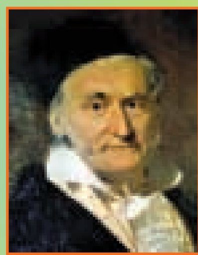
سرگذشت علوم

مهدی شیرزاد

سیری در نظریهٔ اعداد

ریاضیات، ملکهٔ علوم است و نظریهٔ اعداد ملکهٔ ریاضیات.


کارل فرید ریک گاؤس

نظریهٔ اعداد شاخه‌ای از دانش ریاضی است که به ویژگی‌های جالب اعداد ـ به‌طور خاص، اعداد صحیح می‌پردازد. بخش قابل توجهی از نظریه اعداد به کاوش در **«اعداد اول»**[۱] می‌پردازد.

عدد اول، عددی است طبیعی که تنها و تنها دو مقسوم علیه طبیعی دارد: یکی ۱ و دیگری خودش. البته با این تعریف عدد ۱ هم عددی اول خواهد بود. به‌دلیل یکتایی تجزیهٔ هر عدد طبیعی به ضرب عوامل اول، عدد ۱ را از دایرهٔ اعداد اول خارج می‌کنند. اعداد اول کوچک‌تر از ۱۰۰ (که شامل ۲۵ عدد هستند.) عبارت‌اند از:

۲،۳،۵،۷،۱۱،۱۳،۱۷،۱۹،۲۳،۳۱،۳۷،۴۱،۴۳،۴۷،۵۳،۵۹،۶۱،۶۷، ۷۱،۷۳،۷۹،۸۳،۸۹،۹۷

مجموعه اعداد اول نامتناهی است. برهان شورانگیزی که اقلیدس در ۳۰۰ سال پیش از میلاد مسیح اقامه کرده است نشان می‌دهد که بزرگ‌ترین عدد اول وجود ندارد. طبق «قضیهٔ اساسی حساب» هر عدد طبیعی بزرگ‌تر از ۱ را می‌توان به‌صورت ضرب اعداد اول نمایش داد. در واقع اعداد اول آجرهای بنای همهٔ اعداد طبیعی هستند. در عین حال چگالی اعداد اول میان اعداد طبیعی صفر است. در واقع با حداقل مصالح می‌توان بنایی با این عظمت برپا کرد.

توابع مولد اعداد اول

در پاپیروس رایند ـ که شاید قدیم‌ترین متون ریاضی متعلق به ۱۶۰۰ سال پیش از میلاد مسیح است ـ شواهدی دال بر آشنایی با اعداد اول وجود دارد. پس از آن قدیم‌ترین متون معتبر به یونان باستان و سپس به قرن ۱۷ میلادی برمی‌گردد. **فرما** در سال ۱۶۴۰ میلادی ادعا کرد که هر عدد به شکل $F(n)=۲^{۲^n}+۱$، عددی اول است. به ازای $n=۱$ تا $n=۴$ واقعاً اعدادی اول حاصل می‌شود:

$F(۱)=۲^{۲}+۱=۵$

$F(۲)=۲^{۲^{۲}}+۱=۲^{۴}+۱=۱۷$

$F(۳)=۲^{۲^{۳}}+۱=۲^{۸}+۱=۲۵۷$

$F(۴)=۲^{۲^{۴}}+۱=۲^{۱۶}+۱=۶۵۵۳۷$

اما اویلر در سال ۱۷۳۲ ثابت کرد که $F(۵)$ عددی تجزیه‌پذیر است:

$F(۵)=۲^{۲^{۵}}+۱=۶۴۱\times۶۷۰۰۴۱۷$

تاکنون هیچ عدد اولی بزرگ‌تر از $F(۴)$ از فرمول فرما حاصل نشده است. از دیگر توابع مولد اعداد اول می توان به تابع زیر اشاره کرد:

$F(n)=n^{۲}-n+۴۱$

به ازای $n=۱,۲,۳,...,۴۰$ عدد اول حاصل می‌شود. ولی به ازای $n=۴۱$ داریم:

$F(n)=۴۱^{۲}$

که عددی اول نیست.

از دیگر توابع چند جمله‌ای می‌توان به تابع زیر اشاره کرد:

$F(n)=n^{۲}-۷۹n+۱۶۰۱$

به ازای $n=۱$ تا $n=۷۹$ عدد اول حاصل می شود، ولی به ازای $n=۸۰$ عددی غیراول بدست می‌دهد.

ثابت می‌شود که هیچ تابع چند جمله‌ای با ضرایب گویا نمی‌توان یافت که تمام اعداد اول را تولید کند و هیچ عدد غیر اولی هم تولید نکند.

دره‌هایی میان اعداد اول

غیر از ۲ بقیهٔ اعداد اول فرد هســـتند. اگر دو عدد اول، دو عدد فرد متوالی باشـــند، به آن‌ها **اعداد اول دوقلو**[۲] گفته می‌شود: مثل (۳،۵) و (۵،۷)، (۱۱،۱۳)، (۲۹،۳۱) و... این نشان می‌دهد که فاصله دو عدد اول می‌تواند خیلی کم باشد. از آن طرف دره‌هایی بزرگ در میان اعداد اول می‌توان یافت. قضیهٔ ساده‌ای وجود دارد که به ازای هر عدد طبیعی n، دنباله‌ای از (n-۱) عدد طبیعی می‌توان یافت که همگی عدد مرکب هستند:

n!+۲=(۲×۳×...×n)+۲=۲ (۳×۵×...×n+۱)= ۲ مضرب

n!+۳=(۲×۳×...×n)+۳=۳ (۲×۵×...×n+۱)= ۳ مضرب

:

n!+n=(۲×۳×...×n)+n=n (۲×۳×...×(n-۱)+۱)= n مضرب

یعنی دنبالهٔ اعداد فوق همگی مرکب هســـتند. این نشـــان می‌دهد که توزیع اعـــداد اول در میان اعداد طبیعی، توزیع غریبی است. گاهی دو عدد اول متوالی فوق‌العاده نزدیک هم هستند و گاهی هم هزاران کیلومتر از هم فاصله می‌گیرند!

قضیهٔ اعداد اول

اعداد اول در واقع ســـنگ بنا و آجرهای ساختمانی اعداد طبیعی هستند ولی نکته آن است که این آجرها فوق‌العاده اندک هستند. به سوال زیر توجه کنید:

«اگـــر از مجموعـــهٔ $\{۱,۲,۳,...,n\}$ یک عدد بـــه تصادف انتخاب شود به چه احتمال این عدد، عددی اول می‌باشد؟»

تعـــداد اعداد اول کوچکتر یا مســـاوی n را بـــا A(n) نمایش می‌دهیم. به فهرست زیر توجه کنید. اعداد طبیعی ۱ تا ۲۰ درجه شده‌اند و زیر اعداد اول خطی کشیده شده است:

۱،**۲**،**۳**،۴،**۵**،۶،**۷**،۸،۹،۱۰،**۱۱**،۱۲،**۱۳**،۱۴،۱۵،۱۶،**۱۷**،۱۸،**۱۹**،۲۰

در واقع در این فهرست ۸ عدد، اول هستند یعنی:

A(۲۰)=۸

هرچه n افزایش یابد، A(n) هم افزایش می‌یابد ولی سرعت رشـــد A(n) در مقابل n خیلی کم‌تر است. به جدول زیر توجه کنید. در این جدول «فراوانی نســـبی» اعـــداد اول در میان هزار، میلیون و میلیارد عدد طبیعی درج شده است:

n	An/n
۱۰۳	۰/۱۶۸
۱۰۶	۰/۰۷۸۴۹۸
۱۰۹	۰/۰۵۰۸۴۷۴۷۸

دقت کنید فراوانی نسبی را می‌توان عملاً معادل احتمال یافت شـــدن یک عدد اول در میان n عدد طبیعی دانســـت. همانطور که در این جدول پیدا اســـت، با افزایـــش n این احتمال به صفر می‌گراید.

البته جدول بالانظم خاصی برای فراوانی نسبی توزیع اعداد اول نشان نمی‌دهد: یا اگر نظمی هم وجود دارد به این راحتی‌ها قابل رویت نیست. این جا است که نبوغ ریاضی خود را نشان می‌دهد. نابغهٔ بی‌بدیل ریاضیات **«گاؤس»** حدس زد که نسبت $\frac{An}{n}$ بطور مجانبی به $\frac{۱}{\log n}$ میل می‌کند. در واقع مطابق با این حدس برای nهای بزرگ می‌توان نوشت:

$$A(n)=\frac{n}{\log n}$$

دقـــت کنید logn برآوردی از تعداد ارقام یک عدد اســـت (۳) پـــس فراوانی نســـبی اعداد اول در میان اعـــداد طبیعی ۱ تا n با تعداد ارقام n نسبت عکس دارد.

مثلاً فرض کنید بخواهیم برآوردی از تعداد اعداد اول کوچکتر از یک میلیون داشته باشیم:

$$A(۱۰^{۶})=\frac{۱۰^{۶}}{\log ۱۰^{۶}}=\frac{۱۰^{۶}}{۶}=۱۶۷۰۰۰$$

پی‌نوشت

1. Prime number
2. Twine Prim numbers

۳. اگر قسمت صحیح لگاریتم برابر n باشد آن عدد (n+۱) رقم غیر اعشاری دارد. مثلاً اگر $\log A=۳/۱۴$ آنگاه A عددی چهار رقمی است.