سلسله درس‌هایی از ریاضیات گسسته (۶)

فرمولی در اعداد اول و نتایج آن

● سید محمدرضا هاشمی موسوی
hashemi – moosavi@yahoo.com

● جست‌وجوی دستوری برای تعیین اعداد اول

از اساسی‌ترین مسأله‌هایی که در رابطه با اعداد اول مطرح می‌شوند، مسأله‌های زیرند:

۱. تعیین دستور کلی برای محاسبه‌ی p_n (n امین عدد اول) بر حسب n.

۲. تعیین دستور کلی که P_{n+1} را بر حسب P_n بیان کند.

۳. تعیین تابعی که مقادیرش همگی عدد اول باشند.

واضح است که در این مسأله‌ها و مسأله‌های مشابه، جواب‌های بی‌مایه از بحث خارجند. توزیع اعداد اول به حدی نامنظم است که بعضی از ریاضیدانان بزرگ (با اعتذار از محضر ولای ایشان)، شتابزده برخی از این مسأله‌ها را «نامعقول» شمرده‌اند. برای مثال، در صفحه‌ی ۵ کتاب مشهور «مدخلی بر تئوری اعداد»، چاپ سال ۱۹۴۵ هاردی‌ورایت، چنین آمده است: «البته باید به خاطر داشت که یک سؤال طبیعی، اغلب پس از بحث و بررسی، به صورت سؤالی به‌کلی نامعقول در می‌آید... آیا دستوری کلی برای nامین عدد اول P_n وجود دارد؟... گرچه این سؤال را به عنوان یک سؤال طبیعی، می‌توان مقبول دانست، اما به کلی نامعقول است.»

پس از آن‌که در آن ایام، دستور گونه‌هایی برای حل مسأله‌ی ۱ عرضه شد، در چاپ ۱۹۶۸ همان کتاب، پس از مقدمه‌ی ذکر شده چنین می‌خوانیم: «آیا دستور کلی برای nامین عدد اول P_n هست؟... چنین دستوری را نمی‌شناسیم... محققاً امکان وجود چنین دستوری بعیدالاحتمال است.» چنان‌که ملاحظه می‌شود، دیگر صحبتی از «نامعقول» بودن سؤال در میان نیست.

بنابراین، مسأله‌هایی از این قبیل که گذشت و به‌خصوص تفحص در صورت‌های گوناگون اعداد برای حل مسأله‌های (۱) و (۳)، موضوع تحقیقات فراوان ریاضیدانان بوده است. در رابطه با مسأله‌ی (۳)، اعدادی به صورت‌های $a^n \pm 1$ که از مشهورترین آن‌ها اعداد اول فرما ($F(n) = 2^n + 1$) و اعداد اول مرسن ($M_p = 2^p - 1$) را می‌توان نام برد، مورد توجه قرار گرفتند. و در رابطه با مسأله‌ی (۲)، رابطه‌ای که $P_{n+1} \geq 3$ را برحسب «همه‌ی اعداد اول پیش از آن» بیان کند، رابطه‌ای است که گاندی[1] در کنگره‌ی ریاضیدانان مسکو در سال ۱۹۶۶ مطرح کرد.

در رابطه با مسأله‌ی (۳) باید گفت: از مسایل مهم مربوط به اعداد اول، مسأله‌ی توزیع آن‌ها در میان اعداد طبیعی است که مشکلات حل نشده‌ی بسیار دارد. قضیه‌ی زیر، پراکندگی اعداد اول را به خوبی آشکار می‌سازد و نشان می‌دهد که اعداد اول در میان اعداد طبیعی، مانند واحه‌هایی دور افتاده در صحرایی پهناورند.

قضیه: در رشته اعداد طبیعی، فواصلی هر قدر بزرگ که بخواهیم هست که خالی از اعداد اول است.

برهان اول: اگر n، عدد طبیعی دلخواهی باشد، از n عدد طبیعی متوالی زیر:

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

اولی بر ۲، دومی بر ۳و... و nامی بر n+۱ بخش‌پذیر است.

برهان دوم: فرض کنیم، p عددی اول باشد، هر قدربزرگ که بخواهیم و a حاصل‌ضرب اعداد اول از ۲ تا p باشد. واضح است که همه‌ی اعداد طبیعی متوالی زیر مرکب خواهند بود:

$$a+2, a+3, \cdots, a+p$$

تبصره: در مقابل این گونه قضیه‌ها، این قضیه برقرار است که اگر $n > 3$، آن‌گاه حداقل یک عدد اول بین n و $2n-2$ وجود دارد. این قضیه در سال ۱۸۴۵ به وسیله‌ی **برتران** مطرح و برای اولین‌بار در سال ۱۸۵۰ به وسیله‌ی **چبیچف** اثبات شد. قضیه‌ای بالاتر از این نیز ثابت شده که **سرپینسکی** در کتاب خود آن را به چاپ رسانده است.

قضیه: اگر $n > 5$ (عدد طبیعی)، بین n و 2n لااقل دو عدد اول متمایز وجود دارد.

نتیجه‌ی ۱. اگر $n > 1$ عددی طبیعی باشد، بین n و 2n لااقل یک عدد اول وجود دارد.

اثبات: طبق قضیه‌ی چبیچف، این حکم برای عددهای طبیعی بزرگ‌تر از ۳صحیح است. برای عددهای طبیعی ۲ و ۳هم صحیح است؛ زیرا بین ۲ و ۴عدد اول ۳ و بین ۳و۶ عدد اول ۵ قرار دارد.

نتیجه‌ی۲. برای عدد طبیعی $k > 1$، اگر P_k را نمادی برای kامین عدد اول به ردیف به‌کار بریم، می‌توان نوشت: $P_k < 2^k$ و داریم $P_2 = 3 < 2^2$. اگر برای عدد طبیعی k نابرابری $P_k < 2^k$ صحیح باشد، طبق نتیجه‌ی (۱)، لااقل یک عدد اول بین عددهای 2^k و 2^{k+1} وجود دارد که البته از P_k بزرگ‌تر است. بنابراین، نابرابری $P_{k+1} < 2^{k+1}$ هم با استقرای ریاضی صحیح است.

● چکیده‌ای از سیر تاریخی تلاش‌های دوهزار و سیصد ساله برای حل مسأله‌های اساسی اعداد اول

یکی از اولین پرسش‌هایی که درباره‌ی اعداد اول مطرح می‌شود چنین است: آیا تعداد اعداد اول محدود است یا نامحدود؟

پاسخ این سؤال برای اولین‌بار توسط **اقلیدس** (بیش از دوهزار و سیصد سال پیش) داده شد. او با نوعی استدلال ریاضی (برهان خلف) ثابت کرد، تعداد اعداد اول نامحدود است. از این زمان به بعد، ریاضیدانان کوشش بسیاری برای یافتن دستورهای ساده‌ی حساب به‌کار بردند که به مدد آن‌ها بتوان، فقط اعداد اول را یافت؛ حتی اگر این دستورها همه‌ی اعداد اول را به‌دست ندهند.

فرما در این مورد حدس مشهوری دارد (که به صورت حکم قطعی بیان نشد) و آن حدس چنین است:

همه‌ی اعداد به صورت $F(n) = 2^n + 1$ اول هستند.

این حدس به ازای $n = 0, 1, 2, 3, 4$ صحیح است و این گونه اعداد اول را «اعداد اول فرما» نام نهادند.

در سال ۱۷۳۲، اویلر توانست $F(5)$ را به صورت زیر تجزیه کند:

$$F(5) = 2^{2^5} + 1 = 641 \,.\, 6700417$$

بنابراین ثابت شدکه $F(5)$ عدد اول نیست. بعدها، اویلر توانست ثابت کند، بسیاری دیگر از این اعداد تجزیه‌پذیر و در نتیجه مرکب هستند.

لازم به ذکر است که روش‌های بسیار عمیقی برای تجزیه‌ی این اعداد در هر حالت خاص لازم است و به‌خاطر عظمت اعداد، غالباً این روش‌ها با مشکلات رفع نشدنی مواجه می‌شوند. تا به امروز هنوز نتوانسته‌اند ثابت کنند که به ازای

$n > 4$ ، بعضی دیگر از اعداد فرما عدد اول هستند.[2]

تابع بسیار جالب و ساده دیگری که تعدادی از اعداد اول را به دست می‌دهد، تابع اویلر است:

$$f(n) = n^2 - n + 41$$

در واقع به ازای $n = 1, 2, 3, \dots, 40$ ، عبارت $f(n)$ عدد اول به دست می‌دهد و حال آن که به ازای $n = 41$ خواهیم داشت: $f(41) = 41^2$ که عدد اول نیست.

تابع دیگری که به ازای $n = 1, 2, 3, \dots, 79$ عدد اول تولید می‌کند، به صورت زیر است:

$$f(n) = n^2 - 79n + 1601$$

این تابع مولد اعداد اول نیز، به ازای $n = 80$ با شکست مواجه می‌شود. **ریچارد کورانت** می‌گوید: «**در واقع جست‌وجوی عبارت‌های ساده‌ای که فقط عدد اول به دست دهند، کار بیهوده‌ای است و بیهوده‌تر از آن، کوشش برای یافتن دستوری جبری است که «همه‌ی» اعداد اول را به دست دهد.**»

از زمان اقلیدس تا هم‌اکنون، بشر در آرزوی فرمولی بوده است که فقط اعداد اول را بدهد. ابتدا فکر می‌کردند که یک چند جمله‌ای مانند $F(x)$ با ضرایب صحیح یافت می‌شود که وقتی به جای n مقدار صحیح گذاشته شود، عدد اول حاصل شود. اما به زودی دریافتند، اگر $F(a)=p$ اول باشد آن‌گاه $F(a+kp)$ برای هر k صحیح، بر p بخش‌پذیر است. یعنی ثابت شد که تابعی وجود ندارد و F نمی‌تواند فقط اعداد اول را توزیع کند. بعد از این‌که بشر از چند جمله‌ای ناامید شد، سراغ فرمول‌های غیرچند جمله‌ای رفت.

اولین کسی که فرمولی وجودی ارایه داد، **میلز**[3] بود که قضیه‌ی زیبای آن چنین است:

قضیه (میلز): عددی حقیقی مانند a وجود دارد به طوری که $F(n) = \left\lfloor a^{3^n} \right\rfloor_{n=1,2,\dots}$ اعداد اول را می‌دهد.

بعد از میلز این قضیه توسط **کوپیر**[4] به شکل زیر تعمیم داده شد:

قضیه (کوپیر): برای هر عدد صحیح $c \geq 3$ ، یک عدد حقیقی a وجود دارد، به طوری که $(n \in N)F(n) = \left\lfloor a^{c^n} \right\rfloor$ اعداد اول را می‌دهد.

بعدها قید صحیح بودن c نیز برداشته شد.

قضیه: اگر $c > \frac{8}{3}$ یک عدد حقیقی باشد، آن‌گاه یک عدد حقیقی مثل a وجود دارد، به طوری که $(n \in N)F(n) = \left\lfloor a^{c_1^n} \right\rfloor$ اعداد اول را می‌دهد.

و بالاخره **نیون**[5] قضیه‌ی زیر را ثابت کرد:

قضیه (نیون): برای هر عدد حقیقی $c > 1$ ، یک عدد حقیقی a وجود دارد، به طوری که $F(n) = \left\lfloor c^{a^n} \right\rfloor_{n=1,2,\dots}$ اعداد اول را می‌دهد.

توجه: عدد حقیقی a در قضایای بالا یکتا نیست. به علاوه، همه‌ی این فرمول‌ها وجودی هستند و هیچ‌کدام حتی یک عدد اول را هم مشخص نمی‌کنند.

کار روی کشف فرمولی برای تولید اعداد اول ادامه یافت تا سرانجام توسط **ویلانز**[6]، با استفاده از «**قضیه‌ی ویلسن**»، فرمولی برای تشخیص اعداد اول ارایه شد:

$$n \in N \ ; \ F(n) = \left\lfloor \cos^2 \pi \frac{(n-1)!+1}{n} \right\rfloor = \begin{cases} 1 & \text{اگر } n=1 \text{ یا } n \text{ اول باشد} \\ 0 & \text{اگر } n \text{ اول نباشد} \end{cases}$$

توضیح: در این تابع چون عدد $(n-1)!$ به کار رفته، واضح است که کار با آن غیر عملی است و حتی برای عددی نزدیک به $n = 10^{10}$ هم، غیرقابل محاسبه است. به همین علت، این تابع تشخیص فقط می‌تواند جنبه‌ی تئوری داشته باشد (عدد $100!$ نزدیک به عدد 5^{100} است، زیرا: $(n! \approx (\frac{n+1}{2})^n$.

حال اگر $\pi(m)$ تعداد اعداد اول نابیش‌تر از m باشد:

$$\pi(m) = -1 + \sum_{n=1}^{m} F(n) \qquad \text{(F: تابع ویلانز)}$$

و با توجه به این‌که kامین عدد اول، نابیش‌تر از 2^k است؛ P_k (kامین عدد اول) را نیز در قالب فرمولی می‌توان ارایه داد.

به همین ترتیب، فرمول‌های دیگری نیز با استفاده از «قضیه‌ی ویلسن» به دست آمد که به صورت زیر هستند:

(۞) اگر $\frac{(x-1)!^2}{x} = \frac{1}{x} + k$ (یک عدد صحیح) x اول باشد

(۞۞) اگر $x \nmid (x-1)!^2$ ، x اول نباشد

$$F(x) = \frac{\sin^2 \pi \frac{(x-1)!^2}{x}}{\sin^2 \frac{\pi}{x}} = \begin{cases} 1 & (۞) \\ 0 & (۞۞) \end{cases}$$

$$F(x, y) = \frac{y-1}{2}\left[\left|B^2 - 1\right| - (B^2 - 1)\right] + 2 \ ;$$

$x,y \in N$, $B = x(y+1)-(y!+1)$

طبق قضیه‌ی ویلسن، $(y+1)$ اول است و داریم $F(1,1)=2$ و اگر p یک عدد اول فرد باشد، آن‌گاه برای $y=p-1$ داریم:

$$x=\frac{1}{p}\left((p-1)!+1\right)$$

بنابراین:

$$F(x,y)=p$$

توضیح: عدد اول ۲ برای بی‌شمار مقدار x و y به دست می‌آید، ولی هر عدد اول فرد p فقط از یک زوج یکتای (x,y) به دست می‌آید.

فرمول جالب دیگری که در رابطه با یافتن n+1امین عدد اول، با داشتن اعداد اول کم‌تر از آن به دست آمد، توسط گاندی[1] در کنگره‌ی ریاضیدانان مسکو در سال ۱۹۶۶ مطرح شد. به این شکل که اگر p_n، nامین عدد اول فرض شود و μ تابع موبیوس و $Q=P_1.P_2.....P_n$، آن‌گاه $P_{n+1}\geq 3$ از نابرابری زیر به دست می‌آید:

$$1<2^{P_{n+1}}\left(-\frac{1}{2}+\sum_{d|Q}\frac{\mu(d)}{2^d-1}\right)<2$$

توجه داشته باشید، برای هر عدد حقیقی a، حداکثر یک عدد صحیح k یافت می‌شود، به طوری که داشته باشیم:

$$1<2^k.a<2$$

جای شگفتی است که ریاضیدانی چون هاردی نتوانست چنین فرمول‌هایی را به‌دست آورد. او حتی فکر می‌کرد، چنین فرمول‌هایی وجود ندارند. زیرا در سخنرانی خود در سال ۱۹۲۸ در آمریکا گفته است: «مثلاً اگر کسی از من بخواهد فرمولی برای nامین عدد اول بنویسیم یا P_{n+1} را بر حسب P_n بیابم، فقط می‌توانم بگویم که سؤال نامعقولی کرده است و احتمالاً چنین فرمولی وجود ندارد.»

کاش به همین جمله بسنده می‌کرد. او سپس با ارایه‌ی فرمول‌ها و توجیه‌هایی نشان می‌دهد که چنین فرمول‌هایی نباید وجود داشته باشند. البته این سخنرانی خیلی با اهمیت بود و بعداً در مجموعه مقالات MAA که جایزه دریافت می‌کنند، قرار گرفت. ولی باور کردنی نیست، فرمولی که وجودش فقط قضیه‌ی ویلسن را نیاز داشت، چنین دور از ذهن ریاضیدانی نظیر هاردی باشد. اگر او هم حالا زنده بود، برایش باور نکردنی بود که زمانی چنین اظهار نظری کرده است.

در جست‌وجوی قانونی که حاکم بر توزیع اعداد اول باشد، مرحله‌ی قاطع هنگامی طی شد که ریاضیدانان کوشش‌های بیهوده را برای یافتن دستور ریاضی ساده‌ای که «همه»ی اعداد اول را به دست دهد، کنار گذاشتند و از تعیین تعداد واقعی اعداد اولی که در میان n عدد متوالی ابتدا بر واحد وجود دارد، صرف نظر کردند. به جای آن، وجهه‌ی همت خود را متوجه به‌دست آوردن اطلاعاتی درباره‌ی «میزان متوسط» توزیع اعداد اول در میان همه‌ی اعداد کردند.

گائوس به وسیله‌ی ملاحظات تجربی که از مطالعه‌ی جداول اعداد اول حاصل می‌شد، به این نتیجه رسید که نسبت $\frac{\pi(N)}{N}$ به تقریب برابر با $\frac{1}{LnN}$ است و هر قدر که N بزرگ‌تر می‌شود، این مقدار تقریبی به واقعیت نزدیک‌تر خواهد بود. او نشان داد که رابطه‌ی $\frac{\pi(N)}{N}\approx\frac{1}{LnN}$ به‌طور مجانبی برابر است و به این ترتیب، مسأله‌ی تعداد اعداد اول نیز به‌طور تقریبی حل شد:

$$\pi(N)\approx\frac{N}{LnN}$$

نتیجه: با ملاحظه‌ی سیر تاریخی مربوط به مسأله‌های اساسی اعداد اول در می‌یابیم که همه‌ی اطلاعات امروز ما بر پایه‌ی «قضیه‌ی ویلسن» بنا شده‌اند و می‌دانیم که هر تابع بر این قضیه متکی باشد، هیچ ارزش عملی نخواهد داشت و تنها برهانی تئوریک را در بر دارد.

ادامه دارد

زیرنویس

1. J. M. Gandhi

۲. مقاله‌ای تحت عنوان «تجزیه‌ی اعداد فرما» برای $n>4$ و مرکب بودن آن‌ها، از این جانب آماده‌ی چاپ است.

3. W.H.Mills

4. L.Kuiper

5. I.Niven

6. C.P.Willans

منابع

۱. مصاحب، دکتر غلامحسین. تئوری مقدماتی اعداد (دوره ۵ جلدی)

۲. کورانت، ریچارد ورابینز، هربرت. ریاضیات چیست؟

۳. مجله رشد آموزش ریاضی. سازمان پژوهش و برنامه‌ریزی درسی آموزش وپرورش

۴. سرپینسکی، واتسلا. ۲۵۰ مسأله‌ی حساب.

5. The discovery of prime numbers formula and it's results & other top researches (uthor: S.M.R.Hashemi Moosavi)(Brill/Vsp)

6. www.primenumbersformula.com