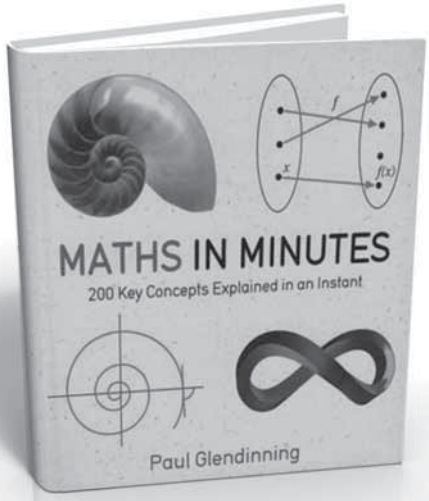
تألیف: پال گلندینینگ
مترجم: غلامرضا یاسی‌پور

ریاضیات در چند دقیقه



اعداد اول

اعداد اول اعداد صحیح مثبتی هستند که تنها بر خودشان و ۱ بخش‌پذیرند. یازده عدد اول نخستین عبارت‌اند از: ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳، ۲۹ و ۳۱، امـا بی‌نهایـت عـدد اول موجودند. بنابر قرارداد، ۱ عدد اول در نظر گرفته نمی‌شـود، در حالی‌که ۲ تنها عدد اول زوج اسـت. عددی که نه ۱ و نه اول اسـت، به «عدد مرکب» (composite number) موسوم است.

هر عدد مرکب را می‌توان به گونه‌ای یکتا به صورت حاصل ضربی از عوامل اولی نوشت که در هم ضرب شده باشند. برای مثال: $۲۷۰=۲\times۳^۳\times۵$ ، $۲۱=۳\times۷$ ، $۱۲=۲^۲\times۳$

از آنجا که خود اعداد اول نمی‌توانند تجزیه شـوند، می‌توان آن‌ها را به‌عنوان بلوک‌های سـاختمانی و بنیانی اعـداد صحیح مثبت در نظر گرفت. اما تعیین اینکه عددی اول اسـت یا نه، و یافتن عوامل اول آن، در صورتی که اول نباشـد، می‌تواند بسیار مشکل باشـد. بنابراین، این فرایند مبنای ایده‌آلی برای دستگاه‌های رمزبندی است.

الگوهای پیچیدهٔ بسیاری در مورد اعداد اول موجودند، و یکی از فرض‌های برجستهٔ بزرگ ریاضیات، یعنی «فرض ریمـان» (Riemann hypothesis)، در مـورد توزیع آن‌هاست.

* جدول اعداد ۱ تا ۱۰۰ که در آن اول‌ها به‌صورت روشـن نمایش داده شده‌اند

۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰
۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰
۳۱	۳۲	۳۳	۳۴	۳۵	۳۶	۳۷	۳۸	۳۹	۴۰
۴۱	۴۲	۴۳	۴۴	۴۵	۴۶	۴۷	۴۸	۴۹	۵۰
۵۱	۵۲	۵۳	۵۴	۵۵	۵۶	۵۷	۵۸	۵۹	۶۰
۶۱	۶۲	۶۳	۶۴	۶۵	۶۶	۶۷	۶۸	۶۹	۷۰
۷۱	۷۲	۷۳	۷۴	۷۵	۷۶	۷۷	۷۸	۷۹	۸۰
۸۱	۸۲	۸۳	۸۴	۸۵	۸۶	۸۷	۸۸	۸۹	۹۰
۹۱	۹۲	۹۳	۹۴	۹۵	۹۶	۹۷	۹۸	۹۹	۱۰۰

الگوریتم اقلیدس

الگوریتم روش یا دستورالعملی برای حل یک مسئله، با انجام مجموعه‌ای از قواعد است. «الگوریتم اقلیدس» (Euclid's algorithm) یکی از قدیمی‌ترین مثال‌هایی است که در حدود سال ۳۰۰ ق.م تنظیم شده است. این الگوریتم برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک، یعنی ب.م.م.، دو عدد طرح شده است. الگوریتم‌ها در علوم رایانه‌ای نقشی اساسی دارند و اغلب ابزارهای الکترونیکی، برای تولید خروجی مفید، از آن‌ها استفاده می‌کنند.

ساده‌ترین صورت الگوریتم اقلیدس از این واقعیت استفاده می‌کند که ب.م.م. دو عدد برابر ب.م.م. عدد کوچک‌تر و تفاضل بین آن‌هاست. این موضوع مجازمان می‌کند که به‌طور مکرر عدد بزرگ‌تر واقع در جفت موردنظر را برداریم و بدین‌ترتیب اندازهٔ اعداد مشمول را تا صفر شدن یکی، کاهش دهیم. در این صورت عدد ناصفر آخری ب.م.م. جفت اولیه است.

این روش می‌تواند تا رسیدن به پاسخ، تکرارهای زیادی داشته باشد. روش کاراتر، یعنی الگوریتم استاندارد، طریقی است که در آن به‌جای عدد بزرگ‌تر، باقی‌مانده‌ای را قرار می‌دهد که از تقسیم آن بر عدد کوچک‌تر به‌دست آمده است. این عمل را تا زمانی که دیگر باقی‌مانده‌ای موجود نباشد، ادامه می‌دهد.

پیدا کردن ب.م.م. ۵۸۵ و ۴۴۲

صورت سادهٔ الگوریتم اقلیدس: ۱۵ مرحله

۱۴۳=۴۴۲-۵۸۵، بنابراین ۴۴۲ و ۱۴۳ را در نظر می‌گیریم.

۲۹۹=۱۴۳-۴۴۲، پس ۲۹۹ و ۱۴۳ را در نظر می‌گیریم.

۱۵۶=۱۴۳-۲۹۹، پس ۱۵۶ و ۱۴۳ را در نظر می‌گیریم.

۱۳=۱۴۳-۱۵۶، پس ۱۴۳ و ۱۳ را در نظر می‌گیریم.

۱۳۰=۱۳-۱۴۳، پس ۱۳۰ و ۱۳ را در نظر می‌گیریم.

(پاسخ در این مرحله واضح است، اما تفریق نه بار دیگر به ۱۳ منجر می‌شود...)

۰=۱۳-۱۳، بنابراین ب.م.م. موردنظر ۱۳ است.

صورت استاندارد الگوریتم اقلیدس: ۳ مرحله

$$\frac{۵۸۵}{۴۴۲} = ۱ \text{ (باقی‌مانده ۱۴۳)}$$

$$\frac{۴۴۲}{۱۴۳} = ۳ \text{ (باقی‌مانده ۱۳)}$$

$$\frac{۱۴۳}{۱۳} = ۱۱ \text{ (بدون باقی‌مانده)}$$

بنابراین فرایند متوقف می‌شود، و ب.م.م. ۱۳ است.

مقسوم‌علیه‌ها و باقی‌مانده‌ها

عددی «مقسوم‌علیه» (divisor)عدد دیگری است اگر دقیقاً و بدون باقی‌مانده در آن عدد شمرده شود. بنابراین ۴ مقسوم‌علیه ۱۲ است، زیرا می‌تواند دقیقاً سه بار در ۱۲ شمرده شود. در این نوع عمل، عددی که در آن شمرده شده، یعنی ۱۲، به‌عنوان «مقسوم» (dividend) شناخته می‌شود.

اما در مورد ۱۳ چون توسط ۴ شمرده شود، چه می‌توان گفت؟ در این حالت، ۴ مقسوم‌علیه ۱۳ نیست، زیرا این عدد سه بار در ۱۳ شمرده می‌شود، اما ۱ واحد باقی می‌ماند. یک راه بیان پاسخ به‌صورت سه، باقی‌ماندهٔ یک بیان می‌شود. این طریق راه دیگری برای گفتن این مطلب است که ۱۲، که ۴×۳ است، بزرگ‌ترین عدد صحیح کمتر از مقسوم (۱۳) است که بر چهار بخش‌پذیر است، و اینکه: ۱+۱۲=۱۳. اکنون چون باقی‌ماندهٔ یک توسط چهار شمرده می‌شود، نتیجهٔ کسر $\frac{۱}{۴}$ است. بنابراین، پاسخ پرسش اولیّه‌مان $۳\frac{۱}{۴}$ است.

۳ و ۴ هر دو مقسوم‌علیه‌های ۱۲اند (همان‌طور که ۱، ۲، ۶ و ۱۲ نیز چنین‌اند). اگر عددی طبیعی، مثلاً p را توسط عدد دیگری، مثل q، بشماریم که مقسوم‌علیه p نیست، در این صورت همواره باقی‌ماندهٔ rی موجود است که کمتر از q است. این موضوع به این معنی است که در حالت عمومی داریم: p=kq+r که در آن، k عددی طبیعی، و r عددی طبیعی و کمتر از q است.

به ازای دو عدد p و q، «بزرگ‌ترین مقسوم‌علیه مشترک، ب.م.م.»(greatest common divisor, GCD) و نیز مشهور به «بزرگ‌ترین عامل مشترک» (greatest common factor) بزرگ‌ترین عددی است که مقسوم‌علیه p و q، هر دو است.

از آنجا که به‌طور واضح ۱ مقسوم‌علیه هر دو عدد است، ب.م.م. همواره بزرگ‌تر از یا برابر با ۱ است. اگر ب.م.م. برابر ۱ باشد، در این صورت اعداد را «متباین» (coprime) می‌گویند. آن‌ها به استثنای ۱، مقسوم‌علیه مثبت مشترک ندارند.

مقسوم‌علیه‌ها خانوادهٔ جالبی از اعداد موسوم به «اعداد کامل» (perfect numbers) را تولید می‌کنند. این اعداد عددهایی هستند که مجموع مقسوم‌علیه‌های مثبتشان، غیر از خودشان، به اندازهٔ خود عدد است. اولین و ساده‌ترین عدد کامل ۶ است، که برابر مجموع مقسوم‌علیه‌های خود، یعنی ۱، ۲ و ۳ است. دومین عدد کامل ۲۸ است که برابر است با: ۱+۲+۴+۷+۱۴. باید برای یافتن سومین عدد کامل، یعنی ۴۹۶، صبر بیشتری داشته باشیم. این عدد برابر است با: ۱+۲+۴+۸+۱۶+۳۱+۶۲+۱۲۴+۲۴۸.

اعداد کامل بسیار کمیاب‌اند و یافتنشان چالشی محسوب می‌شود. ریاضی‌دان‌ها همچنان باید پاسخ‌هایی قطعی برای پرسش‌های مهمی در این زمینه بیابند؛ از قبیل اینکه: آیا تعدادی نامتناهی از این اعداد موجودند؟ یا: آیا جمیع آن‌ها زوج‌اند یا نه؟