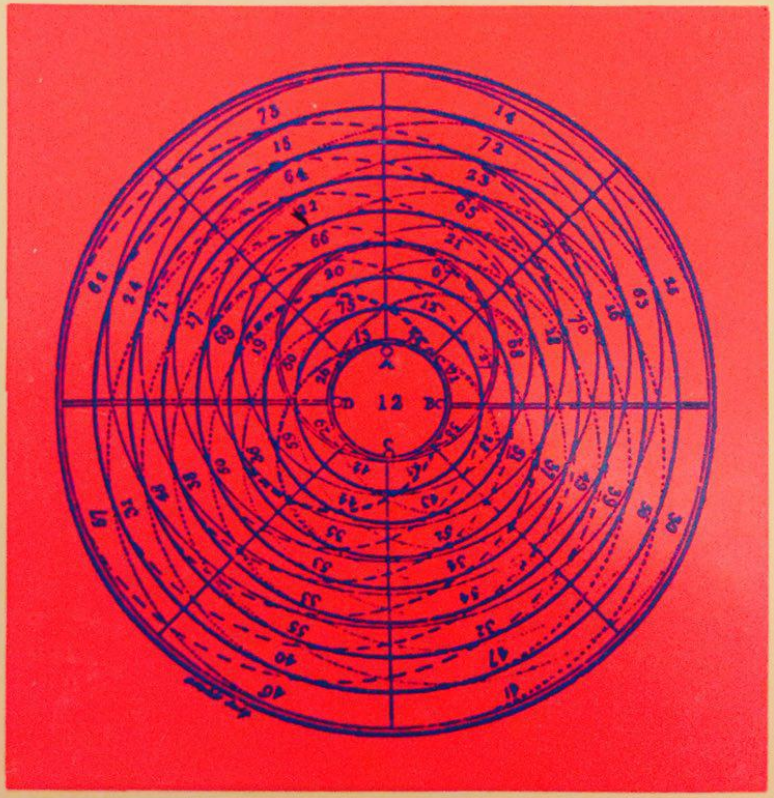
گزیده‌هایی از نظریهٔ اعداد

اویستن اور
ترجمهٔ منوچهر وصال



(ریاضیات پیش‌دانشگاهی ـ ۲۰)

گزیده‌هایی از نظریهٔ اعداد

(ریاضیات پیش‌دانشگاهی ـ ۲۰)

اویستن اور

ترجمهٔ منوچهر وصال

مرکز نشر دانشگاهی، تهران

فهرست

بسم الله الرحمن الرحیم

سخنی با خواننده

ارتباط بین استادان برجستهٔ دانشگاهها و دانش‌آموزان دوره‌های پیش‌دانشگاهی، از مؤثرترین وسیله‌هایی‌است که به‌کشف و پرورش استعدادها کمك می کند و زمینه را برای‌تربیت دانشمندان‌آینده فراهم‌می‌سازد. در بین‌شخصیتهای علمی تراز اول، که پژوهندگان یك علم را در بالاترین سطح ممکن آمـوزش می‌دهند و راهنمایی می‌کنند، عدهٔ‌کمی این‌توانایی را دارندکه درآن زمینهٔ‌علمی، و با رعایت همهٔ دقتها ونکته‌ها، کتابهایی تألیف‌کنند که برای قشر وسیعی از دانش‌آموزان دبیرستانی، وگاه برای افراد عادی، آموزنده وقابل درك باشد. این شخصیتها، که درهرکشور انگشت شمارند، از این راه، ارتباطی بین‌خود وجوانان برقرارمی‌سازند. دسترسی دانش‌آموزان به‌چنین‌کتابهایی، پشتوانه‌ای برای تأمین آیندهٔ علمی جامعه است.

جـامعهٔ ریاضـی آمریـکا مجموعه‌ای از ایـن‌گونه کتابها را زیـر عنوان New Mathematical Library فراهم‌آورده و تاکنون بیش از سی جلد ازآنها را منتشرکرده است‌که بعضی از آنها مستقیماً به زبان انگلیسی تألیف شده و بعضی دیگر از زبانهای مختلف به‌انگلیسی ترجمه شده‌اند. این‌کتابها تاکنون به بسیاری از زبانهای دیگر ترجمه‌شده‌وهرکدام، چه درآمریکا وچه درکشورهای‌دیگر، بارها تجدیدچاپ شده است.

گروه ریاضی، آمار، و کامپیوتر مرکز نشر دانشگاهی، به حکم وظیفه‌ای که برای‌گسترش دانش‌ریاضی به‌عهده دارد، به‌ترجمهٔ این‌کتابها از انگلیسی به‌فارسی، و ویرایش‌آنها پرداخته‌است. مترجمان و ویراستاران ازافرادخبره برگزیده شده‌اند وکوشش لازم به‌عمل‌آمده است تا، ضمن رعایت امانت‌کامل‌درترجمه، متن فارسی روان و خالی از ابهام باشد. کتابها به‌ترتیبی‌که ترجمهٔ آنها آماده شود زیر عنوان **ریاضیات پیش‌دانشگاهی** منتشر می‌شوند.

این مجموعه کتابها را می‌توان دو دسته کرد. یك دسته شامل کتابهایی است که مباحثی از ریاضیات را به زبان ساده تشریح می‌کنند و می‌توانند بـرای درسهای ریاضیات عمومی دانشگاه نیز جنبهٔ کمك درسی داشته باشند. ویراستاران متن اصلی این کتابها در پیشگفتار خود از جمله نوشته‌اند:

مطالب کتابهای این مجموعه در برنامهٔ ریاضیات دبیرستانی یا گنجانیده نشده یا به‌اجمال بیان شده است. میزان دشواری آنها متفاوت است و حتی دریك کتاب هم، مطالعهٔ بعضی از بخشها به‌تمرکز حواس بیشتری نیاز دارد. خواننده برای فهم مطالب اغلب این کتابها، هرچند به‌اطلاعات ریاضی چندانی نیاز ندارد، ولی باید تلاش فکری فراوانی به‌عمل آورد. کتاب ریاضی را نمی‌توان به‌سرعت خواند، و نباید توقع داشت که با یك بار مطالعه، تمام بخشهای آن فهمیده شود. می‌توان بدون معطل‌ماندن روی بخشهای پیچیده از آنها گذشت و بعد، برای مطالعهٔ عمیق به آنها بازگشت، زیرا بسیار پیش می‌آید که مطلبی در مبحث بعدی روشن می‌شود. از سوی دیگر، می‌توان بخشهایی را که مطالب آنها کاملا آشناست خیلی سریع مطالعه کرد. بهترین راه فراگرفتن ریاضیات، حل مسأله‌های آن است. هر کتاب شامل مسأله‌هایی است که حل برخـی از آنها ممکن است مستلزم تأمل قابل‌ملاحظـه‌ای باشد. پاسخها یا راهنماییهای مربوط به حل این مسأله‌ها، غالباً در پایان کتاب آمده‌انـد. به خواننده توصیه می‌شود که کوشش کند هرمسأله را خود حل کند وفقط برای اطمینان از درستی راه‌حل خود به بخش پاسخها مراجعه نماید. بدین‌طریق، مطلب رفته‌رفته برایش پرمعناتر خواهد شد.

دستهٔ دیگر کتابها، شامل مجموعه‌هایی غنی از مسأله‌ها یـا پرسشهای جالب چندگزینه‌ای است که در مسابقه‌های معروف ریاضی مطرح شده‌اند. دراین کتابها، راه‌حل دقیق مسأله‌ها آمده است. درمورد پرسشها به‌ذکر پاسخ درست اکتفا نشده، بلکه حل کامل آنها نیز عرضه شده‌است.

نظرات و پیشنهادهای خوانندگان ما را به‌ادامهٔ کار و گسترش این گونه‌فعالیتها تشویق خواهد کرد.

گروه ریاضی، آمار، وکامپیوتر
مرکز نشر دانشگاهی

فصل ۱

مقدمه

۱.۱ تاریخچه

نظریهٔ اعداد شاخه‌ای از ریاضیات است که دربارهٔ اعداد طبیعی

$$۱, ۲, ۳, \cdots,$$

بحث می‌کند. اعداد طبیعی را اغلب اعداد صحیح مثبت می‌نامند.

باستانشناسی و تاریخ به‌ما می‌آموزند که انسان خیلی زود شمردن را آغاز کرد. آموخت که اعداد را با هم جمع کند و بعدها توانست آنها را درهم ضرب یا از یکدیگر تفریق کند. برای اینکه مقداری سیب یا ماهی را به سهمهای مساوی به‌افرادبدهد به‌عمل‌تقسیم‌اعداد نیازداشت. این‌اعمال روی‌اعداد را در زبان‌انگلیسی «calculation» می‌نامند و از لغت لاتین *calculus* که به‌معنی سنگریزه است، مشتق می‌شود؛ رومیها برای نشان‌دادن اعداد روی تخته‌های محاسبهٔ خود ازسنگریزه استفاده می‌کردند.

پس‌ازاینکه بشرکمی با حساب‌کردن آشنا شد، برای بسیاری از اندیشمندان حساب‌کردن به‌صورت‌سرگرمی درآمد. تجربیات بشر با اعداد درطول‌قرنها به‌طور تصاعدی انباشته شده‌اند و درنتیجه امروز در ریاضیات جدید ساختاری باشکوه به‌نام نظریهٔ اعداد به‌وجود آورده‌اند. بعضی‌از قسمتهای آن هنوز هم بازی ساده با

اعداد است، اما قسمتهای دیگری بخشی از مشکلترین و پیچیده‌ترین فصلهای ریاضیات را تشکیل می‌دهند.

۲.۱ عددشناسی

به‌یقین، در بین خرافات مربوط به‌اعداد به‌بعضی از قدیمترین آثار تحقیقات دربارهٔ اعداد بر می‌خوریم. این خرافات در فرهنگ تمام ملتها دیده می‌شوند. اعدادی خوش‌یمن هستند و باید آنها را بردیگر اعداد ترجیح داد و گرامی داشت، اعدادی هم بدیمن هستند و باید از آنها اجتناب کرد همانطور که از چشم بد می‌پرهیزیم. دربارهٔ عددشناسی یونانیان قدیم، یعنی راجع به‌افکار و خرافات آنها در خصوص معنای اعداد مختلف، اطلاعات زیادی داریم. مثلاً عدد فرد بزرگتر از یك، مذکر را نمایش می‌دهد و عدد زوج مونث را؛ بنابراین عدد ۵ که مجموع اولین عدد مذکر و مونث است، ازدواج یا اتحاد را نشان می‌دهد.

اگر مثالهایی از عددشناسی پیشرفته‌تر می‌خواهید، می‌توانید رسالهٔ سیاست[۱] افلاطون را از کتابخانه به‌امانت بگیرید و کتاب هشتم آن را بخوانید. با اینکه این‌نوع عددشناسی چندان معرف افکار ریاضی نیست، متضمن محاسبات با اعداد و خواص آنهاست. به‌زودی خواهیم دید که بعضی از مسائل جالب در نظریهٔ اعداد که تا به‌حال افکار ریاضیدانان را به خود مشغول کرده‌اند، از عددشناسی یونانیان سرچشمه گرفته‌اند.

خرافات عددی گذشتگان نباید موجب شود که ما امروز خودرا برترحس کنیم. همه می‌دانیم که صاحبخانه‌ها به‌هیچ‌قیمتی حاضر نمی‌شوند ۱۳ میهمان داشته باشند، و جالب است که کمتر می‌بینیم هتلی اطاق شمارهٔ ۱۳ یا طبقهٔ سیزدهم داشته‌باشد. ما واقعاً نمی‌دانیم چطور این عدد نحس شده است. تفسیرهای به ظاهر درست زیادی وجود دارند ولی بیشتر آنها پایه‌ای ندارند؛ مثلاً می‌گویند در آخرین شام حضرت عیسی سیزده میهمان بوده‌اند، سیزدهمین البته یهودا بود. به‌نظر می‌رسد این تفسیر که بیشتر چیزها را با دوجین می‌شمرند و ۱۳ یك قلم زاید دارد که باقی می‌ماند، به‌حقیقت نزدیکتر باشد.

در کتاب «مقدس» به‌خصوص در «عهد قدیم»، عدد ۷ نقش به‌خصوصی دارد. در فولکلور آلمانیهای قدیم اعداد ۳ و ۹ زیاد تکرار می‌شوند؛ و هندوها در

---

۱. Plato's Republic نزد ما به‌رسالهٔ سیاست معروف است و درسال ۱۳۳۵ هجری شمسی به‌نام «جمهور» به‌فارسی ترجمه شده است.ـم.

اساطیرشان خیلی طرفدار عدد ۱۰ بوده‌اند.

۳.۱ مسألهٔ فیثاغورسی

به‌عنوان مثالی از نظریهٔ قدیم اعداد به مسألهٔ فیثاغورسی اشاره می‌کنیم. می‌دانیم که در مثلث قائم‌الزاویه طول ضلعها در رابطهٔ فیثاغورسی

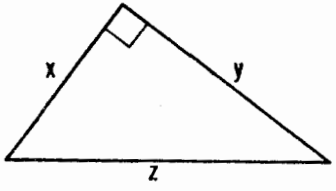
$$z^۲ = x^۲ + y^۲ \qquad (۱.۳.۱)$$

که در آن z طول وتر مثلث است، صدق می‌کنند. وقتی در مثلث قائم‌الزاویه طولهای دو ضلع معلوم‌اند، با این رابطه می‌توان طول ضلع سوم را حساب کرد. ضمناً نامیدن این قضیه به‌نام فیثاغورس، فیلسوف یونانی، تاحدودی نامناسب است، زیرا بابلیها دوهزار سال قبل از زمان فیثاغورس از این قضیه آگاهی داشتند.

گاهی طول تمام ضلعهای مثلث، x، y، z، در (۱.۳.۱) اعداد صحیح هستند. ساده‌ترین حالت

$$x = ۳, \quad y = ۴, \quad z = ۵, \qquad (۲.۳.۱)$$

را روی لوحه‌های بابلیها یافته‌اند. یك تعبیر این حالت این است که فرض کنیم حلقه‌ای نخی داریم که با دوازده علامت یا گره به‌دوازده قسمت مساوی تقسیم شده است؛ به‌وسیلهٔ سه میخ این حلقه‌را به‌صورت مثلثی درمی‌آوریم که طول دو ضلع آن ۳ و ۴ باشد، طول ضلع سوم ۵ و زاویهٔ مقابلش قائمه می‌شود (شکل ۱.۳.۱). در اغلب کتابهای تاریخ ریاضیات نوشته‌اند که بعد از طغیان رود نیل نقشه‌بردارهای مصری در موقع تعیین زمینهای زراعتی از این روش برای ساختن زاویهٔ قائمه استفاده می‌کرده‌اند. این ممکن است یکی از افسانه‌های فراوان تاریخ علم باشد؛ تا به‌حال هیچ مدرکی که آن را تأیید کند نداریم.



شکل ۱.۳.۱

معادلهٔ فیثاغورسی (۱.۳.۱) جوابهای صحیح بسیار دیگری دارد، مانند

$$x=۵, \quad y=۱۲, \quad z=۱۳,$$

$$x=۷, \quad y=۲۴, \quad z=۲۵,$$

$$x=۸, \quad y=۱۵, \quad z=۱۷.$$

بعداً نشان خواهیم داد چطور تمام جوابهای صحیح را می‌توان به‌دست آورد. یونانیها می‌دانستند آنهارا چگونه تعیین کنند، احتمالاً بابلیها هم می‌دانستند.

برای دوعدد صحیح مفروض x و y همواره z را می‌توان به‌قسمی تعیین کرد که درمعادلهٔ (۱.۳.۱) صدق کند، اما ممکن‌است z عددی گنگ باشد. وقتی بخواهید هرسه‌عدد صحیح باشند، امکانات خیلی محدودمی‌شوند، دیوفانت[1]، ریاضیدان یونانی اسکندرانی (درحدود ۲۰۰ سال بعدازمیلاد، تاریخ دقیق آن مشخص نیست) کتابی نوشت به‌نام علم حساب[2] که در آن این‌نوع مسائل مطرح است. از زمان دیوفانت، موضوع پیداکردن جوابهای صحیح یا کسری معادلات را مسألهٔ دیوفانتی می‌گویند، و آنالیز دیوفانتی قسمتی مهم ازنظریهٔ اعداد امروزی است.

مجموعهٔ مسائل ۳.۱

۱. کوشش کنید جوابهای صحیح دیگری برای معادلهٔ فیثاغورسی بیابید.

۲. کوشش کنید جوابهای دیگری بیابید که در آن وتر از بزرگترین دو ضلع، یك واحد بزرگتر باشد.

۴.۱ عددهای شکلی

در نظریهٔ اعداد اغلب به‌عددهای مربعی مانند

$$۳^۲=۹, \quad ۷^۲=۴۹, \quad ۱۰^۲=۱۰۰$$

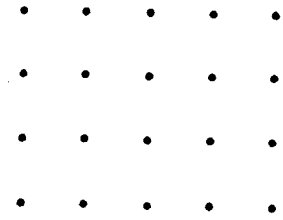
و همچنین به‌عددهای مکعبی[3] نظیر

$$۲^۳=۸, \quad ۳^۳=۲۷, \quad ۵^۳=۱۲۵,$$

---

1. Diophantos 2. Arithmetica

۳. معمولا به‌جای عدد مربعی یا مکعبی، می‌گویند مربع کامل یا مکعب کامل.ـم.



شکل ۱.۴.۱

برمی‌خوریم. این طرز بیان هندسی یکی از میراثهای فراوان ما از اندیشهٔ ریاضی یونانیان است. یونانیها ترجیح می‌دادند که اعداد، از جمله اعداد صحیح را به‌صورت کمیتهای هندسی در نظر بگیرند. در نتیجه به‌حاصلضرب $c = a.b$ به‌صورت مساحت مستطیلی به ضلعهای a و b نگاه می‌کردند. همچنین می‌توانستند $a.b$ را به صورت آرایش مستطیلی با a نقطه در یک طرف و b نقطه در طرف دیگر تصور کنند. مثلا $۴.۵ = ۲۰$، تعداد نقاط در آرایش مستطیلی شکل ۱.۴.۱ است.

هر عدد صحیحی را که حاصلضرب دو عدد صحیح باشد، می‌توانستند عدد مستطیلی بنامند. وقتی دو ضلع مستطیل مساوی هستند، عدد مربعی است. بعضی اعداد را نمی‌توان به‌صورت اعداد مستطیلی نشان داد، مگر اینکه نقاط را پشت سر هم روی یک سطر قرار دهند؛ مثلا ۵ تنها به‌صورت عدد مستطیلی که یک ضلع آن ۱ و ضلع دیگرش ۵ است درمی‌آید (شکل ۲.۴.۱). این نوع اعداد را یونانیها اعداد اول می‌نامیدند. نقطهٔ تک را معمولا عدد به‌حساب نمی‌آوردند. واحد ۱ آجری بود که از آن تمام اعداد ساخته می‌شدند. بنابراین ۱ عدد اول نبود، و اکنون هم نیست.

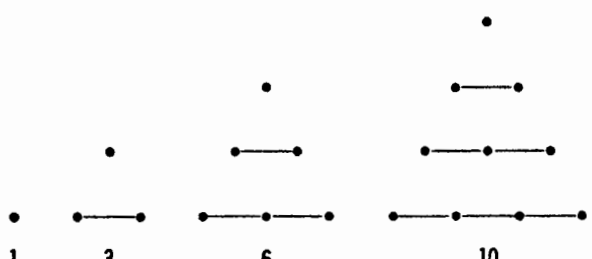
به‌جای مستطیلها و مربعها می‌توانستند نقاط را بـا نظم روی شکلهای هندسی دیگر در نظر بگیرند. در شکل ۳.۴.۱ عددهای مثلثی متوالی را نشان داده‌ایم.

در حالت کلی، n امین عدد مثلثی با فرمول

$$T_n = \frac{۱}{۲}n(n+۱), \quad n = ۱, ۲, ۳, \ldots \qquad (۱.۴.۱)$$

به‌دست می‌آید. این اعداد ویژگیهای زیادی دارند؛ مثلاً، مجموع دو عدد مثلثی

شکل ۲.۴.۱



شکل ۳.۴.۱

متوالی عددی مربعی است.

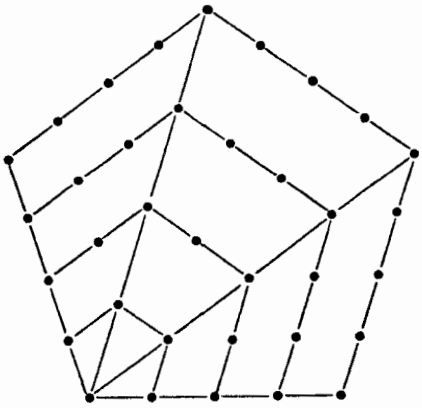
$$۱+۳=۴,\quad ۳+۶=۹,\quad ۶+۱۰=۱۶,\ \cdots \qquad (۲.۴.۱)$$

عددهای مثلثی و مربعی را به‌عددهای چندضلعی با اضلاعی بیشتر تعمیم داده بودند. درشکل ۴.۴.۱ مطلب را با عددهای پنجضلعی توضیح داده‌ایم.

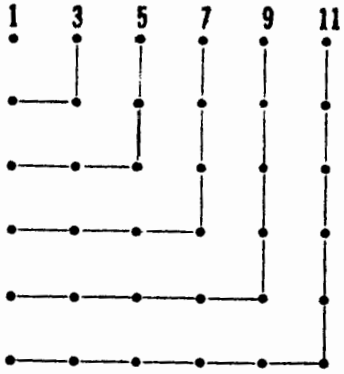
از روی شکل ۴.۴.۱ می‌بینیم که نخستین عددهای پنجضلعی

$$۱,\ ۵,\ ۱۲,\ ۲۲,\ ۳۵, \qquad (۳.۴.۱)$$

هستند. می‌توان نشان داد که p_n، n امین عدد پنجضلعی، برابر است با



شکل ۴.۴.۱



شکل ۵.۴.۱

$$p_n=\frac{1}{2}(3n^2-n). \qquad (۴.۴.۱)$$

عددهای ششضلعی، و به‌طور کلی k- ضلعی که با یك k- ضلعی منتظم تعریف می‌شوند به‌همین‌ترتیب به‌دست‌می‌آیند. بیش‌ازاین دربارهٔ این اعداد بحث‌نمی‌کنیم. عددهای شکلی، به‌ویژه عددهای مثلثی بعدازاینکه نظریهٔ اعداد یونانیها در اواخر رنسانس به‌اروپای غربی راه‌یافت، درمطالعات مربوط به‌اعداد طرف‌توجه‌قرار گرفتند؛ هنوز هم گاهی درمقاله‌های مربوط به‌نظریهٔ اعداد به‌چشم می‌خورند.

از این تحلیلهای هندسی چندین رابطهٔ عددی ساده نتیجه می‌شوند. ما فقط به یکی‌از آنها اشاره می‌کنیم. از قدیم کشف کرده بودندکه مجموع اعداد فرد تا عدد فرد معینی، مربع کامل است؛ مثلا

$$1+3=4,\quad 1+3+5=9,\quad 1+3+5+7=16,\ \cdots$$

برای‌اثبات این رابطه‌ها کافی‌است به‌نمودار مربعهای تودرتوی شکل ۵.۴.۱ نگاهی بیندازیم.

مجموعهٔ مسائل ۴.۱

۱. فرمول کلی (۱.۴.۱) در اعداد مثلثی را با استقرا ثابت کنید.

۲. فرمول (۴.۴.۱) در اعداد پنجضلعی را ثابت کنید.

۳. نشان دهید که $\frac{۱}{۲}k(n^۲-n)-n^۲+۲n$ عبارت کلی عدد k-ضلعی است.

۵۰۱ مربعهای سحرآمیز

اگر شافل بورد[1] بازی کرده باشید ممکن است به‌خاطر بیاورید که روی نه مربع، اعداد از ۱ تا ۹ به‌صورتی که در شکل ۱۰۵۰۱ دیده می‌شود، نوشته شده‌اند:

2	9	4
7	5	3
6	1	8

شکل ۱۰۵۰۱

در این جدول مجموع هرسطر، هرستون، و هرقطر، ۱۵ است.

درحالت کلی، مربع سحرآمیز مربعی است که به $n^۲$ مربع تقسیم شده است و در آن اعداد از ۱ تا $n^۲$ به‌ترتیبی نوشته‌شده‌اند که مجموع هرسطر، هرستون، وهرقطر

1	8	15	10
12	13	6	3
14	11	4	5
7	2	9	16

شکل ۲۰۵۰۱

1. Shuffle board

برابر با s، مجموع سحرآمیز، است. در شکل ۲.۵.۱ یک مربع سحرآمیز $۴^۲ = ۱۶$ عددی دیده می‌شود. دراینجا مجموع سحرآمیز ۳۴ است.

برای هر n، تنها یك مجموع سحرآمیز وجود دارد، و به‌آسانی می‌توان آن راحساب کرد. مجموع اعداد هرستون s است، پس مجموع اعداد n ستون مربع، ns است. اما باتوجه به‌عبارت مجموع یك تصاعد هندسی، مجموع تمام اعداد از ۱ تا $n^۲$ برابر است با

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

بنابراین

$$ns=\frac{۱}{۲}(n^۲+۱)n^۲,$$

یا

$$s=\frac{۱}{۲}n(n^۲+۱); \qquad (۱.۵.۱)$$

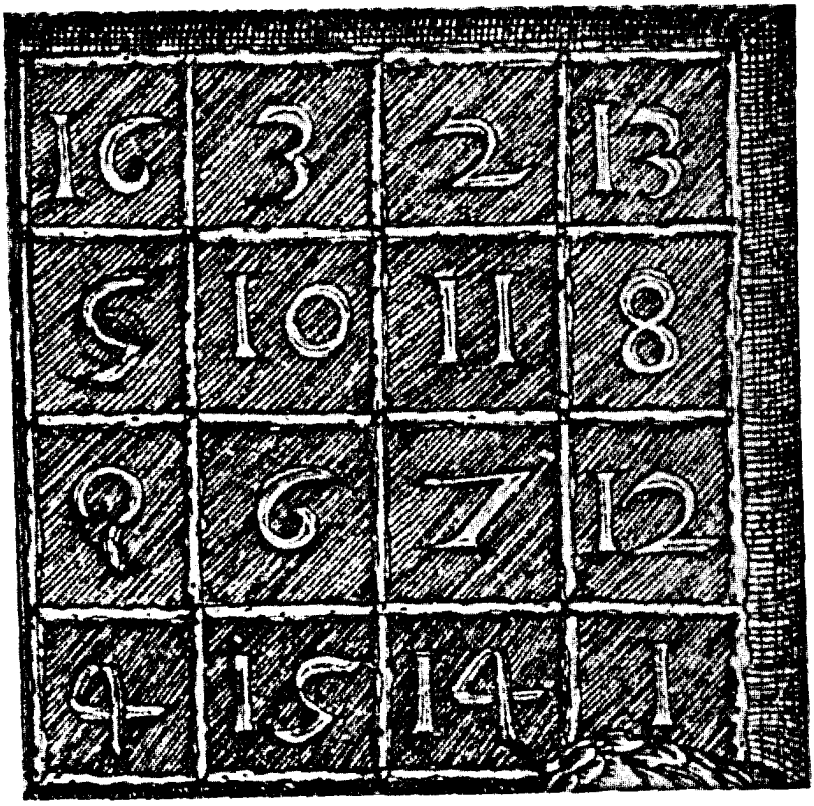
پس اگر n داده شده باشد، s مشخص است. مربعهای سحرآمیز را برای هر n بزرگتر از ۲ می‌توان ساخت؛ تحقیق اینکه برای $n=۲$ مربع سحرآمیز وجود ندارد برای خواننده آسان است.

در قرون وسطی ویژگیهای عجیب این مربعها، سحرآمیز به‌نظر می‌رسید به‌قسمی که آنهارا به‌عنوان طلسم برای محافظت درمقابل ارواح پلید، باخود داشتند. مربع سحرآمیزی که زیاد تکثیر شده است، مربع سحرآمیز در چاپ مشهور ملانکولیای[1] البرشت دورر[2] است. در شکل ۳.۵.۱ این مربع سحرآمیز دیده می‌شود. درضمن می‌بینیم که در زمان دورر رقمهارا چگونه می‌نوشته‌اند. اعداد وسط سطر آخر، ۱۵۱۴ است که می‌دانیم سال چاپ کتاب است. احتمال دارد که دورر بااین‌دوعدد شروع کرده باشد و اعداد دیگر را باآزمون وخطا به‌دست آورده باشد.

نشان می‌دهیم که برای $n=۳$ تنها یك‌مربع سحرآمیز وجود دارد: مربع‌شکل ۱.۵.۱. برای این منظور جدول را به‌صورت کلی

$$\begin{matrix} x_۱ & y_۱ & z_۱ \\ x_۲ & y_۲ & z_۲ \\ x_۳ & y_۳ & z_۳ \end{matrix}$$

1. Melancholia 2. Albrecht Dürer



شکل ۳.۵.۱

می‌نویسیم و بررسی می‌کنیم چه اعدادی به‌جای این حروف می‌توان گذاشت.

نخست نشان می‌دهیم که عدد مرکزی y_2 باید ۵ باشد. از (۱.۵.۱) به‌ازای $n=3$ دیده می‌شود که $s=15$. اینک اعداد سطر دوم، ستون دوم و دوقطر را باهم جمع می‌کنیم. y_2 دراین سطر و ستون و هردو قطر هست، پس y_2 چهاربار در این مجموع می‌آید، اما جمله‌های دیگر تنها یک‌بار ظاهر می‌شوند. بنابراین چون مجموع سطر، ستون یا قطر s است، داریم

$$4s=4\times 15=60$$

$$=x_2+y_2+z_2+y_1+y_2+y_3+x_1+y_2+z_3+z_1+y_2+x_3$$

$$=۳y_۲+x_۱+x_۲+x_۳+y_۱+y_۲+y_۳+z_۱+z_۲+z_۳$$
$$=۳y_۲+۱+۲+\cdots+۹$$
$$=۳y_۲+۴۵;$$

پس

$$۳y_۲=۶۰-۴۵=۱۵,\quad y_۲=۵۰$$

در مربع

$$\begin{array}{ccc} x_۱ & y_۱ & z_۱ \\ x_۲ & ۵ & z_۲ \\ x_۳ & y_۳ & z_۳ \end{array}$$

۹ در گوشه نیست، زیرا، اگر مثلا $x_۱=۹$، آن‌گاه $z_۳=۱$ (زیرا $s=۱۵$) ومربع به‌صورت زیر درمی‌آید

$$\begin{array}{ccc} ۹ & y_۱ & z_۱ \\ x_۲ & ۵ & z_۲ \\ x_۳ & y_۳ & ۱ \end{array}$$

هرچهار عدد $y_۱$، $z_۱$، $x_۲$، $x_۳$ باید از ۶ کوچکتر باشند، زیرا

$$y_۱+z_۱=x_۲+x_۳=۶۰$$

اما بیش از سه عدد کوچکتر از ۶، یعنی ۲، ۳ و ۴، باقی نمانده‌اند. پس ۹ در گوشه نیست و باید در وسط یك سطر یا یك ستون باشد، مانند مربع زیر

$$\begin{array}{ccc} x_۱ & ۹ & z_۱ \\ x_۲ & ۵ & z_۲ \\ x_۳ & ۱ & z_۳ \end{array}$$

عدد ۷ با ۹ دریك سطر نیست، زیرا مجموع ۷ و ۹ از ۱۵ بزرگتر است. همچنین ۷ با ۱ دریك سطر نیست، زیرا دراین‌صورت عدد سوم سطر هم باید ۷ باشد. پس ۷ هم در گوشه نیست و می‌توانیم فرض کنیم که مربع به‌صورت زیر است

$$x_1 \quad ۹ \quad z_1$$
$$۷ \quad ۵ \quad ۳$$
$$x_۳ \quad ۱ \quad z_۳$$

عددهای سطر شامل ۹ باید ۲ و ۴ باشند، چه درغیراین‌صورت مجموع سطر از ۱۵ بیشتر می‌شود. ۲ درستون شامل ۷ است، چه اگر ۴ در این ستون باشد، عدد دیگر آن‌هم ۴ می‌شود. به‌این‌ترتیب‌جاهای ۶ و ۸ هم مشخص‌می‌شوند و به‌مربع‌سحرآمیز شکل ۱.۵.۱ می‌رسیم.

برای‌مقادیر بزرگتر n می‌توان مربعهای سحرآمیز متنوع ساخت؛ درقرنهای شانزدهم و هفدهم وحتی بعدازآن، ساختن مربع سحرآمیز، مانند جدولهای‌متقاطع امروزه، متداول شد. بنجمین فرانکلین به‌ساختن مربع سحرآمیز عشق می‌ورزید. او بعدها اقرارکردکه وقتی دبیر مجمع پنسیلوانیا بوده است برای‌رفع خستگی ازکار رسمی‌اش، مربعهای سحرآمیز عجیب وغریب و حتی دایره‌های سحرآمیزی متشکل ازدایره‌های به‌هم‌پیچیده‌ازاعداد راکه مجموعشان روی‌همهٔ دایره‌ها یکی بوده‌است، می‌ساخته‌است. آنچه در زیر می‌آید نقل‌از نوشته‌های‌بنجمین‌فرانکلین[1] است.

مربعهای‌سحرآمیز فرانکلین وقتی شناخته‌شدکه یکی‌ازدوستانش آقای لوگن[2] چند کتاب دربارهٔ این موضوع به او نشان داد و گفت که باور ندارد یك انگلیسی کار جالبی ازاین‌نوع کرده باشد. «سپس درهمان‌کتاب چندنمونهٔ‌کمیاب وازنوعی عجیبتر به‌من نشان داد، وقتی‌گفتم فکر نمی‌کنم هیچیك به‌پای آنهایی کـه ساخته‌ام برسد، ازمن‌خواست‌که آنهارا ببیند؛ از اینرو دفعهٔ بعدکه به‌ملاقات او رفتم‌برایش مربعی ۸ تایی‌که در بین نوشته‌های قدیمی‌ام پیداکردم، بردم و اکنون ویژگیهایش را برایتان شرح می‌دهم.» (شکل ۴.۵.۱)

فرانکلین تنها به‌چند ویژگی‌مربعش اشاره می‌کند؛ پیداکردن ویژگیهای‌دیگر را به‌عهدهٔ خواننده می‌گذاریم. دیده می‌شودکـه مجموع $s = ۲۶۰$ است، مجموع هرنیمسطر وهرنیمستون ۱۳۰، نصف ۲۶۰ است، مجموع اعداد چهارگوشه وچهار عدد وسط ۲۶۰ است. مجموع سطر خمیده‌کـه از ۱۶ تا ۱۰ به‌بالا و بعداز ۲۳ تا ۱۷ به‌پایین می‌رود ۲۶۰ است، و همچنین است مجموع هرسطر خمیدهٔ ۸ عددی.

«بعد آقای لوگن یك‌کتاب حساب قدیمی، به‌قطع ربعی، گمان می‌کنم نوشتهٔ

---

1. *The Papers of Benjamin Franklin*, Yale University Press, vol. 4, p p. 392-403. 2. Logan

۵۲	۶۱	۴	۱۳	۲۰	۲۹	۳۶	۴۵
۱۴	۳	۶۲	۵۱	۴۶	۳۵	۳۰	۱۹
۵۳	۶۰	۵	۱۲	۲۱	۲۸	۳۷	۴۲
۱۱	۶	۵۹	۵۴	۴۳	۳۸	۲۷	۲۲
۵۵	۵۸	۷	۱۰	۲۳	۲۶	۳۹	۴۲
۹	۸	۵۷	۵۶	۴۱	۴۰	۲۵	۲۴
۵۰	۶۳	۲	۱۵	۱۸	۳۱	۴۴	۴۷
۱۶	۱	۶۴	۴۹	۴۸	۳۳	۳۲	۱۷

شکل ۴.۵.۱

استیفلیوس [مایکل استیفل، حساب اعداد صحیح[1]، نورنبرگ ۱۵۴۴] به‌من نشان‌داد که در آن یك مربع ۱۶ تایی بود، و گفت تصور می‌کنم این جدول خیلی کار برده باشد؛ اما اگر فراموش نکرده باشم تنها ویژگیش این بود که مجموع هرسطر افقی، عمودی، و هرقطر آن ۲۰۵۶ بود.

«چون نمی‌خواستم حتی از نظر اندازهٔ مربع، استیفلیوس از من پیشی گرفته باشد، به‌منزل برگشتم و همان شب مربع ۱۶ تایی راکه در زیر می‌آید ساختم. این مربع علاوه‌براینکه تمام ویژگیهای مربع ۸ تایی سابق‌الذکررا دارد، یعنی مجموع هرسطر، هرستون و هرقطر آن ۲۰۵۶ است، این ویژگی رانیز داردکه اگر دریك تکه‌کاغذ سوراخی به‌شکل مربع ایجادکنیم، به‌اندازه‌ای‌که وقتی‌کاغذ را روی مربع بزرگتر می‌گذاریم، درست ۱۶ مربع کوچك دیده شود، این سوراخ در هرجای مربع‌بزرگ قرارگیرد، مجموع ۱۶ عددی‌که ازسوراخ‌دیده‌می‌شود ۲۰۵۶ است.»

مربع سحرآمیز فرانکلین را در شکل ۵.۵.۱ می‌بینید، خودتان می‌توانید ویژگیهای جالب آن‌را بیازمایید.

ازدنبالهٔ نامهٔ فرانکلین دیده‌می‌شودکه به‌حق به‌چیزی‌که به‌وجود آورده‌است، افتخار می‌کند: «صبح روز بعد این مربع‌را برای دوستمان فرستادم، او چندروز بعد آن‌را با نامه‌ای پس فرستاد، با این عبارات: «کار حیرت‌انگیزت یا عجیب‌ترین

1. Michael Stiefel, *Arithmetica integra*

200	217	232	249	8	25	40	57	72	89	104	121	136	153	168	185
58	39	26	7	250	231	218	199	186	167	154	135	122	103	90	71
198	219	230	251	6	27	38	59	70	91	102	123	134	155	166	187
60	37	28	5	252	229	220	197	188	165	156	133	124	101	92	69
201	216	233	248	9	24	41	56	73	88	105	120	137	152	169	184
55	42	23	10	247	234	215	202	183	170	151	138	119	106	87	74
203	214	235	246	11	22	43	54	75	86	107	118	139	150	171	182
53	44	21	12	245	236	213	204	181	172	149	140	117	108	85	76
205	212	237	244	13	20	45	52	77	84	109	116	141	148	173	180
51	46	19	14	243	238	211	206	179	174	147	142	115	110	83	78
207	210	239	242	15	18	47	50	79	82	111	114	143	146	175	178
49	48	17	16	241	240	209	208	177	176	145	144	113	112	81	80
196	221	228	253	4	29	36	61	68	93	100	125	132	157	164	189
62	35	30	3	254	227	222	195	190	163	158	131	126	99	94	67
194	223	226	255	2	31	34	63	66	95	98	127	130	159	162	191
64	33	32	1	256	225	224	193	192	161	160	129	128	97	96	65

شکل ۵۰۵۰۱

مربع سحرآمیز را به‌تو باز می‌گردانم...» اما تعریف، بیش‌ازحد اغراق‌آمیز است و ازاینرو، بدخاطر او، و همچنین بدخاطر خودم، نباید آن‌را تکرارکنم. تکرار آن هم لازم نیست، زیرا من هیچ ادعایی ندارم، اما با رغبت خواهید پذیرفت که این مربع ۱۶ تایی، سحرآمیزترین مربع سحرآمیزی است که تابه‌حال ساحری ساخته است.»

برای اطلاع بیشتر دربارهٔ ساختن مربعهای سحرآمیز کتاب زیر را ببینید:

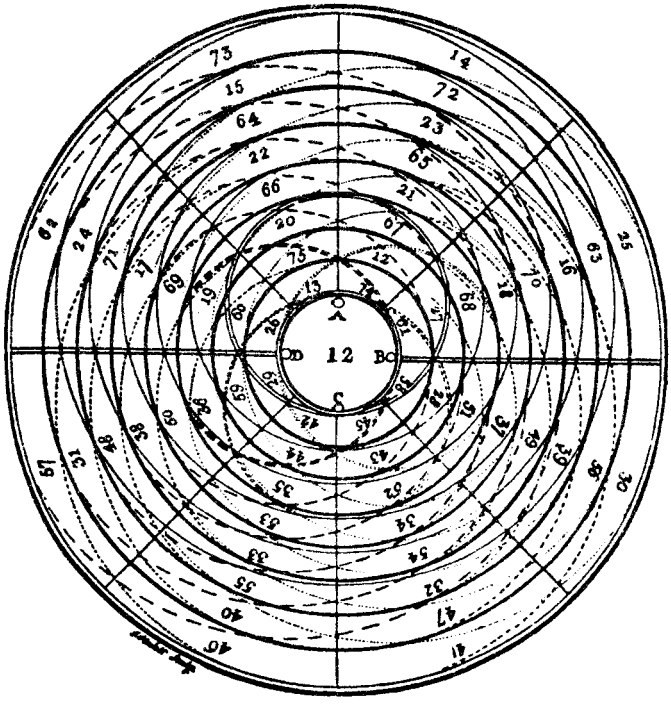
J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, Mc Graw-Hill, New York, 1939.

مجموعهٔ مسائل ۵۰۱

۱. وقتی دورر مربع سحرآمیزش را ساخت (شکل ۳۰۵۰۱) آیا می‌توانست مربعهای دیگری بسازد که در آنها به‌همان شیوهٔ مربعش سال ۱۵۱۴ نشان داده شده باشد؟

۲. دورر تا سال ۱۵۲۸ زنده بود. آیا می‌توانست در کارهای بعدی‌اش به‌همین ترتیب تاریخ را مشخص کند؟

۳. بعضی از ویژگیهای دایره‌های سحرآمیز فرانکلین (شکل ۶۰۵۰۱) را به‌دست آورید.



شکل ۶۰۵۰۱ این یک‌کپی از دایره‌های سحرآمیز فرانکلین‌است. اصل آن رنگی‌است و اخیراً در یک حراج در نیویورک به‌یک‌گردآورندهٔ اشیاء جالب فروخته شده است.

فصل ۲

عددهای اول

۱.۲ اعداد اول و اعداد مرکب

اینکه بعضی از عددها را می‌توان به‌حاصلضرب دو یا چند عدد کوچکتر تجزیه کرد، باید یکی از نخستین ویژگیهایی باشد که به‌آن پی برده‌اند، مثلا

$$۶ = ۲.۳, \quad ۹ = ۳.۳, \quad ۳۰ = ۲.۱۵ = ۳.۱۰,$$

درصورتی که اعداد دیگری نظیر

$$۳, \quad ۷, \quad ۱۳, \quad ۳۷$$

به‌حاصلضرب اعدادی کوچکتر تجزیه نمی‌شوند. یادآوری می‌کنیم که در حالت کلی وقتی

$$c = a.b, \qquad (۱.۱.۲)$$

یعنی c حاصلضرب دو عدد a و b است، a و b را عاملها یا مقسوم‌علیه‌های c می‌نامیم، یا می‌گوییم a و b، عدد c را می‌شمارند. تجزیهٔ c را به

$$c = ۱.c = c.۱ \qquad (۲.۱.۲)$$

تجزیهٔ بدیهی c و متناظراً ۱ و c را مقسوم‌علیه‌های بدیهی می‌گوییم. هرعدد تجزیهٔ

بدیهی دارد.

هرعدد $c > ۱$ که تجزیهٔ نابدیهی داشته باشد، عدد مرکب خوانده می‌شود. اگر c تنها تجزیهٔ بدیهی (۲.۱.۲) را داشته باشد، می‌گوییم c عدد اول است. از صد عدد ۱ تا ۱۰۰، بیست و پنج عدد زیر، اول‌اند:

۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷,

۴۱, ۴۳, ۴۷, ۵۳, ۵۹, ۶۱, ۶۷, ۷۱, ۷۳, ۷۹, ۸۳, ۸۹, ۹۷.

اعدادی که باقی می‌مانند، بجز ۱، اعدادی مرکب‌اند. توجه کنید که:

قضیهٔ ۱.۱.۲. هرعدد صحیح $c > ۱$ یا اول است یا مقسوم‌علیه اول دارد.

برهان. اگر c اول نباشد، یك کوچکترین مقسوم‌علیه نابدیهی p دارد. p اول است، زیرا اگر p مرکب باشد، c مقسوم‌علیهی کوچکتر از p دارد.

ما اکنون به‌اولین مسألهٔمهم نظریهٔ اعداد کشانده شده‌ایم: چطور می‌توان فهمید که عددی اول است یا مرکب؛ و اگر مرکب باشد چطور می‌توان یـك مقسوم‌علیه نابدیهی آن را به‌دست آورد؟

یك‌جواب فوری که رضایتبخش نیست، این‌است که عدد مفروض c را برتمام اعداد کوچکتر از آن تقسیم کنیم. برطبق قضیهٔ ۱.۱.۲ کافی است c را برتمام اعداد اول کوچکتر از c تقسیم کنیم. اما اگر توجه کنیم که‌درتجزیهٔ (۱.۱.۲)، a و b هردوباهم از $\sqrt{c}$ بزرگتر نیستند کار کمتر می‌شود. زیرا اگر a و b بزرگتراز $\sqrt{c}$ باشند،

$$a.b > \sqrt{c}.\sqrt{c} = c$$

نتیجه می‌شود، که ناممکن‌است. پس برای‌اینکه دریابیم c اول است یا مرکب، کافی است بررسی کنیم که آیا بعضی از عددهای اول کوچکتر از $\sqrt{c}$ یا $\sqrt{c}$ عدد c را می‌شمارند یا نه.

مثال ۱. اگر $c = ۹۱$، آن‌گاه $\sqrt{c} = ۹.۵۴۴\ldots$؛ از تقسیم ۹۱ بر ۲، ۳، ۵، ۷ می‌بینیم که $۹۱ = ۷.۱۳$.

مثال ۲. اگر $c = ۱۹۷۳$، به‌دست می‌آورید $\sqrt{c} = ۴۴.۹\ldots$. چون عـدد اول ۴۳ و هیچیك از اعداد اول کوچکتر از ۴۳ مقسوم‌علیه c نیستند، c عدد اول است.

ملاحظه می‌کنید که این روش برای عددهای بزرگ کار زیادی می‌برد. امادر اینجا ودر بسیاری ازمحاسبات دیگر نظریهٔ اعداد،می‌توانیم از تکنیکهای جدیدکمك بگیریم. کامپیوتر با برنامهٔ ساده‌ای c را برتمام اعداد صحیح تا $\sqrt{c}$ تقسیم می‌کند و عددهایی‌راکه تقسیم برآنها باقیمانده ندارد، یعنی آنهایی کـه c را می‌شمارند، صورت می‌دهد.

روش‌دیگری‌که خیلی ساده است تکیه‌کردن برجدولهای عددهای اول است، یعنی استفاده‌کردن از کار دیگران. در دوقرن اخیر چند جدول اعداد اول، تهیه و چاپ شده‌اند. یکی از بزرگترین آنها کـه در دسترس است جدول لمر[1] است که تمام اعداد اول تا ۱۰,۰۰۰,۰۰۰ درآن ثبت شده است. جدول ۱ ما اعداد اول تا ۱۰۰۰ را شامل است.

بعضی‌از محاسبان پرشور جدولهایی از اعداد اول بیش از ۱۰,۰۰۰,۰۰۰ تهیه‌کرده‌اند. اما به‌نظرنمی‌رسد چاپ کردن آنها باتوجه‌به‌هزینه وکار فوق‌العاده‌ای که باید صرف شود، جالب باشد. خیلی‌کم اتفاق می‌افتدکـه ریاضیدانی، حتی یك متخصص نظریهٔ اعداد، با مسألهٔ تعیین‌اینکه عددی بزرگ، اول است یانیست‌مواجه شود. علاوه‌براین، ریاضیدان علاقه‌ندارد بداندکه عددبزرگی مرکب‌است یا اول؛ بلکه دربارهٔ عددهایی تحقیق می‌کندکه معمولا در مسأله‌های ریاضی‌بخصوصی‌ظاهر می‌شوند و صورتهای خاصی دارند.

جدول ۱. عددهای اول بین اعداد از یك تا هزار

۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷, ۴۱, ۴۳, ۴۷, ۵۳,
۵۹, ۶۱, ۶۷, ۷۱, ۷۳, ۷۹, ۸۳, ۸۹, ۹۷,
۱۰۱, ۱۰۳, ۱۰۷, ۱۰۹, ۱۱۳, ۱۲۷, ۱۳۱, ۱۳۷, ۱۳۹, ۱۴۹, ۱۵۱,
۱۵۷, ۱۶۳, ۱۶۷, ۱۷۳, ۱۷۹, ۱۸۱, ۱۹۱, ۱۹۳, ۱۹۷, ۱۹۹,
۲۱۱, ۲۲۳, ۲۲۷, ۲۲۹, ۲۳۳, ۲۳۹, ۲۴۱, ۲۵۱, ۲۵۷, ۲۶۳, ۲۶۹,
۲۷۱, ۲۷۷, ۲۸۱, ۲۸۳, ۲۹۳,
۳۰۷, ۳۱۱, ۳۱۳, ۳۱۷, ۳۳۱, ۳۳۷, ۳۴۷, ۳۴۹, ۳۵۳, ۳۵۹, ۳۶۷,

1. D. N. Lehmer

۳۷۳,, ۳۷۹, ۳۸۳, ۳۸۹, ۳۹۷

۴۰۱, ۴۰۹, ۴۱۹, ۴۲۱, ۴۳۱, ۴۳۳, ۴۳۹, ۴۴۳, ۴۴۹, ۴۵۷, ۴۶۱,

۴۶۳, ۴۶۷, ۴۷۹, ۴۸۷, ۴۹۱, ۴۹۹,

۵۰۳, ۵۰۹, ۵۲۱, ۵۲۳, ۵۴۱, ۵۴۷, ۵۵۷, ۵۶۳, ۵۶۹, ۵۷۱, ۵۷۷,

۵۸۷, ۵۹۳, ۵۹۹,

۶۰۱, ۶۰۷, ۶۱۳, ۶۱۷, ۶۱۹, ۶۳۱, ۶۴۱, ۶۴۳, ۶۴۷, ۶۵۳, ۶۵۹,

۶۶۱, ۶۷۳, ۶۷۷, ۶۸۳, ۶۹۱,

۷۰۱, ۷۰۹, ۷۱۹, ۷۲۷, ۷۳۳, ۷۳۹, ۷۴۳, ۷۵۱, ۷۵۷, ۷۶۱, ۷۶۹,

۷۷۳, ۷۸۷, ۷۹۷,

۸۰۹, ۸۱۱, ۸۲۱, ۸۲۳, ۸۲۷, ۸۲۹, ۸۳۹, ۸۵۳, ۸۵۷, ۸۵۹, ۸۶۳,

۸۷۷, ۸۸۱, ۸۸۳, ۸۸۷,

۹۰۷, ۹۱۱, ۹۱۹, ۹۲۹, ۹۳۷, ۹۴۱, ۹۴۷, ۹۵۳, ۹۶۷, ۹۷۱, ۹۷۷,

۹۸۳, ۹۹۱, ۹۹۷.

مجموعهٔ مسائل ۱۰۲

۱. کدام‌یك از اعداد زیر اول‌اند
(الف) سال تولدتان؟
(ب) سالی‌که در آن هستیم؟
(ج) شمارهٔ منزلتان؟

۲. اولین عدد اول بعداز ۱۹۷۳ را بیابید.

۳. توجه‌کنیدکه هفت عدد از ۹۰ تا ۹۶ مرکب هستند؛نه عدد متوالی مرکب بیابید.

۲.۲ عددهای اول مرسن

چندین‌قرن مسابقهٔاعداد اول ادامه‌یافت. بسیاری‌از ریاضیدانان برای به‌دست‌آوردن

افتخار کشف عدد اولی بزرگتر از اعداد اول شناخته‌شده، رقابت می‌کردند. البته می‌توانستند اعداد بزرگی را که روشن‌بود مقسوم‌علیه‌هایی نظیر ۲، ۳، ۵، ۷ ندارند انتخاب کنند و بررسی کنند اول هستند یا مرکب. اما به‌زودی دریافتند که این راه چندان کارا نیست و مسابقه به‌این ترتیب تنظیم شد که تنها مسیری را طی کنند که معلوم شده است موفقیت‌آمیز است.

عددهای اول مرسن، عددهای اولی به‌صورت

$$M_p = ۲^p - ۱ \qquad (۱.۲.۲)$$

هستند که در آن p عددی اول است. این عددها از قدیم وارد ریاضیات شدند و در بحث اقلیدس دربارهٔ اعداد تام دیده می‌شوند. اعداد تام را در فصل سوم مطرح خواهیم کرد. عددهای اول به صورت (۱.۲.۲) را به خاطر مرسن[1] راهب فرانسوی که روی اعداد تام مجاسبات زیادی کرده‌است، عددهای اول مرسن می‌نامند.

وقتی به محاسبهٔ عددهای (۱.۲.۲) می‌پردازیم، می‌بینیم که تمام آنها اول نیستند. مثلا

$$M_۲ = ۲^۲ - ۱ = ۳ = \text{عدد اول}$$

$$M_۳ = ۲^۳ - ۱ = ۷ = \text{عدد اول}$$

$$M_۵ = ۲^۵ - ۱ = ۳۱ = \text{عدد اول}$$

$$M_۷ = ۲^۷ - ۱ = ۱۲۷ = \text{عدد اول}$$

$$M_{۱۱} = ۲^{۱۱} - ۱ = ۲۰۴۷ = ۲۳ \cdot ۸۹ .$$

برنامهٔ کلی به‌دست‌آوردن عددهای اول بزرگ، از نوع مرسن، این است که تمام‌عددهای M_p را به‌ازای عددهای اول p بیازماییم. اعداد و گرفتاریهای محاسبات خیلی سریع بزرگ می‌شوند. این کار حتی برای اعداد کاملا بزرگ عملی است به‌این دلیل که راههایی بسیار مناسب برای فهمیدن اینکه این اعداد خاص اول هستند یا نه، وجود دارند.

بالاترین نتیجه‌ای که در دورهٔ اول تحقیق در اعداد اول مرسن به دست آمد زمانی بود که اویلر[2] ثابت کرد $M_{۳۱}$ عدد اول است. در آن زمان هشت عدد اول مرسن متناظر با

---

1. Marin Mersenne (1588–1648) 2. Euler

$p=۲$, $p=۳$, $p=۵$, $p=۷$, $p=۱۳$, $p=۱۷$, $p=۱۹$, $p=۳۱$,

را پیداکرده بودند. عدد $M_{۳۱}$ اویلر بیش از یك قرن بزرگترین عدد اولی بود که می‌شناختند. درسال ۱۸۷۶ لوکا[1] ریاضیدان فرانسوی نشان‌دادکه عدد بسیار بزرگ

$$M_{۱۲۷}=۱۷۰\ ۱۴۱\ ۱۸۳\ ۴۶۰\ ۲۶۹\ ۲۳۱\ ۷۳۱\ ۶۸۷\ ۳۰۳\ ۷۱۵\ ۸۸۴$$
$$۱۰۵\ ۷۲۷$$

اول است. این عددی است که دقیقاً ۳۹ رقم دارد. عددهای اول مرسن کوچکتر از این با مقادیر p که در بالا آورده‌ایم و سه مقدار دیگر $p=۶۱$، $p=۸۹$ و $p=۱۰۷$ متناظرند.

این ۱۲ عدد اول مرسن با قلم روی‌کاغذ حساب شده‌اند، اعداد مرسن بعدی با کمك ماشین‌حساب محاسبه شده‌اند. ورود ماشینهای برقی حساب، جستجو تا $p=۲۵۷$ را ممکن ساخت؛ اما نتیجه‌ها مأیوس‌کننده بودند؛ هیچ عدد اول مرسن دیگری به‌دست نیامده بود.

تاکامپیوتر وارد عمل نشده‌بود وضع به‌همین‌منوال بود. پس‌ازظهورماشینهای باظرفیتهای بالاتر، امکان تحقیق در اعداد اول مرسن برای اعداد بزرگتر وبزرگتر به‌وجود آمد. د. ه. لمر نشان‌دادکه عدد M_p مرسن برای هریك از مقدارهای

$$p=۵۲۱,\quad p=۶۰۷,\quad p=۱۲۷۹,\quad p=۲۲۰۳,\quad p=۲۲۸۱$$

اول است. اخیراً پیشرفتهای بیشتری شده است. ریزل[2] (۱۹۵۸) نشان دادکه M_p به‌ازای

$$p=۳۲۱۷$$

عدد اول است و هورویتس[3] (۱۹۶۲) برای p دو مقدار

$$p=۴۲۵۳,\quad p=۴۴۲۳$$

را به‌دست‌آورد. جیلز[4] (۱۹۶۴) پیشرفتی عظیم به‌وجودآورد، نشان دادکه به‌ازای

$$p=۹۶۸۹,\quad p=۹۹۴۱,\quad p=۱۱۲۱۳$$

M_p عدد اول است.

---

1. Lucas
2. Riesel
3. Hurwitz
4. Gillies

تا اینجا به ۲۳ عدد اول مرسن دست یافته‌ایم، و هرچه ظرفیت ماشینها بیشتر شود، می‌توانیم امیدوار باشیم که اعداد اول مرسن بیشتری به‌دست آید. قبلا اشاره کردیم کـه $M_{۱۲۷}$، عدد اول لوکا، ۳۹ رقم دارد. محاسبهٔ $M_{۱۱۲۱۳}$، بزرگترین عدد اول شناخته‌شده، کار کمی نیست، و به‌نظر نمی‌رسد ذکر آن در اینجا لازم باشد. اما شاید علاقه‌مند باشیم که تعداد رقمهای این عـدد را بدانیم. این کار را بدون محاسبهٔ خود عدد به‌طریق زیر انجام می‌دهیم.

به‌جای تعداد ارقام $M_p = ۲^p - ۱$، تعداد ارقام عدد

$$M_p + ۱ = ۲^p$$

را به‌دست می‌آوریم. تعداد ارقام این دوعدد یکی‌است زیرا، برای‌اینکه $M_p + ۱$ یك رقم بیشتر داشته باشد، باید به ۰ ختم شود. اما این ممکن نیست زیرا همان‌طور که از دنبالهٔ

$$۲, ۴, ۸, ۱۶, ۳۲, ۶۴, ۱۲۸, ۲۵۶, \cdots$$

دیده می‌شود، رقم آخر توانهای ۲، فقط یکی از اعداد زیر است

$$۲, ۴, ۸, ۶۰$$

برای به‌دست آوردن تعداد ارقام ۲^p، یادآوری می‌کنیم که $\log ۲^p = p.\log ۲$. در جدول لگاریتم می‌بینیم که $\log ۲$ تقریباً ۰٫۳۰۱۰۳ است. پس

$$\log ۲^p = p.\log ۲ = p.۰٫۳۰۱۰۳۰$$

به‌ازای $p = ۱۱۲۱۳$،

$$\log ۲^{۱۱۲۱۳} = ۳۳۷۵٫۴۴۹\cdots,$$

واز مفسر ۳۳۷۵ نتیجه‌می‌گیریم که ۲^p عددی ۳۳۷۶ رقمی‌است. بنابراین‌می‌گوییم: بزرگترین عدد اولی که تابه‌حال شناخته شده است ۳۳۷۶ رقم دارد. (لغت «تابه‌حال» دراین‌جمله مهم است.) این عدد باکامپیوتر دانشگاه ایلنوی[1] حساب‌شده بود وگروه ریاضی این دانشگاه بدقدری از این موفقیت افتخار می‌کرد کـه روی هرنامهٔ پستی آن‌را چاپ‌کرده بود تا تحسین و تعجب همه‌را برانگیزد.*

---

1. Uuiversity of Illinois

* پس‌از آن، اعداد اول بزرگتری هم به‌دست آمده‌اندکه بزرگترین آنها عدد ۶۵۰۵ رقمی $۲۲۱۶۰۹۱ - ۱$ است که درسال ۱۹۸۵ کشف شده است.ـــو.

۳.۲ عددهای اول فرما

عددهای اول فرما[1] نوع دیگری از اعداد اول است که تاریخی طولانی و جالب دارد. فرما (۱۶۰۱–۱۶۶۵) قاضی و ریاضیدان فرانسوی این اعداد را معرفی کرد. نخستین پنج عدد اول فرما در زیر آمده‌اند

$$F_0 = 2^{2^0} + 1 = 3,\ F_1 = 2^{2^1} + 1 = 5,\ F_2 = 2^{2^2} + 1 = 17,$$

$$F_3 = 2^{2^3} + 1 = 257,\ F_4 = 2^{2^4} + 1 = 65537.$$

برطبق این دنباله، فرمول کلی اعداد اول فرما

$$F_n = 2^{2^n} + 1 \qquad (1.3.2)$$

است. فرما یقین داشت که تمام این اعداد، اول هستند، گرچه تنها پنج عدد بالا را حساب کرده بود. اما اویلر ریاضیدان سویسی یك قدم پیشتر گذاشت و نشان داد که برخلاف حدس فرما

$$F_5 = 4294967297 = 641 \cdot 6700417$$

عدد اول نیست. اگر عددهای فرما در رسم چندضلعیهای منتظم با خط‌کش و پرگار، که مسألهای کاملا متفاوت است، ظاهر نشده بودند، حکایت اعداد فرما احتمالا به‌همین‌جا خاتمه یافته بود.

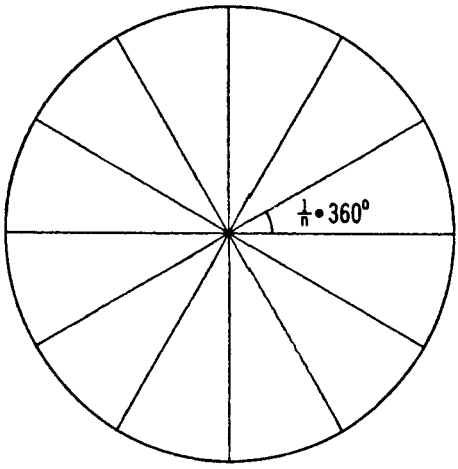
چندضلعی منتظم چندضلعیی است که رأسهای آن به‌فاصله‌های مساوی روی یك دایره واقع‌اند (شکل ۱.۳.۲)، اگر چند ضلعی منتظم، n راس داشته باشد، آن را n ضلعی می‌نامیم. از n خطی که از هر رأس به‌مرکز دایره رسم می‌شود، n زاویهٔ مرکزی به‌وجود می‌آید که اندازهٔ هریك

$$\frac{1}{n}.360^\circ$$

است. اگر بتوانیم این زاویه را رسم کنیم، n ضلعی را نیز می‌توانیم بسازیم.

یونانیان قدیم خیلی علاقه داشتند روشهایی برای رسم چند ضلعیهای منتظم با خط‌کش و پرگار بیابند. البته حالتهای سادهٔ مثلث متساوی‌الاضلاع و مربع را می‌توانستند رسم کنند. بنابراین با نصف کردن زاویهٔ مرکزی و تکرار این عمل قادر

1. Fermat



شکل ۱۰۳۰۲

بودند چندضلعیهای منتظم دارای

$$۴, ۸, ۱۶, ۳۲, \ldots$$

$$۳, ۶, ۱۲, ۲۴, \ldots$$

ضلع رانیز رسم کنند. علاوه‌براینها چون پنجضلعی منتظم‌را می‌توانستند رسم کنند، از عهدهٔ رسم

$$۵, ۱۰, ۲۰, ۴۰, \ldots$$

ضلعی منتظم نیز برمی‌آمدند. زاویهٔ مرکزی در ۱۵ ضلعی منتظم برابر است با

$$\frac{۱}{۱۵} \cdot ۳۶۰^\circ = ۲۴^\circ,$$

و این زاویه را می‌توان از ۷۲°، زاویهٔ مرکزی پنجضلعی منتظم، و ۱۲۰°، زاویهٔ مرکزی سه ضلعی منتظم، به‌دست آورد: می‌توان زاویهٔ اول را دوبار رسم کرد و زاویهٔ دوم را از آن کم کرد. پس می‌توانیم دستهٔ دیگری از چند ضلعیهای منتظم: ۱۵، ۳۰، ۶۰، ۱۲۰، . . . ضلعی را رسم کنیم.

وضع بدین‌منوال بود تا اینکه درسال ۱۸۰۱ ریاضیدان جوان آلمانی گاوس[1] (۱۷۷۷–۱۸۵۵) کتابی در نظریهٔ اعداد به‌نام مطالعاتی درحساب[2] که عصر جدیدی در ریاضیات به‌وجود آورد، منتشر کـرد. گاوس نه‌تنها با ارائهٔ راه رسم ۱۷ ضلعی منتظم با خط‌کش و پرگار از هندسه‌دانان یونانی پیشی گرفت، بلکه خیلی بیش از اینها به‌جلو رفت. گاوس تعیین کرد کـدام n ضلعی منتظم را می‌توان با خط‌کش و پرگار رسم کرد و کدام‌را نمی‌توان. اینك به‌شرح نتیجه‌هایی که گاوس به‌دست‌آورده است می‌پردازیم.

در بالا توصیه کردیم که اگر هرزاویهٔ مرکزی یك n ضلعی منتظم را به‌دونیمه تقسیم کنیم یك $2n$ ضلعی منتظم به دست می آید. از طرف دیگر، از یك $2n$ ضلعی اگر راسها را یك درمیان انتخاب کنیم، یك n ضلعی منتظم نتیجه می‌شود. پس برای اینکه تعیین کنیم کدام n ضلعی منتظم‌را می‌توان رسم کرد، کافی‌است n را فردبگیریم گاوس نشان داد کـه به‌ازای n های فرد، n ضلعی منتظم را می‌توان با خط‌کش و پرگار رسم‌کرد، اگر و تنها اگر n یك‌عدد اول فرما یا حاصلضرب چند عدد اول متمایز فرما باشد.

کوچکترین‌مقادیر n را می آزماییم. می بینیم که ۳ ضلعی‌منتظم و ۵ ضلعی‌منتظم را می‌توان رسم کرد، اما ۷ ضلعی منتظم‌را نمی‌توان رسم کرد، زیرا ۷ یك عدد اول فرما نیست. ۹-ضلعی را نمی‌توان رسم کرد، زیرا $۳.۳ = ۹$ حاصلضرب یـك عدد اول فرما درخودش است. به‌ازای $n = ۱۱$ یا $n = ۱۳$، چندضلعی را نمی‌توان‌رسم کرد، اما به‌ازای $n = ۱۵ = ۳.۵$ و $n = ۱۷$، n ضلعی‌را می‌توان رسم کرد.

کشف **گاوس** طبیعتاً دوباره ریاضیدانان‌را متوجه اعداد (۱.۳.۲) فرما کـرد. درقرن اخیر برای یافتن دیگر عددهای اول فرما، بدون‌کمك ماشین، چندین‌محاسبهٔ بسیار بزرگ انجام شد. اکنون این محاسبات باکمك‌کامپیوتر به‌میزانی بیشتر و رو به‌افزایش ادامه دارد. تا امروز نتیجه‌ها منفی بوده‌اند. هیچ عدد فرمای جدیدی کـه اول باشد به‌دست نیامده و بسیاری از ریاضیدانان فکر می‌کنند که عدد اول فرمای دیگری وجود ندارد.

مجموعهٔ مسائل ۳.۲

۱. تمام عددهای فرد $n < ۱۰۰$ راکـه به‌ازای آنها رسم n ضلعی منتظم امکانپذیر

---

1. C. F. Gauss 2. Disquisitiones Arithmeticae (English edition, Yale University Press, 1966.)

است، بیابید.

۲. فرض کنید می‌توانید ۱۷ ضلعی منتظم را رسم کنید، چگونه ۵۱ ضلعی منتظم را رسم می‌کنید؟

۳. اگر جز ۵ عدد اول فرماکه نام‌برده‌ایم عدد فرمای اول وجود نداشته باشد، چند n ضلعی منتظم (n فرد) می‌توان رسم کرد؟ بزرگترین عدد فرد n که n ضلعی منتظم را می‌توان رسم کرد کدام است؟

۴.۲ غربال اراتستن[1]

گفتیم که جدولهای اعداد اول تا اعدادی بسیار بزرگ وجود دارند. چطور می‌توان چنین جدولهایی را ساخت؟ این مسأله را اراتستن، ریاضیدان اهل اسکندریه (حدود ۲۰۰ سال قبل‌ازمیلاد) حل کرده است. روش او این است: دنبالهٔ تمام عددها را از ۱ تا هرعددی که می‌خواهیم جدول را به‌آن ختم کنیم، می‌نویسیم:

۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
	—	—	—	—	—	—	—	—	—		—		—	—
	۲		۲		۲		۲	۳	۲		۲		۲	۳

با عدد اول ۲ شروع می‌کنیم و عدد دومی بعداز ۲، یعنی ۴، و عدد دومی بعداز ۴ و به‌همین‌ترتیب اعداد ۶، ۸، ۱۰ و غیره (اما نه خود ۲) را با کشیدن خطی زیر آنها، حذف می‌کنیم. بعد از این کار اولین عددی که زیر آن خط ندارد ۳ است. ۳ عدد اول است زیرا بر ۲ تقسیمپذیر نیست. زیر ۳ خط نمی‌کشیم، اما زیر عدد سومی بعداز ۳، یعنی ۶، و عدد سومی بعداز ۶ و به‌همین‌ترتیب زیر اعداد ۹، ۱۲، ۱۵ و غیره خط می‌کشیم؛ زیر بعضی از اینها قبلا خط کشیده شده است، زیرا زوج هستند. در مرحلهٔ بعد اولین عددی که زیرش خط ندارد ۵ است؛ ۵ عدد اول است زیرا بر ۲ و ۳ تقسیمپذیر نیست. زیر ۵ خط نمی‌کشیم، اما زیر عدد پنجمی بعداز ۵ و به‌همین‌ترتیب زیر عدد پنجمی بعدازآن یعنی زیر ۱۰، ۱۵، ۲۰، ... که قبلا خط نکشیده‌ایم، خط می‌کشیم. اکنون کوچکترین عددی که زیرش خط ندارد ۷ است؛ ۷ عدد اول است زیرا بر ۲، ۳، ۵ که عددهای اول کوچکتر از ۷ هستند، تقسیمپذیر نیست. این فرایندرا تکرارمی‌کنیم و بالاخره به‌دنبالهٔ عددهایی که‌زیرشان

1. Eratosthenes

خط ندارد دست می‌یابیم؛ این اعداد (به‌جز ۱) عددهای اول تا عدد مفروض‌هستند.

این‌روش غربال‌کردن عددها به غربال اراتستن معروف شده است. جدولهای اعداد اول با این‌اصل غربالی ساخته می‌شوند. درواقع با استفاده ازحافظهٔ کامپیوترها می‌توان به‌نتایج پیشرفته‌تری دست یافت. از همین‌طریق در آزمایشگاه علمی لاس‌آلاموس[1] تمام عددهای اول کوچکتراز ۱۰۰,۰۰۰,۰۰۰ را درحافظهٔ کامپیوتر ذخیره کرده‌اند.

با مختصر تغییری در روش غربال می‌توان اطلاعات بیشتری به‌دست آورد. فرض کنید وقتی زیر عددی خط می‌کشیم و آن را با این علامت حذف می‌کنیم، عددی‌که آن را حذف می‌کند زیر خط بنویسیم. مثلا ۱۵ و ۳۵ را به‌صورت

$$\frac{۱۵}{۳}, \quad \frac{۳۵}{۵}$$

درآوریم؛ در دنبالهٔ از ۱ تا ۱۵ بالا این‌روش عمل شده است. با این‌روش عددهای اول را مشخص کرده‌ایم و کوچکترین عدد اولی‌که عدد مرکب را می‌شمارد، نشان داده‌ایم. چنین فهرستی از اعداد را جدول عاملها می‌نامند. ساختن جدول عاملها بیش از جدول اعداد اول کار می‌برد. برای اینکه جدول کمی ساده شود، معمولا عددهای مرکبی راکه عاملهای کوچکی مانند ۲، ۳، ۵، ۷ دارند از جدول حذف می‌کنند. بزرگترین جدول‌عاملهای موجود، جدولی‌است‌که **د. ن.** لمر حساب کرده‌است وتا ۱۰,۰۰۰,۰۰۰ پیش رفته است.

دیدیم‌که غربال اراتستن را می‌توان برای‌ساختن جدول اعداد اول و جدول عاملها به‌کار برد. اما این‌غربال برای منظورهای نظری نیز به‌کار می‌رود، و درنظریهٔ جدید اعداد با روش غربال به‌نتیجه‌های مهم رسیده‌اند. حقیقتی راکه اقلیدس هم به آن واقف بوده است در اینجا ذکر می‌کنیم:

مجموعهٔ اعداد اول نامتناهی است.

برهان. فرض کنید تنها k عدد اول

$$۲, ۳, ۵, \ldots, p_k$$

وجود دارند. آن‌گاه درغربال بعداز p_k هیچ عدد بدون خط وجود ندارد. اما این ممکن نیست زیرا حاصلضرب k عدد اول:

---

1. Los Alamos Scientific Laboratory

$$P = ۲.۳.۵...p_k,$$

k بار (به‌ازای هر عدد اول یك‌بار) حذف می‌شود. بنابراین $P+۱$ برهیچیك از عددهای اول تقسیم‌پذیر نیست، پس زیرش خط ندارد.

مجموعهٔ مسائل ۴۰۲

۱. برای هریك از صد عدد: ۱۰۰–۱، ۲۰۰–۱۰۱، ...، ۱۰۰۰–۹۰۱ جدول اعداد اول تشکیل دهید.

۲. کوشش کنید تعداد اعداد اول بین ۱۰۰۰۱ تا ۱۰۱۰۰ را تعیین کنید.

فصل ۳

مقسوم‌علیه‌های اعداد

۱.۳ قضیهٔ اساسی تجزیه به‌عاملهای اول

عدد مرکب c را می‌توان به‌صورت حاصلضرب $c=a.b$ نوشت، که در آن هیچیك از عاملها ۱ نیست و هردو از c کوچکترند؛ مثلا

$$۷۲=۸.۹, \quad ۱۵۰=۱۰.۱۵.$$

در تجزیهٔ c، از دو عامل a و b یکی یا هردو ممکن‌است عدد مرکب باشد. اگر a مرکب باشد، آن‌را می‌توان دوباره تجزیه‌کرد:

$$a=a_۱.a_۲, \quad c=a_۱.a_۲.b.$$

در مثال بالا

$$۷۲=۲.۴.۹, \quad ۱۵۰=۲.۵.۱۵.$$

پس‌از چندبار تکرار این‌فرایند، عمل متوقف‌می‌شود، زیرا عاملها کوچکتر وکوچکتر می‌شوند و باید از ۱ بزرگتر باشند. وقتی عمل تجزیه متوقف می‌شود، تمام عاملها اول هستند. بدین ترتیب نشان داده‌ایم‌که:

هرعدد صحیح بزرگتر از ۱ یا اول است یا حاصلضرب اعداد اول.

تجزیهٔ چندمرحله‌ای عدد را می‌توان از طریقهای زیادی به‌انجام رساند. می‌توانیم جدول عاملها را به‌کار بریم و نخست p_1، کوچکترین عدد اولی که c را می‌شمارد، از جدول پیدا کنیم و c را به‌صورت $p = p_1 \cdot c_1$ بنویسیم. اگر c_1 عدد مرکب باشد، p_2، کوچکترین عدد اولی که c_1 را می‌شمارد از جدول به‌دست آورده می‌نویسیم

$$c_1 = p_2 \cdot c_2, \quad c = p_1 \cdot p_2 \cdot c_2 .$$

سپس کوچکترین عامل اول c_2 را از جدول پیدا می‌کنیم و به‌این‌کار ادامه می‌دهیم.

این حقیقتی اساسی است که از هرراهی عدد را به‌عاملهای اول تجزیه کنیم، صرفنظر از ترتیب عاملها، به‌یك نتیجه می‌رسیم؛ یعنی در دوتجزیهٔ یك عدد، عاملهای اول یکی هستند و هرعامل اول به‌یك‌اندازه تکرار می‌شود. این نتیجه را به‌صورت خلاصهٔ زیر بیان می‌کنیم:

تجزیهٔ هرعدد به‌عاملهای اول یکتاست.

شاید این راکه «قضیهٔ اصلی علم‌حساب» می‌گویند شنیده باشید وآن‌قدر آن را به‌کار برده باشیدکه به‌نظرتان امری واضح جلوه‌کند؛ اما چنین نیست. قضیه را می‌توان ازچندراه اثبات‌کرد، اما هیچیك از راهها پیش‌پاافتاده نیست. ما این‌قضیه را از راهی‌که به برهان خلف معروف است اثبات می‌کنیم. یعنی فرض می‌کنیم که قضیه‌ای‌که بایداثبات‌شود دروغ است ونشان می‌دهیم‌که این‌فرض به‌تناقض می‌رسد.

برهان. فرض کنیدکه قضیهٔ یکتایی‌عاملها راست‌نیست. دراین‌صورت‌عددهایی باید باشندکه تجزیه‌های متعدد به‌عاملهای اول داشته‌باشند. کوچکترین این‌نوع‌عددها را c_0 می‌نامیم. برای اعدادکوچك، مثلا تا ۱۰، دیده می‌شودکه قضیه راست است. کوچکترین عامل اول c_0 را p_0 نامیده می‌نویسیم

$$c_0 = p_0 \cdot d_0 .$$

d_0 چون از c_0 کوچکتر است فقط یك تجزیه به‌عاملهای اول دارد، پس فقط دریکی از تجزیه‌های c_0 به‌عاملهای اول، p_0 وجود دارد.

چون فرض کرده‌ایم‌که دست‌کم c_0 دو تجزیه به‌عاملهای اول دارد، تجزیه‌ای وجود داردکه درآن p_0 نیست. کوچکترین عامل اول این تجزیه به‌عاملهای اول‌را p_1 نامیده می‌نویسیم

$$c_0 = p_1 \cdot d_1 . \qquad (۱۰۱۰۳)$$

از $p_1 > p_0$، $d_1 < d_0$ نتیجه می‌شود، پس $p_0 d_1 < c_0$. اکنون به‌عدد

$$c_0' = c_0 - p_0 . d_1 = (p_1 - p_0) d_1 \qquad (۲.۱.۳)$$

توجه می‌کنیم. c_0' فقط یك تجزیه به‌عاملهای اول‌دارد، زیرا از c_0 کوچکتر است. عاملهای اول c_0' از عاملهای اول $p_1 - p_0$ و عاملهای اول d_1 تشکیل شده‌اند. اما c_0 بر p_0 تقسیمپذیر است، پس از (۲.۱.۳) نتیجه می‌شود که c_0' هم بر p_0 تقسیمپذیر است. بنابراین p_0 یا d_1 را می‌شمارد یا $p_1 - p_0$ را. اما عاملهای اول d_1 از p_0 بزرگترند، پس p_0، $p_1 - p_0$ را می‌شمارد؛ بنابراین p_0، p_1 را می‌شمارد. این یك تناقض است، زیرا p_1 عدد اول است و برعدد اول p_0 تقسیمپذیر نیست.

در بالا گفتیم که به‌هیچ‌وجه واضح نیست که هرعدد تنها یك تجزیه به‌عاملهای اول دارد. درحقیقت «حسابهایی» وجود دارند که در آنها این قضیه راست نیست. برای اینکه مثالی خیلی ساده آورده باشیم، اعداد زوج

$$۲, ۴, ۶, ۸, ۱۰, ۱۲, \ldots$$

را درنظر می‌گیریم. بعضی‌ازاین اعداد به‌حاصلضرب دوعدد زوج تجزیه می‌شوند و بعضی‌دیگر نمی‌شوند. آنهایی‌راکه به‌دوعدد زوج‌تجزیه‌نمی‌شوند، اعداد زوج-اول می‌نامیم. اینها اعدادی هستندکه بر ۲ تقسیمپذیرند ولی بر ۴ تقسیمپذیر نیستند:

$$۲, ۶, ۱۰, ۱۴, ۱۸, \ldots$$

می‌بینیم که‌هرعدد زوج، یا زوج-اول‌است یا به‌حاصلضرب‌اعداد زوج-اول تجزیه می‌شود. اما این تجزیه به‌اعداد زوج-اول یکتا نیست؛ مثلا عدد ۴۲۰ چند تجزیه به‌اعداد زوج-اول دارد:

$$۴۲۰ = ۶.۷۰ = ۱۰.۴۲ = ۱۴.۳۰ .$$

مجموعهٔ مسائل ۱.۳

۱. هریك از عددهای زیر را به‌حاصلضرب عاملهای اول تجزیه‌کنید

$$۱۲۰, \quad ۳۶۵, \quad ۱۹۷۰ .$$

۲. همین‌کار را برای عددهای مساله‌های بخش ۱.۲ صفحهٔ ۱۹ انجام دهید.

۳. تمام تجزیه‌های ۳۶۰ به زوج-اولها را بنویسید.

۴. درچه‌صورتی عدد زوج تنها یك تجزیه به زوج-اولها دارد؟

۲.۳ مقسوم‌علیه‌ها

عددی را، مثلا ۳۶۰۰ را، به‌حاصلضرب اعداد اول تجزیه می‌کنیم. تجزیهٔ

$$۳۶۰۰ = ۲.۲.۲.۲.۳.۳.۵.۵$$

را می‌توانیم به‌صورت

$$۳۶۰۰ = ۲^۴.۳^۲.۵^۲$$

بنویسیم. درحالت کلی نظیر این کار را درتجزیهٔ یك عدد n می‌کنیم و می‌نویسیم

$$n = p_۱^{\alpha_۱}.p_۲^{\alpha_۲}\dots p_r^{\alpha_r}, \qquad (۱.۲.۳)$$

که در آن $p_۱$، $p_۲$، ...، p_r مقسوم‌علیه‌های اول متمایز n هستند، و $p_۱$، $\alpha_۱$ بار، $p_۲$، $\alpha_۲$ بار و ... در تجزیهٔ n وجوددارند. از روی‌تجزیهٔعدد به‌صورت (۱.۲.۳) می‌توانیم بی‌درنگ به‌بعضی از سؤالات پاسخ دهیم.

مثلا می‌خواهیم بدانیم چه عددهایی n را می‌شمارند، [و می‌خواهیم تعداد مقسوم‌علیه‌های n را حساب کنیم]. به‌عنوان مثال عدد ۳۶۰۰ راکه در بالا آوردیم درنظر بگیرید. فرض کنید d یکی از مقسوم‌علیه‌های آن است، یعنی داریم

$$۳۶۰۰ = d.d_۱.$$

تجزیه به‌اعداد اول نشان می‌دهد کـه تنها عددهای اولی‌که می‌توانند مقسوم‌علیه d باشند ۲ یا ۳ یا ۵ هستند. علاوه‌براین درتجزیهٔ d عدد ۲ حداکثر چهاربار و ۳و۵ حداکثر دوبار می‌آیند. پس مقسوم‌علیه‌های ۳۶۰۰

$$d = ۲^{\delta_۱}.۳^{\delta_۲}.۵^{\delta_۳}$$

هستندکه درآن می‌توانیم نماها را

$$\delta_۱ = ۰, ۱, ۲, ۳, ۴; \quad \delta_۲ = ۰, ۱, ۲; \quad \delta_۳ = ۰, ۱, ۲$$

انتخاب کنیم. چون اعداد انتخابی را می‌توانیم به‌تمام راههای ممکن با هم ترکیب کنیم، تعداد مقسوم‌علیه‌ها برابرند با

$$(۴+۱)(۲+۱)(۲+۱) = ۵.۳.۳ = ۴۵.$$

برای هرعددکه تجزیه به‌عاملهای‌اولش به‌صورت (۱.۲.۳) نوشته شده‌باشد، وضع به‌همین منوال است. اگر d یك مقسوم‌علیه n باشد، یعنی

$$n = d \cdot d_1 ,$$

فقط اعداد اولی امکان دارد d را بشمارند کـه مقسوم‌علیه اول n، یعنی p_1، یا p_2، یا، . . . ، یا p_r، باشند. بنابراین می‌توانیم تجزیهٔ d به‌عاملهای اول‌را به‌صورت

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_r^{\delta_r}, \qquad (۲.۲.۳)$$

بنویسیم. در تجزیهٔ d عدد اول p_1 حداکثر α_1 (تعدادموجود در تجزیهٔ n) بارمی‌آید و همچنین است درمـورد p_2 و دیگر عددهای اول. پس δ_1 را می‌توانیم یکی از $\alpha_1 + 1$ عدد زیر انتخاب کنیم:

$$\delta_1 = 0,\ 1,\ \ldots,\ \alpha_1$$

و همچنین است برای دیگر عددهای اول. چون هریك‌از $\alpha_1 + 1$ انتخاب برای δ_1 را می‌توان با $\alpha_2 + 1$ انتخاب برای δ_2 ترکیب کرد، و همچنین است بـرای دیگر δها، می‌بینیم که $r(n)$، تعدادکل مقسوم‌علیه‌های n، برابر است با:

$$r(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1). \qquad (۳.۲.۳)$$

مجموعهٔ مسائل ۲.۳

۱. یك عدد اول چند مقسوم‌علیه دارد؟ یك‌توان عدد اول، p^a، چند مقسوم‌علیه دارد؟

۲. تعداد مقسوم‌علیه‌های اعداد زیر را به‌دست آورید:

شمارهٔ کد پستی شما ؛ ۱۹۷۰ ؛ ۳۶۶ ؛ ۶۰

۳. در بین اعداد ۱ تا ۱۰۰ کوچکتر از ۱۰۰ تعداد مقسوم‌علیه‌های کدام عدد یا اعداد بیشترین است؟

۳.۳ مسأله‌های مربوط به‌مقسوم‌علیه‌ها

تنها عددی که یك‌مقسوم‌علیه دارد $n = 1$ است. عددهای اول p دقیقاً دومقسوم‌علیه دارند: ۱ و p. پس کوچکترین عددی که دو مقسوم‌علیه دارد $p = 2$ است.

ببینیم چه عددهایی دقیقاً ۳ مقسوم‌علیه دارند. برطبق (۳.۲.۳)

$$3 = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1).$$

چون ۳ اول است، در سمت راست تنها یک عامل، مخالف ۱ است، پس $r=1$ و $\alpha_1=2$. بنابراین

$$n=p_1^2.$$

$n=2^2=4$ کوچکترین عددی است که ۳ مقسوم‌علیه دارد. این استدلال را برای هرحالتی که تعداد مقسوم‌علیه‌ها عددی اول مانند q است می‌توان به‌کار برد؛ به‌دست می‌آید

$$q=\alpha_1+1, \quad \alpha_1=q-1, \quad n=p_1^{q-1},$$

وکوچکترین این عددها $n=2^{q-1}$ است.

اینک حالتی را که تعداد مقسوم‌علیه‌ها ۴ است درنظر می‌گیریم. دراین‌حالت

$$4=(\alpha_1+1)(\alpha_2+1)$$

تنها وقتی برقرار است که

$$\alpha_1=3, \quad \alpha_2=0 \quad \text{یا} \quad \alpha_1=\alpha_2=1.$$

برای n دوجواب

$$n=p_1^3, \quad n=p_1 p_2$$

به‌دست می‌آید، وکوچکترین عددی که ۴ مقسوم‌علیه دارد، $n=6$ است.

وقتی n شش مقسوم‌علیه دارد، داریم

$$6=(\alpha_1+1)(\alpha_2+1),$$

و این تنها وقتی ممکن است که

$$\alpha_1=5, \quad \alpha_2=0 \quad \text{یا} \quad \alpha_1=2, \quad \alpha_2=1.$$

پس یا $n=p_1^5$ یا $n=p_1^2 p_2$، وکوچکترین مقدار n درحالت اخیر برای

$$p_1=2, \quad p_2=3, \quad n=12$$

به‌دست می‌آید. این روش‌را برای‌محاسبهٔ کوچکترین عدد صحیحی که تعدادمفروضی مقسوم‌علیه دارد می‌توان به‌کار برد.

جدولهایی هست که تعداد مقسوم‌علیه‌های اعداد را می‌دهد. این جدولها با

$$n = ۱\ \ ۲\ \ ۳\ \ ۴\ \ ۵\ \ ۶\ \ ۷\ \ ۸\ \ ۹\ \ ۱۰\ \ ۱۱\ \ ۱۲$$

$$\tau(n) = ۱\ \ ۲\ \ ۲\ \ ۳\ \ ۲\ \ ۴\ \ ۲\ \ ۴\ \ ۳\ \ \ ۴\ \ \ ۲\ \ \ ۶$$

آغاز می‌شوند و شما می‌توانید به‌راحتی آن‌را ادامه دهید.

می گوییم عدد صحیح n قویاً مرکب است وقتی که تعداد مقسوم‌علیه‌های تمام اعداد کوچکتر از n، از تعداد مقسوم‌علیه‌های n کمتر باشد. در جدول کـوچك بالا می بینیم که

$$۱,\ ۲,\ ۴,\ ۶,\ ۱۲$$

نخستین اعداد قویاً مرکب‌هستند. چیز زیادی دربارهٔ ویژگیهای این‌اعداد نمی‌دانیم.

مجموعه مسائل ۳.۳

۱. یك دستهٔ ۱۲ نفری سربازمی‌توانند درشش‌نوع صف ۱×۱۲، ۲×۶، ۳×۴، ۴×۳، ۶×۲، ۱۲×۱ حرکت کنند. کوچکترین تعداد نفراتی راکه می‌توانند به ۸، ۱۰، ۱۲ و ۷۲ نوع صف حرکت کنند بیابید.

۲. کوچکترین اعداد صحیحی که ۱۴ مقسوم‌علیه، ۱۸ مقسوم‌علیه و ۱۰۰ مقسوم‌علیه دارند بیابید.

۳. اولین دوعدد قویاً مرکب بعداز ۱۲ را به‌دست آورید.

۴. تمام اعداد صحیحی راکه تعداد مقسوم‌علیه‌هایشان حاصلضرب دوعدد اول‌هستند، مشخص کنید.

۴.۳ عددهای تام

یونانیان قدیم خیلی شیفتهٔ عددشناسی بودند. یك‌دلیل طبیعی این شیفتگی این بودکه عددهای یونانی به‌وسیلهٔ الفبای یونانی بیان می‌شدند، به‌طوری که هرلغت، هراسم، باعددی قرین بود. اشخاص، ویژگیهای اعداد اسمهایشان را باهم مقایسه می‌کردند.

مقسوم‌علیه‌های یك عدد در عددشناسی خیلی مهم بودند. کمال‌مطلوب عدد تام (به‌معنی بی‌نقص) بود که دقیقاً از مقسوم‌علیه‌هایش ساخته می‌شد، یعنی عددی برابر با مجموع مقسوم‌علیه‌هایش. توجه کنیدکـه یونانیها خود عدد را مقسوم‌علیه آن عدد به‌حساب نمی‌آوردند.

کوچکترین عدم تام

$$۶=۱+۲+۳$$

است. عدد تام بعدی

$$۲۸=۱+۲+۴+۷+۱۴,$$

و بعدی آن عدد زیر است

$$۴۹۶=۱+۲+۴+۸+۱۶+۳۱+۶۲+۱۲۴+۲۴۸.$$

اغلب وقتی ریاضیدان یك یا چند جواب خاص مساله‌ای را دارد با آنها ورمی‌رود تا شاید بتواند نظم و ترتیبی به‌دست آورد که رهگشای جواب عمومی باشد. در این مسألهٔ خاص، عددهای تام بالارا می‌توانیم به‌صورتهای زیر بنویسیم.

$$۶=۲.۳=۲.(۲^۲-۱)$$

$$۲۸=۲^۲.۷=۲^۲.(۲^۳-۱)$$

$$۴۹۶=۲^۴.۳۱=۲^۴(۲^۵-۱).$$

نوشتن این اعداد به‌صورت بالا مارا بر آن می‌دارد که حدس بزنیم:
عدد تام است اگر به‌صورت

$$P=۲^{p-۱}(۲^p-۱)=۲^{p-۱}q \qquad (۱.۴.۳)$$

باشد، که در آن

$$q=۲^p-۱$$

یك عدد اول مرسن است.
یونانیها به‌این نتیجه رسیده بودند و اثبات آن مشکل نیست. مقسوم‌علیه‌های P راکه شامل خود P هم هست، در زیر آورده‌ایم:

$$۱, ۲, ۲^۲, \ldots, ۲^{p-۱}$$

$$q, ۲q, ۲^۲q, \ldots, ۲^{p-۱}q.$$

مجموع این مقسوم‌علیه‌ها برابر است با

$$۱+۲+\dots+۲^{p-۱}+q(۱+۲+\dots+۲^{p-۱})$$

یا

$$(۱+۲+\dots+۲^{p-۱})(q+۱)=(۱+۲+\dots+۲^{p-۱})۲^{p}.$$

عبارت

$$S=۱+۲+\dots+۲^{p-۱}$$

مجموع جمله‌های یك تصاعد هندسی است. اگر فرمول این مجموع را به‌خاطر ندارید، S را از دو برابر آن

$$۲S=۲+۲^{۲}+\dots+۲^{p-۱}+۲^{p}$$

کم کنید،

$$S=۲^{p}-۱=q$$

به‌دست می‌آید. پس مجموع تمام مقسوم‌علیه‌های P برابر است با

$$۲^{p}q=۲.۲^{p-۱}q,$$

و مجموع تمام مقسوم‌علیه‌های P، به‌جز P برابر است با

$$۲.۲^{p-۱}q-۲^{p-۱}q=۲^{p-۱}q=P,$$

پس P عدد تام است.

این نتیجه نشان می‌دهد که هرعدد اول مرسن یك عدد تام به‌وجود می‌آورد. در بخش ۲.۲ گفتیم که تا به‌حال ۲۳ عدد اول مرسن شناسایی شده‌اند، پس ۲۳ عدد تام می‌شناسیم. آیا عددی تام از نوعی دیگر وجود دارد؟ تمام اعداد تام از نوع (۱.۴.۳) زوج هستند و می‌توان ثابت کرد که اگر عددی تام زوج باشد به‌صورت (۱.۴.۳) است. این سؤال باقی می‌ماند: آیا عدد تام فرد وجود دارد؟ درحال‌حاضر عدد تامی که فرد باشد نمی‌شناسیم و تعیین اینکه آیا عدد تام فرد وجود دارد یکی از معماهای حل‌نشدهٔ نظریهٔ اعداد است. گیرآوردن عدد تام فرد موفقیت بسیار بزرگی خواهد بود و ممکن است وسوسه شوید که اعداد فرد زیادی را آزمایش کنید. شما را از این‌کار برحذر می‌داریم؛ اخیراً (۱۹۶۸) بریانت تاکرمن[1] از آی بی ام اعلام داشته است که عدد تام فرد باید اقلا ۳۶ رقم داشته باشد.

---

1. Bryant Tuckerman

مجموعه مسائل ۴۰۳

۱. به‌کمك فهرست اعداد اول مرسن، چهارمین و پنجمین عدد تام را حساب کنید.

۵.۳ عددهای متحابه

میراث دیگرعددشناسی یونانیان، اعداد متحابه‌است. وقتی مقادیر عددی اسمهای دو نفر به‌قسمی‌بودند که مجموع مقسوم‌علیه‌های هریك‌ازاین دوعدد با عدد دیگر برابر بود، این‌را علامت اینکه بین آن دو نفر صمیمیت برقرار است، می‌دانستند. درواقع یونانیها تنها یك‌جفت ازاین اعداد را می‌شناختند:

$$۲۲۰ = ۲^۲ \cdot ۵ \cdot ۱۱, \quad ۲۸۴ = ۲^۲ \cdot ۷۱$$

مجموع مقسوم‌علیه‌های این دوعدد به‌ترتیب برابرند با

$$۱+۲+۴+۵+۱۰+۲۰+۱۱+۲۲+۴۴+۵۵+۱۱۰ = ۲۸۴,$$

$$۱+۲+۴+۷۱+۱۴۲ = ۲۲۰.$$

فرما با پیداکردن جفت

$$۱۷۲۹۶ = ۲^۴ \cdot ۲۳ \cdot ۴۷, \quad ۱۸۴۱۶ = ۲^۴ \cdot ۱۱۵۱,$$

نظریهٔ اعداد متحابه را از اینکه برپایهٔ یك مثال بناشده باشد، نجات داد.

کامپیوترها برای جستجوی جفتهای متحابه خیلی مناسب هستند. برای هرعدد n، ازماشین می‌خواهند تمام مقسوم‌علیه‌های $(\neq n)$ و m، مجموع این مقسوم‌علیه‌ها را حساب کند. سپس در مرحلهٔ دوم همین عمل روی m انجام می‌شود. اگر با این عمل عدد n به‌دست آید، یك‌جفت متحابهٔ (m, n) کشف شده است. اخیراً باکامپیوتر آی‌بی‌ام ۷۰۹۴، دانشگاه‌ییل[1] برای‌تمام عددهای‌زیر یك‌میلیون‌این‌کار را کرده‌است و ۴۲ جفت‌متحابه به‌دست‌آورده‌که بعضی‌ازآنهاعددهای متحابهٔ جدیدهستند. جفتهای متحابهٔ زیر ۱۰۰,۰۰۰ را درجدول۲ آورده‌ایم. در روش بالاعددهای‌تام هم به‌دست می‌آیند. ادامهٔ عمل برای‌اعداد بالای یك‌میلیون، البته‌باصرف وقت بیشترکامپیوترامکان دارد.

درواقع چیز زیادی دربارهٔ ویژگیهای‌اعداد متحابه نمی‌دانیم اما براساس

1. Yale

جدول ۲. اعداد متحابه تا ۱۰۰,۰۰۰

$۲۸۴ = ۲^۲.۷۱$	$۲۲۰ = ۲^۲.۵.۱۱$
$۱۲۱۰ = ۲.۵.۱۱^۲$	$۱۱۸۴ = ۲^۵.۳۷$
$۲۹۲۴ = ۲^۲.۱۷.۴۳$	$۲۶۲۰ = ۲^۲.۵.۱۳۱$
$۵۵۶۴ = ۲^۲.۱۳.۱۰۷$	$۵۰۲۰ = ۲^۲.۵.۲۵۱$
$۶۳۶۸ = ۲^۵.۱۹۹$	$۶۲۳۲ = ۲^۳.۱۹.۴۱$
$۱۰۸۵۶ = ۲^۳.۲۳.۵۹$	$۱۰۷۴۴ = ۲^۳.۱۷.۷۹$
$۱۴۵۹۵ = ۳.۵.۷.۱۳۹$	$۱۲۲۸۵ = ۳^۳.۵.۷.۱۳$
$۱۸۴۱۶ = ۲^۴.۱۱۵۱$	$۱۷۲۹۶ = ۲^۳.۲۳.۴۷$
$۷۶۰۸۴ = ۲^۲.۲۳.۸۲۷$	$۶۳۰۲۰ = ۲^۲.۵.۲۳.۱۳۷$
$۶۶۹۹۲ = ۲^۴.۵۳.۷۹$	$۶۶۹۲۸ = ۲^۴.۴۷.۸۹$
$۷۱۱۴۵ = ۳^۳.۵.۱۷.۳۱$	$۶۷۰۹۵ = ۳^۳.۵.۷.۷۱$
$۸۷۶۳۳ = ۳^۲.۷.۱۳.۱۰۷$	$۶۹۶۱۵ = ۳^۲.۵.۷.۱۳.۱۷$
$۸۸۷۳۰ = ۲.۵.۱۹.۴۶۷$	$۷۹۷۵۰ = ۲.۵^۳.۱۱.۲۹$

جدولمان حدسهایی می‌توان زد. مثلا، به‌نظر می‌رسد که هرچه اعداد متحابه بزرگتر می‌شوند، خارج قسمت آنها به‌یك نزدیکتر می‌شود. در جدول می‌بینیم که هرجفت متحابه یا دوعدد زوج است یا دوعدد فرد، اما حالتی کـه یکی زوج و دیگری فرد باشد دیده نشده است. دربارهٔ این‌نوع متحابه‌ها جستجو را تا اعدادی خیلی بزرگ ادامه داده‌اند اما برای

$$n \leqslant ۳۰۰۰\ ۰۰۰\ ۰۰۰$$

دو عدد متحابهٔ از این نوع پیدا نشده است.

فصل ٤

بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک

۱.۴ بزرگترین مقسوم‌علیه مشترک

امیدواریم تشخیص دهید که بیشتر این فصل زاید است، و این‌را صادقانه می گوییم. مطالب آن به‌مفاهیمی مربوط می‌شوند که باید در دبستان از زمان آموختن حساب کسرها با آنها آشنا شده باشید. درواقع ایـن فصل را بـرای یادآوری و عرضهٔ مطالب، شاید به‌صورتی اصولیتر ازآنچه آموخته‌اید، دراینجا می‌آوریم.

کسر a/b، خارج قسمت دو عدد صحیح a و b را درنظر می گیریم. معمولا کسر را ساده می کنیم، یعنی عاملهای مشترک a و b را حذف می کنیم. این‌عمل مقدار کسر را تغییر نمی‌دهد؛ مثلا

$$\frac{۲۴}{۳۶}=\frac{۸}{۱۲}=\frac{۲}{۳}.$$

عدد صحیح d مقسوم‌علیه مشترک دوعدد صحیح a و b است، اگر هم عامل a باشد، هم عامل b؛ یعنی اگر

$$a=d.a_۱, \quad b=d.b_۱.$$

اگر d مقسوم‌علیه مشترک a و b باشد، مقسوم‌علیه $a+b$ و $a-b$ نیز هست، زیرا

$$a+b=a_1d+b_1d=(a_1+b_1)d,$$
$$a-b=a_1d-b_1d=(a_1-b_1)d.$$

اگر a و b به‌عاملهای اول تجزیه‌شده باشند، به‌دست آوردن تمام مقسوم‌علیه‌های مشترک a و b مشکل نیست. تجزیه‌های به‌عاملهای اول a و b را به‌صورتی که گویی عاملهای a و b یکی هستند، می‌نویسیم:

$$a=p_1^{\alpha_1}\dots p_r^{\alpha_r},\quad b=p_1^{\beta_1}\dots p_r^{\beta_r},\qquad (۱.۱.۴)$$

با این قرارداد که امکان دارد بعضی از نماها ۰ باشند. مثلا اگر p_1، مقسوم‌علیه a باشد ولی مقسوم‌علیه b نباشد، در (۱.۱.۴)، $\beta_1=0$. بنابراین اگر

$$a=۱۴۰,\quad b=۱۱۰,\qquad (۲.۱.۴)$$

می‌نویسیم

$$a=۲^۲.۵^۱.۷^۱.۱۱^۰\quad b=۲^۱.۵^۱.۷^۰.۱۱^۱.\qquad (۳.۱.۴)$$

عاملهای اول یك مقسوم‌علیه a مانند d، فقط می‌توانند از اعداد اول p_i در (۱.۱.۴) باشند و δ_i نمای p_i در d از α_i در a بزرگتر نیست. شرایطی مشابه برای هر مقسوم‌علیه b مانند d وجود دارند. بنابراین اگر d یك مقسوم‌علیه مشترک a و b باشد، هرعامل اول d فقط یکی از p_iهایی است که هم در a است و هم در b؛ و δ_i نمای p_i در d از هیچیك از دونمای α_i و β_i بزرگتر نیست.

از این بحث نتیجه می‌گیریم که:

هردو عدد صحیح a و b یك بزرگترین مقسوم‌علیه مشترك d_0 دارند. عاملهای اول d_0، p_iهای مشترك در تجزیه‌های a و b هستند، و نمای p_i در d_0 عددکوچکتر دوعدد α_i و β_i است.

مثال. دو عددی راکه در (۲.۱.۴) داده‌ایم انتخاب کنید. از تجزیه‌های بـه عوامل اول (۳.۱.۴) دیده می‌شود که

$$d_0=۲^۱.۵^۱=۱۰.$$

چون نمای p_i در بزرگترین مقسوم‌علیه مشترك حداقل به‌بزرگی نمای p_i در

هرمقسوم‌علیه مشترك دیگر است، ویژگی مشخصهٔ زیر برقرار است:
هرمقسوم‌علیه مشترك، بزرگترین مقسوم‌علیه مشترك را می‌شمارد[1].
ب م م (بزرگترین‌مقسوم‌مشترك) دوعدد به‌قدری اهمیت دارد که با نمادخاص زیر مشخص می‌شود

$$d_0=(a, b). \qquad (۴.۱.۴)$$

مجموعهٔ مسائل ۱.۴

۱. ب م م جفتهای زیر را به‌دست آورید
(الف) ۳۶۰ و ۱۹۷۰
(ب) ۳۰ و ۳۶۵
(ج) شمارهٔ تلفن و شمارهٔ کد پستی خودتان

۲. چطور ثابت می‌کنید که $\sqrt{2}$ عددگنگ است؟ قضیهٔ یکتایی تجزیه به‌حاصلضرب اعداد اول دراین برهان و در برهانهای نظیر آن چگونه وارد می‌شود؟

۲.۴ عددهای متباین (نسبت به‌هم اول)

عدد ۱ مقسوم‌علیه مشترك هردوعدد a و b است. گاهی ۱ تنها مقسوم‌علیه مشترك a و b است، به‌طوری که

$$d_0=(a, b)=1. \qquad (۱.۲.۴)$$

دراین حالت می‌گوییم که a و b نسبت به‌هم اول‌اند، یا a و b متباین هستند.

مثال. $1=(39, 22)$.
اگر عددهایی مقسوم‌علیه‌مشترك بزرگتراز ۱ داشته باشند، مقسوم‌علیه مشترکی که اول باشد، نیز دارند. پس دوعدد تنها وقتی نسبت‌به‌هم اول‌اندکه هیچ‌عامل اول مشترك نداشته باشند. بنابراین شرط (۱.۲.۴) بدین‌معنی است که a و b هیچ عامل اول مشترك ندارند، یعنی تمام عاملهای اولشان متفاوت‌اند.
برگردیم به‌نقطهٔ شروع این فصل، تحویل کسر a/b به‌کوچکترین صورت و

---

۱. به‌عبارتی دیگر، هرمقسوم‌علیه مشترك، یك مقسوم‌علیه بزرگترین مقسوم‌علیه مشترك است.ـم.

مخرجش. اگر d_0 ب م م a و b باشد، می‌نویسیم

$$a=a_0d_0,\quad b=b_0d_0, \tag{۲.۲.۴}$$

آن‌گاه داریم

$$\frac{a}{b}=\frac{a_0d_0}{b_0d_0}=\frac{a_0}{b_0}. \tag{۳.۲.۴}$$

در(۲.۲.۴)، a_0 و b_0 عامل‌اول مشترک‌ندارند، زیرا درغیراین‌صورت عامل‌مشترکی بزرگتر از d_0 می‌داشتند. نتیجه می‌گیریم که

$$(a_0, b_0)=1, \tag{۴.۲.۴}$$

یعنی سمت راست (۳.۲.۴) ساده‌ترین صورت‌کسر است؛ عامل دیگری‌که بتوان از صورت و مخرج‌کسر حذف‌کرد، وجود ندارد.

از این ویژگی عددهای متباین‌که در زیر می‌آید اغلب استفاده می‌شود:

قاعدهٔ تقسیم. اگر حاصلضرب ab بر c تقسیمپذیر باشد و c و b متباین باشند، آن‌گاه a بر c تقسیمپذیر است.

برهان. چون c، ab را می‌شمارد، عاملهای‌اول c دربین عاملهای اول a و b هستند. اما چون $(b, c)=1$، دربین‌عاملهای اول b هیچ عامل‌اول c وجود ندارد. پس هرعامل اول c، a را می‌شمارد اما b را نمی‌شمارد، و توان آن در a کمتر از توانش در c نیست، زیرا c، ab را می‌شمارد.

ویژگی زیر را بعداً به‌کار خواهیم برد:

اگر حاصلضرب دو عدد متباین یك مربع باشد،

$$ab=c^2,\quad (a, b)=1, \tag{۵.۲.۴}$$

آن‌گاه a و b دو مربع هستند:

$$a=a_1^2,\quad b=b_1^2. \tag{۶.۲.۴}$$

برهان. برای اینکه عددی مربع باشد، لازم وکافی است‌که درتجزیهٔ عدد به عاملهای اول تمام نماها زوج‌باشند. چون a و b متباین‌هستند، در (۵.۲.۴) هرعامل اول c^2 یا در a است یا در b، اما هم در a وهم در b نیست؛ پس نماهای‌عاملهای

اول a و عاملهای اول b باید زوج باشند.

مجموعهٔ مسائل ۲.۴

۱. چه عددهایی نسبت به ۲ اول‌اند؟

۲. چرا دو عدد متوالی n و $n+1$ متباین‌اند؟

۳. جفتهای متحابهٔ جدول ۲ صفحهٔ ۳۹ را بررسی کنید و ببینید کدام‌جفت متباین‌است.

۴. آیا قاعده‌ای که در (۵.۲.۴) و (۶.۲.۴) برای توان ۲ بیان شده است، برای هر توانی صادق است؟

۳.۴ آلگوریتم اقلیدس

دوباره برمی‌گردیم به‌کسر a/b. اگر $a > b$، کسر عددی است بزرگتر از ۱، و اغلب آن‌را به‌مجموع یك عدد صحیح و یك کسر کوچکتر از ۱ تجزیه می‌کنیم.

چند مثال. می‌نویسیم

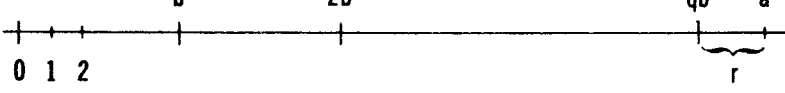
$$\frac{۳۲}{۵}=۶+\frac{۲}{۵}=۶\frac{۲}{۵}\;;\quad \frac{۶۳}{۷}=۹+\frac{۰}{۷}=۹\;.$$

برای این‌عمل درحالت کلی، تقسیم (ناقص) دوعدد $a \geqslant b$ را به‌کار می‌بریم:

می‌نویسیم

$$a=qb+r,\quad ۰\leqslant r\leqslant b-۱ \qquad \text{باشرط} \qquad (۱.۳.۴)$$

برای اینکه ببینیم همواره می‌توان a را به‌این صورت نوشت، عددهای صحیح ۰، ۱، ۲، ... را روی محور اعداد (شکل ۱.۳.۴) نمایش می‌دهیم. یکی از نقاط این‌محور نمایش عدد a است. عددهای ۰، b، $2b$، $3b$ تا qb را روی‌محور اعداد



شکل ۱.۳.۴

نشان می‌دهیم به قسمی که qb از a بزرگتر نباشد و $b(q+1)$ از a بزرگتر باشد. r فاصلهٔ qb از a است. r را باقیماندهٔ تقسیم (۱.۳.۴) و q را خارج قسمت (ناقص) می‌نامیم. چون خارج قسمت q زیاد درمتن می‌آید نماد خاصی داردکه در زیر می‌آوریم:

$$q=\left[\frac{a}{b}\right];$$

این نماد، بزرگترین عدد صحیح در a/b را نشان می‌دهد. در مثالهای بالا داریم

$$\left[\frac{۳۲}{۵}\right]=۶, \quad \left[\frac{۶۳}{۷}\right]=۹۰$$

در بخش پیش بزرگترین مقسوم‌علیه مشترک دوعدد صحیح a و b

$$d_۰=(a, b) \qquad (۲.۳.۴)$$

را بررسی کردیم. برای پیداکردن $d_۰$ فرض کردیم که تجزیه به‌عاملهای اول a و b را می‌دانیم. اگر اعداد بزرگ باشند تجزیه به‌عاملهای اول آنها کاری بس بزرگ است. روشی مهم وکاملا متفاوت برای پیداکردن ب م م وجود داردکه ارتباطی با تجزیه به‌عاملهای اول ندارد. این روش برپایهٔ حکم زیر استوار است:

اگر $a=bq+r$ و $۰\leqslant r\leqslant b-۱$، آن‌گاه

$$(a, b)=d_۰=(r, b). \qquad (۳.۳.۴)$$

برهان. اگر

$$d_۰=(a, b), \quad d_۱=(r, b)$$

باید نشان دهیم که $d_۰=d_۱$. هرمقسوم‌علیه مشترک a و b، مقسوم‌علیه

$$r=a-qb$$

نیز هست؛ در نتیجه $d_۰$ یك مقسوم علیه مشترك r و b است، پس $d_۰$، $d_۱=(b, r)$ را می‌شمارد، بنابراین $d_۱\geqslant d_۰$. از طرف دیگر از (۱.۳.۴) نتیجه می‌شود که هر مقسوم‌علیه‌مشترك r و b، a را می‌شمارد، پس $d_۱$، a را می‌شمارد. چون $d_۱$ مقسوم‌علیه b هم‌هست، $d_۰=(a, b)$ را می‌شمارد، پس $d_۱\geqslant d_۰$. نتیجه‌می‌شود که $d_۰=d_۱$.

مثال. $(۱۰۶۶, ۲۰۰) = (۲۰۰, ۶۶)$؛ پس $۱۰۶۶ = ۵ \cdot ۲۰۰ + ۶۶$.

از قاعده‌ای که بنا (۳.۳.۴) بیان می‌شود، راه ساده‌ای برای محاسبهٔ ب م م دو عدد a و b به دست می‌آید. به‌جای محاسبهٔ ب م م a و b کافی است ب م م r و b را حساب کنیم. این محاسبه ساده‌تر است زیرا r هم از a کوچکتر است هم از b. برای پیداکردن ب م م r و b همین روش را به‌کار می‌بریم و b را بر r تقسیم می‌کنیم:

$$b = q_۱ r + r_۱,$$

که در آن $r_۱$ از هردوعدد b و r کوچکتر است. برطبق قاعدهٔ (۳.۳.۴) به‌دست می‌آید

$$d_۰ = (a, b) = (b, r) = (r, r_۱).$$

اکنون این عمل را با r و $r_۱$ و بعد با ... ادامه می‌دهیم:

$$d_۰ = (a, b) = (b, r) = (r, r_۱) = (r_۱, r_۲) = \dots. \qquad (۴.۳.۴)$$

چون باقیمانده‌ها دائماً کوچك می‌شوند، دنبالهٔ باقیمانده‌ها به باقیماندهٔ $r_{k+۱} = ۰$ ختم می‌شود. باقیماندهٔ ۰ در تقسیم

$$r_{k-۱} = q_{k+۱} r_k + ۰,$$

ظاهر می‌شود، پس r_k، $r_{k-۱}$ را می‌شمارد. بنابراین

$$(r_{k-۱}, r_k) = r_k,$$

و از (۴.۳.۴) دیده می‌شود که

$$d_۰ = (a, b) = r_k.$$

به‌عبارت‌دیگر، $d_۰$ برابر است با اولین باقیمانده r_k که باقیماندهٔ قبلی‌را می‌شمارد.

مثال. ب م م دوعدد ۱۹۷۰ و ۱۰۶۶ را حساب می‌کنیم. از تقسیم عدد بزرگتر بر عدد کوچکتر و ادامهٔ عمل تقسیم مانند بالا، به‌دست می‌آید:

$$۱۹۷۰ = ۱ \cdot ۱۰۶۶ + ۹۰۴$$

$$۱۰۶۶ = ۱ \cdot ۹۰۴ + ۱۶۲$$

$$۹۰۴ = ۵ \cdot ۱۶۲ + ۹۴$$

$$۱۶۲ = ۱.۹۴ + ۶۸$$

$$۹۴ = ۱.۶۸ + ۲۶$$

$$۶۸ = ۲.۲۶ + ۱۶$$

$$۲۶ = ۱.۱۶ + ۱۰$$

$$۱۶ = ۱.۱۰ + ۶$$

$$۱۰ = ۱.۶ + ۴$$

$$۶ = ۱.۴ + ۲$$

$$۴ = ۲.۲ + ۰$$

درنتیجه ۲ = (۱۹۷۰, ۱۰۶۶).

این‌روش پیداکردن ب م م دوعدد را آلگوریتم‌اقلیدس می‌نامند، زیرا برای اولین‌بار درکتاب اصول اقلیدس[1] آمده است. این روش برای‌محاسبه با ماشینهای محاسبه خیلی مناسب است.

مجموعهٔ مسائل ۳.۴

۱. مسالهٔ‌های بخش ۱.۴ (صفحهٔ ۲۲) را از راه آلگوریتم اقلیدس حل‌کنید.

۲. ب م م هر یك‌از نخستین‌چهارجفت‌عدد متحابه‌را پیداکنید. نتیجه‌هارا با نتیجه‌هایی که از تجزیهٔ عاملهای اول به‌دست می‌آید مقایسه‌کنید.

۳. تعداد صفرهای سمت راست عدد $n! = ۱.۲.۳...n$ را پیدا کنید. درستی نتیجه را از روی جدول فاکتوریلها بررسی‌کنید.

۴.۴ کوچکترین مضرب مشترك

برگردیم به‌کسرها. برای جمع (یا تفریق) دوکسر

$$\frac{c}{a}, \quad \frac{d}{b},$$

1. Euclid's *Elements*

اول مخرج مشترك می‌گیریم، یعنی مخرج دوکسر را یکی می‌کنیم، و بعد صورتهارا باهم جمع (یا از یکدیگر کم) می‌کنیم.

مثال.

$$\frac{۲}{۱۵}+\frac{۵}{۹}=\frac{۶}{۴۵}+\frac{۲۵}{۴۵}=\frac{۳۱}{۴۵}.$$

درحالت کلی برای به‌دست آوردن مجموع

$$\frac{c}{a}+\frac{d}{b}$$

باید یك مضرب مشترك a و b را پیدا کنیم؛ یعنی عددی مانند m پیدا کنیم که هم بر a قابل‌قسمت باشد هم بر b. واضح است که $m=ab$ یکی از این عددهاست؛ پس مجموع دوکسر برابر است با

$$\frac{c}{a}+\frac{d}{b}=\frac{cb}{ab}+\frac{da}{ab}=\frac{cb+da}{ab}.$$

اما بینهایت مضرب مشترك دیگر a و b وجود دارند. فرض کنید تجزیه به عاملهای اول دوعدد a و b را داریم:

$$a=p_۱^{\alpha_۱}\cdots p_r^{\alpha_r},\quad b=p_۱^{\beta_۱}\cdots p_r^{\beta_r}. \qquad (۱.۴.۴)$$

m وقتی بر a و b تقسیمپذیر است که برهرعدد اول p_i به‌توان μ_i، که ازبزرگترین α_i و β_i کوچکتر نیست، تقسیمپذیر باشد. پس دربین مضربهای مشترك یکی هست که از m های دیگرکوچکتر است، و آن

$$m_۰=p_۱^{\mu_۱}\cdots p_r^{\mu_r}, \qquad (۲.۴.۴)$$

است و μ_i برابر است با بزرگتر α_i و β_i. پس $m_۰$ کوچکترین مضرب مشترك (ك م م) a و b است، و هرمضرب مشترك دیگر a و b بر $m_۰$ تقسیمپذیر است. نماد خاص ك م م در زیر آمده است:

$$m_۰=[a,\ b]. \qquad (۳.۴.۴)$$

مثال.

$$a=۱۴۰, \quad b=۱۱۰.$$

تجزیه بـه عـاملهای اول دو عـدد a و b را می‌نـویسیم: $a=۲^۲.۵^۱.۷^۱.۱۱^۰$، $b=۲^۱.۵^۱.۷^۰.۱۱^۱$؛ پس

$$[a, b]=۲^۲.۵^۱.۷^۱.۱۱^۱=۱۵۴۰.$$

رابطهٔ ساده‌ای بین ب م م و ک م م وجود دارد:

$$ab=(a, b).[a, b] \qquad (۴.۴.۴)$$

برهان. از ضرب دو عدد (۱.۴.۴)

$$ab=p_۱^{\alpha_۱+\beta_۱}\dots p_r^{\alpha_r+\beta_r} \qquad (۵.۴.۴)$$

به دست می‌آید. قبلا توجه کردیم که p_i در (a, b) عـدد کوچکتر α_i و β_i و در $[a, b]$ عدد بزرگتر α_i و β_i است. مثلا فرض کنید $\alpha_i\leqslant\beta_i$. آن‌گاه نمای p_i در (a, b)، α_i ودر $[a, b]$، β_i است؛ بنابراین درحاصلضرب

$$(a, b).[a, b]$$

نمای p_i، $\alpha_i+\beta_i$، همان‌نمای p_i درحاصلضرب (۵.۴.۴) است. ازاین دیده‌می‌شود که (۴.۴.۴) برقرار است.

مثال.

$$a=۱۴۰, b=۱۱۰, (a, b)=۱۰, [a, b]=۱۵۴۰;$$

$$ab=۱۴۰.۱۱۰=۱۰.۱۵۴۰=(a, b).[a, b].$$

ازقاعدهٔ (۴.۴.۴) می‌بینیم که اگـر a و b متباین باشند، آن‌گاه حاصلضربشان با کوچکترین مضرب مشترکشان برابر است، زیرا دراین‌حالت $(a, b)=۱$، پس

$$ab=[a, b].$$

مجموعهٔ مسائل ۴.۴

۱. ک م م جفتهای اعداد مسألهٔ ۱ ازمجموعهٔ مسائل ۱.۴ (صفحهٔ ۴۲) را پیداکنید.

۲. ک م م هرجفت از نخستین چهارجفت عددهای متحابه را پیداکنید.

فصل ۵

مسألهٔ فیثاغورسی

۱.۵ مقدمات

درمقدمهٔ (بخش ۳.۱) به‌یکی‌از قدیمیترین‌مسأله‌های نظریهٔ اعداد اشاره‌کردیم: یافتن تمام‌مثلثهای قائم‌الزاویه بااضلاع‌صحیح، یعنی، پیداکردن تمام‌جوابهای‌صحیح‌معادلهٔ

$$x^2+y^2=z^2. \qquad (۱.۱.۵)$$

این‌مسأله‌را می‌توان به‌کمك خواص سادهٔ اعداد حل‌کرد، اما قبل‌ازآن، توجه شمارا به‌چندنکتهٔ مقدماتی جلب می‌کنیم. مجموعهٔ سه عدد صحیح

$$(x,\ y,\ z) \qquad (۲.۱.۵)$$

که در (۱.۱.۵) صدق‌کند سه‌تایی فیثاغورسی نامیده‌می‌شود. حالت بی‌حاصلی‌راکه یکی‌از ضلعهای مثلث صفر است، کنار می‌گذاریم.

واضح است‌که اگر سه‌تایی (۲.۱.۵) فیثاغورسی باشد، هرسه‌تایی

$$(kx,\ ky,\ kz) \qquad (۳.۱.۵)$$

که ازضرب هریك ازاعداد درعدد صحیح k به‌دست می‌آید، نیز فیثاغورسی است، وبرعکس. پس‌درجستجوی‌جوابها کافی‌است مثلثهای اولیه را پیداکنیم‌که اضلاعشان برخلاف (۳.۱.۵) عامل‌مشترکی مانند $k>1$ ندارند. مثلا

$$(۶, ۸, ۱۰), \quad (۱۵, ۲۰, ۲۵)$$

سه‌تاییهای فیثاغورسی هستندکه ازجواب اولیهٔ $(۵, ۴, ۳)$ نتیجه می‌شوند.

در سه‌تایی اولیهٔ (x, y, z)، عددی‌که مقسوم‌علیه هرسه عدد x، y، z باشد، وجود ندارد. درواقع می‌توانیم این حکم قویتر را بیان‌کنیم: در یك سه‌تایی اولیه هیچ دوعدد آن مقسوم‌علیه مشترك ندارند، یعنی،

$$(x, y)=۱, (x, z)=۱, (y, z)=۱۰ \qquad (۴.۱.۵)$$

برای اثبات فرض می‌کنیم مثلا x و y مقسوم‌علیه مشترك دارند. دراین‌صورت x و y یك مقسوم‌علیه‌اول p دارند. از (۱.۱.۵) نتیجه می‌شودکه p، z رانیز می‌شمارد، پس (x, y, z) سه‌تایی اولیه نیست. همین استدلال برای دوشرط دیگر (۴.۱.۵) به‌کار می‌رود.

از آنچه گفتیم نتیجه می‌شودکه x، y هردو زوج نیستند؛ می‌توانیم نشان‌دهیم x و y هردو فرد هم نیستند. فرض‌کنیدکه

$$x=۲a+۱, \quad y=۲b+۱۰$$

مجموع مربعهای دوعدد را حساب می‌کنیم

$$\begin{aligned} x^۲+y^۲ &=(۲a+۱)^۲+(۲b+۱)^۲ \\ &=۲+۴a+۴a^۲+۴b+۴b^۲ \\ &=۲+۴(a+a^۲+b+b^۲). \end{aligned}$$

این عدد بر ۲ تقسیمپذیر است اما بر ۴ نیست. پس باتوجه به (۱.۱.۵) $z^۲$ بر ۲ تقسیمپذیر است ولی بر ۴ نیست. اما این امکان‌ندارد، زیرا اگر $z^۲$ بر ۲ تقسیمپذیر باشد، آن‌گاه z بر ۲ تقسیمپذیر است و درنتیجه $z^۲$ بر ۴ تقسیمپذیر می‌شود.

بنابراین از x و y یکی زوج‌ودیگری فرداست، z نیز فرد است. دراین‌فصل فرض می‌کنیم‌که x زوج و y فرد است.

۲.۵ جوابهای معادلهٔ فیثاغورسی

برای پیداکردن جوابهای اولیهٔ معادلهٔ فیثاغورسی (۱.۱.۵)، آن‌را به‌صورت

$$x^۲=z^۲-y^۲=(z-y)(z+y) \qquad (۱.۲.۵)$$

می‌نویسیم. یادآوری می‌کنیم که x زوج و y و z فرد هستند، پس هرسه عدد

$$x, \quad z+y, \quad z-y$$

زوج‌اند. پس‌می‌توانیم‌دوطرف (۱.۲.۵) را بر ۴ تقسیم کنیم ومعادلهٔزیررا به‌دست آوریم.

$$\left(\frac{۱}{۲}x\right)^۲ = \frac{۱}{۲}(z+y).\frac{۱}{۲}(z-y). \qquad (۲.۲.۵)$$

اگر بنویسیم

$$m_۱ = \frac{۱}{۲}(z+y), \quad n_۱ = \frac{۱}{۲}(z-y) \qquad (۳.۲.۵)$$

(۲.۲.۵) به‌صورت زیر درمی‌آید

$$\left(\frac{۱}{۲}x\right)^۲ = m_۱n_۱. \qquad (۴.۲.۵)$$

اعداد $m_۱$ و $n_۱$ در (۳.۲.۵) متباین هستند. برای اثبات، فرض‌کنید

$$d = (m_۱, n_۱)$$

ب م م $m_۱$ و $n_۱$ است. همان‌طورکه در بخش ۱.۴ گفتیم، d دوعدد صحیح

$$m_۱+n_۱ = z, \quad m_۱-n_۱ = y.$$

را می‌شمارد. اما در سه‌تایی اولیه، ۱ تنها مقسوم‌علیه مشترك z و y است، پس

$$d = (m_۱, n_۱) = ۱. \qquad (۵.۲.۵)$$

چون در(۴.۲.۵)حاصلضرب‌این دوعدد متباین، یك‌مربع است،نتیجه‌ای‌راکه در آخر بخش ۲.۴ (صفحهٔ ۴۳) به‌دست آوردیم بـه‌کار برده می‌گوییم $m_۱$ و $n_۱$ مربع هستند:

$$m_۱ = m^۲, \quad n_۱ = n^۲, \quad (m, n) = ۱. \qquad (۶.۲.۵)$$

بدون ازدست‌دادن‌کلیت مسأله، فرض‌می‌کنیم $m > ۰$، $n > ۰$. حال درمعادله‌های (۳.۲.۵) و (۴.۲.۵) به‌جای $m_۱$ و $n_۱$ می‌نویسیم $m^۲$ و $n^۲$، به‌دست می‌آید

$$m^2=\frac{1}{2}z+\frac{1}{2}y,\quad n^2=\frac{1}{2}z-\frac{1}{2}y,\quad m^2n^2=\frac{1}{4}x^2,$$

یا

$$x=2mn,\quad y=m^2-n^2,\quad z=m^2+n^2. \qquad (۷.۲.۵)$$

می‌توانید تحقیق کنید که این سه‌عدد همیشه در رابطهٔ $x^2+y^2=z^2$ صدق می‌کنند.

مطلبی که باقی می‌ماند این است کـه مشخص شود کدام اعداد مثبت m و n واقعاً با مثلثهای اولیه متناظرند. ثابت می‌کنیم که سه‌شرط زیر برای m و n، لازم و کافی هستند.

$$(m, n)=1 \quad (۱)$$

$$m>n \quad (۲) \qquad (۸.۲.۵)$$

(۳) یکی‌از دوعدد m و n زوج و دیگری فرد باشد.

برهان. اول نشان می‌دهیم کـه اگر x، y، z سه‌تایی اولیه باشد، سرطهای (۸.۲.۵) برقرارند. در بالا نشان‌دادیم که شرط (۱) ازاینکه x، y، z عددهای‌مثبت متباین هستند نتیجه می‌شود. شرط (۲) از مثبت‌بودن x، y، z نتیجه می‌شود. بـرای اینکه ببینیم شرط (۳) لازم است، توجه می‌کنیم کـه اگر m و n هردو فرد باشند، برطبق (۷.۲.۵)، y و z هردو زوج‌اند واین برخلاف‌نتیجه‌ای‌است که درآخر بخش قبلی به‌دست آوردیم.

برعکس‌ازشرایط (۸.۲.۵) نتیجه‌می‌شودکه (۷.۲.۵) یك سه‌تایی اولیه‌است: شرط (۲) به‌ما اطمینان می‌دهدکه x، y و z مثبت‌اند. اگر دوعدد ازاین سه‌عدد یك عامل اول مشترك p داشته باشند، p عامل مشترك عددسوم نیز هست،زیرا این سه‌عدد در$z^2=y^2+x^2$ صدق می‌کنند. اگر p، x را بشمارد، برطبق (۷.۲.۵)، $2mn$ را می‌شمارد؛ p نمی‌تواند ۲ باشد، زیرا از شرط (۳) واز (۷.۲.۵) نتیجه می‌شودکه y و z فرد هستند. [پس عدد اول p یا m را می‌شمارد یا n را.] فـرض کنید عدد اول فرد $p\neq 2$، m را می‌شمارد. آن‌گاه از شرط (۱) وعبارتهای (۷.۲.۵) نتیجه می‌شودکه p عددهای y و z را نمی‌شمارد؛ همین‌استدلال برای حالتی‌که p، n را می‌شمارد، به‌کار می‌رود.

حال‌که شرطهای لازم و کافی (۸.۲.۵) را برای اینکه از m و n یـك مثلث

جدول ۳

n \ m	۲	۳	۴	۵	۶	۷
۱	۴، ۳، ۵		۸، ۱۵، ۱۷		۱۲، ۳۵، ۳۷	
۲		۱۲، ۵، ۱۳		۲۰، ۲۱، ۲۹		۲۸، ۴۵، ۵۳
۳			۲۴، ۷، ۲۵			
۴				۴۰، ۹، ۴۱		۵۶، ۳۳، ۶۵
۵					۶۰، ۱۱، ۶۱	
۶						۸۴، ۱۳، ۸۵

اولیه به‌دست می‌آید، یافته‌ایم، می‌توانیم تمام مثلثهای اولیه‌را از روی عبارتهای (۷.۲.۵) حساب کنیم. مثلا فرض کنید

$$m=۱۱, \quad n=۸.$$

شرطهای (۸.۲.۵) برقرارند، و به‌دست می‌آید

$$x=۱۷۶, \quad y=۵۷, \quad z=۱۸۵.$$

درجدول ۳ تمام مثلثهای اولیهٔ x، y، z را به‌ازای $m\leqslant ۷$ و $n\leqslant ۶$ آورده‌ایم.

مجموعه مسائل ۲.۵

۱. جدول را تا $m\leqslant ۱۰$ ادامه دهید.

۲. آیا امکان‌دارد از دومجموعهٔ متمایز مقادیر m، n که در (۸.۲.۵) صدق کنند، یك مثلث به‌دست آید؟

۳. تمام مثلثهای فیثاغورسی راکه وترشان از ۱۰۰ نابزرگتر هستند، به‌دست آورید.

۳.۵ مسأله‌های مربوط به‌مثلثهای فیثاغورسی

مسألهٔ پیداکردن تمام مثلثهای فیثاغورسی را حل‌کردیم. در ریاضیات، تقریباً همیشه حل یك مسأله موجب طرح مسائلی دیگر می‌شود. اغلب، مسائل جدید از مسأله‌های اولی به‌مراتب مشکلترند.

درمورد مثلثهای اولیه طبیعتاً این‌سؤال مطرح می‌شود: اگر یـك ضلع مثلث قائم‌الزاویه داده شده‌باشد، دوضلع دیگر چطور تعیین می‌شوند؟ اول فرض‌کنیدضلع y داده شده است. برطبق (۷.۲.۵)،

$$y=m^2-n^2=(m+n)(m-n) \qquad (۱.۳.۵)$$

کـه در آن m و n در شرطهای (۸.۲.۵) صدق می‌کنند. در (۱.۳.۵) دو عـامل $(m+n)$ و $(m-n)$ متباین‌اند. برای اثبات توجه‌کنیدکه دو عامل

$$a=m+n, \quad b=m-n \qquad (۲.۳.۵)$$

هردو فردهستند، زیرا یکی‌از m و n زوج ودیگری فرد است. اگر a و b یك‌عامل اول p داشتند، p دوعدد

$$a+b=m+n+(m-n)=2m$$

و

$$a-b=m+n-(m-n)=2n$$

رامی‌شمرد، پسp هر دوعدد m و nرا می‌شمرد*. اما این‌ممکن‌نیست‌زیرا $(m,n)=1$.

حال فرض‌کنید عدد فرد y به‌صورت حاصلضرب دوعامل a و b باشرایط

$$y=ab, \quad a>b, \quad (a,b)=1 \qquad (۳.۳.۵)$$

داده شده است. از (۲.۳.۵)

$$m=\frac{1}{2}(a+b) \quad n=\frac{1}{2}(a-b) \qquad (۴.۳.۵)$$

به دست می‌آیند. این اعداد نیز متباین هستند، زیرا هرعامل مشترك m و n، دو عدد

---

* زیرا a و b فردهستند و درنتیجه $p\neq 2$، پس $(p,2)=1$ وبنابرقاعدهٔ تقسیم، p دو عدد m و n را می‌شمارد. م.

$a=m+n$ و $b=m-n$ را می‌شمارد. به‌علاوه m و n هردوفرد نیستند. زیرا اگر فرد باشند، a و b زوج می‌شوند. نتیجه اینکه m و n در شرایط (۸.۲.۵) صدق می‌کنند و مثلثی اولیه به‌وجود می‌آورند که در آن $y=m^2-n^2$.

مثال. فرض کنید $y=۱۵$. در این مثال y به‌دوصورت به‌دوعامل متباین تجزیه می‌شود:

$$y=۱۵.۱=۵.۳.$$

از تجزیهٔ اولی

$$m=۸,\ n=۷,\ x=۱۱۲,\ y=۱۵,\ z=۱۱۳,$$

و از دومی

$$m=۴,\ n=۱,\ x=۸,\ y=۱۵,\ z=۱۷,$$

به‌دست می‌آیند.

اینک فرض کنید ضلع x داده شده‌است. چون m یا n زوج است، از $x=۲mn$ دیده می‌شود که x مضربی از ۴ است. $\frac{۱}{۲}x$ را به‌حاصلضرب دو عامل متباین تجزیه کرده، عامل بزرگتر را m و کوچکتر را n می‌نامیم.

مثال. فرض کنید $x=۲۴$. در این مثال $\frac{۱}{۲}x$ به‌دو صورت

$$\frac{۱}{۲}x=۱۲.۱=۴.۳$$

تجزیه می‌شود. از تجزیهٔ اول

$$m=۱۲,\ n=۱,\ x=۲۴,\ y=۱۴۳,\ z=۱۴۵,$$

و از تجزیهٔ دوم

$$m=۴,\ n=۳,\ x=۲۴,\ y=۷,\ z=۲۵,$$

به‌دست می‌آیند.

درحالت سوم، که آخرین حالت است، به‌یک مسألهٔ مهم نظریهٔ اعداد برمی‌خوریم. اگر z وتر یک مثلث فیثاغورسی اولیه باشد، آن‌گاه برطبق (۷.۲.۵)

$$z=m^۲+n^۲; \qquad (۵.۳.۵)$$

یعنی، z مجموع مربعهای دوعدد m و n است که درشرایط (۸.۲.۵) صدق می کنند.

این موجب می‌شود که مسأله‌ای را که فرما حل کرده است، مطرح کنیم: چه‌موقع می‌توان عددی را به‌صورت مجموع دو مربع

$$z=a^۲+b^۲, \qquad (۶.۳.۵)$$

نوشت؟ فعلاشرطی برای a و b نمی گذاریم، a و b می‌توانندعامل‌مشترك داشته‌باشند و یکی‌ازآنها یا هردو می‌تواند صفرباشد. دربین اعداد نابزرگتراز ۱۰،

$$۰=۰^۲+۰^۲,\ ۱=۱^۲+۰^۲,\ ۲=۱^۲+۱^۲,\ ۴=۲^۲+۰^۲,$$

$$۵=۲^۲+۱^۲,\ ۸=۲^۲+۲^۲,\ ۹=۳^۲+۰^۲,\ ۱۰=۳^۲+۱^۲,$$

مجموع دو مربع هستند. اعداد ۳، ۶ و ۷ را که باقی می‌مانند نمی‌تـوان به‌صورت مجموع دومربع نوشت.

حال شرح می‌دهیم که چگونه می‌توان تعیین کردکه عددی مجموع دو مربع هست، یا نیست. متاسفانه برهانها ساده نیستند وناچاریم از ذکرآنها خودداری کنیم.

نخست‌اعداد اول‌را درنظرمی‌گیریم. هرعدد اول p به‌صورت $p=۴n+۱$، مجموع دومربع است؛ مثلا

$$۵=۲^۲+۱^۲,\ ۱۳=۳^۲+۲^۲,\ ۱۷=۴^۲+۱^۲,\ ۲۹=۵^۲+۲^۲.$$

جالب است که تجزیهٔ این اعداد به‌مجموع دومربع یکتاست.

بقیهٔ اعداد اول فرد، به‌صورت $q=۴n+۳$ هستند؛ یعنی

$$q=۳,\ ۷,\ ۱۱,\ ۱۹,\ ۲۳,\ ۳۱,\ \ldots.$$

هیچیك ازاین‌اعداد مجموع دومربع نیستند؛ درواقع هیچ عدد به‌صورت $۴n+۳$، مجموع دومربع نیست. برای‌اثبات آن توجه‌کنیدکه اگر a و b هردو زوج باشند، $a^۲$ و $b^۲$ هر دو بر ۴ تقسیمپذیرند، پس $a^۲+b^۲$ بر ۴ تقسیمپذیر است. اگر a و b هردو فرد باشند، $a=۲k+۱$، $b=۲l+۱$، آن‌گاه

$$a^۲+b^۲=۴k^۲+۴k+۱+۴l^۲+۴l+۱$$

$$=۴(k^۲+l^۲+k+l)+۲.$$

پس باقیماندهٔ $a^۲+b^۲$ بر ۴، ۲ است. بالاخره اگر یکی فرد و دیگری زوج باشد، $a=۲k+۱$ و $b=۲l$، آن‌گاه باقیماندهٔ

$$a^۲+b^۲=۴k^۲+۴k+۴l^۲+۱$$

بر ۴، ۱ است. چون تمام حالتهای ممکن را بررسی کرده‌ایم، نتیجه می‌گیریم که مجموع دومربع هیچوقت به‌صورت $۴n+۳$ نیست.

برای تکمیل این بررسی اعداد اول، توجه می‌کنیم که $۱^۲+۱^۲=۲$.

برای اینکه ببینیم عدد مرکب z مجموع دومربع کامل هست یا نیست؛ تجزیه به‌عوامل اول z،

$$z=p_۱^{\alpha_۱}p_۲^{\alpha_۲}\dots \qquad (۷.۳.۵)$$

را درنظر می‌گیریم. آن‌گاه z مجموع دو مربع است اگر وفقط اگر هر p_i که به صورت $۴n+۳$ است، نمای زوج داشته باشد.

چند مثال.

$$z=۱۹۸=۲.۳^۲.۱۱$$

مجموع دومربع نیست، زیرا ۱۱ به‌صورت $۴n+۳$ است و نمای آن زوج نیست.

$$z=۱۹۴=۲.۹۷$$

مجموع دومربع است، زیرا هیچیك از عاملهای اول آن به‌صورت $۴n+۳$ نیست. به‌دست می‌آید که

$$۱۹۴=۱۳^۲+۵^۲.$$

برگردیم به‌مسألهٔ اصلی: تعیین تمام z هایی که می‌توانند وترهای مثلثهای فیثاغورسی‌اولیه باشند. این‌اعداد را باید بتوان به‌صورت $z=m^۲+n^۲$، که در آن m و n درشرایط (۸.۲.۵) صدق‌می‌کنند، نمایش داد. ثابت می‌کنند که یك‌شرط لازم وکافی این است که تمام عاملهای اول z به‌صورت $p=۴n+۱$ باشند، از ذکر این برهان نیز خودداری می‌کنیم.

چند مثال.

۱) $z=۴۱$.

در این مثال نمایش z به‌مجموع دومربع یکتاست،

$$z=۵^۲+۴^۲$$

پس $m=۵$، $n=۴$ و

$$x=۴۰, \quad y=۹, \quad z=۴۱$$

مثلث متناظر است.

۲) $z=۱۱۰۵=۵\cdot۱۳\cdot۱۷$

در این مثال z به‌چهار صورت به‌مجموع دومربع نمایش داده می‌شود:

$$۱۱۰۵=۳۳^۲+۴^۲=۳۲^۲+۹^۲=۳۱^۲+۱۲^۲=۲۴^۲+۲۳^۲.$$

پیداکردن مثلثهای متناظررا به‌عهدهٔ خواننده می‌گذاریم.

مسائلی متنوع مربوط به مثلثهای فیثاغورسی را می‌توان به کمك فرمولهای (۷.۲.۵)،

$$x=۲mn, \quad y=m^۲-n^۲, \quad z=m^۲+n^۲,$$

حل کرد. یکی‌از این‌مسائل پیداکردن مثلثهای فیثاغورسی بامساحت مفروض A است. اگر مثلث، اولیه باشد، مساحتش برابر است با

$$A=\frac{۱}{۲}xy=mn(m-n)(m+n). \qquad (۸.۳.۵)$$

سه عامل ازچهار عامل A فرد هستند. به‌آسانی دیده می‌شودکه این‌عاملها دو به دو متباین‌اند. پس برای‌تعیین مقادیر ممکن m و n، دوعامل فرد اول متباین A، مانند k و l، $k>l$ را انتخاب می‌کنیم و می‌نویسیم.

$$m+n=k, \quad m-n=l,$$

و نتیجه می‌گیریم

$$m=\frac{۱}{۲}(k+l), \quad n=\frac{۱}{۲}(k-l).$$

بعد بررسی می‌کنیم که این اعداد m و n در (۸.۳.۵) صدق می‌کنند یا نه.

اگر توجه شودکه تنها درحالت خاص

$$m=۲,\ n=۱,\ A=۶$$

دوعامل ازچهارعامل (۸.۳.۵) با ۱ برابر می‌شوند، بحث کمی ساده‌تر می‌شود،زیرا تنها در حالت

$$n=m-n=۱$$

دوعامل (۸.۳.۵) با ۱ برابر می‌شوند.

مثال. تمام‌مثلثهای فیثاغورسی راکه مساحتشان $A=۳۶۰$ است، پیداکنید. ازتجزیهٔ A به‌عاملهای اول،

$$A=۲^۳.۳^۲.۵,$$

دیده می‌شود که تنها راه نوشتن A به‌صورت چهارعامل متباین،

$$A=۸.۱.۵.۹$$

است،پس $m+n=۹$. اگر $m=۸$، آن‌گاه $n=۱$ و $m-n=۷$، A رانمی‌شمارد. امکان دیگر $n=۸$، $m=۱$ است که قابل قبول نیست، زیـرا m باید از n بزرگتر باشد. پس مثلث فیثاغورسی‌اولیه به‌مساحت $A=۳۶۰$ وجود ندارد.

اما بااینحال، امکان‌وجود مثلثهای‌غیراولیه به‌مساحت $A=۳۶۰$ منتفی‌نمی‌شود. استدلالی راکه در زیر می‌آید می‌توان بـرای مثلثهایی غیراولیه به‌مساحتی مشخص به‌کار برد. اگر

$$dx,\quad dy,\quad dz$$

اضلاع مثلثی با عامل مشترك d باشند، مساحت مثلث برابر است با

$$A=\frac{۱}{۲}dx\,dy=d^۲mn(m-n)(m+n).$$

پس $d^۲$ یك عامل A است و، اگر d ب م م اضلاع باشد،

$$A_۰=\frac{A}{d^۲}=mn(m-n)(m+n)$$

باید مساحت یك مثلث اولیه باشد.

حال این استدلال را درمثال بالاکه درآن $A=۳۶۰$ است به‌کارمی‌بریم. عدد ۳۶۰ سه‌عامل مربع دارد:

$$d_۱=۴,\quad d_۲=۹,\quad d_۳=۳۶.$$

مساحتهای مثلثهای اولیهٔ متناظر برابرند با:

$$\frac{A}{d_۱}=۹۰=۲.۳^۲.۵,\ \frac{A}{d_۲}=۴۰=۲^۳.۵,\ \frac{A}{d_۳}=۱۰=۲.۵.$$

۴۰ و ۱۰ را به‌هیچ‌طریقی نمی‌توان به‌حاصلضرب چهار عامل متباین تجزیه کرد، ۹۰ تنها به‌یك طریق

$$۹۰=۱.۲.۳^۲.۵$$

به‌چهارعامل متباین تجزیه می‌شود (جز درحالت $m=۲$، $n=۱$، $A=۶$، حداکثر یکی‌از چهارعامل امکان‌دارد ۱ باشد.) چون ۹ بزرگترین عامل است، $m+n=۹$. اما $m=۱, ۲, ۵$ تنها مقادیر ممکن m هستند. به‌ازای‌این‌مقادیر، برای n به‌ترتیب مقادیر $n=۸, ۷, ۴$ نتیجه می‌شوند. از شرط $m>n$ مقادیر $m=۱, ۲$ حذف می‌شوند و تنها $m=۵$، $n=۴$ می‌مانند. اما برای این مقدارها $mn(m+n)(m-n)\neq ۹۰$، پس نتیجه می‌گیریم که مثلث فیثاغورسی، اولیه یا غیراولیه‌که مساحتش $A=۳۶۰$ باشد، وجود ندارد.

مسائل زیاد دیگری می‌توان مطرح کرد، ما فقط به‌یکی از این مسائل اشاره می‌کنیم. محیط مثلث برابر است با

$$c=x+y+z. \qquad (۹.۳.۵)$$

اگر مثلث، فیثاغورسی‌اولیه باشد محیطش به‌صورت

$$c=۲mn+(m^۲-n^۲)+(m^۲+n^۲)=۲m(m+n)$$

درمی‌آید. به‌عهدهٔ خواننده می‌گذاریم که یك‌روش‌پیدا کردن تمام‌مثلثهای‌فیثاغورسی بامحیطی مفروض‌را توضیح دهد؛ روش‌را برای چندمثال عددی به‌کار برید.

مسألهٔ ساختن تمام مثلثهای فیثاغورسی را حل کردیم. حل این مسأله مارا به بررسی مسائلی‌کلیتر در این زمینه می‌کشاند. یك تعمیم طبیعی آن مثلثهای هرونی،

منسوب به‌هرون، ریاضیدان یونانی اسکندریه، است. فرض براین است که ضلعهای مثلثها عددهای صحیح هستند، اما این شرط که یکی از زاویه‌ها ۹۰° است، حذف شده، به‌جای آن فرض می‌شود که مساحت مثلث عدد صحیح است. واضح است که مثلثهای فیثاغورسی ازاین نوع‌اند.

برای بررسی اینکه مثلثی مفروض هرونی است یانه، ساده‌ترین راه به‌کاربردن فرمول هرونی مساحت مثلث، یعنی

$$A=\sqrt{\tfrac{1}{2}c\left(\tfrac{1}{2}c-x\right)\left(\tfrac{1}{2}c-y\right)\left(\tfrac{1}{2}c-z\right)}$$

است، که در آن c محیط مثلث، وقبلا بارابطهٔ (۹.۳.۵) تعریف شده‌است. گرچه تعداد قابل ملاحظه‌ای مثلث هرونی می‌شناسیم، بـرای پیداکردن تمام آنها فرمولی کلی نداریم. در اینجا چند مثال (که مثلث قائم‌الزاویه نیستند) می‌آوریم:

$x=۷$	$y=۱۵$	$z=۲۰$
۹	۱۰	۱۷
۱۳	۱۴	۱۵
۳۹	۴۱	۵۰

گذشتن ازمثلثهای فیثاغورسی را، بدون اشاره به‌یکی ازمشهورترین مسائل ریاضی: مسألهٔ حدس فـرما، جایز نمی‌شمریم: اگر n بزرگتر از ۲ باشد، سه عدد صحیح و مثبت x، y، z که در

$$x^n+y^n=z^n$$

صدق کنند، وجود ندارند. وقتی فرما ترجمه‌ای از اصل یونانی علم‌حساب دیوفانت[1] را مطالعه می‌کرد، به‌این فکر افتاد. این اثر عمدتاً به‌مسائلی می‌پردازد که در آنها از فرمولهای مثلثهای فیثاغورسی استفاده شده‌است، وفرما نظریاتش را در حاشیهٔ کتاب نوشته است.

فرما از «کشف» خود به‌هیجان آمده‌بود وفکر می‌کرد که برهانی عالی دارد،

1. Diophantos' *Arithmetica*

اما متاسفانه حاشیهٔ کتاب برای توضیح آن زیادی باریك بوده است. از آن زمان تا به‌حال ریاضیدانها درشگفت‌هستند. استادانه‌ترین روشها برای‌یافتن یك‌برهان به‌کار گرفته شده‌است؛ ازاین‌جستجوها نظریه‌های جدیداساسی در ریاضیات نتیجه‌شده‌اند. قضیهٔ فرما به‌وسیلهٔ ترکیبی از تئوری وکامپیوترها برای تعداد زیادی از نماهای n ثابت شده است. اکنون می‌دانیم که قضیهٔ فرما برای تمام nهای $3 \leqslant n \leqslant 4002$ راست است[1].

چون برجسته‌ترین ریاضیدانان در مدت چند قرن موفق نشده‌اند برهانی کلی برای‌قضیهٔ فرما بیابند، به‌نظر می‌رسد بیشتر براین‌عقیده باشندکه فرما باوجودمهارت مسلمش، باید یك‌لحظه مرتکب اشتباه شده‌باشد. اگرهم کتاب حاشیهٔ‌بهتری‌می‌داشت، احتمال نمی‌رود برهانی‌که فرما می‌آورد معتبر می‌بود.

شما البته حق دارید برای اثبات قضیه بکوشید؛ اما بدانید که برای هیچ قضیه‌ای در ریاضیات به‌این اندازه برهانهای غلط ارائه نشده‌است، چند تایی را ریاضیدانان‌خوب وتعداد بیشماری‌را افراد غیرعادی عرضه‌کرده‌اند. هنوزهم، مانند گذشته، در بین نامه‌هایی‌که برای‌متخصصین برجستهٔ نظریهٔ اعداد نوشته می‌شود، برهانهای «آخرین قضیهٔ فرما» به‌چشم می‌خورند؛ اغلب آنها با نامه‌های تقاضای شناسایی فوری صحت برهان و پرداخت نقدی جایزهٔ مالی همراه است، جایزه‌ای که روزی یك‌ریاضیدان آلمانی به‌عنوان پاداش برای شخصی که برهان درست آخرین قضیهٔ فرما را ارائه دهد، تعیین کرده است و امروز در اثر تورم بی‌ارزش شده است.

مجموعه مسائل ۳.۵

۱. تمام مثلثهای فیثاغورسی راکه یك‌ضلع آن ۵۰ است تعیین‌کنید؛ همین مسأله را وقتی ضلع مثلث به‌جای ۵۰، ۲۲ است حل‌کنید.

۲. از محك امکان نمایش یك عدد به‌صورت مجموع دومربع استفاده کرده، تعیین کنیدکدامیك از اعداد

$$100,\ 101,\ \ldots,\ 110$$

---

۱. در این زمینه تحقیقات ادامه دارد، درستی قضیهٔ فرما به ازای $3 \leqslant n \leqslant 125000$ مسجل شده است و نتایج مهم دیگری نیز به‌دست آمده است.ـم.

را می‌توان به‌این‌صورت نمایش‌داد؟ وقتی‌که ممکن‌است، تمام نمایشها را معین کنید. کدامیك از این اعداد می‌تواند وتر یك‌مثلث فیثاغورسی اولیه باشد؟

۳. آیا مثلثهایی فیثاغورسی با مساحت

$$A=۷۸, \quad A=۱۲۰, \quad A=۱۰۰۰$$

وجود دارند؟

۴. تمام مثلثهای فیثاغورسی با محیطهای $c=۸۸$ و $c=۱۱۰$ را پیدا کنید.

فصل ٦

دستگاههای شمارش

۱.۶ دستگاه دهدهی

فیثاغورسیان قدیم عقیده داشتندکه همه چیز عدد است؛ و حال آنکه در مقایسه با زندگانی روزانهٔ ما که به هرکجا نظر می‌افکنیم عدد است آنها گهگاه به عدد برمی‌خوردند. ما با اعداد بسیار بزرگ می‌شماریم وشمرده‌می‌شویم. با شماره‌های بیمه، کدهای پستی، شماره‌های حساب، شماره‌های تلفن، شماره‌های اطاق وشماره‌های منزل زندگانی می‌کنیم. هرروز باصورتحسابها،چکها،هزینه‌ها وموجودیها سروکار داریم. بودجه‌های اداری بدون‌شك سربه‌بیلیونها می‌زنند، وآمارهای کلان به‌عنوان‌صورتی از استدلال پذیرفته شده‌اند. این ارقام در کامپیوترها جریان دارند، کامپیوترهایی که با سرعت چندین عمل دریك بیلیونیم ثانیه اصول معاملات بزرگ را تجزیه وتحلیل می‌کنند، مسیرهای اقمار مصنوعی‌را دنبال می‌کنند، وبه‌بررسی درون هسته‌های‌اتمی مشغول‌اند.

تمام اینها ازنخستین‌کوششهای انسان درمنظم‌کردن اعدادش، وقتی تعدادآنها به‌جایی رسیده بودکه دیگر با انگشتانش به‌شمارش درنمی‌آمدند، در طول مسیری پیوسته گسترش یافت. روشهای متنوعی برای دسته‌بندی اعداد به‌کارمی‌رفتندکه بیشتر آنها، وقتی معلوم‌شد درمقایسه با دستگاههای دیگر ضعیف‌اند، متروك شدند. دستگاه

دهدهی کنونی، که بردسته‌بندیهای دهدهی پایه‌گذاری شده است، در حال حاضر، خوشبختانه، در دنیا کاملا پذیرفته شده است. ازچندین‌جهت به‌نظر می‌رسد که دستگاه دهدهی اتفاقاً برای کارهای ما با اعداد، راه میانهٔ مناسبی باشد.

شرح‌دادن دستگاه با ذکر جزئیات لزومی ندارد. پس‌از تمرینهای دوسال اول دبستان، تاعمرداریم تقریباً خودبه‌خود می‌دانیم مجموعه‌ای‌از ارقام چه‌معنی‌دارد، مثلا

$$۷۵ = ۷\cdot۱۰ + ۵,$$

$$۱۰۶۶ = ۱\cdot۱۰^{۳} + ۰\cdot۱۰^{۲} + ۶\cdot۱۰ + ۶,$$

$$۱۹۷۰ = ۱\cdot۱۰^{۳} + ۹\cdot۱۰^{۲} + ۷\cdot۱۰ + ۰$$

به‌طور کلی، در دستگاه دهدهی، دنبالهٔ

$$a_n a_{n-۱} \cdots a_۲ a_۱ a_۰ \qquad (۱.۱.۶)$$

عدد

$$N = a_n\cdot۱۰^{n} + a_{n-۱}\cdot۱۰^{n-۱} + \cdots + a_۲\cdot۱۰^{۲} + a_۱\cdot۱۰ + a_۰ \qquad (۲.۱.۶)$$

را مشخص می‌کند، و در آن ضرایب یا ارقام a_i یکی‌از مقادیر زیر هستند

$$a_i = ۰, ۱, \cdots, ۹۰ \qquad (۳.۱.۶)$$

عدد $b = ۱۰$ پایهٔ دستگاه نامیده می‌شود.

این‌دستگاه عددی هندی ـ عربی درحدود سال ۱۲۰۰ میلادی ازشرق به‌اروپا آمد و تابه‌حال بدون رقیب مانده است. دستگاه را موضعی می‌نامند، زیرا موضع هررقم مقدار آن‌را مشخص می‌کند؛ استعمال نماد ۰ برای نشان‌دادن موضع خالی، که نمادی بی‌گزند ولی استادانه است، این‌کار را ممکن ساخته‌است. علاوه‌براین معلوم شده است که نماد ۰ برای‌انجام اعمال‌حسابی: جمع، تفریق، ضرب و تقسیم، خیلی مفید است.

۲.۶ دستگاههای دیگر

دربارهٔ بسیاری‌از دستگاههایی‌که ملتهای مختلف‌دنیا برای سازمان‌دادن به‌اعدادشان به‌کار برده‌اند، اطلاعات‌زیادی وجود دارند. اما اینکه چرا و چطور این دستگاهها به‌وجود آمده‌اند نکاتی‌هستند که بیشتر آنها درگذشتهٔ غبارآلود نوع بشر محوشده‌اند.

شکی نیست که دسته‌بندیهای دهدهی که همه‌جا متداول است، به‌این‌علت است که انسانها با انگشتان خود حساب می‌کرده‌اند. تعجب‌آور است که آثار کمی از شمارش با یك دست وجود دارند؛ دستگاههای پنج‌پنجی به‌ندرت دیده می‌شوند. اما نمونه‌های دستگاههای بیست‌بیستی خیلی‌فراوان هستند، و به‌آسانی می‌توان دریافت که این دستگاهها از به‌کاربردن انگشتان‌پا و دست درفرایند شمارش به‌وجود آمده است. شایدحساب مایَن[1]ها معروفترین دستگاه بیست‌بیستی باشد، اما تاچندقرن‌پیش این دستگاه‌کاملا در اروپا شایع بود. شمارش بیست‌بیستی از ۸۰ تا ۱۰۰ در زبان فرانسه متداول است. مثلا فرانسویان ۸۰ را چهار ـ بیست[2]، نود را چهار-بیست-ده[3] و ۹۱ را چهار-بیست-یازده[4] و... می‌گویند.

شاید ندانید که شمارش بیست‌بیستی در دانمارك تا امروز معمول است. این دستگاه قدیمی که قبلا در بین ملل‌ژرمن بیشتر شایع‌بود، به‌قدری غریب وجالب‌توجه است که نمی‌توانیم از دادن مختصر شرحی دربارهٔ آن خودداری‌کنیم. وقتی بیست بیست می‌شماریم‌کاملا طبیعی است که اصطلاحهای سه‌بار بیست[5]، چهاربار بیست[6]، پنج‌بار بیست[7]، را به‌کار بریم. اما با این‌قاعده که هروقت‌تعدادکاملی بیست‌تایی‌شمردیم و ده تا اضافه آوردیم، بگوییم نصف بیست‌تای بعدی، دستگاه پیچیده می‌شود؛ مثلا ۹۰ = نصف ازپنجمین بیست[8]. برای تکمیل‌عدد، دانمارکیها اصل‌آوردن واحدها قبل‌از دهتاییها را به‌کار می‌برند، مانند

۹۳ = سه و نصف از پنجمین بیست[9].

روشن‌است که این‌نوع‌دستگاهها دریك تمدن پرازعدد، نظیر تمدن ما، محکوم به‌فناست. یکی‌از صورتهای بسیار زیان‌آور در بعضی از روشهای شمارش، آوردن واحدها قبل‌ازده‌تاییهاست. تاقرن هجدهم این‌امر درانگلستان متداول بود، می گفتند سه‌و بیست[10] به‌جای بیست‌وسه. چندسال‌قبل، پارلمان‌نروژ‌استفاده‌ازاین‌روش‌را قانوناً درمدارس و درخبرهای رسمی‌قدغن‌کرد. اما درآلمان هنوز این‌روش متداول است

---

1. Mayan (قومی درآمریکای مرکزی و مکزیك.ـم)
2. quatre - vingts
3. quatre - vingt - dix
4. quatre - vingt - onze
5. tredsindslyve
6. firsindslyve
7. femsindslyve
8. halvfemsindslyve
9. treoghalvfemsindslyve
10. three and twenty

و موجب اشتباههای زیاد، مثلا در گرفتن شمارهٔ تلفن، می‌شود.

دستگاه شصت‌شصتی بابلیها از زمان قدیم تا به‌حال مورد استفادهٔ منجمین بوده و هست، گرچه طرفدارانش رو به‌کاهش هستند. ما هنوز آن‌را درشمارش زاویه‌ها و زمان به‌دقیقه وثانیه به‌کار می‌بریم. نمی‌دانیم چرا بابلیها دستگاهی با پایه‌ای به‌این بزرگی انتخاب کرده‌اند. حدس می‌زنند که این دستگاه از ترکیب دودستگاه با پایه‌های متفاوت، مثلا ۱۰ و ۱۲ که کوچکترین مضرب مشترکشان ۶۰ است، به‌وجود آمده باشد.

وقت آن رسیده است کـه چند کلمه دربارهٔ مسائل ریاضی مربوط به‌کاربرد دستگاههای با پایه‌های گوناگون بگوییم. عدد صحیح N در پایهٔ b را به‌صورت

$$N=c_nb^n+c_{n-1}b^{n-1}+\cdots+c_2b^2+c_1b+c_0 \qquad (۱.۲.۶)$$

درست مانند (۲.۱.۶) می‌نویسیم، با این تفاوت که ضریبهای c_i در اینجا به‌جای مقادیر (۳.۱.۶) یکی از مقادیر زیر است،

$$c_i=0,\ 1,\ \cdots,\ b-1. \qquad (۲.۲.۶)$$

به‌خاطر اختصار، می‌توانیم عدد N در (۱.۲.۶) را به‌صورت خلاصهٔ

$$(c_n,\ c_{n-1},\ \cdots,\ c_2,\ c_1\ c_0)_b \qquad (۳.۲.۶)$$

که نظیر (۱.۱.۶) است بنویسیم؛ اما در (۳.۲.۶) نوشتن پایهٔ b برای اجتناب از ابهام لازم است.

چند مثال. در دستگاه شصت‌شصتی

$$(3,\ 11,\ 43)_{60}=3.60^2+11.60+43=11503.$$

در دستگاه به‌پایهٔ $b=4$

$$(3,\ 2,\ 0,\ 1)_4=3.4^3+2.4^2+0.4+1=225.$$

درحالت کلی، وقتی عددی در پایهٔ b، مانند (۱.۲.۶)، داده شده است، برای به‌دست‌آوردن عدد در دستگاه معمولی دهدهی، مقادیر توانهای b را حساب می‌کنند و هریک‌را در رقم مربوط ضرب کرده سپس باهم جمع می‌کنند، کاری که درمثالهای بالا کردیم.

حال سؤال وارون آن‌را درنظر می‌گیریم. عدد N داده شده‌است و می‌خواهیم آن‌را درپایهٔ b نمایش دهیم. این کار را می‌توانیم باتقسیم مکرر بر b انجام دهیم. نگاهی به (۱.۲.۶) بیندازید. می‌توانیم آن‌را به‌صورت زیر بنویسیم

$$N=(c_nb^{n-1}+\cdots+c_2b+c_1)b+c_0.$$

چون c_0 از b کوچکتر است، باقیماندهٔ تقسیم N بر b است. این تقسیم‌را به‌صورت زیر می‌نویسیم

$$N=q_1b+c_0,\quad q_1=c_nb^{n-1}+\cdots+c_2b+c_1,$$

تا نشان دهیم که به‌همین ترتیب c_1 ازتقسیم q_1 بر b به‌دست می‌آید و قس‌علیهذا. پس ضرایب c_i با تقسیمهای بر b به‌دست می‌آیند:

$$N=q_1b+c_0$$

$$q_1=q_2b+c_1$$

$$q_{n-1}=q_nb+c_{n-1}$$

$$q_n=0b+c_n;$$

تقسیم بر b را تا $q_n<b$، $q_{n+1}=0$ ادامه می‌دهیم. با دو مثال روش کار روشن خواهد شد.

مثال ۱. عدد ۱۰۱ را درپایهٔ ۳ بنویسید. مانندبالاتقسیمهای بر ۳ را انجام‌می‌دهیم، تا

$$101=33.3+2$$

$$33=11.3+0$$

$$11=3.3+2$$

$$3=1.3+0$$

$$1=0.3+1.$$

به‌دست آیند. بنابراین

$$۱۰۱=(۱,\ ۰,\ ۲,\ ۰,\ ۲)_{۳۰}$$

مثال ۲. عدد ۱۹۷۰ را درپایهٔ ۱۲ بنویسید. دراینجا از تقسیمهای بر ۱۲ داریم

$$۱۹۷۰=۱۶۴\cdot۱۲+۲$$
$$۱۶۴=۱۳\cdot۱۲+۸$$
$$۱۳=۱\cdot۱۲+۱$$
$$۱=۰\cdot۱۲+۱۰$$

بنابراین

$$۱۹۷۰=(۱,\ ۱,\ ۸,\ ۲)_{۱۲۰}$$

مجموعهٔ مسائل ۲.۶

۱. $(۱, ۲, ۳, ۴)_{۵}$ و $(۱, ۱, ۱, ۱, ۱, ۱)_{۲}$ را در دستگاه دهدهی بنویسید.

۲. اعداد ۳۶۲؛ ۱۹۶۹؛ ۱۰۰۰۰ را درپایه‌های ۱۷ ؛۶ ؛۲ $= b$ بنویسید.

۳.۶ مقایسهٔ دستگاههای شمارش

هدف آشکار انجمن دوازده دوازدهی امریکا[1] تغییردادن دستگاه دهدهی به‌دستگاه برپایهٔ ۱۲ است که به‌تصور انجمن دستگاهی مؤثر و مناسبتر است. پیشنهاددهندگان خاطرنشان می‌کنند که ترجیح دارد پایهٔ دستگاه براعداد ۲، ۳، ۴ و ۶ تقسیمپذیر باشد، زیرا تقسیم براین اعداد را، که زیاد هم پیش می‌آید، ساده‌تر می‌کند. تعمیم این استدلال مارا به‌دستگاه شصت‌شصتی که پایه‌اش براعداد صحیح

$$۲, ۳, ۴, ۵, ۶, ۱۰, ۱۲, ۱۵, ۲۰, ۳۰,$$

تقسیمپذیر است، هدایت می‌کند.

خیلی چیزها را هنوز به‌دوجین وقراصه (۱۲ دوجین) می‌شمارند، و دستگاه دوازده دوازدهی البته عملی خواهدبود. برای این‌کار لازم‌است دوازده نماد جدید

---

1. The Duodecimal Society of America

برای ارقام این دستگاه تعریف کنیم و روی این ارقام تقریباً به‌همان اندازهٔ دستگاه دهدهی عمل کنیم. بعضی از هواخواهان این دستگاه می‌گویند فقط به‌دو نماد جدید برای ۱۰ و ۱۱ نیاز خواهیم داشت؛ توجه‌نمی‌کنند که دراین‌صورت، درمرحلهٔ‌تغییر دستگاه دهدهی به‌دستگاه جدید، چه‌کسی می‌تواند تشخیص‌دهد که مثلا ۳۲۵ به‌معنی

$$۳\cdot۱۰^۲+۲\cdot۱۰+۵=۳۲۵$$

است، یا به‌معنی

$$۳\cdot۱۲^۲+۲\cdot۱۲+۵=۶۴۱\cdot$$

برای اینکه تصوری اجمالی از چگونگی تغییر تعداد رقمهای عددی از یک دستگاه به‌دستگاهی دیگر داشته باشیم، عدد

$$۱۰^n-۱=\overbrace{۹۹\ldots۹}^{n}=N \qquad (۱\cdot۳\cdot۶)$$

در دستگاه دهدهی را درنظر می‌گیریم. این بزرگترین عدد n رقمی در این دستگاه است. برای پیدا کردن m، یعنی تعداد ارقام N در پایهٔ b، توجه‌می‌کنیم که m بایددر

$$b^m > ۱۰^n-۱ \geqslant b^{m-۱} \qquad (۲\cdot۳\cdot۶)$$

صدق کند. این شرط را می‌توان به‌صورت زیر نوشت

$$b^m \geqslant ۱۰^n > b^{m-۱}\cdot$$

از این سه‌عدد لگاریتم می‌گیریم. باتوجه به‌اینکه $\log ۱۰ = ۱$، نتیجه می‌شود

$$m\log b \geqslant n > (m-۱)\log b$$

که می‌توان آن‌را به‌صورت

$$m \geqslant \frac{n}{\log b} > m-۱ \qquad (۳\cdot۳\cdot۶)$$

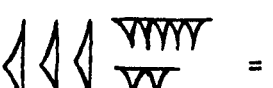
نوشت؛ پس m اولین عدد صحیح ناکوچکتر از

$$\frac{n}{\log b} \qquad (۴\cdot۳\cdot۶)$$

است. نتیجه می‌گیریم که یك عدد n رقمی در پایهٔ ۱۰ تعداد ارقامش در پایهٔ b، در حدود خارج قسمت n بر $\log b$ است.

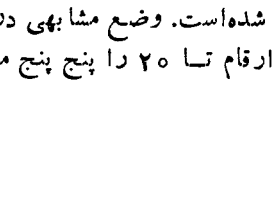
چند مثال. فرض کنید عددی در پایهٔ ۱۰، n رقم دارد. به‌ازای $b=2$ داریم $\log 2 \approx 0{,}30103$، پس تعداد ارقام در دستگاه دو دویی نزدیك به $3{,}32n$ است. به‌ازای $b=60$، $\log 60 \approx 1{,}778$، پس تعداد ارقام نزدیك به $0{,}56n$، یعنی کمی بیش از نصف تعداد ارقام در دستگاه دهدهی است.

روشن است که عمل با اعداد کم‌رقم مزایایی دارد، اما ازطرف دیگر پایه وقتی بزرگ باشد با اشکالاتی جدی روبه‌رو می‌شویم. نخست باید b رقم را نامگذاری کنیم و برای آنها نماد متمایز بسازیم. معمولا وقتی b بزرگ بوده است، این کار نشده است. مثلا در دستگاه شصت‌شصتی بابلی، واحدهای تا ۶۰ را در گروههای ده‌تایی می‌شمردند. درشکل ۱.۳.۶ طرز نوشتن ۳۷ را می‌بینیم



شکل ۱.۳.۶

این درواقع به‌این معنی است که دستگاه به دستگاههای کوچکتری که در دستگاه دهدهی نوشته شده‌اند تقسیم شده‌است. وضع مشابهی در دستگاه بیست‌بیستی مایاها وجود دارد. دراین دستگاه ارقام تا ۲۰ را پنج پنج می‌شمردند. در شکل ۲.۳.۶ نمونه‌ای آورده‌ایم.



شکل ۲.۳.۶

اشکالات دیگری، خیلی بزرگتر، در عمل محاسبات معمولی ظاهر می‌شوند. درضرب از اینکه جدول‌ضرب، یعنی تمام حاصلضربهای یك‌رقمی در یك رقمی، را از حفظ هستیم استفاده می‌کنیم. این جدول فیثاغورسی[1] را در سالهای اول مدرسه یادگرفته‌ایم به‌طوری‌که برای ما تقریباً به‌صورت خودکار درآمده‌است. اما این‌دانش آن‌قدر که فکر می‌کنیم بی‌ارزش نیست، درنوشته‌های ریاضی قرون‌وسطی به‌روشنی دیده می‌شود که ضرب درجزء ریاضیات عالی محسوب می‌شده و به‌راستی اشخاصی که در تقسیمهای بزرگ مهارت داشتند، نادر بوده‌اند. بهتر است چندمثال بیاوریم.

ساموئل پپیس[2] در دفتر خاطرات مشهورش نوشته است، در تابستان ۱۶۶۲ زمانی‌که نزدیك به‌سی‌سال داشت و دبیر پرایوی‌سیل[3] بود تصمیم گرفت که برای بررسی مستقل حسابهایش مقداری ریاضیات، حداقل اصول حساب را فراگیرد. درآن‌زمان درجهٔ کارشناسی و درجهٔ کارشناسی ارشد ازکمبریج داشت، اما برای یك جنتلمن انگلیسی تحصیلکرده پدیده‌ای غیرعادی نبودکه بامحاسباتی‌که هرروز مورد نیاز است، کاملا ناآشنا باشد؛ این کارها را به‌دفتردارهای زیردستشان واگذارمی‌کردند.

پپیس در ژوئیهٔ ۱۶۶۲ در دفتر خاطراتش می‌نویسد: «به‌زودی آقای کوپر[4]، افسر رویال چارلز[5]، که تصمیم‌دارم ازاو ریاضیات بیاموزم، واز امروز بااوشروع به‌آموختن کنم، می‌آید؛ او مرد خیلی واردی است، وفکر می‌کنم باچیزکمی راضی خواهد شد. بعداز یك ساعت که بااو حساب خواندم (اولین کوششم در یادگرفتن جدول ضرب) تا فردا از هم جدا شدیم.»

پپیس روزانه با معلم دریانوردش، صبح زود و اواخر شب، برای یادگرفتن خسته‌کنندهٔ جدول‌ضرب سخت می‌کوشید. مثلا درنهم‌ژوئیه می‌نویسد: «ساعت چهار بیدار شدم وسخت بـا جدول ضرب که تمام‌گرفتاری من در حساب است، مشغولم» روزهای بعد به‌همین‌ترتیب می‌گذرند تا در ۱۱ ژوئیه می‌تواند ازتوفیق خود خبر دهد: «ساعت چهار بیدار شده‌ام وسخت باجدول‌ضربی‌که اکنون تقریباً برآن‌احاطه دارم، مشغولم.» پپیس به‌بهترین‌وجه ازعلم جدیدی‌که آموخته بود دربه‌دست‌آوردن مقامهای مهم و مهمتر استفاده‌کرد، دوسال ونیم پس‌از یادگرفتن جدول ضرب عضو فرهنگستان علوم‌مشهور انگلستان، یعنی‌انجمن‌سلطنتی‌شد ــ پیشرفتی بیش‌ازحدسریع.

این حکایت کوچك‌راکه به‌هیچ‌وجه استثنایی‌نیست برای‌این آوردیم‌که تأکید

---

۱. در بسیاری ازکشورها، جدول‌ضرب را جدول فیثاغورسی می‌گویند.

2. Samuel Pepys 3. Privy Seal

4. Cooper 5. Royall Charles

کنیم در ریاضیات، آموختن جدول ضرب در زمان قدیم کاری پیش پا افتاده نبوده است. پس هم از نظر ذهنی و هم از نظر مکانیکی پایه‌های کوچك اعداد در اعمال حسابی ما خیلی بهترهستند. مثلا وقتی پایهٔ b، ۳ است، فقط یك ضرب حفظ کردنی

$$۲\cdot۲ = ۴ = (۱, ۱)_۳$$

در جدول ضرب

	۰	۱	۲
۰	۰	۰	۰
۱	۰	۱	۲
۲	۰	۲	$(۱, ۱)_۳$

وجود دارد. برای $b = ۲$ جدول کاملا ساده است

	۰	۱
۰	۰	۰
۱	۰	۱

مجموعهٔ مسائل ۳.۶

۱. ثابت کنید که در دستگاه به‌پایهٔ b، تعداد ضربهای ارقام، جز ضربهای در ۰ و ۱ برابر است با

$$\frac{۱}{۲}(b-۱)(b-۲).$$

۲. مجموع تمام اعداد جدول ضرب را پیدا کنید. این مجموع را برای $b = ۱۰$ بررسی کنید.

۴.۶ چند مساله مربوط به دستگاههای شمارش

چند مسألهٔ دستگاههای شمارش را که به‌انتخاب پایه‌ها برای محاسبه باماشین مربوط

می‌شوند، بررسی می‌کنیم. فرض کنید ماشین‌حسابی داریم که بـه وسیلهٔ چرخهای اعداد که هریك‌دارای رقمهای ۰، ۱، ...، ۹ است،کارمی‌کند. اگر n تعداد چرخها باشد، با این ماشین تمام اعداد از ۰ تا

$$N=\overbrace{۹۹\ldots۹}^{n} \qquad (۱.۴.۶)$$

را می‌توانیم نشان دهیم، (۱.۳.۶) را ببینید.

حال فرض‌کنید به‌جای پایهٔ ۱۰، از پایهٔ b برای نمایش اعداد از ۰ تـا N استفاده می‌کنیم. آن‌گاه باید m چرخ داشته باشیم، عدد صحیح m در (۲.۳.۶) و (۳.۳.۶) صفحهٔ ۷۱ صدق می‌کند. در (۴.۳.۶) دیدیم که m، عدد صحیح بعد از

$$\frac{n}{\log b}$$

یاخوداین‌عدداست.چون‌هرچرخ b رقم‌دارد،$m.b$، تعدادکل‌ارقام‌چرخها تقریباً برابر با

$$D=n.\frac{b}{\log b} \qquad (۲.۴.۶)$$

است.

حال این‌سؤال‌را مطرح می‌کنیم: b چه باشد تا تعدادکل ارقام‌کمترین‌باشد؟ برای پیداکردن‌کمترین مقدار عدد D کافی است مقادیر تابع

$$f(b)=\frac{b}{\log b} \qquad (۳.۴.۶)$$

را به‌ازای‌پایه‌های‌مختلف $b=۲,۳,۴,\ldots$ بررسی‌کنیم. ازجدول‌لگاریتم‌مقادیر زیر نتیجه می‌شوند

b	۲	۳	۴	۵	۶
$f(b)$	۶٫۶۴	۶٫۲۹	۶٫۶۴	۷٫۱۵	۷٫۷۱

مقادیر بعدی $f(b)$، بزرگتر هستند؛ مثلا بـه‌ازای $b=۱۰$، قبلا توجه کردیم کـه $f(۱۰)=۱۰$. از این محاسبات نتیجه می‌گیریم:

تعدادکل ارقام دریك ماشین محاسبه به‌ازای $b=۳$ مینیمم است.

همچنین می بینیم که به‌ازای $b=۲$ و $b=۴$، تعداد کل ارقام چندان بزرگتر نیست؛ پس ازاین‌نظر پایه‌های کوچك ترجیح دارند.

حال مسأله را کمی تغییر می‌دهیم. یادآوری می کنیم کـه چرتکهٔ معمولی از نوعی که گاهی برای آموزش‌شمردن به‌بچه‌ها به‌کار می‌رود، تعدادی مفتول فلزی‌دارد و هر مفتول، برای نشان‌دادن رقمهای اعداد، دارای ۹ مهرهٔ متحرك است. به جـای چرتکه می‌توان روی‌کاغذ خطوطی موازی رسم کرد و با چوبهای‌کبریت روی خطها رقمهارا مشخص کرد، یامانند زمان‌قدیم که با ریگ محاسبه می کردند، خطهایی‌روی زمین‌کشید و ارقام‌را با ریگها مشخص کرد.

چرتکه را اختیار می کنیم، اگـر چرتکه n مفتول و هرمفتول ۹ مهرهٔ متحرك داشته باشد، می‌توان با آن تمام اعداد را تا $N=\overbrace{۹۹\ldots۹}^{n}$ نمایش داد. حال این مساله را مطرح می کنیم: آیا با انتخاب پایهٔ دیگری مانند b، می توانیم چرتکه‌ای جمع وجورتر، یعنی با مهره‌هایی کمتر، بسازیم؟

درپایهٔ b، هرمفتول $b-۱$ مهره‌دارد. مانندگذشته، برای‌اینکه گنجایش‌چرتکه N باشد، تعداد ارقام از روی (۴.۳.۶) مشخص می‌شود. ازاین طریق، برای تعداد کل مهره‌ها به‌مقدار تقریبی زیر می‌رسیم

$$E=\frac{n}{\log b}\cdot(b-۱). \qquad (۴.۴.۶)$$

برای پیداکردن کوچکترین مقدار ممکن، باید تابع

$$g(b)=\frac{b-۱}{\log b} \qquad (۵.۴.۶)$$

را به‌ازای مقادیر $b=۲,۳,\ldots$ بررسی کنیم. مقادیر $g(b)$ برای مقادیر کوچك b درجدول زیر داده شده‌اند:

b	۲	۳	۴	۵	۶
$g(b)$	۳٫۳۲	۴٫۱۹	۴٫۹۸	۵٫۷۲	۶٫۴۳

هرچه b بزرگ شود، مقدار تابع بزرگتر می‌شود، پس می‌توانیم نتیجه بگیریم:

تعداد مهره‌های لازم در چرتکه به‌ازای $b=۲$، کمترین است.

این نتیجه را می‌توانیم از دیدگاهی دیگر تعبیر کنیم. فـرض کنید رقمهای

عددمان را باقراردادن چوب‌کبریت یاریگ روی‌خطها مشخص می‌کنیم. در دستگاه دهدهی روی هرخط از ۰ تا ۹ علامت خواهیم داشت. وقتی اعداد را به تصادف اختیارکنیم به‌طور متوسط ۴٫۵ چوب‌کبریت روی هرخط وجود دارد. بنابراین، اگرانتخاب اعداد تصادفی‌باشد، برای اعداد n رقمی به‌طورمتوسط $4.5n$ چوب کبریت لازم است.

ببینیم گذاشتن چوب‌کبریتها به‌جای‌خود چه‌مدت طول می‌کشد. برای‌اینکه‌عدد معینی درخاطرمان بماند فرض‌کنیم گذاشتن هرچوب‌کبریت یك‌ثانیه وقت می‌گیرد. دراین‌صورت گذاشتن تمام چوب‌کبریتها به‌طور متوسط درحدود n . $4\frac{1}{2}$ ثانیه طول خواهدکشید.

فرض کنیدکه پـایه را از ۱۰ به b تبدیل می‌کنیم و ظرفیت نمایش اعداد را تغییر نمی‌دهیم. آن‌گاه روی هرخط از ۰ تا $b-1$ چوب کبریت خواهیم داشت، به‌طورمتوسط

$$\frac{1}{2}(b-1)$$

چوب‌کبریت روی هرخط. چندین‌بار تابحال گفته‌ایم‌که تقریباً به

$$\frac{n}{\log b}$$

خط نیاز خواهیم داشت. نتیجه می‌گیریم‌که زمان متوسط برای نشان‌دادن یك‌عدد n رقمی تقریباً درحدود

$$\frac{n}{\log b}\cdot\frac{1}{2}(b-1)=\frac{1}{2}E$$

ثانیه است، E همان‌عبارت(۴.۴.۶) است. چون E به‌ازای $b=2$ مینیمم‌است، در اینجا هم نتیجه‌می‌گیریم:

به‌طورمتوسط، مدت‌زمان‌لازم برای نشان‌دادن‌عدد، به‌ازای $b=2$ مینیمم‌است.

مجموعهٔ مسائل ۴.۶

۱. نمودار تابعهای $y=f(b)$ و $y=g(b)$ در (۳.۴.۶) و (۵.۴.۶) را به ازای

$b > ۱$ رسم کنید. اگر با حساب دیفرانسیل آشنا هستید، از آن برای تعیین شیب خمها استفاده کنید.

۵.۶ کامپیوترها و دستگاههای شمارش آنها

قبل از به‌وجودآمدن کامپیوترهای الکترونیکی، دستگاه دهدهی بر تمام میدانهای محاسبات‌عددی حاکم بود. عمدتاً ازنظرتاریخی وفرهنگی به‌دستگاههای‌دیگرشمارش توجه می‌شد. تنها چند مسألهٔ ریاضی در دستگاههای دودویی یا سه‌سه‌ای به‌بهترین صورت بیان‌می‌شدند. بازی نیم[1] یکی‌ازمثالهای موردتوجه‌کتابهای نظریهٔ‌اعدادبود.

وقتی‌کامپیوترها به‌تدریج به‌چندین‌صورت‌ظاهر شدند،لازم‌شدکه «سخت‌افزار» را به‌قسمی بسازندکه تاحدامکان‌کارآمد و بدون‌زواید باشد. این‌موجب شدکه برای تعیین مناسبترین دستگاه عددشماری رسیدگی دقیقی بشود. به‌دلایل زیاد (بعضی از آنها را در بخش قبل مورد بحث قرار دادیم) دستگاه دودویی بهترین انتخاب بود. درواقع مانع اصلی این است‌که ما بادستگاه دهدهی عادت‌کرده‌ایم وبرای اکثر ما امکان ندارد به‌آسانی با دستگاه دودویی‌خو بگیریم. درنتیجه، چون اعدادی‌که به کامپیوتر داده می‌شوند، معمولا در دستگاه دهدهی نوشته شده‌اند، لازم‌است که‌نخست کامپیوتر اعداد داده‌شده‌را به‌اعداد دودویی تبدیل‌کند؛ ودرآخرکار به‌ملاحظهٔ آنهایی که‌کمتر با ریاضیات آشنایی‌دارند، جوابها را به‌صورت دهدهی بیان‌کند.

البته دستگاه دودویی‌که در کامپیوترها به‌کار می‌رود، همان است‌که در بخش قبل دربارهٔ آن بحث‌کرده‌ایم، اما اصطلاحی‌که به‌کار می‌رود بیشتر فنی است. ارقام دوتایی ۰ و ۱ را بیتس (*bits*)، که‌خلاصهٔ‌ارقام‌دوتایی (BInary digiTS) است، می‌نامند. همچنین‌چون‌درهرموضع‌فقط دو امکان ۰ و ۱ وجوددارد، اغلب دستگاه‌را دوحالتی می‌گویند.

اگر قاعدهٔ کلی راکه دربخش ۲.۶ توضیح دادیم به‌کار بریم. نوشتن عددی مفروض در دستگاه دودویی بسیارساده‌است. مثلا بسط عدد $N = ۱۹۷۱$ دردستگاه دودویی از تقسیم مکرر بر $b = ۲$ به‌دست می‌آید:

$$۱۹۷۱ = ۹۸۵ \cdot ۲ + ۱,$$

$$۹۸۵ = ۴۹۲ \cdot ۲ + ۱,$$

$$۴۹۲ = ۲۴۶ \cdot ۲ + ۰,$$

---

1. game of Nim

$$۲۴۶ = ۱۲۳.۲ + ۰,$$
$$۱۲۳ = ۶۱.۲ + ۱,$$
$$۶۱ = ۳۰.۲ + ۱,$$
$$۳۰ = ۱۵.۲ + ۰,$$
$$۱۵ = ۷.۲ + ۱,$$
$$۷ = ۳.۲ + ۱,$$
$$۳ = ۱.۲ + ۱,$$
$$۱ = ۰.۲ + ۱.$$

نتیجه اینکه

$$۱۹۷۱_{۱۰} = (۱, ۱, ۱, ۱, ۰, ۱, ۱, ۰, ۰, ۱, ۱)_{۲}.$$

قبلا توجه کردیم که در دستگاه دودویی، اعداد باعبارتهای طویلتر بیان می‌شوند؛ بنابراین، شناسایی اعداد بایك نظر مشکل می‌شود. به‌این‌جهت در زبان کامپیوتر اغلب دستگاه ۸ اوکتال (پایهٔ ۸) را به‌کار می‌برند. این دستگاه، بامختصر تغییر، دستگاه دودویی است که از جدا کردن سه به‌سهٔ بیتهای یك عدد در دستگاه دودویی به‌دست می‌آید. این عمل را می‌توان عددنویسی در پایهٔ

$$b = ۸ = ۲^{۳}$$

به‌حساب آورد؛ ضریبها هشت عدد زیر هستند:

۰ = ۰۰۰	۴ = ۱۰۰
۱ = ۰۰۱	۵ = ۱۰۱
۲ = ۰۱۰	۶ = ۱۱۰
۳ = ۰۱۱	۷ = ۱۱۱

به‌عنوان مثال عدد ۱۹۷۱ مثال قبل را در نظر می‌گیریم. این عدد در دستگاه اوکتال به‌صورت زیر نوشته می‌شود

$$۱۹۷۱ = ۰۱۱;\ ۱۱۰;\ ۱۱۰;\ ۰۱۱ = (۳;\ ۶;\ ۶;\ ۳)_{۸۰}$$

می‌بینیدکه ازاین‌راه تنها جزئی تغییری درنوشتن عدد به‌وجود آمده است. درواقع ما با این‌راه در دستگاه دهدهی کاملا آشنا هستیم؛ وقتی عدد بزرگی‌را می‌نویسیم یا می‌خوانیم، معمولا ارقام را به‌گروههای سه‌تایی تقسیم می‌کنیم، مثلا

$$N = ۸۹\ ۷۴۷\ ۳۲۱\ ۹۲۴۰$$

درحقیقت می‌توانیم بگوییم این یك نمایش عدد درپایهٔ

$$b = ۱۰۰۰ = ۱۰^{۳}$$

است.

گاهی در کامپیوتر مفید است اعداد به‌صورتهای دیگری نمایش داده شوند. فرض‌کنید مثلا عدد $N = ۲۹۴۷$ را می‌خواهیم در ماشینی‌که شمارش اعداد برپایهٔ ۲ است، واردکنیم. به‌جای‌اینکه N راکاملا در دستگاه دودویی بنویسیم، می‌توانیم تنها ارقام

$$۲ = ۰۰۱۰$$

$$۹ = ۱۰۰۱$$

$$۴ = ۰۱۰۰$$

$$۷ = ۰۱۱۱$$

را به‌ماشین بدهیم و N را به‌صورت

$$N = ۰۰۱۰;\ ۱۰۰۱;\ ۰۱۰۰;\ ۰۱۱۱$$

درماشین واردکنیم. این اعداد به دهدهیهای رمزی معروف‌اند. این روش را گاهی دستگاه ۸۴۲۱ می‌نامند، زیرا ارقام دهدهی به‌صورت مجموعهای واحدهای دودویی زیر بیان می‌شوند

$$۰ = ۰۰۰۰,\ ۱ = ۰۰۰۱,\ ۲ = ۰۰۱۰,\ ۲^{۲} = ۴ = ۰۱۰۰,\ ۲^{۳} = ۸ = ۱۰۰۰$$

این دهدهیهای رمزی برای هر نوع محاسبهٔ عددی نامناسب‌اند، اما همیشه کار ماشین محاسبه‌کردن نیست. به‌همین‌طریق، به‌هریك از حروف الفبا و به‌هر نماد دیگری می‌توان یك‌عدد دودویی تخصیص داد. یعنی هرکلمه یا جمله را می‌توان در

حافظهٔ کامپیوتر به‌صورت یك عدد دودویی نگهداشت. پس اگـر ما کاملا ورزیده می‌بودیم و شنوندگان ورزیده‌ای‌هم می‌داشتیم، می‌توانستیم تنها با زبان بیتها گفتگو کنیم.

مجموعهٔ مسائل بخش ۵.۶

۱. اعداد فرما، $۲^{۲^{n}}+۱$ (بخش ۳.۲، صفحهٔ ۲۳) را در دستگاه به پایهٔ ۲ بنویسید.

۲. اعداد تام زوج (بخش ۴.۳ صفحهٔ ۳۶).

$$P=۲^{p-۱}(۲^{p}-۱)$$

را در دستگاه به‌پایهٔ ۲ بنویسید.

۶.۶ بازیهای با ارقام

انواع زیادی بازی با ارقام وجوددارند. بعضی از آنها ازقرون وسطی به‌ما رسیده‌اند. بیشتر آنها ازنظر تئوری درنظریهٔ اعداد ارزش زیادی ندارند، بلکه نظیر مربعهای سحرآمیز در ردهٔ جدولهای متقاطع هستند. چندتایی از آنها را باچند مثال دراینجا توضیح می‌دهیم.

این تقاضای فوری تلگرافی دانشجویی به‌خانواده‌اش را درنظر بگیرید:

$$\begin{array}{r} \text{SEND} \\ \text{MORE} \\ \hline \text{MONEY}. \end{array}$$

این‌طرح‌را دوعدد چهار رقمی SEND و MORE تصورکنیدکه‌مجموعشان MONEY است. هرحرف به‌معنای رقم مشخصی است. می‌خواهیم این ارقام‌را تعیین کنیم. چون تنها ده رقم داریم، در چنین مسأله‌ای حداکثر می‌توانیم ده حرف مختلف داشته باشیم؛ در این مسأله هشت حرف مختلف داریم. ایدال این است که مسأله تنها یك‌جواب داشته باشد.

درمثال بالا $S+M$ یا $S+M+۱$ عدد دو رقمی MO است، اما S و M از ۹ بزرگتر نیستند، پس رقم اول MO،

$$M=۱۰$$

چون $S+۱$ یا $S+۲$ عددی دورقمی است،

$$S=۸ \text{ یا } S=۹$$

نشان می‌دهیم که S، هشت نیست. اگر S هشت باشد، باید ازستون صدها یك واحد به‌ستون هزارها اضافه شود تا

$$S+M+۱=۸+۱+۱=۱۰$$

دورقمی شود. درنتیجه O باید صفر باشد و تلگرام به‌صورت زیر درمی‌آید

$$\begin{array}{r} ۸\ E\ N\ D \\ ۱۰\ R\ E \\ \hline ۱۰\ N\ E\ Y\cdot \end{array}$$

اما ازبررسی‌ستون صدها دیده‌می‌شودکه باید ازستون دهها یك واحد به‌ستون صدها اضافه شود (وگرنه $E+O=E$ و نه N)، و چون $E\leqslant ۹$، و $E+O+۱$ باید دورقمی باشد

$$E+O+۱=۱۰\cdot$$

پس ناچار $N=۰$؛ اما قبلا $O=۰$ به‌دست آمده است، و بنابراین $S\neq ۸$. نتیجه می‌گیریم‌که $S=۹$ و تلگرام به‌صورت

$$\begin{array}{r} ۹\ E\ N\ D \\ ۱۰\ R\ E \\ \hline ۱۰\ N\ E\ Y \end{array}$$

درمی‌آید. چون $E\neq N$، از ستون صدها به

$$E+۱=N,$$

می‌رسیم، و صورت زیر حاصل می‌شود

$$\begin{array}{r} ۹\quad E\quad E+۱\quad D \\ ۱\quad ۰\quad R\quad E \\ \hline ۱\quad ۰\quad E+۱\quad E\quad Y\cdot \end{array}$$

از مجموع ستون دهها نتیجه می‌شود که

$$E+۱+R=۱۰+E \quad \text{یا} \quad E+۱+R+۱=۱۰+E.$$

از رابطهٔ سمت‌چپ $R=۹$، که با $S=۹$ تناقض دارد، نتیجه‌می‌شود. پس بنا بر رابطهٔ سمت راست،

$$R=۸$$

و تلگرام به‌صورت زیر است:

	۹	E	E+۱	D
	۱	۰	۸	E.
۱	۰	E+۱	E	Y.

سرانجام مجموع ستون واحدها برابر است با[۱]

$$D+E=۱۰+Y.$$

برای سه‌حرف D، E، Y فقط رقمهای ۲، ۳، ۴، ۵، ۶، ۷ باقیمانده است. پس $D+E$ از ۱۳ بزرگتر نیست و Y یا ۲ است یا ۳. اما $Y\neq ۳$، زیرا اگر $Y=۳$، آن‌گاه $D+E=۱۳$، پس یا $E=۶$ یا $E=۷$. از $E=۷$، $R=۸=۱+E=N$ نتیجه می‌شود که با $N\neq R$ متناقض است. از $E=۶$، تناقض

$$N=E+۱=۷=D,$$

نتیجه می‌شود. پس $Y=۲$ و $D+E=۱۲$. از بین اعداد ۲، ۳، ۴، ۵، ۶، ۷ تنها مجموع دو عدد ۷ و ۵ دوازده است. اما $E\neq ۷$، پس $D=۷$ و $E=۵$، و تنها جواب مسأله

۹	۵	۶	۷	
۱	۰	۸	۵	
۱	۰	۶	۵	۲

است.

---

۱. زیرا از مجموع ستون دهها نتیجه می‌شود که $D+E$ عددی دورقمی است.ـم.

ایـن روند نسبتاً پرزحمت است؛ گـرچه جواب در حالات بسیاری آسانتر به‌دست می‌آید.

مجموعهٔ مسائل ۶.۶

۱. سعی کنید مثالهای زیر را با روشی کـه در این بخش توضیح دادیم تجزیه و تحلیل کنید.

۱.
```
  SEND
  MORE
  GOLD
------
 MONEY
```

۲.
```
  ADAM
   AND
   EVE
    ON
     A
------
  RAFT
```

۲.
```
 HOCUS
 POCUS
------
PRESTO
```

۳.
```
 FORTY
   TEN
   TEN
------
 SIXTY
```

۵.
```
  SEE
  SEE
  SEE
  YES
------
 EASY.
```

اگر بخواهید می‌توانید خودتان مثالهای بیشتری بسازید. اگر با کامپیوتر آشنایی دارید سعی کنید برنامه‌هایی برای به‌دست آوردن جوابهای این نوع مسائل بریزید.

فصل ۷

همنهشتیها

۱.۷ تعریف همنهشتی

نظریهٔ اعداد برای خود جبری داردکه به نظریهٔ همنهشتیها معروف است. در آغاز، جبر به‌عنوان یك‌خلاصه‌نویسی اعمال حساب ظاهر شد. همنهشتی هم یك‌زبان‌نمادی برای مفهوم اساسی نظریهٔ اعداد، یعنی بـرای تقسیمپذیری است. اولین‌بار گاوس مفهوم همنهشتی را معرفی کرد.

قبل از اینکه وارد بحث در همنهشتی شویم، دربارهٔ اعدادی که در این فصل مطالعه خواهیم کرد تذکری می‌دهیم. درآغاز کتاب گفتیم که‌کار ما با اعداد صحیح و مثبت ۱، ۲، ۳، ... خواهد بود، در فصلهای گذشته، خود را به این اعداد و عدد اضافی ۰ محدودکردیم. اما حالا به‌مرحله‌ای رسیده‌ایم‌که بهتراست میدان بحث را به‌تمام اعداد صحیح مثبت یا منفی

$$0, \pm 1, \pm 2, \pm 3, \ldots$$

گسترش‌دهیم. این‌کار تغییری اصولی درمفهومهای قبلی به‌وجود نمی‌آورد؛ درآنچه می‌آید، وقتی ازعدد اول، مقسوم‌علیه، بزرگترین مقسوم‌علیه مشترك ونظیر اینها گفتگو می‌شود، مانند سابق آنهارا مثبت فرض می‌کنیم.

حال به‌زبان همنهشتیها می‌پردازیم. اگر a و b دوعدد صحیح باشند و تفاضلشان $a-b$ بر m تقسیمپذیر باشد، می‌نویسیم

$$a \equiv b \ (m \text{ به پیمانهٔ}) \qquad (۱۰۱۰۷)$$

و می‌گوییم

a با b همنهشت به‌پیمانهٔ m است. (۱۰۱۰۷)

مقسوم‌علیه m را مثبت فرض می‌کنیم و آن را پیمانهٔ همنهشتی می‌نامیم. حکمهای (۱۰۱۰۷) بدین‌معنی است که

$a-b=mk$ و k عددی صحیح است. (۲۰۱۰۷)

چند مثال.

۱) (به‌پیمانهٔ ۵) $۲۳ \equiv ۸$ زیرا $۲۳-۸=۱۵=۵.۳$

۲) (به‌پیمانهٔ ۹) $۴۷ \equiv ۱۱$ زیرا $۴۷-۱۱=۳۶=۹.۴$

۳) (به‌پیمانهٔ ۸) $-۱۱ \equiv ۵$ زیرا $-۱۱-۵=-۱۶=۸.(-۲)$

۴) (به‌پیمانهٔ ۲۷) $۸۱ \equiv ۰$ زیرا $۸۱-۰=۸۱=۲۷.۳$

مثال آخر نشان می‌دهد که، به‌طور کلی، به‌جای اینکه بگوییم عدد a بر m تقسیمپذیر است، می‌توانیم بنویسیم

$$a \equiv ۰ \ (m \text{ به پیمانهٔ}),$$

زیرا این عبارت به‌معنی

$$a-۰=a=mk$$

است، که در آن k عددی صحیح است. مثلا به‌جای اینکه بگوییم a عددی زوج است، می‌توانیم بنویسیم

$$a \equiv ۰ \ (\text{به‌پیمانهٔ } ۲).$$

همچنین می‌بینیم عددی فرد است که در

$$a \equiv ۱ \quad (\text{به‌پیمانهٔ } ۲)$$

صدق کند. این اصطلاحها که تاحدودی به‌نظر عجیب می‌آیند، در نوشته‌های ریاضی کاملا متداول‌اند.

۲.۷ بعضی از ویژگیهای همنهشتی

طرز نوشتن همنهشتی‌ما را به‌یاد معادله می‌اندازد، ودرواقع، همنهشتی ومعادلهٔ جبری، ویژگیهای مشترکی دارند. ساده‌ترین آنها سه‌ویژگی زیرند:

$$a \equiv a \pmod{m}; \qquad (۱.۲.۷)$$

که از $a - a = ۰ = m.۰$ نتیجه می‌شود.

$$b \equiv a \pmod{m}, \qquad (۲.۲.۷)$$

از $a \equiv b \pmod{m}$، نتیجه می‌شود زیرا $b - a = -(a-b) = m(-k)$.

$$a \equiv c \pmod{m}. \qquad (۳.۲.۷)$$

از $a \equiv b \pmod{m}$ و $b \equiv c \pmod{m}$ نتیجه می‌شود

زیرا دوحکم اول به‌معنی

$$a - b = mk, \quad b - c = ml,$$

هستند و بنابراین

$$a - c = (a-b) + (b-c) = m(k+l).$$

مثال. از $۳۵ \equiv ۱۳ \pmod{۱۱}$، $۳۵ \equiv -۹ \pmod{۱۱}$ نتیجه می‌شود $۱۳ \equiv -۹ \pmod{۱۱}$.

گفتیم که ویژگیهای همنهشتی وبرابری با هم شباهت دارند. درواقع برابری نوعی همنهشتی است: همنهشتی به‌پیمانهٔ ۰. بنابرتعریف

$$a \equiv b \pmod{۰}$$

یعنی $a - b = ۰ . k = ۰$ یا $a = b$.

شما هیچوقت درنوشتارهای ریاضی به‌برابریهایی که به‌صورت این همنهشتی نوشته شده باشند برنمی‌خورید. اما همنهشتی دیگری که ظاهراً ارزشی ندارد، گاهی به‌کار می‌رود. وقتی پیمانه، $m = ۱$ است، به‌ازای هردو عدد صحیح a و b

$$a \equiv b \pmod{۱}, \qquad (۴.۲.۷)$$

زیرا این همنهشتی بدین‌معنی است که

$$a-b=۱۰k=k \qquad (۵.۲.۷)$$

عددی صحیح است. اما برای چندلحظه فرض کنید a و b اعدادی حقیقی هستند، نه الزاماً صحیح. آن‌گاه همنهشتی (به‌پیمانهٔ ۱) بدین‌معنی‌است که تفاضل a و b عددی صحیح‌است، یعنی‌قسمتهای کسری دوعدد (یا قسمتهای دهدهی آن‌دو، اگر به‌صورت دهدهی نوشته شوند) باهم برابرند.

مثال.

$$۸\frac{۱}{۳}\equiv ۱\frac{۱}{۳} \quad (\text{به‌پیمانهٔ } ۱)$$

یا

$$۸,۳۳۳\ldots\equiv ۱,۳۳۳\ldots \quad (\text{به‌پیمانهٔ } ۱)$$

برگردیم به‌ویژگیهای همنهشتیهای معمولی اعداد صحیح؛ ازحالا به‌بعد فرض می‌کنیم‌که پیمانهٔ m عدد صحیحی از ۲ بزرگتر یا ۲ است.

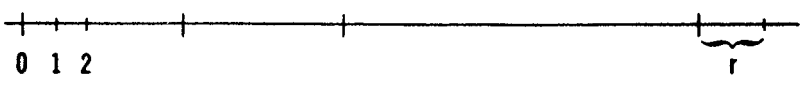
محور اعداد را از مبدأ در دوجهت، مانند شکل ۱.۲.۷ به‌بازه‌های به‌طول m تقسیم می‌کنیم. آن‌گاه هرعدد a، مثبت یا منفی، در داخل یکی از این بازه‌ها یا روی یکی‌از نقاط تقسیم واقع می‌شود، پس می‌توانیم بنویسیم

$$a=km+r, \qquad (۶.۲.۷)$$

که در آن k عددی صحیح و r یکی‌از اعداد

$$۰, ۱, ۲, \ldots, m-۱ \qquad (۷.۲.۷)$$

است. این تعمیمی جزئی‌از تقسیم‌اعداد صحیح ومثبت بخش ۳.۴ است. دراینجاهم، در رابطهٔ (۶.۲.۷). r را باقیماندهٔ a در تقسیم بر m، یا باقیماندهٔ (به پیمانهٔ m)، می‌نامیم.



شکل ۱.۲.۷

چند مثال.

(۱ $a=۱۱, \quad m=۷, \qquad ۱۱=۷\cdot۱+۴.$

(۲ $a=-۱۱, \quad m=۷, \quad -۱۱=۷\cdot(-۲)+۳.$

تقسیم (۶.۲.۷) را می‌توان به‌صورت همنهشتی

$$a\equiv r(m \text{ به پیمانهٔ}) \qquad (۸.۲.۷)$$

نوشت؛ پس هرعدد با باقیماندهٔ (به‌پیمانهٔ m)اش، همنهشت است. درمثالهای بالا

$$۱۱\equiv ۴ \text{ (به‌پیمانهٔ ۷)}, \quad -۱۱\equiv ۳ \text{ (به‌پیمانهٔ ۷)}.$$

در باقیمانده‌های (۷.۲.۷) هیچیك بـا دیگری همنهشت (به‌پیمانهٔ m) نیست، زیـرا اختلاف بین هردو بـاقیمانده از m کمتر است. بنابراین دو عدد ناهمنهشت (به‌پیمانهٔ m)، دوباقیماندهٔ متمایز دارند. نتیجه می‌گیریم:

همنهشتی (به‌پیمانهٔ $a\equiv b(m$ برقرار است[۱] اگروتنهااگر a و b اعدادی باشند که چون بر m تقسیم شوند، یك باقیمانده داشته باشند.

مفهوم این‌همنهشتی را از راه‌دیگری می‌توان بیان‌کرد. فعلا a و b را صحیح ومثبت می‌گیریم. دربحث از دستگاههای شمارش در بخش ۲.۶ توجه‌کردیم که‌وقتی a را در دستگاه به‌پایه m می‌نویسیم،

$$a=(a_m, \ldots, a_۱, a_۰)_m,$$

$a_۰$، رقم آخـر، باقیماندهٔ تقسیم a بر m است. اگر این نکته را بـه کار بـریم، می‌توانیم همنهشتی را با بیان زیر تعبیرکنیم:

همنهشتی (به پیمانهٔ $a\equiv b(m$ برقرار است، اگـر و تنها اگر رقم آخر دو عدد صحیح (مثبت) a و b درپایهٔ m یکی باشد.

مثلا

$$۳۷\equiv ۸۷ \text{ (به‌پیمانهٔ ۱۰)}$$

زیرا در دستگاه دهدهی رقم آخر این دوعدد یکی است.

---

۱. به‌عبارت دیگر a و b همنهشت (به‌پیمانهٔ m) هستند.ـم.

مجموعهٔ مسائل ۲.۷

۰۱ باقیمانده‌های (به‌پیمانهٔ ۷) -۳۷، (به‌پیمانهٔ ۱۱) $۱۱۱-$، (به‌پیمانهٔ ۳۰) -۳۶۵ را پیدا کنید.

۳.۷ جبر همنهشتیها

به‌خاطر داریم که درجبر معادله‌ها را می‌توان باهم جمع، از هم تفریق، درهم ضرب کرد. دقیقاً همین قاعده‌ها درهمنهشتیها برقرار هستند. همنهشتیهای

$$a\equiv b(m \text{ به‌پیمانهٔ}),\quad c\equiv d(m \text{ به‌پیمانهٔ}) \qquad (۱.۳.۷)$$

را درنظر بگیرید، بنابر تعریف

$$a=b+mk,\quad c=d+ml, \qquad (۲.۳.۷)$$

k و l اعداد صحیح هستند. معادله‌های (۲.۳.۷) را باهم جمع می‌کنیم. نتیجه

$$a+c=b+d+m(k+l)$$

است و می‌توان آن را به‌صورت

$$a+c\equiv b+d(m \text{ به پیمانهٔ}) \qquad (۳.۳.۷)$$

نوشت؛ به‌عبارت دیگر دو همنهشتی را می‌توان باهم جمع کرد. به‌همین طریق دیده می‌شود که یك همنهشتی را می‌توان ازهمنهشتی دیگری کم کرد، یعنی

$$a-c\equiv b-d\ (m \text{ به پیمانهٔ}). \qquad (۴.۳.۷)$$

مثال.

$$۱۱\equiv -۵(\text{به‌پیمانهٔ } ۸),\quad ۸\equiv -۹(\text{به‌پیمانهٔ } ۸) \qquad (۵.۳.۷)$$

از جمع و تفریق این‌دو همنهشتی،

$$۱۸\equiv -۱۴(\text{به‌پیمانهٔ } ۸),\quad ۴\equiv ۴(\text{به‌پیمانهٔ } ۸)$$

که واقعاً دوهمنهشتی هستند، به‌دست می‌آیند.

همچنین دو همنهشتی را می‌توان درهم ضرب کرد. از (۱.۳.۷) و (۲.۳.۷) نتیجه می‌شود

$$ac = bd + m(kd + bl + mkl),$$

پس

$$ac \equiv bd (m \text{ به پیمانهٔ}) \qquad (۶.۳.۷)$$

مثال. از ضرب دوهمنهشتی (۵.۳.۷) به‌دست می‌آید

$$۷۷ \equiv ۴۵ (\text{به‌پیمانهٔ } ۸) .$$

همنهشتی

$$a \equiv b \ (m \text{ به پیمانهٔ})$$

را می‌توان درهرعدد صحیح c ضرب کرد:

$$ac \equiv bc (m \text{ به‌پیمانهٔ}) . \qquad (۷.۳.۷)$$

این‌را می‌توانیم حالتی از ضرب (۶.۳.۷)، یعنی حالت $c = d$، فرض کنیم؛ یا آن را مستقیماً از تعریف همنهشتی نتیجه بگیریم.

مثال. از ضرب همنهشتی اول (۵.۳.۷) در ۳، همنهشتی زیر به‌دست می‌آید

$$۳۳ \equiv -۱۵ (\text{به پیمانهٔ } ۸) .$$

این سؤال طبیعتاً پیش می‌آید که در چه حالتی می‌توانیم در (۷.۳.۷) عامل مشترك c را حذف کنیم و همنهشتی

$$a \equiv b (m \text{ به‌پیمانهٔ}) ,$$

که به‌دست می‌آید صحیح باشد. در اینجا همنهشتی با معادله یکسان نیست. مثلا از حذف دوعامل مشترك ۲ در همنهشتی

$$۲۲ \equiv -۲ (\text{به پیمانهٔ } ۸)$$

همنهشتی

$$۱۱ \equiv -۱ (\text{به‌پیمانهٔ } ۸)$$

به‌دست می‌آید که حقیقت ندارد.

درحالت مهم زیر حذف عامل مشترك جایز است:

اگر (m به‌پیمانهٔ $ac\equiv bc$) و m و c متباین باشند، آن‌گاه (m به‌پیمانهٔ $a\equiv b$).

برهان. همنهشتی اول به‌این معنی است که

$$ac-bc=(a-b)c=mk.$$

از $(m, c)=1$، برطبق قاعدهٔ تقسیمی که در بخش ۲.۴ صفحهٔ ۴۳ ثابت کردیم، نتیجه می‌شود که $a-b$ بر m تقسیم‌پذیر است.

مثال. در همنهشتی

$$۴\equiv ۴۸ \quad (\text{به پیمانهٔ } ۱۱)$$

می‌توانیم عامل ۴ را حذف کنیم، زیرا $(۴, ۱۱)=۱$. به‌دست می‌آید

$$۱\equiv ۱۲ \quad (\text{به‌پیمانهٔ } ۱۱).$$

مجموعهٔ مسائل ۳.۷

مثالهایی برای قاعده‌های همنهشتی که در بالا آورده‌ایم، بسازید.

۴.۷ توانهای همنهشتیها

بازهم همنهشتی

$$a\equiv b \quad (\text{به پیمانهٔ } m)$$

را در نظر می‌گیریم. دیدیم که می‌توانیم این همنهشتی را در خودش ضرب کنیم و همنهشتی

$$a^۲\equiv b^۲ \quad (\text{به پیمانهٔ } m),$$

را به‌دست آوریم. به‌طور کلی اگر n عددی صحیح و مثبت باشد، می‌توانیم آنقدر همنهشتی را درخودش ضرب کنیم تا

$$a^n\equiv b^n \quad (\text{به‌پیمانهٔ } m)$$

به‌دست آید.

مثال. از مربع کردن

$$۸ \equiv -۳ \text{ (به پیمانهٔ ۱۱)}$$

همنهشتی

$$۶۴ \equiv ۹ \text{ (به پیمانهٔ ۱۱)}$$

و از به‌توان ۳ رساندن آن

$$۵۱۲ \equiv -۲۷ \text{ (به پیمانهٔ ۱۱)}$$

نتیجه می‌شود.

بسیاری‌از مطالب همنهشتیها به‌پیداکردن باقیمانده‌های توانهای بزرگ‌اعداد مربوط هستند. ببینیم چطور می‌توان عمل کرد. مثلا فرض کنید می‌خواهیم باقیماندهٔ

$$۳^{۸۹} \text{ (به پیمانهٔ ۷)}$$

را پیداکنیم. از راه مجذورهای مکرر عمل می‌کنیم:

$$۹ = ۳^۲ \equiv ۲ \text{ (به پیمانهٔ ۷)}$$

$$۳^۴ \equiv ۴$$

$$۳^۸ \equiv ۱۶ \equiv ۲$$

$$۳^{۱۶} \equiv ۴$$

$$۳^{۳۲} \equiv ۱۶ \equiv ۲$$

$$۳^{۶۴} \equiv ۴ \text{ (به پیمانهٔ ۷)}.$$

از

$$۸۹ = ۶۴ + ۱۶ + ۸ + ۱ = ۲^۶ + ۲^۴ + ۲^۳ + ۱$$

نتیجه می‌شود

$$۳^{۸۹} = ۳^{۶۴}.۳^{۱۶}.۳^۸.۳ \equiv ۴.۴.۲.۳ \equiv ۵ \text{ (به پیمانهٔ ۷)}.$$

پس باقیماندهٔ (به‌پیمانهٔ ۷)، ۵ است؛ به‌عبارت‌دیگر بنابرآنچه دربخش ۲.۷ گفتیم، در دستگاه به‌پایهٔ ۷، آخرین رقم $۳^{۸۹}$، ۵ است.

درواقع برای‌پیداکردن‌باقیمانده، نمای $۳^{۸۹}$، یعنی ۸۹، را در دستگاه دودویی نوشتیم:

$$۸۹ = ۲^۶ + ۲^۴ + ۲^۳ + ۱ = (۱, ۰, ۱, ۱, ۰, ۰, ۱)_۲$$

و باقیمانده‌های (به پیمانه ۷) اعداد ۳، $۳^۲$ (مربع ۳)، $۳^۴$ (مربع $۳^۲$)، $۳^{۶۴}$، ... (مربع $۳^{۳۲}$) را به‌دست آوردیم. همواره نظیر این روش را می‌توان به‌کار برد. اما درحالتهای‌خاص اغلب با تیزبینیهایی می‌توان‌عمل‌را بسیار ساده‌کرد. مثلا درحالت بالا می‌بینیم که

$$۳^۳ \equiv -۱ \quad (\text{به‌پیمانهٔ } ۷),$$

$$۳^۶ \equiv ۱ \quad (\text{به‌پیمانهٔ } ۷),$$

و نتیجه می‌گیریم که

$$۳^{۸۴} = (۳^۶)^{۱۴} \equiv ۱ \quad (\text{به‌پیمانهٔ } ۷).$$

بنابراین، نتیجهٔ قبلی به‌صورت زیر به‌دست می‌آید:

$$۳^{۸۹} = ۳^{۸۴}.۳^۳.۳^۲ \equiv ۱.(-۱).۲ = -۲ \equiv ۵ \quad (\text{به پیمانهٔ } ۷)$$

به‌عنوان مثالی دیگر، اعداد فرما:

$$F_t = ۲^{۲^t} + ۱,$$

را که در بخش ۳.۲ معرفی کردیم، در نظر می‌گیریم. اگر به‌نخستین پنج عدد فرما

$$F_۰ = ۳, \quad F_۱ = ۵, \quad F_۲ = ۱۷, \quad F_۳ = ۲۵۷, \quad F_۴ = ۶۵۵۳۷$$

توجه کنیم، حدس می‌زنیم که شاید اعداد فرما، جز $F_۰$ و $F_۱$، در دستگاه دهدهی به رقم ۷ ختم شوند.

اینك با همنهشتیها ثابت می‌کنیم که این‌حدس درست است. باید ثابت کنیم که اعداد

$$۲^{۲^t}, \quad t = ۲, \quad ۳, \ \ldots$$

به‌رقم ۶ ختم می‌شوند. می‌بینیم که

$$۲^{۲۲} = ۱۶ \equiv ۶ \quad (\text{به‌پیمانهٔ } ۱۰)$$

$$۲^{۲۳} = ۲۵۶ \equiv ۶ \quad (\text{به‌پیمانهٔ } ۱۰)$$

$$۲^{۲^۴} = ۶۵۵۳۶ \equiv ۶ (\text{به‌پیمانهٔ } ۱۰).$$

علاوه‌براین، مربع $۲^{۲^k}$ برابر است با

$$(۲^{۲^k})^۲ = ۲^{۲\cdot ۲^k} = ۲^{۲^{k+۱}}.$$

فرض کنید برای یك مقدار t

$$۲^{۲^t} \equiv ۶ (\text{به‌پیمانهٔ } ۱۰),$$

این همنهشتی را مربع کرده به‌نتیجهٔ مطلوب می‌رسیم:

$$۲^{۲^{t+۱}} \equiv ۳۶ \equiv ۶ (\text{به پیمانهٔ } ۱۰)$$

۵.۷ همنهشتی فرما

قانون دوجمله‌ای

$$\begin{aligned} x+y &= x+y \\ (x+y)^۲ &= x^۲+۲xy+y^۲ \\ (x+y)^۳ &= x^۳+۳x^۲y+۳xy^۲+y^۳ \\ (x+y)^۴ &= x^۴+۴x^۳y+۶x^۲y^۲+۴xy^۳+y^۴ \end{aligned} \qquad (۱.۵.۷)$$

و به‌طور کلی

$$(x+y)^p = x^p + \binom{p}{۱}x^{p-۱}y + \binom{p}{۲}x^{p-۲}y^۲ + \dots + y^p \qquad (۲.۵.۷)$$

را که در جبر خوانده‌اید به‌خاطر بیاورید. ضرایب جمله‌های اول و آخر ۱ است و ضریبهای جمله‌های دیگر

$$\binom{p}{۱} = \frac{p}{۱}, \quad \binom{p}{۲} = \frac{p(p-۱)}{۱.۲}, \qquad (۳.۵.۷)$$
$$\binom{p}{۳} = \frac{p(p-۱)(p-۲)}{۱.۲.۳}, \dots,$$

و به‌طور کلی

$$\binom{p}{r}=\frac{p(p-1)(p-2)\dots(p-r+1)}{1\cdot2\dots r}, \qquad (۴.۵.۷)$$

$$r=1, 2, \dots, p-1,$$

هستند. روشن است که این ضریبها اعدادی صحیح‌اند، زیرا در (۱.۵.۷) نشان داده شده است که این ضریبها از ضریبهای متوالی $x+y$ درخودش به‌دست آمده‌اند.

از اینجا به بعد فرض می‌کنیم که p عدد اول است. برای به‌دست‌آوردن (۴.۵.۷) به‌صورت عددی صحیح، باید بین مخرج، یعنی

$$1\cdot2\dots r$$

و صورت، یعنی

$$p(p-1)\dots(p-r+1)$$

تمام عاملهای‌مشترک‌را حذف کنیم. اما درمخرج عامل اول p وجود ندارد، بنابراین پس‌از حذف عاملهای مشترک، p درصورت باقی می‌ماند. نتیجه می‌گیریم:

تمام ضرایب دوجمله‌ای (مگر اولی و آخری) در (۲.۵.۷)، اگر p اول‌باشد، بر p تقسیم‌پذیرند.

اکنون فرض‌می‌کنیم در (۲.۵.۷)، x و y اعدادی صحیح هستند. اگرفرمول (۲.۵.۷) را به‌صورت همنهشتی (به‌پیمانهٔ p) بنویسیم، می‌توانیم بگوییم

اگر x و y اعدادی صحیح باشند و p اول باشد

$$(x+y)^p\equiv x^p+y^p \ (\text{به‌پیمانهٔ } p). \qquad (۵.۵.۷)$$

مثلا p را ۵ می‌گیریم،

$$(x+y)^5=x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5.$$

چون ضریب تمام جمله‌ها، جز جمله‌های اولی و آخری، بر ۵ تقسیم‌پذیرند،

$$(x+y)^5\equiv x^5+y^5 \ (\text{به‌پیمانهٔ } 5),$$

که حالتی خاص از (۵.۵.۷) است.

نتایج مهمی از (۵.۵.۷) به‌دست می‌آیند. نخست درحالت $x=y=1$،

$$۲^p=(۱+۱)^p\equiv ۱^p+۱^p=۲ \quad (p\text{به پیمانهٔ})$$

بعد درحالت $x=۲$، $y=۱$،

$$۳^p=(۲+۱)^p\equiv ۲^p+۱^p,$$

یا پس‌از استفاده از نتیجهٔ (به‌پیمانهٔ p)$۲^p\equiv ۲$ که هم‌اکنون به‌دست آوردیم،

$$۲^p+۱^p\equiv ۲+۱\equiv ۳(p\text{ به‌پیمانهٔ}),$$

پس داریم (به‌پیمانهٔ p)$۳^p\equiv ۳$. بعد حالت $x=۳$، $y=۱$ را درنظر می‌گیریم،

$$۴^p\equiv ۴(p\text{ به‌پیمانهٔ})$$

به‌دست می‌آید. ازاین‌طریق می‌توانیم با استقرا ثابت‌کنیم‌که به‌ازای جمیع مقادیر

$$a=۰,\ ۱,\ \dots,\ p-۱, \qquad (۶.۵.۷)$$

(به پیمانهٔ p)$a^p\equiv a$. حالتهای خاص $a=۰$ و $a=۱$ واضح هستند. چون هرعدد با یکی از باقیمانده‌های (۶.۵.۷) همنهشت (به‌پیمانهٔ p) است، نتیجه می‌گیریم:

اگر a عددی صحیح و p عددی اول باشد،

$$a^p\equiv a(p\text{ به‌پیمانهٔ}). \qquad (۷.۵.۷)$$

این قانون همنهشتی به‌قضیهٔ فرما معروف است، گرچه بعضی برای تشخیص‌دادن این قانون از آخرین‌قضیه یاحدس‌فرما، که در بخش ۳.۵ به‌آن اشاره‌کردیم، (۷.۵.۷) را قضیهٔ کوچك فرما می‌نامند.

مثال. فرض کنید $p=۱۳$ و $a=۲$. از $۱۳=۸+۴+۱$،

$$۲^{۱۳}=۲^{۸+۴+۱}=۲^۸.۲^۴.۲^۱$$

نتیجه می‌شود. چون

$$۲^۴=۱۶\equiv ۳(\text{به‌پیمانهٔ }۱۳),\quad ۲^۸\equiv ۹(\text{به‌پیمانهٔ }۱۳),$$

پس

$$۲^{۱۳}=۲^۸.۲^۴.۲\equiv ۹.۳.۲\equiv ۲(\text{به‌پیمانهٔ }۱۳)$$

که باحکم قضیهٔ فرما مطابقت دارد.

برطبق قانون حذف که در آخر بخش ۳.۷ آمده است، اگر a و پیمانهٔ p متباین باشند، می‌توان عامل مشترک a را از دوطرف همنهشتی (۷.۵.۷) فرما حذف کرد. نتیجهٔ زیرکه آن‌هم به قضیهٔ فرما معروف است به‌دست می‌آید:

اگر a برعدد اول p تقسیمپذیر نباشد، آن‌گاه

$$a^{p-1} \equiv 1 \ (p \text{ به‌پیمانهٔ }) . \qquad (۸.۵.۷)$$

مثال. فرض کنید $a = ۷$، $p = ۱۹$، داریم

$$۷^۲ = ۴۹ \equiv ۱۱ \ (\text{به‌پیمانهٔ } ۱۹)$$

$$۷^۴ \equiv ۱۲۱ \equiv ۷ \ (\text{به‌پیمانهٔ } ۱۹)$$

$$۷^۸ \equiv ۴۹ \equiv ۱۱ \ (\text{به‌پیمانهٔ } ۱۹)$$

$$۷^{۱۶} \equiv ۱۲۱ \equiv ۷ \ (\text{به‌پیمانه } ۱۹) .$$

از این همنهشتیها نتیجه می‌شود

$$a^{p-1} = ۷^{۱۸} = ۷^{۱۶} . ۷^۲ \equiv ۷ . ۱۱ \equiv ۱ \ (\text{به‌پیمانهٔ } ۱۹)$$

که با همنهشتی (۸.۵.۷) فرما سازگار است.

برمی‌گردیم به‌مثلثهای فیثاغورسی فصل پنجم و به‌عنوان کاربردی از همنهشتی (۸.۵.۷) فرما ثابت می‌کنیم که:

حاصلضرب اضلاع مثلث فیثاغورسی بر ۶۰ تقسیمپذیر است.

برهان. واضح است که کافی است قضیه را برای مثلثهای اولیه ثابت کنیم. برطبق فرمول (۷.۲.۵)، P، حاصلضرب اضلاع برابر است با:

$$P = ۲mn(m^۲ - n^۲)(m^۲ + n^۲) = ۲mn(m^۴ - n^۴) .$$

P بر ۶۰ تقسیمپذیر است اگر وتنها اگر بر ۴ و ۳ و ۵ تقسیمپذیر باشد. چون یکی از دو عدد m و n زوج است، $۲mn$ بر ۴ تقسیمپذیر است. اگر m یا n بر ۳ تقسیمپذیر باشد، P بر ۳ تقسیمپذیر است؛ درحالتی هم که m و n بر ۳ تقسیمپذیر نیستند باز هم P بر ۳ تقسیمپذیر است، زیرا $(m, ۳) = ۱$ و $(n, ۳) = ۱$ و بنابر (۸.۵.۷)، $m^۲ \equiv ۱ \ (\text{به‌پیمانهٔ } ۳)$ و $n^۲ \equiv ۱ \ (\text{به‌پیمانهٔ } ۳)$، پس

$$m^۲ - n^۲ \equiv ۱ - ۱ \equiv ۰ \quad (\text{به‌پیمانهٔ } ۳).$$

P بر ۵ هم تقسیم‌پذیر است: واضح است که اگر m یا n بر ۵ تقسیم‌پذیر باشد، P بر ۵ تقسیم‌پذیر است. اگر m و n بر ۵ تقسیم‌پذیر نباشند، باز از همنهشتی (۸.۵.۷) فرما نتیجه می‌شود

$$m^۴ - n^۴ \equiv ۱ - ۱ \equiv ۰ \quad (\text{به‌پیمانهٔ } ۵).$$

فصل ۸

چند کاربرد همنهشتیها

۱۰۸ امتحان درستی محاسبات

گفتیم که واضع نظریهٔ همنهشتی، گاوس ریاضیدان آلمانی بود. اثر مشهورش دربارهٔ نظریهٔ اعداد به‌نام مطالعاتی در حساب[1]، وقتی بیست و چهار سال داشت، در سال ۱۸۰۱ منتشر شد. مطالعاتی در حساب اخیراً به‌زبان انگلیسی ترجمه شده است[2]، پس اگر به خواندن قسمتهایی از یکی از شاهکارهای ریاضیات علاقه‌مند باشید، امکان آن را دارید. فصلهای اول به نظریهٔ همنهشتی مربوط می‌شود و شما اکنون دربارهٔ همنهشتیها آنقدر می‌دانید که بتوانید طرز بیان گاوس را درک کنید.

اما ناگفته نماند که ازچندقرن پیش از زمان گاوس، آثاری ازنظریهٔ همنهشتی دیده‌می‌شود. بعضی‌ازاینها، قاعده‌های قدیمی امتحان درستی محاسبات درحساب‌اند. این قاعده‌ها، قسمت مهمی از تدریس حساب در دورهٔ رنسانس را تشکیل می‌داده است. بعضی‌از این قاعده‌ها هنوز به‌کار می‌روند، وتنها چیزی که راجع به‌مبدأ آنها می‌دانیم این است که احتمال دارد ریشهٔ آنها در زمان باستان باشد.

نمی‌دانیم در اوایل چگونه وارد حساب شده‌اند، اما می‌خواهیم به راهی

---

1. Disquisitiones Arithmeticae

۲. از انتشارات Yale University Press

پذیرفتنی که امکان‌دارد ازآن راه‌کشف شده باشند، اشاره‌کنیم. برمی‌گردیم به‌عقب، به زمانهای تخته‌های محاسبه. روی این تخته‌ها هررقم عددهایی که برای محاسبات لازم بودند به‌وسیلهٔ شمارنده‌ها یاسنگها یا چوبها یا مهره‌ها چیده می‌شدند،هرگروه، تعدادیکانها، دهگانها، صدگانها، وغیره‌را برحسب مکانشان نشان‌می‌داد. در دستگاه دهدهی عدد

$$N=a_n\cdot 10^n+a_{n-1}\cdot 10^{n-1}+\cdots+a_2\cdot 10^2+a_1\cdot 10+a_0 \quad (1.1.8)$$
$$=(a_n,\ a_{n-1},\ \cdots,\ a_2,\ a_1,\ a_0)_{10}$$

تعداد

$$S_N=a_n+a_{n-1}+\cdots+a_2+a_1+a_0 \quad (2.1.8)$$

شمارنده لازم دارد. S_N را مجموع رقمهای N می‌نامیم.

حال فرض‌کنید می‌خواهیم یك‌عمل‌ساده روی‌تخته انجام دهیم، یعنی عدد M را با N جمع کنیم. عدد دوم

$$M=(b_m,\ b_{m-1},\ \cdots,\ b_1,\ b_0)_{10}$$

را نیز روی تخته با

$$S_M=b_m+b_{m-1}+\cdots+b_2+b_1+b_0$$

شمارندهٔ دیگر روی همان خطها نشان می‌دهیم. حالا ممکن است روی بعضی‌ازخطها بیش‌از نه شمارنده باشد. عمل به‌دست‌آوردن $N+M$ به‌این‌طریق انجام‌می‌شود‌که به‌جای هرده شمارندهٔ یك خط، یك شمارنده روی خط بعدی بگذاریم وآنقدر ادامه دهیم‌که دیگر چنین‌عملی امکانپذیر نباشد. درهرمرحله به‌جای ده‌شمارنده یك‌شمارنده می‌گذاریم، پس هربار نه‌شمارندهٔ تخته‌کم می‌شود، پس اگر عمل‌جمع درست‌انجام شود، می‌بینیم که تعداد شمارنده‌هایی‌که روی تخته باقی مانده است باید در رابطهٔ

$$S_{N+M}\equiv S_N+S_M \quad (\text{به‌پیمانهٔ } 9) \quad (3.1.8)$$

صدق کند، یعنی اختلاف تعداد شمارنده‌های باقی مانده روی تخته، با تعداد کل شمارنده‌های‌اولیه باید مضربی از ۹ باشد. این امتحان درستی (۳.۱.۸) را هنوز به نام قدیمش طرح نه‌نهی می‌نامند.

بعدازکشف این‌قاعده احتمالاً به‌زودی متوجه‌شده‌اندکه قاعده‌را برای‌مجموع

چند عدد، تفاضل وضرب نیز می‌توان به‌کار برد؛ درحالت اخیر داریم

$$S_M \cdot S_N \equiv S_{MN} \text{(به‌پیمانهٔ ۹)} \qquad (۴.۱.۸)$$

که نظیر رابطهٔ (۳.۱.۸) است.

اگر همنهشتیها را به‌کار بگیریم، اثبات این قاعده‌ها از راه نظری ساده‌است. واضح است که

$$۱ \equiv ۱,\ ۱۰ \equiv ۱,\ ۱۰^۲ \equiv ۱,\ ۱۰^۳ \equiv ۱, \ldots \text{(به‌پیمانهٔ ۹)}, \qquad (۵.۱.۸)$$

پس‌از (۱.۱.۸) و (۲.۱.۸) نتیجه می‌گیریم

$$N \equiv S_N \text{(به‌پیمانهٔ ۹)} \qquad (۶.۱.۸)$$

بنابراین اگر قاعده‌های همنهشتی راکه در بخش ۳.۷ اثبات کرده‌ایم، به‌کار بریم واضح است که

$$S_M \pm S_N \equiv N \pm M \equiv S_{N \pm M},\ S_N \cdot S_M \equiv N \cdot M \equiv S_{N \cdot M} \text{(به‌پیمانهٔ ۹)}.$$

طرح نه نهی را بیشتر برای امتحان عمل‌ضرب به‌کار می‌برند. به‌عنوان مثال دو عدد

$$M = ۳۱۱۹, \quad N = ۳۷۲۴ \qquad (۷.۱.۸)$$

و حاصلضرب

$$M \cdot N = ۱۱۶۱۴۱۵۶$$

را درنظر بگیرید. این محاسبه درست نیست، زیرا

$$M \equiv S_M = ۳+۱+۱+۹ \equiv ۵ \text{(به‌پیمانهٔ ۹)},$$

$$N \equiv S_N = ۳+۷+۲+۴ \equiv ۷ \text{(به‌پیمانهٔ ۹)},$$

و

$$MN \equiv S_{MN} = ۱+۱+۶+۱+۴+۱+۵+۶ \equiv ۷ \text{(به‌پیمانهٔ ۹)}.$$

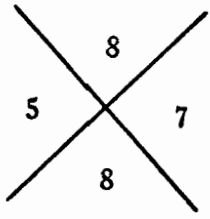
اما

$$۵ \cdot ۷ = ۳۵ \equiv ۸ \not\equiv ۷ \text{(به‌پیمانهٔ ۹)}.$$

درواقع

$$M.N = ۱۱۶۱۵۱۵۶۰$$

درمدارس قرون‌وسطی به‌شاگردان تأکید می‌کردندکه درتمرینهایشان امتحان درستی محاسبات را بنویسند. به‌طوری‌که در دستنویسهای آن زمانها مجموعه‌ای از علامتهای صلیب‌گونه (شبیه به‌علامت خطر مرگ) درنوشته‌ها دیده می‌شود. در مثال (۷.۱.۸) امتحان درستی به‌صورت



شکل ۱.۱.۸

نوشته می‌شده است. ۵ و ۷ که در سمت چپ و راست نوشته شده‌اند، باقیمانده‌های M و N (به‌پیمانهٔ ۹) هستند و عدد ۸ در قسمت بالا، باقیماندهٔ حاصلضرب $M.N$ است. باقیماندهٔ حاصلضرب دوباقیمانده درقسمت پایین نوشته می‌شود و باید با عدد قسمت بالا برابر باشد. دراین مثال

$$۵.۷ = ۳۵ \equiv ۸ \quad (\text{به‌پیمانهٔ } ۹)$$

این علامت امتحان صلیب‌گونه، مانند شکل ۱.۱.۸ درکتابهای حساب چاپ قدیم، مانندکتابهای انگلیسی قرنهای‌هفدهم وهجدهم، زیاد دیده می‌شوند. البته ممکن‌است در محاسبه خطایی باشدکه با روش طرح نه‌نهی مشخص نشود؛ اما در این صورت می‌دانیم‌که اشتباه یك «خطای به‌پیمانهٔ ۹» است.

روشن است‌که شبیه این امتحان درستی‌را درپایه‌های دیگرهم می‌توان به‌کار برد. برای عدد

$$M = m_n b^n + m_{n-۱} b^{n-۱} + \cdots + m_۲ b^۲ + m_۱ b + m_۰$$

درپایهٔ b، مانند (۵.۱.۸)، داریم

$$۱ \equiv ۱,\ b \equiv ۱,\ b^۲ \equiv ۱,\ \ldots (b-۱ \text{ به‌پیمانهٔ});$$

پس مانند قبل

$$M \equiv S_M = m_n + m_{n-1} + \cdots + m_2 + m_1 + m_0 \ (\text{به‌پیمانهٔ } b-1),$$

و همان قاعده‌های امتحان درستی معتبر هستند.

این تذکار کـه خیلی بی‌ارزش به نظر می‌رسد، کاربردهایی حتی در دستگاه دهدهی دارد. دربخش ۵.۷ اشاره کردیم که اگر رقمهارا به‌گروههای سه‌تایی ازهم جداکنیم، این گروه‌بندی را می‌توانیم بسط عدد درپایهٔ

$$b = 10^3 = 1000$$

تصور کنیم. همچنین تقسیم‌رقمها به‌گروههای‌دوتایی، متناظر است با بسط عدد درپایهٔ

$$b = 10^2 = 100.$$

دوباره اعداد ۳۱۱۹ و ۳۷۲۴ را مثال می‌زنیم و می‌نویسیم

$$M = 31\ 19, \quad N = 37\ 24$$

$$M.N = 11\ 61\ 51\ 56,$$

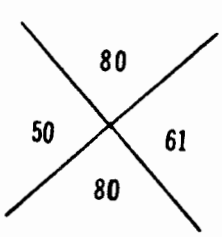
همنهشتیهای زیر به‌دست می‌آیند

$$M \equiv 31 + 19 = 50 \ (\text{به‌پیمانهٔ } 99),$$

$$N \equiv 37 + 24 = 61 \ (\text{به‌پیمانهٔ } 99),$$

$$M.N \equiv 11 + 61 + 51 + 56 = 179 \equiv 80 \ (\text{به‌پیمانهٔ } 99)$$

در اینجا صلیب امتحانی به‌صورت زیر است



زیرا دیده می‌شود که

Rechnung auff der Linien vnnd Federn/

Auff allerley Handtierung/

Gemacht durch

Adam Riesen.

obal 1559

Auffs new mit fleis durchlesen/ vnd zu recht bracht.

Gedruckt zu Magdeburgk/ In verlegung Johan Francken.

$$۵۰.۶۱ \equiv ۸۰ \ (\text{به‌پیمانهٔ } ۹۹).$$

این امتحان درستی چون با پیمانهٔ بزرگتری عمل می‌شود، احتمال اینکه جواب درست باشد بیشتر از احتمال درستی درطرح نه‌نهی است. به‌عبارت دیگر، «خطای به‌پیمانهٔ ۹۹» کمتر از «خطای به‌پیمانهٔ ۹» است.

۲.۸ روزهای هفته

بسیاری از مسائل نجوم و «زمانشناسی» که در آنها تناوب وجود دارد، برحسب مفهومهای نظریهٔ اعداد بیان می‌شوند. ما در اینجا به ذکر یک مثال اکتفا می‌کنیم: تعیین کنید تاریخی مفروض با چه روزی از هفته منطبق می‌شود. روزهای هفته، هرهفت روز یک‌بار تکرار می‌شوند، پس می‌توانیم به جای نامهای معمول، هر روز هفته را با اعداد زیر مشخص کنیم[۱].

یکشنبه = ۰، دوشنبه = ۱، سه‌شنبه = ۲، چهارشنبه = ۳، پنجشنبه = ۴، جمعه = ۵، شنبه = ۶.

به‌این‌ترتیب اگر هرعدد صحیح را با باقیمانده‌اش (به‌پیمان ۷) نظیر کنیم، هرعدد با یک روز از هفته منطبق می‌شود[۲].

اگر در وضع خوشایندی بودیم که تعداد روزهای سال بر ۷ تقسیم‌پذیر بود، هرتاریخی، در تمام سالها با روزی مشخص از هفته منطبق می‌شد، برنامه‌ریزی ساده می‌شد و بازارکار ناشرین تقویم رواجی نمی‌داشت. اما تعداد روزهای سال

$$۳۶۵ \equiv ۱ \ (\text{به‌پیمانهٔ } ۷),$$

و درسالهای کبیسه

$$۳۶۶ \equiv ۲ \ (\text{به‌پیمانهٔ } ۷).$$

این نشان می‌دهدکه اگر W شمارهٔ روز هفتهٔ تاریخی مشخص در یک سال معمولی باشد، در سال بعد شمارهٔ روز هفتهٔ آن تاریخ، $W+۱$ خواهد بود؛ مثلا اگر در سالی اول ژانویه روز یکشنبه باشد، سال بعد روز دوشنبه است: این زیاد

---

۱. دراین مبحث این اعداد را «شماره‌های روزهای هفته» خواهیم گفت.ـم.

۲. مثلا ۲۳ باروز سه‌شنبه = ۲ منطبق می‌شود، زیرا $۲۳ \equiv ۲ \ (\text{به‌پیمانهٔ } ۷)$.ـم.

پیچیده نیست، اما سالهای کبیسه این الگورا بهم می‌زنند. درهرچهارسال، یك سال کبیسه است، واگر سال کبیسه باشد، درسال بعد شمارهٔ روزهفته $W+2$ خواهد شد. اشکال دیگری که وجود دارد این است که روز کبیسه به اول یا آخر سال اضافه نمی‌شود[1]، بلکه در بیست ونهم فوریه یك روز به سال اضافه می‌شود. این مارا برآن می‌دارد که مارس را ماه اول سال، آوریل را ماه دوم سال بگیریم، به همین ترتیب پیش برویم و ژانویه را ماه یازدهم، فوریه را ماه دوازدهم سال قبل به حساب آوریم.

اما اشکالات به پایان نرسیده‌اند. در تقویم قیصری، که به فرمان قیصر روم، یولیوس معمول شد، سال دقیقاً $365\frac{1}{4}$ روز حساب شده است، که با یك سال کبیسه در چهارسال مطابقت دارد. اما این کاملا درست نیست، زیرا سال نجومی واقعاً

روز ۳۶۵٫۲۴۲۲

است. این خطای کوچك موجب شد فصلها به‌تدریج در رابطه با تقویم تغییر کنند؛ مثلا درقرن شانزدهم اعتدال ربیعی (روز اول بهار) به ۱۱ مارس افتاد، درصورتی که انتظار می‌رفت ۲۱ مارس باشد.

برای رفع این گرفتاری، پاپ گرگوری سیزدهم بعد از تردید زیاد، درسال ۱۵۸۲ برای کشورهای کاتولیك، تقویم را اصلاح کرد. از آن سال ده روز حذف کردند وجمعهٔ پنجم اکتبر را جمعهٔ پانزدهم اکتبر گرفتند. علاوه‌براین، برای همگام‌کردن تقویم بازمان، قاعده‌های گرگوری را که در زیر می‌آیند، برای سالهای کبیسه برقرار کردند.

سالهای قرنی

۱۷۰۰, ۱۸۰۰, ۱۹۰۰, ۲۱۰۰, ۲۲۰۰, ۲۳۰۰, ...

که تعداد قرنهای آنها بر ۴ تقسیم‌پذیر نیستند، سالهای کبیسه نیستند. بقیهٔ سالهای قرنی، یعنی

۱۶۰۰, ۲۰۰۰, ۲۴۰۰, ...

سالهای کبیسه هستند. با این قاعده‌ها، تقریبی خیلی خوب برای طول سال به‌دست می‌آید ولی طول سال کمی کمتر از این تقریب است. پیشنهاد شده است که برخلاف قاعدهٔ گرگوری ۴۰۰۰، ۸۰۰۰، ... را سالهای کبیسه نگیرند؛ چون هنوز تصمیم

---

۱. این اشکال در تقویم ایرانی وجود ندارد.ـم.

قطعی در این باره اتخاذ نشده‌است و این پیشنهاد به آینده‌ای نزدیک‌هم مربوط نمی‌شود، آن را در فرمولی که موردبحث است به‌حساب نمی‌آوریم.

اینک فرض کنید می‌خواهیم بدانیم روز dام از ماه mام سال N چه‌روزی‌از هفته است. عدد m درسال N به‌طریقی که در صفحهٔ ۱۰۷ شرح دادیم حساب شده است. سال N را به‌صورت

$$N=G.100+Y, \qquad (1.2.8)$$

می‌نویسیم؛ C تعداد قرنها و Y تعداد سالها درآن قرن است. می‌توان ثابت کرد که W، عدد روز هفته، با همنهشتی

$$W=d+\left[\frac{1}{5}(13m-1)\right]+Y+\left[\frac{1}{4}Y\right]+\left[\frac{1}{4}C\right]-2C \quad (\text{به‌پیمانهٔ } 7)$$

$$(2.2.8)$$

به دست می‌آید. یادآوری می‌کنیم کـه در بخش ۳.۴ کروشه‌ها را که در فرمولها می‌آیند، بزرگترین عددصحیحی که ازعدد داخل کروشه بزرگتر نیست تعریف کردیم.

مثال. روز پیرل‌هاربور، هفتم‌دسامبر ۱۹۴۱. دراینجا $d=7$، $m=10$، $C=19$، $Y=41$. پس،

$$W\equiv 7+25+41+10+4-38\equiv 0 \quad (\text{به‌پیمانهٔ } 7).$$

یعنی روز پیرل هاربور یکشنبه بوده است.

مثال. اول ژانویهٔ سال ۲۰۰۰ چه روزی ازهفته است؟ دراینجا $d=1$، $m=11$، $C=19$، $Y=99$ و

$$W\equiv 1+28+1+3+4-38=6 \quad (\text{به‌پیمانهٔ } 7).$$

بنابراین اولین روز قرن آینده شنبه است.

در ارتباط با این محاسبات باید توجه شودکـه فرمول را نمی‌توان درمورد زمان قبل از شروع تقویم گرگوری بـه‌کار بـرد. درانگلستان و مستعمراتش تقویم گرگوری از سال ۱۷۵۲، که با تبدیل کردن سوم سپتامبر به‌چهاردهم سپتامبر، یازده روز از سال‌را حذف کردند، به‌روش جدید آغاز شد.

ممکن است مایل باشید به تفصیل بدانید که فرمول (۲.۲.۸) چگونه به‌دست آمده است. درغیراین‌صورت از بقیهٔ این بخش بگذرید. تحلیل فرمول‌را به‌دومرحله تقسیم می‌کنیم.

درمرحلهٔ اول «شمارهٔ روز هفتهٔ» اول مارس را درهرسال N تعیین می‌کنیم؛ N بافرمول (۱:۲.۸) مشخص‌شده‌است.سال‌شروع‌را به‌دلخواه، مثلا ۱۶۰۰، انتخاب می‌کنیم وشمارهٔ روز هفتهٔ آن را d_{1600} می‌نامیم. می‌توانستیم در نوشته‌های قدیمی پیداکنیم d_{1600} شمارهٔ چه روزی از هفته بوده است، ولی به‌این‌کار نیازنیست؛ این روز از فرمولی‌که به‌دست خواهیم آورد، نتیجه خواهد شد.

اگر سالهای کبیسه وجود نداشتند، d_N «روز هفتهٔ» اول مارس درسال N با افزودن یك روز به d_{1600} به‌ازای هرسالی‌که گذشته است، به‌دست می‌آمد. با این عمل عدد

$$d_{1600}+(100C+Y-1600) \quad (\text{به‌پیمانهٔ } 7) \qquad (۳.۲.۸)$$

حاصل می‌شود. حال سالهای‌کبیسه را به‌حساب می‌آوریم و فرض می‌کنیم فاصلهٔ دو سال‌کبیسهٔ متوالی ۴ سال است، پس باید به (۳.۲.۸) عدد

$$\left[\frac{1}{4}(100C+Y-1600)\right]=25C-400+\left[\frac{1}{4}Y\right] \qquad (۴.۲.۸)$$

را بیفزاییم. این عددکمی زیاد است، زیرا سالهای قرن معمولا کبیسه نیستند، پس باید از (۳.۲.۸).

$$C-16 \qquad (۵.۲.۸)$$

روزکم‌کنیم. اماگفتیم اگر قرن C بر ۴ تقسیمپذیر باشد، سال $100C$ کبیسه است، پس تصحیح نهائی این است‌که عدد

$$\left[\frac{1}{4}(C-16)\right]=\left[\frac{1}{4}C\right]-4 \qquad (۶.۲.۸)$$

را به‌آن اضافه‌کنیم.

اینك‌عبارتهای (۳.۲.۸) و (۴.۲.۸) را باهم جمع می‌کنیم، (۵.۲.۸) را از مجموع کم می‌کنیم و (۶.۲.۸) را به‌آن می‌افزاییم. به‌این ترتیب روز هفتهٔ اول مارس سال N به‌دست می‌آید

$$d_N \equiv d_{۱۶۰۰} + ۱۲۴C + Y - ۱۹۸۸ + \left[\frac{۱}{۴}C\right] + \left[\frac{۱}{۴}Y\right] \text{(به پیمانهٔ ۷)}.$$

در این عبارت اعداد را (به‌پیمانهٔ ۷) ساده می‌کنیم، عبارت زیر نتیجه می‌شود

$$d_N \equiv d_{۱۶۰۰} - ۲C + Y + \left[\frac{۱}{۴}C\right] + \left[\frac{۱}{۴}Y\right] \text{(به‌پیمانه ۷)}. \quad (۷.۲.۸)$$

این فرمول را برای سال $N = ۱۹۶۸$ که می‌دانیم اول مارس به‌روز جمعه می‌افتد به‌کار می‌بریم؛ بنابراین $d_{۱۹۶۸} = ۵$. در اینجا

$$C = ۱۹, \quad \left[\frac{۱}{۴}C\right] = ۴, \quad Y = ۶۸, \quad \left[\frac{۱}{۴}Y\right] = ۱۷,$$

واز (۷.۲.۸) به‌دست می‌آید

$$d_{۱۹۶۸} = ۵ \equiv d_{۱۶۰۰} + ۲ \text{(به‌پیمانهٔ ۷)}.$$

پس $d_{۱۶۰۰} \equiv ۳$، یعنی اول‌مارس سال ۱۶۰۰ روز چهارشنبه بوده است، وازفرمول (۷.۲.۸) به

$$d_N \equiv ۳ - ۲C + Y + \left[\frac{۱}{۴}C\right] + \left[\frac{۱}{۴}Y\right] \text{(به پیمانهٔ ۷)} \quad (۸.۲.۸)$$

که روز هفتهٔ اول مارس سال N را مشخص می‌کند، می‌رسیم.

در مرحلهٔ دوم، باید تعداد روزهای بین اول مارس و هرروز دیگر سال (به پیمانهٔ ۷) را تعیین کنیم. چون تعداد روزهای ماههای مختلف، متفاوت هستند باید راهی برای بیان جمعها به صورت ریاضی پیدا کرد. نخست تعیین می‌کنیم برای پیداکردن شمارهٔ روز هفتهٔ اولین روز یکی از ماهها، چند روز باید به شمارهٔ روز هفتهٔ اول مارس افزود.

چون مارس ۳۱ روز است، باید به‌روز اول مارس ۳ روز بیفزاییم تاشمارهٔ روز اول آوریل به‌دست‌آید؛ برای‌پیداکردن روز اول‌مه باید ۲ + ۳ روزبیفزاییم، زیرا آوریل ۳۰ روز است. اگر به‌همین ترتیب عمل‌کنیم به‌جدول افزایشهای زیر می‌رسیم.

I	مارس ۰	VII	سپتامبر ۱۶
II	آوریل ۳	VIII	اکتبر ۱۸
III	مه ۵	IX	نوامبر ۲۱
IV	ژون ۸	X	دسامبر ۲۳
V	ژوئیه ۱۰	XI	ژانویه ۲۶
VI	اوت ۱۳	XII	فوریه ۲۹

جالب توجه است که شمارش ماههای سال از اول مارس درواقع برگشت به تقویم رومیان قدیم است کـه قیصر روم یولیوس به‌وجود آورد و در آن سپتامبر، اکتبر، نوامبر، دسامبر، به‌طوری‌که از اسمهایشان پیداست [septem، octo، novem، decem در زبان لاتین به‌ترتیب به‌معنای هفت، هشت، نه، ده‌اند. م]، ماههای‌هفتم، هشتم، نهم و دهم هستند.

برگردیم به‌جدول افزایشها. گرچه اعداد جدول نامنظم‌اند، به‌طور متوسط

$$\frac{۲۹}{۱۱} = ۲,۶\ldots$$

به‌شمارهٔ روز هفتهٔ هرماه افزوده می‌شود. چون‌عدد اول جدول ۰ است، بایددرحدود ۲٫۶ از m ۲٫۶کم کنیم ونزدیکترین عدد صحیح نابزرگتر از آن‌را بگیریم. اما با این‌کارکاملا به‌نتیجه نمی‌رسیم. ولی باکم و زیادکردن عددی‌که باید از m ۲٫۶کم شود به‌عبارت زیر می‌رسیم.

$$[۲٫۶\,m - ۲٫۲] = \left[\frac{۱}{۵}(۱۳m - ۱۱)\right],\quad m = ۱,\ ۲,\ \ldots,\ ۱۲ \qquad (۹.۲.۸)$$

بسیار جالب است کـه با این فرمول کاملا نتیجهٔ مطلوب حاصل می‌شود: اگـر در (۹.۲.۸)، m را ۱، ...، ۱۲ بگیریم دقیقاً اعداد جدول بالا ظاهر می‌شوند.

پس، بـاید به‌شمارهٔ اول مارس (۸.۲.۸)، عبارت (۹.۲.۸) را بیفزاییم تـا شمارهٔ روز هفتهٔ اول ماه mام به‌دست آید. بالاخره، چون شمارهٔ روز dام ایـن ماه را می‌خواهیم، باید $d-۱$ روز به‌آن بیفزاییم، حال باکمی پس وپیش‌کردن‌جمله‌ها دقیقاً به‌فرمول (۲.۲.۸) می‌رسیم.

مجموعهٔ مسائل ۲۰۸

۱. تعیین کنید درچه روز هفته به‌دنیا آمده‌اید.

۲. وقتی فقط سالهای بین ۱۹۰۰ و ۱۹۹۹ را در نظر می‌گیرید، چگونه فرمول (۲.۲.۸) ساده می‌شود؟

۳. روزهای تولد درکلاس شما برحسب روزهای هفته[1] چگونه توزیع می‌شوند؟

۳.۸ برنامه‌های مسابقه

به‌عنوان‌کاربرد سادهٔ دیگر نظریهٔ همنهشتی، تهیهٔ برنامه‌های مسابقه‌های‌دوری، معمول در انواع مسابقه‌ها، از شطرنج گرفته تا بیس‌بال را مطرح می‌کنیم.

تعداد شرکت کنندگان یا تیمهای شرکت‌کننده در مسابقه‌ها را N می‌گیریم. وقتی N فرد است، نمی‌توانیم در هردور مسابقه تمام تیمها را در مقابل یکدیگر بگذاریم، همیشه یك تیم بی‌حریف می‌ماند. برای رفع این اشکال یك تیم‌جعلی T_0 به‌تیمها می‌افزاییم و برنامه را برای $N+1$ تیم، شامل T_0، می‌ریزیم. در هردور، تیمی راکه قرار است با T_0 بازی‌کند حذف می‌کنیم.

پس می‌توانیم فرض‌کنیم‌که N، تعداد تیمها، زوج است. هرتیم‌را بایك‌عدد

$$x = 1, 2, \cdots, N-1, N$$

مشخص می‌کنیم. تعدادکل دورهایی‌که هرتیم بازی می‌کند $N-1$ است.

فرض‌کنید x یکی‌از اعداد مجموعهٔ

$$1, 2, \cdots, N-10 \qquad (1.3.8)$$

است. تیم y_r، حریف x در دورهٔ rام مسابقه را عددی از مجموعهٔ (۱.۳.۸) که با همنهشتی

$$x + y_r \equiv r \pmod{N-1} \qquad (2.3.8)$$

مشخص می‌شود، انتخاب می‌کنیم. برای اینکه ببینیم x های متمایز، حریفهای متمایز y_r دارند، توجه می‌کنیم‌که از

---

۱. اگر با تاریخ تقویم در ایران آشنایی دارید، کوشش‌کنید فرمول نظیر (۲.۲.۸) را برای روزهای هفته درایران به‌دست آورید.ـم.

$$x+y_r\equiv r\equiv x'+y_r(N-1\text{ به‌پیمانهٔ}),$$

همنهشتی ($N-1$ به پیمانهٔ $x\equiv x'$) و از آن $x=x'$ نتیجه می‌شود، زیرا x و x' اعدادی ازمجموعهٔ (۱.۳.۸) هستند.

تنها اشکالی که پیش می‌آید، حالت $x=y_r$ است، یعنی بنابر (۲.۳.۸)

$$2x\equiv r(N-1\text{ به‌پیمانهٔ}). \qquad (3.3.8)$$

تنها برای یك عدد از اعداد (۱.۳.۸) ممکن است این حالت پیش آید، زیرا اگر

$$2x\equiv r\equiv 2x'(N-1\text{ به‌پیمانهٔ}),$$

آن‌گاه

$$2(x-x')\equiv 0(N-1\text{ به‌پیمانهٔ}),$$

یا

$$x\equiv x'(N-1\text{ به‌پیمانهٔ}),$$

زیرا $N-1$ فرداست. همواره‌همنهشتی (۳.۳.۸) درمجموعهٔ (۱.۳.۸) جواب‌دارد: وقتی r زوج است $x=\frac{r}{2}$ ووقتی r فرداست، $x=\frac{r+N-1}{2}$، جواب است.

با رابطهٔ (۲.۳.۸) برای هر x مجموعهٔ (۱.۳.۸) یك حریف در دور rام مشخص کردیم، مگر برای آن x_0ی‌که در (۳.۳.۸) صدق می‌کند؛ حریف این x_0 را تیم Nام انتخاب می‌کنیم.

حال باید نشان‌دهیم که با این‌طرزی‌که حریفهارا انتخاب‌کرده‌ایم، هرتیم در هردور $r=1,\ldots,N-1$، باحریف متفاوتی بازی می‌کند. نخست این مطلب را برای‌حالت‌استثنایی‌تیم Nام تحقیق‌می‌کنیم. در دور rام حریف x_0 که با (۳.۳.۸) مشخص می‌شود باتیم N بازی می‌کند. فرض‌کنید $s\neq r$؛ در دور sام، N باتیم x'_0 که در

$$2x'_0\equiv s(N-1\text{ به‌پیمانهٔ})$$

صدق می‌کند، بازی می‌کند. x_0 و x'_0 دو تیم مختلف‌اند، زیرا از $x_0=x'_0$،

$$2x_0=2x'_0\equiv r\equiv s(N-1\text{ به‌پیمانهٔ})$$

و از آن $r=s$ نتیجه می‌شود.

اینك حریفهای مختلف یك تیم x درمجموعهٔ (۱.۳.۸) را درنظر بگیرید. x فقط یك‌بار با تیم Nام، مثلاً در دور r_0ام، که با

$$۲x \equiv r_0 \ (\text{به‌پیمانهٔ } N-۱)$$

تعریف می‌شود، بازی می‌کند. حال فرض کنید $r \neq r_0$ و $s \neq r_0$. آن‌گاه حریفهای x در دورهای rام و sام از روی (۲.۳.۸) با

$$x+y_r \equiv r \ (\text{به‌پیمانهٔ } N-۱), \quad x+y_s \equiv s \ (\text{به‌پیمانهٔ } N-۱)$$

مشخص می‌شوند. در اینجا نیز از $y_r = y_s$، $r = s$ نتیجه می‌شود، پس $y_r \neq y_s$.

در جدول زیر، مسابقات دوری را به‌ازای $N = ۶$ با روشی که در بالا شرح داده‌ایم، بنا کرده‌ایم. با چند محاسبهٔ ساده این جدول به‌دست می‌آید.

r \ x	۱	۲	۳	۴	۵	۶
۱	۵	۴	۶	۲	۱	۳
۲	۶	۵	۴	۳	۲	۱
۳	۲	۱	۵	۶	۳	۴
۴	۳	۶	۱	۵	۴	۲
۵	۴	۳	۲	۱	۶	۵

درایهٔ واقع درسطر rام وستون xام، حریف بازیکن x را در دور rام نشان‌می‌دهد.

مجموعهٔ مسائل ۳.۸

۱. جدولی برای $N = ۸$ بازیکن بسازید.

۲. نشان‌دهید که‌وقتی $r = ۲$، تیمهای $N, \ldots, ۳, ۲, ۱$ به‌ترتیب با N، $N-۱$، $\ldots$، ۳، ۲، ۱ بازی می‌کنند.

۳. چرا تیم $N-۱$ همیشه دردور rام با تیم r بازی‌می‌کند به‌جزوقتی $r = N-۱$؟

دراین حالت استثنایی، تیم $N-1$ باچه تیمی بازی می‌کند؟

۴. تحقیق کنیدکه اگر در دور rام، x با y بازی کند، برطبق فرمولها، y با x بازی می‌کند.

۴.۸ عدد اول یا مرکب؟

آخرین کاربرد همنهشتیهاکه مطرح می‌کنیم بحث در روشی است برای تحقیق اینکه عددی بزرگ اول است یا مرکب. کارایی این روش زیاد است، وبرای بررسی عدد خاصی که به‌تصادف انتخاب شده است بهترین روش کلی است. اساس این روش، همنهشتی (۸.۵.۷) فرما (صفحهٔ۹۸)است.

فرض کنید N عددی است که می‌خواهیم بررسی کنیم. a را عددی کوچك که با N متباین است می‌گیریم. دراغلب موارد مناسب است a را عدد اول کوچکی که N را نشمارد، مانند ۲ یا ۳ یا ۵ بگیریم. اگر N اول باشد، بنابرهمنهشتی‌فرما، در

$$a^{N-1}\equiv 1 \quad (\text{به‌پیمانهٔ } N) \qquad (۱.۴.۸)$$

صدق می‌کند. پس اگر محقق شود که (۱.۴.۸) برقرار نیست، معلوم می‌شودکه N مرکب است.

مثال. N را ۹۱ و a را ۲ بگیرید. آن‌گاه

$$a^{N-1}=2^{90}=2^{64}.2^{16}.2^{8}.2^{2}.$$

علاوه‌براین

$$2^{8}=256\equiv -17 \quad (\text{به‌پیمانهٔ } 91),$$

$$2^{16}=(2^{8})^{2}\equiv(-17)^{2}=289\equiv 16 \quad (\text{به‌پیمانهٔ } 91),$$

$$3^{32}=(2^{16})^{2}=(16)^{2}=256\equiv -17 \quad (\text{به‌پیمانهٔ } 91),$$

$$2^{64}=(2^{32})^{2}\equiv(-17)^{2}=289\equiv 16 \quad (\text{به‌پیمانهٔ } 91),$$

پس

$$2^{90}=2^{64}.2^{16}.2^{8}.2^{2}\equiv 16.16.(-17).4\equiv 64\not\equiv 1 \quad (\text{به‌پیمانهٔ } 91).$$

نتیجه می‌گیریم که N مرکب است. درواقع، $7\times 13=91$.

چون این مثال خیلی ساده است، قدرت واقعی روش نمایان نمی‌شود. با برنامه‌ریزی مناسبی برای کامپیوتر می‌توان با این روش مشخص کرد که بعضی از اعداد خیلی بزرگ مرکب‌اند. متأسفانه این روش هیچ اطلاعی از عاملهای N به‌ما نمی‌دهد؛ بنابراین، در بسیاری از اوقات می‌دانیم که N عدد اول نیست اما دربارهٔ عاملهای آن اطلاعی نداریم.

به‌خصوص این روش‌را می‌توان برای اعداد فرما، یعنی

$$F_n = ۲^{۲^n} + ۱$$

که در بخش ۳.۲ بررسی کردیم، به‌کار برد. توجه کردیم که این اعداد به ازای $n = ۰, ۱, ۲, ۳, ۴$ اول هستند. برای آزمودن

$$F_۵ = ۲^{۲^۵} + ۱ = ۲^{۳۲} + ۱ = ۴\ ۲۹۴\ ۹۶۷\ ۲۹۷$$

با همنهشتی فرما، a را ۳ می‌گیریم. اگر $F_۵$ اول باشد، باید داشته باشیم

$$۳^{۲^{۳۲}} \equiv ۱ \pmod{F_۵} \qquad \text{(به پیمانهٔ } F_۵\text{)} \qquad (۲.۴.۸)$$

برای محاسبهٔ باقیماندهٔ طرف چپ همنهشتی باید ۳۲ بار عمل مربع کردن را انجام دهیم و هر بار نتیجه‌را به (به‌پیمانهٔ $F_۵$) تبدیل کنیم. ما خواننده را از تفصیل این محاسبات معاف می‌کنیم. به‌دست می‌آید که همنهشتی (۲.۴.۸) برقرار نیست، پس $F_۵$ مرکب است. عامل ۶۴۱ را با آزمون وخطا پیدا کرده‌اند. همین روش برای نشان‌دادن اینکه چندین عدد بزرگ فرما اول نیستند به‌کار برده شده است. عاملهای بعضی‌ازآنها شناخته شده‌اند و عاملهای بعضی دیگر را نمی‌دانیم.

وقتی همنهشتی (۱.۴.۸) برای یک‌عدد a که با N متباین است، برقرار است، N ممکن است اول نباشد، اما این حالتی استثنایی است، پس می‌توان حدس زد که N اول باشد. ولی در اکثر موارد می‌خواهیم جوابی قاطع داشته باشیم. برای این منظور از این نکته استفاده می‌کنیم که اگر (۱.۴.۸) به‌ازای نمای $N-۱$ برقرار باشد و به‌ازای هیچیک از مقسوم‌علیه‌های سرهٔ $N-۱$ برقرار نباشد، آن‌گاه N اول است.

راه دیگری هست که برای اعدادی که خیلی بزرگ نیستند کاراست. a را ۲ می‌گیریم. پوله[1] و لمر تمام اعداد $N \leqslant ۱۰۰\ ۰۰۰\ ۰۰۰$ استثنایی، یعنی N هایی راکه در

---

1. Poulet

$$۲^{N-۱} \equiv ۱ \quad (N \text{ به پیمانه}) \qquad (۳.۴.۸)$$

صدق می‌کنند و اول نیستند، حساب کرده‌اند؛ این اعداد را گاهی شبه اول می‌نامند. برای هریك از این اعداد بزرگترین عامل را نیز به‌دست آورده‌اند.

با کمك جدولهای پوله و لمر، از راه زیر می‌توان اول بودن هر $N \leqslant ۱۰۰\,۰۰۰\,۰۰۰$ را تحقیق کرد: اول تحقیق کنید آیا N در همنهشتی (۳.۴.۸) صدق می‌کند یا نه. اگر صدق نکند مرکب است. اگر N در همنهشتی (۳.۴.۸) صدق کند و در جدول باشد، بازهم مرکب است و می‌توانیم یك عامل آن را در جدول بیابیم. سرانجام اگر N در (۳.۴.۸) صدق کند و در جدول نباشد، اول است.

کوچکترین عدد مرکبی که در (۳.۴.۸) صدق می‌کند عدد زیر است:

$$N = ۳۴۱ = ۱۱ \cdot ۳۱$$

بجز این عدد، تنها دو عدد مرکب کوچکتر از ۱۰۰۰، یعنی اعداد

$$N = ۵۶۱ = ۳۰ \cdot ۱۱ \cdot ۱۷,$$

$$N = ۶۴۵ = ۳۰ \cdot ۵ \cdot ۴۳$$

در این همنهشتی صدق می‌کنند. عدد ۵۶۱ از این نظر جالب است که به‌ازای جمیع اعداد a که با N متباین‌اند، در (۱.۴.۸) صدق می‌کند. وقتی عددی دارای چنین ویژگی است، می‌گوییم دارای ویژگی فرماست؛ تحقیقات زیادی روی این اعداد شده است. برای نوشتارها و جدولهای مربوط به این اعداد راهنمای جدولهای نظریهٔ اعداد را که در آخرین قسمت فهرست منابع آمده است ببینید.

پاسخها و راه‌حل مسأله‌های برگزیده

مجموعهٔ مسائل ۳.۱

برای هر دو مسأله جدول ۳، صفحهٔ ۵۴ را ببینید.

مجموعهٔ مسائل ۴.۱

۱. فرض کنید می‌دانیم که

$$T_{n-1}=\frac{1}{2}(n-1)n.$$

می‌توانید امتحان کنید که این رابطه برای $n=2, 3, 4$ درست است. از شکل ۳.۴.۱ دیده می‌شود که T_n از افزودن n به T_{n-1} به‌دست می‌آید به‌طوری که

$$T_n=T_{n-1}+n=\frac{1}{2}n(n+1).$$

۲. از شکل ۴.۴.۱ دیده می‌شود که برای به‌دست آوردن P_n، باید

$$1+3(n-1)=3n-2$$

را به P_{n-1} بیفزاییم. اگر بدانیم که

$$P_{n-1}=\frac{1}{2}(3(n-1)^2-(n-1))$$

(برطبق فهرست (۳.۴.۱)، این‌رابطه به‌ازای $n=۲, ۳, ۴$ برقرار است)، آن‌گاه

$$P_n = P_{n-۱} + ۳n - ۲ = \frac{۱}{۲}(۳n^۲ - n).$$

۳. از افزودن

$$(k-۲)(n-۱)+۱$$

به $(n-۱)$ امین عدد k ضلعی، n امین عدد k ضلعی نتیجه‌می‌شود واز راهی‌که در مسألهٔ ۲ رفتیم‌فرمول به‌دست‌می‌آید. مسأله‌های ۲ و ۳ را می‌توانستیم از راه‌دیگری حل‌کنیم: نقطه‌ها را مانند شکل ۴.۴.۱ به‌عددهای مثلثی تجزیه‌کنیم وفرمول T_n را به‌کار بریم. به‌تفصیل این برهان را بررسی کنید.

مجموعهٔ مسائل ۵.۱

۱. مثلاً

۱۶	۳	۲	۱۳
۹	۶	۷	۱۲
۵	۱۰	۱۱	۸
۴	۱۵	۱۴	۱

که از مربع‌دورر با مبادلهٔ سطرهای دوم وسوم حاصل‌می‌شود، نیز مربع سحرآمیز است. یکی دیگر مربع سحرآمیز زیر است.

۱۶	۴	۱	۱۳
۹	۵	۸	۱۲
۶	۱۰	۱۱	۷
۳	۱۵	۱۴	۲

۲. چون در مربع سحرآمیز ۴×۴ اعداد از ۱۶ تجاوز نمی‌کنند، تنها دو سال ۱۵۱۵ و ۱۵۱۶ را باید درنظرگرفت. واضح است‌که عدد اول قابل قبول نیست، با عدد دوم هم مربع سحرآمیز نمی‌توان ساخت.

مجموعهٔ مسائل ۱۰۲

۱۹۷۹ .۲

۳. تمام اعداد از ۱۱۴ تا ۱۲۶ مرکب هستند.

مجموعهٔ مسائل ۲۰۳

۱. $n=3, 5, 15, 17, 51, 85$

۲. $\frac{360^\circ}{51}=6\frac{360^\circ}{17}-\frac{360^\circ}{3}$

۳. وقتی n ضلعی‌را می‌توان ساخت که n یا یکی‌از ۵ عدد اول فرما یا حاصلضربی از ۲، ۳، ۴ یا ۵ عدد از این‌اعداد باشد. پس تعداد کل این‌چندضلعیها برابر است با

$$5+10+10+5+1=31.$$

بزرگترین مقدار برابر است با

$$n=3.5.17.257.65\,537=4\,294\,967\,295.$$

مجموعهٔ مسائل ۴۰۲

۱. درصد تاهای اول، دوم، ...، دهم به‌ترتیب

$$24, 20, 16, 16, 17, 14, 16, 14, 15, 14$$

عدد اول هست.

۲. ۱۱ عدد اول وجود دارد.

مجموعهٔ مسائل ۱۰۳

۱. $1970=2.5.197$; $365=5.73$; $120=2^3.3.5$

۳. $360=2.2.90=2.6.30=2.10.18=6.6.10$

۴. عددی تنها وقتی‌زوج ـ اول است که به‌صورت $2k$ بوده، k فرد باشد. فرض‌کنید n یك تجزیه به‌اعداد زوج ـ اول مانند

$$n=(۲k_۱).(۲k_۲)...$$

دارد، با حداقل دوعامل ضرب. از این تجزیه، تجزیهٔ دیگر

$$n=(۲k_۱.k_۲).۲...$$

نتیجه می‌شود. ایـن تجزیه از تجزیهٔ اول متمایز است، مگـر اینکه $k_۲=۱$. همین استدلال را برای $k_۳$، $k_۴$، ... می‌توان کرد. نتیجه می‌گیریم: برای اینکه تجزیهٔ n به‌اعداد زوج ـ اول یکتا باشد باید n به‌صورت

$$n=(۲k).۲.۲...=k.۲^{\alpha},\quad k \text{ فرد}$$

باشد. به‌آسانی می‌بینیم که اگر $k=۱$، یعنی $n=۲^{\alpha}$، تجزیه یکتاست. اگر $k>۱$ شرط دیگری هم هست: k باید عدد اول باشد. اگر $k=a.b$،

$$n=(۲a).(۲b).۲.۲...$$

یك تجزیهٔ دیگر n است.

مجموعهٔ مسائل ۲.۳

۱. عدد اول ۲ مقسوم‌علیه دارد؛ توان αام عدد اول p، $\alpha+۱$ مقسوم‌علیه دارد.

$$\tau(۶۰)=۱۲,\quad \tau(۳۶۶)=۸,\quad \tau(۱۹۷۰)=۸$$

۲.

۳. بیشترین تعداد مقسوم‌علیه‌های اعداد $\leqslant ۱۰۰$، ۱۲ است و اعداد ۶۰، ۷۲، ۸۴، ۹۰، ۹۶ دوازده مقسوم‌علیه دارند.

مجموعهٔ مسائل ۳.۳

۱. ۱۰۰۸۰؛ ۶۰؛ ۴۸؛ ۲۴

۲. ۴۵ ۳۶۰؛ ۱۸۰؛ $۲^{۱۳}$

۳. ۲۴ و ۳۶

۴. فرض کنید تعداد مقسوم‌علیه‌ها $r.s$ است و r و s اعداد اول هستند. آن‌گاه

$$n=p^{r-۱}.q^{s-۱}\quad \text{یا}\quad n=p^{rs-۱},$$

p و q اعدادی اول هستند.

مجموعهٔ مسائل ۴.۳

۰۱ ۸۱۲۸, ۳۳ ۵۵۰ ۳۳۶

مجموعهٔ مسائل ۱.۴

۰۱ (الف) $(۳۶۰, ۱۹۷۰) = ۱۰$ (ب) $(۳۰, ۳۶۵) = ۵$

۰۲ فرض کنید $\sqrt{۲}$ گویاست

$$\sqrt{۲} = \frac{a}{b}.$$

می‌توانیم فرض کنیم که عاملهای مشترک کسر را حذف کرده‌ایم و a و b عامل مشترک ندارند. دوطرف را مربع می‌کنیم. به دست می‌آید

$$۲b^۲ = a^۲.$$

چون تجزیه به‌اعداد اول یکتاست a بر ۲ تقسیمپذیر است، پس $a^۲$ بر۴ تقسیمپذیر است. دوباره از یکتابودن‌تجزیه به حاصلضرب اعداد اول نتیجه می‌شود کـه $b^۲$ و همچنین b بر ۲ قـابل قسمت‌اند و این با فرض اینکه a و b عـامل مشترک ندارند متناقض است. این تناقض نشان می‌دهدکه $\sqrt{۲}$ امکان نداردگویا باشد.

مجموعهٔ مسائل ۲.۴

۰۱ اعداد فرد.

۰۲ اگر p عدد اولی باشدکه n و $n+۱$ را بشمارد، باید

$$(n+۱) - n = ۱$$

را نیز بشمارد.

۰۳ هیچیک ازآنها متباین نیستند.

۰۴ بلی

مجموعهٔ مسائل ۳.۴

۲.۲ $(۲۲۰, ۲۸۴) = ۴, (۱۱۸۴, ۱۲۱۰) = ۲$

۴. $(۲۶۲۰, ۲۹۲۴) = ۴, (۵۰۲۰, ۵۵۶۴) = ۴$

۳. برای تعیین بزرگترین توان ۱۰ که

$$n! = ۱.۲.۳.\ldots.n$$

را می‌شمارد، نخست بزرگترین توان ۵ را که $n!$ را می‌شمارد پیدا می‌کنیم. هر پنجمین عدد

$$۵, ۱۰, ۱۵, ۲۰, ۲۵, ۳۰$$

بر ۵ تقسیمپذیر است وتعداد آنها تا n، $[n/۵]$ است. اما بعضی‌ازآنها، یعنی ۲۵، ۵۰، ۷۵، ۱۰۰، ... برتوان دوم ۵ نیز تقسیمپذیرند، و تعداد اینها $[n/۲۵]$ است. تعداد آنهایی‌که برتوان سوم ۵، $۱۲۵ = ۵^۳$، هم تقسیمپذیر هستند، $[n/۵^۳]$ است، الی آخر. این روشن می‌سازدکه نمای توان ۵ که $n!$ را می‌شمارد

$$\left[\frac{n}{۵}\right]+\left[\frac{n}{۵^۲}\right]+\left[\frac{n}{۵^۳}\right]+\ldots \qquad (E)$$

است. در عبارت (E) جمله‌ها تا وقتی مخرج از صورت بزرگتر نشده است ادامه می‌یابد.

همین استدلال را برای پیداکردن توان هرعدد اول دیگر p می‌توان به کار برد. به‌ویژه وقتی $p = ۲$، نمای

$$\left[\frac{n}{۲}\right]+\left[\frac{n}{۲^۲}\right]+\left[\frac{n}{۲^۳}\right]+\ldots$$

به‌دست می‌آید. واضح است‌که این نما از عبارت (E) کوچکتر نیست، پس در $n!$ هرعامل ۵ را بایك عامل ۲ می‌توان ترکیب‌کرد. پس (E)، نمای توان ۱۰ که $n!$ را می‌شمارد، نیز هست. یعنی (E) تعداد صفرهای آخر $n!$ را نشان می‌دهد.

چند مثال. $n = ۱۰$، $[۱۰/۵] = ۲$، $[۱۰/۵^۲] = ۰$، پس $۱۰!$ به ۲ صفر ختم می‌شود.

$n=۳۱$، $[۳۱/۵]=۶$، $[۳۱/۵^۲]=۱$، $[۳۱/۵^۳]=۰$، پس $۳۱!$ به ۷ صفر ختم می‌شود.

مجموعهٔ مسائل ۴.۴

۱. $[۳۶۰, ۱۹۷۰]=۷۰۹۲۰$, $[۳۰, ۳۶۵]=۲۱۹۰$

۲. $[۲۲۰, ۲۸۴]=۱۵\,۶۲۰$, $[۱۱۸۴, ۱۲۱۰]=۷۱۶\,۳۲۰$,

$[۲۶۲۰, ۲۹۲۴]=۱۹۱۵\,۲۲۰$, $[۵۰\,۲۰, ۵۵۶۴]=۶\,۹۸۲\,۸۲۰$.

مسأله‌های بخش ۲.۵

۱. $m=۸, n=۱, (۱۶, ۶۳, ۶۵)$, $n=۳, (۲۴, ۵۵, ۷۳)$

$n=۵, (۸۰, ۳۹, ۸۹)$, $n=۷, (۱۱۲, ۱۵, ۱۱۳)$

$m=۹, n=۲, (۳۶, ۷۷, ۸۵)$, $n=۴, (۶۴, ۶۵, ۹۷)$

$n=۸, (۱۴۴, ۱۷, ۱۴۵)$

$m=۱۰, n=۱, (۲۰, ۹۹, ۱۰۱)$, $n=۳, (۶۰, ۹۱, ۱۰۹)$

$n=۷, (۱۴۰, ۵۱, ۱۴۹)$, $n=۹, (۱۸۰, ۱۹, ۱۸۱)$

۲. نه. اگر

$$۲mn=۲m_۱n_۱,\ m^۲-n^۲=m_۱^۲-n_۱^۲,\ m^۲+n^۲=m_۱^۲+n_۱^۲$$

نتیجه می‌شد

$$m=m_۱,\ n=n_۱ \text{ یا } m^۲=m_۱^۲,\ n^۲=n_۱^۲$$

۳. وقتی عدد c وتر یک مثلث فیثاغورسی است، هرمضرب c مانند $k.c$ نیز همان ویژگی را دارد. پس کافی‌است تنها مقادیر $c\leqslant ۱۰۰$ را که هیچیک‌از مقسوم‌علیه‌های c وتر نیست، در فهرست بیاوریم. این مقادیر از جدول ادامه یافته‌ای که در مسألهٔ اول همین مجموعهٔ مسائل به‌دست آمده است پیدا می‌شود:

$$c=۵, ۱۳, ۱۷, ۲۹, ۳۷, ۴۱, ۵۳, ۶۱, ۷۳, ۸۹, ۹۷.$$

مجموعهٔ مسائل ۳۰۵

۰۱ (۱۲۰, ۵۰, ۱۳۰) (۶۲۴, ۵۰, ۶۲۶) (۴۸, ۱۴, ۵۰) (۴۰, ۳۰, ۵۰)
(۱۲۰, ۲۲, ۱۲۲).

۰۲ $۱۰۰=۱۰^۲+۰^۲$, $۱۰۱=۱۰^۲+۱^۲$, $۱۰۴=۱۰^۲+۲^۲$,
$۱۰۶=۹^۲+۵^۲$, $۱۰۹=۱۰^۲+۳^۲$.

اعداد ۱۰۱، ۱۰۶، ۱۰۹ وترهای مثلثهای فیثاغورسی هستند.

۰۳ مثلث فیثاغورسی با مساحت ۷۸ یا ۱۰۰۰ وجود ندارد. یك مثلث (۲۶, ۱۰, ۲۴)
با مساحت ۱۲۰ وجود دارد.

۰۴ این اعداد، محیط هیچیك از مثلثهای فیثاغورسی نیستند.

مجموعهٔ مسائل ۳۰۶

۰۱ ۱۹۴۰ و ۳۶۴.

۰۲ $۳۶۲=(۱, ۰, ۱, ۱, ۰, ۱, ۰, ۱, ۰)_۲=(۱, ۴, ۰, ۲)_۶$
$=(۱, ۴, ۵)_{۱۷}$

$۱۹۶۹=(۱, ۱, ۱, ۱, ۰, ۱, ۱, ۰, ۰, ۰, ۱)_۲$
$=(۲, ۲, ۰, ۰, ۲, ۲, ۱)_۳$
$=(۶, ۱۳, ۱۴)_{۱۷}$

$۱۰۰۰۰=(۱, ۰, ۰, ۱, ۱, ۱, ۰, ۰, ۰, ۱, ۰, ۰, ۰, ۰)_۲$
$=(۱, ۱, ۱, ۲, ۰, ۱, ۱, ۰, ۱)_۳=(۲, ۰, ۱۰, ۴)_{۱۷}$

مجموعهٔ مسائل ۳۰۶

۰۱ اعداد ۰, ۱ را کنار می‌گذاریم؛ ضربها، حاصلضربهای جفتی از اعداد ۲،
۳، ...، $b-۱$ هستند. چون ترتیب درضرب تأثیری ندارد، می‌توانیم عامل کوچکتر
را عامل اول ضرب بگیریم. آن‌گاه عامل ۲ در $b-۲$ حاصلضرب وجود دارد:

$$۲۰۲, ۲۰۳, \ldots, ۲۰(b-۱),$$

و عامل ۳ در $b-۳$ حاصلضرب وجود دارد که کوچکترین عامل آنها ۳ است:

$$۳.۳,\ ۳.۴,\ \dots,\ ۳(b-۱).$$

اگر ادامه دهیم به‌تعداد مطلوب

$$(b-۲)+(b-۳)+\dots+۳+۲+۱=\frac{۱}{۲}(b-۱)(b-۲)$$

می‌رسیم.

۲. اگر عامل ۱ را هم در حاصلضربها در نظر بگیریم مجموع تمام آنها برابر می‌شود با

$$(۱+۲+\dots+(b-۱))(۱+۲+\dots+(b-۱))=\left(\frac{۱}{۲}b(b-۱)\right)^{۲}.$$

به‌ازای $b=۱۰$ این مجموع برابر است با $۴۵^{۲}=۲۰۲۵$. اگر ۱ را کنار بگذاریم مجموع برابر می‌شود با

$$(۲+\dots+(b-۱))(۲+\dots+(b-۱))=\left(\frac{۱}{۲}(b+۱)(b-۲)\right)^{۲}$$

به‌ازای $b=۱۰$ مجموع $۱۹۳۶=(۴۴)^{۲}$ به‌دست می‌آید. در هردو حالت مجموع یك عدد مربعی است.

مجموعهٔ مسائل ۴.۶

۱. تابع

$$f(b)=\frac{b}{\log b}$$

در بازهٔ $۱<b<\infty$ مثبت است و وقتی $b\to ۱$ یا $b\to\infty$، $f(b)\to\infty$. مشتق $f(b)$،

$$f'(b)=\frac{\log b-۱}{(\log b)^{۲}},$$

تنها به‌ازای

$$\log b=۱,\ b=e=۲٫۷۱۸۲۸\dots$$

صفر می‌شود، در بازهٔ $۱<b<e$ منفی و در بازهٔ $e<b<\infty$ مثبت است.

پس $f(b)$ در $1 < b < e$ نزولی و در $e < b < \infty$ صعودی است. مقدار مینیمم تابع برابر است با

$$f(e) = e = ۲٫۷۱۸۲۸ \ldots .$$

تابع

$$g(b) = \frac{b-1}{\log b}$$

درفاصلهٔ $1 < b < \infty$ مثبت است و وقتی $b \to 1$، $g(b) \to 1$؛ وقتی $b \to \infty$، $g(b) \to \infty$. مشتق g،

$$g'(b) = \frac{\log b + \frac{1}{b} - 1}{(\log b)^2}$$

و درفاصلهٔ $1 < b < \infty$ مثبت است، پس تابع صعودی است.

مجموعهٔ مسائل ۵.۶

۱. $(1, 0, 0, \ldots, 0, 1)_2 = 2^n + 1$ با $n-1$ صفر.

۲. $(1, 1, \ldots, 1)_2 = 2^p - 1$ با p رقم ۱، پس

$$2^{p-1}(2^p - 1) = (1, \ldots, 1, 0, \ldots, 0)_2$$

با p رقم ۱ و $p-1$ صفر.

مجموعهٔ مسائل ۶.۶

۹۲۸۳۶ ۰۲	۲۹۷۸۶ ۰۳	۴۱۱ ۰۵
۱۲۸۳۶	۸۵۰	۴۱۱
۱۰۵۶۷۲	۸۵۰	۴۱۱
	۳۱۴۸۶	۷۱۴
		۱۹۴۷

تحلیل مسأله‌های ۱ و ۴ را به خودتان واگذار می‌کنیم. اگر از عهدهٔ حل آنها برنیامدید با دوستانی که با کامپیوتر آشنا هستند مشورت کنید.

مجموعهٔ مسائل ۲۰۷

۰۱ $-۳۷\equiv ۵(۷)$ (به‌پیمانهٔ ۷), $-۱۱۱\equiv ۱۰(۱۱)$ (به‌پیمانهٔ ۱۱),
$-۳۶۵\equiv ۲۵(۳۰)$ (به‌پیمانهٔ ۳۰).

مجموعهٔ مسائل ۲۰۸

۰۲ به‌ازای $C=۱۹$ دو جملهٔ آخر فرمول (۲۰۲۰۸) به

$$\left[\frac{۱}{۴}C\right]-۲C\equiv ۱(۷) \quad \text{(به‌پیمانهٔ ۷)}$$

خلاصه می‌شود.

مجموعهٔ مسائل ۳۰۸

۰۱
۱ : ۲ : ۳ : ۴ : ۵ : ۶ : ۷ : ۸
۴ : ۱ : ۲ : ۳ : ۸ : ۵ : ۶ : ۷
۸ : ۷ : ۶ : ۵ : ۴ : ۳ : ۲ : ۱
۵ : ۳ : ۴ : ۸ : ۶ : ۷ : ۱ : ۲
۲ : ۴ : ۵ : ۶ : ۷ : ۱ : ۸ : ۳
۶ : ۵ : ۸ : ۷ : ۱ : ۲ : ۳ : ۴
۳ : ۶ : ۷ : ۱ : ۲ : ۸ : ۵ : ۴
۷ : ۸ : ۱ : ۲ : ۳ : ۴ : ۵ : ۶

۰۲ وقتی $r=۲$، درحالت استثنایی تیم N با $x=۱$ بازی می‌کند. [برای سهولت، مسأله در حالت $N=۸$ حل شده است. م.] پس ۱ با ۸ و ۸ با ۱ بازی می‌کند. برای دیگر مقادیر $x=۲, ۳, \ldots, ۷$ داریم

$$y\equiv ۲-x\equiv ۹-x(۷) \quad \text{(به‌پیمانهٔ ۷)}$$

پس مقادیر y به‌ترتیب برابر است با $y=۷, ۶, \ldots, ۲$

۰۳ تیم $N-۱$ در دور rام با

$$y \equiv r-(N-1) \equiv r(N-1 \text{ به‌پیمانهٔ})$$

بازی می‌کند. $N-1$ تنها وقتی تیم استثنایی است که

$$r(N-1) \equiv 2(N-1 \text{ به‌پیمانهٔ}),$$

بنابراین $r=N-1$ و دراین صورت $N-1$ با N بازی می‌کند.

۴. وقتی x استثنایی نیست، شرط (۲.۳.۸) نسبت به x و y قرینه است. وقتی x در (۳.۳.۸) صدق می‌کند، x با N بازی می‌کند و بنابر تعریف، N با x بازی می‌کند.

مراجع

شمارا به‌مطالعهٔ نظریهٔ اعداد دعوت کرده‌ایم. اگر علاقه‌مند هستید ومیل‌دارید دعوت را قبول کنید، می‌توانید مطالعه را با خواندن کتابهای پیشرفته‌تر درسطح درسهای دانشگاهی ادامه دهید. کتابهای زیادی از این قبیل می‌توان توصیه کرد. من مسایلم نخست به‌کتاب خودم اشاره کنم:

Number Theory and Its History, McGraw-Hill Book Co., New York.

این کتاب طبیعتاً در مرحلهٔ بعدی کتاب حاضر می‌آید، زیرا از بعضی مطالب کتاب حاضر باعمقی بیشتر بحث می‌کند ونظریه‌های پیشرفته‌تر دیگری‌را شرح می‌دهد. درنظریهٔ اعداد کتابهای بسیارخوب‌دیگر برای‌درسهای دانشگاهی زیادهستند:

B. W. Jones, *The Theory of Numbers*, Rinehart, New York.

W. J. Leveque, *Elementary Theory of Numbers*, Addison-Wesley, New York.

C. T. Long, *Elementary Introduction to Number Theory*, D. C. Heath, Boston.

N. H McCoy, *The Theory of Numbers*, Macmillan, New York.

I. Niven and H. S. Zuckerman, *Introduction to the Theory of Numbers*, Wiley New York.

H. Rademacher, *Lectures on Elementary Number Theory*, Blaisdell, New York.

J. M. Vinogradov, *Elements of Number Theory* (translated from Russian), Dover, New York.

کتابهای زیر کمی پیشرفته هستند.

H. Cohn; *A Second Course in Number Theory*, Wiley, NewYork

E. Grosswald, *Topics from the Theory of Numbers*, Macmillan, New York,

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon, Oxford,

W. J. Leveque, *Topics in Number Theory* (2vols.), Addison-Wesley, New York.

D. Shanks, *Solved and Unsolved Problems in Number Theory*, Spartan books, Washington.

اگر مایل باشید دربارهٔ تاریخ نظریهٔ اعداد اطلاعاتی داشته باشید و بدانید هر نتیجه را چه کسی پیدا کرده است. می‌توانید به کتاب زیر رجوع کنید:

L. E. Dickson, *History of the Theory of Numbers* (3 vol.), Carnegie Institution of Washington, Publication No. 256. Reprinted by G. E. Stechert, New York.

بررسی کلی برجدولهای اعداد خاصی راکه در نظریهٔ اعداد به‌کار می‌روند می‌توانید در نوشتار زیر بیابید:

D. H. Lehmer; *Guide to Tables in the Theory of Numbers*, Bulletin of the National Research Council, No. 105, 1941 and 1961.

فهرست راهنما