

مقالات کوتاه از

مجلات ریاضی معتبر جهان (۱۵)

ترجمه: غلامرضا یاسی پور

اعداد اول، تجزیه و رمزهای مخفی (قسمت اول)

توده‌ای از 2^n ژتون خواهیم داشت. بخصوص، بر مربع آخر توده‌ای از 2^{64} ژتون خواهیم داشت. تصور می‌کنید ضخامت این توده چقدر است؟ ۱ متر؟ ۱۰۰ متر؟ یک کیلومتر؟ مطمئناً خیر! خوب، باور بکنید یا خیر، توده‌مان از ماه (به فاصله ۴۰۰۰۰۰ کیلومتر) و از خورشید (به فاصله ۱۵۰ میلیون کیلومتر) خواهد گذشت و در حقیقت تقریباً به پروکسیما سنتوری، نزدیکترین ستاره به زمین، به فاصله حدوداً ۴ سال نوری از آن، خواهد رسید. عدد 2^{64} در صورت دهمی عبارت است از

۶۱۶ ۵۵۱ ۷۰۹ ۰۷۳ ۷۴۴ ۴۴۶ ۱۸

این از 2^{64} است. اما برای به دست آوردن عدد 2^{16091} که در عدد اول مورد بحث ظاهر شده است به صفحه شطرنجی با 2^{16091} مربع نیاز داریم - صفحه‌ای با اندازه‌های 465×465 مربع این کار را انجام می‌دهد!

اما چگونه به عددی با این اندازه می‌پردازیم؟ برای آغاز کار از کامپیوتر استفاده می‌کنیم. اما نه هر کامپیوتری. عدد رکورددار فوق‌الذکر با استفاده از یکی از قدرتمندترین کامپیوترهای دنیا کشف شد - کامپیوتری که توانایی انجام دویست میلیارد عمل حسابی را در یک ثانیه دارد - و با این وصف محاسبه بیش از سه ساعت طول کشید. اما در این مورد

بزرگترین عدد اول در دنیا

بزرگترین عدد اول* (شناخته شده) در دنیا عدد غول‌آسایی است که برای نوشته شدن به صورت دهمی متعارف به 65050 رقم نیازمند است. این عدد، با استفاده از نماد نمایی (یا توانی)، دارای صورت قابل کنترلتر زیر است:

$2^{16091} - 1$

یعنی، عدد مورد بحث را با ضرب 2^{16091} بار ۲ در خودش و بعد تقریق ۱ از جواب آن به دست می‌آورید.

نماد نمایی فریب‌دهنده است. برای به دست آوردن ایده‌ای از توانایی این نماد در ارائه اعداد بزرگ، صفحه شطرنج 8×8 معمولی‌ای را در نظر می‌گیریم و بر مربعهای آن توده‌هایی از ژتونهایی به ضخامت 2 mm را طبق قاعده زیر قرار می‌دهیم. مربعهای مزبور را، چون در شکل ۱، از ۱ تا ۶۴ شماره‌گذاری می‌کنیم. در مربع اول ۲ ژتون می‌گذاریم. در مربع دوم ۴ ژتون. در مربع سوم ۸ ژتون. و همینطور بر هر مربع دقیقاً دو برابر تعداد مربع ماقبل آن ژتون قرار می‌دهیم. به این ترتیب بر مربع n ام

* مطلب بعدی را برای توضیح این عبارت ملاحظه کنید.

بزرگترین عدد اول وجود دارد، یا اعداد اول همین طور بزرگتر و بزرگتر شده ادامه می‌یابند؟

در نظر اول به نظر می‌رسد که اعداد اول در واقع بسیار فراوانند. از ده عدد اولیه بعد از ۱ (یعنی ۲ تا ۱۱ و خود ۱۱)، پنج عدد، یعنی، ۲، ۳، ۵، ۷، ۱۱، اولند، که دقیقاً نیمی از گردایه مزبورند. از ده عدد بعدی، ۱۲ تا ۲۱، سه عدد (۱۳، ۱۷، ۱۹) که اولند موجودند، یعنی، به نسبت $3/10$ ، بین ۲۲ و ۳۱ نسبت همان $3/10$ است، در حالی که در مورد دو گروه ده عددی بعدی نسبت مورد بحث به $2/10$ سقوط می‌کند. بنابراین به نظر می‌رسد که اولها هر چه که در امتداد دنباله اعداد طبیعی جلوتر برویم «تنک» می‌شوند. جدول ۱ نشان می‌دهد که چگونه تعداد اولهای کمتر از n (که با $\pi(n)$ نمایش داده می‌شود) به ازای مقادیر منتخب n ، با n تغییر می‌کند، و رقم «جگالی» $\pi(n)/n$ را در هر حالت به دست می‌دهد.

بنابراین، اعداد اول هر چه در دنباله عددی مورد بحث جلوتر برویم کمیابتر می‌شوند. اما آیا سرانجام به تدریج محو و نابود می‌شوند؟ پاسخ منفی است.

n	$\pi(n)$	$\pi(n)/n$
۱۰۰۰	۱۶۸	۰/۱۶۸
۱۰۰۰۰	۱۲۲۹	۰/۱۲۲
۱۰۰۰۰۰	۹۵۹۲	۰/۰۹۶
۱۰۰۰۰۰۰	۷۸۴۹۸	۰/۰۷۸

جدول ۱. توزیع اولها، نشان می‌دهد که تعداد اولها، $\pi(n)$ ، به ازای مقادیر گوناگون n ، کوچکتر از n است. این موضوع نیز توسط اقلیدس با استفاده از استدلالی به اثبات رسید که تا به امروز به عنوان مدلی عالی از برهان ریاضی ظریف باقیمانده است. برای شروع این اثبات، تصور می‌کنیم اعداد اول به ترتیب اندازه فهرست شده باشند:

$$P_1, P_2, P_3, \dots$$

بنابراین $P_1 = 2, P_2 = 3, P_3 = 5$ ، و غیره. هدف، نشان دادن این موضوع است که باید این فهرست برای همیشه ادامه داشته باشد. به عبارت دیگر، باید اثبات شود که اگر در هر مرحله n در فهرست، با شمارش کردن $P_1, P_2, \dots, P_n$ ، که باشیم، آنگاه باید در آن اول دیگری بالاتر از P_n موجود باشد. طریق اثبات نگرستن به عدد

$$N = P_1 P_2 P_3 \dots P_n + 1$$

حاصل از ضرب درهم جمیع اولهای P_1, P_2, P_3 و غیره تا P_n ، و بعد افزودن ۱ به نتیجه آن است. به طور وضوح N بزرگتر از P_n است، بنابراین اگر N اول باشد آنگاه می‌دانیم که عدد اولی بزرگتر از P_n وجود دارد، و این همان است که سعی در اثباتش داریم. از طرف دیگر، اگر N اول نباشد باید بر اولی بخشپذیر باشد، این اول را P می‌نامیم. اما اگر بخواهیم N را بر هر یک از اولهای $P_1, P_2, \dots, P_n$ تقسیم کنیم باقیمانده ۱ موجود می‌شود (همان ۱ که هنگامی که N را در مرتبه اول به دست آوردیم افزودیم). بنابراین P مان باید اولی متفاوت با آنها باشد، و بار دیگر مطلوب را ثابت کرده‌ایم. بنابراین، در هر وضعیت عدد اولی بزرگتر از P_n موجود است، و می‌توان نتیجه گرفت که فهرست اعداد اول برای همیشه ادامه دارد.

توجه داشته باشید که هیچ ایده‌ای در این مورد که عدد N فوق اول است یا خیر نداریم. اگر چند مثال را در نظر بگیریم کشف می‌کنیم که اعدادی از این دست اغلب اولند. به عنوان نمونه،

$$N_1 = 2 + 1 = 3$$

$$N_2 = 2 \times 3 + 1 = 7$$

$$N_3 = 2 \times 3 \times 5 + 1 = 31$$

$$N_4 = 2 \times 3 \times 5 \times 7 + 1 = 211$$

$$N_5 = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$$

جمعاً اولند. اما سه عدد بعدی چنین نیستند:

$$N_6 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$$

$$N_7 = 19 \times 97 \times 277$$

$$N_8 = 347 \times 27953$$

در واقع، هیچ کس نمی‌داند بینهایت عدد به صورت

$$N_n = P_1 P_2 \dots P_n + 1$$

اولند یا خیر، نیز بینهایت عدد از این اعداد مرکبند یا نه (گرچه البته باید یکی از این دو امکان راست باشد). و این تنها یکی از دهها سؤال بسادگی بیان شده درباره اعدادی اول است که پاسخش نامعلوم است.

یادداشتها:

۱. Proxima Centauri

۲. Francis Hutcheson

۳. natural (or counting) numbers

۴. Leopold Kronecker

۵. divides

۶. Perfect Square

۷. Prime

۸. Composite

۹. Elements

۱۰. Fundamental theorem of mathematics

۱۱. Prime factor

۱۲. Repeated factor

۱۳. Prime factorization