سفری به اعماق اقیانوس نظریه‌ی اعداد

مجید صفری
دبیر ریاضی ناحیه‌ی ۱ شیراز

گاهی در عناوین خبرها به‌خصوص در مجلات ریاضی صحبت‌هایی پیرامون کشف بزرگ‌ترین عدد اول شناخته‌شده مطرح می‌شود. به‌عنوان نمونه، نام یک دانشجوی ۲۶ ساله با کشف بزرگ‌ترین عدد اول شناخته‌شده، در تاریخ ریاضیات ماندگار شده است. عددی که او کشف کرد، ۶۳۲۰۴۳۰ رقمی است و برای پیدا کردن این عدد، بیش از دو سال وقت صرف شد. او ۲۰۰ هزار کامپیوتر متصل به شبکه‌ی اینترنت را برای یافتن آن عدد به کار گرفت. مایکل شافر (دانشجوی ۲۶ ساله) این پروژه را با کمک بیش از ۶۰ هزار داوطلب از سراسر دنیا به انجام رسانید.

بحث امروز ما پیرامون این موضوع است که واقعاً یافتن چنین عدد غول‌آسایی چه فایده‌ای می‌تواند داشته باشد؟

اگر خودِ ما به عنوان معلم ریاضی، چنین سؤالی برایمان مطرح نباشد، بارها و بارها از سوی دانش‌آموزانمان مورد پرسش‌های مشابه قرار خواهیم گرفت. ضمن این که این پرسش نه‌تنها در رابطه با این مسأله، بلکه در رابطه با اغلب مفاهیم ریاضی که جنبه‌ی کاربردی کمتری دارند و یا لااقل کاربرد آن‌ها برای دانش‌آموزان ملموس نیست، مطرح می‌شود. همین اندازه کافی است بدانیم که در این پروژه‌ی ۶۰ هزار نفری، بعضی از شرکت‌کنندگان، علاوه بر حس کنجکاوی ریاضی، قصد داشتند سخت‌افزار کامپیوتر خود را نیز محک بزنند. عده‌ای نیز صرفاً به‌خاطر شهرت و ثبت نامشان در تاریخ با این پروژه همکاری کردند. ضمن آن‌که برای عده‌ای از شرکت‌کنندگان، انگیزه‌ی مالی نیز وجود داشت. زیرا یک شرکت خصوصی، جایزه‌ای ۱۰۰ هزار دلاری برای کشف اولین عدد اول ده‌میلیون رقمی تعیین کرده بود. (بزرگ‌ترین عدد اول شناخته‌شده تا آن زمان، کم‌تر از ده میلیون رقم داشت.)

در بیست سال گذشته اعداد اول موقعیتی استثنائی در عرصه‌ی رمزنگاری و دانش طراحی و شکستن رمزها کسب کرده‌اند. رمزها تنها از نظر نظامی و جاسوسی حائز اهمیت نیستند بلکه از آن‌ها در عرصه‌های تجاری، به‌خصوص تجارت اینترنتی به‌وفور استفاده می‌شود. هیچ‌کس نمی‌خواهد که دزدان دریایی عصر جدید، به اطلاعات شخصی مربوط به حساب‌های بانکی و یا شماره‌ی کارت‌های اعتباری آن‌ها دست یابند. می‌دانید که هم‌اکنون دزدی مشخصات فردی و جعل هویت افراد به‌صورت یکی از بزرگ‌ترین قلمروهای فعالیت تبهکاران در سطح بین‌المللی درآمده است و سازندگان کامپیوترها و ارایه‌دهندگان خدمات اینترنتی که بسیاری از فعالیت‌های خود را با اینترنت انجام می‌دهند، در تلاش هستند تا از خطر دست‌یابی این قبیل افراد به این اطلاعات، جلوگیری کنند.

یکی از مهم‌ترین سیستم‌هایی که در این رابطه مورد استفاده قرار می‌گیرد سیستم .R.S.A نام دارد که متکی به اعداد اول است.

به نظر می‌رسد مقدمه‌ی فوق برای تحریک حس کنجکاوی دانش‌آموزان و ارایه‌ی یک جلسه درس مؤثر در مورد اعداد اول کافی باشد. از نظر قدرت استدلالی و تحریک حس کنجکاوی آدمی، پر واضح است که نظریه‌ی اعداد در بین شاخه‌های دیگر ریاضی، نظیر ندارد و به قول هاردی، ریاضی‌دان انگلیسی، یک ماه آموزش محققانه در نظریه‌ی اعداد، دوبار آموزنده‌تر؛ دوبار مفیدتر؛ و دست‌کم ده‌بار سرگرم‌کننده‌تر از همان مدت تعلیم حسابان برای مهندسان است.

در ادامه، مطالبی را که درخصوص نظریه‌ی اعداد و دروس مرتبط با آن در دوره‌ی دبیرستان و پیش‌دانشگاهی جمع‌آوری شده است، می‌خوانید.

مطالب تخصصی

شاید بتوان موقعیت اعداد اول را همانند عناصر در شیمی و یا آجرهای یک ساختمان، تصور کرد. مبین این مطلب دو قضیه‌ی زیر است:

قضیه‌ی ۱. اگر p عددی اول باشد و $p|a.b$، آن‌گاه $p|b$ یا $p|a$.

قضیه‌ی ۲. (قضیه‌ی اساسی حساب) هر عدد صحیح بزرگ‌تر از یک را می‌توان به صورت حاصل‌ضربی از اعداد اول

نوشت (این نمایش به‌جز در ترتیب قرار گرفتن عوامل اول، یکتا است.)

با وجود مطالعه‌ی اعداد اول از قرن‌ها پیش، هنوز این اعداد، دارای رموز بسیاری هستند و ساختار آن‌ها به درستی شناخته نشده است. چگونگی توزیع آن‌ها بین اعداد، بسیار ناهنجار است. هر چند می‌توان با استفاده از تابع لگاریتم طبیعی، کرانی برای این ناهنجاری مشخص کرد، اما شکافی به اندازه‌ی دلخواه بزرگ در بین اعداد اول وجود دارد بدین معنی که به ازای هر عدد طبیعی دلخواه n، همواره می‌توان n عدد طبیعی متوالی یافت که هیچ‌یک از آن‌ها، اول نباشند. بهترین انتخاب، دنباله‌ی زیر است:

$$(n+1)!+2;(n+1)!+3,\cdots,(n+1)!+(n+1)$$

از سوی دیگر، بنابر اصل برتراند؛ همواره بین دو عدد طبیعی بزرگ‌تر از واحد n و $2n$، یک عدد اول وجود دارد. به‌عبارت دیگر $p_{k+1} < 2p_k$.

اصل مطلب

آیا اعداد اول همواره همانند آجرهای یک ساختمان و یا عناصر شیمی، متناهی هستند؟

قضیه‌ی اقلیدس. تعداد اعداد اول، نامتناهی است.

شاید قدیمی‌ترین و ساده‌ترین اثبات این قضیه، همان اثبات منسوب به اقلیدس باشد که در زیر ارایه می‌شود.

اثبات. فرض کنید تعداد اعداد اول متناهی بوده و این اعداد، عبارت باشند از $p_1, p_2, p_3, \cdots, p_k$. حال عدد $n = (p_1p_2p_3\cdots p_k)+1$ را در نظر بگیرید. واضح است که $n \neq p_i$. حال اگر فرض کنیم n، عدد اول نباشد (فرض خلف)، حتماً دارای عامل اولی مانند p_j است؛ پس $p_j|n$ و چون $p_j|p_1p_2p_3\cdots p_k$ درنتیجه $p_j|1$ که این نیز تناقض است. بنابراین فرض خلف باطل است و درنتیجه بی‌نهایت عدد اول وجود دارد.

اولین نکته‌ی حائز اهمیت در این‌جا، این است که فقط یک عدد اول زوج داریم و بقیه‌ی اعداد اول، فرد هستند و می‌دانیم هر عدد اول غیر از ۲ را فقط می‌توان به یکی از دو صورت $4k+3$ و یا $4k+1$ نوشت.

قضیه. بی‌نهایت عدد اول به شکل $4k+3$ وجود دارد.

اثبات. فرض کنیم تعداد اعداد اول به صورت $4k+3$ متناهی باشد و این اعداد، عبارت باشند از $p_1 = 3, p_2, p_3, \cdots, p_n$. عدد $m = 4(p_2, p_3, \cdots, p_n)+3$ را در نظر می‌گیریم. اگر m اول باشد که با فرض خلف تناقض دارد. اگر m اول نباشد، حداقل دارای عامل اول $p \neq 3$ و به شکل $p = 4k+3$ است. زیرا تمام عوامل اول m نمی‌توانند به فرم $4k+1$ باشند. از طرفی این $p > 3$، هیچ‌یک از اعداد اول $p_2, p_3, \cdots, p_n$ نیست. زیرا در غیر این صورت

$$\left.\begin{matrix} p|4(p_2p_3\cdots p_n) \\ P|m \end{matrix}\right\} \Rightarrow p|3 \Rightarrow p = 3$$

که تناقض است. بنابراین بی‌نهایت عدد اول به شکل $4k+3$ وجود دارد.

در کتاب **نظریه‌ی تحلیلی** اعداد، نوشته‌ی تام آپوستل، که کتابی تخصصی است، به نامتناهی بودن اعداد اول، به شکل $4k+1$ نیز اشاره شده است. در کتاب‌های دیگر، این مطلب را از قضیه‌ی دریکله نتیجه گرفته‌اند که اثبات آن از حوصله‌ی یک کتاب نظریه‌ی اعداد مقدماتی خارج است و خود به‌تنهایی، یک فصل از یک کتاب نظریه‌ی اعداد پیشرفته را شامل می‌شود.

هدف این مقاله، آن است که اثباتی از نامتناهی بودن اعداد اول به شکل $4k+1$ ارایه دهد به نحوی که قابل ارایه در کلاس‌های ریاضی دوره‌ی پیش‌دانشگاهی بوده و بتواند مورد استفاده‌ی معلمان قرار گیرد.

قضیه. تعداد اعداد اول به شکل $4k+1$ نامتناهی است.

اثبات. فرض کنیم $n > 1$ عددی طبیعی باشد. نشان می‌دهیم عدد اول p، که $p > n$ وجود دارد به‌طوری که $p \equiv 1 \pmod 4$.

قرار دهید

$$m = (n!)^2 + 1$$

واضح است که m، عددی فرد و بزرگ‌تر از ۱ است و هیچ‌یک از اعداد کوچک‌تر و یا مساوی n، مقسوم‌علیه m نمی‌باشد. بنابراین اگر p، یک عامل اول m باشد، خواهیم داشت $p > n$.

داریم

$$(n!)^2 \equiv -1 \pmod p$$

و درنتیجه

$$(n!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p \qquad (1)$$

و بنا به قضیه‌ی اویلر

$$(n!)^{p-1} \equiv 1 \pmod p \qquad (2)$$

زیرا $(p, n!) = 1$

از روابط (۱) و (۲) نتیجه می‌گیریم

$$1 \equiv (-1)^{(p-1)/2} \pmod p$$

بنابراین یکی از دو حالت زیر اتفاق می‌افتد:

الف) $1 \equiv -1 \pmod p$ به شرط آن‌که $(p-1)/2 = 2k+1$ یا به عبارتی $2 \mid p$ که این غیرممکن است زیرا $p > 2$.

ب) $1 \equiv 1 \pmod p$ به شرط آن‌که $(p-1)/2 = 2k$ و درنتیجه $p = 4k+1$ یعنی به‌ازای هر عدد طبیعی $n > 1$، عددی اول به شکل $p = 4k+1$ و بزرگ‌تر از n وجود دارد و از آن‌جایی که مجموعه اعداد طبیعی نامتناهی است، تعداد این گونه اعداد اول نیز نامتناهی است.

تذکر. می‌توان در اثبات این قضیه، $m = (2 \times 3 \times \cdots \times p_j)^2 + 1$ اختیار کرد که در آن p_j، بزرگ‌ترین عدد اول شناخته شده به شکل $4k+1$ است و $(2 \times 3 \times \cdots \times p_j)$ حاصل ضرب تمام اعداد اول کوچک‌تر یا مساوی p_j است. این انتخابِ m، علاوه بر آن‌که با اثبات اقلیدس از نامتناهی بودن اعداد اول، شباهت دارد، به ما این امکان را می‌دهد که اعداد اول را در فاصله‌های کوتاه‌تری جست‌وجو کنیم.*

اثبات قضیه با برهان خلف

فرض کنید تعداد اعداد اول شناخته شده به شکل $4k+1$ متناهی است و بزرگ‌ترین آن‌ها p_j باشد. قرار دهید $m = (2 \times 3 \times \cdots \times p_j)^2 + 1$. مطابق برهان قبل یا m اول است که در این صورت یک عدد اول به شکل $4k+1$ و بزرگ‌تر از p_j است که با فرض خلف متناقض است و یا m مرکب است که در این صورت دارای عامل اولی مانند p و بزرگ‌تر از p_j می‌باشد. حال ثابت می‌کنیم که p لزوماً به شکل $4k+1$ است.

$$m = (2 \times 3 \times \cdots \times p_j)^2 + 1 \Rightarrow (2 \times 3 \times \cdots \times p_j)^2 \equiv -1 \pmod p$$

$$\Rightarrow (2 \times 3 \times \cdots \times p_j)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p$$

از طرفی، بنا به قضیه‌ی اویلر

$$(2 \times 3 \times \cdots \times p_j)^{p-1} \equiv 1 \pmod p$$

درنتیجه

$$1 \equiv (-1)^{(p-1)/2} \pmod p$$

و بنابراین

$$p = 4k+1$$

و چون p بزرگ‌تر از p_j است، با فرض خلف تناقض دارد و درنتیجه تعداد اعداد اول به شکل $4k+1$، نامتناهی است.

در خاتمه، به بیان قضیه‌ی دریکله می‌پردازیم که دانستن آن خالی از لطف نیست. ضمن آن‌که بعضی از معلمان، برای توجیه نامتناهی بودن اعداد اول به شکل $4k+1$، به این قضیه استناد می‌کنند. البته باید توجه کنیم که این قضیه، بسیار کلی‌تر از این حکم است.

قضیه‌ی دریکله

هر دنباله‌ی حسابی از اعداد طبیعی که جمله‌ی اول و قدر نسبت آن نسبت به هم اول باشند، شامل بی‌نهایت عدد اول است.

به عبارت دیگر:

فرض کنید $a > 0$ و $b > 0$ و a و b نسبت به هم اول باشند. در این صورت بی‌نهایت عدد اول به شکل $ak+b$ وجود دارد.

چنان‌چه قبلاً اشاره شد، اثبات این قضیه نیازمند ابزارهای آنالیزی است ولیکن با یک شرط اضافه در بعضی از کتب، این قضیه را به صورت زیر اثبات کرده‌اند که از نظر نگارنده، این فرض اضافه معادل با حکم مسأله است و بنابراین، این اثبات خالی از ابهام نیست. درواقع این اثبات، نامتناهی بودن اعداد اول به شکل $ak+b$ را ثابت نمی‌کند بلکه نشان می‌دهد که در دنباله‌ی نامتناهی از اعداد اول به این فرم، زیر دنباله‌های دلخواه و نامتناهی وجود دارند.