)$، آنگاه این همنهشتی حلپذیر است اگر، وفقط اگر،

$$a^{(p-۱)/۳}\equiv ۱(\text{هنگ } p)$$

برهان: از قضیهٔ ۱۴ استفاده می‌کنیم. اگـر $p\equiv ۲(\text{هنگ } ۳)$ ، همنهشتی حلپذیر است اگر، وفقط اگر، $a^{p-۱}\equiv ۱(\text{هنگ } p)$ ، که بنابرقضیهٔ کوچك فرما برقرار است. ■

۶.۳ تمرینات

۱. فرض کنیم n عددصحیحی مثبت(که لزوماً اول نیست)، و a عددصحیحی باشدبه‌طوری که $۱=$ بمعم$(a ، n)$. مرتبهٔ a به‌هنگ n ، بنابر تعریف، کوچکترین عـدد صحیح مثبتی است مانند k به‌طوری که $a^{k}\equiv ۱(\text{هنگ } n)$ (می‌نویسیم $k=\operatorname{ord}_n a$). احکام زیـر راکه مشابه احکام قضیهٔ ۴ است ثابت کنید:

(آ) $\operatorname{ord}_n a$ موجود است.

(ب) $\operatorname{ord}_n a$ عدد $\varphi(n)$ را عاد می‌کند.

(ج) اگر $a^{v}\equiv ۱(\text{هنگ } n)$ ، آنگاه $\operatorname{ord}_n a|v$.

(د) $\operatorname{ord}_n(a^{u})=(\operatorname{ord}_n a)/$بمعم$(u ، \operatorname{ord}_n a)$.

۲. مقدار $\operatorname{ord}_n a$ را درحالات زیر تعیین کنید:

(آ) $n=۱۱$ ، $۱\leqslant a\leqslant ۱۰$.

(ب) $n=۱۳$ ، $۱\leqslant a\leqslant ۱۲$.

(ج) $n=۹$ ، $a=۱ ، ۲ ، ۴ ، ۵ ، ۷ ، ۸$.

(د) $n=۱۲$ ، $a=۱ ، ۵ ، ۷ ، ۱۱$.

(ه) $n=۱۵$ ، $a=۱ ، ۲ ، ۴ ، ۷ ، ۸ ، ۱۱ ، ۱۳ ، ۱۴$.

به‌خاطر داشته‌باشید که قضیهٔ ۴ یا تمرین۱ کار شمارا ساده می‌کند.

۳. فرض کنیم p عـددی اول باشد. ثـابت کنید کـه $\operatorname{ord}_p a=۲$ اگـر ، وفقط اگـر، $a\equiv -۱(\text{هنگ } p)$. آیا این‌نتیجه، اگر p عددی اول‌نباشد درست است؟

۴. تمرین ۸ از بخش ۳ را با استفاده از مفهوم مرتبه حل کنید. یعنی، ثابت کنید $\operatorname{ord}_n a = n-1$ ایجاب می‌کند که n اول باشد.

۵. ثابت کنید که قسمت (دوم) قضیهٔ ۴ مستقیماً از قسمت (سوم) آن نتیجه می‌شود.

۶. نتیجهٔ ۷ را ثابت کنید.

۷. ریشه‌های اولیهٔ اعداد زیر را تعیین کنید:

$$p = ۱۱ ، ۱۳ ، ۱۹ ، ۲۳ ، ۲۹$$

۸. فرض کنیم p عددی اول و g یك ریشهٔ اولیه به‌هنگ p باشد. به‌ازای اعداد صحیح $n(\geqslant ۱)$، نشان دهید که g^n یك ریشهٔ اولیه به هنگ p است اگر، و فقط اگر، $(n , p-۱)$ بمعم $= ۱$.

۹. فرض کنیم p عدد اول فردی باشد، $p \nmid a$. نشان‌دهید که $a^{(p-۱)/۲} \equiv \pm ۱$ (هنگ p).

۱۰. فرض کنیم p عددی اول باشد. فرض کنیم a عددصحیحی باشد به‌طوری که $p \nmid a$. a را یك ماندهٔ درجهٔ دوم به‌هنگ p نامیم اگر همنهشتی $x^۲ \equiv a$ (هنگ p) جواب داشته باشد. درغیر این‌صورت a را یك ناماندهٔ درجهٔ دوم می‌نامیم. بااستفاده از قضیهٔ ۱۴ (محك اویلر) وتمرین ۹ نشان دهید که حاصلضرب دوماندهٔ درجهٔ دوم یا دو ناماندهٔ درجهٔ دوم به‌هنگ p یك ماندهٔ درجهٔ دوم به‌هنگ p است، درحالی که حاصلضرب یك ماندهٔ درجهٔ دوم دریك ناماندهٔ درجهٔ دوم یك ناماندهٔ درجهٔ دوم به‌هنگ p است. چندمثال عددی برای روشن ساختن این نتیجه بسازید.

۱۱. از وجود ریشه‌های اولیه برای اثبات قضیهٔ ویلسن استفاده کنید.

۱۲. فرض کنیم p عددی اول و a عددی‌صحیح باشد به‌طوری که $p \nmid a$.

(آ) نشان‌دهید که اگر $\operatorname{ord}_p a = nm$ و (n , m) بمعم $= ۱$، آنگاه $a \equiv bc$ (هنگ p)، که‌درآن $\operatorname{ord}_p b = n$ و $\operatorname{ord}_p c = m$. (از تبصرهٔ صفحهٔ ۲۵ استفاده کنید.)

(ب) نشان دهید که اگر $\operatorname{ord}_p a = n_۱ n_۲ \dots n_k$ و n_i ها دوبدو نسبت به‌هم‌اول باشند، آنگاه $a \equiv b_۱ b_۲ \dots b_k$ (هنگ p)، که در آن $\operatorname{ord}_p b_i = n_i$ (راهنمایی: از استقرا استفاده کنید.)

۱۳. فرض کنیم p عددی اول باشد. نشان دهید که $\varphi(p-۱)$ ریشهٔ اولیه به‌هنگ p موجود است (راهنمایی: از تمرین ۸ استفاده کنید).

۱۴. فرض کنیم p عددی اول و n عددی‌صحیح و مثبت باشد به‌طوری که $n \mid p-۱$. نشان دهید که تعداد اعدادصحیح a به‌هنگ p که $\operatorname{ord}_p a = n$، مساوی $\varphi((p-۱)/n)$[1] است. (به تمرین ۱۳ مراجعه کنید.)

---

۱. صحیح آن $\varphi(n)$ است (مترجم).

۱۵. (اندیسها) فرض کنیم p عددی اول و g یك ریشهٔ اولیه به‌هنگ p باشد. دراین‌صورت اگر a عددصحیحی باشد به‌طوری که $p\nmid a$، می‌دانیم که به‌ازای عدد صحیحی مانند i، $0 \leqslant i \leqslant p-1$، $a \equiv g^i$ (هنگ p). i را اندیس a نسبت‌به g به‌هنگ p نامیم. وقتی که p و g معلوم باشند، می‌نویسیم $i = \operatorname{ind} a$. ثابت کنید

(آ) $a \equiv b$ (هنگ p) اگر، وفقط اگر، $\operatorname{ind} a \equiv \operatorname{ind} b$ (هنگ $p-1$).

(ب) $\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b$ (هنگ $p-1$).

(ج) $\operatorname{ind} a^* \equiv -\operatorname{ind} a$ (هنگ $p-1$)، که در آن a^* معرف عکس‌حسابی a به‌هنگ p است.

به‌شباهت مابین اندیسها و لگاریتمها توجه کنید.

۱۶. جدول اندیسها را به‌ازای $a = 1, 2, \ldots, p-1$ برای ریشه‌های اولیه به‌هنگ p که در تمرین ۷ حساب کردید محاسبه‌نمایید.

۱۷. از جداولی که در تمرین ۱۶ محاسبه کردید برای محاسبهٔ مقادیر اعداد ذیل به‌هنگ p استفاده کنید (جواب بایستی مابین ۱ و $p-1$ قرار گیرد):

(آ) $5 \times 6 \times 7 \times 8 \equiv ?$ (هنگ ۱۱).

(ب) $17^5 \times 14^9 \times 9^{21} \times 25 \equiv ?$ (هنگ ۲۹).

(ج) $15^4 (-8)^{10} \times 4^{11} \times 21^6 \equiv ?$ (هنگ ۱۳).

۱۸. کلیهٔ جوابهای همنهشتیهای زیر را بیابید:

(آ) $x^5 \equiv 13$ (هنگ ۲۳).

(ب) $x^{17} \equiv 50$ (هنگ ۲۳).

(ج) $5x^9 \equiv 43$ (هنگ ۲۳).

(د) $x^{93} \equiv 100$ (هنگ ۲۳).

(ه) $x^{10} \equiv 8$ (هنگ ۲۳).

(و) $x^{26} \equiv 10$ (هنگ ۲۳).

(توجه: از جدول ۳-۲ استفاده کنید.)

۱۹. فرض کنیم p عددی اول باشد. یك عددصحیح a که $p\nmid a$ یك ماندهٔ قوهٔ پنجم نامیده می‌شود اگر، وفقط اگر، همنهشتی $x^5 \equiv a$ (هنگ p) حل‌پذیر باشد. نشان دهید که

(آ) اگر $(p-1, 5) = 1$ بمعم، آنگاه هرعددصحیح یك ماندهٔ قوهٔ پنجم است.

(ب) اگر $5 \mid p-1$، آنگاه درست $(p-1)/5$ ماندهٔ قوهٔ پنجم به‌هنگ p وجود دارد.

۲۰. فرض کنیم p عددی اول و $n \geqslant 1$ و a عددی صحیح باشد. دستوری برای تعداد جوابهای $x^n \equiv a$ (هنگ p) ارائه دهید (فرض براین است که جواب وجود دارد).

درتمرینات ۲۱-۲۹ دقیقاً تعیین خواهیم کرد که چه هنگهایی مانند n ریشه‌های اولیه

دارند. یك ریشهٔ اولیه به‌هنگ n عددصحیحی است مانند a به‌طوری که (a , n) بمعم $= ۱$ و $\mathrm{ord}_n a = \varphi(n)$. (به‌تمرین ۱ مراجعه کنید.) دستوری‌را که برای $\varphi(n)$ درتمرین ۱۵ بخش ۴.۳ داده شده است مفروض بگیرید. دراین مسائل p معرف یك‌عدد اول فرد است.

۲۱. همنهشتی زیر را ازقضیهٔ دوجمله‌ای استنتاج کنید:

$$(a+p^k b)^{np^l} \equiv a^{np^l} + np^l a^{np^l - ۱} p^k b (p^{۲k+l} \text{ هنگ}) ، k \geqslant ۱ .$$

۲۲. (آ) فرض کنیم g یك ریشهٔ اولیه به‌هنگ p باشد و $r = g + pt$. نشان‌دهید که عددی مانند t وجود دارد به‌طوری که

$$r^{p-۱} = ۱ + ps ،$$

که درآن $p \nmid s$ ، نتیجه بگیرید که r یك ریشهٔ اولیه به‌هنگ $p^۲$ است.

(ب) بالعکس، نشان دهید که اگر r ریشهٔ اولیه‌ای به‌هنگ $p^۲$ باشد، آنگاه، به‌ازای مقداری مانند s که $p \nmid s$ ، $r^{p-۱} = ۱ + ps$.

۲۳**. نشان‌دهید که عددصحیح r درتمرین ۲۲ یك‌ریشهٔ اولیه‌به‌هنگ p^k ، به‌ازای کلیهٔ‌اعداد صحیح $k \geqslant ۱$ ، است. این امر را درمراحل زیر نشان دهید:

(آ) فرض کنیم $m = \mathrm{ord}_{p^k} r$. نشان دهید کــه $m = p^l d$ ، که‌درآن $l \leqslant k - ۱$ و $d | p - ۱$.

(ب) با درنظر گرفتن $(r^d)^{p^l}$ به‌هنگ p ، نشان‌دهید که $d = p - ۱$.

(ج) بااستفاده از دستور $r^{p-۱} = ۱ + ps (p \nmid s)$ ، نشان‌دهید که $l = k - ۱$.

(د) بااستناد به‌قسمتهای (آ)ـ(ج) وتمرین ۲۲ توجه کنید کــه، اگر r ریشهٔ اولیه‌ای به‌هنگ $p^۲$ باشد، آنگاه r نیز یك‌ریشهٔ اولیه به‌هنگ p^k $(k \geqslant ۱)$ است.

۲۴. ریشه‌های اولیه به‌هنگ ۹ ، ۲۷ ، ۸۱ ، ۲۴۳ ، ۲۵ ، ۱۲۵ را تعیین کنید.

۲۵. فرض کنیم p عدد اول فردی باشد و r یك ریشهٔ اولیه به‌هنگ p^k. اگر r فــرد باشد، فرض می‌کنیم $s = r$، واگر r زوج باشد، فرض می‌کنیم $s = r + p^k$. نشان دهید کــه s یك ریشهٔ اولیه به‌هنگ $۲p^k$ است.

۲۶. یك ریشهٔ اولیه به‌هنگ ۵۰ و ۹۸ بیابید.

۲۷. نشان دهید که ۲ و ۴ ریشه‌های اولیه دارند.

۲۸. بااستفاده ازتمرین ۱۱.۳ نتیجه‌بگیرید که اگر $k \geqslant ۳$، آنگاه ریشهٔ اولیه‌ای به‌هنگ ۲^k موجود نیست.

۲۹. حال فرض کنیم $n = p_۱^{a_۱} \dots p_l^{a_l}$. فرض می‌کنیم M مساوی کوچکترین مضرب‌مشترك $\varphi(p_۱^{a_۱})$ ، ... ، $\varphi(p_l^{a_l})$ باشد.

(آ) نشان‌دهید که به‌ازای کلیهٔ aهایی که ۱ = بمعم$(a \text{ ، } n)$، داریم $a^M \equiv 1$ (هنگ n).

(ب) نشان دهید که برای‌اینکه n ریشهٔ اولیه داشته باشد بایستی داشته‌باشیم $\varphi(n)|M$، بنابراین، ۴ یا ۲ ، p^k ، $n = 2p^k$.

۳۰. بااستفاده از ریشهٔ اولیه‌ای که درتمرین ۲۴ به‌دست‌آمده است، همنهشتیهای زیر را حل کنید:

(آ) $x^{17} \equiv 50$ (هنگ ۸۱).

(ب) $7x^{25} \equiv 10$ (هنگ ۸۱).

۳۱. روشی برای محاسبه‌کردن جدول قوای a به‌هنگ p موجود است. ابتدا جدول زیر را بسازید:

۱	۲	...	$p-1$
a	$2a$	...	$(p-1)a$ (هنگ p)

اگر $a^r \equiv j$ (هنگ p)، $0 \leqslant j < p-1$ ، می‌توانیم $a^{r+1} \equiv aj$ (هنگ p) را از روی این جدول بیابیم. ازاین روش برای محاسبهٔ قوای ۱۳ به‌هنگ ۲۳ استفاده کنید.

۷.۳ همنهشتیها ـ چندملاحظهٔ تاریخی

این فصل را به‌پایان رسانیدیم بی‌آنکه ازتکامل تاریخی نظریهٔ همنهشتیها قبلا به‌طور جدی بحث کرده‌باشیم. اینک به‌رفع این نقیصه می‌پردازیم.

درسده‌های هفدهم وهیجدهم فکر اساسی‌ای که درپس همنهشتیها وجود دارد به‌کار گرفته می‌شده است ومطالب خاص زیادی‌دربارهٔ همنهشتیها نوشته شده است. به‌عنوان‌مثال، همنهشتیهای فرما، اویلر، و ویلسن متعلق به‌همین دوره است. درسدهٔ هیجدهم، لاگرانژ و لژاندر تلاشهای بیشتری دراین‌زمینه به‌عمل‌آوردند. ولی، پیدایش واقعی همنهشتیها به‌صورت یك نظریهٔ منطقی، باانتشار کتاب تحقیقات‌حسابی[1] گاوس، در ۱۷۹۹ میلادی‌آغازشد. گاوس کسی بودکه برای اولین‌بار همنهشتیها را ازلحاظ خودآنها بطور منظم موردمطالعه‌قرارداد ونیز هم‌او بودکه‌علامت مناسبی راکه هنوزهم متداول است واردکرد. همچنین گاوس‌بودکه برای اولین‌بار مسئلهٔ حل همنهشتی بسجمله‌ای‌کلی

$$a_0 + a_1x + a_2x^2 + \dots + a_mx^m \equiv 0 \text{ (هنگ } n)$$

را مطرح‌کرد. درکتاب تحقیقات وکارهای بعدیش، گاوس مطالعهٔ همنهشتی‌کلی راتاآنجاکه می‌توانست ادامه داد، وسپس به‌مطالعهٔ عمیق همنهشتیهای درجات اول، دوم، سوم، و چهارم

1. Disquisitions Arithmeticae

پرداخت. درحل همنهشتیهای درجهٔ دوم، قانون تقابل مربعی‌راکه موضوع مورد بحث فصل بعدی خواهد بود، کشف وثابت کرد[1].

همنهشتیهای درجهٔ سوم بعداً بوسیلهٔ شاگرد ممتاز گاوس یعنی آیزنشتاین[2] موردمطالعه قرارگرفت. آیزنشتاین کسی بودکه در ۱۸۴۰ میلادی یك قانون تقابل مکعبی راثابت‌کرد. گاوس، خودش قانون تقابل مرتبهٔ چهارم‌را، که‌سروکارش باتعیین جواب همنهشتیهای‌درجهٔ چهارم است، ثابت‌کرد.

آثار گاوس خطسیری راکه قسمت اعظم نظریهٔ اعداد درتمام سدهٔ نوزدهم درپیش گرفت پیش‌بینی‌کرد. درکوششی برای تنظیم مجدد وبهترفهماندن تحقیقات گاوس، لوژون دیریکله رسالهٔ قاطعی در ۱۸۶۳ میلادی با نام دروس نظریهٔ اعداد[3] نوشت. سالهای بعد دیریکله، برای منعکس ساختن پژوهشهایی‌که دراین زمینه درجریان بود، متممهایی‌به‌چاپهای گوناگون‌کتابش اضافه‌کرد. دریك متمم خیلی مشهور، خلف دیریکله، ریچارد ددکیند[4] نظریهٔ همنهشتیهای‌گاوس را مجدداً برحسب ایده‌آلهاکه توسط ارنست‌کومر[5]، درارتباط با کارهایش روی آخرین قضیهٔ فرما، معرفی شده بود، مورد تفسیر قرارداد. آنچه‌که اصطلاحاً متمم دوازدهم ددکیند نام دارد نخستین مقالهٔ منظم از موضوعی است‌که امروزه به نظریهٔ جبری اعداد معروف شده‌است. بدین‌ترتیب، می‌بینیم‌که کارگاوس، به‌روشی کاملا مستقیم، به‌بسط میدان‌کاملا جدیدی درنظریهٔ اعداد منجرشد.

ازپنجاه سال‌قبل، تحقیقات وسیعی‌دربارهٔ همنهشتیهای بسجمله‌ای خصوصاًهمنهشتیهایی باچندمتغیر انجام‌گرفته است. این‌کار خیلی فنی است. اغلب سؤالات حسابی به‌ظاهر ساده درمورد همنهشتیهای‌چندمتغیره، از ریاضیات‌سطح بالایی همچون هندسهٔ جبری جداناپذیرند. کافی است بگوییم‌که همنهشتیها، حتی امروزه، ابزاری برای فرصتهای تحقیقاتی دامنه‌دار هستند.

---

۱. درواقع قسمتهایی ازآن توسط اویلرحدس زده شده بود، و قانون‌کامل‌آن توسط لژاندر حدس زده شده بود، هرچندکه‌گاوس ازکار آنها بی‌خبر بود.

2. Eisenstein

3. Vörlesungen über Zahlentheorie

4. Richard Dedekind

5. Ernst Kummer

۴

قانون تقابل مربعی

۱.۴ مقدمه

در فصل ۳ ، وقت نسبتاً زیادی را به بحث دربارهٔ همنهشتی بسجمله‌ای

$$f(x) \equiv 0 \quad (\text{هنگ } m)$$

اختصاص دادیم که درآن $f(x)$ بسجمله‌ای ازیك متغیر و m عدد صحیح مثبتی است. نشان دادیم که اگر بتوانیم همنهشتی

$$f(x) \equiv 0 \quad (\text{هنگ } p)$$

را به ازای هرعدد اول p که m را عاد می‌کند حل کنیم ، آنگاه می‌توانیم همنهشتی اصلی به هنگ m را حل کنیم. سپس به بحث دربارهٔ همنهشتیهای بسجمله‌ای به هنگ اعداد اول پرداختیم و برتعدادی از خواصی که حل آنها را مقدار زیادی تسهیل می‌کرد دست یافتیم. ولی، وقتی که‌همه‌چیز گفته وانجام‌شد، هیچ روش کلی برای حل‌همنهشتیها به‌هنگ اعداد اول ارائه ندادیم وحتی تعیین نکردیم که چه وقت چنین جوابی وجود دارد یا ندارد. (البته ، آزمون وخطا روشی است که متضمن‌بررسی فقط p حالت برای همنهشتیها به‌هنگ p است، ولی ما روشی درنظرداریم که تا اندازه‌ای بیشتر از بررسی صرف یك دستگاه کامل‌مانده‌ها به ما آگاهی می‌دهد.) علت اینکه هیچ روشی برای حل همنهشتیهای بسجمله‌ای کلی ارائه ندادیم این‌است که معمولاً چنین روشی در دست‌نیست. زیرا ، همچنانکه درفصل پیش‌متذکر شدیم ، یافتن یك روش کلی برای حل همنهشتیهای بسجمله‌ای به‌هنگ یك عدد اول یکی‌از مهمترین مسائل حل نشده در نظریهٔ اعداد است. در حالت‌کلی، این مسئله اساساً حل نشده است. ولی ، اگر توجه خود را به دستهٔ خاصی از همنهشتیها محدود بکنیم ، بعضی اوقات

ممکن است به جواب رضایت‌بخشی برسیم.

به عنوان مثال، ما روشی برای حل همنهشتیهای خطی در فصل قبل مقرر داشتیم. اینك نتایج خود را یادآوری می کنیم. درمورد همنهشتیهای خطی، $f(x)=ax+b$، بی‌آنکه خللی به کلیت وارد آید، می‌توانیم فرض کنیم $p\nmid a$. (در غیراین صورت، همنهشتی ما با همنهشتی بسیار سادهٔ $b\equiv 0 \pmod p$ معادل می‌باشد.) در این صورت همنهشتی خطی $ax+b\equiv 0 \pmod p$ همواره حلپذیراست ودقیقاً یك جواب به‌هنگ p دارد. این‌جواب به طور صریح توسط

$$x\equiv -ba^{p-2} \pmod p$$

داده می‌شود. (به تبصرهٔ بعد از قضیهٔ ۲.۳.۳ رجوع کنید.) از این‌رو، در مورد همنهشتیهای خطی، ما ازکلیهٔ اطلاعات ممکن بهترین‌آنها را دراختیار داریم: همواره یك جواب وجود دارد، وما می‌توانیم دستور صریحی برای جواب آن بنویسیم.

دراین فصل، حالتی راکه ازلحاظ دشواری در مرحلهٔ بعد قرار دارد، یعنی حالتی‌را که درآن $f(x)$ بسجملهٔ درجهٔ دومی مثل $f(x)=ax^2+bx+c$ است مورد بحث قرار خواهیم‌داد. معلوم‌خواهدشد که نظریهٔ همنهشتی

$$ax^2+bx+c\equiv 0 \pmod p \qquad (1)$$

از نظریهٔ همنهشتیهای خطی خیلی پیچیده‌تر است. اولا، ممکن است جوابی وجود نداشته باشد. ثانیاً، حتی وقتی‌که بدانیم جوابی موجود است توضیح محاسبهٔ آن ساده‌نیست. ولی حکمهای مثبتی وجود دارندکه می‌توانیم عرضه بکنیم. ما روشی را برای تعیین اینکه چه وقت همنهشتی (۱) جواب دارد وچه وقت ندارد بیان خواهیم‌کرد. این روش، که نتیجهٔ‌مهم این بخش است، ازقانون تقابل مربعی گاوس بهره می گیرد. ولی، باید تأکیدکنیم که‌گرچه، از طریق قانون تقابل، همواره می‌توانیم تعیین‌کنیم که‌آیا (۱) حلپذیراست یا نه، این‌روش هیچ وسیله‌ای بهتر از روش آزمون و خطا برای یافتن جوابها، وقتی که موجودند، در اختیار ما نمی‌گذارد.

قانون تقابل‌مربعی یکی از مشهورترین ومهمترین نتایج درنظریهٔ اعداد است. علاوه برنقشی که در تعیین حلپذیری همنهشتی (۱) دارد، اثبات می‌شود که غالباً به‌طور غیرمنتظره مفتاحی برای‌حل‌بعضی مسائل نظریهٔ اعداد است. بعضی از این‌کاربردها را درفصل۶ و در نیمهٔ دوم این‌کتاب خواهیم دید.

اینك، مطلب را با همنهشتی درجهٔ دوم کلی

$$ax^2+bx+c\equiv 0 \pmod p, \qquad (2)$$

که درآن p عددی اول است، شروع می‌کنیم. بی‌آنکه خللی به‌کلیت وارد آید، فرض می‌کنیم $p\nmid a$، زیرا اگر $p|a$، آنگاه همنهشتی(۲) باهمنهشتی‌خطی $bx+c\equiv 0 \pmod p$ معادل است، که می‌تواند به همان روشی که در فوق شرح داده شد مورد بحث قرار‌گیرد. اگر $p=2$، آنگاه (۲) بسادگی از راه آزمون وخطا حل می‌شود. این قضایا را به‌عنوان

تمرین می گذاریم. از این پس، فرض می کنیم $p \neq ۲$. (متأسفانه، بحثی که در زیرمی آید به ازای $p=۲$ معتبر نیست.) اکنون سعی می کنیم همنهشتی (۲) را با پیروی از روشی که درجبر دبیرستانی برای حل معادلات درجهٔ دوم متداول است، یعنی، از راه تبدیل آن به‌صورت مربع کامل ، حل کنیم. اینك روش حل معادلهٔ

$$ax^۲+bx+c=۰ ,$$

راکه درآن a ، b ، c اعدادی حقیقی هستند و $a\neq ۰$ ، یادآوری می کنیم. این معادله را به صورت زیر می‌نویسیم

$$ax^۲+bx+c=a\left(x^۲+\frac{b}{a}x+\frac{c}{a}\right)$$

$$.=a\left(\left(x+\frac{b}{۲a}\right)^۲+\frac{c}{a}-\frac{b^۲}{۴a^۲}\right)$$

بنابراین ، عبارت $ax^۲+bx+c$ فقط و فقط زمانی صفر می‌شود که داشته باشیم:

$$\left(x+\frac{b}{۲a}\right)^۲=\frac{b^۲}{۴a^۲}-\frac{c}{a}=\frac{b^۲-۴ac}{۴a^۲}$$

بنابراین ، برای یافتن x ، باید جذر $(b^۲-۴ac)/۴a^۲$ را به دست آوریم. برحسب جذر، x می‌تواند توسط دستور

$$x=\frac{-b\pm\sqrt{b^۲-۴ac}}{۲a}$$

داده شود. دستور اخیر همان به اصطلاح دستور حل معادلهٔ درجهٔ دوم جبر دبیرستانی است. از این دستور ، می بینیم که مشکل اصلی در حل معادلهٔ درجهٔ دوم استخراج ریشهٔ دوم $b^۲-۴ac$ است . اگر $b^۲-۴ac\geqslant ۰$ ، آنگاه یك عدد حقیقی نامنفی موجود است که مربعش $b^۲-۴ac$ می باشد، بنابراین می توانیم قرار دهیم $\alpha=\sqrt{b^۲-۴ac}$. ولی ، اگر $b^۲-۴ac<۰$ ، آنگاه هیچ عدد حقیقی α که مربعش $b^۲-۴ac$ باشد وجود ندارد. برای استخراج جذر $\sqrt{b^۲-۴ac}$ درحالت اخیر، لازم‌است از اعداد مختلط استفاده کنیم. ولی ، اگر $b^۲-۴ac<۰$ و اگر بخواهیم جوابها حقیقی باشند ، در این صورت معادلات اولیه جوابی ندارند. برای همنهشتیهای درجهٔ دوم ، وضع شبیه به معادلات درجهٔ دوم خواهد بود.

اینك به همنهشتی درجهٔ دوم

$$ax^۲+bx+c\equiv ۰ (p \text{ هنگ})$$

برمی گردیم، که درآن a ، b ، c اعدادی صحیح هستند و $p\nmid a$ و $p\neq ۲$. حال همان‌روش

حل معادلات درجهٔ دوم را اختیار می‌کنیم. اولین مرحله جدا کردن عامل a بود. بجای $1/a$، به عکس حسابی a به هنگ p، یعنی a^*، احتیاج داریم. چون $p \nmid a$، (قضیهٔ ۸.۲.۳) می‌توانیم چنین عکسی را بیابیم. در این صورت a^* خاصیت $aa^* \equiv 1 \ (\text{هنگ } p)$ را دارد، بنابراین

$$ax^2+bx+c \equiv_x a(x^2+a^*bx+a^*c)\ (\text{هنگ } p)\,. \tag{3}$$

مرحلهٔ بعدی به صورت مربع کامل درآوردن عبارت داخل پرانتز در (۳) است. برای انجام این امر، به عکس ۲ به هنگ p، یعنی 2^*، احتیاج داریم. چون $p \neq 2$، این عکس را می‌توانیم بیابیم. در حقیقت، می‌توانیم 2^* را مساوی $(p+1)/2$ بگیریم، زیرا $2\times 2^* = p+1 \equiv 1\ (\text{هنگ } p)$. در این صورت

$$x^2+a^*bx+a^*c \equiv_x (x+2^*a^*b)^2+(a^*c-2^{*2}a^{*2}b^2)\ (\text{هنگ } p)\,. \tag{4}$$

(بسط دهید و سپس مطابقت کنید.) بنابراین، چون $p \nmid a$، لم اقلیدس از فصل ۲ همراه با (۳) و (۴) ایجاب می‌کند که $ax^2+bx+c \equiv 0\ (\text{هنگ } p)$ اگر، وفقط اگر،

$$(x+2^*a^*b)^2 \equiv 2^{*2}a^{*2}b^2-a^*c\ (\text{هنگ } p)\,. \tag{5}$$

قرار می‌دهیم $y = x+2^*a^*b$، $d = 2^{*2}a^{*2}b^2-a^*c$. در این صورت می‌توانیم معادلهٔ اصلی را برحسب x حل کنیم اگر، وفقط اگر، بتوانیم همنهشتی

$$y^2 \equiv d\ (\text{هنگ } p)$$

را برحسب y حل کنیم.

مثال ۱: برای روشن ساختن روش فوق، همنهشتی

$$5x^2+9x+11 \equiv 0\ (\text{هنگ } 13) \tag{6}$$

را حل می‌کنیم. توجه داشته باشید که چون $8\times 5 \equiv 1\ (\text{هنگ } 13)$، عدد ۸ یک عکس ۵ به هنگ ۱۳ است؛ یعنی، می‌توانیم 5^* را مساوی ۸ اختیار کنیم. بنابراین (۶) معادل است با

$$8\times 5x^2+8\times 9x+8\times 11 \equiv 0\ (\text{هنگ } 13)$$

یا

$$x^2+7x+10 \equiv 0\ (\text{هنگ } 13)\,. \tag{7}$$

اما ۷ یک عکس ۲ به هنگ ۱۳ است، بنابراین (۷) معادل است با

$$(x+7\times 7)^2+10-(7\times 7)^2 \equiv 0\ (\text{هنگ } 13)$$

یا

$$(x+10)^2 \equiv -1\ (\text{هنگ } 13)\,.$$

قرارمی‌دهیم $y=x+10$ ، می‌بینیم که مسئلهٔ حل(۶) به‌حل

$$y^{2}\equiv -1\ (\text{هنگ } 13) \qquad (8)$$

بدل می‌شود. بنابراین احتیاج داریم ریشه‌های دوم ۱− به‌هنگ ۱۳ را ، درصورت وجود، بیابیم . می‌توانیم به روش آزمون و خطا متوسل شویم. (یا ملاحظه می‌کنیم که چون $13\equiv 1\ (\text{هنگ } 4)$ ، قضیهٔ ۵.۳.۳ ایجاب می‌کند که $6!=((13-1)/2)!$ دارای‌خاصیت $(6!)^{2}\equiv -1\ (\text{هنگ } 13)$ است). در هرحال، مشاهده می‌کنیم که $y\equiv \pm 5\ (\text{هنگ } 13)$ دو جواب (۸) هستند ، و بنابر نتیجهٔ ۹.۵.۳ ، (۸) حداکثر دو جواب دارد ، لذا $y\equiv \pm 5\ (\text{هنگ } 13)$ تنها جوابهای (۸) می‌باشند. بنابراین،

$$x=y-10\equiv -5 ,\ -2\ (\text{هنگ } 13)$$

جوابهای همنهشتی(۶) می‌باشند. زیرا

$$5(-5)^{2}+9(-5)+11=125-45+11=91\equiv 0\ (\text{هنگ } 13)\ .$$

متعلم می‌تواند بررسی کند که $x\equiv -2\ (\text{هنگ } 13)$ نیز یك جواب می‌باشد.

توجه داشته باشید که اگر به‌جای (۶) همنهشتی

$$5x^{2}+9x+9\equiv 0\ (\text{هنگ } 13)$$

را بگذاریم ، آنگاه هیچ جوابی نخواهیم داشت ، زیرا به جای (۸) همنهشتی

$$y^{2}\equiv 2\ (\text{هنگ } 13)$$

را خواهیم داشت که جوابی ندارد. (بیازمایید .)

نتیجهٔ مهم بحث ما این است که برای حل همنهشتی

$$ax^{2}+bx+c\equiv 0\ (\text{هنگ } p) ,\ p\nmid a ,\ p\neq 2$$

همواره کافی است یك همنهشتی از نوع

$$y^{2}\equiv d\ (\text{هنگ } p) \qquad (9)$$

را حل کنیم.

بقیهٔ این فصل به بحث در بارهٔ همنهشتی (۹) اختصاص خواهد یافت. نکته در این است که بحث دربارهٔ (۹) خیلی ساده‌تر از بحث دربارهٔ همنهشتی درجه دوم کلی است و ، بعلاوه، قانون تقابل مربعی روشی بسیار ساده واز لحاظ محاسبه روش پابرجایی است برای تعیین اینکه (۹) جواب دارد یا نه . ما بیان قانون تقابل مربعی را فعلا به‌تعویق می‌اندازیم، وبحث دربارهٔ تاریخچهٔ طولانی آن رانیز به‌بعد ازاینکه زمینهٔ اطلاعات خود را اندکی بیشتر وسعت بخشیدیم موکول می‌کنیم.

۱.۴ تمرینات

۱. هریك از همنهشتیهای زیر را به یك همنهشتی به صورت $x^{2}\equiv a$ (هنگ p) تبدیل کنید:

(آ) $2x^{2}+x+3\equiv 0$ (هنگ ۵) . (ب) $8x^{2}+5x+2\equiv 0$ (هنگ ۷) .

(ج) $4x^{2}+2\equiv 0$ (هنگ ۱۷) . (د) $14x^{2}+8x+7\equiv 0$ (هنگ ۲۳)

(ه) $3x^{2}+x+9\equiv 0$ (هنگ ۱۱) .

۲. قسمتهای (آ) تا (ه) تمرین ۱ را با استفاده از نتایج تمرین ۱ و آزمایش یك دستگاه کامل مانده‌ها حل کنید. (انتخاب مناسب دستگاه کامل مانده‌ها و رعایت چند نکته می‌تواند سنگینی بار محاسبه را به‌مقدار قابل ملاحظه‌ای سبك کند.)

۳. فرض کنیم n عدد صحیح مثبت فردی (که لزوماً اول نیست) باشد. نشان دهید که همنهشتی $ax^{2}+bx+c\equiv 0$ (هنگ n) می‌تواند به‌یك‌همنهشتی به‌صورت $x^{2}\equiv d$ (هنگ n) تبدیل شود مشروط بر آنکه $1 =$ بمعم$(a ، n)$.

۴. همنهشتیهای زیر را حل کنید:

(آ) $x^{2}\equiv 2$ (هنگ ۱۵) .

(ب) $3x^{2}+2x+5\equiv 0$ (هنگ ۲۲) .

۵. نشان‌دهید که همنهشتی درجهٔ سوم کلی $ax^{3}+bx^{2}+cx+d\equiv 0$ (هنگ p) می‌تواند به‌یك همنهشتی به‌صورت $x^{3}+rx+q\equiv 0$ (هنگ p) تبدیل شود مشروط براینکه $p\neq 3$ و $p\nmid a$.

۶. فرض کنیم a عددصحیح فردی‌باشد. کلیهٔ جوابهای‌همنهشتی $ax^{2}+bx+c\equiv 0$ (هنگ ۲) را به‌طورکامل تعیین کنید.

۲.۴ خواص بنیادی مانده‌های درجهٔ دوم

اینك مطالعهٔ همنهشتی

$$x^{2}\equiv a \text{ (هنگ } p) \qquad (1)$$

را ، که درآن p یك عدد اول فرد و a یك عدد صحیح می‌باشد آغاز می‌کنیم. همانگونه که در بخش ۱ دیده‌ایم ، کلیهٔ همنهشتیهای درجهٔ دوم به هنگ p می‌توانند به همنهشتی (۱) تبدیل شوند .

اگر $a\equiv 0$ (هنگ p) ، درآن‌صورت دیده‌ایم که $x\equiv 0$ (هنگ p) تنها جواب (۱) می‌باشد. بنابراین، ازاین به‌بعد فرض می‌کنیم $p\nmid a$. به‌ازای بعضی مقادیر a ، (۱)جوابی خواهد داشت، درحالی که به‌ازای بعضی مقادیردیگرa، (۱) جوابی ندارد. بگذارید مابین این دو قسم a تمایزی قایل شویم.

تعریف ۱ : فرض کنیم p عددی اول باشد، و فرض کنیم a عدد صحیح دلخواهی باشد به طوری که $p \nmid a$. گوییم a یك ماندهٔ درجهٔ دوم به هنگ p است به شرط آنکه همنهشتی

$$x^{2} \equiv a \ (p \text{ هنگ})$$

جوابی داشته باشد. در غیر این صورت گوییم a یك نامانده درجهٔ دوم به هنگ p است.

فرض کنیم p مفروض باشد. حال مسئلهٔ تعیین کلیهٔ ماندههای درجهٔ دوم به هنگ p را درنظر می‌گیریم. اگر a یك ماندهٔ درجهٔ دوم به‌هنگ p باشد، آنگاه $p \nmid a$ و به ازای مقداری مانند x داریم $a \equiv x^{2} (p \text{ هنگ})$. ولی، چون هر عدد صحیح با یکی از اعداد $۰ ، ۱ ، \ldots ، p-۱$ همنهشت به هنگ p است، می‌بینیم که a بایستی با یکی از اعداد

$$۱^{۲} , ۲^{۲} , \ldots , (p-۱)^{۲}$$

همنهشت به‌هنگ p باشد. اگر p زیاد بزرگ نباشد، آنگاه این‌روش واقعاً می‌تواند برای محاسبه به‌کار رود.

مثال ۲ : فرض کنیم $p=۱۳$. دراین صورت a فقط وفقط وقتی یك ماندهٔ درجهٔ دوم به هنگ ۱۳ است که بایکی ازاعداد $۱^{۲} ، ۲^{۲} ، \ldots ، ۱۲^{۲}$ همنهشت به هنگ ۱۳ باشد، یعنی a یك ماندهٔ درجهٔ دوم به‌هنگ ۱۳ است اگر ، و فقط اگر ،

$$a \equiv ۱ , ۴ , ۹ , ۳ , ۱۲ , ۱۰ , ۱۰ , ۱۲ , ۳ , ۹ \text{ و } ۴ , \text{ یا } ۱ \ (۱۳ \text{ هنگ})$$

بنابراین، ماندههای‌درجهٔ دوم به‌هنگ ۱۳ اعداد ۱ ، ۳ ، ۴ ، ۹ ، ۱۰ ، ۱۲ می‌باشند. پس، ناماندههای درجهٔ دوم به‌هنگ ۱۳ عبارت‌اند از ۲ ، ۵ ، ۶ ، ۷ ، ۸ ، ۱۱.

توجه داشته باشید که فهرست اولیهٔ ماندههای درجهٔ دوم در مثال ۲ را که به دست آوردیم متقارن است و هرعضو در فهرست دقیقاً دوبار ظاهر می‌شود. این یك پدیدهٔ کلی است. زیرا داریم $p-x \equiv -x (p \text{ هنگ})$ ، بنابراین $(p-x)^{۲} \equiv (-x)^{۲} (p \text{ هنگ})$ ، و بنابراین

$$(p-x)^{۲} \equiv x^{۲} (p \text{ هنگ}) . \qquad (۲)$$

پس ، اگر a یك ماندهٔ درجهٔ دوم به هنگ p باشد ، آنگاه بایکی ازاعداد

$$۱^{۲} , ۲^{۲} , \ldots , \left(\frac{p-۱}{۲}\right)^{۲}$$

همنهشت به هنگ p می‌باشد.

لم ۳ : فرض کنیم $p>۲$ عددی اول باشد و a یك ماندهٔ درجهٔ دوم به‌هنگ p ، $p \nmid a$. در این صورت همنهشتی $x^{۲} \equiv a (p \text{ هنگ})$ درست دارای دو جواب متمایز است.

برهان: بنابر نظریهٔ عمومی همنهشتیهای بسجمله‌ای ، همنهشتی $x^{۲} \equiv a (p \text{ هنگ})$ حداکثر

دو جواب دارد (نتیجهٔ ۹.۵.۳) . چون a یك مـانده‌ٔ درجهٔ دوم به هنگ p است ، عـددی مانند x_0 وجود دارد به‌طوری که(هنگ $x_0^2 \equiv a(p$. بعلاوه ، چون $p \nmid a$، داریم $p \nmid x_0$. اما (هنگ $x^2 \equiv a(p$ ، بنابراین $-x_0$ نیزیك‌جواب‌همنهشتی (هنگ $(-x_0)^2 \equiv x_0^2 \equiv a(p$ است. بعلاوه ، (هنگ $x_0 \not\equiv -x_0(p$ زیرا که $p > 2$ و $p \nmid x_0$. بنابراین، جوابهای x_0 و $-x_0$ متمایزند، پس حداقل دو جواب موجود است. ثابت‌کرده‌ایم که حداکثر دو جواب موجود است، بنابراین دقیقاً دو جواب متمایز وجود دارد. ■

در فوق ثابت‌کردیم که هرماندهٔ درجهٔ دوم به هنگ p ، با یکی از اعداد

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

همنهشت به هنگ p است. در واقع هیچ دو عددی از این اعداد نمی‌تـوانند همنهشت به هنگp باشند، زیرا اگربه‌ازای $1 \leqslant x_0 < y_0 \leqslant (p-1)/2$، (هنگ $x_0^2 \equiv y_0^2(p$، آنگاه همنهشتی(هنگ $x^2 \equiv a(p$ با این‌شرط که $a = y_0^2$ دارای‌جوابهای $x = x_0 , y_0 , p - x_0$ (معادلهٔ (۲)) است. بعلاوه، این‌جوابها متمایزند (تمرین). ولی ، بنابر لم ۳ ، این‌همنهشتی نمی‌تواند سه جواب متمایز داشته باشد . بنابراین (هنگ $x_0^2 \not\equiv y_0^2(p$ ، و هیچ دو عددی از اعداد صحیح

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

نمی‌تـوانند همنهشت به هنگ p باشند . به عنوان نتیجه‌ای از آنچه‌کـه هم اکنون ثابت کرده‌ایم ، توجه می‌کنیم که یك ماندهٔ درجهٔ دوم به هنگ p با یك وفقط یکی از اعداد

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

همنهشت است. اینك ملاحظات خود را دریك قضیه خلاصه می‌کنیم.

قضیهٔ ۴ : فرض‌کنیم p عدد اول فردی باشد، $p \nmid a$. دراین صورت a یك ماندهٔ درجهٔ دوم به هنگ p است اگر وفقط اگر a بایکی از اعداد

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \tag{۳}$$

همنهشت به‌هنگ p باشد، هیچ دوعددی از اعداد(۳) همنهشت به هنگ p نیستند. بنابراین درمیان اعداد صحیح ۱ ، ۲ ، ... ، $p-1$، دقیقاً $(p-1)/2$ ماندهٔ درجهٔ دوم به‌هنگp و دقیقاً $(p-1)/2$ نامانده‌ٔ درجهٔ دوم به‌هنگ p وجود خواهند داشت .

قرارداد علامتی زیر را خیلی مناسب می‌دانیم:

تعریف ۵: فرض کنیم p عدد اول فردی باشد و a عددی صحیح به طوری‌که $p \nmid a$ [1] . حال نماد لژاندر $\left(\frac{a}{p}\right)$ را به صورت زیر تعریف می کنیم:

$$\left(\frac{a}{p}\right)=\begin{cases} +1 & \text{هر گاه } a \text{ ماندهٔ درجهٔ دومی به هنگ } p \text{ باشد ،} \\ -1 & \text{هر گاه } a \text{ ناماندهٔ درجهٔ دومی به‌هنگ } p \text{ باشد .} \end{cases}$$

متعلم نبایستی نماد $\left(\frac{a}{p}\right)$ را با کسر $\frac{a}{p}$ اشتباه کند. از محاسبات فوق برای مانده‌های درجهٔ دوم به هنگ ۱۳ (مثال ۲) می بینیم که

$$\left(\frac{۲}{۱۳}\right)=-۱ \ , \ \left(\frac{۳}{۱۳}\right)=۱, \left(\frac{۴}{۱۳}\right)=۱, \left(\frac{۵}{۱۳}\right)=-۱ \ .$$

بعلاوه ، چون (هنگ ۱۳)$۵\equiv۱۸$ و ۵ یك ناماندهٔ درجهٔ دوم به هنگ ۱۳ می باشد ، ۱۸ نیز یك ناماندهٔ درجهٔ دوم به هنگ ۱۳ بوده ، وبنابراین داریم

$$\left(\frac{۱۸}{۱۳}\right)=-۱$$

نماد لژاندر ابتدا توسط لژاندر ریاضیدان فرانسوی درسدهٔ هیجدهم برای تسهیل محاسبات با مانده‌های درجهٔ دوم معرفی شده بود. در واقع ، قانون تقابل مربعی را برحسب خواص نماد لژاندر بیان خواهیم کرد. ابتدا بعضی خواص مقدماتی نماد لژاندر را ثابت می کنیم.

قضیهٔ ۶ : فرض کنیم p عدد اول فردی باشد و a ، b اعدادی صحیح به‌طوری که $p\nmid a$ و $p\nmid b$. در این صورت نتایج زیر برقرارند:

(یکم) $\left(\frac{a^۲}{p}\right)=۱$.

(دوم) $\left(\frac{۱}{p}\right)=۱$.

(سوم) اگر $a\equiv b$ (هنگ p)، آنگاه $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

---

۱. گاهی از اوقات $\left(\frac{a}{p}\right)$ را به ازای a هایی که $p|a$ ، صفر تعریف می‌کنند. توجه‌کنیدکه دراین حالت شرط $p\nmid a$ در قضیهٔ ۷ زائد می‌باشد (مترجم) .

برهان :

(یکم) همنهشتی (هنگ p)$x^{2} \equiv a^{2}$ جوابی به صورت $x = a$ دارد.

(دوم) در نتیجهٔ (یکم) قرار دهید ۱ $= a$.

(سوم) اگر (هنگ p)$a \equiv b$ ، آنگاه جوابهای (هنگ p)$x^{2} \equiv a$ همان جوابهای (هنگ p)$x^{2} \equiv b$ هستند. بنابراین اولین همنهشتی وقتی وفقط وقتی دارای جواب است که دومی جواب‌داشته باشد. پس، $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. ■

خواص نماد لژاندر که در قضیهٔ ۶ آورده شدند، خیلی مقدماتی هستند. ولـی، یك خاصیت این نماد که به هیچ وجه بدیهی نیست، نتیجهٔ زیر می‌باشد:

قضیهٔ ۷ (محك اویلر): فرض کنیم p عدد اول فردی باشد و a عددی صحیح به‌طوری که $p \nmid a$. آنگاه

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} .$$

برهان: بنا بر قضیهٔ کوچك فرما (قضیهٔ ۱.۳.۳)، داریم (هنگ p) ۱ $\equiv a^{p-1} = (a^{(p-1)/2})^{2}$.
بنابراین ، اگر $h = a^{(p-1)/2}$ ، آنگاه (هنگ p) ۱ $\equiv h^{2}$ ، ولذا $p|(h-1)(h+1)$.
پس، $p|h-1$ یا $p|h+1$ ، و بنابراین (هنگ p) ۱ $\pm \equiv h = a^{(p-1)/2}$. اما ، p ، فرد است، و بنابراین ، قضیهٔ ۱۴.۶.۲ ایجاب می‌کند که $\left(\frac{a}{p}\right) = +1$ اگـر ، و فقط اگـر ،

$$a^{(p-1)/2} \equiv 1 \pmod{p} .$$

در نتیجه ، $\left(\frac{a}{p}\right) = \pm 1$ اگر ، و فقط اگر ، بترتیب

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p} .$$ ■

قضیهٔ ۷ از لئونهارد اویلر ریاضیدان سویسی می‌باشد، که آن را درسال ۱۷۵۵ میلادی ثابت کرده است. محك اویلر یك تدبیر فنی بینهایت مفید در اثبات خواص گوناگون نماد لژاندر خواهد بود. ولی ، محك اویلر خیلی کار دارد تا به‌جایی برسد که به عنوان یك‌وسیلهٔ آزمون ساده برای حلپذیری همنهشتی (هنگ p)$x^{2} \equiv a$ به‌کار رود، زیرا بـرای استفاده از محك اویلر به محاسبهٔ (هنگ p)$a^{(p-1)/2}$ نیاز داریم تـا بتوانیم $\left(\frac{a}{p}\right)$ را تعیین کنیم . ولی حال‌دو نتیجهٔ سادهٔ محك اویلر را اثبات می‌کنیم که برای نشان‌دادن مفید بودن آن کفایت خواهند کرد.

نتیجهٔ ۸ : فرض کنیم p عدد اول فردی باشد، و a و b اعدادی صحیح به طوری که $p \nmid a$ و $p \nmid b$. دراین صورت

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

برهان: بنابر محك اویلر

$$\left(\frac{ab}{p}\right)\equiv(ab)^{(p-1)/2}=a^{(p-1)/2}b^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(p \text{ هنگ}).$$

چون اعداد $\left(\frac{ab}{p}\right)$ و $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ می‌توانند فقط مساوی ۱ یا ۱ — باشند و چون همنهشت به هنگ p با شرط $p>2$ می‌باشند، می‌بینیم که

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

و این همان نتیجهٔ مطلوب است.

■

یك نتیجهٔ مستقیم نتیجهٔ ۸ آن است که (یکم) حاصلضرب دو ماندهٔ درجهٔ دوم به هنگ p یك ماندهٔ درجهٔ دوم به هنگ p است، (دوم) حاصلضرب دو ناماندهٔ درجهٔ دوم به هنگ p یك ماندهٔ درجهٔ دوم به هنگ p است، و (سوم) حاصلضرب یك ماندهٔ درجهٔ دوم در یك ناماندهٔ درجهٔ دوم نامانده‌ای است درجهٔ دوم[1]. این نتایج در مرحلهٔ اول شگفت‌آورند و در عین حال خیلی سودمند می‌باشند. این حقایق را با یك مثال عددی به هنگ ۱۳ بررسی می‌کنیم (به مثال ۲ رجوع کنید.) بنابر محاسبات قبلی ۳ و ۱۲ مانده‌های درجهٔ دوم به‌هنگ ۱۳ می‌باشند، و در واقع $3\times 12=36\equiv 6^2$ (هنگ ۱۳) یك ماندهٔ درجهٔ دوم است. ولی ۲ و ۵ نامانده‌های درجهٔ دوم هستند، و $2\times 5=10\equiv 6^2$ (هنگ ۱۳) یك ماندهٔ درجهٔ دوم است. بالاخره، ۷ یك نامانده و ۱۰ یك‌مانده است، و $7\times 10=70\equiv 5$ (هنگ ۱۳) هم یك نامانده است.

یك نتیجهٔ دیگر محك اویلر قضیه‌ای است که در فصل ۳ ثابت کردیم، هرچند که در آنجا آن را برحسب مانده‌های درجهٔ دوم یا نمادهای لژاندر بیان نکردیم. یعنی، قضیهٔ زیر را داریم:

نتیجهٔ ۹: فرض کنیم p عدد اول فردی باشد. در این صورت

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}.$$

به عبارت دیگر،

---

۱. توجه داشته باشید که (یکم) و (سوم) مستقیماً بسادگی ثابت می‌شوند. ولی (دوم) از تمامی قدرت نتیجهٔ ۸ استفاده می‌کند.

$$\left(\frac{-۱}{p}\right)=\begin{cases} +۱ & p\equiv ۱ \text{ (هنگ ۴)، هرگاه} \\ -۱ & p\equiv ۳ \text{ (هنگ ۴). هرگاه} \end{cases}$$

برهان: بنا بر محک اویلر،

$$\left(\frac{-۱}{p}\right)\equiv(-۱)^{(p-۱)/۲}\ (\text{هنگ } p)\ .$$

بنا براین، چون $\pm ۱ = \left(\frac{-۱}{p}\right)$ وچون $p>۲$ ، نتیجهٔ مطلوب حاصل است. ■

توجه‌داشته باشید که نتیجهٔ ۹ با قضیهٔ ۵.۳.۳ معادل‌است. فرما، در اوایل قرن هفدهم برنتیجهٔ ۹ واقف‌بود. ولی اول‌بار اویلر آن را درسال ۱۷۴۹ میلادی به‌دشواری اثبات کرد. چون‌اویلر محک‌سادهٔ خودش را تا ۱۷۵۵ میلادی کشف نکرده‌بود، مجبور بود روشهای‌دیگری جهت اثبات نتیجهٔ ۹ طرح کند. این روشها، روشهای خیلی دشواری بودنـد. در ۱۷۷۳ میلادی بود که لاگرانژ متوجه شد که می‌توان آشکارا ریشهٔ درجهٔ دوم ۱ — به هنگ p ، را با استفاده از قضیهٔ ویلسن به ازای $p\equiv ۱$ (هنگ ۴)، به صورت $((p-۱)/۲)!$ نوشت. بنابراین، برهانی که قبلا برای نتیجهٔ ۹ آوردیم از آن لاگرانژ است.

اینک این بخش را باذکر چند مثال از خواص نماد لژاندرکه ثابت‌کرده‌ایم همچنین با چند تذکر به پایان می‌بریم.

مثال ۱۰: بنابر قضیهٔ ۶، قسمت (یکم)، نتیجهٔ ۸، و نتیجهٔ ۹، داریم

$$\left(\frac{-a^۲}{p}\right)=\left(\frac{-۱}{p}\right)\left(\frac{a^۲}{p}\right)=\left(\frac{-۱}{p}\right)=(-۱)^{(p-۱)/۲}\ .$$

بنابراین، همنهشتی $x^۲\equiv -a^۲$ (هنگ p) حلپذیراست اگر، وفقط اگر، $p\equiv ۱$ (هنگ ۴).

مثال ۱۱. آیا می‌توانیم همنهشتی $x^۲\equiv ۱۹$ (هنگ ۲۳) را حل کنیم؟ چون $۱۹\equiv -۴$ (هنگ ۲۳)، داریم

$$\left(\frac{۱۹}{۲۳}\right)=\left(\frac{-۴}{۲۳}\right)=\left(\frac{-۱}{۲۳}\right)\left(\frac{۲}{۲۳}\right)^۲=-۱$$

زیرا $۲۳\equiv ۳$ (هنگ ۴). بنابراین، $x^۲\equiv ۱۹$ (هنگ ۲۳) حلپذیر نیست.

مثال ۱۲: چگونه $\left(\frac{a}{p}\right)$ را به ازای $p\nmid a$ حساب کنیم؟ فرض کنیم $a=\pm p_۱^{a_۱}\cdots p_t^{a_t}$ که‌درآن $p_۱$ ، ... ، p_t اعداداول متمایزند. چون $p\nmid a$ ، می‌بینیم که $p\neq p_i$. دراین‌صورت،

بنابر نتیجهٔ ۷ ، داریم

$$\left(\frac{a}{p}\right)=\left(\frac{\pm ۱}{p}\right)\left(\frac{p_۱}{p}\right)^{a_۱}\cdots\left(\frac{p_t}{p}\right)^{a_t}. \qquad (۴)$$

از این قرار ، به عنوان مثال ، اگر $p=۵$ ، و $a=-۲۴$ ، آنگاه

$$\left(\frac{-۲۴}{۵}\right)=\left(\frac{-۱}{۵}\right)\left(\frac{۲}{۵}\right)^{۳}\left(\frac{۳}{۵}\right)=۱(-۱)^{۳}(-۱)=۱.$$

مطلب اساسی در نمایش (۴) این است که این تساوی نشان می‌دهد که برای محاسبهٔ $\left(\frac{a}{p}\right)$ کافی است بتوانیم $\left(\frac{q}{p}\right)$ را که در آن p و q اعداد اول متمایزند حساب کنیم. این دقیقاً همان کاری است که قانون تقابل مربعی اجازهٔ انجام آن را به ما می‌دهد.

۲.۴ تمرینات

۱. نشان دهید که همنهشتی $x^{۲}\equiv ۰$ (هنگ p) فقط یک جواب به هنگ p دارد.

۲. کلیهٔ مانده‌های درجهٔ دوم و نامانده‌های درجهٔ دوم به هنگ p را به ازای

(آ) $p=۵$ ، (ب) $p=۷$ ، (ج) $p=۱۱$ ، (د) $p=۱۷$ ،

تعیین کنید.

۳. مقادیر زیر را محاسبه کنید:

(آ) $\left(\frac{۲}{۳}\right)$. (ب) $\left(\frac{۷}{۵}\right)$. (ج) $\left(\frac{۱۱}{۷}\right)$. (د) $\left(\frac{۹}{۱۷}\right)$.

(ه) $\left(\frac{-۱}{۱۱}\right)$. (و) $\left(\frac{۲}{۱۷}\right)$. (ز) $\left(\frac{۲}{۱۱}\right)$. (ح) $\left(\frac{۱۶}{۱۱}\right)$.

۴. از نتایج تمرین ۲ برای تحقیق صحت تساوی‌های زیر استفاده کنید.

(آ) $\left(\frac{۲}{۵}\right)\left(\frac{۳}{۵}\right)=\left(\frac{۶}{۵}\right)$.

(ب) $\left(\frac{۷}{۱۷}\right)\left(\frac{۵}{۱۷}\right)=\left(\frac{۳۵}{۱۷}\right)$.

۵. با محاسبهٔ عددی ، درستی همنهشتی زیر را بررسی کنید

$$\left(\frac{۶}{۱۷}\right)\equiv ۶^{(۱۷-۱)/۲} \quad (\text{هنگ } ۱۷).$$

۶. ثابت کنید که یک ریشهٔ اولیه به هنگ p نمی‌تواند یک ماندهٔ درجهٔ دوم به هنگ p باشد.

۷. با استفاده ازوجود یك ریشهٔ اولیه به هنگ p، نشان دهید که همنهشتی $x^۲ \equiv a$ (هنگ p) $(p \nmid a)$ یا دو جواب دارد و یا جوابی ندارد.

۸. همنهشتی $x^۲ \equiv ۳۸$ (هنگ ۴۷) را حل کنید. (راهنمایی: $۳۸ \equiv -۹$ (هنگ ۴۷))

۹. فرض کنیم n عدد صحیح مثبتی باشد و $n = m^۲k$، به‌طوری که k برهیچ مربع کاملی بخشپذیر نیست[1]. (k قسمت خالی از مربع n نامیده می‌شود.) نشان‌دهید که اگر $p \nmid n$، آنگاه $p \nmid k$ و

$$\left(\frac{n}{p}\right) = \left(\frac{k}{p}\right).$$

۱۰. فرض کنیم p عدد اول فردی باشد. مانده‌های درجهٔ دوم و نامانده‌های درجهٔ دوم به هنگ p^a را به روش معمول تعریف کنید. نشان دهید که حاصلضرب دو ماندهٔ درجهٔ دوم به هنگ p^a یك ماندهٔ درجهٔ دوم است، حاصلضرب دو ناماندهٔ درجهٔ دوم یك ماندهٔ درجهٔ دوم است، و حاصلضرب یك ماندهٔ درجهٔ دوم در یك ناماندهٔ درجهٔ دوم یك ناماندهٔ درجهٔ دوم است. (راهنمایی: بنا بر تمرین ۲۳.۶.۳ یك ریشهٔ اولیه به هنگ p^a وجود دارد.)

۱۱. نشان دهید که نتایج تمرین ۱۰، اگر به جای p^a یك عدد صحیح دلخواه n گذاشته شود، لزوماً برقرار نمی‌باشد. (راهنمایی: هنگ ۱۵ را در نظر بگیرید.)

۱۲. نشان‌دهید که مجموع مانده‌های درجهٔ دوم، به‌هنگ p، به‌ازای $p > ۳$، بر p بخشپذیر است.

۱۳. نشان دهید که

$$\left(\frac{۱}{p}\right) + \left(\frac{۲}{p}\right) + \cdots + \left(\frac{p-۱}{p}\right) = ۰.$$

۱۴. با استفاده از محك اویلر، قسمت (سوم) قضیهٔ ۶ را ثابت کنید.

برای تمرینات ۱۵ و ۱۶ به نکات زیر توجه کنید[2]: فرض کنیم p عدد اول فردی باشد. نشان دادیم که $(p-۱)/۲$ ناماندهٔ درجهٔ دوم به هنگ p، و $\varphi(p-۱)$ ریشهٔ اولیه بین ۰ و $p-۱$ وجود دارند. همچنین، بنا بر تمرین ۶، هر ریشهٔ اولیه یك ناماندهٔ درجهٔ دوم است.

۱۵. (آ) فرض کنیم $p = ۲q + ۱$، و q عددی اول باشد. دراین صورت q ناماندهٔ درجهٔ دوم و $q - ۱$ ریشهٔ اولیه موجودند. بنابراین، ریشه‌های اولیه دقیقاً نامانده‌های درجهٔ

---

۱. باستثنای ۱ (مترجم).

۲. مؤلفین از دکتر جان همپرلی John Hemperly که این تمرینات را خاطرنشان کرده‌اند تشکر می‌کنند.

دوم می‌باشند با یك استثنا. نشان دهید که آن استثنا (هنگ p) $2q \equiv -1$ می‌باشد.

(ب) ازقسمت (آ) برای‌محاسبهٔ ریشه‌های اولیه به هنگ ۷ ، ۱۱ ، ۲۳ ، ۴۷ استفاده کنید.

۱۶. فرض کنیم p عدداول فردی باشد. نشان دهید که تعداد مانده‌های درجهٔ دوم به‌هنگ p^n (یعنی، اعـداد صحیح a که برای آنها همنهشتی (هنگ p^n) $x^2 \equiv a$ حلپذیراست) برابر است با

$$\frac{p^{n+1}-p}{2(p+1)}+1 \quad n \text{ زوج،}$$

$$\frac{p^{n+1}-1}{2(p+1)}+1 \quad n \text{ فرد.}$$

۳.۴ لم گاوس

اینك محکی برای اینکه یك عدد صحیح مفروض a یك ماندهٔ درجـهٔ دوم به هنگ p باشد را ثابت می کنیم. محکی که اثبات خواهیم کرد محکی است تاحدی فوق‌العاده ومتعلق به‌گاوس . این لم ، در ابتدا خیلی عجیب به نظر خواهد آمد. در واقع ، ده سال طول کشید تا گاوس این خاصیت مانده‌های درجهٔ دوم را کشف کرد . درستی آن به هیچ وجه بـدیهی نیست. ولی ، نه‌فقط صحیح است، بلکه مفتاحی برای یك برهان مقدماتی و نسبتاً ساده‌برای قانون تقابل مربعی است. اینك بیان محك گاوس.

قضیهٔ ۱ (لم گاوس): فرض کنیم p یك‌عدد اول‌فرد و a عدد صحیحی باشدبه‌طوری که $p \nmid a$. اعداد صحیح a ، $2a$ ، $3a$ ، ... ، $((p-1)/2)a$ رادرنظر می گیریم. به‌جای هریك ازاین اعداد عددی همنهشت با آن به هنگ p بگذارید که بین $-(p-1)/2$ و $(p-1)/2$ قـرار داشته باشد. فرض کنیم تعداد اعـداد صحیح منفی در اعداد حاصل ν باشد. دراین صورت

$$\left(\frac{a}{p}\right)=(-1)^{\nu}.$$

پیش از اینکه به این برهان ساده بپردازیم ، مثالی را در نظرمی گیریم.

مثال ۲ : مجدداً $p=13$ رادرنظرمی گیریم،بنابراین $(p-1)/2=6$. فرض کنیم $a=5$ دراین صورت اعداد

۵ ، ۱۰ ، ۱۵ ، ۲۰ ، ۲۵ ، ۳۰

را در نظر می‌گیریم. با کم کردن مضرب مناسبی از ۱۳ از هریك از این اعداد، ترتیبی می‌دهیم که کلیهٔ مانده‌ها بین ۶− و ۶ قرار گیرند و سپس به جای اعداد فوق اعداد زیر را می‌گذاریم

۵ ، −۳ ، ۲ ، −۶ ، −۱ ، ۴.

دراین‌صورت $\left(\frac{۵}{۱۳}\right)=(-۱)^{۳}=-۱$ و $\nu=۳$. اگر $a=۳$ ، آنگاه به اعداد

۳ ، ۶ ، ۹ ، ۱۲ ، ۱۵ ، ۱۸

که به جای اعداد

۳ ، ۶ ، −۴ ، −۱ ، ۲ ، ۵

گذاشته‌شده‌اند می‌نگریم. بنابراین $\nu=۲$ و $\left(\frac{۳}{۱۳}\right)=(-۱)^{۲}=۱$. این نتایج باآنچه که درمثال ۲.۲ مشاهده کردیم مطابقت دارند.

برهان قضیهٔ ۱ : ابتدا ملاحظه‌می کنیم که اگر $۱\leqslant k , k'\leqslant (p-۱)/۲$ و $k\not\equiv k'$، آنگاه

$$ka\not\equiv k'a(p\ \text{هنگ})$$

و

$$ka\not\equiv -k'a(p\ \text{هنگ}) .$$

زیرا، اگر $ka\equiv k'a(p\ \text{هنگ})$ ، آنگاه $k\equiv k'(p\ \text{هنگ})$. اما، چون $۱\leqslant k$و$k'\leqslant (p-۱)/۲$ ، پس $k=k'$ که یك تناقض است. از طرف دیگر، اگر $ka\equiv -k'a(p\ \text{هنگ})$، آنگاه $k+k'\equiv ۰(p\ \text{هنگ})$. ولی چون $۱\leqslant k, k'\leqslant (p-۱)/۲$، داریم $۱\leqslant k+k'<p$ ، بنابراین $k+k'\not\equiv ۰(p\ \text{هنگ})$.

به‌ازای هر k که $۱\leqslant k\leqslant (p-۱)/۲$، فرض کنیم r_k جانشین $ka(p\ \text{هنگ})$ باشد. یعنی، r_k را طوری انتخاب می کنیم که

$$-\frac{p-۱}{۲}\leqslant r_k\leqslant \frac{p-۱}{۲} ,$$

$$r_k\equiv ka(p\ \text{هنگ}) .$$

دراین صورت اعدادی که به جای اعدادلم گاوس گذارده می‌شوند درست

$$r_{۱} , r_{۲} , \ldots , r_{(p-۱)/۲} \qquad (*)$$

هستند. فرض کنیم $k\neq k'$ ، به استناد استدلالی که در فوق کردیم، داریم

(هنگ p) $r_k \not\equiv r_{k'}$ و (هنگ p) $r_k \not\equiv -r_{k'}$، بنابراین $r_k \neq \pm r_{k'}$. به‌عبارت دیگر $|r_k| \neq |r_{k'}|$. چون تعداد $(p-۱)/۲$ عدد

$$|r_۱|, \ldots, |r_{(p-۱)/۲}|$$

موجودند که بین ۱ و $(p-۱)/۲$ قرار دارند وتمام آنها متمایزند، پس باید به‌ترتیبی متشکل از اعداد ۱، ۲، ...، $(p-۱)/۲$ باشند. بنابراین، چون درفهرست اعداد (*)، ν درایهٔ منفی قرار دارد، داریم

$$r_۱ r_۲ \cdots r_{(p-۱)/۲} = (-۱)^{\nu} ۱ \times ۲ \times \cdots \times \frac{(p-۱)}{۲}. \qquad (۱)$$

از طرف دیگر، چون (هنگ p) $r_k \equiv ka$، داریم

$$r_۱ \cdots r_{(p-۱)/۲} \equiv a(۲a) \cdots \left(\frac{p-۱}{۲}a\right) \qquad (۲)$$

$$\equiv a^{(p-۱)/۲} ۱ \times ۲ \times \cdots \times \frac{p-۱}{۲} \ (p \text{ هنگ}).$$

از مقایسهٔ (۱) و (۲)، داریم

$$(-۱)^{\nu} \times ۱ \times ۲ \cdots \frac{(p-۱)}{۲} \equiv a^{(p-۱)/۲} \times ۱ \times ۲ \times \cdots \times \frac{p-۱}{۲} \ (p \text{ هنگ}),$$

لذا، پس از حذف عامل $۱ \times ۲ \times \cdots \times (p-۱)/۲$، داریم

$$a^{(p-۱)/۲} \equiv (-۱)^{\nu} \ (p \text{ هنگ}). \qquad (۳)$$

حال بنابر محک اویلر (قضیهٔ ۷.۲) و (۳) می‌بینیم که

$$\left(\frac{a}{p}\right) \equiv (-۱)^{\nu} \ (p \text{ هنگ}).$$

بنابراین، چون $p > ۲$،

$$\left(\frac{a}{p}\right) = (-۱)^{\nu}. \qquad \blacksquare$$

اینک مثالهایی ارائه می‌دهیم تا نشان دهیم چگونه لم گاوس می‌تواند بـرای محاسبهٔ $\left(\frac{a}{p}\right)$ به‌کار برده شود.

مثال ۳: با یک مثال ساده شروع می‌کنیم. از لم گاوس استفاده می‌کنیم تا (برای بارسوم) نشان دهیم که

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}.$$

در اینجا $a=-1$ ، اعداد زیر را در نظر می گیریم

$$1(-1),\ 2(-1),\ \ldots,\ \frac{p-1}{2}(-1)$$

کلیهٔ این اعداد منفی هستند و بین $-(p-1)/2$ و $(p-1)/2$ قرار دارند . بنابراین $\nu=(p-1)/2$ ، همانگونه که انتظار داشتیم .

مثال ۴ : اینك به مثال $\left(\frac{2}{p}\right)$ ، که ازبداهت کمتری برخوردار است، می‌پردازیم . دراینجا $a=2$ ، و اعداد زیر را در نظر می گیریم

$$1\times 2,\ 2\times 2,\ 3\times 2,\ \ldots,\ \frac{p-1}{2}\times 2.$$

کلیهٔ این اعداد بین ۱ و p قرار دارند. بعلاوه ، روشن است آنهایی که پس از جایگزینی منفی می‌شوند ، بین $p/2$ و p قرار دارند. (اگر متوجه این نکته نمی‌شوید ، محاسبات واضح را به‌ازای $p=13,\ 17$ انجام دهید.) بنابراین، ν تعداد اعداد صحیح k است که

$$\frac{p}{2}\leqslant 2k\leqslant p,$$

یا با عبارت معادل آن

$$\frac{p}{4}\leqslant k\leqslant\frac{p}{2}.$$

p را مساوی $8m+r$ می گیریم ، که $0\leqslant r<8$. چون p فرد است ، بایــد داشته باشیم $r=1,\ 3,\ 5$ یا ۷ . بنابراین، باید تعداد اعداد صحیح k را که

$$2m+\frac{r}{4}\leqslant k\leqslant 4m+\frac{r}{2}$$

بشماریم. ما فقط چهار حالت ممکن را بـرای r بررسی می کنیم. وقتی $r=1$ ، می‌خواهیم k هایی را بشماریم که

$$2m+\frac{1}{4}\leqslant k\leqslant 4m+\frac{1}{2},$$

و این اعداد صحیح عبارت‌اند از $2m+1$ ، $2m+2$ ، ... ، $4m$. بنابراین تعداد آنها $2m$ است و داریم $\nu=2m$. بالاخص، می بینیم که وقتی $p\equiv 1$ (هنگ ۸)، آنگاه $\nu=2m$ زوج است، وبنابراین

$$\left(\frac{۲}{p}\right)=(-۱)^{\nu}=(-۱)^{۲m}=۱.$$

اگر $r=۳$، آنگاه حوزهٔ مقادیر k عبارت است از

$$۲m+\frac{۳}{۴}\leqslant k\leqslant ۴m+\frac{۳}{۲},$$

و بنا براین مقادیر مربوطه برای k عبارت انداز $۲m+۱$، ...، $۴m$، $۴m+۱$. پس، $\nu=۲m+۱$ فرد است، و $\left(\frac{۲}{p}\right)=(-۱)^{\nu}=-۱$. به ازای $r=۵$، حوزهٔ مقادیر k عبارت است از

$$۲m+\frac{۵}{۴}\leqslant k\leqslant ۴m+\frac{۵}{۲},$$

که $k=۲m+۲$ ، ... ، $۴m+۲$ را می‌دهد، و بنابراین $\nu=۲m+۱$. پس اگر $p\equiv ۵$ (هنگ ۸)، آنگاه $\left(\frac{۲}{p}\right)=(-۱)^{۲m+۱}=-۱$. بالاخره، $r=۷$ نتیجه می‌دهد $۲m+۷/۴\leqslant k\leqslant ۴m+۷/۲$ یا $k=۲m+۲$ ، ... ، $۴m+۲$ ، $۴m+۳$ ، یا $\nu=۲m+۲$.

بنابراین، $p\equiv ۷$ (هنگ ۸) ایجاب می‌کند که $\left(\frac{۲}{p}\right)=۱$. بنابراین، مقادیر $\left(\frac{۲}{p}\right)$ را به‌ازای کلیهٔ اعداد اول فرد p کاملا تعیین کرده‌ایم. اینك نتایج خود را در یك قضیهٔ مجزا خلاصه می‌کنیم، زیرا نتیجهٔ قبلی‌ما معمولا به‌صورت قسمتی ازقانون تقابل‌مربعی بیان می‌شود ولی‌از استدلالی که در بخش ۴ می‌شود پیروی نخواهد کرد.

قضیهٔ ۵ : فرض‌کنیم p عدد اول فردی باشد. دراین صورت

$\left(\frac{۲}{p}\right)=+۱$ اگر، و فقط اگر، $p\equiv\pm۱$ (هنگ ۸)،

$\left(\frac{۲}{p}\right)=-۱$ اگر، و فقط اگر، $p\equiv\pm۵$ (هنگ ۸)،

از این‌رو، به عنوان مثال، $\left(\frac{۲}{۱۳}\right)=-۱$ و $\left(\frac{۲}{۱۷}\right)=۱$ همچنانکه $۱۳\equiv ۵$ (هنگ ۸) و $۱۷\equiv ۱$ (هنگ ۸).

اگر $p\equiv\pm۱$ (هنگ ۸)، آنگاه $(p^{۲}-۱)/۸$ زوج است، در حالی که اگر $p\equiv\pm۵$ (هنگ ۸)، آنگاه $(p^{۲}-۱)/۸$ فرد است. بنابراین، قضیهٔ ۵ می‌تواند دوباره به صورت زیر نوشته شود:

نتیجهٔ ۶: فرض‌کنیم p عدد اول فردی باشد. دراین صورت

$$\left(\frac{۲}{p}\right)=(-۱)^{(p^۲-۱)/۸}$$

هدف خاص این فصل این است که محکی برای تعیین حلپذیری همنهشتی $x^۲\equiv a$ (هنگ p) به‌دست‌آوریم. وچنین‌محکی درست‌برابر تعیین روشی برای محاسبهٔ نماد $\left(\frac{a}{p}\right)$ لژاندر است. ما درضمن دو مثال تقریباً مفصل نشان خواهیم داد که لم‌گاوس چنین روشی را در اختیار ما می‌گذارد. این مثالها ارزشمند هستند ولو اینکه قانون تقابل مربعی ارزش‌آنها را بپوشاند، زیرا لم‌گاوس جزء قاطعی برای اثبات آن قانون است. امیدواریم که این مثالها بینش بیشتری از طرز رفتار نماد لژاندر به ما بدهند.

مثال ۷ : فرض‌کنیم $a=۳$ و p عدد اول فردی باشد به طوری‌که $p\nmid a$. در این صورت p بایدبزرگتر از ۳ باشد. $\left(\frac{۳}{p}\right)$ را تعیین خواهیم‌کرد. در مثال ۴ دیدیم (به ازای $a=۲$) که مقدار $\left(\frac{۲}{p}\right)$ به دستهٔ مانده‌های p به هنگ ۸ بستگی دارد. همچنین مقدار $\left(\frac{۳}{p}\right)$ به دستهٔ مانده‌های p به هنگ $۴a(=۱۲)$ بستگی دارد. در لم‌گاوس ما به فهرست

$$۱\times۳ ، ۲\times۳ ، ۳\times۳ ، \ldots ، \frac{p-۱}{۲}\times۳.$$

نگاه می‌کنیم. کلیهٔ اعداد بین ۱ و $۳p/۲$ قرار دارند. واضح است‌که پس از جایگزینی، به جای اعداد صحیح بین ۱ و $p/۲$ اعداد صحیح مثبت، وبجای اعدادبین $p/۲$ و p اعداد صحیح منفی وبه‌جای‌اعدادبین p و $۳p/۲$ اعداد صحیح مثبت‌گذاشته خواهندشد. بنابراین، ν برابر است با تعداد اعداد صحیح k به طوری‌که

$$\frac{p}{۲}\leqslant ۳k\leqslant p$$

یا

$$\frac{p}{۶}\leqslant k\leqslant\frac{p}{۳}$$

می‌نویسیم $p=۱۲m+r$ که درآن[۱] $r=۱ ، ۵ ، ۷ ،$ یا ۱۱. دراین‌صورت ν تعداد اعداد صحیح k است به طوری‌که

$$۲m+\frac{r}{۶}\leqslant k\leqslant ۴m+\frac{r}{۳}\cdot$$

---

۱. اگر $r=۰ ، ۲، ۳ ، ۴ ، ۶ ، ۸، ۹ ، ۱۰$ ، آنگاه به‌ازای $m\geqslant ۱$ ، $p=۱۲m+r$ اول نخواهد بود، و به ازای $m=۰$ فقط می‌تواند به‌ازای $r=۳$ اول باشد، ولی $p=۳$ مستثنا شده‌است.

اگر مقادیر $r = ۱ ، ۵ ، ۷ ، ۱۱$ را به طور تك‌تك بررسی کنیم و مـانند مثال ۴ استدلال کنیم به‌نتایج جدول ۴-۱ می‌رسیم. بنابراین ، به ازای $p > ۳$ ،

$$\left(\frac{۳}{p}\right) = +۱$$ اگر، وفقط اگر،(هنگ ۱۲) $p \equiv \pm ۱$.

جدول ۴-۱

مقادیر $\left(\frac{۳}{p}\right)$ ، $p > ۳$

r	حوزهٔ مقادیر k	v	زوجیت v	$\left(\frac{۳}{p}\right)$
۱	$۲m+۱$ تا $۴m$	$۲m$	زوج	$+۱$
۵	$۲m+۱$ تا $۴m+۱$	$۲m+۱$	فرد	-۱
۷	$۲m+۲$ تا $۴m+۲$	$۲m+۱$	فرد	-۱
۱۱	$۲m+۲$ تا $۴m+۳$	$۲m+۲$	زوج	$+۱$

قبل از اینکه مثال مفصلتری را از نظر بگذرانیم، به ذکـر چند نکتهٔ کلی می‌پردازیم. ابتدا ملاحظه می‌کنید که به‌طورصریح احتیاج به‌تعیین v نداریم. فقط احتیاج داریم بدانیم که آیا v زوج است یافرد. یعنی، باید زوجیت v را تعیین کنیم.

سپس، ملاحظه می‌کنیم که ، هنگام تحویل به هنگ p ، یك عدد صحیح مثبت n بـه طوری که $p \nmid n$ ، جایگزین عددی منفی‌واقع بین $(p-۱)/۲$ و $-(p-۱)/۲$ خواهدشد اگر ، وفقط اگر ،

$$\frac{p}{۲} \leqslant n \leqslant p$$

یا

$$\frac{۳}{۲}p \leqslant n \leqslant ۲p$$

یا

$$\frac{۵}{۲}p \leqslant n \leqslant ۳p$$

و الی آخر. به بیانی دیگر، به جای n یك عدد صحیح منفی گذاشته می‌شود اگـر یك عـدد

صحیح $1 \leqslant t$ موجود باشد به‌طوری‌که

$$\frac{2t-1}{2}p \leqslant n \leqslant tp\,.$$

چون $2t-1$ و p فرد هستند، می‌بینیم که $(2t-1)p/2$ عددی صحیح نیست، و بنابراین لازم‌خواهدبود تعداد اعداد صحیح k را که $\alpha \leqslant k \leqslant \beta$ بشماریم، که دراینجا α و β اعداد حقیقی‌مفروضی هستند و α عدد صحیح نیست. اینک لمی (لم۹) را که متضمن تمام‌حقایقی است‌که برای تسهیل تعیین زوجیت این‌گونه اعداد صحیح مورد نیاز است اثبات خواهیم کرد.

تعریف ۸ : فرض کنیم α عددی حقیقی باشد. فرض کنید بزرگترین عدد صحیح نابیشتراز α را به $[\alpha]$ نمایش دهیم. بنابراین، $[3]=3$ ، $[\pi]=3$ ، $[27/4]=6$. همچنین، به‌ازای هرعدد حقیقی مفروض α ، فرض کنیم $\alpha_1=\alpha-[\alpha]$ ، بنابراین $0 \leqslant \alpha_1 < 1$. در این صورت α_1 جزء کسری α نامیده می‌شود.

لم ۹ : فرض‌کنیم α و β اعداد حقیقی باشند، و α عددی ناصحیح، $\alpha \leqslant \beta$. دراین‌صورت

(یکم) تعداد اعداد صحیح k ، به‌طوری‌که $\alpha \leqslant k \leqslant \beta$ ، برابر $[\beta]-[\alpha]$ است.

(دوم) اگر n عددی صحیح باشد، آنگاه $[n+\beta]=n+[\beta]$.

(سوم) اگر $n_1 \leqslant n_2$ اعداد صحیح باشند، آنگاه تعداد اعداد صحیح k که در نامساویهای $2n_1+\alpha \leqslant k \leqslant 2n_2+\beta$ صدق‌می‌کنندو تعداد اعدادی که‌در $\alpha \leqslant k \leqslant \beta$ صدق می‌کنند دارای زوجیت یکسان هستند.

برهان :

(یکم) اعداد صحیح k (چون α عدد صحیحی نیست)، دقیقاً $[\alpha]+1$ ، $[\alpha]+2$ ، ... ، $[\beta]$ هستند و تعداد آنها $[\beta]-[\alpha]$ است .

(دوم) فرض کنیم $\beta_1=\beta-[\beta]$ جزء کسری β باشد . در این صورت $n+\beta=(n+[\beta])+\beta_1$ و $n+[\beta]$ عددی است صحیح ، بنابراین حکم محقق است.

(سوم) بنابر قسمتهای (یکم) و (دوم) ، دوعدد قسمت (سوم) عبارت‌اند از $[2n_2+\beta]-[2n_1+\alpha]=2n_2+[\beta]-2n_1-[\alpha]$ و $[\beta]-[\alpha]$ که‌واضح است که یك زوجیت‌دارند. ■

اینك این مبحث را بامثال نسبتاً پیچیده‌ای ختم می‌کنیم.

مثال ۱۰: می‌خواهیم $\left(\frac{۷}{p}\right)$ را به‌ازای کلیهٔ اعداد اول p ، مخالف ۲ و ۷، محاسبه کنیم. نظیر مثالهای ۳ ، ۴ ، ۷ ، جواب مطلوب به‌مانده‌های p به‌هنگ ۲۸ $= ۷ \times ۴$ بستگی خواهد داشت. در لم گاوس، اعداد صحیح

$$۱\times۷ ، ۲\times۷ ، \dots ، \frac{p-۱}{۲}۷$$

را درنظر می‌گیریم. بایدزوجیت تعدادکل اعدادصحیح واقع دربازه‌های زیر را تعیین کنیم از

$$\frac{p}{۲}\leqslant ۷k\leqslant p ،$$

$$\frac{۳p}{۲}\leqslant ۷k\leqslant ۲p ،$$

$$\frac{۵p}{۲}\leqslant ۷k\leqslant ۳p .$$

اینها تنها بازه‌هایی‌هستند که باید درنظر گرفته شوند زیرا $۱ \leqslant k \leqslant p/۲$ مستلزم $۷k \leqslant ۷p/۲$ است، وبازهٔ بعدی غیراز بازه‌های مفروض

$$\frac{۷}{۲}p\leqslant ۷k\leqslant ۴p$$

خواهد بود، که بیرون ازحوزهٔ مقادیر $۷k$ قرارمی‌گیرد. بنابراین، سه‌بازهٔ k عبارت‌اند از

$$\frac{p}{۱۴}\leqslant k \leqslant\frac{p}{۷} ،$$

$$\frac{۳}{۱۴}p\leqslant k\leqslant\frac{۲}{۷}p ،$$

$$\frac{۵}{۱۴}p\leqslant k\leqslant\frac{۳}{۷}p .$$

می‌نویسیم $p = ۲۸m + r$ ، که دراینجا r یکی‌از ۱۲ عدد ۱ ، ۳ ، ۵ ، ۹ ، ۱۱ ، ۱۳ ، ۱۵ ، ۱۷ ، ۱۹ ، ۲۳ ، ۲۵ ، ۲۷ می‌باشد. پس بازه‌های ما برای k عبارت‌انداز

$$۲m+\frac{r}{۱۴}\leqslant k\leqslant ۴m+\frac{r}{۷} ،$$

$$۶m+\frac{۳r}{۱۴} \leqslant k\leqslant ۸m+ \frac{۲r}{۷} ،$$

$$۱۰m+\frac{۵r}{۱۴}\leqslant k\leqslant ۱۲m+\frac{۳r}{۷} .$$

بنابر لم ۹ ، قسمت (سوم) ، اگر تعداد کل اعداد صحیح را در سه بازهٔ زیر بشماریم همان زوجیت را به‌دست خواهیم آورد،

$$\frac{r}{۱۴}\leqslant k\leqslant\frac{r}{۷}\,,$$

$$\frac{۳r}{۱۴}\leqslant k\leqslant\frac{۲r}{۷}\,,$$

$$\frac{۵r}{۱۴}\leqslant k\leqslant\frac{۳r}{۷}\,.$$

حال به‌آسانی ۱۲ مقدار r را بررسی می‌کنیم. به‌عنوان‌مثال، اگر $r=۱$ آنگاه درهیچ‌بازه‌ای عدد صحیحی برای k به‌دست نمی‌آید، و بنابراین (هنگ ۲)$v\equiv ۰$ زوج است. یا اگر $r=۱۳$ ، دقیقاً یك k درهریك ازسه بازه موجود است (بترتیب، $k=۱\,،\,۳\,،\,۵$)، و بنابراین (هنگ ۲)$v\equiv ۳$ فرد است. این نتایج درجدول ۴-۲ جدول‌بندی شده است.

جدول ۴-۲

مقادیر $\left(\frac{۷}{p}\right)$

$\left(\frac{۷}{p}\right)$	v	تعداد kها	$p\equiv r$ (هنگ ۲۸)
۱+	زوج	۰	۱
۱+	زوج	۰	۳
۱−	فرد	۱	۵
۱+	زوج	۲	۹
۱−	فرد	۳	۱۱
۱−	فرد	۳	۱۳
۱−	فرد	۳	۱۵
۱−	فرد	۳	۱۷
۱+	زوج	۴	۱۹
۱−	فرد	۵	۲۳
۱+	زوج	۶	۲۵
۱+	زوج	۶	۲۷

۳.۴ تمرینات

۱. ازلم گاوس برای محاسبهٔ

(آ) $\left(\frac{۱۱}{۱۷}\right)$ (ب) $\left(\frac{۱۲}{۲۳}\right)$ (ج) $\left(\frac{۵}{۱۱}\right)$ (د) $\left(\frac{۶}{۳۱}\right)$

استفاده کنید.

۲. نشان دهید که $\left(\frac{-۳}{p}\right)=۱$ اگر، وفقط اگر، $p\equiv ۱$ (هنگ ۳) .

۳. نتیجهٔ ۶ را ثابت کنید.

۴. یك برنامهٔ کامپیوتری برای محاسبهٔ $\left(\frac{a}{p}\right)$ بااستفاده ازلم گاوس بنویسید.

۵. بااستفاده ازقضیهٔ باقیماندهٔ چینی ونتایج بخشهای ۴.۳ و ۳.۴ کلیهٔ اعدادصحیح مثبت n را تعیین کنید به‌طوری که $x^۲\equiv ۲$ (هنگ n) دارای جواب باشد.

۶. بااستفاده ازلم گاوس

(آ) $\left(\frac{۵}{p}\right)$،

(ب) $\left(\frac{۱۱}{p}\right)$،

را تعیین کنید.

۷. با استفاده ازبخش ۳.۴ وهمچنین تمرین ۶ حقایق زیر را نشان‌دهید:

(آ) $\left(\frac{۵}{p}\right)=\left(\frac{p}{۵}\right)$ $(p\neq ۲ ، ۵)$.

(ب) $\left(\frac{۳}{p}\right)=(-۱)^{(p-۱)/۲}\left(\frac{p}{۳}\right)$ $(p\neq ۲ ، ۳)$.

(ج) $\left(\frac{۷}{p}\right)=(-۱)^{(p-۱)/۲}\left(\frac{p}{۷}\right)$ $(p\neq ۲ ، ۷)$.

(د) $\left(\frac{۱۱}{p}\right)=(-۱)^{(p-۱)/۲}\left(\frac{p}{۱۱}\right)$ $(p\neq ۲ ، ۱۱)$.

۸. (آ) ثابت کنید که اگر p و q اعداد اولی باشند به‌طوری که $p\equiv q$ (هنگ ۲۰)، آنگاه

$$\left(\frac{۵}{p}\right)=\left(\frac{۵}{q}\right).$$

(ب) ثابت کنید که اگر p و q اعداداولی باشند به‌طوری که $p\equiv q$ (هنگ ۴۴)، آنگاه

$$\left(\frac{11}{p}\right)=\left(\frac{11}{q}\right).$$

۹. فرض کنیم p و q اعداد اولی باشند و a یکی از اعداد ۳، ۵، ۷، ۱۱ باشد. نشان دهید که اگر $p\equiv -q$ (هنگ $4a$)، آنگاه

$$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right).$$

۱۰. $[7.1]$، $[5/2]$، $[22/13]$، $[-1.8]$، $[e]$، $[\sqrt{5}]$، $[\pi^3]$ را محاسبه کنید.

۱۱. نشان دهید که تعداد اعداد صحیح n به قسمی که $\alpha\leqslant n\leqslant\beta$، α و β اعدادی حقیقی و α عددی صحیح، برابر با $[\beta]-[\alpha]+1=[\beta]-\alpha+1$ است.

۱۲*. نشان دهید که تعدادی نامتناهی عدد اول به صورت $p\equiv +1$ (هنگ ۳) و تعدادی نامتناهی عدد اول همنهشت $1-$ به هنگ ۳ وجود دارد. (راهنمایی: به ازای $p\equiv -1$ (هنگ ۳)، برهان اقلیدس را درمورد اینکه تعداد اعداد اول نامتناهی است به صورت زیر تعمیم دهید: فرض کنید فقط تعدادی متناهی عدد اول، مثلا p_1، ...، p_t وجود داشته باشند. اگر t فرد باشد عدد $p_1\ldots p_t+3$ و اگر t زوج باشد، عدد $p_1\ldots p_t+1$ را در نظر بگیرید. برای $p\equiv 1$ (هنگ ۳)، به همین روش استدلال کنید، به استثنای اینکه $(p_1\ldots p_t)^2+3$ را در نظر بگیرید و از تمرین ۲ استفاده کنید.)

۱۳. فرض کنیم x عددی مثبت[1] و n عدد صحیح مثبتی باشد. نشان دهید که

$$\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right].$$

۱۴. فرض کنیم n عدد صحیح مثبتی باشد. نشان دهید که بزرگترین توان عدد اول p که $n!$ را عاد می‌کند برابر با

$$\sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right]$$

است. (توجه داشته باشید که بعد از مرحلهٔ معینی کلیهٔ جملات این سری صفر می‌شوند.)

۱۵. نشان دهید که به ازای یك عدد صحیح مثبت مفروض n کلیهٔ ضرایب دوجمله‌ای $\binom{n}{j}$ $(0\leqslant j\leqslant n)$ فرد هستند اگر، وفقط اگر، n به صورت 2^k-1 باشد.

۱۶*. (آیزنشتاین) فرض کنیم m و n دو عدد صحیح مثبت فرد متباین باشند، $m\neq 1$، $n\neq 1$. نشان دهید که

---

۱. ذکر مثبت بودن x زائد است (مترجم).

$$\sum_{x=1}^{(m-1)/2}\left[\frac{nx}{m}\right]+\sum_{y=1}^{(n-1)/2}\left[\frac{my}{n}\right]=\frac{m-1}{2}\cdot\frac{n-1}{2}.$$

(راهنمایی: یك مستطیل $m\times n$ در ربع اول صفحهٔ مختصات رسم کنید که یك رأس آن در (۰ ، ۰) واضلاع آن روی محورها باشند. قطر آن را بکشید و نقاط زیر قطر راکه‌مختصات آنها صحیح هستند بشمارید.)

۱۷. نشان‌دهید که تعداد نقاط $(x ، y)$ ، xوy صحیح ومثبت‌هستند، که‌روی‌هذلولی $xy=n$ ویا درزیرآن قرار دارند درست‌برابر $2\sum_{0<x<\sqrt{n}}[n/x]-[\sqrt{n}]^2$ است.

۱۸. تعداد نقاط $(x ، y)$ ، x و y صحیح هستند، راکه در داخل دایرهٔ $x^2+y^2=n$ ویا روی آن‌قرار دارند برحسب‌تابع [ ] محاسبه‌کنید.

۱۹. (آیزنشتاین) فرض‌کنیم x و n مثبت‌باشند[1]، n عددی است صحیح. نشان دهیدکه

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx].$$

*۲۰. فرض‌کنید a ، b ، m اعدادصحیح باشند و بمم$(a ، m)=d$. نشان‌دهیدکه

$$\left[\frac{b}{m}\right]+\left[\frac{a+b}{m}\right]+\left[\frac{2a+b}{m}\right]+\cdots+\left[\frac{(m-1)a+b}{m}\right]$$
$$=\frac{(a-1)(m-1)}{2}+\frac{d-1}{2}+b-r,$$

که درآن $b=qd+r$ ، $0\leqslant r<d$.

۲۱. (آ) نشان دهیدکه اگر h ، k ، l سه‌عددصحیح مثبت باشند، آنگاه

$$\left[\frac{2h}{k}\right]+\left[\frac{2l}{k}\right]\geqslant\left[\frac{h}{k}\right]+\left[\frac{l}{k}\right]+\left[\frac{h+l}{k}\right]$$

(ب) نشان دهیدکه

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

عددی صحیح است.

۲۲. فرض‌کنیم p عدد اولی به‌صورت $4q+1$ باشد، که q اول است: امثله‌عبارت‌اند از $p=13 ، 29 ، 53$. نشان‌دهیدکه بنابراستدلال زیر ۲ یك ریشهٔ اولیه به‌هنگ p است: با بررسی مستقیم، می‌توانیم فرض‌کنیم $p>16$.

---

۱. دراینجا مثبت بودن x زائد است (مترجم).

(آ) نشان دهید که $\left(\frac{۲}{p}\right)=-۱$.

(ب) نشان دهید که $۲^{۲q}\equiv -۱$ (هنگ p) . (راهنمایی: محك اویلر را به‌کار برید.)

(ج) نشان دهید که $\left(\frac{۲^{q}}{p}\right)=-۱$.

(د) نتیجه بگیرید که ۲ یك ریشهٔ اولیه به هنگ p است. (راهنمایی: چه امکاناتی برای $\mathrm{ord}_p ۲$ وجود دارند؟)

۴.۴ قانون تقابل مربعی

اینك به‌موضوع اصلی این فصل یعنی، قانون تقابل مربعی، می‌پردازیم. همچنانکه قبلا بیان‌کرده‌ایم، قانون تقابل مربعی روشی برای محاسبهٔ نماد لژاندر $\left(\frac{a}{p}\right)$ به ما خواهد داد وبدان وسیله می‌توانیم حلپذیر بودن همنهشتی $x^۲\equiv a$ (هنگ p) را تعیین کنیم. اویلر پس‌از محاسبات عددی زیاد توانست قانونی را برای محاسبهٔ $\left(\frac{a}{p}\right)$ به‌ازای بعضی مقادیر خاص a و p ، حدس بزند. درمثالهای بخش قبل بسیاری از حالات خاص $\left(\frac{a}{p}\right)$ رامحاسبه کردیم. درواقع، اطلاعات ما از اطلاعات اویلر بیشتر است زیرا ما $\left(\frac{a}{p}\right)$ را به‌ازای $a=-۱ ، ۲ ، ۳ ، ۷$ وکلیهٔ اعداد اول p محاسبه کردیم. (البته، اویلر لم گاوس‌را دراختیار نداشت.)

اینك اطلاعات خود را برای $\left(\frac{۲}{p}\right)$ ، $\left(\frac{۳}{p}\right)$ ، و $\left(\frac{۷}{p}\right)$ می‌آزماییم، واستدلال اویلر را درنظر می‌گیریم. (بترتیب، به‌قضیهٔ ۵.۳ ومثالهای ۷.۳ و ۱۰.۳ رجوع کنید.)

ابتدا، توجه می‌کنیم که درکلیهٔ حالاتی که محاسبه‌کردیم، مقدار دقیق p برای محاسبهٔ $\left(\frac{a}{p}\right)$ مورد احتیاج نبود، ولی بیشتر فقط باقیمانده‌ای که درتقسیم بر $۴a$ به‌جا می‌ماند لازم بود . به‌عبارت دیگر ، اگر p و q اعداد اول باشند و $p\equiv q$ (هنگ $۴a$) ، آنگاه $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$.

ثانیاً، ملاحظه می‌کنیم که جداول ۴-۱ و ۴-۲ نسبت به‌خط میانی خود متقارن هستند. یعنی ، $\left(\frac{a}{p}\right)$ برای باقیمانده‌های r و $۴a-r$ یك‌مقدار دارد. به‌بیانی دیگر مشاهده می‌کنیم

که اگر p و q اعداد اول باشند و (هنگ $p\equiv -q(\text{۴}a$ ، آنگاه $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$.

آیا خواصی که برمبنای محاسبات پیدا کردیم به‌عنوان خواص کلی نماد لژاندر $\left(\frac{a}{p}\right)$ باقی می‌مانند؟ اویلر حدس زد که چنین است، و این است دقیقاً محتوای قانون تقابل مربعی، که ما اینك آن‌را بیان خواهیم کرد.

قضیهٔ۱ (قانون تقابل مربعی-صورت اول): فرض کنیم $a(>\text{۱})$ عدد صحیح معینی باشد. به‌ازای عدد اول p به‌طوری که $p\nmid \text{۴}a$، می‌نویسیم $p=\text{۴}am+r$ ، $\text{۰}<r<\text{۴}a$. دراین صورت $\left(\frac{a}{p}\right)$ فقط به‌باقیماندهٔ r بستگی دارد و نه بـه p. بعلاوه، $\left(\frac{a}{p}\right)$ به‌ازای باقیمانده‌های r و $\text{۴}a-r$ یك مقدار اختیار می‌کند.

ولی، اویلر نتوانست حدس خود را اثبات کند. گاوس که بدون هیچ اطلاعی از کار اویلر کار می‌کرد، حدس اویلر را کشف کرد و اولین برهان را برای آن به‌دست آورد. کار گاوس زمانی انجام شده بود که او نوزده ساله بـود و اولین‌بار در کتاب معروف و بسیار ارزندهٔ تحقیقات حسابی کـه در ۱۷۹۹ میلادی چاپ شد، ظاهـر گشت. (اخیراً، تـرجمهٔ انگلیسی آن باجلدکاغذی منتشر شده‌است.)[1] برهان اولیهٔ گاوس برای قانون تقابل مـربعی، خیلی پیچیده بود و درآن از استقرای مضاعف استفاده شده بود. ولی، گاوس آنچنان شیفتهٔ نتیجهٔ کار خود شده بود که تجسسات خودرا ادامه داد و سرانجام هفت دلیل بـرای قانـون تقابل مربعی فراهم آورد. این قضیه صاحبنظران نظریهٔ اعـداد را سخت فریفتهٔ خود کـرد تاجایی که اکنون صدها دلیل برای‌آن پیدا کرده‌اند. برهانی که ما برای قضیهٔ۱ ارائه‌خواهیم داد یکی از هفت برهان گاوس می‌باشد که براساس لم گاوس متکی است.

برهان قضیهٔ۱: از لم گاوس (قضیهٔ ۱.۳) و بحث پی‌آمد آن دربخش۳، بایستی زوجیت ν ، تعدادکل اعداد صحیح k، $\text{۱}\leqslant k\leqslant p/\text{۲}$ ، راچنان تعیین کنیم که k دریکی ازبازه‌های

$$\frac{\text{۱}}{\text{۲}}p\leqslant ka\leqslant p ,$$

$$\frac{\text{۳}}{\text{۲}}p\leqslant ka\leqslant \text{۲}p ,$$

$$\frac{\text{۵}}{\text{۲}}p\leqslant ka\leqslant \text{۳}p ,$$

و الی‌آخر قرار داشته باشد. ازتقسیم‌طرفین نامساویها بر a ، می‌بینیم که بایستی زوجیت ν،

---

1. *Disquisitiones Arithmeticae*, A.A.Clarke, S.J.(trans.), Yale University Press, New Haven, Conn., 1966.

تعداد کل اعداد صحیح k، $1 \leqslant k \leqslant \frac{p}{2}$ را تعیین کنیم چنان که k در یکی از بازه‌های

$$\frac{p}{2a} \leqslant k \leqslant \frac{p}{a},$$

$$\frac{3p}{2a} \leqslant k \leqslant \frac{2p}{a},$$

$$\frac{5p}{2a} \leqslant k \leqslant \frac{3p}{a},$$

و الی‌آخر قرار داشته باشد. آخرین بازه‌ای که ما باید درنظر بگیریم کدام است؟ تمام بازه‌ها به‌صورت

$$\frac{2s-1}{2a} p \leqslant k \leqslant \frac{sp}{a},$$

به‌ازای عددصحیح $s(\geqslant 1)$، هستند. بنابراین، چون $1 \leqslant k \leqslant p/2$ ، مطمئناً ما احتیاج نداریم که هیچ بازه‌ای بعداز بازهٔ شامل $p/2$ را درنظربگیریم، وبرای این بازه داریم

$$\frac{2t-1}{2a} p \leqslant \frac{p}{2} \leqslant \frac{tp}{a}$$

یا ، با عبارتی معادل باآن،

$$\frac{2t-1}{2} \leqslant \frac{a}{2} \leqslant t. \qquad (1)$$

از (۱)، می‌بینیم که چون a و t اعداد صحیح هستند، بایستی داشته‌باشیم

$$t = \begin{cases} \frac{a}{2} & \text{اگر } a \text{ زوج باشد} \\ \frac{a}{2}+\frac{1}{2} & \text{اگر } a \text{ فرد باشد} \end{cases}$$

بنابراین، احتیاج به‌تعیین زوجیت ν ، تعدادکل اعداد صحیح k ، $1 \leqslant k \leqslant p/2$ ، داریم به‌طوری که k دریکی از بازه‌های

$$\begin{aligned} &\frac{p}{2a} \leqslant k \leqslant \frac{p}{a}, \\ &\frac{3p}{2a} \leqslant k \leqslant \frac{2p}{a}, \\ &\qquad\vdots \\ &\frac{2t-1}{2a} p \leqslant k \leqslant \frac{tp}{a}. \end{aligned} \qquad (2)$$

قرار داشته باشد. اگر a زوج باشد، آنگاه $tp/a = p/۲$ ، بنابراین نامساویهای (۲) خودبخود ایجاب می کنند که داشته باشیم $۱ \leqslant k \leqslant p/۲$ ، وبنابراین‌شرط $۱ \leqslant k \leqslant p/۲$ می‌تواند حذف شود. اگر a فرد باشد، آنگاه $t = a/۲ + ۱/۲$ و آخرین بازهٔ (۲) فقط

$$\frac{p}{۲} \leqslant k \leqslant \frac{p}{۲} + \frac{p}{۲a}$$

است، وبنابراین‌ما می‌توانیم شرط $۱ \leqslant k \leqslant p/۲$ را حذف کنیم به‌شرط آنکه آخرین بازهٔ (۲) را حذف کنیم. پس قرار می‌دهیم $u = t$ اگر a زوج باشد، و $u = t - ۱$ اگر a فرد باشد. دراین‌صورت ما بایستی زوجیت ν ، تعدادکل اعدادصحیح k واقع درهریك از بازه‌های ذیل، را تعیین کنیم:

$$\frac{p}{۲a} \leqslant k \leqslant \frac{p}{a},$$

$$\frac{۳p}{۲a} \leqslant k \leqslant \frac{۲p}{a},$$

$$\vdots$$

$$\frac{۲u - ۱}{۲a} p \leqslant k \leqslant \frac{up}{a}.$$

بدین‌ترتیب، می‌بینیم که نکتهٔ مهم درآن است که آخرین بازه‌ای که بایستی درنظر بگیریم فقط بستگی به a دارد ونه به p، چون $u = a/۲$ اگر a زوج باشد و $u = (a/۲) - ۱/۲$ اگر a فرد باشد.

مانند بخش پیش، قرار می‌دهیم $p = ۴am + r$، که درآن $۰ < r < ۴a$. (توجه کنید که‌چون $p \nmid ۴a$ ، پس $r \neq ۰$.) پس‌احتیاج به‌تعیین زوجیت ν ، تعدادکل اعدادصحیح k واقع درهریك از بازه‌های ذیل داریم

$$۲m + \frac{r}{۲a} \leqslant k \leqslant ۴m + \frac{r}{a},$$

$$۶m + \frac{۳r}{۲a} \leqslant k \leqslant ۸m + \frac{۲r}{a},$$

$$۱۰m + \frac{۵r}{۲a} \leqslant k \leqslant ۱۲m + \frac{۳r}{a},$$

$$۲(۲u-۱)m+\frac{۲u-۱}{۲a}r \leqslant k \leqslant ۴um+\frac{ur}{a} \cdot$$

با استفاده ازقسمت (سوم)، لم ۹.۰۳، می‌بینیم که زوجیت vی فوق همان زوجیت تعداد کل اعداد صحیح k است که درهریك از بازه‌های زیر قرار دارند

$$\frac{r}{۲a} \leqslant k \leqslant \frac{r}{a} \cdot$$

$$\frac{۳r}{۲a} \leqslant k \leqslant \frac{۲r}{a},$$

$$\vdots \qquad (۳)$$

$$\frac{۲u-۱}{۲a}r \leqslant k \leqslant \frac{ur}{a} \cdot$$

ولی آشکارا دیده می‌شود کــه این زوجیت فقط به r بستگی دارد نه‌به p. بنابرایــن، ثابت کردیم که $\left(\frac{a}{p}\right)$ به‌شرط‌آنکه $p=۴am+r$، فقط بستگی به r دارد نه به p. این امر نیمهٔ اول قضیهٔ ۱ را ثابت می‌کند.

حال فرض‌کنید در(۳) به‌جای r، $۴a-r$ را بگذاریم. دراین صورت بازه‌های (۳) به‌صورت زیر

$$\frac{۴a-r}{۲a} \leqslant k \leqslant \frac{۴a-r}{a},$$

$$\frac{۳(۴a-r)}{۲a} \leqslant k \leqslant \frac{۲(۴a-r)}{a},$$

$$\frac{۵(۴a-r)}{۲a} \leqslant k \leqslant \frac{۳(۴a-r)}{a},$$

$$\vdots$$

$$\frac{(۲u-۱)(۴a-r)}{۲a} \leqslant k \leqslant \frac{u(۴a-r)}{a},$$

ویا به‌صورت معادل باآن

$$۲-\frac{r}{۲a} \leqslant k \leqslant ۴-\frac{r}{a},$$

$$۶-\frac{۳r}{۲a}\leqslant k\leqslant ۸-\frac{۲r}{a},$$

$$۱۰-\frac{۵r}{۲a}\leqslant k\leqslant ۱۲-\frac{۳r}{a}, \qquad (۴)$$

$$\vdots$$

$$۴u-۲-\frac{r(۲u-۱)}{۲a}\leqslant k\leqslant ۴u-\frac{ru}{a}.$$

درمی‌آیند. بنابر قسمتهای (یکم) و (دوم) لم ۹.۳ ، تعداد اعداد صحیح دراولین بازهٔ (۴) عبارت است از

$$\left[۴-\frac{r}{a}\right]-\left[۲-\frac{r}{۲a}\right]=۴+\left[-\frac{r}{a}\right]-\left(۲+\left[-\frac{r}{۲a}\right]\right)$$
$$=۲+\left[\frac{r}{۲a}\right]-\left[\frac{r}{a}\right]$$

زیرا r/a و $r/۲a$ اعداد صحیح نیستند و به ازای هرعدد حقیقی α که عدد صحیح نباشد $[-\alpha]=-[\alpha]-۱$ (تمرین). بنابراین، تعداد اعداد صحیح دراولین بازهٔ (۴) عبارت است از

$$۲+\left[\frac{r}{۲a}\right]-\left[\frac{r}{a}\right]\equiv\left[\frac{r}{۲a}\right]-\left[\frac{r}{a}\right]\ (\text{هنگ } ۲).$$

بدین‌ترتیب، زوجیت تعداد اعداد صحیح دراولین بازهٔ(۴) همان زوجیت

$$\left[\frac{r}{۲a}\right]-\left[\frac{r}{a}\right],$$

است، که همان تعداد اعداد صحیح واقع دراولین بازهٔ(۳) می‌باشد. هرگاه برای هریك از بازه‌های(۴) همین گونه استدلال کنیم، می‌بینیم که زوجیت ν' ، تعداد کل اعداد صحیح واقع درهریك از بازه‌های (۴)، همان زوجیت ν ، تعداد کل اعداد صحیح واقع در هریك از بازه‌های(۳)می‌باشد. ازاین‌رو، بنابرلم گاوس، اگر p و q اعدادی‌اول باشند، $p\nmid ۲a$، $q\nmid ۲a$، وبااین شرط که $p=۲am+r$ ، $q=۲am'+(۲a-r)$ ، آنگاه

$$\left(\frac{a}{p}\right)=(-۱)^{\nu}=(-۱)^{\nu'}=\left(\frac{a}{q}\right).$$

بنابراین، نماد لژاندر $\left(\frac{a}{p}\right)$ برای باقیمانده‌های r و $۴a-r$ یکی می‌باشند. این اثبات

حکم دوم قضیهٔ ۱ است. ■

می‌توانیم قضیهٔ ۱ را با بیان معادل دیگری بیان کنیم:

نتیجهٔ ۳: فرض کنیم a عددصحیحی بزرگتراز ۱ باشد، و p ، q اعداد اولی که $4a$ را عاد نمی‌کنند. اگر $p \equiv \pm q$ (هنگ $4a$)، آنگاه $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$.

قانون تقابل مربعی را می‌توان به‌نحوی ظریفتر، ولی اندکی پیچیده‌تر، فرمولبندی مجدد کرد. این فرمولبندی‌جدید اول‌بار توسط لژاندر در ۱۷۸۵ میلادی به‌صورت‌یک‌حدس بیان شده بود.

قضیهٔ ۳ (قانون تقابل مربعی-صورت دوم): فرض کنیم p و q اعداد اول فرد متمایزی‌باشند. دراین‌صورت

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{((p-1)/2)((q-1)/2)} .$$

بنابراین، $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ ، مگر اینکه $p \equiv q \equiv -1$ (هنگ ۴)، که دراین حالت $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$.

قضیهٔ ۳ بسیار شگفت‌انگیز وکاملا غیرمنتظره است، زیرا بیان می‌کند که بین‌حلپذیری همنهشتی $x^2 \equiv p$ (هنگ q) وحلپذیری همنهشتی $x^2 \equiv q$ (هنگ p) رابطه‌ای وجود دارد. بعلاوه، همچنانکه در زیر خواهیم دید، قضیهٔ ۳ الگوریتم ساده‌ای را برای محاسبهٔ $\left(\frac{p}{q}\right)$ پیش‌پای ما می‌گذارد.

برهان قضیهٔ ۳: ابتدا فرض می‌کنیم $p \equiv q$ (هنگ ۴). بی‌آنکه خللی به کلیت وارد آید، فرض می‌کنیم $p>q$. می‌نویسیم $p=q+4a$. دراین‌صورت، بنابر نتایج ۸.۲ و ۹.۲ و قضیهٔ ۶.۲، داریم

$$\left(\frac{p}{q}\right)=\left(\frac{q+4a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{4}{q}\right)\left(\frac{a}{q}\right)=\left(\frac{a}{q}\right)$$

و

$$\left(\frac{q}{p}\right)=\left(\frac{p-4a}{p}\right)=\left(\frac{-4a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{4}{p}\right)\left(\frac{a}{p}\right)=(-1)^{(p-1)/2}\left(\frac{a}{p}\right).$$

چون $p\equiv q$ (هنگ $4a$)، بنابر نتیجهٔ ۲ داریم $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$، پس

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(p-1)/2}.$$

بالاخره $(p-1)/2=(q-1)/2+2a$، و بنابراین $(p-1)/2$ زوج است اگر و فقط اگر $(q-1)/2$ زوج باشد، و بدین ترتیب

$$(-1)^{(p-1)/2}=(-1)^{((p-1)/2)((q-1)/2)},$$

لذا قضیه در این حالت ثابت شده است. اگر $p\not\equiv q$ (هنگ ۴)، آنگاه چون p و q فرد می‌باشند، بایستی یا داشته باشیم $p\equiv 1$ (هنگ ۴)، $q\equiv 3$ (هنگ ۴) یا $p\equiv 3$ (هنگ ۴)، $q\equiv 1$ (هنگ ۴). درهر دوحـال، اگر $p\not\equiv q$ (هنگ ۴)، آنگاه $p\equiv -q$ (هنگ ۴). در این‌صورت می‌توانیم بنویسیم $p=-q+4a$. مجدداً بنا بر نتیجهٔ ۸.۲ و قضیهٔ ۶.۲، داریم

$$\left(\frac{p}{q}\right)=\left(\frac{-q+4a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{4}{q}\right)\left(\frac{a}{q}\right)=\left(\frac{a}{q}\right)$$

و

$$\left(\frac{q}{p}\right)=\left(\frac{-p+4a}{p}\right)=\left(\frac{4a}{p}\right)=\left(\frac{4}{p}\right)\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right).$$

چون $p\equiv -q$ (هنگ $4a$)، نتیجهٔ ۲ ایجاب می‌کند که $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$، بنابراین $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ و $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=1$. ولی، در این‌حالت،

$$\frac{p-1}{2}+\frac{q-1}{2}=2a-1$$

فرد است، پس یکی از کمیات $(p-1)/2$، $(q-1)/2$ بایستی زوج باشد. بنابراین، $(-1)^{((p-1)/2)((q-1)/2)}=1$، و قضیه به‌طور کامل ثابت می‌شود. ■

با استفاده از قانون تقابل مربعی به‌صورتی که در قضیهٔ ۳ بیان شد، توأم با قضیهٔ ۶.۲ و نتایج ۸.۲ و ۹.۲ و قضیهٔ ۵.۳، می‌توانیم مسئلهٔ حلپذیری همنهشتی $x^2\equiv a$ (هنگ p) را تماماً به‌یک‌محاسبهٔ ساده بدل کنیم. (ولی، مجدداً تأکید می‌کنیم که روش ما هیچ گونه اطلاعی دربارهٔ اینکه جوابها، درصورت‌وجود، چه‌هستند نمی‌دهد.) اینک به‌ذکر چندمثال می‌پردازیم.

مثال ۴: آیا همنهشتی $x^۲ \equiv ۳ \ (\text{هنگ } ۴۳)$ حل‌پذیر است؟ داریم

$$\left(\frac{۳}{۴۳}\right)=\left(\frac{۴۳}{۳}\right)(-۱)^{((۳-۱)/۲)((۴۳-۱)/۲)}=-\left(\frac{۱}{۳}\right)=-۱ \text{ ،}$$

بنابراین، همنهشتی فوق را نمی‌توان حل کرد. چون $-۴۰ \equiv ۳ \ (\text{هنگ } ۴۳)$، به‌استناد قضیهٔ ۶.۲ می‌دانیم که

$$\left(\frac{-۴۰}{۴۳}\right)=\left(\frac{۳}{۴۳}\right)=-۱ \text{ ،}$$

ولی، به‌عنوان مثال دیگر، $\left(\frac{-۴۰}{۴۳}\right)$ را مستقیماً حساب می‌کنیم:

$$\left(\frac{-۴۰}{۴۳}\right)=\left(\frac{(-۱)۲^۳\times ۵}{۴۳}\right)=\left(\frac{-۱}{۴۳}\right)\left(\frac{۲}{۴۳}\right)^۳\left(\frac{۵}{۴۳}\right)$$

$$=(-۱)^{(۴۳-۱)/۲}\left(\frac{۲}{۴۳}\right)\left(\frac{۵}{۴۳}\right) \qquad (\text{مثال } ۳.۳)$$

$$=-(-۱)\left(\frac{۵}{۴۳}\right) \qquad (\text{چون } ۴۳\equiv ۳ \ (\text{هنگ } ۸)\text{، با استفاده از قضیهٔ } ۵.۳)$$

$$=\left(\frac{۵}{۴۳}\right)$$

بنابراین، با استفاده از قانون تقابل‌مربعی، می‌بینیم که

$$\left(\frac{-۴۰}{۴۳}\right)=\left(\frac{۵}{۴۳}\right)=\left(\frac{۴۳}{۵}\right)(-۱)^{((۴۳-۱)/۲)((۵-۱)/۲)}$$

$$=\left(\frac{۳}{۵}\right)=\left(\frac{۵}{۳}\right)(-۱)^{((۵-۱)/۲)((۳-۱)/۲)}$$

$$=\left(\frac{۲}{۳}\right)=-۱ .$$

برای اینکه تصوری از کارآیی روش فوق به‌شما بدهیم، اجازه دهید مثالی را که شامل اعداد بزرگتری است محاسبه کنیم.

مثال ۵: آیا همنهشتی

$$x^۲ \equiv ۲۰۹۶۴ \ (\text{هنگ } ۱۹۸۷)$$

را می‌توان حل کرد؟ توجه کنید که ۱۹۸۷ عددی اول است. (می‌توانید تحقیق کنید که بر هیچ

عدد اولی کمتر از $\sqrt{1987}$ بخش‌پذیر نیست.) بنابراین، کافی است $\left(\frac{20964}{1987}\right)$ را محاسبه کنیم. چون $20964 \equiv 1094 \pmod{1987}$ وچون $1094 = 2 \times 547$، می‌بینیم که

$$\left(\frac{20964}{1987}\right)=\left(\frac{1094}{1987}\right)=\left(\frac{2}{1987}\right)\left(\frac{547}{1987}\right)=-\left(\frac{547}{1987}\right)$$

زیرا $1987 \equiv 3 \pmod{8}$ ایجاب می‌کند که $\left(\frac{2}{1987}\right)=-1$ (قضیهٔ ۵.۳). اما ۵۴۷ عددی اول است و $547 \equiv 1987 \equiv -1 \pmod{4}$، پس بنابرقانون تقابل مربعی، داریم

$$\left(\frac{20964}{1987}\right)=-\left(\frac{547}{1987}\right)=\left(\frac{1987}{547}\right)=\left(\frac{346}{547}\right)$$
$$=\left(\frac{2}{547}\right)\left(\frac{173}{547}\right)=-\left(\frac{173}{547}\right)$$

زیرا $547 \equiv 3 \pmod{8}$. مجدداً با استفاده ازقانون تقابل مربعی (۱۷۳ عددی است‌اول)، داریم

$$\left(\frac{20964}{1987}\right)=-\left(\frac{173}{547}\right)=-\left(\frac{547}{173}\right)=-\left(\frac{28}{173}\right)=-\left(\frac{4}{173}\right)\left(\frac{7}{173}\right)=-\left(\frac{7}{173}\right)$$
$$=-\left(\frac{173}{7}\right)=-\left(\frac{5}{7}\right)=-\left(\frac{7}{5}\right)=-\left(\frac{2}{5}\right)=1.$$

بدین‌ترتیب، همنهشتی اولیه حلپذیر می‌باشد.

اجازه دهید این‌بخش را بامثال‌دیگری شبیه به‌مثالهایی که با استفاده از لم گاوس‌طرح کردیم، پایان دهیم.

مثال ۶: $\left(\frac{5}{p}\right)$ را، به‌ازای $p>5$، به‌طور کامل تعیین می‌کنیم. می‌نویسیم $p=5a+r$، $r=1$، ۲، ۳ یا ۴. چون $5 \equiv 1 \pmod{4}$، از قانون تقابل مربعی داریم

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)(-1)^{((p-1)/2)((5-1)/2)}=\left(\frac{p}{5}\right)=\left(\frac{5a+r}{5}\right)=\left(\frac{r}{5}\right).$$

ازآنجاکه $\left(\frac{r}{5}\right)=1$ اگر،وفقط اگر، $r=1$ یا ۴، می‌بینیم که

$$\left(\frac{5}{p}\right)=\begin{cases} 1 & \text{اگر } p \equiv \pm 1 \pmod{5} \\ -1 & \text{اگر } p \equiv \pm 2 \pmod{5} \end{cases}$$

توجه کنید که، بنا بر قضیهٔ ۱ ، بایستی مسئله بایك شرط همنهشتی به‌هنگ ۲۰ خاتمه می‌یافت، درصورتی که آن‌را بایك شرط همنهشتی به‌هنگ ۵ خاتمه دادیم. ولی، البته، چون ۲۰|۵ ، هر شرط همنهشتی به‌هنگ ۵ می‌تواند به‌صورت یك همنهشتی به‌هنگ ۲۰ نشان داده شود.

۴.۴ تمرینات

۱. با استفاده از قانون تقابل مربعی تعیین کنید که آیا همنهشتیهای زیر حلپذیرند:

(آ) $x^{۲} \equiv ۱۵$ (هنگ ۳۱) .　　(ب) $x^{۲} \equiv ۴۸$ (هنگ ۸۹) .

(ج) $x^{۲} \equiv -۱۷$ (هنگ ۸۹) .　　(د) $x^{۲} \equiv ۱۷$ (هنگ ۳۱) .

(ه) $x^{۲} \equiv ۲۳$ (هنگ ۵۹) .　　(و) $x^{۲} \equiv ۲۶۴$ (هنگ ۱۷۳) .

(ز) $x^{۲} \equiv ۴۹۷۷$ (هنگ ۱۹۸۷) .

۲. با استفاده از قانون تقابل مربعی، به‌ازای کلیهٔ اعداد اول فرد p ، به‌طور کامل مقادیر زیر را تعیین کنید:

(آ) $\left(\frac{۳}{p}\right)$ ، $(p \neq ۳)$.　　(ب) $\left(\frac{۷}{p}\right)$ $(p \neq ۷)$.　　(ج) $\left(\frac{۳۱}{p}\right)$ ، $(p \neq ۳۱)$.

(د) $\left(\frac{۶}{p}\right)$ ، $(p \neq ۳)$.　　(ه) $\left(\frac{-۵}{p}\right)$ ، $(p \neq ۵)$.

(می‌توانید قسمتهای (آ) و (ب) را بامثالهای بخش ۳ مطابقت کنید).

۳. تعیین کنید که آیا همنهشتیهای زیر برحسب اعداد صحیح x و y با این شرط که $x \not\equiv ۰$ (هنگ ۱۷) و $y \not\equiv ۰$ (هنگ ۱۷) حلپذیرند:

(آ) $x^{۲} + ۱۵y^{۲} \equiv ۰$ (هنگ ۱۷) .

(ب) $x^{۲} + ۱۱y^{۲} \equiv ۰$ (هنگ ۱۷) .

۴. تعیین کنید که آیا همنهشتیهای زیر را می‌توان حل کرد:

(آ) $x^{۲} \equiv ۲۳$ (هنگ ۱۷۷) ، $(۱۷۷ = ۵۹ \times ۳)$.

(ب) $x^{۲} \equiv ۵$ (هنگ ۱۱۰۲) ، $(۱۱۰۲ = ۲ \times ۱۹ \times ۲۹)$.

۵. یك برنامهٔ کامپیوتری برای محاسبهٔ $\left(\frac{a}{p}\right)$ ، به‌ازای اعداد اول فرد p ، بنویسید.

*۶. نشان دهید که قضیهٔ ۴، قضیهٔ ۱ را ایجاب می‌کند. (راهنمایی: a را به‌صورت حاصلضرب اعداد اول بنویسید.)

۷. نشان دهید که اگر p عددی اول باشد و $p \equiv \pm ۱$ (هنگ $۴a$) ، آنگاه $\left(\frac{a}{p}\right) = ۱$.

(راهنمایی: a را به‌صورت حاصلضرب اعداد اول بنویسید وقانون تقابل مربعی را به‌کار برید.)

۸. نشان دهید که اگر p عددی اول باشد و $p\equiv 2a-1$ (هنگ $4a$) و $a\equiv 1$ (هنگ ۴)، آنگاه $\left(\frac{a}{p}\right)=1$.

بقیهٔ این‌تمرینات دربارهٔ تعمیم تعریف و خواص نماد لژاندر $\left(\frac{a}{p}\right)$ است.

تعریف: اگر n عدد صحیح فردی بزرگتر از ۱ باشد و ۱ = بمعم$(a ، n)$، n را به‌صورت حاصلضربی از اعداد اول می‌نویسیم

$$n=p_1p_2\cdots p_t\,.$$

نماد ژاکوبی $\left(\frac{a}{n}\right)$ را توسط

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$$

تعریف می‌کنیم.

توجه کنید که این تعریف هنگامی که n عددی اول است با تعریف قبلی تطابق دارد. کاربرد اصلی آن این است که درمحاسبهٔ نماد لژاندر کار را ساده می‌کند. درسراسر این تمرینات n معرف عدد صحیح فردی است بزرگتر از ۱ و a عدد صحیحی است که ۱ = بمعم$(a ، n)$.

۹. نشان دهید که اگر $a\equiv a'$ (هنگ n)، آنگاه $\left(\frac{a}{n}\right)=\left(\frac{a'}{n}\right)$.

۱۰. نشان دهید که $\left(\frac{aa'}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{a'}{n}\right)$.

۱۱. نشان دهید که $\left(\frac{a}{n}\right)\left(\frac{a}{m}\right)=\left(\frac{a}{nm}\right)$. درنتیجه، $\left(\frac{a}{n^2}\right)=1$.

۱۲. نشان دهید که اگر p_1، p_2، ...، p_t اعداد اول فرد (که لزوماً متمایز نیستند) باشند، آنگاه

$$\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_t-1}{2}\equiv\frac{p_1p_2\cdots p_t-1}{2}\ (\text{هنگ } 2)\,.$$

۱۳. نشان دهید که $\left(\frac{-1}{n}\right)=(-1)^{(n-1)/2}$.

۱۴. نشان‌دهید که اگر p_1، p_2، ...، p_t اعداد اول فرد باشند، آنگاه

$$\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\dots+\frac{p_t^2-1}{8}\equiv\frac{(p_1p_2\cdots p_t)^2-1}{8} \pmod 2$$.

۱۵. نشان‌دهید که $\left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$. لذا ، $\left(\frac{2}{n}\right)=1$ اگر ، و فقط اگر ، $n\equiv\pm1 \pmod 8$.

۱۶. نشان‌دهید که اگر p_1 ، p_2 ، … ، p_t و q_1 ، q_2 ، … ، q_s اعداد اول فرد باشند، آنگاه

$$\sum_{i=1}^{t}\sum_{j=1}^{s}\frac{p_i-1}{2}\times\frac{q_j-1}{2}\equiv\frac{p_1p_2\cdots p_t-1}{2}\times\frac{q_1q_2\cdots q_s-1}{2} \pmod 2$$.

۱۷. (قانون تقابل) نشان دهید که اگر m و n اعداد صحیح فرد بزرگتراز ۱ باشند و بمعم$(m , n)=1$ ، آنگاه

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{((n-1)/2)((m-1)/2)}$$

۱۸. بااستفاده از نتایج فوق درباب نماد ژاکوبی ببینید که آیا همنهشتیهای زیرحلپذیرند:

(آ) $x^2\equiv 264 \pmod{173}$ (ب) $x^2\equiv 4977 \pmod{1987}$

(ج) $x^2\equiv 187 \pmod{389}$.

توجه کنید که مزیت روش فوق برروشی که درآن فقط از نماد لژاندر استفاده می‌شود این است که به‌تجزیهٔ صورت کسر قبل‌از معکوس کردن نماد احتیاجی ندارد.

۱۹. یك برنامهٔ کامپیوتری برای محاسبهٔ $\left(\frac{a}{n}\right)$ ، به‌ازای اعداد صحیح فرد n ، بنویسید. (برنامه کامپیوتری خود را که درتمرین ۵ نوشته بودید کنار بگذارید.)

۲۰. (آ) نشان دهید که اگر $x^2\equiv a \pmod n$ حلپذیر باشد، آنگاه $\left(\frac{a}{n}\right)=1$.

(ب) نشان‌دهید که‌عکس قسمت (آ) غلط است؛ یعنی، اعداد صحیح a ، و n موجودند که n فرد است و بمعم$(a , n)=1$ و $\left(\frac{a}{n}\right)=1$ و $x^2\equiv a \pmod n$ حلپذیر نیست.

۵.۴ کاربردها درمعادلات سیاله

اینك به‌ذکر چندکاربرد از نظریهٔ بخشهای پیشین درمعادلات سیاله می‌پردازیم. به‌عنوان اولین مثال، معادلهٔ سیالهٔ

$$ax^2+by+c=0 \qquad (1)$$

را درنظر می‌گیریم، که درآن a ، b ، c اعداد صحیح مفروض و x ، y اعدادصحیحی هستند

که باید تعیین شوند. اگر $b=0$ ، معادلهٔ(۱) فقط و فقط وقتی جواب دارد که c/a — مربع یك عدد صحیح باشد. از این‌رو ، فرض می‌کنیم $b>0$. این معادله معادل است با همنهشتی

$$ax^2 \equiv -c(b \text{ هنگ}) \;. \qquad (۲)$$

فرض کنیم، بمعم(a , b) $d=$. پس واضح است که اگر (۱) بتواند حل شود، باید داشته باشیم $d|c$. اگر $d|c$ و $c=dc'$ ، $a=da'$ ، $b=db'$ ، آنگاه ۱ = بمعم(a' , b') و معادلهٔ(۱) معادل است با معادلهٔ

$$a'x^2+b'y+c'=0 \;,$$

که معادله‌ای است از همان‌نوع که درابتدا بود، جزاینکه بعلاوه داریم ۱ = بمعم(a' , b'). بنابراین، کافی است معادلهٔ(۱) را به‌ازای مقادیری از a و b که نسبت به‌هم اول هستند درنظر بگیریم. بنابرقضیهٔ ۸.۲.۳ می‌توانیم a^* را چنان بیابیم که

$$aa^* \equiv 1(b \text{ هنگ}) \;.$$

دراین‌صورت همنهشتی (۲) معادل است با

$$x^2 \equiv -a^*c(b \text{ هنگ}) \;. \qquad (۳)$$

فرض کنیم $b=p_1^{\alpha_1} \dots p_t^{\alpha_t}$ تجزیهٔ b به‌حاصلضرب توانهای اول متمایز باشد. به‌استناد قضیهٔ ماندهٔ چینی وقضیهٔ ۱.۴.۳ می‌دانیم که (۳) حلپذیر است اگر، وفقط اگر، به‌ازای $1 \leqslant i \leqslant t$،

$$x^2 \equiv -a^*c(p_i^{\alpha_i} \text{ هنگ}) \qquad (۴)$$

حلپذیر باشد. بعلاوه، بنابرتمرین ۱۱.۴.۳ ، می‌دانیم که اگر p_i فرد باشد، فقط‌وفقط وقتی (۴) حلپذیر است که بتوانیم

$$x^2 \equiv -a^*c(p_i \text{ هنگ}) \qquad (۵)$$

را حل کنیم، ومعادلهٔ اخیر حلپذیر است اگروفقط اگر $\left(\frac{-a^*c}{p_i}\right)=1$. بنابراین، می‌بینیم که‌معادلهٔ سیالهٔ(۱) هنگامی که ۱ = بمعم(a , b) و b فرد باشد حلپذیر است اگر،وفقط اگر، به‌ازای کلیهٔ اعداد اول p که $p|b$ ،

$$\left(\frac{-a^*c}{p}\right)=1 \;.$$

از این‌رو ، به‌عنوان مثال، اگر p عدد اول فردی باشد، آنگاه

$$x^2+py+c=0$$

جواب دارد اگر و فقط اگر $\left(\frac{-c}{p}\right)=1$.

بنابراین، با استفاده از محاسبات مثالهای ۴.۴ ، ۵.۴ ، و ۶.۴ ، می بینیم که

$x^2+43y-3=0$ حلپذیر نیست ،

$x^2+43y+40=0$ حلپذیر نیست ،

$x^2+1987y-20964=0$ حلپذیر است ،

و $x^2+py-5=0$ به‌ازای عدد اول p، حلپذیر است اگر، و فقط اگر، $p\equiv\pm1$ (هنگ ۵).

به‌عنوان مثال دوم، معادلهٔ

$$y^2=x^3+45 \tag{6}$$

را درنظر می گیریم و می‌خواهیم نشان‌دهیم که چگونه آگاهی ما از $\left(\frac{2}{p}\right)$ می‌تواند برای نشان‌دادن اینکه جوابی موجود نیست مورد استفاده واقع شود. توجه کنید که معادلهٔ (۶) حالت خاصی از معادلهٔ $y^2=x^3+k$ است. حالت $k=23$ دربخش ۳.۳ موردبحث واقع شده بود، و دراین‌حالت نیز روش مشابهی ارائه خواهیم داد. ما مثال دیگری از این نوع گنجانده‌ایم تا نشان دهیم که چگونه آگاهی ما از نماد لژاندر (یعنی، قانون تقابل) اغلب می‌تواند به‌طور جدی وناخواسته درمسئله‌ای راه‌یابد.

اینك نشان می‌دهیم که (۶) جواب ندارد. طرح برهان این است که نشان دهیم هریك از هشت دستهٔ ممکن مانده‌ها به‌هنگ ۸ برای x غیرممکن هستند. ابتدا کلیهٔ مانده‌های زوج ۰ ، ۲ ، ۴ ، ۶ را حذف می کنیم. این همان حذف امکان زوج بودن x است. اگر $x\equiv0$ (هنگ ۲) ، آنگاه $x^3\equiv0$ (هنگ ۸) (بنابر (۶)) ایجاب می کند که $y^2\equiv45\equiv5$ (هنگ ۸)، ولی‌این غیرممکن است زیرا یك مربع کامل، همنهشت ۰ ، ۱ ، یا ۴ است به‌هنگ ۸ . پس x نمی‌تواند زوج باشد. بعداً ، نشان می‌دهیم که ۵ یا ۱ $\neq x$ (هنگ ۸)زیرا، اگر $x\equiv1$ یا ۵ (هنگ ۸)، آنگاه $x\equiv1$ (هنگ ۴)، بنابراین $x^3\equiv1$ (هنگ ۴)، پس از (۶) نتیجه می‌شود $y^2\equiv46\equiv2$ (هنگ ۴) ، که باز غیرممکن است. بنابراین، تنها امکاناتی که برای x باقی می‌مانندعبارت‌اند از $x\equiv7$ (هنگ ۸) یا $x\equiv3$ (هنگ ۸) . این موارد احتیاج به‌فوت‌وفن ماهرانه‌ای دارند. ابتدا حالت $x\equiv7\equiv-1$ (هنگ ۸) را درنظر می گیریم. (۶) را به‌صورت

$$y^2-2\times3^2=x^3+27=(x+3)(x^2-3x+9) \tag{7}$$

می نویسیم. دراین‌صورت $x\equiv-1$ (هنگ ۸) ایجاب می کند که

$x^2-3x+9\equiv1+3+9\equiv-3$ (هنگ ۸) .

ازآنجا، نتیجه می‌شود که عددی مانند p که x^2-3x+9 را عاد می کند وجود دارد به‌قسمی که $p\equiv\pm3$ (هنگ ۸) ، زیرا درغیراین‌صورت $x^2-3x+9=p_1p_2\cdots p_r$، که در آن، به‌ازای کلیهٔ iها، کلیهٔ p_iها اعداد اول می باشند و $p_i\equiv\pm1$ (هنگ ۸) . (توجه داشته‌باشید که چون $x^2-3x+9\equiv-3$ (هنگ ۸) ، کلیهٔ p_iها باید فرد باشند.) اما دراین‌صورت $x^2-3x+9=p_1p_2\cdots p_r\equiv(\pm1)\cdots(\pm1)\equiv\pm1$ (هنگ ۸) ، که یك تناقض

است. پس، به‌ازای عدد اول $p\equiv\pm ۳ (\text{هنگ } ۸)$ که هم‌اکنون وجودش را اثبات کرده‌ایم، داریم $y^{۲}-۲\times ۳^{۲}\equiv ۰ (\text{هنگ } p)$. بنابراین، $\left(\frac{۲\times ۳^{۲}}{p}\right)=۱$*. ولی

$$۱=\left(\frac{۲\times ۳^{۲}}{p}\right)=\left(\frac{۲}{p}\right)\left(\frac{۳^{۲}}{p}\right)=\left(\frac{۲}{p}\right).$$

اما، مطابق قضیهٔ ۵.۳، می‌بینیم که $\left(\frac{۲}{p}\right)=۱$ اگر، وفقط اگر، $p\equiv\pm ۱ (\text{هنگ } ۸)$، که متناقض باانتخاب p است. بنابراین، x نمی‌تواند همنهشت ۷ به‌هنگ ۸ باشد. بالاخره، حالت $x\equiv ۳ (\text{هنگ } ۸)$ را درنظرمی‌گیریم. (۶) را به‌صورت

$$y^{۲}-۲\times ۶^{۲}=x^{۳}-۲۷=(x-۳)(x^{۲}+۳x+۹)$$

می‌نویسیم. مشاهده می‌کنید که چون $x\equiv ۳ (\text{هنگ } ۸)$، داریم

$$x^{۲}+۳x+۹\equiv ۳ (\text{هنگ } ۸).$$

بنابراین، مقداری مانند p که $x^{۲}+۳x+۹$ را عاد می‌کند موجود است به‌طوری که $p\equiv\pm ۳ (\text{هنگ } ۸)$* (همان استدلال‌فوق)، وبه‌ازای این p، داریم $\left(\frac{۲\times ۶^{۲}}{p}\right)=۱$، که به همان روش حالت قبلی به‌تناقض منجرمی‌شود. بنابراین، تمام دسته‌های مانده‌ها، به هنگ ۸ رد شدند، ومعادلهٔ $y^{۲}=x^{۳}+۴۵$ دراعدادصحیح جواب ندارد.

۵.۴ تمرینات

۱. کلیهٔ جوابهای معادلات سیالهٔ زیر را تعیین کنید:

(آ) $۵x^{۲}+۲x+۱۱y+۵=۰$.

(ب) $۳x^{۲}+۲۰x+۱۱y-۳=۰$.

(ج) $۷x^{۲}+۱۰x+۱۳y-۶=۰$.

۲. نشان‌دهید که معادلهٔ‌سیالهٔ $x^{۲}-۷xy+y^{۲}=۳$ جواب‌ندارد (ازهنگ ۵ استفاده کنید).

۳. کلیهٔ جوابهای معادلهٔ سیالهٔ زیر را بیابید:

$$۲x^{۲}+۳xy+۸y^{۴}+۱۳z=۰.$$

بیشک نشان خواهید دادکه کلیهٔ جوابها را به‌دست‌آورده‌اید. جواب:

$$(x ، y ، z)=(k ، k+۱۳t ، -k^{۲}-۱۹kt-۱۰۴t^{۲})$$

یا

$$(x ، y ، z)=(k ، -۳k+۱۳t ، -۵k^{۲}+۴۵kt-۱۰۴t^{۲})،$$

که k و t می‌توانند هرعدد صحیحی باشند.

---

* حالت $p=۳$ را جداگانه بحث‌کنید. -(مترجم).

۵

توابع حسابی

۱.۵ مقدمه

در فصول دوم تا چهارم ، مقدماتی‌ترین خواص اعداد صحیح را مطالعه کرده و نشان دادیم که چگونه حتی ساده‌ترین حقایق درمورد اعداد صحیح ما را به حل بعضی ازمعادلات سیاله هدایت می‌کنند . اجازه دهید موضوعات فصول قبل را با مطالعهٔ بعضی از ظریفترین خواص اعداد صحیح ، بدان گونه که در حقایق بنیادی مربوط به توابع حسابی منعکس شده‌اند ادامه دهیم .

به بیان ساده ، یك تابع حسابی تابعی است که به هرعدد صحیح مثبت n یك عدد حقیقی $f(n)$ مربوط می‌کند. برای اینکه معنی کامل منظور مارا درك کنید ، چند مثال در نظر می‌گیریم .

مثال ۱ : همهٔ توابع معمولی جبردبیرستانی توابع حسابی هستند. به‌عنوان‌مثال $f_1(n) = n$ ، $f_2(n) = n^2$ ، $f_3(n) = n^3$ ، و $f_4(n) = 1/n^2$ تماماً مثالهای ساده‌ای از توابع حسابی هستند.

مثال ۲ : فرض کنیم $\varphi(n)$ معرف تابع فی‌اویلر باشد . یعنی ، $\varphi(n)$ برابر است با تعداد اعداد صحیح مثبت نابیشتر از n که نسبت به n اول هستند ، دراین صورت $\varphi(n)$ یك تابع حسابی است.

مثال ۳: فرض کنیم $d(n)$ مساوی تعداد مقسوم علیه‌های مثبت عدد صحیح مثبت n باشد . دراین‌صورت $d(1) = 1$ ، $d(2) = 2$ (مقسوم‌علیه‌های مثبت ۲ ، اعداد ۱ و ۲ می‌باشند) ، $d(6) = 4$ (مقسوم علیه‌های مثبت ۶ ، اعداد ۱ ، ۲ ، ۳ ، و ۶ می‌باشند)، و اگر p عددی

اول باشد ، آنگاه $d(p)=۲$ (مقسوم علیه‌های مثبت p ، ۱ و p هستند).

مثال ۴: فرض کنیم $\sigma(n)$ مساوی مجموع مقسوم‌علیه‌های مثبت عدد صحیح مثبت n باشد. دراین صورت $\sigma(۱)=۱$ ، $\sigma(۲)=۳$ ، $\sigma(۶)=۱۲$ ، و اگر p عددی‌اول باشد ، آنگاه $\sigma(p)=p+۱$.

مثال ۵: به‌ازای عدد حقیقی r ، فرض کنیم $\sigma_r(n)$ مساوی مجموع قوای r مقسوم‌علیه‌های مثبت عدد صحیح مثبت n باشد. در این صورت $\sigma_۱(n)=\sigma(n)$ ، که در اینجا $\sigma(n)$ همان است که در مثال ۴ تعریف شد. همچنین ، $\sigma_۰(n)=d(n)$.

می‌توانیم به همین منوال ادامه دهیم و مثالهای بیشتری ازتوابع حسابی ارائه دهیم ، ولی اجازه دهید دراین لحظه ازاین امر خودداری کنیم و در عوض به این سؤال بدیهی که «چرا باید خواص توابع حسابی را مطالعه کنیم؟» بپردازیم .

اولا ، قبلا درفصل ۲ ، لازم آمده بود φ ، یعنی تابع اویلر را تعریف کنیم. این تابع شمارشی ازتعداد اعضا درهر دستگاه مخفف‌مانده‌ها به‌دست می‌داد (قضیهٔ ۲۵.۲.۳). همچنین، در حکم قضیهٔ اویلر (قضیهٔ ۲.۳.۳) ، که بالاخص ، دستوری، صریح برای عکس حسابی به‌ما داد ، به‌کار برده شده بود. دراین صورت ، واضح خواهدبودکه داشتن دستوری‌صریح برای $\varphi(n)$ به‌جا و مفید خواهد بود. یکی ازکاربردهای اساسی این نظریه‌که در این فصل بسط یافته به دست آوردن چنین دستوری است.

به عنوان دلیل دوم توجه می کنیم که توابع حسابی ، خواصی از اعداد صحیح را که اغلب ظریفتر از آنهایی هستند که تاکنون در مطالعهٔ اعداد صحیح به آنها برخورده‌ایم منعکس می‌کنند. به عنوان مثال ، تابع $d(n)$ را درنظر می‌گیریم . این تابع اندازه دوری یك عدد n را از اول بودن تعیین می کند ، زیرا چنانکه دیده‌ایم ، اگر p عددی اول باشد، آنگاه $d(p)=۲$ ، بالعکس به‌سهولت می‌بینیم که اگر $d(n)=۲$ ، آنگاه n عددی اول است. بنابراین $d(n)=۲$ اگر ، وفقط اگر ، n اول‌باشد. بعلاوه ، هرقدر $d(n)$ بزرگتر می‌شود به‌همان اندازه n از اول بودن دورتر می‌شود. بدین‌ترتیب ، می‌بینیم که تابع $d(n)$ اطلاعاتی، تا حدی نارسا، درمورد عدد صحیح n به دست می‌دهد.

یك دلیل دیگر برای مطالعهٔ توابع حسابی ارتباط نزدیك آنهاست با معادلات‌سیاله. مثالی دراین‌باره ذکر می کنیم. فرض‌کنیم n عدد صحیح مثبتی باشد. فرض‌کنیم می‌خواهیم معادلهٔ سیالهٔ

$$x^۲+y^۲+z^۲+w^۲=n \qquad (۱)$$

را حل‌کنیم. به عبارت دیگر در پی عددی مانند n هستیم که به صورت مجموع چهار مربع کامل بیان‌شود. لاگرانژ ثابت‌کردکه معادلهٔ (۱) همواره لااقل یك‌جواب دارد. ما این‌نتیجه را درفصل ۶ ثابت خواهیم کرد. ولی معادلهٔ (۱) چند جواب متمایز (x , y , z , w) دارد؟ فرض‌کنیم تعدادجوابها را به $r_۴(n)$ نشان‌دهیم. دراین‌صورت $r_۴(n)$یك تابع حسابی بسیار

جالبی خواهدبود. قضیهٔ لاگرانژ معادل با این‌حکم است که به‌ازای کلیهٔ nها، $۱ \leqslant r_{۴}(n)$، در واقع، می‌توان دستور کاملا صریحی برای $r_{۴}(n)$ بیان کرد، که ابتدا توسط ژاکوبی کشف‌شد، یعنی: فرض کنیم $\sigma^*(n)$ معرف مجموع مقسوم‌علیه‌های مثبت فرد n باشد. در این صورت قضیهٔ ژاکوبی حکم می‌کند که

$$r_{۴}(n)=\begin{cases} ۸\sigma^*(n) & \text{اگر } n \text{ فرد باشد} \\ ۲۴\sigma^*(n) & \text{اگر } n \text{ زوج باشد} \end{cases}$$

از این رو، مثلا، چون مقسوم‌علیه‌های فرد ۱۲ اعداد ۱ و ۳ هستند، می‌بینیم که

$$r_{۴}(۱۲)=۲۴\sigma^*(۱۲)=۲۴(۱+۳)=۹۶\cdot$$

بنابراین، معادلهٔ

$$x^{۲}+y^{۲}+z^{۲}+w^{۲}=۱۲$$

۹۶ جواب متمایز دارد. این جوابها عبارتند از $(۰, \pm ۲, \pm ۲, \pm ۲)$، $(\pm ۲, ۰, \pm ۲, \pm ۲)$، $(\pm ۲, \pm ۲, ۰, \pm ۲)$، $(\pm ۲, \pm ۲, \pm ۲, ۰)$، $(\pm ۱, \pm ۱, \pm ۱, \pm ۳)$، $(\pm ۱, \pm ۱, \pm ۳, \pm ۱)$، $(\pm ۱, \pm ۳, \pm ۱, \pm ۱)$ و $(\pm ۳, \pm ۱, \pm ۱, \pm ۱)$ که در آن تمامی حالات ممکن برای انتخاب علامتها مجاز می‌باشند. (متعلم می‌تواند این محاسبه را بررسی کند.) بنابراین، می‌بینیم که تابع حسابی $\sigma^*(n)$ مفتاحی برای تعداد جوابهای معادلهٔ سیالهٔ (۱) است. این‌مورد نمونهٔ تقریباً شاخصی برای ارتباط بین معادلات سیاله و توابع حسابی است.

بالاخره، یك دلیل برای مطالعهٔ توابع حسابی جنبهٔ تاریخی و سرگرم کنندهٔ آنها می‌باشد. خواص اعداد صحیح به صورتی که از راه مطالعهٔ توابع حسابی بیان شده‌اند، هزاران سال به توسط گروههای بسیار متنوعی از مردم، از جمله ریاضیدانانی که عشق به ریاضی داشته یا اهل تصوف پی‌گیری شده‌اند. خواص بعضی از توابع حسابی اغلب برای افسون خوشبختی، که طلسم نامیده می‌شوند، در خلال قرون وسطی حکاکی شده بودند. دربارهٔ مثالی از این قبیل، یعنی دربارهٔ اعداد تام و متحابه در بخش ۴.۵ بحث خواهیم کرد. برای صاحبنظران درنظریهٔ اعداد که عشق به این‌کار داشته‌اند، همواره کشف خواص توابع حسابی سرچشمهٔ علاقهٔ آنها بوده است، قسمتی به خاطر آسانی‌ای که به توسط آن شخص می‌تواند جداولی جمع‌آوری کند و به کمك آنها حدسیات ناشی از تجربه را پدید آورد. ما جدولی که ازراه کامپیوتر تهیه شده برای $\varphi(n)$، $d(n)$، و $\sigma(n)$ و تابعی دیگر، $\mu(n)$، که در بخش ۳ تعریف خواهیم کرد به ازای $n \leqslant ۱۰۰$ ضمیمه کرده‌ایم (جدول ۱).

۵. ۱ تمرینات

۱. مقادیر زیر را بدون استفاده از جدول ۱ که در آخر کتاب آمده است محاسبه کنید:

(آ) $d(۲۱)\cdot$ (ب) $d(۴۵)\cdot$ (ج) $d(۳۰۵)\cdot$

(د) $d(۱۸۰)\cdot$ (ه) $d(۳۶۸)\cdot$ (و) $d(۵۰۴)\cdot$

۲. مقادیر زیر را بدون استفاده‌از جدول ۱ که درآخر کتاب آمده است محاسبه کنید:

(آ) $\sigma(۳۸)$. (ب) $\sigma(۲۵)$. (ج) $\sigma(۲۵۳)$.

(د) $\sigma(۱۰۰)$. (ه) $\sigma(۱۲۸)$. (و) $\sigma(۲۹۷)$.

۳. (آ) به ازای $n = ۱ ، ۲ ، \ldots$ ، $d(۲^n)$ را محاسبه کنید.

(ب) به ازای $n = ۱ ، ۲ ، \ldots$ ، $d(۶^n)$ را محاسبه کنید.

(ج) نشان دهید که به ازای $n = ۱ ، ۲ ، ۳ ، \ldots$ ، $d(۶^n) = d(۲^n)\, d(۳^n)$.

۴. روابط زیر را تحقیق کنید:

(آ) $\sigma(۲۴) = \sigma(۸)\, \sigma(۳)$.

(ب) $\sigma(۷۲) = \sigma(۸)\, \sigma(۹)$.

(ج) $\sigma(۱۰۸) = \sigma(۴)\, \sigma(۲۷)$.

۵. حکم $r_۴(n) = ۸\, \sigma^*(n)$ (n فرد) ، $r_۴(n) = ۲۴\, \sigma^*(n)$ (n زوج) را درحالات خاص $n = ۶، ۱۵ ، ۲۱$ تحقیق کنید.

۵ . ۲ توابع حسابی ضربی

این مبحث را با تعریف دسته‌ای از توابع حسابی که شامل جالبترین توابع برای مقاصد ماست، یعنی توابع حسابی ضربی آغاز می‌کنیم. نشان خواهیم داد که تمام مثالهایی که دربخش ۱ مورد بحث واقع شده‌اند، در حقیقت، مشمول دراین طبقه ازتوابع حسابی هستند. از این رو در عین حال، با مطالعهٔ خواص توابع حسابی ضربی در حالت کلی، خواص تمامی توابع خاص راکه دربخش ۱ آورده‌ایم مطالعه خواهیم کرد.

تعریف ۱: فرض کنیم $f(n)$ یك تابع حسابی باشد. $f(n)$ را تابع ضربی گوییم مشروط براینکه هرگاه اعداد صحیح مثبت m و n طوری باشند که ۱ = بمم$(m ، n)$ آنگاه داشته باشیم

$$f(mn) = f(m)\, f(n) \qquad (۱)$$

مثال ۲: فرض کنیم به ازای تمام nهای مثبت $f(n) = n$. دراین صورت

$$f(nm) = nm = f(n)\, f(m).$$

بنابراین، می‌بینیم که معادلهٔ (۱) حتی بدون فرض ۱ = بمم$(m ، n)$ برقرار است. پس $f(n) = n$ ضربی است. ما آن دسته ازتوابع حسابی راکه برای آنها (۱) به ازای همهٔ مقادیر m و n برقرار است توابع ضربی قوی می‌نامیم. به همین ترتیب، اگر $g(n) = n^r$، که r عددی حقیقی (مثبت، منفی، و یا صفر) می‌باشد، آنگاه $g(n)$ ضربی قوی است.

قبل‌از اینکه متعلم به‌تصور غلطی برسد، باید توجه کند که کلیهٔ توابع‌حسابی که طبیعتاً ازنظریهٔ اعداد ناشی می‌شوند ضربی قوی‌نیستند. در واقع، $d(n)$ ، $\sigma(n)$ ، و $\varphi(n)$ضربی

هستند ولی نه ضربی قوی. به‌عنوان مثال ، ضربی قوی نبودن $d(n)$ بدیهی است ، چون‌که

$$d(۱۲)=d(۲\times۶)=۶ ،$$

در حالی‌که

$$d(۲)\times d(۶)=۲\times۴=۸ .$$

اثبات مستقیم ضربی بودن $d(n)$ امری است بسیار ساده . ولی یکی از مقاصد اصلی ما در این فصل این است که روش نسبتاً عادی و روشنی برای بررسی توابع حسابی ارائه دهیم. بنابراین ، ما آن روش را در مورد $d(n)$ اعمال می‌کنیم و برهان مستقیم را به‌عنوان تمرینی به عهدهٔ متعلم می‌گذاریم.

اجازه دهید ابتدا مزیتی را که ضربی بودن تابع مورد نظر نصیبمان خواهد کرد مورد توجه قرار دهیم . می‌نویسیم

$$n=p_۱^{a_۱}\ p_۲^{a_۲}\ \dots\ p_t^{a_t} ،$$

که در آن $p_۱$ ، $p_۲$ ، … ، p_t اعداد اول متمایز و $a_۱$ ، $a_۲$ ، … ، a_t اعداد صحیح مثبت هستند. در این صورت چون $f(n)$ ضربی است و چون $۱=$ بمعم$(p_۱^{a_۱} ، p_۲^{a_۲}\dots p_t^{a_t})$، داریم

$$f(n)=f(p_۱^{a_۱})f(p_۲^{a_۲}\ \dots\ p_t^{a_t}).$$

با ادامهٔ این روش ، می‌بینیم که

$$f(n)=f(p_۱^{a_۱})f(p_۲^{a_۲})\ \dots\ f(p_t^{a_t}).$$

بنابراین ، مسئلهٔ محاسبهٔ $f(n)$ به حالتی که n توانی از یك عدد اول باشد تبدیل می‌شود ، که معمولاً مسئلهٔ ساده‌تری است. نکتهٔ اخیر را چنین بیان می‌کنیم

قضیهٔ ۳ : فرض کنیم $f(n)$ تابعی ضربی باشد. می‌نویسیم

$$n=p_۱^{a_۱}\ p_۲^{a_۲}\dots\ p_t^{a_t} ،$$

که در آن $p_۱$ ، $p_۲$ ، … ، p_t اعداد اول متمایزند. در این صور

$$f(n)=f(p_۱^{a_۱})f(p_۲^{a_۲})\ \dots\ f(p_t^{a_t}).$$

اینك به ذکر نتیجه‌ای می‌پردازیم که در روش «عادی» ما برای استخراج دستوراتی برای توابع حسابی نقش اساسی دارد.

قضیهٔ ۴ : فرض کنیم $g(n)$ یك تابع‌حسابی ضربی باشد. تابع حسابی دیگری مانند $f(n)$ را با ضابطهٔ

$$f(n)=\sum_{d|n} g(d) ،$$

تعریف می‌کنیم ، در اینجا $\sum_{d|n}$ معرف مجموع روی کلیهٔ مقسوم‌علیه‌های مثبت n می‌باشد. در این صورت $f(n)$ یك تابع حسابی ضربی است.

توجه کنید که بنا بر تعریف

$$f(۱)=g(۱)\text{ ، }f(۲)=g(۱)+g(۲)\text{ ، }f(۳)=g(۱)+g(۳)\text{ ، }$$
$$f(۴)=g(۱)+g(۲)+g(۴)\text{ ، }f(۵)=g(۱)+g(۵)\text{ ، و}$$
$$f(۱۲)=g(۱)+g(۲)+g(۳)+g(۴)+g(۶)+g(۱۲)\cdot$$

بنابراین ،کاملا شگفت‌آور است که $f(n)$ ضربی می‌شود.

برهان قضیهٔ ۴: فرض کنیم ۱ = بمعم$(m\text{ ، }n)$. در این صورت وقتی که d مقسوم علیه‌های m را اختیارمی کند و e مقسوم‌علیه‌های n را، بسهولت می‌بینیم که de مقسوم‌علیه‌های mn را اختیار می‌کند ، و هر مقسوم علیه دقیقاً یکبار ظاهر می‌شود. (تمرین: یك طریق اثبات آن این است که ازیکتایی تجزیه استفاده کنیم.) حال ازاین مطلب ساده ، به صورت زیراستفاده می‌کنیم:

$$f(m)\,f(n)=\Big(\sum_{d|m}g(d)\Big)\Big(\sum_{e|n}g(e)\Big)$$ (بنا برتعریف f)

$$=\sum_{d|m}\sum_{e|n}g(d)g(e)$$ (با ضرب‌کردن مجموعها)

$$=\sum_{d|m}\sum_{e|n}g(de)$$ (زیرا g ضربی‌است؛ وروابط $d|m$ و$e|n$ و ۱ = بمعم(m,n)ایجاب می‌کنند که ۱ = بمعم(d,e))

$$=\sum_{c|mn}g(c)$$ (زیرا هنگامی که d و e ، بترتیب ،کلیهٔ مقسوم علیه‌های m و n را اختیار می‌کنند ، $c=de$ کلیهٔ مقسوم‌علیه‌های mn را یکبار وفقط یکبار اختیارمی کند.)

$$=f(mn)$$ (بنا برتعریف f).

بنابراین ، $f(n)$ ضربی است. ■

توجه کنید که عکس قضیهٔ ۴ هم درست است. تمرین ۱۲ در بخش ۳.۵ را ببینید. ذکرمراحل برهان بتفصیل ، به‌ازای مقادیرخاص m و n ، مثلا $m=۱۲$ و$n=۳۵$، آموزنده خواهد بود.

حال به طور صریح روش عادی خود را برای پرداختن به بعضی توابع حسابی بتفصیل ذکر می‌کنیم ، فرض‌کنیم $f(n)$ یك تابع حسابی باشد.

مرحلهٔ ۱: $f(n)$ را به صورت حاصلجمعی از یك تابع ضربی $g(n)$ برروی کلیهٔ مقسوم‌علیه‌های dی عدد n بیان می‌کنیم:

$$f(n)=\sum_{d|n}g(d)\cdot \tag{۲}$$

از قضیهٔ ۴ نتیجه بگیرید که $f(n)$ ضربی است .

مرحلهٔ ۲: فرض کنیم p عددی اول و $a(\geqslant 1)$ عددی صحیح باشد . با استفاده از (۲) ، $f(p^a)$ را محاسبه کنید. در واقع ،

$$f(p^a)=\sum_{i=0}^{a} g(p^i).$$

مرحلهٔ ۳: می‌نویسیم $n=p_1^{a_1}p_2^{a_2}\ldots p_t^{a_t}$ ، از ترکیب مرحلهٔ ۲ با قضیهٔ ۳ دستوری برای $f(n)$ استخراج می کنیم

$$f(n)=f(p_1^{a_1})f(p_2^{a_2})\ldots f(p_t^{a_t}).$$

(مرحلهٔ ۱ به ما اجازهٔ استفاده از قضیهٔ ۳ را می‌دهد.)

اینك اجازه دهید بعضی مثالهای بنیادی ازروش فوق را ارائه دهیم. یعنی، قرار دهیم $f(n)=d(n)$ و $f(n)=\sigma(n)$. در این حالت ، $f(n)$ «طبیعتاً» به‌صورتی داده شده‌است که می توانیم مرحلهٔ ۱ را انجام دهیم.

ابتدا حالت $f(n)=d(n)$ را درنظر خواهیم گرفت. چون $d(n)$ تعداد مقسوم‌علیه‌های مثبت n است ، این تابع مجموعی ازتابع ثابت ۱ روی کلیهٔ مقسوم‌علیه‌های مثبت n خواهد بود. یعنی ، اگر به ازای کلیهٔ مقادیر n ، $g(n)=1$ ، آنگاه

$$f(n)=\sum_{d|n} g(n) ;$$

یعنی ،

$$d(n)=\sum_{d|n} 1 .$$

چون ضربی بودن $g(n)$ روشن است ، نتیجه می گیریم که $f(n)=d(n)$ ضربی است. و مرحلهٔ ۱ را داریم. برای‌مرحلهٔ ۲ ، فرض‌کنیم p عددی اول $a(\geqslant 1)$ عدد صحیحی باشد. در این صورت

$$d(p^a)=\sum_{i=0}^{a} 1=a+1 .$$

یعنی، بدیهی است که p^a دارای $a+1$ مقسوم‌علیه ۱ ، p ، p^2 ، … ، p^a می‌باشد. بنابراین، از مرحلهٔ ۳ به دست می‌آوریم :

قضیهٔ ۵ : اگر $n=p_1^{a_1}p_2^{a_2}\ldots p_t^{a_t}$ ، که درآن p_1 ، p_2 ، … ، p_t اعداد اول متمایزند، آنگاه

$$d(n)=(a_1+1)(a_2+1)\ldots(a_t+1).$$

بعلاوه، $d(n)$ ضربی است.

اکنون، حالتی را در نظر می‌گیریم که $f(n)=\sigma(n)$. چون $\sigma(n)$ مجموع کلیهٔ مقسوم‌علیه‌های مثبت n است، این تابع مجموعی از تابع $g(m)=m$ روی مقسوم‌علیه‌های مثبت n است. یعنی،

$$f(n)=\sum_{d|n} g(d)=\sum_{d|n} d=\sigma(n).$$

چون، ضربی بودن $g(n)=n$ واضح است، نتیجه می‌گیریم که $f(n)=\sigma(n)$ ضربی است، مرحلهٔ ۱ را داریم. برای مرحلهٔ ۲ فرض کنیم p عددی اول و $a(\geqslant ۱)$ عددی صحیح باشد. در این صورت

$$\begin{aligned}\sigma(p^a)&=\sum_{d|p^a} d=\sum_{i=۰}^{a} p^i\\&=۱+p+p^۲+\cdots+p^a\\&=\frac{p^{a+۱}-۱}{p-۱}\end{aligned}$$

(آخرین عبارت، مجموع یک تصاعد هندسی است.) بنابراین، ازمرحلهٔ ۳ به‌دست‌می‌آوریم:

قضیهٔ ۶: اگر $n=p_۱^{a_۱}p_۲^{a_۲}\ldots p_t^{a_t}$ که در آن $p_۱$، $p_۲$، ...، p_t اعداد اول متمایز هستند، آنگاه

$$\begin{aligned}\sigma(n)&=(۱+p_۱+p_۱^۲+\cdots+p_۱^{a_۱})(۱+p_۲+p_۲^۲+\cdots+p_۲^{a_۲})\ldots\\&\qquad(۱+p_t+p_t^۲+\cdots+p_t^{a_t})\\&=\frac{p_۱^{a_۱+۱}-۱}{p_۱-۱}\ \frac{p_۲^{a_۲+۱}-۱}{p_۲-۱}\cdots\frac{p_t^{a_t+۱}-۱}{p_t-۱}.\end{aligned}$$

بعلاوه، $\sigma(n)$ ضربی است.

مثال ۷: فرض کنیم $n=۱۷۶۴۰=۲^۳\times ۳^۲\times ۵\times ۷^۲$. در این صورت

$$d(۱۷۶۴۰)=(۳+۱)(۲+۱)(۱+۱)(۲+۱)=۴\times ۳\times ۲\times ۳=۷۲$$

همچنین،

$$\begin{aligned}\sigma(۱۷۶۴۰)&=(۱+۲+۲^۲+۲^۳)(۱+۳+۳^۲)(۱+۵)(۱+۷+۷^۲)\\&=۱۵\times ۱۳\times ۶\times ۵۷=۶۶۶۹۰\end{aligned}$$

$$\sigma(۱۷۶۴۰)=\frac{۲^۴-۱}{۲-۱}\times\frac{۳^۳-۱}{۳-۱}\times\frac{۵^۲-۱}{۵-۱}\times\frac{۷^۳-۱}{۷-۱}$$

$$= ۱۵ \times ۱۳ \times ۶ \times ۵۷ = ۶۶۶۹۰ .$$

مثال دیگری ارائه می‌کنیم.

مثال ۸: به ازای عدد حقیقی r، $\sigma_r(n)$ را به صورت مجموع قوای r م مقسوم‌علیه‌های[1] n تعریف می‌کنیم. یعنی،

$$\sigma_r(n) = \sum_{d|n} d^r .$$

بنابراین، اگر $g(n) = n^r$، می‌بینیم کـه $g(n)$ ضربی است، و بنابراین $\sigma_r(n)$ ضربی است. اگر p عددی اول و $a(\geqslant ۱)$ عددی صحیح باشد، آنگاه

$$\sigma_r(p^a) = \sum_{d|p^a} d^r = \sum_{i=0}^{a} p^{ir} = \frac{p^{(a+1)r} - ۱}{p^r - ۱} .$$

(عبارت آخر ایجاب می‌کند کـه $r \neq ۰$.) پس، اگر $n = p_۱^{a_۱} p_۲^{a_۲} \dots p_t^{a_t}$، کـه $p_۱$، $p_۲$، ...، p_t اعداد اول متمایز هستند، آنگاه

$$\sigma_r(n) = (۱ + p_۱^r + p_۱^{۲r} + \dots + p_۱^{a_۱ r}) \dots (۱ + p_t^r + p_t^{۲r} + \dots + p_t^{a_t r})$$

$$= \frac{p_۱^{(a_۱+۱)r} - ۱}{p_۱^r - ۱} \dots \frac{p_t^{(a_t+۱)r} - ۱}{p_t^r - ۱} .$$

(عبارت آخر ایجاب می‌کند که $r \neq ۰$.) هرگاه درسمت چپ تساوی اخیر $r = ۰$ و $r = ۱$ اختیار شود آنگاه بترتیب $d(n)$ و $\sigma(n)$ به عنوان حالات خاص پدید می‌آیند.

۲.۵ تمرینات

۱. برهان قضیهٔ ۴ را مفصلا بنویسید، کلیهٔ جزئیات را به طـور صریح، به ازای $n = ۴$ و $m = ۹$، تحقیق کنید.

۲. مستقیماً ثابت کنید کـه اگر $n = p_۱^{a_۱} p_۲^{a_۲} \dots p_r^{a_r}$، به‌طوری که $p_۱$، $p_۲$، ...، p_r اعداد اول متمایز هستند، آنگاه

$$d(n) = (a_۱ + ۱)(a_۲ + ۱) \dots (a_r + ۱)$$

از این دستور نتیجه بگیرید که d ضربی است.

۳. نشان دهید که $d(n) = ۲$ اگر و فقط اگر n اول باشد.

۴. نشان دهید که $d(n)$ فرد است اگر و فقط اگر n یك مربع کامل باشد.

---

۱. مقسوم علیه‌های مثبت (مترجم).

۵. نشان دهید که به ازای هر عدد صحیح مثبت[1] m تعدادی نامتناهی عدد صحیح مانند n موجود است به‌طوری که $d(n)=m$. کوچکترین عددصحیح n که دارای این‌خاصیت باشد کدام است؟

۶. نشان دهید که $\prod_{d|n} d = n^{d(n)/2}$. ($\prod_{d|n} d$ برابراست باحاصلضرب کلیهٔ مقسوم‌علیه‌های مثبت n.)

۷. فرض کنیم $F(n)=\sum_{k|n} d(k)$. دستوری برای $F(n)$ به‌دست‌آورید. اگر $n=p_1\cdots p_r$، که p_iها اعداد اول متمایزاند، آنگاه مقدار $F(n)$ چه خواهد شد؟

۸. ثابت کنید که $\sum_{d|n} 1/d = \sigma(n)/n$.

۹. فرض کنیم $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$، و p_1، ...، p_r اعداد اول متمایز باشند. ملاحظه می‌کنید که $m|n$ اگر و فقط اگر $m=p_1^{\nu_1}p_2^{\nu_2}\cdots p_r^{\nu_r}$ با این شرط که $0\leqslant \nu_i \leqslant a_i$ $(1\leqslant i \leqslant r)$ و بنابراین

$$\sigma(n)=\sum_{\nu_1=0}^{a_1}\sum_{\nu_2=0}^{a_2}\cdots\sum_{\nu_r=0}^{a_r} p_1^{\nu_1}p_2^{\nu_2}\cdots p_r^{\nu_r}$$
$$=\sum_{\nu_1=0}^{a_1}\cdots\sum_{\nu_{r-1}=0}^{a_{r-1}} p_1^{\nu_1}\cdots p_{r-1}^{\nu_{r-1}}\sum_{\nu_r=0}^{a_r} p_r^{\nu_r}$$

دستور قضیهٔ ۶ را برای $\sigma(n)$ نتیجه‌گیری کنید. از این‌دستور نتیجه بگیرید که $\sigma(n)$ ضربی است.

۱۰. به ازای هر تابع حسابی $f(n)$ نشان دهید که

$$\sum_{d|n} f(d)=\sum_{d|n} f\left(\frac{n}{d}\right)$$

۱۱. اگر $n=p_1p_2\cdots p_k$ (p_1، p_2، ...، p_k، کـه لزوماً متمایز نیستند، اعداد اول می‌باشند) قرار دهید

$$\lambda(n)=(-1)^k.$$

(بنابراین $\lambda(2)=-1$، $\lambda(4)=(-1)^2=1$، $\lambda(12)=(-1)^3=-1$). قراردهید $\lambda(1)=1$.

(آ) نشان دهید که $\lambda(n)$ ضربی قوی است.

(ب) نشان دهید که

$$F(n)=\sum_{d|n}\lambda(d)=\begin{cases} 1 & \text{اگر } n \text{ مربع کامل باشد} \\ 0 & \text{درغیراینصورت}\end{cases}$$

---

۱. ناچاریم قیدکنیم $m\geqslant 2$ زیرا اگر $m=1$، آنگاه فقط ۱ و ۱− در $d(n)=1$ صدق می‌کنند (مترجم).

۱۲. اگر $n=p_1p_2\cdots p_k$، که p_1، ...، p_k اعداد اول‌هستند، قرارمی‌دهیم $\nu(n)=2^k$ (قرار دهید $\nu(1)=1$).

(آ) نشان دهید که $\nu(n)$ ضربی قوی است.

(ب) عبارتی را برای $\sum_{d|n}\nu(d)$ نتیجه بگیرید.

۱۳. اگر $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ که p_1، p_2، ...، p_k اعداد اول متمایز هستند، و t عددی صحیح است، قرار دهید

$$\omega(n)=t^k.$$

(قرار دهید $\omega(1)=1$.)

(آ) نشان دهید که $\omega(n)$ ضربی است.

(ب) نشان دهید که به ازای n به صورت فوق

$$\sum_{d|n}\omega(d)=(1+a_1t)(1+a_2t)\cdots(1+a_kt).$$

۱۴. فرض کنیم p یك عدد اول باشد. تعریف می کنیم

$$Q(n)=\begin{cases}0 & \text{اگر } p|n,\\ \left(\dfrac{n}{p}\right) & \text{اگر } p\nmid n.\end{cases}$$

فرض کنیم $F(n)=\sum_{d|n}Q(d)$

(آ) نشان دهید که Q ضربی است.

(ب) $F(p^k)$ را به ازای $k=1, 2, \ldots$ محاسبه کنید.

(ج) فرض کنیم $q\neq p$ عددی اول باشد. با در نظر گرفتن حالات $\left(\dfrac{q}{p}\right)=1$ و $\left(\dfrac{q}{p}\right)=-1$، دستوری برای $F(q^k)$، به ازای $k=1, 2, \ldots$ به دست آورید.

(د) به ازای $n=1, 2, \ldots$ عبارتی برای $F(n)$ به دست آورید.

(ه) بالاخص، تابع فوق را به صورت $F_p(n)$ بنویسید؛ نشان دهید که اگر p و q اعداد اول متمایز باشند و یکی از آنها همنهشت ۱ به هنگ ۴ باشد، آنگاه

$$F_p(q^k)=F_q(p^k).$$

اگر $p\equiv q\equiv 3$ (هنگ ۴)، آیا همین نتیجه برقرار است؟

۱۵. برای توابع‌حسابی f و g، تابع حسابی دیگری راکه به $f*g$ نمایش داده می‌شود (به نام همنورد f و g) به توسط

$$(f*g)(n)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right)$$

تعریف می‌کنیم. نتایج زیر را، به ازای توابع حسابی f، g، h ثابت کنید:

(آ) $f*g=g*f$.

(ب) $(f*g)*h=f*(g*h)$.

(ج) $(f+g)*h=f*h+g*h$. (بنا بر تعریف $(f+g)(n)=f(n)+g(n)$.)

(د) ضربی بودن f و g ایجاب می‌کند که $f*g$ ضربی باشد.

توابع خاص $I(n)=n$، $I_k(n)=n^k$، $\mathbf{1}(n)=1$ را تعریف می‌کنیم.

(ه) ضربی بودن f ایجاب می‌کند که $\mathbf{1}*f$ ضربی باشد.

(و) $d=\mathbf{1}*\mathbf{1}$. (ز) $\sigma=\mathbf{1}*I$. (ح) $\sigma_k=\mathbf{1}*I_k$.

(ط) اگر f ضربی قوی باشد، آنگاه

$$(f*f)(n)=f(n)d(n).$$

(ی) $\sigma*d$ را محاسبه کنید.

(ك) $I_k*I_l=n^l\sigma_{k-l}(n)$.[1]

۱۶. نشان دهید که $d(n)\leqslant ۲\sqrt{n}$. (راهنمایی: اگر $n=kl$، آنگاه k یا l، نابیشتر از $\sqrt{n}$ است.)

۱۷. نشان دهید که تعدادی نامتناهی عدد صحیح n موجودند به طوری که

$$d(n)\geqslant \log n/\log ۲.$$

۱۸**. نشان دهید که به‌ازای هر عدد صحیح k، یک‌عدد ثابت $C(>0)$ وجود دارد به‌طوری که تعدادی نامتناهی عدد صحیح n موجودند که در $d(n)\geqslant C(\log n)^k$ صدق می‌کنند.

۱۹. نشان دهید که به ازای کلیهٔ مقادیر n

$$n\leqslant \sigma(n)\leqslant n^۲.$$

۲۰. فرض کنیم $f(n)$ معرف تعداد جوابهای متمایز به‌هنگ n ازهمنهشتی $x^۲\equiv a$ (هنگ n) باشد

(آ) نشان دهید که $f(n)$ ضربی است.

(ب) دستوری برای $f(n)$ بیابید.

۲۱. فرض کنیم $g(x)$ بسجملهٔ دلخواهی باضرایب صحیح باشد و فرض کنیم $f_g(n)$ معرف تعداد جوابهای متمایز به هنگ n از همنهشتی $g(x)\equiv 0$ (هنگ n) باشد. نشان دهید که $f_g(n)$ ضربی است.

۲۲*. فرض کنیم $\lambda(n)$ همان تابع نظریهٔ اعدادی تمرین ۱۱ باشد. نشان دهید که

---

۱. در طرف اول باید $(I_k*I_l)(n)$ باشد (مترجم).

$$\sum_{n=1}^{x} \lambda(n)\left[\frac{x}{n}\right]=[\sqrt{x}] \cdot$$

۳.۵ دستور عکس موبیوس[1]

تاکنون ما ازتوابع حسابی که اساساً به‌صورت مجموعی ازیك تابع ضربی، برروی مقسوم علیه‌های یك عدد صحیح تعریف شده بودند بحث‌کردیم. اما ، همواره چنین نیست. به‌عنوان مثال ، $\varphi(n)$ عبارت آشکاری به‌این شکل‌ندارد، وبنا براین واضح نیست که‌روشی راکه در فوق طرح کردیم ، دراین مورد، چگونه به‌کار بندیم . به کار بستن این روش برای به دست آوردن دستوری برای $\varphi(n)$ ، یکی از محرکهای اولیهٔ ما دراین بخش است.

نکتهٔ مهم این‌است که عبارت نسبتاً روشنی ازنوع عبارت مورد نظر، منتهی به‌صورت «قهقرایی» موجود است. مثلا، در قضیهٔ ۷ نشان خواهیم داد که

$$n=\sum_{d\mid n}\varphi(d) \cdot$$

از این‌رو، سؤال کلی زیر مطرح می‌شود : فرض‌کنیم به ازای کلیهٔ اعـداد صحیح مثبت n،

$$f(n)=\sum_{d\mid n} g(d) \cdot \tag{۱}$$

آیا می‌توانیم $g(n)$ را برحسب $f(n)$ تعیین‌کنیم ؟ با عبارتی خالی از دقت، می‌پرسیم آیا می‌توانیم این معادله را برای $g(n)$ برحسب $f(n)$ «حل» کنیم ؟ در این بخش مـا به این پرسش پاسخ مثبت خواهیم داد. نتیجه همان چیزی است کـه دستور عکس موبیوس نامیده می‌شود .

پیش ازاینکه جلوتر برویم، اجازه دهید خود را متقاعد سازیم کـه ، حداقل به طور اصولی، می‌توانیم از (۱) برای محاسبهٔ $g(n)$ ، با داشتن $f(n)$ ، استفاده کنیم. بنابر(۱)، به ازای $n=1$ ، می‌بینیم که

$$g(1)=f(1) \cdot \tag{۲}$$

به ازای $n=2$ ، می‌بینیم که

$$f(2)=g(1)+g(2) ,$$

پس، بنابر (۲) ،

$$g(2)=f(2)-f(1) \cdot \tag{۳}$$

به ازای $n=3$ ، (۱) نتیجه می‌دهد

$$f(3)=g(1)+g(3) ,$$

1. Mobius

پس، بنا بر (۲)،

$$g(۳)=f(۳)-f(۱).$$

به ازای $n=۴$، (۱) نتیجه می‌دهد

$$f(۴)=g(۱)+g(۲)+g(۴),$$

پس، بنا بر (۲) و (۳)،

$$\begin{aligned} g(۴)&=f(۴)-g(۱)-g(۲) \\ &=f(۴)-f(۱)-(f(۲)-f(۱))=f(۴)-f(۲). \end{aligned}$$

اگر به‌همین روش پیش‌رویم، می‌توانیم، به‌ازای مقدار دلخواه n، $g(n)$ را برحسب $f(n)$ محاسبه کنیم. ولی آیا الگویی برای این‌دستورات وجود دارد؟ در واقع چنین الگویی‌وجود دارد، واین الگو درسال ۱۸۳۲ میلادی توسط موبیوس ریاضیدان آلمانی تعیین شده است. نامبرده آن را برحسب چیزی بیان کرده است که هم اکنون تابع موبیوس، $\mu(n)$، نامیده می‌شود. تعریف او ممکن است به نظر، اندکی عجیب آید. ولی خیلی ساده است، و باید به‌خاطر داشته باشیم که‌مسئلهٔ حل (۱) برای $g(n)$ برحسب $f(n)$ سبب‌تعریف آن شده‌است.

تعریف ۱: فرض کنیم n عدد صحیح مثبتی باشد. تابع موبیوس، $\mu(n)$، به صورت زیر تعریف‌می‌شود

$$\mu(۱)=۱,$$

$$\mu(n)=\begin{cases} ۰, & \text{اگر } n \text{ برمربع یک‌عدد اول بخشپذیر باشد} \\ (-۱)^t, & \text{اگر } n=p_۱p_۲\cdots p_t\text{، که‌درآن } p_۱,p_۲,\ldots,p_t \text{ اعداداول‌متمایزمی‌باشند} \end{cases}$$

بدین ترتیب، مثلاً، $\mu(۲)=-۱$، $\mu(۳)=-۱$، $\mu(۴)=۰$، $\mu(۵)=-۱$، و $\mu(۶)=۱$. مامقادیر $\mu(n)$ را به ازای کلیهٔ nهای نابیشتر از ۱۰۰ درجدول ۱ درآخر کتاب‌ضمیمه کرده‌ایم. چنانکه هم‌اکنون خواهیم دید، تابع حسابی $\mu(n)$ تابع مهمی است. قبل ازاینکه اصل‌مسئله را حل‌کنیم بایستی بعضی خواص $\mu(n)$ را به دست آوریم.

قضیهٔ ۴: $\mu(n)$ ضربی است.

برهان: فرض‌کنیم m و n دوعدد صحیح مثبت باشند به طوری که (m, n)بمم $=۱$. اگر $n=۱$، آنگاه چون $\mu(۱)=۱$، داریم:

$$\mu(mn)=\mu(m)=\mu(m)\mu(۱)=\mu(m)\mu(n).$$

بدین ترتیب، می‌توانیم فرض‌کنیم $m>۱$ و $n>۱$. سپس فرض می‌کنیم p عددی اول باشد و $p^۲|n$. دراین صورت، البته، $p^۲|mn$، وبنابراین، چون $\mu(n)=۰$،

$$\mu(mn)=0=\mu(m)\times 0=\mu(m)\mu(n)\,.$$

اینك می‌توانیم فرض کنیم m و n هر دو برمربع هیچ عــدد اولی بخشپذیر نیستند. در این صورت‌می‌توانیم بنویسیم $m=p_1p_2\cdots p_r$ و $n=q_1q_2\cdots q_s$ ، که p_1 ، ... ، p_r اعداد اول متمایز و q_1 ، ... ، q_s اعداد اول متمایز هستند. پس، چون ۱ = بمم$(m ، n)$ هیچ p_i نمی‌تواند یك q_j باشد. بنابراین $mn=p_1\cdots p_rq_1\cdots q_s$ حاصلضربی از اعــداد اول است،که در آن کلیهٔ اعداد اول متمایزند. بدین ترتیب

$$\mu(mn)=(-1)^{r+s}=(-1)^r(-1)^s=\mu(m)\mu(n)\,. \qquad ■$$

قضیهٔ ۳ : فرض کنیم n عدد صحیح مثبتی باشد. دراین صورت

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{اگر } n=1\\ 0 & \text{اگر } n>1\end{cases}$$

برهان : تابع حسابی $f(n)$ را با ضابطهٔ

$$f(n)=\sum_{d|n}\mu(d)$$

تعریف می‌کنیم، $f(n)$ را با روشی که دربخش ۲ مطرح شده محاسبه می‌کنیم. اولا ، $\mu(n)$ تابعی است ضربی. پس، بنابر قضیهٔ ۴.۲ ، $f(n)$ ضربی است . اما اگر p عــددی اول و $a(\geqslant 1)$ عددی صحیح باشد ، آنگاه

$$f(p^a)=\sum_{d|p^a}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^a)=1-1=0$$

زیــرا که، $\mu(1)=1$ و $\mu(p)=-1$ و $p^2|p^2$ ، $p^2|p^3$ ، ... ، $p^2|p^a$ ، و بنابراین جملات $\mu(p^i)$ $(i\geqslant 2)$ صفر می‌باشند . بالاخــره ، اگــر $n=p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ کــه p_1 ، p_2 ، ... ، p_t اعداد اول متمایزند ، آنگاه

$$f(n)=f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_t^{a_t})=0\times 0\times\cdots\times 0=0\,.$$

همچنان روشن‌است‌که $f(1)=\mu(1)=1$ ، قضیهٔ ۳ به‌طور کامل ثابت می‌شود. ■

حال از تابع موبیوس استفاده می‌کنیم تابه پرسشی که درآغاز این بخش مطرح شده بود پاسخ گوییم.

قضیهٔ ۴ (دستور عکس موبیوس) : فرض کنیم $g(n)$ تابع حسابی دلخواهی باشد و $f(n)$ به توسط

$$f(n)=\sum_{d|n}g(d)$$

داده شده باشد. دراین صورت

$$g(n)=\sum_{d|n}\mu(d)\,f\left(\frac{n}{d}\right).$$

(توجه: لازم نیست که $g(n)$ ضربی باشد.)

برهان : واضح است که داریم

$$\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\left(\sum_{c|(n/d)}g(c)\right)$$
$$=\sum_{d|n}\ \sum_{c|(n/d)}\mu(d)g(c)$$

جمع مضاعف آخری روی کلیهٔ زوجهای اعداد صحیح مثبت $(c\,،\,d)$ انجام می‌شود به‌طوری که $d|n$ و $c|(n/d)$. و این همان جمع روی کلیهٔ زوجهایی است از اعداد صحیح مثبت $(c\,،\,d)$ به طوری که $cd|n$ (تمرین). بنابراین، جمع مضاعف را به طریق زیــر محاسبه می‌کنیم . ابتدا ، روی کلیهٔ c هایی که n را عاد می‌کنند جمع می‌بندیم، و به ازای هریك از مقادیر ثابت c ، روی dهایی جمع‌بندی می‌کنیم که $d|(n/c)$. از این‌رو می‌بینیم که

$$\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{c|n}\ \sum_{d|(n/c)}\mu(d)g(c)$$
$$=\sum_{c|n}g(c)\left(\sum_{d|(n/c)}\mu(d)\right).$$

بنابر قضیهٔ ۳ ، حاصلجمع داخلی برابر صفر است، مگر آنکه $n/c=۱$ ، که دراین حالت برابر ۱ است. پس، کلیهٔ جملات در مجموع روی c صفر هستند ، باستثنای جمله‌ای کـه با $c=n$ متناظر است. بنابراین ،

$$\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)=g(n)\sum_{d|1}\mu(d)=g(n)\,. \qquad \blacksquare$$

اینك چند مثال برای کاربرد دستور عکس موبیوس می‌آوریم .

مثال ۵ : چون $d(n)=\sum_{e|n}1$ ، می‌توانیم قراردهیم $g(n)=1$ و $f(n)=d(n)$ و نتیجه بگیریم که

$$\sum_{e|n}\mu(e)d\left(\frac{n}{e}\right)=1\,,$$

حقیقتی که به هیچ وجه بدیهی نیست.

مثال ۶: چون $\sigma(n)=\sum_{d|n} d$، می‌توانیم قراردهیم $g(n)=n$ و $f(n)=\sigma(n)$ و نتیجه بگیریم که

$$\sum_{d|n}\mu(d)\sigma\left(\frac{n}{d}\right)=n\ .$$

حال بحث خود را دربارهٔ تابع فی اویلر، $\varphi(n)$، تکمیل می‌کنیم. همچنانکه قبلا ذکر شد، به نتیجهٔ زیر احتیاج داریم:

قضیهٔ ۷: فرض کنیم n عدد صحیح مثبتی باشد. دراین صورت

$$n=\sum_{d|n}\varphi(d)\ . \tag{۴}$$

قبل از اثبات قضیهٔ ۷، اجازه دهید ازآن وهمچنین از دستور عکس موبیوس و روش بخش ۲ برای استخراج خواص بنیادی $\varphi(n)$ استفاده کنیم.

ابتدا، دستور عکس موبیوس را با قراردادن $g(n)=\varphi(n)$ و $f(n)=n$ درمعادلهٔ (۴) به کار می‌بریم تا تساوی زیر را به دست آوریم

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$$

$$=n\sum_{d|n}\frac{\mu(d)}{d}\ . \tag{۵}$$

اینك ما در شرایطی هستیم که می‌توانیم روش بخش ۲ را به‌کار بریم. اول اینکه، $\mu(n)$ ضربی و تابع $g(n)=1/n$ نیز ضربی است. بدین ترتیب، تابع $h(n)=\mu(n)/n$ ضربی می‌باشد. از معادلهٔ (۵) وقضیهٔ ۴.۲ نتیجه می‌گیریم که $k(n)=\varphi(n)/n$، و بنابراین، سرانجام، $\varphi(n)=nk(n)$ ضربی است. حال اگر p عددی اول و $a\geqslant(1)$ عددی‌صحیح باشد، آنگاه

$$\varphi(p^a)=p^a\sum_{d|p^a}\frac{\mu(d)}{d}=p^a\left(\frac{\mu(1)}{1}+\frac{\mu(p)}{p}+\frac{\mu(p^2)}{p^2}+\dots+\frac{\mu(p^a)}{p^a}\right)$$
$$=p^a\left(1-\frac{1}{p}\right).$$

بالاخره، اگر $n=p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}$، که p_1، p_2، ...، p_t اعداد اول‌متمایزند، آنگاه

$$\varphi(n)=\varphi(p_1^{a_1})\varphi(p_2^{a_2})\dots\varphi(p_t^{a_t})$$

$$=p_۱^{a_۱}\left(۱-\frac{۱}{p_۱}\right)p_۲^{a_۲}\left(۱-\frac{۱}{p_۲}\right)\cdots p_t^{a_t}\left(۱-\frac{۱}{p_t}\right)$$
$$=n\left(۱-\frac{۱}{p_۱}\right)\left(۱-\frac{۱}{p_۲}\right)\cdots\left(۱-\frac{۱}{p_t}\right)$$
$$=p_۱^{a_۱-۱}(p_۱-۱)p_۲^{a_۲-۱}(p_۲-۱)\cdots p_t^{a_t-۱}(p_t-۱)\,.$$

می‌توانیم نتایج حاصل را در قضیهٔ زیر ذکر کنیم.

قضیهٔ ۸ : اگر $n=p_۱^{a_۱}p_۲^{a_۲}\cdots p_t^{a_t}$ و $p_۱$ ، $p_۲$ ، ...، p_t اعداد اول متمایز باشند، آنگاه

$$\varphi(n)=n\left(۱-\frac{۱}{p_۱}\right)\left(۱-\frac{۱}{p_۲}\right)\cdots\left(۱-\frac{۱}{p_t}\right)$$
$$=p_۱^{a_۱-۱}(p_۱-۱)p_۲^{a_۲-۱}(p_۲-۱)\cdots p_t^{a_t-۱}(p_t-۱)$$

بعلاوه، $\varphi(n)$ ضربی است. دیگر اینکه، داریم

$$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}\,.$$

مثال ۹ :
$$\varphi(۴۳۲۰)=\varphi(۲^۶\times ۳^۳\times ۵)=۲^۴(۲-۱)۳^۲(۳-۱)۵^۰(۵-۱)$$
$$=۱۱۵۲$$

کلیهٔ استدلالهای فوق براساس قضیهٔ ۷، که هنوز آن را ثابت نکرده‌ایم، صورت گرفته بود. ولی، قبل از اینکه بتوانیم قضیهٔ ۷ را ثابت کنیم، مطلب زیر را احتیاج داریم:

لم ۱۰ : فرض کنیم n یك عدد صحیح مثبت باشد و d مقسوم علیهی از n. دراین صورت تعداد اعداد صحیح k که $۱\leqslant k\leqslant n$ و $d=$ بمعم$(k ، n)$ برابر است با $\varphi(n/d)$.

برهان: اگر $d=$ بمعم$(k ، n)$، آنگاه $d|k$ و $۱=$ بمعم$(k/d ، n/d)$. بعلاوه اگر $۱\leqslant k\leqslant n$، آنگاه $۱\leqslant k/d\leqslant n/d$. بنابراین، هرعدد صحیح k که درشرایط لم صدق کند درشرایط $d|k$ ، $۱=$ بمعم$(k/d ، n/d)$ و $۱\leqslant (k/d)\leqslant n/d$ صدق می کند. اگر k یك چنین عدد صحیحی باشد، آنگاه $k=k'd$ و k' در $۱=$ بمعم$(k' ، n/d)$ و $۱\leqslant k'\leqslant n/d$ صدق می کند. بالعکس، عدد k' داده شده است به‌طوری که $۱=$ بمعم$(k' ، n/d)$ و $۱\leqslant k'\leqslant n/d$ ، عدد صحیح $k=k'd$ در شرایط این لم صدق می کند. بنابراین، تعداد kهایی که در این لم صدق می کنند برابر است با تعداد اعداد صحیح k' به‌طوری که

$n/d \geqslant k' \geqslant ۱$ و ۱ = بمعم$(k' \text{ ، } n/d)$. واضح است که این عدد $\varphi(n/d)$ می‌باشد. ■

برهان قضیهٔ ۷: اول توجه کنید که هرعدد صحیح k که $n \geqslant k \geqslant ۱$. به ازای یك وفقط یك مقسوم علیه d از n ، در d = بمعم$(k \text{ ، } n)$ صدق می کند. لذا ، بنابر لم ۱۰ ، داریم

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d'|n} \varphi(d')$$

زیرا وقتی که d کلیهٔ مقسوم علیه‌های n را اختیار کند، $d' = n/d$ نیز آنها را اختیار خواهد کرد . ■

۳.۵ تمرینات

۱. فرض کنیم $f(n)$ تابعی حسابی باشد، و فرض کنیم $h(n) = \sum_{d|n} f(d)$. $f(۲۴)$ را برحسب h محاسبه کنید.

۲. دستور عکس موبیوس را به ازای $n \leqslant ۱۰$ ، با برهان مستقیمی که در متن ارائه شده است ثابت کنید.

۳. $\mu(۵)$ ، $\mu(۶۴)$ ، $\mu(۳۹)$ و $\mu(۳۰)$ را محاسبه کنید.

۴. $\varphi(۲)$ ، $\varphi(۵)$ ، $\varphi(۴۷)$ ، و $\varphi(۱۴۴)$ را محاسبه کنید.

۵. نشان دهید که به ازای $n > ۲$ ، $\varphi(n)$ زوج است .

۶. فرض کنیم $f(n)$ تابعی ضربی باشد.

(آ) نشان دهید که $\sum_{d|n} \mu(d) f(d) = \prod_{p|n \text{ ، اول } p} (۱ - f(p))$.

(ب) نشان دهید که $\sum_{d|n} \mu(d)/d = \prod_{p|n \text{ ، اول } p} (۱ - (۱/p))$.

۷. فرض کنیم $\omega(n)$ معرف تعداد عوامل اول متمایز n باشد . نشان دهید که

$$\sum_{d|n} |\mu(d)| = ۲^{\omega(n)} .$$

۸. نشان‌دهید که $\sum_{d|n} \mu(d)\varphi(d) = (-۱)^{\omega(n)} \prod_{p|n} (p - ۲)$ ، که‌درآن $\omega(n)$ توسط تمرین ۷ تعریف شده است.

۹. نشان دهید که $\sum_{d|n} \mu^۲(d)/d = \prod_{p|n} (۱ + (۱/p))$.

۱۰. نشان‌دهید که تعداد کسرهای تحویل‌ناپذیر a/b که $۰ \leqslant a/b < ۱$ و b ثابت‌باشد درست $\varphi(b)$ است.

۱۱. یك حدس مشهور از مرتنس[1] بیان می کند که به ازای هر r ،

$$\left|\sum_{n=۱}^{r} \mu(n)\right| < \sqrt{r}$$

1. Mertens

حدس مرتنس را به ازای $r \leqslant ۳۰$ تحقیق کنید. یك برنامهٔ کامپیوتری برای بررسی حدس مرتنس به ازای r های کوچکتر از حد مفروضی بنویسید. این حدس به ظاهر ساده، خیلی دشوار است. در حقیقت، این حدس مستلزم فرض معروف به فرض ریمان است که یکی از مشهورترین مسائل حل نشده در ریاضیات می باشد. به نظر می‌رسد که ظاهراً حدس مرتنس غلط باشد، ولی کامپیوترهای امروزه سرعت کافی ندارند تا اجازهٔ یك تحقیق دامنه‌دار وجامعی را برای پیدا کردن یك مثال نقض به ما بدهند.

۱۲. فرض کنیم $f(n)$ یك تابع حسابی باشد و $F(n)$ را با

$$F(n)=\sum_{d|n} f(d)$$

تعریف می کنیم، نشان دهید که اگر $F(n)$ ضربی باشد، آنگاه $f(n)$ ضربی است.

۱۳. فرض کنیم n عدد صحیح مثبت ثابتی باشد. نشان‌دهید که فقط تعدادی متناهی عدد صحیح x وجود دارد به طوری که $\varphi(x)=n$.

۱۴. فرض کنیم $f(n)$ یك تابع حسابی باشد و فرض کنیم به ازای کلیهٔ مقادیر n ،

$$\sum_{d|n} f(d)=n .$$

نشان دهید که $f(n)=\varphi(n)$.

۱۵. اثبات این امر که $\varphi(m)|m-۱$ ، آنگاه m اول است، مسئلهٔ حل نشده‌ای است. نشان دهید که اگر $\varphi(m)|m-۱$ ، آنگاه m خالی ازمربع است.

۱۶. ثابت کنید که

$$\sum_{d=۱}^{n}\varphi(d)\left[\frac{n}{d}\right]=\frac{n(n+۱)}{۲}$$

(راهنمایی: از استقرا روی n استفاده کنید.)

۱۷. به ازای اعداد صحیح مثبت n و k ، قرار می‌دهیم

$$\sigma_k^*(n)=\sum_{i=۱,\ (i,n)_{\text{بمعم}}=۱}^{n} i^k$$

(آ) نشان دهید که

$$\sum_{d|n}\frac{\sigma_k^*(d)}{d^k}=\frac{۱^k+۲^k+\cdots+n^k}{n^k}$$

(ب) از (آ) و دستور عکس موبیوس برای محاسبهٔ $\sigma_۱^*(n)$ ، $\sigma_۲^*(n)$ ، و $\sigma_۳^*(n)$ استفاده کنید

۱۸. ثابت کنید که

$$\sum_{a=۱,\ (a,n)_{\text{بمعم}}=۱}^{n} a=\frac{۱}{۲}n\varphi(n)$$

۱۹. فرض‌کنیم a و b اعداد صحیح مثبت‌باشند وفرض‌کنیم c معرف حاصلضرب کلیهٔ اعداد اولی‌که هم a و هم b را عاد می‌کنند باشد.

(آ) ثابت‌کنید که

$$\varphi(ab)=\varphi(a)\varphi(b)\frac{c}{\varphi(c)}\ .$$

(ب) از قسمت (آ) استفاده‌کنید، وکلیهٔ اعداد صحیح a و b را که به ازای آنها $\varphi(a)\varphi(b)=\varphi(ab)$ بیابید.

۲۰. فرض‌کنید $f(n)$ تابع حسابی غیرمشخصی باشد وفرض‌کنید $g(n)$ با

$$g(n)=\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)$$

تعریف شود، ثابت‌کنید که

$$f(n)=\sum_{d|n}g(d)\ .$$

۴.۵ اعداد تام و متحابه

حال به عنوان یك‌کاربرد نظریهٔ توابع حسابی، به مطالعهٔ دو دسته از اعداد که از ادوار کهن‌شناخته شده و موردمطالعه قرارگرفته‌بوده‌اند، یعنی‌اعداد تام ومتحابه‌می‌پردازیم.

تعریف ۱ : عدد تام عددصحیح مثبتی است مانند n که با مجموع مقسوم‌علیه‌های واقعی‌خود (یعنی، مقسوم‌علیه‌های مثبت n غیراز خود n) برابر باشد.

مثال ۲ :

(یکم) مقسوم‌علیه‌های واقعی ۶ اعداد ۱ ، ۲ ، و ۳ می‌باشند، و ۶ = ۳ + ۲ + ۱، و بنابراین ۶ عددی تام است.

(دوم) مقسوم علیه‌های واقعی ۲۸ اعداد ۱ ، ۲ ، ۴ ، ۷ ، و ۱۴ می‌باشند ، و ۲۸ = ۱۴ + ۷ + ۴ + ۲ + ۱ ، و بنابراین ۲۸ عددی تام است.

(سوم) متعلم به‌آسانی می‌تواند تحقیق کندکه اعداد ۴۹۶ و ۸۱۲۸ اعدادی تام‌اند.

اعداد تام در سراسر تاریخ همواره در ارتباط با صورتهای گوناگون عدد شناسی[1] ظاهر شده‌اند. این اعداد درآثار فیثاغورسیان از دوران‌کهن پدیدار شده‌اند. به‌تصور اینان خاصیتی که اعداد تام نشان می‌دهند نمایشگر نوعی تمامیت وکمال در علم زیبایی‌شناسی

1. numerology

است، که ازآنجا نام «تام» برآنها نهاده شده است. بسیاری از خرافه‌های قدیمی ومعتقدات باطنی مبتنی برخواص اعداد صحیح از جمله اعداد تام هستند. و چه بسا ، در دنیای کهن ، برهان از راه توسل به علم اعداد جانشین تعابیر علمی‌تـر پدیده‌های طبیعی می‌شده است. و بـرهمین اساس بوده که بخش اعظم نظریهٔ اعداد، و همچنین بحث کنونی ما از اعداد تام آغاز شده است.

چگونه می‌توانیم اعداد تام را بیابیم؟ آیا تعدادی نامتناهی از این اعداد موجودند؟ اینها سؤالاتی هستند که هزاران سال است ریاضیدانان مطرح کرده‌اند وهنوز هم به‌طورکامل جواب دریافت نکرده‌اند. ما همان جوابهای جزئی را درزیر خواهیم آورد.

چون $\sigma(n)$ برابر با مجموع مقسوم‌علیه‌های n (به انضمام n) است، می‌بینیم که n تام است اگر و فقط اگر $\sigma(n)-n=n$ ، که معادل است با

$$\sigma(n)=۲n\,. \tag{۱}$$

دسته‌ای ازاعداد تام وجود دارند که قبلا اقلیدس ازآنها اطلاع داشته است، یعنی

قضیهٔ ۳ : فرض کنیم که $۲^a-۱$ عددی اول باشد. در این صورت $۲^{a-۱}(۲^a-۱)$ عددی تام است .

برهان: اگر $p=۲^a-۱$ عدد اول باشد، آنگاه روشن است که $a>۱$ و p فرد است. قرار می‌دهیم $n=۲^{a-۱}p$ دراین‌صورت $(۲^{a-۱}, p)$بمعم $=۱$. بنابراین، بنابرقضیهٔ ۲.۶داریم

$$\sigma(n)=\sigma(۲^{a-۱})\sigma(p)=\frac{۲^a-۱}{۲-۱}(p+۱)=۲n\,. \qquad ■$$

هرعدد اول p به‌صورت $p=۲^a-۱$ یك عدد اول مرسن نامیده می‌شود. بنابرآنچه که هم‌اکنون ثابت کـردیم تجسس بـرای پیدا کردن اعداد تام ارتباط کاملا نـزدیکی به جستجوی اعداد اول مرسن دارد. مطلب مقدماتی زیـر در تشخیص اعداد اول مـرسن سودمند است.

قضیهٔ ۴ : اگر $۲^a-۱$ عددی اول باشد، آنگاه a اول است.

برهان : تمرین ■

بنابرقضیهٔ ۴ ، کلیهٔ اعداد اول مرسن به صورت $۲^p-۱$ هستند ، که p عـددی اول می‌باشد. چند تای اول از آنها عبارت‌اند از

$$۲^۲-۱=۳$$
$$۲^۳-۱=۷$$

$$۲^۵ - ۱ = ۳۱$$
$$۲^۷ - ۱ = ۱۲۷$$
$$۲^{۱۳} - ۱ = ۸۱۹۱$$
$$۲^{۱۷} - ۱ = ۱۳۱۰۷۱$$
$$۲^{۱۹} - ۱ = ۵۲۴۲۸۷ .$$

ولی، توجه کنید که چنین نیست که هرعدد صحیح به صورت $۲^p - ۱$، که p عددی اول است، خودش یک‌عدد اول باشد. نشان‌دادن‌این امر را که عدد $۲^{۱۱} - ۱$ اول نیست، به‌متعلم واگذار می کنیم.

آیا درست‌است که اعدادتام فقط‌آن‌اعدادی‌هستند که به‌توسط قضیهٔ ۳ بدست‌می‌آیند؟ این امر تاکنون معلوم نشده است. ولی می‌توانیم قضیه زیر راکه از اویلر است ثابت‌کنیم:

قضیهٔ ۵ : فرض‌کنیم n عدد تام زوجی باشد. دراین صورت n به‌صورت $۲^{a-۱}(۲^a - ۱)$ است، که درآن $۲^a - ۱$ یك عدد اول مرسن‌می‌باشد.

برهان: می‌نویسیم $n = ۲^c b$، که $c \geqslant ۱$ و b فرداست. چون n عددی‌است تام $\sigma(n) = ۲n$، و چون $\sigma(n)$ ضربی است، داریم

$$۲n = \sigma(n) = \sigma(۲^c b) = \sigma(۲^c)\sigma(b)$$
$$= (۲^{c+۱} - ۱)\sigma(b) .$$

بنا براین،

$$۲^{c+۱}b = (۲^{c+۱} - ۱)\sigma(b).$$

توجه‌کنید که $(۲^{c+۱}، ۲^{c+۱} - ۱)$ بمعم $= ۱$ وبنا براین $۲^{c+۱}|\sigma(b)$، مثلا $\sigma(b) = ۲^{c+۱}d$، دراین صورت

$$b = (۲^{c+۱} - ۱)d$$

فرض‌کنیم $d > ۱$. پس‌درمیان مقسوم‌علیه‌های b حداقل ۱، d، و b وجود دارند. بنابراین

$$\sigma(b) \geqslant b + d + ۱ = (۲^{c+۱} - ۱)d + d + ۱ = ۲^{c+۱}d + ۱ ,$$

که متناقض با حقیقت $\sigma(b) = ۲^{c+۱}d$ است. پس $d = ۱$ و $b = ۲^{c+۱} - ۱$، بنابراین $n = ۲^c(۲^{c+۱} - ۱)$. بعلاوه،

$$\sigma(۲^{c+۱} - ۱) = \sigma(b) = ۲^{c+۱}d = ۲^{c+۱} . \qquad (۲)$$

ولی اگر $۲^{c+۱} - ۱$ عددی اول نباشد آنگاه $\sigma(۲^{c+۱} - ۱) > (۲^{c+۱} - ۱) + ۱$، زیراکه $۲^{c+۱} - ۱$ مقسوم‌علیهی غیراز $۲^{c+۱} - ۱$ و ۱ دارد. اما این متناقض بامعادلهٔ (۲) می باشد،

بنابراین $2^{c+1}-1$ عددی اول است. پس، اگر قرار دهیم $a=c+1$، می‌بینیم $n=2^{a-1}(2^a-1)$، که درآن 2^a-1 یك عدد اول مرسن است. ■

در حال حاضر دو سؤال اساسی در مورد اعداد تام مطرح است که ریاضیدانان نمی‌توانند به آنها جواب دهند. اول اینکه، معلوم نیست آیا عدد تام فردی وجود دارد یا نه. دوم اینکه، معلوم نیست آیا تعداد اعداد تام نامتناهی است یا نه. یك طریق پرداختن به‌سؤال آخری این خواهد بود که ثابت‌کنیم تعدادی نامتناهی عدد اول مرسن وجود دارد. ولی معلوم نیست که این روش، روش درستی باشد. با استفاده ازکامپیوترهای با سرعت زیاد، کارهای تازه‌ای توسط تعدادی از افراد، از جمله د. ه. و ا. لهمر[1]، ج. سلفریج[2]، و ج. بریلهارت[3] انجام شده است. یك نتیجهٔ تازه از ب. تکرمن[4] این است که $2^{19937}-1$ یك عدد اول مرسن است. این عدد دارای ۶۰۰۲ رقم و بزرگترین عدد اولی است که تاکنون معلوم شده است[5]. بعلاوه، این فقط بیست وچهارمین عدد اول مرسن است که تعیین شده است. همچنین ازکامپیوترها جهت تجزیهٔ کامل اعداد 2^p-1 به عوامل اول، به ازای اعداد اولp، استفاده شده‌است. مثلا یك‌قضیهٔ تازهٔ د. ه. و ا. لهمر و ج. سلفریج، بیان می‌دارد که

$$2^{157}-1=852133201\times 60726444167\times 1654058017289$$
$$\times 2134387368610417.$$

نوع دیگری از اعدادکه ازطریق اهل تصوف و طالع‌بینها مطرح شدند، و به توسط صاحبنظران در نظریهٔ اعداد مورد توجه قرار گرفته‌اند اعداد به‌اصطلاح متحابه می‌باشند.

تعریف ۶: دو عدد m، n متحابه نامیده می‌شوند اگر مجموع مقسوم علیه‌های واقعی m برابر n، و مجموع مقسوم‌علیه‌های واقعی n برابر m باشد.

با استدلالی مشابه با استدلالی که برای اعداد تام کردیم، می‌بینیم که برای اینکه m و n متحابه باشند، لازم وکافی است که

$$\sigma(m)=m+n=\sigma(n).$$

اعداد متحابه در ساختن تعویذات وتهیهٔ طلسمها (طلسمهای خوشبختی) به کار برده می‌شدند. و چنین فرض می‌شدکه این اعداد قادرند بین افراد محبت ایجاد کنند. یك مثال از یك زوج متحابه اعداد $m=220$ و $n=284$ هستند، زیراکه

$$\sigma(n)=\sigma(m)=504=220+284.$$

دیگری مثالی است ازفرما، بدین صورت که $m=17296$ و $n=18416$. چند صدزوج از اعداد متحابه شناخته شده‌اند، ولی معلوم نیست که تعدادآنها متناهی است یا نه.

---

1. D. H. and E. Lehmer 2. J. Selfridge 3. J. Brillhart
4. B. Tuckerman

۵. تاریخ چاپ‌کتاب‌که ۱۳۵۵ ه. ش. می‌باشد ملاحظه شود. زیرا هرآن ممکن‌است عدد اولی بزرگتر از دیگری‌کشف شود (مترجم).

۴.۵ تمرینات

۱. نشان دهید که اگر n عددی تام باشد، آنگاه

$$\sum_{d|n}\frac{1}{d}=2 .$$

۲. کلیهٔ اعداد تام زوج کمتر از ۱۰۰۰ را بیابید.

۳. نشان دهید که یك عدد تام فرد نمی‌تواند عددی اول یا حاصلضرب دوعدد اول باشد.

۴. نشان دهید که اگر m و n اعداد متحابه باشند، آنگاه $\sigma(n)=\sigma(m)=n+m$.

٦

چند معادلهٔ سیاله

۱.۶ مقدمه

دراین فصل، نظریه‌ای را که درپس پنج معادلهٔ سیالهٔ خاص قرار دارد بتفصیل مورد مطالعه قرارخواهیم داد. همهٔ آنها، بجز یکی، به‌معنی زیر از درجهٔ دوم می‌باشند. فرض کنیم اعداد صحیح a_1 ، a_2 ، ... ، a_k ، و n مفروض باشند. بسجملهٔ $f(x_1, \dots, x_k)$ برحسب متغیرهای x_1 ، ... ، x_k را باضابطهٔ

$$f(x_1, \dots, x_k) = a_1 x_1^2 + \dots + a_k x_k^2$$

تعریف می‌کنیم. دراین صورت می‌توانیم معادلهٔ سیالهٔ درجهٔ دوم

$$f(x_1, \dots, x_k) = n \tag{1}$$

را درنظر بگیریم. کلیهٔ معادلاتی را که دراین‌فصل بررسی می‌کنیم، به‌استثنای یکی، حالتهای خاص این معادلهٔ سیالهٔ کلی خواهند بود. به‌عنوان مثال، دربخش۲، معادلهٔ فیثاغورسی

$$x^2 + y^2 = z^2 \tag{2}$$

را ازنظر می‌گذرانیم، که دراین مورد، می‌تواند چنین نوشته شود $x_1^2 + x_2^2 - x_3^2 = 0$ ، بنابراین (۲) حالت خاص (۱) است که درآن $k = 3$ ، $a_1 = a_2 = 1$ ، $a_3 = -1$ ، $n = 0$. دربخش۴، مسئلهٔ نمایش یك عدد صحیح مثبت n به‌صورت مجموع دو مربع را درنظر خواهیم گرفت، که با معادلهٔ سیالهٔ

$$x^2 + y^2 = n \tag{3}$$

متناظر است. این حالت، حالت خاص(۱) است که در آن $k=۲$ ، $a_۱=a_۲=۱$. در بخش۵، مسئلهٔ نمایش یك عدد صحیح مثبت n به‌صورت مجموع چهار مربع را، که بامعادلهٔ سیالهٔ

$$x^۲+y^۲+z^۲+w^۲=n \qquad (۴)$$

متناظر است، بررسی می‌کنیم. این حالت، حالت خاص(۱) است، که در آن $k=۴$ ، $a_۱=a_۲=a_۳=a_۴=۱$. بالاخره، در بخش۶، معادلهٔ پل[1] ،

$$x^۲-dy^۲=۱ , \qquad (۵)$$

را، که حالت خاص(۱) است، که در آن $k=۲$ ، $a_۱=۱$ ، $a_۲=-d$ ، $n=۱$ ازنظر می گذرانیم. همچنین، در بخش ۳، آخرین قضیهٔ فرما را درحالتی که نمای معادله ۴ است مورد مطالعه قرار خواهیم داد:

$$x^۴+y^۴=z^۴ .$$

بااینکه این معادله حالت خاص(۱) نیست، مع‌هذا برنظریهٔ معادلهٔ فیثاغورسی (۲) مبتنی بوده، ولذا درهرحال ارتباط نزدیکی بامعادلهٔ(۱) دارد.

قبل از اینکه به مطالعهٔ پنج معادلهٔ سیاله بپردازیم، اجازه بدهید معادلهٔ کلی (۱) را درنظر بگیریم و اطلاعی از نوع سؤالاتی که می‌توانیم بکنیم به‌دست آوریم. اولین و بدیهی‌ترین سؤال این است که‌آیا معادلهٔ(۱) جوابی دارد؟ اگر جواب این سؤال (به‌ازای مقادیر خاصی برای $a_۱$ ، ... ، a_k ، n) منفی است، آنگاه با مسئلهٔ اثبات نداشتن جواب روبرو هستیم. ما دراین فصل، دقیقاً به‌همین‌منظور، باروش جدیدی که «روش نزول‌نامتناهی فرما» نام دارد آشنا خواهیم شد .

اگر معادلهٔ سیالهٔ(۱) (به‌ازای مقادیر خاص $a_۱$ ، ... ، a_k ، n) جواب داشته باشد، آنگاه مسئلهٔ بدیهیی که باآن مواجهیم، پیداکردن کلیهٔ آنها است. حل این مسئله خیلی مشکل، ولی بعضی‌اوقات ممکن است. برای مثال، نشان خواهیم داد که چگونه کلیهٔ‌جوابهای معادلات فیثاغورسی و پل رامی‌یابیم. درهریك ازحالات نشان خواهیم داد که تعداد جوابها نامتناهی است وآنهارا کاملا تعیین خواهیم کرد.

آخرین مسئله‌ای راکه معادلات (۳) و (۴) به ذهن القا می‌کنند، پیدا کردن کلیهٔ nهایی است‌که به‌ازای آنها معادلهٔ (۱) (به‌ازای مقادیر ثابت $a_۱$ ، ... ، a_k) دارای‌جواب باشد. درمورد معادلهٔ(۳)، این امر به‌معنی پیداکردن‌کلیهٔ اعداد صحیحی است‌که می‌توانند به‌صورت‌مجموع دومربع نوشته شوند. درمورد معادلهٔ(۴) ، این عمل، همان پیداکردن‌کلیهٔ اعداد صحیحی است‌که می‌توانند به‌صورت مجموع چهار مربع نوشته شوند.

ممکن است معادلهٔ سیالهٔ(۱) را ، بااستفاده از بسجملهٔ درجهٔ دوم کلیتری برحسب $x_۱$ ، ... ، x_k تعمیم داد. زیرا، فرض کنیم a_{ij} $(۱\leqslant i , j\leqslant k)$ اعداد صحیح مفروضی باشند. فرض کنیم

1. Pell

$$g(x_1, \ldots, x_k)=a_{11}x_1^2+a_{12}x_1x_2+a_{13}x_1x_3+\cdots+a_{kk}x_k^2 .$$

دراین‌صورت $g(x_1, \ldots, x_k)$ کلیترین بسجملهٔ درجهٔدوم برحسب k متغیر باضرایب‌صحیح می‌باشد. می‌توان معادلهٔ سیالهٔ

$$g(x_1, \ldots, x_k)=n$$

را به‌ازای عدد صحیح مفروض n، مطالعه‌کرد. این امر منجر به‌شاخهٔ‌کاملی از نظریهٔ اعداد می‌شود که هنوز بررسی‌آن‌ادامه‌دارد. متعلم کمی بااین نظریه در نیمهٔ‌دوم این کتاب، درآنجایی که ما حالت خاص $k=2$ را درنظر خواهیم گرفت، آشناخواهد شد. یعنی، نظریهٔ‌معادلات سیاله به‌صورت

$$a_{11}x_1^2+a_{12}x_1x_2+a_{22}x_2^2=n \tag{۶}$$

را بسط خواهیم داد. سؤالات مطروحه همان سؤالاتی خواهند بودکه درفوق کـردیم: آیا (به‌ازای مقادیر مفروض a_{11}، a_{12}، a_{22}، n) جوابهایی‌وجود دارند؟ اگرجوابهایی‌وجود دارند آنهارا صریحاً مشخص‌کنید. فرض‌کنیم a_{11}، a_{12}، a_{22} مفروض باشند. به‌ازای چه مقادیری از n، (۶) جواب دارد؟ این سؤالات خیلی بسرعت مارا به‌سمت نظریه میدانهای درجهٔ دوم، که اول‌بار توسط‌گاوس مطالعه شدند، سوق خواهند داد.

دربخش۵، این نتیجهٔ قابل‌توجه راکـه معادلهٔ(۴)، به‌ازای هر عدد صحیح مثبت n، حلپذیر می‌باشد ثابت خواهیم‌کرد. به‌عبارت دیگر، هـرعدد صحیح مثبت n مجموع چهار مربع‌کامل می‌باشد. این نکته ما را به‌طرح یك‌سؤال طبیعی متوجه مـی‌کند: آیا هر عدد صحیح مثبت n می‌تواند به‌صورت مجموع‌تعداد ثابتی مکعب‌کامل نمایش داده شود؟ یعنی، می‌پرسیم‌که آیا عدد صحیح مثبتی چون k وجود دارد چنانکه معادلهٔ

$$x_1^3+\cdots+x_k^3=n ,$$

به‌ازای هرعدد صحیح مثبتn، حلپذیرباشد. می‌توانیم سؤال‌مشابهی را درمورد قوای‌چهارم، قوای پنجم، وغیره مطرح‌کنیم. در ۱۷۷۵ میلادی، ریاضیدان انگلیسی ورینگ[1] ادعاکـرد که هرعدد صحیح مثبت n می‌تواند به‌صورت مجموع ۴ مربع، ۹ مکعب، ۱۹ قوهٔ‌چهارم، والی‌آخر نوشته شود. ورینگ هیچ برهانی برای مدعای خود نداشت، وحکم او تا ۱۹۰۹ میلادی اثبات نشده باقی ماند، تا اینکه دراین هنگام سرانجام دیوید هیلبرت آن را اثبات کرد. هیلبرت نشان دادکـه به‌ازای هر $k(\geqslant 2)$، عددی صحیح مانند N_k مـوجود است به‌طوری‌که هرعدد صحیح‌مجموع N_k قوهٔ kام می‌باشد. فرض‌کنیم $g(k)$ کوچکترین‌مقدار ممکن N_k باشد. دراین‌صورت به‌استناد نتایجی‌که دربخش ۵ به‌دست خواهیم آورد، نشان خواهیم دادکه $g(2)=4$. همچنین معلوم است‌که $g(3)=9$. ولی مقادیر $g(4)$ و $g(5)$ معلوم نیستند. درصورتی‌که مقادیر $g(k)$، به‌ازای $k\geqslant 6$، تماماً معلوم‌اند.

---

1. Waring

۱.۶ تمرینات

۱. کلیهٔ جوابهای معادلات سیالهٔ زیر را بیابید:

(آ) $x^۲+y^۲=۸$.

(ب) $x^۲+y^۲=۵۱$.

(ج) $x^۲+y^۲+z^۲=۱۰$.

(د) $x^۲+y^۲+z^۲+w^۲=۱۸$.

(ه) $x^۲+۲xy+۲y^۲=۱۷$.

۲. فرض کنیم $(x_۰ , y_۰)$ یك جواب معادلهٔ $x^۲-۶y^۲=۱$ باشد.

(آ) نشان دهید که $(۵x_۰+۱۲y_۰ , ۵y_۰+۲x_۰)$ نیز یك جواب می‌باشد.

(ب) ازقسمت (آ) برای‌محاسبهٔ حداقل پنج‌جواب متمایز $x^۲-۶y^۲=۱$ استفاده کنید.

(ج) نشان‌دهید که $x^۲-۶y^۲=۱$ تعدادی نامتناهی جواب دارد.

۳. نشان دهید که نمی‌توان گفت کلیهٔ اعداد صحیح مثبت مجموع دومربع (مجموع سه‌مربع) هستند.

۴. کلیهٔ اعداد صحیح نابیشتراز ۲۵ را به‌صورت مجموع چهار مربع بنویسید.

۵. به‌ازای هرعدد صحیح $x(<۶۴)$، کوچکترین تعداد مکعبهای کاملی را که مجموعشان x می‌باشد تعیین کنید.

۶. تعیین کنید که کدام اعداد اول $p(\leqslant ۳۰)$ مجموع دومربع می‌باشند. آیا می‌توانید یك حدس کلی بزنید؟

۷. تعیین کنید که کدام اعداد اول $p(\leqslant ۳۰)$ مجموع سه‌مربع می‌باشند. آیا می‌توانید یك حدس کلی بزنید؟

۸. فرض کنیم a و b اعداد صحیح باشند وقرار می‌دهیم $x=a^۲-b^۲$، $y=۲ab$، و $z=a^۲+b^۲$ نشان‌دهید که $x^۲+y^۲=z^۲$. نتیجه بگیرید که تعداد سه‌تایی‌های متمایز فیثاغورسی نامتناهی است.

۹. فرض کنیم $z^n=x^n+y^n$ هیچ جواب ناصفر برای x، y، z درحالتی که $n=۴$ یا n مساوی یك عدد اول $p(>۲)$ است، ندارد. نشان‌دهید که $x^n+y^n=z^n$، به‌ازای کلیهٔ مقادیر $n(\geqslant ۳)$ هیچ‌جواب ناصفر برای x، y، z ندارد.

۱۰. فرض کنیم $f(x , y)$ بسجملهٔ دلخواهی با ضرایب صحیح و a، b، c و d اعداد صحیحی باشند به‌طوری که $ad-bc=\pm۱$. فرض کنیم

$$g(x , y)=f(ax+by , cx+dy) .$$

نشان‌دهید که $f(x, y) = n$ برحسب اعداد صحیح xوy حلپذیر می‌باشد اگر، وفقط اگر، $g(x, y) = n$ دراعداد صحیح حلپذیر باشد. این مسئله روشی کلی برای تعویض یك‌معادله بامعادله‌ای دیگر، بی‌آنکه جوابها عوض شوند، ارائه می‌دهد. شما باید ایـن تعویض را، برای بعضی حالات خاص، مثلا برای معادلهٔ تمرین۲ انجام دهید.

۲.۶ معادلهٔ $x^2 + y^2 = z^2$

یکی از قدیمیترین مسائل‌سیاله تعیین‌کلیهٔ مثلثهای قائم‌الزاویه‌ای هستندکه طول‌اضلاع آنها اعداد صحیح‌باشند. اگرx ، y ، z طولهای سه‌ضلع باشند و z طول وتر باشد، آنگاه قضیهٔ فیثاغورس حکم می کندکه

$$x^2 + y^2 = z^2 \qquad (1)$$

ازین‌رو، کافی‌است‌معادلهٔ سیالهٔ(۱)را حل کنیم. بااینکه‌معادلهٔ(۱) معمولا بامکتب‌فیثاغورسیان (درحدود ۵۷۰ قبل‌از میلاد) وابسته می‌باشد به‌نظر می‌رسد اطلاعاتی‌که بابلیان عهدباستان، متجاوز از هزار سال قبل‌از فیثاغورسیان، دربارهٔ حل آن داشتند بیشتر بوده است. بابلیان، به‌دلایل فلسفی ومحاسباتی، فقط بااعدادگویایی سروکار داشتندکه محاسبه بامخرجهای‌آنها در دستگاه شمارستینی‌آسان بوده است. آنان از جوابهای(۱) به‌منظور تهیهٔ جدولی‌مقدماتی برای توابع مثلثاتی، به‌ازای زوایایی بایك درجه اختلاف استفاده کرده‌اند، به‌این‌نحو که برای x ، y ، z مقادیری برگزیده‌اندکه درایه‌های این جدول در دستگاه‌شمار آنها دارای بسط متناهی بودنـد. این امـر مستلزم داشتن اطلاعات بسیار پیچیده‌ای از معادلهٔ(۱) و از ریاضیات به‌طورکلی بود.

اینك به‌تعیین کلیهٔ جوابهای صحیح (۱) می‌پردازیم. ابتدا، ملاحظه می‌کنیم که اگر (x, y, z) یك‌جواب باشد، آنگاه $(\pm x, \pm y, \pm z)$، به‌ازای تمامی حالتهای‌ممکن برای علامتها، نیز یك جواب است. بدین‌ترتیب، می‌توانیم فـرض‌کنیم $x > 0$ ، $y > 0$ ، $z > 0$. حال توجه‌کنیدکه اگر x ، y ، و z دارای یك عامل مشترك d باشند، آنگاه اگر قرار دهیم $x_0 = x/d$ ، $y_0 = y/d$ ، $z_0 = z/d$ ، داریم

$$x_0^2 + y_0^2 = z_0^2 , \qquad (**)$$

بنابراین (x_0, y_0, z_0) هم یك‌جواب(۱) است. به‌وضوح می‌توانیم d را چنان انتخاب کنیم‌که x_0 ، y_0 ، و z_0 دارای هیچ‌عامل مشترکی‌نباشند، و $x_0 > 0$ ، $y_0 > 0$ ، $z_0 > 0$. فرض‌کنیم چنین انتخابی برای d انجام شده‌باشد می‌گوئیم‌که

$$(x_0, y_0) \text{بمعم} = (x_0, z_0) \text{بمعم} = (y_0, z_0) \text{بمعم} = 1 . \qquad (2)$$

زیرا، فرض‌کنیم $e | x_0$ ، $e | y_0$. درایـن‌صورت $e^2 | x_0^2 + y_0^2$ ، لـذا $e^2 | z_0^2$. بدین‌ترتیب، $e | z_0$ ، و e یك‌عامل مشترك‌برای x_0 ، y_0 ، و z_0 است. بنابراین، مطابق فرض، $e = \pm 1$ و $(x_0, y_0) \text{بمعم} = 1$. به‌همین روش می‌تـوانیم ثـابت کنیم کـه $(x_0, z_0) \text{بمعم} = 1$ و $(y_0, z_0) \text{بمعم} = 1$.

سپس، ملاحظه می‌کنیم که یا x_0 ویا y_0 بایستی‌زوج باشد، زیرا اگر x_0 و y_0 هردو فردباشند، آنگاه (هنگ ۴) $x_0^2 \equiv y_0^2 \equiv 1$. بنابراین

$$z_0^2 = x_0^2 + y_0^2 \equiv 1 + 1 = 2 \ (\text{هنگ } 4)$$

همچنانکه پیش‌از این بارها مشاهده کرده‌ایم، یك مربع‌کامل نمی‌تواند همنهشت ۲ به‌هنگ ۴ باشد. بنابراین، یا x_0 بایستی زوج باشد یا y_0. توجه کنیدکه بنابر (۲)، چون (x_0, y_0) بمعم $= 1$، هردو نمی‌توانند زوج باشند. پس، فرض می‌کنیم x_0 زوج است. دراین صورت y_0 فرد است، وهمچنین، چون $z_0^2 = x_0^2 + y_0^2$، می‌بینیم که z_0 فردمی‌باشد. بنابراین، $z_0 - y_0$ و $z_0 + y_0$ هردو زوج هستند، ومی‌بینیم که

$$\left(\frac{x_0}{2}\right)^2 = \frac{z_0 - y_0}{2} \times \frac{z_0 + y_0}{2}. \qquad (3)$$

سپس، توجه کنید که

$$\text{بمعم}\left(\frac{z_0 - y_0}{2}, \frac{z_0 + y_0}{2}\right) = 1, \qquad (4)$$

زیرا هرعامل مشترك $(z_0 - y_0)/2$ و $(z_0 + y_0)/2$، اعداد

$$\frac{z_0 + y_0}{2} + \frac{z_0 - y_0}{2} = z_0$$

و

$$\frac{z_0 + y_0}{2} - \frac{z_0 - y_0}{2} = y_0$$

را عاد می‌کند و ثابت کرده‌ایم که (z_0, y_0) بمعم $= 1$.

بنابر(۳)،حاصلضرب $(z_0 - y_0)/2$ و $(z_0 + y_0)/2$ یك‌مربع‌کامل‌است. بعلاوه،چون $z_0 > 0$ و $y_0 > 0$، داریم $(z_0 + y_0)/2 > 0$. واز(۳)معلوم‌می‌شود که $(z_0 - y_0)/2 > 0$، بنابراین، مطابق (۴)، $(z_0 - y_0)/2$ و $(z_0 + y_0)/2$ مربع‌کامل‌هستند. پس، اعداد صحیح a و b موجودند به‌طوری که

$$\frac{z_0 - y_0}{2} = b^2,$$

$$\frac{z_0 + y_0}{2} = a^2.$$

از حل این معادلات برحسب y_0 و z_0 حاصل می‌شود

$$y_0 = a^2 - b^2, \quad z_0 = a^2 + b^2.$$

لذا از (**) نتیجه می‌شود[1] که $x_{\circ}=2ab$. بنابراین، می‌بینیم که

$$x=2abd \ , \quad y=(a^2-b^2)d \ , \quad z=(a^2+b^2)d \ . \tag{۵}$$

تحقیق اینکه a ، b ، d هرچه باشند، (۵) جوابی برای (۱) می‌دهد، موضوع ساده‌ای است. کلیهٔ استدلالهای فوق مبتنی برزوج بودن $x_{\circ}$ است. اگر $y_{\circ}$ زوج بود، آنگاه همان دستورات(۵) حاصل‌می‌آمد، به‌استثنای اینکه‌جای x و y باهم عوض‌می‌شد. بنابراین، قضیهٔ زیر را ثابت‌کرده‌ایم:

قضیهٔ ۱ : هرجواب معادلهٔ سیالهٔ $x^2+y^2=z^2$ به‌صورت

$$x=\pm 2abd \ , \quad y=\pm(a^2-b^2)d \ , \quad z=\pm(a^2+b^2)d \tag{*}$$

یا به‌صورت مشابهی است که جای x و y باهم عوض شده‌اند. بالعکس، اگر a ، b ، d اعداد صحیح دلخواهی باشند، آنگاه، به‌ازای تمام حالات ممکن برای علامتها، (*) یك جواب این معادلهٔ سیاله می‌باشد.

از قضیهٔ ۱ ، می‌توانیم نتیجه‌ای بگیریم که دربخش بعدی به‌کار ما خواهدآمد. ولی، ابتدا تعریف زیر را درنظر می‌گیریم

تعریف ۲: فرض‌کنیم $(x \ , y \ , z)$ یك جواب $x^2+y^2=z^2$ باشدبه‌طوری‌که x ، y ، وz هیچ عامل مشترکی بزرگتر از ۱ نداشته باشند. دراین صورت $(x \ , y \ , z)$ را یك جواب اولیه گویند.

فرض‌کنیم $(x \ , y \ , z)$ یك‌جواب‌اولیهٔ $x^2+y^2=z^2$ باشد. مطلب‌را باقراردادهای قضیهٔ ۱ ادامه می‌دهیم. واضح است که‌d یك‌عامل مشترك x ، y ، z است وبنابراین‌$d=1$. ازاین گذشته، اگر e یك عامل مشترك a و b باشد، آنگاه e یك عامل مشترك x ، y ، z است، وبنابراین e نیز برابر ۱ است. یعنی، $1=$ بمعم$(a \ , b)$. بعلاوه، یکی‌از دوعدد a یا b بایستی زوج باشد. زیرا اگر a و b هردو فرد باشند، آنگاه ۲ یك عامل مشترك y و z است، که معنی‌آن این است که $2|z^2-y^2=x^2$ ، بنابراین x زوج است، که اولیه‌بودن جواب $(x \ , y \ , z)$را نقض می‌کند. بعلاوه ، فرض می‌کنیم $x>0$ ، $y>0$ ، $z>0$. دراین‌صورت آشکار است که می‌توانیم a و b را مثبت، و $a>b$ ، انتخاب کنیم. بنابراین، قضیهٔ زیررا ثابت‌کردیم.

قضیهٔ ۳ : فرض‌کنیم $(x \ , y \ , z)$ ، بااین شرط‌که $x>0$ ، $y>0$ ، $z>0$ ، یك جواب اولیهٔ معادلهٔ فیثاغورسی باشد. در این صورت دو عدد صحیح مثبت a و b با شرایط

---

۱. به‌نظر مترجم دراینجا، برای یافتن $x_{\circ}$ باید به‌دستور (۳) رجوع کرد و سپس برای یافتن دستورات‌کلی(۵) به (**) ویا به $x/d=x_{\circ}$ ، $y/d=y_{\circ}$ ، $z/d=z_{\circ}$ رجوع‌کرد (مترجم).

۱ = بمعم$(a\ ،\ b)$، یکی ازآنهازوج ، و $a>b$ ، موجودند به‌قسمی که یا

$$x=2ab \ ، \ y=a^2-b^2 \ ، \ z=a^2+b^2$$

برقرار است ویا همین دستورها، وقتی که درآنها جای x و y باهم عوض شده باشند.

۲.۶ تمرینات

۱. پنج سه‌تایی اولیهٔ متمایز فیثاغورسی را بنویسید.

۲. کلیهٔ جوابهای معادلهٔ سیالهٔ $x^2+4y^2=z^2$ را بیابید.

۳. کلیهٔ زوایای θ راکه به‌ازای آنها $\sin\theta$ و $\cos\theta$ اعدادگویا باشند بیابید.

۴. کلیهٔ جوابهای معادلهٔ سیالهٔ $5x^2+10xy+10y^2=z^2+2z+1$ را بیابید.

۵. کلیهٔ جوابهای $x^2+y^2=z^4$ را بیابید.

۶. بااستقرا روی n، نشان‌دهیدکه به ازای کلیهٔ‌مقادیر $n(\geqslant 1)$، تعدادجوابهای $x^2+y^2=z^{2^n}$ باشرط $xyz\neq 0$ نامتناهی است.

۷. نشان‌دهید که $x^2+y^4=z^2$ دارای تعدادی نامتناهی جواب است که به‌ازای آنها $xyz\neq 0$ و ۱ = بمعم$(x\ ،\ y)$.

۸. عدد $n(\geqslant 3)$ مفروض است. نشان دهیدکه یك سه‌تایی فیثاغورسی $(x\ ،\ y\ ،\ z)$ وجود دارد به‌طوری که یکی از مقادیر x ، y ، z برابر n باشد.

۹. کلیهٔ مثلثهای قائم‌الزاویه‌ای را بیابیدکه طولهای اضلاع آنها اعداد صحیح باشند و اختلاف یك ضلع باوتر ۲ یا ۳ باشد.

۱۰. کلیهٔ جوابهای

(آ) $x^2+2y^2=z^2$ ،

(ب) $x^2+5y^2=z^2$

را بیابید.

۱۱. کلیهٔ جوابهای معادله $x^2+py^2=z^2$ را ، که درآن p عددی اول است، بیابید.

۱۲. نشان دهیدکه معادلهٔ سیالهٔ $x^2-y^2=m^3$ ، هرگاه m معلوم باشد، همواره نسبت به x و y حلپذیر است.

۱۳. نشان دهیدکه معادلهٔ سیالهٔ $x^2-y^2=m^k$ ، به‌ازای هرمقدار مفروض m و $k\geqslant 3$ ، نسبت به x و y حلپذیر است.

۱۴. به‌ازای چه‌مقدار m معادلهٔ $x^2-y^2=m$ نسبت به x و y حلپذیر می‌باشد؟

۱۵. به‌ازای چه مقدار m معادلهٔ $x^2-y^2=m^2$ نسبت به x و y حلپذیر است؟

۳.۶ معادلهٔ $x^4+y^4=z^2$

دربخش ۲ ، نشان دادیم که معادلهٔ سیالهٔ $x^2+y^2=z^2$ تعدادی نامتناهی جواب دارد. این مطلب، طبیعتاً، ما را به‌تحقیق درمورد جوابهای

$$x^n+y^n=z^n \qquad (n\geqslant 3) \tag{1}$$

می‌کشاند. چنانکه درفصل ۱ متذکر شدیم، فرما حدس زد که (۱) هیچ جواب ناصفر x ، y ، z ندارد.

لم ۱: کافی‌است حدس فرما را به‌ازای یك عدد اول فرد n وهمچنین $n=4$ ثابت‌کنیم.

برهان: این برهان موضوع تمرین ۹ از بخش ۱ است. ■

دراین بخش ، حدس فرما را به‌ازای $n=4$ ثابت خواهیم کرد. درحقیقت، به‌دلیل ساده بودن، ثابت خواهیم کرد که معادلهٔ

$$x^4+y^4=z^2 \tag{2}$$

هیچ جواب ناصفری دراعداد صحیح ندارد. واضح است‌که این امر مستلزم، درستی حدس فرما برای $n=4$ است.

دراثبات این قضیه استفاده از نتیجهٔ مربوط به سه‌تایی فیثاغورسی بخش ۲ ضروری است. البته، اگر $x^4+y^4=z^2$ ، آنگاه (x^2 , y^2 , z) یك سه‌تایی فیثاغورسی است. پس، نحوهٔ دیگر بیان این‌قضیه این است‌که نمی‌تواند مثلث‌قائم‌الزاویه‌ای وجود داشته‌باشد که طول اضلاع‌آن اعداد صحیح وهر دوساق آن مربع‌کامل باشند.

مهمتر از خود این نتیجه روش کلی‌ای است که دربرهان به‌کار گرفته شده است، این روش کاربردهای زیادی در نظریهٔ اعداد دارد. این روش به‌روش نزول نامتناهی موسوم و به‌قرار زیر است. فرض‌کنیم (x_1 , y_1 , z_1) یك‌جواب‌دلخواه(۲) باشد که‌درآن $z_1>0$. فرض‌کنیم از این جواب بتوانیم جواب دیگری مانند (x_2 , y_2 , z_2) از (۲) استخراج کنیم که‌درآن $z_1>z_2>0$. دراین‌صورت، البته‌می‌توانیم جواب‌دیگری‌مانند(x_3 , y_3 , z_3) از (۲) استخراج کنیم که درآن $z_1>z_2>z_3>0$. ادامهٔ این روش به‌یك تناقض منجر می‌شود، زیرا نمی‌توانیم دنباله‌ای به‌دلخواه طولانی از اعداد صحیح مابین ۰ و z_1 داشته باشیم. بنابراین، از ابتدا جوابی نمی‌توانسته وجود داشته باشد.

می‌توانیم این روش را دقیقتر بیان‌کنیم. فرض‌کنیم (x_1 , y_1 , z_1) یك جواب (۲) باشد که درآن $z_1(>0)$ کمترین‌عدد ممکن است. (اگر اصلا جوابی‌ناصفر موجودباشد، آنگاه بنابراصل خوشترتیبی بایستی جوابی موجود باشدکه برای آن $z_1(>0)$ کمترین

مقدار را داشته باشد. سپس از این جواب، جواب (x_2 , y_2 , z_2) باشرط $0 < z_2 < z_1$ را برای معادلهٔ(۲) استخراج خواهیم کرد و بلافاصله دچار تناقض می‌شویم.

این برهان حلناپذیری معادلهٔ(۲) ازآن فرماست. اواین برهان را بااستفاده از روش نزول نامتناهی خود در یادداشت معروف دیگرش، درحاشیهٔ نسخه‌ای از آثار دیوفانتوس که دراختیار داشت ذکر کرده است. خود فرما از این روش خیلی‌خوشش‌آمده بود و می‌نویسد «من زمانی به‌برهان این قضیه دست یافتم که کوشش سخت و طاقت‌فرسایی به‌عمل آورده بودم. ایـن برهان را دراینجا مجدداً می‌آورم، زیـرا این‌نوع برهان پیشرفت شگـرفی را درنظریهٔ اعداد ممکن خواهد ساخت.» این اتفاق خوبی بود که او تصمیم گـرفت برهانش را بتفصیل بنویسد، فرما اغلب قضایای خود را بدون ذکر برهان بیان می‌کرد، وبدین‌ترتیب تهیهٔ براهین آنهارا به‌عهدهٔ ریاضیدانان بعدی می‌گذاشت. تلاش ایـن دانشمندان نیز اغلب باموفقیت همراه نبوده، وتوفیق فقط پس‌از تلاشهای فراوان وپی گیر حاصل می‌شده است.

قضیهٔ ۲: معادلهٔ سیالهٔ $x^4 + y^4 = z^2$ برحسب‌اعداد صحیح x ، y ، z جوابی ندارد، مگر $x = 0$ یا $y = 0$.

برهان: برهان طولانی است، ولی کلیهٔ مراحل آن ساده می‌باشند. فرض می‌کنیم یك جواب (x , y , z) وجود داشته باشد که درآن $x \neq 0$ ، $y \neq 0$ ، $z > 0$ ، وفرض می‌کنیم ایـن جواب طوری باشد که درآن z حداقل باشد. از قضیهٔ ۳.۲ دوبار استفاده می‌کنیم تا جوابی با یك z کوچکتر استخراج کنیم.

حکم حـداقل بودن z بلافاصله ایجاب می‌کند کـه ۱ = بمم(x , y) ، زیرا اگـر d = بمم(x , y) آنگاه $d^4 | x^4 + y^4 = z^2$ ، بنابراین $d^2 | z$ ، که ایجاب می‌کند که

$$\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{z}{d^2}\right)^2 .$$

اگر $d > 1$ ، معادلهٔ اخیر جوابی بـرای معادلهٔ $x^4 + y^4 = z^2$ بامقدار کـوچکتری از z خواهد داد. پس، $d = 1$.

سپس می‌بینیم کـه x^2 ، y^2 ، و z نمی‌تـوانند عـامل مشترکی داشته بـاشند؛ یعنی یك جواب اولیه بـرای $X^2 + Y^2 = Z^2$ تشکیل می‌دهند. بنابـراین، مطابق‌قضیهٔ ۳.۲، اعداد صحیح a ، b ، $0 < b < a$ موجودند، به‌طوری که ۱ = بمم(a , b) ویکی‌از اعداد a یا b زوج است و

$$x^2 = 2ab \quad , \quad y^2 = a^2 - b^2 \quad , \quad z = a^2 + b^2 \qquad (3)$$

یامعادلات متناظرآنها وقتی که جای x و y باهم عوض‌شوند. ازآنجایی که معادلات‌اولیهٔ ما نسبت به x و y متقارن هستند، می‌توانیم فرض کنیم(۳) برقرار است.

توجه کنید که a فرد است، زیرا اگـر a زوج باشد، آنگاه، چـون x ، y ، z عامل مشترکی بزرگتراز ۱ ندارند، b فرد است، وبنابراین

$$y^{2} \equiv -b^{2} \equiv -1 \ (\text{هنگ } 4),$$

که ممتنع است. پس، b زوج است و

$$b^{2}+y^{2}=a^{2}$$

که درآن b ، y ، a عامل‌مشترکی ندارند (چون $1 = $ بمعم$((a, b))$ ، وبنابراین یک‌جواب اولیهٔ دیگر را برای معادلهٔ $X^{2}+Y^{2}=Z^{2}$ تشکیل می‌دهند. مجدداً بنابرقضیهٔ ۳.۲ اعداد صحیح u ، v موجودند به‌طوری‌که $1 = $ بمعم(u, v) و

$$b=2uv \ , \ y=u^{2}-v^{2} \ , \ a=u^{2}+v^{2}$$

حال داریم

$$x^{2}=2ab=4uv(u^{2}+v^{2}) \ . \tag{4}$$

چون $1 = $ بمعم(u, v) ، همچنین داریم $1 = $ بمعم$(v, u^{2}+v^{2}) = $ بمعم$(u, u^{2}+v^{2})$. بنابراین، کلیهٔ مقادیر u ، v ، $u^{2}+v^{2}$ بایستی مربع‌کامل باشند؛ یعنی،

$$u=r^{2} \ , \ v=s^{2} \ , \ u^{2}+v^{2}=t^{2}$$

بدین‌ترتیب

$$s^{4}+r^{4}=t^{2} \tag{5}$$

و جواب دیگری برای(۲) به‌دست می‌آوریم.

فقط احتیاج داریم بررسی‌کنیم که این جواب در $0<t<z$ ، بااین‌شرط که r و s ناصفرند، صدق می‌کند. ولی $r=0$ ایجاب می‌کند $u=0$ ، که بنابر(۴) ایجاب می‌کند $x=0$ ، واین خلاف فرض است به‌همین‌طریق، $s\neq 0$. بعلاوه، چون $b\neq 0$ (زیرا $x^{2}=2ab$ ، $x\neq 0$) ، داریم

$$t \leqslant t^{2} = u^{2}+v^{2}=a\leqslant a^{2}<a^{2}+b^{2}=z \ ,$$

وبنابراین $t<z$. پس، z حداقل نیست، وقضیهٔ ۲ ثابت شد. ■

۳.۶ تمرینات

۱. نشان‌دهید‌که $(1/x^{4})+(1/y^{4})=(1/z^{4})$ دراعداد صحیح جواب ندارد.

۲. نشان‌دهید‌که $(x^{2}+1)^{4}+(y^{2}+2)^{4}=(z+4)^{2}$ دراعداد صحیح جواب ندارد.

۳. کلیهٔ جوابهای معادلهٔ سیالهٔ زیر را تعیین‌کنید.

$$(x^{4}+1)^{4}+y^{12}=(z^{2}+1)^{4} \ .$$

۴. کلیهٔ جوابهای معادلهٔ سیالهٔ زیر را تعیین‌کنید.

$$(x^{2}+y^{2}-2)^{4}+16=z^{2}.$$

۵. نشان‌دهید که $x^4+16=(y^2+z^2-2)^2$ دراعداد صحیح جواب ندارد.

۶. نشان‌دهید که $x^4-y^4=z^2$ دراعداد صحیح جوابی ندارد که $xyz\neq 0$.

۷. نشان‌دهید که معادلات سیالهٔ زیر دراعداد صحیح جوابی ندارند که $xyz\neq 0$.

(آ) $x^4+2y^4=z^2$

(ب) $x^4+6y^4=z^2$.

۴.۶ معادلهٔ $x^2+y^2=n$

دراین بخش، به‌سؤال زیر پاسخ خواهیم داد: کدام یك از اعداد صحیح می‌توانند به‌صورت مجموع دومربع‌کامل نوشته شوند؟ (توجه: ۰ یك مربع‌کامل است.) این عیناً مثل این است‌که بپرسیم به‌ازای چه‌مقادیری از اعداد صحیح مثبت n، معادلهٔ سیالهٔ

$$x^2+y^2=n$$

حلپذیر است. ماحل‌کاملی برای این مسئله خواهیم داد. قضایای این‌بخش، اول‌بار به‌صورت یکی‌دیگر ازآن یادداشتهای حاشیه‌ای مشهور فرما، درنسخهٔ شخصی او ازکتاب دیوفانتوس داده شده بود.

قبل از شروع مطلب، اجازه بدهید چند تبصره را متذکر شویم. اولا، توجه‌کنید که ۳ نمی‌تواند به‌صورت مجموعی از دومربع نوشته شود، وبنابراین، مطمئناً چنین نیست‌که معادلهٔ فوق به‌ازای‌کلیهٔ مقادیر n حلپذیر باشد. ثانیاً متعلم دراینجا، برای اولین‌بار، ملاحظه خواهدکردکه ما از نظریهٔ همنهشتیها به‌روشی علمی بـرای نشان دادن اینکه معادلهٔ سیالـهٔ مفروضی واقعاً دارای جواب است استفاده می‌کنیم.

ابتدا، نشان می‌دهیم که چگونه این ملاحظات را به‌حالتی کـه $n=p$ یك عدد اول است تبدیل می‌کنیم. مطلب را با اتحاد زیرشروع می‌کنیم:

$$(*)\qquad (x_1^2+y_1^2)(x_2^2+y_2^2)=(x_1x_2+y_1y_2)^2+(x_1y_2-y_1x_2)^2.$$

اگر با اعداد مختلط آشنایی داشته باشید، ایـن اتحاد به‌نظر شما مرموز نخواهد آمد. این اتحاد دراصل بیان این حکم است‌کـه قدرمطلق حاصلضرب دوعدد مختلط برابر است بـا حاصلضرب قدرمطلقهای آن دوعدد[1]. درهرحال، حتی اگر بااعداد مختلط آشنایی نداشته باشید، می‌توانید از ضرب طرفین اتحاد مستقیماً درستی آن‌را تحقیق‌کنید.

فایدهٔ این اتحاد چیست؟ این اتحاد، بالاخص، بیان می‌داردکه

لم ۱: اگر m و n هردو بتوانند به‌صورت مجموع دومربع نوشته شوند، mn نیز می‌تواند چنین نوشته شود.

---

۱. دوعدد مختلطی‌که منظورماست عبارت‌انداز $x_1-\sqrt{-1}\,y_1$ و $x_2+\sqrt{-1}\,y_2$.

مثال ۲: چون $۱۳=۲^۲+۳^۲$ و $۲۹=۲^۲+۵^۲$ می‌دانیم که $۳۷۷=۲۹\times۱۳$ مجموع دومربع است. درواقع، دراینجا به‌ازای $n=۱۳$ ، $m=۲۹$ داریم $x_1=۲$ ، $y_1=۳$ ، $x_2=۲$ ، $y_2=۵$ وبنابراین

$$۳۷۷=(۲\times۲+۳\times۵)^۲+(۲\times۵-۲\times۳)^۲$$

یا

$$۳۷۷=۱۹^۲+۴^۲ .$$

از لم ۱ روشن است‌که بایدکوشش کنیم اعداد اولی را که می‌توانند به‌صورت مجموع دومربع نوشته شوند تعیین‌کنیم. ابتدا، از همنهشتیها به روال عادی استفاده می‌کنیم تا به‌نتیجه‌ای منفی برسیم.

لم ۳: فرض کنیم p عددی‌اول‌باشد. هرگاه $p\equiv۳$ (هنگ ۴) ، آنگاه p نمی‌تواندبه‌صورت مجموع دومربع نوشته شود.

برهان: فرض می‌کنیم، فرض خلف، اعداد صحیحی مانند x و y داریم به‌طوری‌که

$$x^۲+y^۲=p \qquad (۱)$$

دراین‌صورت $x^۲+y^۲\equiv۳$ (هنگ ۴) ، که به‌وضوح غیرممکن بودن آن دیده می‌شود زیراکه یك مربع، همنهشت ۰ یا ۱ است به‌هنگ ۴ . ■

حال عکس لم ۳ را ثابت می‌کنیم. این مهمترین و دشوارترین گام، درتعیین اعداد صحیحی است‌که می‌توانند به‌صورت مجموع دومربع نوشته شوند.

لم ۴: فرض کنیم p عددی اول باشد. هرگاه $p=۲$ یا $p\equiv۱$ (هنگ ۴) ، آنگاه p می‌تواند به‌صورت مجموع دومربع نوشته شود.

برهان: اگر $p=۲$ ، آنگاه $p=۲=۱^۲+۱^۲$ ، پس این حالت محقق است.

فرض کنیم $p\equiv۱$ (هنگ ۴) . دراین‌صورت، بنابرقضیهٔ ۵.۳.۳، می‌توانیم همنهشتی

$$x^۲\equiv-۱ \ (\text{هنگ } p)$$

را حل کنیم. چون اعداد صحیح $\pm(p-۱)/۲$ ، … ، ±۲ ، ±۱ ، ۰ ، به‌هنگ p، یك دستگاه کامل مانده‌ها تشکیل می‌دهند، البته، می‌توانیم فرض‌کنیم عدد صحیح x یکی ازاین اعداد می‌باشد. بنابراین، اعداد صحیحی‌مانند x و t ، $|x|\leqslant(p-۱)/۲<p/۲$، داریم به‌قسمی که

$$x^۲+۱=tp .$$

دراین‌صورت $t>0$ ، و

$$t=\frac{x^2+1}{p}<\frac{(p/2)^2+1}{p}=\frac{p}{4}+\frac{1}{p}<p\,.$$

چون $1^2=1$، پس نشان داده‌ایم که: اعدادصحیح x ، y ، t ($y=1$) موجودندبه‌طوری‌که

$$x^2+y^2=tp \quad \text{و} \quad 1\leqslant t<p\,. \tag{2}$$

این کاملا همان چیزی که ما احتیاج داریم نیست. ما همین عبارت را با $t=1$ لازم داریم. نشان خواهیم داد که اگر $t>1$ ، آنگاه مقدار t می‌توانـد (بااستفاده از x و y متفاوت) تقلیل یابد، به‌این طریق (۲) را به‌ازای $t=1$ به‌دست می‌آوریم. (بهمشابهت این روش با روش نُزول نامتناهی توجه کنید.)

فرض کنیم $k(\geqslant 1)$ کوچکترین عدد صحیحی باشد که kp مجموع دومربع باشد. بنابراین اعداد صحیحی مانند x_1 و y_1 داریم به‌طوری‌که

$$x_1^2+y_1^2=kp\,. \tag{3}$$

فرض می‌کنیم $k>1$ ، ومقدار کوچکتری برای k به‌دست می‌آوریم، وبنابراین دچارتناقض می‌شویم. باتوجه به (۲) می‌دانیم که $1<k<p$.

اعداد صحیحی مثل x_2 و y_2 انتخاب می‌کنیم به‌قسمی که

$$x_2\equiv x_1\ (\text{هنگ } k) \quad \text{و} \quad y_2\equiv y_1\ (\text{هنگ } k)\,. \tag{4}$$

بااستفاده از دستگاه‌کامل مانده‌های ... ، ± 2 ، ± 1 ، 0 می‌توانیم فرض کنیم

$$|x_2|\leqslant\frac{k}{2} \quad \text{و} \quad |y_2|\leqslant\frac{k}{2}\,. \tag{5}$$

علاوه‌براین،نمی‌توانیم‌داشته‌باشیم $x_2=y_2=0$ زیرا دراین‌صورت $x_1\equiv y_1\equiv 0\ (\text{هنگ } k)$ و بنابراین $x_1^2\equiv y_1^2\equiv 0\ (\text{هنگ } k^2)$. ولی دراین‌صورت، باتوجه به (۳)، داریم

$$kp=x_1^2+y_1^2\equiv 0\ (\text{هنگ } k^2)$$

که ایجاب می‌کند $k\mid p$ ، که ناقض فرض $1<k<p$ است. حال بااستفاده از (۳) و(۴)

$$x_2^2+y_2^2\equiv x_1^2+y_1^2\equiv 0\ (\text{هنگ } k)\,.$$

بنابراین، عددی چون m وجود دارد به‌طوری‌که

$$x_2^2+y_2^2=km\,. \tag{6}$$

دراین‌صورت، چون یکی از مقادیر x_2 ، y_2 ناصفر است و $k>0$ ،

$$m=\frac{x_2^2+y_2^2}{k}\geqslant 1\,.$$

بعلاوه ، با استفاده از (۵) ، داریم

$$m\leqslant\frac{(k/2)^2+(k/2)^2}{k}=\frac{1}{2}k<k\,.$$

یعنی، $1\leqslant m<k$ ، از ترکیب (۳) و (۶) با اتحاد اساسی(*) ، داریم

$$k^2mp=(x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2\,.$$

با استفادهٔ مجدد از (۴) ، داریم

$$x_1x_2+y_1y_2\equiv x_1^2+y_1^2\equiv 0\ (\text{هنگ } k)$$

و

$$x_1y_2-x_2y_1\equiv x_1y_1-x_1y_1\equiv 0\ (\text{هنگ } k)\,.$$

بنابراین،

$$mp=\left(\frac{x_1x_2+y_1y_2}{k}\right)^2+\left(\frac{x_1y_2-x_2y_1}{k}\right)^2,$$

که در آن $(x_1x_2+y_1y_2)/k$ و $(x_1y_2-x_2y_1)/k$ هردو اعداد صحیح می‌باشند. حال به تناقض مطلوب رسیده‌ایم. یعنی، mp مجموع دومربع است و $1\leqslant m<k$. ■

حال لمهای ۱ ، ۳ ، و ۴ را باهم ترکیب می‌کنیم تا تعیین نماییم دقیقاً چه اعداد صحیحی می‌توانند به‌صورت مجموع دومربع نوشته شوند. اولاً هر مربع کامل s^2 بدیهی است که می‌تواند چنین نمایش داده شود:

$$s^2+0^2=s^2 \qquad (x=s\,,\ y=0)\,.$$

بنابراین، اگر n عدد صحیح مثبتی باشد ، می‌نویسیم $n=s^2n_0$ ، که در آن n_0 هیچ عامل مربع ندارد. می‌نویسیم $n_0=p_1p_2\cdots p_t$ ، که در آن p_1 ، ... ، p_t اعداد اول متمایز هستند. با استفاده از لمهای ۱ و ۴ ملاحظه می‌کنیم که اگر ، به‌ازای هر i ، $p_i=2$ یا $p_i\equiv 1$ (هنگ ۴) ، آنگاه $n=s^2p_1p_2\cdots p_t$ می‌تواند به‌صورت مجموع دومربع نوشته شود.

بالعکس، فرض کنیم n بتواند به‌صورت مجموع دومربع نوشته شود. ثابت می‌کنیم که اگر بنویسیم $n=s^2p_1\cdots p_t$ که p_1 ، ... ، p_t اعداد اول متمایزند، آنگاه، به‌ازای هر $1\leqslant i\leqslant t$ ، یا $p_i=2$ یا $p_i\equiv 1$ (هنگ ۴) به‌روش برهان خلف استدلال می‌کنیم، فرض می‌کنیم عددی مانند p_i همنهشت ۳ به‌هنگ ۴ باشد. بی‌آنکه خللی در کلیت ایجاد کند فرض می‌کنیم $p_1\equiv 3$ (هنگ ۴). پس اگر $n=x^2+y^2$ ، آنگاه داریم $x^2+y^2\equiv 0$ (هنگ p_1). فرض کنیم $p_1\nmid y$. دراین‌صورت y یک عکس حسابی، y^* ، به‌هنگ p_1 ، دارد. پس داریم $(xy^*)^2\equiv -1$ (هنگ p_1)، بنابراین -1 یک ماندهٔ درجهٔ دوم به‌هنگ p_1 می‌باشد، که متناقض با این حقیقت است که $p_1\equiv 3$ (هنگ ۴). پس، $p_1\nmid y$ به یک تناقض منجر می‌شود. به‌همین طریق هم، $p_1\nmid x$ به تناقض می‌رسد. بنابراین، نتیجه می‌گیریم که $p_1|x$ و $p_1|y$. پس،

$$p_1^2 \mid x^2+y^2=n=s^2p_1\cdots p_t \;.$$

چون p_1 ، p_2 ، … ، p_t اعداد اول متمایز هستند، باید داشته باشیم $p_1|s^2$ ، پس $p_1|s$. بنابراین،

$$\left(\frac{x}{p_1}\right)^2+\left(\frac{y}{p_1}\right)^2=\left(\frac{s}{p_1}\right)^2p_1\cdots p_t$$

هرگاه به‌جای n ، n/p_1^2 بگذاریم می‌بینیم که n/p_1^2 مجموع دومربع است و $n/p_1^2=w^2p_1\cdots p_t$. اگر همین استدلال را با قرار دادن n/p_1^2 به‌جای n تکرار کنیم، می‌توانیم عامل‌دیگر p_1 از w را حذف کنیم. با تکرار این‌فرآیند، سرانجام به‌عدد صحیحی مانند n_1 می‌رسیم که n_1 مجموع دومربع است، یعنی $n_1=a^2+b^2$ ، $n_1=v^2p_1\cdots p_t$، به‌شرط آنکه $p_1\nmid v$. اما دراین صورت اگر یکبار دیگرهم، همین‌استدلال را به‌کار بریم، به‌تناقض $p_1|v$ می‌رسیم بنابراین، (هنگ ۴)$p_1\not\equiv 3$. (توجه داشته باشید که استدلالی که هم‌اکنون کردیم کاربرد دیگری از روش نزول نامتناهی است.)

پس قضیهٔ زیر را به‌طورکامل ثابت کردیم:

قضیهٔ ۵: فرض کنیم n عدد صحیح مثبتی باشد. می‌نویسیم $n=s^2n_0$ ، که درآن n_0 عامل[۱] مربعی ندارد. دراین‌صورت فقط وفقط وقتی n می‌تواند به‌صورت مجموع دومربع نوشته شودکه عوامل اول n_0 فقط درمیان اعداد اول ۲ و (هنگ ۴)$p\equiv 1$ باشند.

مثال ۶: $888=2^3\times 3\times 37$. بنابراین $888=2^2(2\times 3\times 37)$. چون (هنگ ۴)$3\equiv 3$ ، می‌بینیم که ۸۸۸ نمی‌تواند به‌صورت مجموع دومربع نوشته‌شود.

مثال ۷: $332514=2\times 3^2\times 7^2\times 13\times 29=(3\times 7)^2(2\times 13\times 29)$. چون (هنگ ۴)$29\equiv 13\equiv 1$، می‌بینیم که ۳۳۲۵۱۴ می‌تواند به‌صورت مجموع دومربع نوشته شود. حال از اتحاد(*) استفاده‌می‌کنیم تامحاسبات را عملا انجام دهیم واطلاعی ازکارآیی آن به‌دست‌آوریم. قبلا درمثال ۲ از (*) استفاده‌کردیم تا نشان دهیم

$$13\times 29=19^2+4^2$$

از ترکیب این تساوی با $2=1^2+1^2$ به‌دست می‌آوریم

$$2\times 13\times 29=(19\times 1+4\times 1)^2+(19\times 1-4\times 1)^2=23^2+15^2$$

بالاخره

$$332514=(3\times 7)^2(23^2+15^2)$$

---

۱. منظور عامل اول است (مترجم).

$$=(۳\times ۷\times ۲۳)^{۲}+(۳\times ۷\times ۱۵)^{۲}$$
$$=۴۸۳^{۲}+۳۱۵^{۲}.$$

۴.۶ تمرینات

۱. فرض کنیم ۱ = بمعم$(a \text{ ، } b)$. نشان‌دهید که اگر a مجموع دو مربع نباشد، ab مجموع دومربع نیست.

۲. بااستفاده ازنتایج این بخش ثابت کنید که تعدادی‌نامتناهی‌سه‌تایی فیثاغورسی‌وجود دارد.

۳. تعیین کنید که آیا اعداد صحیح زیر می‌توانند به‌صورت مجموع دومربع نوشته شوند؟ درهرحالت کلیهٔ نمایشهای ممکن عدد موردنظر را به‌صورت مجموع دومربع مشخص کنید. (درحالت دادن مربعهای اعداد صحیح منفی را فراموش نکنید.)

(آ) $n=۳$.　(ب) $n=۵$.　(ج) $n=۴۹$.　(د) $n=۶۰$.

(ه) $n=۸۵$.　(و) $n=۲۹$.

۴. با استفاده ازنتایج تمرین ۳ ، عدد $۲۴۶۵=۲۹\times ۸۵$ را آشکارا به‌صورت مجموع دومربع بنویسید.

۵. به‌ازای عدد صحیح‌مثبت n ، فرض کنیم $r_{۲}(n)$ معرف‌تعداد نمایشهای n به‌صورت $x^{۲}+y^{۲}$ باشد. قرارداد می‌کنیم که ، مثلاً، $۵^{۲}+۳^{۲}$ و $۳^{۲}+۵^{۲}$ را دونمایش متمایز به‌حساب‌آوریم.

(آ) با استفاده ازتمرین ۳، مقادیر $r_{۲}(۳)$ ، $r_{۲}(۵)$ ، $r_{۲}(۴۹)$ ، $r_{۲}(۶۰)$ ، $r_{۲}(۸۵)$، و $r_{۲}(۲۹)$ را حساب کنید.

(ب) بااستفاده از اتحاد متن کتاب، نشان دهید که $r_{۲}(n)$ ضربی است.

(ج) نشان دهید که به‌ازای یك عدد اول p ،

$$r_{۲}(p)=\begin{cases} ۸ & p \text{ فرد و } p\equiv ۱\ (\text{هنگ } ۴) \\ ۴ & p=۲ \\ ۰ & \text{درغیراین‌صورت} \end{cases}$$

(راهنمایی: کافی است حالت اول را درنظر بگیریم. بعلاوه، کافی است نشان دهیم که $p=x^{۲}+y^{۲}$ ، باشرط $۰<x<y<p$ ، فقط یك جواب دارد. فرض کنیم $(x \text{ ، } y)$ و $(x_{۱} \text{ ، } y_{۱})$ چنین دوجوابی باشند. نشان‌دهید که

$$(xy^{*})^{۲}\equiv (x_{۱}y_{۱}^{*})^{۲}\equiv -۱\ (\text{هنگ } p)$$

وسپس $x=x_{۱}$ ، $y=y_{۱}$.)

۶. نشان دهید که معادلهٔ سیالهٔ $۵x^{۲}+۱۴xy+۱۰y^{۲}=n$ نسبت به x و y حلپذیر است اگر، وفقط اگر، n مجموع دومربع باشد.

*۷. فرض کنیم $n(>0)$ مفروض باشد. یك شرط لازم و کافی پیدا کنید برای آنکه $n=x^2+2y^2$، نسبت به اعداد صحیح x و y حلپذیر باشد.

۵.۶ معادلهٔ $x^2+y^2+z^2+w^2=n$

در بخش قبل، این مسئله را که چه اعداد صحیحی می‌توانستند به‌صورت مجموع دومربع کامل نوشته شوند کاملا معین کردیم. بالاخص مشاهده کردیم که چنین نیست که کلیهٔ اعداد بتوانند به‌این طریق نوشته شوند. دراین صورت آیا می‌توانیم هر عدد صحیح را به‌صورت مجموع سه‌مربع بنویسیم؟ مثلاً، ۳ مجموع دومربع نیست ولی $1^2+1^2+1^2=3$، و ۴۳ مجموع دو مربع نیست ولی $5^2+3^2+3^2=43$. ولی، متأسفانه، همچنانکه بسهولت می‌توان تحقیق کرد، ۷ مجموع سه‌مربع نیست. حال آنکه $1^2+1^2+1^2+2^2=7$ مجموع چهار مربع است. باشه در ۱۶۲۱ میلادی حدس زد که هرعدد صحیح مجموع چهار مربع است.

حال باز با یکی دیگر از یادداشتهای حاشیه‌ای مشهور فرما مواجه می‌شویم. نامبرده متذکر می‌شود که در واقع با استفاده از روش نزول نامتناهی خویش این موضوع را ثابت کرده است. متأسفانه اشارهٔ بیشتری به‌اینکه برهان چگونه صورت گرفته، نمی‌کند. سپس از ریاضیدانان معاصر خود طلب می‌کند که درستی قضیه را ثابت و تعیین کنند که، به گفتهٔ خودش، «آیا من به اکتشاف خود بیش‌از استحقاقی که دارد ارزش می‌گذارم.» تردیدی هست که فرما توانسته باشد این قضیه را ثابت کند، ولی بیش‌از ۱۰۰ سال بعد از مرگ فرما بود که بالاخره بعد از اینکه تلاش اویلر کبیر به‌شکست منجر شده بود، درسال ۱۷۷۰ میلادی برهانی توسط ج. ل. لاگرانژ ریاضیدان فرانسوی برای آن ارائه شد. در واقع افتخار اثبات این قضیه از آن لاگرانژ است نه فرما.

از دیدگاه کنونی، برهان را می‌توان با برهانی خیلی نزدیك به برهانی که برای مجموع دومربع ذکرشده موازی باآن انجام داد. نخست اتحاد (*) را (که به‌توسط اویلر کشف شده) می‌نویسیم که می‌گوید اگر m و n بتوانند به‌صورت مجموع چهارمربع نوشته شوند، آنگاه mn نیز می‌تواند چنین نوشته شود. این اتحاد، برعکس آنچه که دربخش قبل بود، یك کاربرد بدیهی اعداد مختلط نیست، بلکه کشف آن دستاوردی اساسی بود[1]. ولی اثبات آن بسیار ساده است، زیرا شخص می‌تواند طرفین آن‌را بسط دهد. این امر شاهدی است بر نظر معروف ج.ا. لیتل‌وود[2] که هر اتحاد چیز پیش‌پا افتاده‌ای است به‌شرطی که‌شخص دیگری آن‌را نوشته باشد.

باتوجه به‌این اتحاد، کافی است که نشان دهیم هرعدد اول p می‌تواند به‌صورت مجموع چهار مربع نوشته شود. برای انجام این امر نخست نشان می‌دهیم که با توجه به

---

۱. ولی این، از یك دستگاه اعداد پیچیده‌ای ناشی می‌شود موسوم به چهارتایی‌ها که به‌توسط هامیلتون (Hamilton) درنیمهٔ سدهٔ نوزدهم‌کشف شدکه درزمان اویلر شناخته نشده بود.

2. J. E. Littlewood

لم ۳ می‌توان همنهشتیی را پیدا وحل کرد تا نشان داد که مضربی از p مجموع چهارمربع است. سپس، با برهانی که دقیقاً موازی برهان مشابهش برای دومربع است نشان می‌دهیم که کوچکترین مضرب p که می‌تواند به‌صورت مجموعی ازچهارمربع نوشته شود $(p=)\,p\times ۱$ است و برهان تکمیل می‌شود.

ابتدا اتحاد زیر را درنظر می‌گیریم:

$$\begin{aligned}(x_۱^۲+y_۱^۲+z_۱^۲+w_۱^۲)(x_۲^۲+y_۲^۲+z_۲^۲+w_۲^۲)&=(x_۱x_۲+y_۱y_۲+z_۱z_۲+w_۱w_۲)^۲\\ (*)\qquad &+(x_۱y_۲-y_۱x_۲+z_۱w_۲-w_۱z_۲)^۲+(x_۱z_۲-z_۱x_۲+w_۱y_۲-y_۱w_۲)^۲\\ &+(x_۱w_۲-w_۱x_۲+y_۱z_۲-z_۱y_۲)^۲.\end{aligned}$$

چنانکه درفوق اشاره کردیم، این اتحاد را می‌توان مستقیماً از راه بسط طرفین آن تحقیق کرد. بنابراین، داریم

لم ۱: اگر m و n بتوانند به‌صورت مجموع چهار مربع نوشته شوند، آنگاه mn نیز می‌تواند چنین نوشته شود. بالاخص، اگر نشان دهیم که هرعدد اول را می‌توان به صورت مجموع چهار مربع نوشت، آنگاه ثابت کرده‌ایم که هرعدد صحیح (نامنفی) را می‌توان به صورت مجموع چهار مربع نوشت.

مثال ۲: چون $۳۰=۱^۲+۲^۲+۳^۲+۴^۲$ و $۲۹=۲^۲+۵^۲=۲^۲+۵^۲+۰^۲+۰^۲$، می‌دانیم که $۸۷۰=۲۹\times ۳۰$ مجموع چهارمربع است. زیرا، دراینجا به‌ازای $n=۳۰$، $m=۲۹$،داریم $x_۱=۱$، $y_۱=۲$، $z_۱=۳$، $w_۱=۴$ و $x_۲=۲$، $y_۲=۵$، $z_۲=۰$، $w_۲=۰$، وبنابراین

$$۸۷۰=(۲+۱۰)^۲+(۵-۴)^۲+(-۶+۲۰)^۲+(-۸-۱۵)^۲$$

یا

$$۸۷۰=۱۲^۲+۱^۲+۱۴^۲+۲۳^۲.$$

اینك لم زیر را دربارهٔ همنهشتیها عرضه می‌کنیم. برهان‌آن تمرین ساده و جالبی در مانده‌های درجهٔ دوم است.

لم ۳: فرض کنیم p عددی‌اول باشد. دراین‌صورت اعداد صحیح x و yموجودندبه‌طوری که

$$x^۲+y^۲\equiv -۱\ (p\ \text{هنگ}).$$

برهان: اگر $p=۲$، فرض می‌کنیم $x=۱$ و $y=۰$. اگر $p\equiv ۱\ (۴\ \text{هنگ})$، آنگاه می‌دانیم که $\left(\frac{-۱}{p}\right)=۱$، و می‌توانیم y رامساوی ۰ و x را جواب $x^۲\equiv -۱\ (p\ \text{هنگ})$ بگیریم.

بالاخره ، حالت $p \equiv 3 \pmod 4$ (هنگ ۴) باقی ماند، دراین حالت ۱ $- = \left(\frac{-1}{p}\right)$.

می‌خواهیم اعداد صحیح x و y را بیابیم به‌قسمی که

$$x^2 \equiv -(y^2+1) \pmod p$$

یعنی، می‌خواهیم عددی صحیح مانند y بیابیم به‌قسمی که

$$\left(\frac{-(y^2+1)}{p}\right) = 1$$

اما

$$\left(\frac{-(y^2+1)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y^2+1}{p}\right) = -\left(\frac{y^2+1}{p}\right).$$

بنابراین، می‌خواهیم عدد صحیح y را بیابیم به‌طوری که

$$\left(\frac{y^2+1}{p}\right) = -1$$

چون اعداد صحیح y^2 ، عیناً نظیر مانده‌های درجهٔ دوم به‌هنگ p می‌باشند، پس مسئلهٔ ما چنین است: یك ماندهٔ درجهٔ دوم a به‌هنگ p بیابید به‌طوری که $a+1$ یك ناماندهٔ درجهٔ دوم باشد. یعنی، a را چنان بیابید که $\left(\frac{a}{p}\right) = 1$ و $\left(\frac{a+1}{p}\right) = -1$. بدیهی است که چنین aای بایستی موجود باشد. زیرا، اگر a موجود نباشد ، آنگاه $\left(\frac{1}{p}\right) = 1$ ایجاب می‌کند که $\left(\frac{2}{p}\right) = \left(\frac{1+1}{p}\right) = 1$ واین به‌نوبهٔ خود ایجاب می‌کند که $\left(\frac{3}{p}\right) = \left(\frac{2+1}{p}\right) = 1$ و الی آخر. دراین‌صورت، هرعدد صحیح بایستی یك ماندهٔ درجهٔ دوم به‌هنگ p باشد ومی‌دانیم که چنین نیست. ∎

حال می‌توانیم قضیهٔ زیر را ثابت‌کنیم:

قضیهٔ ۴: فرض‌کنیم n عدد صحیح مثبتی باشد. دراین‌صورت n می‌تواند به‌صورت‌مجموع چهار مربع نوشته شود.

برهان: بنابر لم ۱ می‌توانیم فرض کنیم $n = p$ عددی اول باشد. اگر $p = 2$ آنگاه $p = 1^2+1^2+0^2+0^2$ ، وبنابراین می‌توانیم فرض‌کنیم $p > 2$ ، پس p فرد است.
به‌استناد لم ۳، می‌توانیم همنهشتی

$$x^{2}+y^{2}\equiv -1 \ (p \text{ هنگ})$$

را حل کنیم. چون مجموعهٔ اعداد صحیح $\pm(p-1)/2$ ، ... ، ± 1 ، 0 یك دستگاه کامل مانده‌ها به‌هنگ p می‌باشد، می‌توانیم فرض کنیم اعداد صحیح x و y یکی از ایـن اعداد صحیح باشند. پس اعداد صحیح x و y و t ، به‌طوری که $|x|, |y|\leqslant(p-1)/2<p/2$ ، وجود دارند به‌قسمی که

$$x^{2}+y^{2}+1=tp$$

دراین‌صورت $t>0$ و

$$t=\frac{x^{2}+y^{2}+1}{p}<\frac{(p/2)^{2}+(p/2)^{2}+1}{p}=\frac{p}{2}+\frac{1}{p}<p \cdot$$

چون $1^{2}=1$ ، $0^{2}=0$، نشان‌داده‌ایم که: اعداد صحیح x ، y ، z ، w ، t ($z=1$ ، $w=0$) وجود دارند به‌طوری که

$$x^{2}+y^{2}+z^{2}+w^{2}=tp \text{ و } 1\leqslant t<p \cdot \tag{1}$$

ما حکم (۱) را به‌ازای $t=1$ لازم داریم، مجدداً نشان می‌دهیم که اگر $t>1$ ، آنگاه t از لحاظ مقدار می‌تواند تقلیل یابد. یا به‌عبارت دیگر، نشان خواهیم داد که $t=1$ کمترین مقدار برای t است که (۱) را برقرار می‌سازد.

ازاین‌رو ، فرض می کنیم $k\geqslant 1$ کـوچکترین عدد صحیحی باشد به‌طوری که kp مجموع چهار مربع کامل باشد. دراین صورت اعداد صحیح x_1 ، y_1 ، z_1 ، w_1 را داریم به‌قسمی که

$$x_{1}^{2}+y_{1}^{2}+z_{1}^{2}+w_{1}^{2}=kp \cdot \tag{2}$$

فرض می کنیم $k>1$. دراین‌صورت بااستناد به (۱) داریم $1<k<p$

اعداد صحیح x_2 ، y_2 ، z_2 ، w_2 از دستگاه کامل مانده‌های 0 ، ± 1 ، ± 2 ، ... ، (هنگ k) را طوری انتخاب می کنیم که

$$x_{2}\equiv x_{1}\ (k \text{ هنگ}) ,\ y_{2}\equiv y_{1}\ (k \text{ هنگ}) ,\ z_{2}\equiv z_{1}\ (k \text{ هنگ}) ;\ w_{2}\equiv w_{1}\ (k \text{ هنگ}) \tag{3}$$

دراین‌صورت

$$|x_{2}|\leqslant\frac{k}{2} ,\quad |y_{2}|\leqslant\frac{k}{2} ,\quad |z_{2}|\leqslant\frac{k}{2} ,\quad |w_{2}|\leqslant\frac{k}{2} \cdot \tag{4}$$

بعلاوه، نمی‌توانیم داشته باشیم $x_2=y_2=z_2=w_2=0$ زیرا دراین صورت

$$x_{1}\equiv y_{1}\equiv z_{1}\equiv w_{1}\equiv 0\ (k \text{ هنگ})$$

وبنابر (۲)

$$kp=x_{1}^{2}+y_{1}^{2}+z_{1}^{2}+w_{1}^{2}\equiv 0\ (k^{2} \text{ هنگ}) ,$$

که ایجاب می‌کند $k|p$ ، که ناقض فرض $1<k<p$ است.

مجدداً امکان ندارد که $|x_2|=|y_2|=|z_2|=|w_2|=k/2$ زیرا دراین‌صورت k زوج می‌باشد وبنابراین $-(k/2)\equiv k/2$ (هنگ k)، وبدین‌ترتیب

$$x_1\equiv y_1\equiv z_1\equiv w_1\equiv (k/2) \pmod{k},$$

ولذا $x_1^2\equiv y_1^2\equiv z_1^2\equiv w_1^2\equiv (k^2/4) \pmod{k^2}$، که دوباره مطابق(۲) ایجاب‌می‌کند که

$$kp=x_1^2+y_1^2+z_1^2+w_1^2\equiv\frac{k^2}{4}+\frac{k^2}{4}+\frac{k^2}{4}+\frac{k^2}{4}=k^2\equiv 0 \pmod{k^2}$$

که باز یك‌تناقض است.

اینك بااستفاده از (۲) و (۳) داریم

$$x_2^2+y_2^2+z_2^2+w_2^2\equiv x_1^2+y_1^2+z_1^2+w_1^2\equiv 0 \pmod{k}$$

بنابراین، مقداری مانند m وجود دارد به‌طوری که

$$x_2^2+y_2^2+z_2^2+w_2^2=km. \tag{5}$$

بعلاوه، چون یکی‌از مقادیر x_2 ، y_2 ، z_2 ، w_2 ناصفر و $k>0$ می‌باشد،

$$m=\frac{x_2^2+y_2^2+z_2^2+w_2^2}{k}\geqslant 1$$

علاوه‌براین، بنابر(۴) واین‌حقیقت‌که کلیهٔ مقادیر $|x_2|$ ، $|y_2|$ ، $|z_2|$ ، $|w_2|$ نمی‌توانند برابر $k/2$ باشند، داریم

$$m<\frac{(k/2)^2+(k/2)^2+(k/2)^2+(k/2)^2}{k}=k.$$

یعنی $1\leqslant m<k$. از ترکیب (۲) و (۵) بااتحاد اولیهٔ (*) ، داریم

$$k^2mp=A^2+B^2+C^2+D^2,$$

که دراینجا A ، B ، C ، D چهار جملهٔ طرف راست (*) می‌باشند. دوباره با استفاده از (۳) ، داریم

$$A=x_1x_2+y_1y_2+z_1z_2+w_1w_2\equiv x_1^2+y_1^2+z_1^2+w_1^2\equiv 0 \pmod{k}$$

و

$$B=x_1y_2-y_1x_2+z_1w_2-w_1z_2\equiv x_1y_1-y_1x_1$$
$$+z_1w_1-w_1z_1\equiv 0 \pmod{k}$$

وبه‌همین‌طریق $C\equiv 0$ (هنگ k) و $D\equiv 0$ (هنگ k) . پس ،

$$mp=\left(\frac{A}{k}\right)^۲+\left(\frac{B}{k}\right)^۲+\left(\frac{C}{k}\right)^۲+\left(\frac{D}{k}\right)^۲,$$

که درآن A/k ، B/k ، C/k ، D/k همه اعـداد صحیح هستند . حـال به‌تناقض مطلوب رسیده‌ایم. یعنی mp مجموع چهار مربع کامل است و $۱\leqslant m<k$. ■

۵.۶ تمرینات

۱. (آ) ۵ ، ۷ ، و ۱۱ را به‌صورت مجموع چهار مربع کامل نمایش دهید.
(ب) بااستفاده ازمتن کتاب ۷ × ۵ و۱۱ × ۷ را به‌صورت مجموع چهارمربع نشان‌دهید.

۲. فرض کنیم $r_۴(n)$ معرف تعداد نمایشهای n به‌صورت‌مجموع چهارمربع باشد. می‌پذیریم که ترتیب نوشتن مربعات را درچنین نمایشی به‌حساب مـی‌آوریم. بدین‌تـرتیب $r_۴(۱)=۸$ مربوط است به ۸ نمایش

$$\begin{aligned}۱&=(\pm۱)^۲+۰^۲+۰^۲+۰^۲=۰^۲+(\pm۱)^۲+۰^۲+۰^۲\\&=۰^۲+۰^۲+(\pm۱)^۲+۰^۲=۰^۲+۰^۲+۰^۲+(\pm۱)^۲.\end{aligned}$$

(آ) $r_۴(۵)$ ، $r_۴(۷)$ ، $r_۴(۱۰)$ را محاسبه کنید.

(ب) نشان‌دهید که $r_۴(n)$ ضربی است.

(ج) نشان‌دهید که دستور

$$r_۴(n)=۸\sum_{\substack{d|n\\ ۴\nmid d}} d$$

بـه‌ازای $n=۵$ ، ۷ ، ۱۰ بـرقرار است . (ایـن دستور متعلق بـه ژاکوبی مـی‌باشد. بـرای اثبات آن بـه صفحهٔ ۳۱۴ کتاب نظریهٔ اعـداد نـوشته هاردی و رایت مـراجعه کنید.)[1]

۳. نشان دهید که اگر $n\equiv۷$ (هنگ ۸) ، آنگاه n به‌صورت مجموع سه مربع نمی‌باشد.

۴. طرح زیر را برای برهان دیگری از لم ۳ تکمیل کنید:

تعداد $(p+۱)/۲$ طبقه متمایز مانده‌ها از اعـداد به‌صورت $x^۲$ و تعداد $(p+۱)/۲$ طبقه متمایز مانده‌ها از اعداد به‌صورت $-(y^۲+۱)$ وجود دارند، بنابراین بایستی xی و yی باشند به‌طوری که $x^۲\equiv-(y^۲+۱)$ (هنگ p) .

۶.۶ معادلهٔ پل $x^۲+dy^۲=۱$

اینک به بحث درمعادلهٔ $x^۲-dy^۲=۱$ ، که در زبان ریاضی به معادلهٔ پل معروف

1. Hardy and Wright, *The Theory of Numbers*, Oxford Universiy Press, Inc., New York, P. 314.

شده است می‌پردازیم. دراینجا فرض می‌کنیم d یك عدد صحیح مثبت باشد. یك حالت معادلهٔ پل ، که خیلی پیش‌پا افتاده است، حالتی است که فرض کنیم به‌ازای عدد صحیحی مانند a ، $d=a^2$. دراین‌صورت

$$1=x^2-dy^2=x^2-a^2y^2=(x-ay)(x+ay)\ ,$$

که صادق است اگر، وفقط اگر، $x-ay=\pm1$ ، $x+ay=\pm1$ ، که با $x=\pm1$ و $y=0$ معادل است. بنابراین ، ازاین پس معادلهٔ پل را به‌ازای $d(>0)$ که برابر با یك مربع کامل نیست درنظر می‌گیریم. ثابت خواهیم کرد که اگر d مساوی مربع کاملی نباشد، آنگاه معادلهٔ پل تعدادی نامتناهی جواب دارد. این امر را ثابت و تقریباً کلیهٔ جوابها را به‌طور صریح ذکر خواهیم کرد. خواهیم دید که مشکلترین قسمت برای به‌دست آوردن این بیان تعیین یك جواب معادلهٔ پل غیراز $(\pm1 , 0)$ است. نشان خواهیم داد که چگونه تعداد نامتناهی از جوابهای دیگر را، از روی جوابی غیراز $(\pm1 , 0)$، محاسبه می‌کنیم. برای اینکه متعلم این روش را درك کند، اجازه دهید ابتدا مطلب را با یك مثال عددی شروع کنیم.

مثال ۹: می‌خواهیم تعدادی نامتناهی از جوابهای معادلهٔ $x^2-2y^2=1$ را بیابیم. واضح است که $x=3$ ، $y=2$ یك جواب است. بنابراین جوابهایی غیراز $x=\pm1$ و $y=0$ وجود دارند. فرض می‌کنیم x_0 و y_0 جواب دلخواهی باشد. دراین‌صورت، حکم می‌کنیم که $x=3x_0+4y_0$ ، $y=2x_0+3y_0$ نیز یك جواب می‌باشد. زیرا

$$x^2-2y^2=(3x_0+4y_0)^2-2(2x_0+3y_0)^2$$
$$=x_0^2-2y_0^2=1\ .$$

به‌عنوان مثال، اگر $x_0=3$ ، $y_0=2$ آنگاه جواب $x=17$ ، $y=12$ را به‌دست می‌آوریم. سپس اگر ۱۷ را با x_0 و ۱۲ را با y_0 نشان دهیم خواهیم داشت $x=99$ ، $y=70$. اگر به‌همین روش ادامه دهیم، تعدادی نامتناهی از جوابهای $x^2-2y^2=1$ را به‌دست می‌آوریم. کلیهٔ جوابها متمایزند، زیراکه y پیوسته زیاد می‌شود. بعداً دراین‌قسمت‌خواهیم دید که، در روش‌فوق برای‌تولید جوابها، هیچ عمل‌تصادفی‌وحساب نشده‌ای‌انجام نداده‌ایم.

معادلهٔ $x^2-dy^2=1$ را اویلر معادلهٔ پل نامیده بود. ولی این موردی (از موارد زیاد در ریاضیات) است که نامی به‌غلط، برروی قضیه‌ای گذاشته شده وبه‌طور وسیعی درنوشته‌های مربوط به‌آن پذیرفته شده‌است. در واقع پل کار چندانی روی معادلهٔ پل‌انجام نداده است. به‌نظر می‌رسد که اولین باری که ذکری از این معادله به‌میان آمده به زمان ارشمیدس[1] برمی‌گردد، هرچندکه معلوم نیست او چقدر در مورد این معادله اطلاع داشته است. یك روش برای حل آن به‌توسط ریاضیدان انگلیسی لرد برانکر[2] درسال ۱۶۵۷ میلادی داده شده بود، که درآن از به‌اصطلاح کسرهای مسلسل استفاده شده بود. والیس[3]

1. Archimedes 2. Lord Brouncker 3. Wallis

و مجدداً فرما مدعی‌شدند که ثابت کرده‌اند که این معادله همواره جوابی غیراز $x = \pm 1$ و $y = 0$ دارد. و فرما برای نخستین‌بار متذکر شد که این معادله همواره تعدادی نامتناهی جواب دارد. طبق معمول، فرما برهان خودش را منتشر نکرد. اولین برهانی که منتشر شد به‌توسط لاگرانژ بود که درسال ۱۷۶۶ میلادی انجام گرفت.

برهان اینکه $x^2 - dy^2 = 1$، به‌ازای کلیهٔ نامربعهای d، می‌تواند حل شود، تاحدی به‌موازات براهینی است که دربخشهای قبلی برای قضایای دو مربع وچهار مربع داده شده است. درابتدا یك اتحاد وجود دارد. سپس نشان می‌دهیم که $x^2 - dy^2 = t$ حل می‌شود. بعداً بااستفاده از همنهشتیها و اتحاد مذکور، نشان می‌دهیم که می‌توانیم t را مساوی ۱ بگیریم. ولی، درمورد معادلهٔ پل گرفتاریها بیشتراز آنهایی هستند که دربخشهای قبلی پدید آمده‌بودند: مثلا، کافی نیست که نشان‌دهیم به‌ازای مقداری از t، $x^2 - dy^2 = t$ می‌تواند حل شود. بلکه به tای احتیاج داریم که تعداد نامتناهی جواب بدهد. علاوه‌براین به روش تازه‌ای برای یافتن t نیازمندیم. (ما همنهشتیها را برای به‌دست آوردن t درقضایای‌دومربع وچهار مربع حل‌کردیم.) هم در به‌دست آوردن t وهم درتحلیلهای متعدد دیگر مربوط به معادلهٔ پل بایستی با عدد گنگ $\sqrt{d}$ دست وپنجه نرم‌کنیم. این امر که حساب اعداد گنگ باید بتواند هرچیزی را درمورد اعداد صحیح به‌ما بگوید به‌هیچ‌وجه بدیهی نیست وبخش حاضر وهمین‌طور ضمیمهٔ ب (که درآن وجود t نشان داده خواهد شد) مارا به‌مطالعهٔ جامع اعدادگنگی از نوع معین وادار می‌کند، که درنیمهٔ دوم این‌کتاب به‌آنها خواهیم پرداخت.

حال مطالعهٔ خود دربارهٔ معادلهٔ پل را بااتحادی‌که قول داده بودیم‌آغاز می‌کنیم:

$$(*) \qquad (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2$$

برای تحقیق این‌اتحاد، صرفاً‌کافی است دوطرف رابسط دهیم. این اتحاد بهما اجازه می‌دهد نامشابه نتایجی راکه درمسائل دومربع و چهار مربع استخراج کرده بودیم به‌دست آوریم (لمهای ۱۰۴ و ۱۰۵). یعنی، اگر (x_1 , y_1) و (x_2 , y_2) هردو جوابهای $x^2 - dy^2 = 1$ باشند، آنگاه می‌توانیم جواب دیگر (x_3 , y_3) رابه‌کمك دستورهای

$$x_3 = x_1x_2 - dy_1y_2 \text{ و } y_3 = x_1y_2 - y_1x_2$$

به‌دست آوریم. مثلا، اگر $d = 2$، $x_1 = 3$، $y_1 = 2$، $x_2 = 99$، $y_2 = 70$، آنگاه می‌بینیم که $x_3 = 17$، $y_3 = 12$ نیز یك جواب می‌باشد. بدین‌ترتیب، معادلهٔ $(*)$ به ما جازه می‌دهد جوابهای جدیدی را از جوابهای مفروض به‌وجود آوریم. حال به‌مسئلهٔ تعیین حداقل یك جواب (غیراز $x = \pm 1$ و $y = 0$) برمی‌گردیم. به‌عنوان نخستین‌گام دراین راه، اجازه دهید نتیجه‌ای راکه به‌نتایج بخشهای پیشین مربوط است و حکم می‌کندکه بعضی از همنهشتیها حل‌پذیرند، بیان‌کنیم. (یعنی، حکم بخش۴ که $p \equiv 1$ (هنگ ۴) ایجاب می‌کندکه $x^2 \equiv -1$ (هنگ p) بتواند حل بشود، وحکم بخش ۵ که

$$x^2 + y^2 \equiv -1 \;(\text{هنگ } p)$$

می‌تواند حل بشود (لم ۳۰۵).)

لم ۲: فرض می‌کنیم $B=2\sqrt{d}+1$. دراین‌صورت تعدادی نامتناهی زوجهای متمایز از اعداد صحیح (x , y) وجود دارند که

$$|x^2-dy^2|\leqslant B$$

به‌عنوان مثال، اگر $d=2$ ، آنگاه $B=2\sqrt{2}+1\leqslant 4$ ، بنابراین ، لم ۲ حکم می‌کند که تعدادی نامتناهی ازاعداد صحیح (x,y) موجودند به‌قسمی که $|x^2-2y^2|\leqslant 4$. البته، لم ۲ به‌خودی‌خود فایده‌ای ندارد، چونکه ثابت خواهیم کرد که $x^2-dy^2=1$ تعدادی نامتناهی جواب دارد، که آشکار است که لم فوق را ایجاب می‌کند. ولی این لم شیوه‌ای است فنی برای وصول به‌این موضوع. برای اثبات این لم روشهای کاملا جدیدی مورد نیاز است، که بیشتر به‌تقریب اعداد گنگ به‌وسیلهٔ اعداد گویا مربوط است. برای اینکه این روشها را درجای واقعی خود درمتن واردکنیم ، اجازه دهید برای بحث دربارهٔ آنها مطالعهٔ خود را درمورد معادلهٔ پل دراین‌نقطه قطع نکنیم. بلکه بگذارید، اثبات لم۲را تاضمیمه ب به‌تعویق بیندازیم ومستقیماً نشان دهیم که چگونه لم۲ ایجاب می‌کند که معادلهٔ پل تعدادی نامتناهی جواب داشته باشد.

قضیهٔ ۳: فرض‌کنیم $d(>0)$ مربع‌کامل نباشد. دراین صورت معادلهٔ سیالهٔ

$$x^2-dy^2=1 \tag{1}$$

برحسب اعداد صحیح x و y ، تعدادی نامتناهی جواب دارد.

برهان: به‌استناد لم۲، تعداد نامتناهی از زوجهای صحیح (x , y) موجودند به‌قسمی که $|x^2-dy^2|\leqslant B$ ، که درآن $B=2\sqrt{d}+1$. ازآنجایی‌که فقط تعداد متناهی ازاعداد صحیح k وجود دارند که $|k|\leqslant B$ و چون هریك ازاعداد x^2-dy^2 عددی است صحیح، لذا عدد صحیحی مانند k وجود دارد به‌طوری که تعداد نامتناهی از زوجهای عدد صحیح (x , y) وجود دارند که درمعادلهٔ

$$x^2-dy^2=k \tag{2}$$

صدق‌می‌کنند. اگر $k=0$، آنگاه $d=(x/y)^2$ ، که این‌حقیقت را که d مربع‌کاملی‌نیست نقض می‌کند. (چرا x/y یك عدد صحیح است؟) بنابراین $k\neq 0$.

حال به جوابهای (x , y) از (۲) به‌هنگ $|k|$ نظر می‌افکنیم. به‌ازای جمیع اعداد صحیح x و y اعداد صحیحی مانند a و b موجودند به‌طوری که $0\leqslant a , b<|k|$ و $x\equiv a(|k|$ هنگ$)$ ، $y\equiv b(|k|$ هنگ$)$. تنها k^2 مقدار ممکن برای زوج (a , b) موجودند. بنابراین، چون (۲) دارای تعدادی نامتناهی جواب است، می‌بینیم که می‌توانیم a و b رابه‌قسمی بیابیم که‌تعداد نامتناهی (x , y) ازجوابهای (۲) در $x\equiv a(|k|$ هنگ$)$، $y\equiv b(|k|$ هنگ$)$ صدق کنند. به‌ازای هر زوج (x_1 , y_1) و (x_2 , y_2) از این جوابها داریم

$$x_1^2-dy_1^2=k \quad , \quad x_2^2-dy_2^2=k$$

و

$$x_1\equiv a\equiv x_2(|k| \text{ هنگ}) \quad , \quad y_1\equiv b\equiv y_2(|k| \text{ هنگ}) . \qquad (3)$$

با استفاده از اتحاد بنیادی (*) به‌دست می‌آوریم

$$k^2=(x_1x_2-dy_1y_2)^2-d(x_1y_2-y_1x_2)^2 .$$

ولی،

$$x_1x_2-dy_1y_2\equiv x_1^2-dy_1^2\equiv 0(|k| \text{ هنگ})$$

$$x_1y_2-y_1x_2\equiv x_1y_1-y_1x_1\equiv 0(|k| \text{ هنگ})$$

بنابراین،

$$1=\left(\frac{x_1x_2-dy_1y_2}{k}\right)^2-d\left(\frac{x_1y_2-y_1x_2}{k}\right)^2 ,$$

پس یك جواب (x , y) برای (۱) به‌دست می‌آوریم:

$$x=\frac{x_1x_2-dy_1y_2}{k} , \quad y=\frac{x_1y_2-y_1x_2}{k} .$$

حال (x_1 , y_1) را یك جواب ثابت (۲) و(۳) می گیریم. چون $k\neq 0$ ، به‌روشنی‌می‌بینیم که یکی از مقادیر x_1 یا y_1 ناصفر می‌باشد. فرض‌کنیم (x_2 , y_2) یك مجموعهٔ نامتناهی از جوابهای (۲) و (۳) را اختیار کند. دراین‌صورت یا x_2 تعداد نامتناهی مقدارمی‌پذیرد یا y_2 ، بنابراین یا x یا y تعداد نامتناهی مقدار می‌پذیرد. (چـرا؟) پس، (x , y) تعداد نامتناهی از جوابهای (۱) را اختیار می کند. ■

اینك روشی برای به‌دست‌آوردن تعداد نامتناهی از جـوابهای (۱) ارائه مـی‌دهیم. برای این مقصود به دو اتحاد زیر احتیاج داریم:

$$(x_1+\sqrt{d}y_1)(x_2+\sqrt{d}y_2)=(x_1x_2+dy_1y_2)+\sqrt{d}(x_1y_2+y_1x_2)$$

$$(x_1-\sqrt{d}y_1)(x_2-\sqrt{d}y_2)=(x_1x_2+dy_1y_2)-\sqrt{d}(x_1y_2+y_1x_2) . \qquad (**)$$

معنی‌این اتحادها این است‌که حاصلضرب دوعدد به‌صورت $x+\sqrt{d}y$ (و یا ، $x-\sqrt{d}y$) مجدداً عددی است به‌همان صورت.

فرض‌کنیم x_1 و y_1 اعداد صحیح باشند. دراین‌صورت، با استفادهٔ مکرر از (**) ، می بینیم‌که اعداد صحیح x_n و y_n وجود دارند به قسمی که

$$(x_1+\sqrt{d}y_1)^n=x_n+\sqrt{d}y_n . \qquad (4)$$

زیرا، به‌ازای $n(\geqslant 2)$ داریم

$$(x_1+\sqrt{d}y_1)^n=(x_1+\sqrt{d}y_1)(x_1+\sqrt{d}y_1)^{n-1}$$
$$=(x_1+\sqrt{d}y_1)(x_{n-1}+\sqrt{d}y_{n-1}),$$

(**) ایجاب می کند که

$$x_n=x_1x_{n-1}+dy_1y_{n-1},\quad y_n=x_1y_{n-1}+y_1x_{n-1}. \tag{5}$$

به‌همین‌طریق،

$$(x_1-\sqrt{d}y_1)^n=x_n-\sqrt{d}y_n,$$

که درآن x_n و y_n می‌توانند، بااستفاده از معادلات (۵) ، برحسب x_1 و y_1 محاسبه‌شوند.

لم ۴: فرض‌کنیم $n>0$ و (x_1, y_1) یك جواب معادلهٔ پل $x^2-dy^2=1$ باشد. فرض کنیم x_n و y_n به‌توسط

$$(x_1+\sqrt{d}y_1)^n=x_n+\sqrt{d}y_n$$

تعریف شده باشند. دراین‌صورت (x_n, y_n) یك جواب $x^2-dy^2=1$ می‌باشد.

برهان: داریم

$$(x_1-\sqrt{d}y_1)^n=x_n-\sqrt{d}y_n,$$

بنابراین،

$$x_n^2-dy_n^2=(x_n+\sqrt{d}y_n)(x_n-\sqrt{d}y_n)$$
$$=(x_1+\sqrt{d}y_1)^n(x_1-\sqrt{d}y_1)^n$$
$$=((x_1+\sqrt{d}y_1)(x_1-\sqrt{d}y_1))^n$$
$$=(x_1^2-dy_1^2)^n=1^n=1. \qquad \blacksquare$$

مثال ۵: مجدداً $x^2-2y^2=1$ را درنظر می گیریم. قرار مـی‌دهیم $x_1=3$ ، $y_1=2$. دراین‌صورت x_n و y_n را به‌توسط

$$x_n+\sqrt{2}y_n=(3+2\sqrt{2})^n$$

تعریف می‌کنیم، بنابراین

$$(3+2\sqrt{2})^2=17+12\sqrt{2}$$
$$(3+2\sqrt{2})^3=(17+12\sqrt{2})(3+2\sqrt{2})=99+70\sqrt{2},$$

که جوابهای مفروض درمثال ۱ ، یعنی (۱۲ ، ۱۷) ، (۷۰ ، ۹۹) را به‌دست می‌دهند. توجه کنید که دستورهای مثال ۱ دقیقاً همان روابط (۵) هستند، یعنی بازای $n \geqslant ۲$ ،

$$x_n = ۳x_{n-۱} + ۴y_{n-۱} \text{ ، } y_n = ۲x_{n-۱} + ۳y_{n-۱} \cdot$$

به‌ازای $n = ۲$ ، می‌بینیم که به‌ازای هرجواب $(x_۱ \text{ ، } y_۱)$ از (۱) ،

$$x_۲ = ۳x_۱ + ۴y_۱ \text{ ، } y_۲ = ۲x_۱ + ۳y_۱$$

یك جواب (۱) می‌باشد.

حال که ماشینی برای‌تولید جوابها ازیك‌جواب‌ساده داریم، می‌توانیم کلیه جوابها را بیابیم. ابتدا، توجه کنید که اگر $(x \text{ ، } y)$ یك جواب باشد، آنگاه به‌ازای هرحالت ممکن برای انتخاب علامتها $(\pm x \text{ ، } \pm y)$ نیز یك جواب است. بنابراین، کافی است کلیهٔ جوابهایی را تعیین کنیم که درآنها $x \geqslant ۰$ ، $y \geqslant ۰$. علاوه‌براین، بدیهی است ملاحظه کنیم که تنها جوابهایی که به‌ازای آنها x یا y صفر می‌باشد یا y ، عبارت‌انداز $(\pm ۱ \text{ ، } ۰)$. بنابراین، کافی است کلیهٔ جوابهایی را تعیین کنیم که به‌ازای آنها $x > ۰$ ، $y > ۰$. چنین جوابهایی جوابهای مثبت نامیده می‌شوند. می‌توان راه ساده‌ای برای تعیین مثبت بودن یا نبودن یك جواب ارائه کرد.

لم ۶ : فرض کنیم $(x \text{ ، } y)$ یك جواب $x^۲ - dy^۲ = ۱$ باشد. دراین‌صورت $(x \text{ ، } y)$ جوابی مثبت است اگر، وفقط اگر،

$$x + \sqrt{d}y > ۱ \cdot \qquad (۶)$$

برهان: اگر $x > ۰$ و $y > ۰$ آنگاه $x \geqslant ۱$ و $y \geqslant ۱$ ؛ بنابراین

$$x + \sqrt{d}y \geqslant ۱ + \sqrt{d} \geqslant ۲ > ۱ \cdot$$

بالعکس، فرض کنیم (۶) صادق باشد. اگر یکی از مقادیر x یا y صفر باشد، آنگاه $(x \text{ ، } y) = (\pm ۱ \text{ ، } ۰)$ که به‌ازای آنها (۶) برقرار نیست. بنابراین، فرض کنیم $x \neq ۰$، $y \neq ۰$. چهار حالت برای x و y درنظر می‌گیریم.

حالت ۱: $x < ۰$ و $y < ۰$. دراین‌حالت $x + \sqrt{d}y < ۰$ و (۶) برقرار نیست.

حالت ۲: $x > ۰$ و $y < ۰$. دراین‌حالت، $x - \sqrt{d}y \geqslant ۱ + \sqrt{d} > ۱$ ، بنابر (۶) و (۱) ، داریم

$$۱ = x^۲ - dy^۲ = (x - \sqrt{d}y)(x + \sqrt{d}y) > ۱ \times ۱ = ۱$$

که ممتنع می‌باشد.

حالت ۳: $x<0$ و $y>0$. دراین صورت $-x+\sqrt{d}y>1$، و مجدداً بنابر (۶) و (۱)، داریم

$$-1=-x^2+dy^2=(-x+\sqrt{d}y)(x+\sqrt{d}y)>1\times 1=1$$

که ممتنع می‌باشد.

بنابراین تنها حالت ممکن آن است که $x>0$ و $y>0$. ■

حال به داستان کامل مربوط به جوابهای معادلهٔ پل می‌پردازیم. به استناد قضیهٔ (۳) می‌دانیم که معادلهٔ $x^2-dy^2=1$، در اعداد صحیح، دارای حداقل یک جواب (x_0, y_0) با $x_0\neq 0$، $y_0\neq 0$ می‌باشد. علاوه براین، چون به ازای هرحالت ممکن برای انتخاب علامتها، $(\pm x_0, \pm y_0)$ نیز یک جواب می‌باشد، می‌بینیم که حداقل یک جواب مثبت، مثل (x'_0, y'_0) دارد. می‌گیریم $M=x'_0+\sqrt{d}y'_0$. اگر (x_1, y_1) یک جواب مثبت $x_1^2-dy_1^2=1$ باشد، آنگاه شرط

$$x_1+\sqrt{d}y_1\leqslant M \tag{۷}$$

ایجاب می‌کند که $x_1\leqslant M$ و $y_1\leqslant M$. بنابراین، بالاخص، فقط تعدادی متناهی انتخاب برای x_1 و y_1 وجود دارد. بیاییم جواب مثبت (x_1, y_1) را که به ازای آن $x_1+\sqrt{d}y_1$ حداقل است انتخاب کنیم. این امر ممکن است، زیرا (۱) فقط تعدادی متناهی جواب مثبت دارد. (x_1, y_1) را یک جواب بنیادی معادلهٔ پل می‌نامیم. اینک می‌توانیم قضیهٔ اصلی خود را دربارهٔ معادلهٔ پل بیان کنیم.

قضیهٔ ۷: فرض کنیم (x_1, y_1) یک جواب مثبت معادلهٔ پل که به ازای آن $x_1+\sqrt{d}y_1$ حداقل است، باشد. به ازای هرعدد صحیح مثبت n، x_n و y_n را به توسط رابطهٔ

$$x_n+\sqrt{d}y_n=(x_1+\sqrt{d}y_1)^n$$

تعریف می‌کنیم. دراین صورت کلیهٔ جوابهای معادلهٔ پل، $x^2-dy^2=1$، به توسط

$$(x, y)=(\pm 1, 0) \text{ و } (x, y)=(\pm x_n, \pm y_n) \tag{۸}$$

داده می‌شوند، که در اینجا کلیهٔ انتخابهای ممکن برای علامتها مجاز می‌باشند. بعلاوه، کلیهٔ این جوابها متمایزند.

برهان: با استناد به لم ۴ می‌دانیم که کلیهٔ مقادیر (x_n, y_n) از (۴)، در واقع جوابهای $x^2-dy^2=1$ می‌باشند. حال ثابت می‌کنیم که (x, y)های مندرج در (۸) تماماً متمایزند. چون x_1 و y_1 هر دو مثبت‌اند، از معادلات (۵) معلوم می‌شود که به ازای کلیهٔ مقادیر n، $x_n>0$ و $y_n>0$ (از استقرا استفاده کنید)، از این‌رو هیچیک ازمقادیر $(\pm x_n, \pm y_n)$ نمی‌توانند مساوی $(\pm 1, 0)$ باشند. بدین‌ترتیب ثابت می‌کنیم که زوجهای $(\pm x_n, \pm y_n)$

تماماً متمایزند. واضح است که چون $x_n > 0$ و $y_n > 0$ ، کافی است ثابت کنیم که زوجهای (x_n , y_n) تماماً متمایزند. ولی، چون (x_1 , y_1) یك جواب مثبت است، بنابر لم ۶، داریم $x_1 + \sqrt{d} y_1 > 1$. اما، اگر مثلا به ازای $n < m$ داشته باشیم ، $(x_n , y_n) = (x_m , y_m)$ آنگاه بایستی داشته باشیم

$$(x_1 + \sqrt{d} y_1)^n = x_n + \sqrt{d} y_n = x_m + \sqrt{d} y_m = (x_1 + \sqrt{d} y_1)^m$$

بنابراین

$$(x_1 + \sqrt{d} y_1)^{m-n} = 1$$

که ممکن نیست ، زیرا $x_1 + \sqrt{d} y_1 > 1$. بنابراین ، کلیهٔ (x , y) های مذکور در (۸) متمایزند .

فرض کنیم (u , v) یك جواب $x^2 - dy^2 = 1$ باشد . چون $(\pm 1 , 0)$ تنها جوابهایی هستند که درآنها یکی از مقادیر x یا y مساوی صفر است، وچون اگر (x , y) یك جواب باشد آنگاه زوجهای $(\pm x , \pm y)$ نیز جواب هستند، بی آنکه خللی به کلیت واردآید، می‌توانیم فرض کنیم $u > 0$ ، $v > 0$. حال نشان می‌دهیم که به ازای یك مقدار $n (\geqslant 1)$ ، $(u , v) = (x_n , y_n)$.

چون (x_1 , y_1) به عنوان یك جواب مثبت $x^2 - dy^2 = 1$ ، که در آن $x_1 + \sqrt{d} y_1$ حداقل می‌باشد، انتخاب شده است، می‌بینیم که

$$x_1 + \sqrt{d} y_1 \leqslant u + \sqrt{d} v . \qquad (۹)$$

می‌گوییم عدد مثبتی مانند n موجود است به قسمی که

$$(x_1 + \sqrt{d} y_1)^n \leqslant u + \sqrt{d} v < (x_1 + \sqrt{d} y_1)^{n+1} . \qquad (۱۰)$$

زیرا ملاحظه کرده‌ایم که $x_1 + \sqrt{d} y_1 > 1$ ، بنابراین $(x_1 + \sqrt{d} y_1)^n$ به اندازهٔ دلخواه بزرگ می‌شود. پس، برای n بزرگترین مقداری وجود دارد به طوری که

$$u + \sqrt{d} v \geqslant (x_1 + \sqrt{d} y_1)^n .$$

بنابر (۹) این بزرگترین مقدار n حداقل ۱ است. بعلاوه واضح است که این بزرگترین مقدار n موجب می‌شود که (۱۰) برقرار باشد.

حال (۱۰) را در $(x_1 - \sqrt{d} y_1)^n$، که مثبت می‌باشد ــ زیرا که $x_1 + \sqrt{d} y_1 > 0$ و $(x_1 + \sqrt{d} y_1)(x_1 - \sqrt{d} y_1) = x_1^2 - dy_1^2 = 1$ ــ ضرب می‌کنیم . در این صورت می‌بینیم که

$$1 \leqslant (u + \sqrt{d} v)(x_1 - \sqrt{d} y_1)^n < x_1 + \sqrt{d} y_1 \qquad (۱۱)$$

یادآوری می‌کنیم که $(x_1 - \sqrt{d} y_1)^n = x_n - \sqrt{d} y_n$. قرارمی‌دهیم $u_1 = ux_n - dvy_n$ و $v_1 = vx_n - y_n u$. دراین‌صورت $(u + \sqrt{d} v)(x_1 - \sqrt{d} y_1)^n = u_1 + \sqrt{d} v_1$. بعلاوه،

یك محاسبهٔ ساده نشان می‌دهد که

$$u_1^2-dv_1^2=(u^2-dv^2)(x_n^2-dy_n^2)=1 \, .$$

بنابراین، (u_1 , v_1) یك جواب معادلهٔ $x^2-dy^2=1$ است. علاوه براین، (۱۱) حکم می کند که

$$1\leqslant u_1+\sqrt{d}v_1<x_1+\sqrt{d}y_1 \, . \qquad (12)$$

اگر $u_1+\sqrt{d}\, v_1>1$، آنگاه، بنابر لم ۶، (u_1 , v_1) یك‌جواب‌مثبت $x^2-dy^2=1$ است. ولی، اگرچنین‌باشد، (۱۲) ناقض نحوه انتخاب (x_1 , y_1) است. بدین ترتیب‌باید داشته باشیم $u_1+\sqrt{d}v_1\leqslant 1$. ولی، (۱۲) ایجاب‌می کند که $u_1+\sqrt{d}v_1=1$. بنابراین،

$$(u+\sqrt{d}v)(x_1-\sqrt{d}y_1)^n=1 \, .$$

از ضرب کردن هردو طرف این معادله در $(x_1+\sqrt{d}y_1)^n$، می‌بینیم که

$$u+\sqrt{d}v=(x_1+\sqrt{d}y_1)^n=x_n+\sqrt{d}y_n \qquad (13)$$

بدین ترتیب، $u-x_n=\sqrt{d}(y_n-v)$. اگر $y_n-v\neq 0$، خواهیم داشت

$$\sqrt{d}=\frac{u-x_u}{y_n-v}$$

پس،

$$d=\left(\frac{u-x_n}{y_n-v}\right)^2 ,$$

که متناقض با مربع‌کامل نبودن d است. (چرا $(u-x_n)/(y_n-v)$ عددی صحیح است؟) بنابراین، تناقضی حاصل شده است و در نتیجه $y_n-v=0$. دراین صورت، بنابر (۱۳) داریم $u=x_n$، پس ثابت‌کرده‌ایم که $(u , v)=(x_n , y_n)$. ■

مثال ۸ : مجدداً معادلهٔ $x^2-2y^2=1$ را درنظرمی گیریم. قبلا ملاحظه کرده‌ایم که $x=3$ و $y=2$ یك جواب می‌باشد. بنابراین‌کوچکترین جواب (x_1 , y_1) بایستی در

$$x_1+\sqrt{2}y_1\leqslant 3+\sqrt{2}\times 2<6$$

صدق کند و بنابراین $x_1\leqslant 5$ و $y_1\leqslant 5$. بسهولت‌دیده می‌شود که تنها زوج جواب x، y از $x^2-2y^2=1$ که در $0<x\leqslant 5$ و $0<y\leqslant 5$ صدق مـی کنند $x=3$ و $y=2$ می‌باشند (کلیهٔ حالات را امتحان‌کنید) بنابراین $x_1=3$ و $y_1=2$، و بدین ترتیب کلیهٔ جوابهای $x^2-2y^2=1$ به‌توسط $x=\pm x_n$ و $y=\pm y_n$ (والبته $x=\pm 1$ ، $y=0$) داده می‌شوند، که درآن

$$x_n+\sqrt{2}y_n=(3+\sqrt{2}\times 2)^n \, .$$

ملاحظه می‌کنیم که می‌توانیم x_n و y_n را به‌طور تراجعی از x_{n-1} و y_{n-1} به‌توسط (۵) آسانتر به دست آوریم.

$$x_n = 3x_{n-1} + 4y_{n-1} \text{ ،} \quad y_n = 2x_{n-1} + 3y_{n-1}$$

این نتیجه را بامثال ۱ مقایسه کنید.

باید متذکر شد که قضیهٔ ۷ به‌ما اجازه می‌دهد کلیهٔ جوابهای (۱) را، وقتی که جواب «کمترین» را می‌دانیم، تعیین کنیم. همچنین از بحث فوق‌معلوم می‌شود که، اگرما یك‌جواب (۱) را باشرط $y \neq 0$ بدانیم، تعیین‌جواب «کمترین»کارساده‌ای است. ولی، درعمل،تعیین جوابی برای (۱)، می‌تواند کار پرزحمتی‌باشد، زیرا حتی برای‌مقادیر کوچك d، x_1 و y_1 «کمترین»می‌توانند خیلی بزرگ‌باشند. مثلا، به‌ازای$d = 46$، خواهیم‌داشت$x_1 = 24335$و $y_1 = 3588$. ما هیچ روشی برای تعیین یك جواب ارائه نداده‌ایم. البته یك روش وجود داردکه روش کسرهای مسلسل نامیده می‌شود. متعلمین علاقمند می‌توانند به کتاب مقدمه‌ای برنظریهٔ اعداد نوشته هاردی و رایت‌چاپ دانشگاه‌آکسفرد صفحات۱۲۹ تا ۱۵۳رجوع کنند.

یك نتیجهٔ خیلی ساده دربارهٔ معادلهٔ کلیتر

$$x^2 - dy^2 = k \text{ ،} \tag{۱۴}$$

به‌ازای عدد ثابت k، وجود داردکه هم اکنون می‌توانیم به دست آوریم. همان‌گونه که قبلا بارها ملاحظه کرده‌ایم، (۱۴) ممکن است اصلا جوابی نداشته باشد. به‌عنوان یك مثال کلی، اگر$d(=p)$ عدد اولی‌باشد، $p \nmid k$ و $\left(\frac{k}{p}\right) = -1$، آنگاه (۱۴) می‌تواند جوابی نداشته باشد. زیرا یك جواب (۱۴) جوابی برای

$$x^2 \equiv k \pmod{p}$$

خواهد بود، که متناقض بافرض $\left(\frac{k}{p}\right) = -1$ است. درنیمهٔ دوم این کتاب‌ما روی این‌مسئله که به ازای چه مقادیری ازk، (۱۴) می‌تواند حل شود، بحث خواهیم کرد. فعلا به قضیهٔ زیر می‌پردازیم:

قضیهٔ ۹: اگر $x^2 - dy^2 = k$ یك جواب داشته باشد، آنگاه تعدادی نامتناهی جواب خواهدداشت.

برهان: اگر x_1، y_1 یك جواب (۱۴) و x_2، y_2 یك جواب (۱) باشند، آنگاه $x = x_1x_2 + dy_1y_2$، $y = x_1y_2 + y_1x_2$ یك جواب (۱۴) است. وقتی که x_2 و y_2 کلیهٔ جوابهای (۱) را اختیار کند (تعدادی‌نامتناهی‌ازاین‌جوابها باشرط $x_2 > 0$ و $y_2 > 0$ وجود دارند)، به‌آسانی‌می‌بینیم که تعدادی نامتناهی‌جواب برای (۱۴) به‌دست‌می‌آید. ■

مثال ۱۰: چون $5^2 - 2 \times 3^2 = 7$، x_n و y_n $(n \geqslant 0)$ رابا ضابطهٔ

$$x_n+\sqrt{۲}\,y_n=(۳+\sqrt{۲}\times ۲)^n(۵+\sqrt{۲}\times ۳)$$

تعریف می‌کنیم. دراین صورت به‌ازای کلیهٔ مقادیر $n(\geqslant ۰)$ ، $x_n^۲-۲y_n^۲=۷$. به‌عنوان مثال اگر $n=۱$ ، آنگاه

$$x_۱=۳\times ۵+۲\times ۲\times ۳=۲۷$$
$$y_۱=۳\times ۳+۲\times ۵=۱۹$$

و در نتیجه $۲۷^۲-۲\times ۱۹^۲=۷$.

۶.۶ تمرینات

۱. به ازای اعداد صحیح a و n ، کلیهٔ جوابهای $x^۲-a^۲y^۲=n$ را تعیین کنید.

۲. تعدادی نامتناهی جواب برای معادلهٔ سیالهٔ $x^۲-۳y^۲=۶$ بیابید.

۳. جوابهای بنیادی معادلات پل زیرین را محاسبه کنید:

(آ) $x^۲-۸y^۲=۱$ (ب) $x^۲-۷y^۲=۱$ (ج) $x^۲-۳y^۲=۱$
(د) $x^۲-۱۵y^۲=۱$ (ه) $x^۲-۱۷y^۲=۱$.

۴. کلیهٔ جوابهای معادلات سیالهٔ (آ) تا (ه) در تمرین ۳ را محاسبه کنید.

۵. فرض کنیم $(x_۱ , y_۱)$ یک جواب مثبت معادلهٔ پل باشد که به ازای آن $x_۱+\sqrt{d}\,y_۱$ حداقل است. به‌ازای هر عدد صحیح n (مثبت، منفی، یا صفر) x_n و y_n را چنین تعریف می‌کنیم

$$x_n+\sqrt{d}\,y_n=(x_۱+\sqrt{d}\,y_۱)^n .$$

در این صورت نشان دهید که کلیهٔ جوابهای معادلهٔ $x^۲-dy^۲=۱$ به توسط $(x , y)=(x_n , y_n)$ و $(x , y)=(-x_n , -y_n)$ داده می‌شوند. بعلاوه کلیهٔ این جوابها متمایزند.

۶. فرض کنیم d عدد صحیح نامربعی باشد، و فرض کنیم معادلهٔ سیالهٔ $x^۲-dy^۲=-۱$ یک جواب $(x_۰ , y_۰)$ داشته باشد.

(آ) نشان‌دهید که چگونه کلیهٔ جوابهای این‌معادله برحسب کوچکترین جواب (x , y) را ، که به ازای‌آن $x+y\sqrt{d}>۱$ ، (موسوم به‌جواب بنیادی) باید تعیین کنیم.

(ب) نشان دهید که همواره یک جواب بنیادی وجود دارد.

(ج) نشان دهید که اگر $(x_۱ , y_۱)$ یک جواب بنیادی $x^۲-dy^۲=-۱$ باشد ، آنگاه‌باقراردادن $(x_۱+y_۱\sqrt{d})^۲=x+y\sqrt{d}$ ، (x , y) یک جواب بنیادی‌معادلهٔ پل، $x^۲-dy^۲=۱$ خواهد شد.

۷. نشان دهید که تعدادی نامتناهی‌جواب (x , y) برای معادلهٔ پل موجود است به‌طوری که $y\equiv ۰ \pmod N$ (هنگ N) N عدد صحیح مفروضی است.

۸. فرض کنیم Γ مجموعه‌ای از اعداد حقیقی مثبت باشد که در سه‌خاصیت زیر صدق می‌کند:

(یکم) اگر γ_1 و γ_2 به Γ متعلق باشند $\gamma_1\gamma_2$ نیز به‌آن‌متعلق باشد؛ (دوم) اگر γ متعلق به Γ باشد، γ^{-1} نیز به‌آن متعلق باشد؛ (سوم) بازه‌ای شامل ۱ وجود داشته باشد که فقط تعدادی متناهی‌از اعضای Γ را دربر بگیرد. نشان دهید که Γ دقیقاً مجموعهٔ کلیهٔ قوای (مثبت، منفی، یا صفر) عضوی از Γ است.

۹. ما دستوری جهت اعداد فیبوناتچی که در زیر تعریف شده‌اند استخراج خواهیم کرد: $f_0=0$، $f_1=1$ و به‌طور تراجعی، به ازای $n\geqslant 2$، $f_n=f_{n-1}+f_{n-2}$.

(آ) اعداد صحیح a و b و یك عدد صحیح مثبت n مفروض‌اند، نشان‌دهید که اعداد صحیح c و d موجودند به قسمی که

$$\left(a+\frac{1+\sqrt{5}}{2}b\right)^n=c+\frac{1+\sqrt{5}}{2}d\,.$$

(ب) اعداد صحیح c_n و d_n را به‌توسط

$$\left(\frac{1+\sqrt{5}}{2}\right)^n=c_n+\left(\frac{1+\sqrt{5}}{2}\right)d_n$$

تعریف می‌کنیم، نشان دهید که به ازای $n\geqslant 0$، $d_n=f_n$.

(ج) نشان دهید که

$$\left(\frac{1-\sqrt{5}}{2}\right)^n=c_n+\left(\frac{1-\sqrt{5}}{2}\right)d_n$$

(با همان c_n و d_n در قسمت (ب)).

(د) نشان دهید که

$$f_n=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n\,.$$

۱۰. (آ) فرض کنیم $d>0$ عدد صحیحی‌خالی‌ازمربع باشد به‌طوری که $d\equiv 1\ (4 \text{ هنگ})$. فرض کنیم $f(x,y)=x^2+xy+((1-d)/4)y^2$. نشان دهید که $f(x,y)=1$ تعدادی نامتناهی جواب دارد.

(راهنمایی: ملاحظه کنید که $x+y\sqrt{d}=(x-y)+((1+\sqrt{d})/2)(2y)$ و نیز
$f(x,y)=(x+((1+\sqrt{d})/2)y)(x+((1-\sqrt{d})/2)y)$.)

(ب) نشان دهید که اگر $f(x_0,y_0)=1$ و x_n و y_n به توسط

$$x_n+\frac{1+\sqrt{d}}{2}y_n=\left(x_0+\frac{1+\sqrt{d}}{2}y_0\right)^n$$

(n عدد صحیح دلخواهی است، خواه مثبت خواه منفی) تعریف شوند، آنگاه x_n و y_n اعدادی صحیح می‌باشند و $f(x_n,y_n)=1$.

(ج) نشان دهید که $f(x , y)=1$ یک‌جواب x_0 ، y_0 دارد به طوری که $x_0>0$، $y_0>0$ و $x_0+((1+\sqrt{d})/2)y_0$ کمترین است.

(د) به وسیله‌ی (x_0 , y_0)ی که در قسمت (ج) تعیین‌شد و زوجهای (x_n , y_n) که در قسمت (ب) تعیین شدند نشان دهید که کلیهٔ جوابهای $f(x , y)=1$ به توسط $(x , y)=(x_n , y_n)$ یا $(x , y)=(-x_n , -y_n)$ $(n=0 , \pm 1 , \pm 2 , \ldots)$ داده می‌شوند.

ضمیمهٔ ب

تقریبات دیوفانتوسی

مطلب را با توجه به عدد π ، که یونانیان عهد قدیم به‌صورت نسبت محیط دایره برقطرش، تعریف کرده‌اند، آغاز می‌کنیم. همچنانکه همهٔ ما در دبیرستان آموخته‌ایم ، π همان ۲۲/۷ «است» . در حقیقت مجلس مقننهٔ یکی از ایالات امریکا تا آنجا پیش رفت که قانونی گذرانید دایر براینکه π باید ۲۲/۷ باشد (آخر، «احتیاجی به‌این نیست که‌ریاضیات را بیش‌ازحد لزوم دشوار کنیم»). واقعاً ، درمورد مقدار تقریبی ۲۲/۷ برای π که اول بار توسط ارشمیدس در ۲۱۲ قبل از میلاد ارائه شده است مطلب زیادی باید گفته شود . عدد

$$\pi = ۳٫۱۴۱۵۹۲۶۵۳۵ \ldots$$

یك عدد اعشاری نامتناهی می‌باشد و بنابراین ، استفاده ازآن درجریان محاسبات بسیار دشواراست. به‌طور قطع شخص در استفاده از ۲۲/۷ بیشتر احساس راحتی می‌کند، زیرا هنگامی‌که با اعداد صحیح (و نسبتهای آنها) بویژه با اعداد صحیح کوچك سروکار داریم خود را راحت‌تر حس می‌کنیم. در واقع ، ۲۲/۷ نسبت دو عدد صحیح کوچك (۲۲ و ۷) می‌باشد و

$$\frac{۲۲}{۷} = ۳٫۱۴۲۸۵۷ \ldots$$

تقریب نسبتاً خوبی برای π می‌باشد (اختلافش برابر ... ۰٫۰۰۱۲۶ است). در حقیقت می‌توان نشان‌داد که اختلاف $|۲۲ - ۷\pi|$ ازاختلاف $|q\pi - p|$، به‌ازای کلیهٔ کسرهای p/q به‌طوری که $۱ \leqslant q \leqslant ۱۰۵$ ، کوچکتراست. درحقیقت، π یك تقریب استثنایی دیگری دارد که ۳۵۵/۱۱۳ است. این کسر دارای این خاصیت است که اختلاف $|۳۵۵ - ۱۱۳\pi|$ از اختلاف $|q\pi - p|$ ، به ازای کلیهٔ کسرهای p/q به طوری که $۱ \leqslant q \leqslant ۳۳۱۰۱$

کوچکتر می‌باشد. این کسر تا شش‌رقم اعشار دقیق‌می‌باشد (خطا کمتر از ۰٫۰۰۰۰۰۰۲۶۸ است) زیرا

$$\frac{۳۵۵}{۱۱۳}=۳٫۱۴۱۵۹۲۹۲۰۳ \ldots$$

این تقریبات برای π بی‌اندازه خوب می‌باشند، و در واقع بهتر از تقریباتی هستند که اکثر اعداد اصم از آن برخوردارند. تا چه اندازه انتظار داریم بتوانیم یك عدد حقیقی را به اعداد منطق با مخارج کوچك نزدیك کنیم؟ روشن بگوییم، فرض کنید α عددی حقیقی و $N(>۱)$ عدد صحیح ثابتی باشد. در میان کلیهٔ کسرهای p/q به‌طوری که $۱\leqslant q\leqslant N$ چه مقدار می‌توانیم $|\alpha-p/q|$ را کوچك بسازیم؟ به‌این‌سؤال درقضیهٔ ۱ جواب داده خواهد شد، ولی ابتدا اجازه دهید مثال دیگری را مطالعه کنیم.

اکنون مسئلهٔ طرح یك تقویم را درنظرمی گیریم. مدت زمانی که لازم است زمین یك دورکامل به دور خورشید بزند ۳۶۵ روز، ۵ ساعت، ۴۸ دقیقه، و ۴۶ ثانیه محاسبه شده است. از آنجایی که می‌خواهیم سالهای ما تعداد صحیحی روز داشته باشند، بایستی طول سالها را تغییر دهیم. روش مؤثر برای انجام این کار کدام است؟ چون هرروز ۸۶۴۰۰ ثانیه است و ۵ ساعت و ۴۸ دقیقه و ۴۶ ثانیه برابر ۲۰۹۲۶ ثانیه می‌باشد، زمان واقعی برای اینکه زمین خورشید را دور بزند به‌اندازهٔ ۲۰۹۲۶/۸۶۴۰۰ روز از سال تقویمی ۳۶۵ روزه زیادتراست. بنابراین، با افزودن ۲۰۹۲۶ روزدرپایان ۸۶۴ قرن می‌توان تقویم را اصلاح کرد. بدیهی است که این کارمناسبی نیست. چیزی که ما نیاز داریم یك تقریب منطقی است از عدد ۲۰۹۲۶/۸۶۴۰۰ که استفاده از آن برای تصحیح تقویم آسان‌تر باشد. داشتن تقریبی مانند p/q که q مقدار کوچکی باشد زحمت ما را کم می‌کند. تقریبات متعددی مورد استفاده واقع شده است. در ۴۵ قبل از میلاد ژول سزار[1] از تقریب ۱/۴ استفاده می‌کند با این قرارداد که در هر ۴ سال ۱ سال ۳۶۶ روز داشته باشد. این تقریب نسبتاً خوبی است و در هر ۱۲۸ سال ۱ روز اختلاف دارد. کسر ۸/۳۳ به‌توسط عمرخیام در ۴۵۸ هـ. ش. (۱۰۷۹ میلادی) پیشنهاد شده بود و به افزایش فارسی موسوم است. این افزایش دقیقتر از افزایش ژول سزار است. تقویمی که ما به‌کار می‌بریم با طرح زیر مطابقت دارد. هر سالی که بر ۴ بخشپذیر باشد به‌استثنای سالهایی که بر ۱۰۰ بخشپذیرند ولی بر ۴۰۰ بخشپذیر نیستند یك سال کبیسه است (مثلا ۱۹۰۰ یك سال کبیسه نیست ولی ۲۰۰۰ کبیسه است). این، متناظر با تقریب ۹۷/۴۰۰ بجای ۲۰۹۲۶/۸۶۴۰۰ است. این تقویم درهر سال ۲۶ ثانیه کسر می‌آورد. مزیت ۹۷/۴۰۰ بر، مثلا، ۸/۳۳ که نزدیکتر از ۹۷/۴۰۰ است، این است که اصلاحات آن راساده‌تر می‌توان به‌خاطر سپرد. درحقیقت، پیشنهاد شده است که سال کبیسه ۴۰۰۰ و کلیهٔ سالهای دیگر که مضربی از ۴۰۰۰ می‌باشند حذف شود. این روش دقت تقویم را فقط یك روز در ۲۰۰ قرن کم می‌کند.

---

1) Julius Ceasar

قبل از اینکه مطالب این ضمیمه را رسمیتر شروع کنیم، مسئلهٔ تعیین عملی این تقریبات خوب گویا را در نظر می‌گیریم. در آنچه که در زیر می‌آید نشان خواهیم داد که این تقریبات را چه اندازه می‌توان خوب انتخاب کرد، ولی روشی برای تعیین تقریبات ارائه نخواهیم داد. درحقیقت یك روش سازنده‌ای برای تعیین این تقریبات وجود دارد که روش کسرهای مسلسل نام دارد. این مبحثی است که معمولا درهمهٔ کتابهای مقدماتی نظریهٔ اعداد هست (برای مثال به مقدمه‌ای بر نظریهٔ اعداد نوشتهٔ نیون وتسوکرمان [1] رجوع کنید). و به دانشجویان توصیه می‌کنیم که این موضوع گیرا را دنبال کنند.

حال نشان خواهیم داد که چقدر می‌توان $|\alpha - p/q|$ را کوچك کرد. این قضیه، معمولا قضیهٔ دیریکله نامیده می‌شود، با اینکه به‌طور قطع کسان دیگری قبل از او بر آن وقوف داشته‌اند.

قضیهٔ ۱: فرض کنیم α عددی حقیقی و $N(>1)$ عددی صحیح باشد. عدد صحیحی مانند q موجود است به قسمی که $1 \leqslant q \leqslant N$ و

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}. \tag{1}$$

برهان قضیهٔ ۱ متکی بر گزارهٔ سهلی است که به نامهای مختلف مثلا اصل لانهٔ کبوتر یا اصل حجره (دیریکله) خوانده می‌شود:

اگر $N+1$ شیء را در N حجره قراردهیم، آنگاه حداقل یکی از این حجره‌ها، بایستی شامل بیش از یك شیء باشد.

بعضی از نتایج فصل ۶ را می‌توانستیم از این طریق ثابت کنیم، برای مثال برهان دیگری را برای لم ۳.۵.۶ درتمرین ۴ در بخش ۵.۶ توصیه کردیم.

نتیجهٔ (۱) قضیهٔ ۱ را می‌توان به راحتی به صورت دیگر نوشت:

عددی صحیح مانند q موجود است به قسمی که $1 \leqslant q \leqslant N$ و

$$|q\alpha - p| \leqslant \frac{1}{N}.$$

برهان قضیهٔ ۱: اعداد $0 = 0 \times \alpha$ ، $\alpha - [\alpha]$ ، $2\alpha - [2\alpha]$ ، … ، $N\alpha - [N\alpha]$ را در نظر می‌گیریم. یعنی اعداد $k\alpha - [k\alpha]$ را به ازای $0 \leqslant k \leqslant N$ در نظر می‌گیریم. این $N+1$ عدد اشیاء ماخواهند بود. کلیهٔ آنها بین ۰ و ۱ قراردارند. بازهٔ ۰ تا ۱ را به N زیربازهٔ مساوی تقسیم می‌کنیم (به‌شکل ب-۱ مراجعه کنید):

$$0 = \frac{0}{N} \text{ تا } \frac{1}{N} \text{ و } \frac{1}{N} \text{ تا } \frac{2}{N}, \frac{2}{N} \text{ تا } \frac{3}{N}, \ldots, \frac{N-1}{N} \text{ تا } \frac{N}{N} = 1$$

---

1. I. Niven and H. Zuckerman, *An Introduction to the Theory of Numbers*, 3rd ed. Wiley, 1973.

شکل ب.۱۰
$N=۶$.

این N زیربازه، حجره‌ها هستند. تعدادآنها Nتاست، وبنابراین دوتا ازاعداد $k\alpha-[k\alpha]$ $(۰\leqslant k\leqslant N)$ بایستی دریك زیربازه قرار گیرند ؛ یعنی آنها نمی‌توانند به‌اندازهٔ بیشتر از $۱/N$ از همدیگر دور باشند. فرض‌کنیم این دو عدد $n\alpha-[n\alpha]$ و $m\alpha-[m\alpha]$ باشند به طوری که $۰\leqslant n<m\leqslant N$. قرار می‌دهیم $q=m-n$ و $p=[m\alpha]-[n\alpha]$. دراین صورت

$$|q\alpha-p|=|(n\alpha-[n\alpha])-(m\alpha-[m\alpha])|\leqslant\frac{۱}{N}\cdot$$

بعلاوه، $q=m-n\leqslant m\leqslant N$ و چون $m-n>۰$، پس $q\geqslant ۱$ ■

نتیجهٔ ۲ : تعداد نامتناهی از اعداد صحیح $q(\geqslant ۱)$ و p موجودند به‌طوری که

$$\left|\alpha-\frac{p}{q}\right|\leqslant\frac{۱}{q^{۲}}\cdot \qquad (۲)$$

برهان: اگر α گویا باشد، برهان تمرین ساده‌ای خواهد بود. بنابراین، فرض می‌کنیم α گنگ باشد.

هرگاه درقضیهٔ ۱، $N_۱$ را مساوی ۱ بگیریم، $p_۱$ و $q_۱(=۱)$ را به قسمی می‌یابیم که

$$\left|\alpha-\frac{p_۱}{q_۱}\right|\leqslant\frac{۱}{q_۱N_۱}=\frac{۱}{q_۱^{۲}}$$

چون α گنگ است $|q_۱\alpha-p_۱|\neq ۰$ ، وبنابراین می‌توانیم $N_۲$ را به‌قسمی‌انتخاب کنیم که

$$\frac{۱}{N_۲}<|q_۱\alpha-p_۱| \qquad (۳)$$

بنابراین،به‌استناد قضیهٔ ۱ ، اعدادصحیح $p_۲$ و$q_۲$ وجود دارند به طوری که $۱\leqslant q_۲\leqslant N_۲$ و

$$\left|\alpha-\frac{p_۲}{q_۲}\right|\leqslant\frac{۱}{q_۲N_۲}\leqslant\frac{۱}{q_۲^{۲}}\cdot$$

پس، بنابر (۳) $|q_۲\alpha-p_۲|\leqslant ۱/N_۲<|q_۱\alpha-p_۱|$ ، وبنابراین $(q_۲ ، p_۲)$ متمایز از $(q_۱ ، p_۱)$ است. مجدداً چون α گنگ است ، بنابراین $|q_۲\alpha-p_۲|\neq ۰$ ، و می‌توانیم $N_۳$ را به قسمی بیابیم که

$$\frac{1}{N_3} < |q_2\alpha - p_2| \cdot$$

به استناد قضیهٔ ۱ می‌توانیم اعداد صحیح p_3 و q_3 را به‌قسمی بیابیم که $1 \leqslant q_3 \leqslant N_3$ و

$$\left|\alpha - \frac{p_3}{q_3}\right| \leqslant \frac{1}{q_3 N_3} \leqslant \frac{1}{q_3^2}$$

همچنین، $|q_3\alpha - p_3| \leqslant 1/N_3 < |q_2\alpha - p_2| < |q_1\alpha - p_1|$ ، وبنابراین $(q_3 ، p_3)$ متمایزاز $(q_2 ، p_2)$ و $(q_1 ، p_1)$ است. اگر استدلال را به‌همین روش (استقرا) ادامه‌دهیم، تعداد نامتناهی جواب برای (۲) فراهم می‌سازیم. ■

مثال ۳ : قبلا ملاحظه کردیم که

$$\left|\pi - \frac{22}{7}\right| = 0{,}00126\ldots < \frac{1}{7^2}$$

و

$$\left|\pi - \frac{355}{113}\right| \leqslant 0{,}000000268 < \frac{1}{113^2} \cdot$$

بعلاوه، هرگاه $|22 - 7\pi|$ را به ازای هر کسر دیگر p/q به طوری‌که $1 \leqslant q \leqslant 105$ کوچکتر از $|q\pi - p|$ فرض‌کنیم از قضیهٔ ۱ با قراردادن $N = 105$ می‌بینیم که بایستی داشته باشیم

$$\left|\pi - \frac{22}{7}\right| \leqslant \frac{1}{7 \times 105} = 0{,}0013605\ldots ,$$

که نزدیك به اندازهٔ واقعی تفاضل می‌باشد.

سؤال بعدی که مطرح می‌کنیم این است که آیا می‌توانیم بهتر از (۲) عمل‌کنیم . به عنوان مثال،آیا می‌توانیم تضمین‌کنیم که تعداد نامتناهی‌عدد صحیح p و q موجودند به‌قسمی که $|\alpha - p/q| < 1/q^3$ یا تابع‌دیگری ازq کوچکتر از $1/q^2$ (درطرف‌دوم) باشد. جواب این سؤال منفی است، بدین معنی که اعدادگنگی مانند α موجودند به‌طوری‌که

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{3q^2} \qquad (۴)$$

به‌ازای کلیهٔمقادیر p و q. ولی، می‌توان‌نشان‌داد که $|\alpha - p/q| \leqslant 1/\sqrt{5}q^2$ همواره تعداد نامتناهی‌جواب‌دارد؛ این‌امر موضوع‌قضیهٔ‌معروف‌به هارویتس[1] است‌ودراینجانمی‌تواندثابت شود. درمسئلهٔ بعد مثالی برای (۴) ارائه خواهیم‌داد، که به مبحث اصلی این ضمیمه، یعنی اثبات لم ۶.۶.۲ منجر خواهد شد.

1. Hurwitz

مثال ۴ : اگر $\alpha=\sqrt{۲}$. به‌ازای هرعددصحیح مفروض $(\geqslant ۱)$ qوp،داریم $p-q\alpha\neq ۰$ و $p+q\alpha\neq ۰$. بنابراین

$$(p-q\alpha)(p+q\alpha)=p^{۲}-۲q^{۲}\neq ۰$$

(البته ، این را در بخش ۶.۶ دیده بودیم.) ملاحظه می‌کنیم که اگر n عدد صحیح ناصفری باشد، آنگاه $|n|\geqslant ۱$. بنابراین

$$۱\leqslant|p^{۲}-۲q^{۲}|=|q\alpha-p||q\alpha+p|\,.$$

اگر $|\alpha-p/q|\leqslant ۱/q^{۲}$ ، آنگاه $|q\alpha-p|\leqslant ۱/q$. بنابراین ، چون $q\geqslant ۱$ و $\alpha>۰$ خواهیم داشت $p>۰$ و $p\leqslant q\alpha+(۱/q)$. پس به ازای $q\geqslant ۳$ ، داریم

$$۱\leqslant|q\alpha-p||q\alpha+p|\leqslant|q\alpha-p|\left(q\alpha+q\alpha+\frac{۱}{q}\right)\leqslant|q\alpha-p|(۳q)\,.$$

لذا به ازای $q\geqslant ۳$ ، داریم

$$|q\alpha-p|\geqslant\frac{۱}{۳q},$$

پس

$$|\alpha-\frac{p}{q}|\geqslant\frac{۱}{۳q^{۲}}\,.$$

با استفاده از روش مثال ۴ ، لم ۲.۶.۶ را ثابت خواهیم کرد.

لم ۵: فرض کنیم $B=۲\sqrt{d}+۱$ ، که در آن d عدد صحیح‌مثبتی‌است. دراین صورت‌تعداد نامتناهی عدد صحیح مانند x و y وجود دارند به طوری که

$$|x^{۲}-dy^{۲}|\leqslant B\,.$$

برهان: به استناد نتیجهٔ ۲ تعدادی نامتناهی عدد صحیح x و y وجود دارند به طوری که $y\geqslant ۱$ و

$$|y\sqrt{d}-x|\leqslant\frac{۱}{y}$$

بنابراین $|\sqrt{d}-x/y|\leqslant ۱/y^{۲}$ و $|x/y|\leqslant\sqrt{d}+۱/y^{۲}\leqslant\sqrt{d}+۱$. بالاخره ،

$$|x^{۲}-dy^{۲}|=|y\sqrt{d}-x|\;|y\sqrt{d}+x|\leqslant\frac{|y\sqrt{d}+x|}{y}$$

$$=\left|\sqrt{d}+\frac{x}{y}\right|\leqslant\sqrt{d}+\left|\frac{x}{y}\right|\leqslant\sqrt{d}+\sqrt{d}+۱=B\,. \qquad \blacksquare$$

تمرینات

۱. فرض کنیم $a_۱$ ، $a_۲$ ، $a_۳$ ، $a_۴$ ، $a_۵$ ، $a_۶$ اعداد صحیحی که همزمان صفر نیستند باشند به طوری که به‌ازای $۱\leqslant i\leqslant ۶$ ، $|a_i|\leqslant A$. با توسل به اصل لانهٔ کبوتر نشان دهید که معادلات خطی

$$a_۱x+a_۲y+a_۳z=۰$$
$$a_۴x+a_۵y+a_۶z=۰$$

یك جواب x ، y ، z دارند به‌طوری که حداقل یکی از مقادیر x ، y ، z ناصفر است و

$$|x| , |y| , |z|\leqslant ۷۲A^۲ .$$

۲. تمرین ۱ را به یك دستگاه معادلات خطی با متغیرهای بیشتر به‌صورت زیر تعمیم دهید: فرض کنیم

$$a_{۱۱}x_۱+\cdots+a_{۱n}x_n=۰$$
$$\vdots$$
$$a_{r۱}x_۱+\cdots+a_{rn}x_n=۰$$

r معادلهٔ n مجهولی ، $n>r$، باشند و a_{ij}ها به ازای کلیهٔ مقادیر i و j اعدادی صحیح و $|a_{ij}|\leqslant A$. دراین صورت اعداد صحیح $x_۱$ ، … ، x_n موجودند به‌طوری که همزمان‌صفر نیستند و

$$|x_i|\leqslant ۲(۲nA)^{r/(n-r)} \qquad (۱\leqslant i\leqslant n)$$

۳. فرض‌می کنیم α عددگویایی باشد. نشان دهید که $|q\alpha-p|<۱/q$ ، به ازای‌عددصحیح p و q تعداد نامتناهی جواب دارد.

۴. فرض کنیم $d(>۰)$ یك عدد صحیح نامربع باشد . نشان دهید که مقدار ثابتی مانند C (وابسته به d) موجود است به‌طوری که به ازای کلیهٔ اعداد صحیح $(۱\leqslant)q$ و p ،

$$|q\sqrt{d}-p|>\frac{C}{q} .$$

۵. از اصل لانهٔ کبوتر برای اثبات نتیجهٔ زیر منسوب به دیریکله استفاده کنید . فرض کنیم $\alpha_۱$ ، … ، α_n اعداد حقیقی باشند. نشان دهید که یك عدد ثابت $C(>۰)$ وجود دارد به طوری که به ازای کلیهٔ اعداد صحیح $B(\geqslant ۱)$ اعداد صحیحی‌مانند q ، $p_۱$ ، $p_۲$ ، … ، p_n موجودند به‌قسمی که

$$|q\alpha_i-p_i|\leqslant\frac{C}{B^{۱/n}} \quad (۱\leqslant i\leqslant n , ۱\leqslant q\leqslant B)$$

۶. ازتمرین ۵ نتیجه بگیرید که نامساویهای $|q\alpha_i-p_i|<C/q^{۱/n}$ $(۱\leqslant i\leqslant n)$ به‌ازای

مقدار ثابت $C(>0)$، دارای تعداد نامتناهی جواب برحسب اعـداد صحیح $q(\geqslant 1)$ و p_1، ...، p_n است.

۷. قضیهٔ مشهوری از توئه[1] بیان می‌داردکه فقط تعداد متناهی عدد صحیح q و p موجودند به‌طوری که

$$|q\sqrt[3]{2}-p|<\frac{1}{q^{3/2}}\cdot$$

با استفاده ازاین قضیه نشان دهیدکه معادلهٔ سیالهٔ

$$x^3-2y^3=1$$

فقط تعدادی متناهی جواب دارد.

1. Thue

جدول ۱

مقادیر $\sigma(n)$ ، $d(n)$ ، $\mu(n)$ ، و $\varphi(n)$

$\varphi(n)$	$\mu(n)$	$d(n)$	$\sigma(n)$	n	$\varphi(n)$	$\mu(n)$	$d(n)$	$\sigma(n)$	n
۱۸	۰	۴	۴۰	۲۷	۱	۱	۱	۱	۱
۱۲	۰	۶	۵۶	۲۸	۱	-۱	۲	۳	۲
۲۸	-۱	۲	۳۰	۲۹	۲	-۱	۲	۴	۳
۸	-۱	۸	۷۲	۳۰	۲	۰	۳	۷	۴
۳۰	-۱	۲	۳۲	۳۱	۴	-۱	۲	۶	۵
۱۶	۰	۶	۶۳	۳۲	۲	۱	۴	۱۲	۶
۲۰	۱	۴	۴۸	۳۳	۶	-۱	۲	۸	۷
۱۶	۱	۴	۵۴	۳۴	۴	۰	۴	۱۵	۸
۲۴	۱	۴	۴۸	۳۵	۶	۰	۳	۱۳	۹
۱۲	۰	۹	۹۱	۳۶	۴	۱	۴	۱۸	۱۰
۳۶	-۱	۲	۳۸	۳۷	۱۰	-۱	۲	۱۲	۱۱
۱۸	۱	۴	۶۰	۳۸	۴	۰	۶	۲۸	۱۲
۲۴	۱	۴	۵۶	۳۹	۱۲	-۱	۲	۱۴	۱۳
۱۶	۰	۸	۹۰	۴۰	۶	۱	۴	۲۴	۱۴
۴۰	-۱	۲	۴۲	۴۱	۸	۱	۴	۲۴	۱۵
۱۲	-۱	۸	۹۶	۴۲	۸	۰	۵	۳۱	۱۶
۴۲	-۱	۲	۴۴	۴۳	۱۶	-۱	۲	۱۸	۱۷
۲۰	۰	۶	۸۴	۴۴	۶	۰	۶	۳۹	۱۸
۲۴	۰	۶	۷۸	۴۵	۱۸	-۱	۲	۲۰	۱۹
۲۲	۱	۴	۷۲	۴۶	۸	۰	۶	۴۲	۲۰
۴۶	-۱	۲	۴۸	۴۷	۱۲	۱	۴	۳۲	۲۱
۱۶	۰	۱۰	۱۲۴	۴۸	۱۰	۱	۴	۳۶	۲۲
۴۲	۰	۳	۵۷	۴۹	۲۲	-۱	۲	۲۴	۲۳
۲۰	۰	۶	۹۳	۵۰	۸	۰	۸	۶۰	۲۴
۳۲	۱	۴	۷۲	۵۱	۲۰	۰	۳	۳۱	۲۵
۲۴	۰	۶	۹۸	۵۲	۱۲	۱	۴	۴۲	۲۶

دنبالهٔ جدول ۱

مقادیر $\sigma(n)$ ، $d(n)$ ، $\mu(n)$ ، و $\varphi(n)$

n	$\sigma(n)$	$d(n)$	$\mu(n)$	$\varphi(n)$	n	$\sigma(n)$	$d(n)$	$\mu(n)$	$\varphi(n)$
۵۳	۵۴	۲	−۱	۵۲	۷۷	۹۶	۴	۱	۶۰
۵۴	۱۲۰	۸	۰	۱۸	۷۸	۱۶۸	۸	−۱	۲۴
۵۵	۷۲	۴	۱	۴۰	۷۹	۸۰	۲	−۱	۷۸
۵۶	۱۲۰	۸	۰	۲۴	۸۰	۱۸۶	۱۰	۰	۳۲
۵۷	۸۰	۴	۱	۳۶	۸۱	۱۲۱	۵	۰	۵۴
۵۸	۹۰	۴	۱	۲۸	۸۲	۱۲۶	۴	۱	۴۰
۵۹	۶۰	۲	−۱	۵۸	۸۳	۸۴	۲	−۱	۸۲
۶۰	۱۶۸	۱۲	۰	۱۶	۸۴	۲۲۴	۱۲	۰	۲۴
۶۱	۶۲	۲	−۱	۶۰	۸۵	۱۰۸	۴	۱	۶۴
۶۲	۹۶	۴	۱	۳۰	۸۶	۱۳۲	۴	۱	۴۲
۶۳	۱۰۴	۶	۰	۳۶	۸۷	۱۲۰	۴	۱	۵۶
۶۴	۱۲۷	۷	۰	۳۲	۸۸	۱۸۰	۸	۰	۴۰
۶۵	۸۴	۴	۱	۴۸	۸۹	۹۰	۲	−۱	۸۸
۶۶	۱۴۴	۸	−۱	۲۰	۹۰	۲۳۴	۱۲	۰	۲۴
۶۷	۶۸	۲	−۱	۶۶	۹۱	۱۱۲	۴	۱	۷۲
۶۸	۱۲۶	۶	۰	۳۲	۹۲	۱۶۸	۶	۰	۴۴
۶۹	۹۶	۴	۱	۴۴	۹۳	۱۲۸	۴	۱	۶۰
۷۰	۱۴۴	۸	−۱	۲۴	۹۴	۱۴۴	۴	۱	۴۶
۷۱	۷۲	۲	−۱	۷۰	۹۵	۱۲۰	۴	۱	۷۲
۷۲	۱۹۵	۱۲	۰	۲۴	۹۶	۲۵۲	۱۲	۰	۳۲
۷۳	۷۴	۲	−۱	۷۲	۹۷	۹۸	۲	−۱	۹۶
۷۴	۱۱۴	۴	۱	۳۶	۹۸	۱۷۱	۶	۰	۴۲
۷۵	۱۲۴	۶	۰	۴۰	۹۹	۱۵۶	۶	۰	۶۰
۷۶	۱۴۰	۶	۰	۳۶	۱۰۰	۲۱۷	۹	۰	۴۰

واژه‌نامهٔ فارسی به انگلیسی

آزمون مقایسه	comparison test
آزمون و خطا	trial and error
اساسی	basic
استقرا	induction
اصل	principle
ـ حجره	box ـ
ـ لانهٔ کبوتر	pigeon hole ـ
افسونهای خوشبختی	good luck charms
اقلیدس	Euclid
الگو	pattern
الگوریتم	algorithm
اندیس	index
اولیه	primitive
ایده‌آل	ideal
بازه	interval
باقیمانده	remainder
بخشپذیر	divisible
بخشپذیری	divisibility
برهان	proof
بزرگترین	greatest
ـ مقسوم‌علیه مشترک (بمعم)	—common divisor—
بسجمله (بسجمله‌ای در صفت)	polynomial
بنیادی	fundamental
پدیده	phenomenon
تابع	function
ـ فی	phi ـ
تام	perfect
تجسس	inspection
تحلیلی	analytic
تحویل‌ناپذیر (درکسرها)	reduced
تفریق	subtraction
تقابل	reciprocity
ـ مربعی	quadratic—
ـ مکعبی	cubic—
تقریب	approximation
تقسیم	division
تقویم	calendar
جبری	algebraic

جذر square root
جزء کسری fractional part
جمع addition
جواب اولیه primitive solution
جواب کمترین least solution
جوابهای متمایز distinct solutions

چگال dense
چهارتایی quaternion
چهار ـ مربع four-square

حاصلضرب نامتناهی infinite product
حدس conjecture
حذف cancellation
حساب (حسابی) arithmetic
حساب دیفرانسیل و انتگرال calculus
حلقه ring

خارج قسمت quotient
خاص special
خالی از مربع square-free
خطی linear
خوشترتیبی well-ordering

درایه entry
درجه degree
درجهٔ دوم quadratic
درجهٔ سوم cubic
دستگاه system
دستور formula
دنباله sequence
دو ـ مربع two-square

رابطهٔ هم‌ارزی equivalence relation
روش method
ریاضی mathematical
ریشهٔ اولیه primitive root

زوج even
زوجیت parity
زیر بازه sub-interval
زیر گروه subgroup

سری series
سه تایی triple

شمارگر counter

صوری formal
صوفیان mystics

ضرب multiplication
ضربی multiplicative
ـ قوی totally—

طلسم talisman

عاد می‌کند divides
عامل factor
عدد number
ـ حقیقی real—
ـ گویا (منطق) rational—
ـ مختلط complex—
عدد اول prime
عدد شناسی numerology
عدد صحیح integer
عضو element
عکس inverse

عکس inversion

غربال sieve
ـ اراتستن —of Eratosthenes

فرد odd
فرمولبندی مجدد reformulation
فیثاغورسی pythagorean

قانون law
قدر مطلق absolute value
قضیهٔ باقیماندهٔ چینی
chinese remainder theorem
قوه power

کامل complete
کسر fraction
ـ تحویل ناپذیر reduced—
ـ مسلسل continued—
کسری fractional
کوچکترین least
ـ مضرب‌مشترك —common multiple

گردایه collection
گروه group
ـ خارج قسمتی quotient—
گنگ irrational
گویا rational

مانده (درسری‌ها) tail end
مانده residue
مبنا base
متحابه amicable
متمایز distinct

مثلثی triangular
محك criterion
مخفف reduced
(در دستگاه مانده‌ها)
مخمسی pentagonal
مربعی square
مرتبه order
مسبعی septagonal
مسدسی hexagonal
مشتق derivative
مصور figurate
مضرب multiple
معادله equation
ـ سیاله Diophantine—
مقسوم‌علیه divisor
موبیوس Möbius
میدان field

نامانده nonresidue
نزول descent
ـ نامتناهی infinite—
نسبت به هم اول (متباین)
relatively prime
نظریهٔ اعداد number theory
نظریهٔ تحلیلی اعداد analytic—
نظریهٔ جبری اعداد algebraic—
نظریهٔ مقدماتی اعداد elementary—
نظریهٔ تجزیه factorization theory
نما exponent
نماد symbol
ـ لژاندر Legendre—
نمایش representation
نه نه کنار گذاشتن
casting out nines

وارون	reciprocal
واقعی	proper
همزمان	simultaneous
همگرا	convergent
همورد	convolution
همنهشت	congruent
هندسی	geometric
هنگ	modulo
یکتایی تجزیه (به عوامل اول)	unique factorization

واژه‌نامهٔ انگلیسی به‌فارسی

absolute value قدر مطلق
addition جمع
algebraic جبری
—number theory نظریهٔ ـ اعداد
algorithm الگوریتم
amicable متحابه
analytic تحلیلی
—number theory نظریهٔ ـ اعداد
approximation تقریب
arithmetic حساب ، حسابی

base مبنا
basic اساسی
box principle اصل حجره

calculus حساب دیفرانسیل وانتگرال
calendar تقویم
cancellation حذف
casting out nines نه نه‌کنار گذاشتن
chinese remainder theorem قضیهٔ باقیماندهٔ چینی
collection گردایه
comparison test آزمون مقایسه
complete کامل
complex number عددمختلط
congruent همنهشت
conjecture حدس
continued fractions کسرهای مسلسل
convergent همگرا
convolution همنورد
counter شمارگر
criterion محک
cubic درجهٔ سوم
—reciprocity تقابل مکعبی

degree درجه
dense چگال
derivative مشتق
descent نزول
Diophantine equation معادلهٔ سیاله
distinct متمایز
—solutions جوابهای ـ
divisibility بخشپذیری
divisible بخشپذیر

divides	عاد می کند
division	تقسیم
divisor	مقسوم‌علیه
element	عضو
elementary	مقدماتی
–number theory	نظریهٔ–اعداد
entry	درایه
equation	معادله
equivalence relation	رابطهٔ هم‌ارزی
Euclid	اقلیدس
even	زوج
exponent	نما
factor	عامل
factorization theory	نظریهٔ تجزیه
field	میدان
figurate	مصور
formal	صوری
formula	دستور
four-square	چهار-مربع
fractional	کسری
–part	جزء–
function	تابع
fundamental	بنیادی
–solution	جواب–
geometric	هندسی
good luck charms	افسونهای خوشبختی
greatest	بزرگترین
–common divisor	– مقسوم‌علیه مشترک (بمعم)
group	گروه
hexagonal	مسدسی
ideal	ایده‌آل
index	اندیس
induction	استقرا
infinite	نامتناهی
–descent	نزول–
–product	حاصلضرب
inspection	تجسس
integer	عدد صحیح
interval	بازه
inverse	عکس
inversion	عکس
irrational	گنگ
law	قانون
least	کوچکترین
–common multiple	–مضرب مشترک
least solution	جواب کمترین
Legendre symbol	نماد لژاندر
linear	خطی
mathematical	ریاضی
method	روش
Möbius	موبیوس
modulo	هنگ
multiple	مضرب
multiplication	ضرب
multiplicative	ضربی
mystics	صوفیان
nonresidue	نامانده
number	عدد
– theory	نظریهٔ اعداد

numerology	عدد شناسی
odd	فرد
order	مرتبه
parity	زوجیت
pattern	الگو
pentagonal	مخمسی
perfect	تام
phenomenon	پدیده
phi function	تابع فی
pigeon hole principle	اصل لانهٔ کبوتر
polynomial(بسجمله‌ای‌درصفت)	بسجمله
power	قوه
prime	عدد اول
primitive	اولیه
_root	ریشهٔ_
_solution	جواب_
principle	اصل
proof	برهان
proper	واقعی
pythagorean	فیثاغورسی
quadratic	درجهٔ دوم
_reciprocity	تقابل مربعی
quaternion	چهارتایی
quotient	خارج قسمت
_ group	گروه خارج قسمتی
rational number	عدد گویا (منطق)
real number	عدد حقیقی
reciprocal	وارون
reduced	تحویل‌ناپذیر (درکسرها)
_fractions	کسور_
reduced	مخفف (دردستگاه مانده‌ها)
reformulation	فرمولبندی مجدد
relatively prime	نسبت به هم اول (متباین)
remainder	باقیمانده
representation	نمایش
residue	مانده
ring	حلقه
root	ریشه
septagonal	مسبعی
sequence	دنباله
series	سری
sieve	غربال
_of Eratosthenes	_ اراتستن
simultaneous	همزمان
special	خاص
square	مربعی
square–free	خالی از مربع
square root	جذر
subgroup	زیرگروه
sub–interval	زیربازه
subtraction	تفریق
symbol	نماد
system	دستگاه
tail end	مانده (در سری‌ها)
talisman	طلسم
totally multiplicative	ضربی قوی
trial and error	آزمون و خطا
triangular	مثلثی
triple	سه تایی
two_square	دو_مربع
unique factorization	یکتایی تجزیه (به عوامل اول)
well–ordering	خوشترتیبی

فهرست الفبایی مندرجات