سلسله درس‌هایی از ریاضیات گسسته ۵

سیدمحمدرضا هاشمی موسوی

می‌دانیم که بی‌نهایت عدد اول وجود دارد، توزیع اعداد اول در مجموعه‌ی اعداد طبیعی بسیار پر رمز و راز است و به ظاهر هیچ قاعده و قانونی ندارد. آن‌ها مانند علف‌های هرز در میان اعداد طبیعی رشد می‌کنند و هیچ کس نمی‌تواند پیش‌بینی کند، عدد اول بعدی کجا سبز خواهد شد. چاپ مقاله‌ای با عنوان «نخستین ۵۰ میلیون عدد اول»[۱]، دید اندیشمندان و محققان ریاضی را به کلی عوض کرد و نظر فعلی آن‌ها چنین است: «اعداد اول از نظم حیرت‌آوری پیروی می‌کنند. قوانینی بر چگونگی رفتار آن‌ها حکمفرماست و این اعداد، تقریباً با انضباطی نظامی از این قوانین تبعیت می‌کنند.»

می‌دانیم که به جز نخستین دو عدد اول، یعنی ۲ و ۳، هیچ دو عدد اولی متوالی نیستند؛ زیرا همه‌ی اعداد اول غیر از ۲، فردند. بنابراین، اختلاف دو عدد اول متوالی حداقل برابر ۲ است. برای بیان این حالت، تعریف زیر را می‌آوریم:

تعریف: دو عدد اول متوالی که اختلاف آن‌ها برابر ۲ باشد را در اصطلاح «جفت دوقلو» می‌نامیم. برای مثال، جفت‌های دوقلوی «۵ و ۷»، «۱۱ و ۱۳»، «۱۷ و ۱۹»، «۲۹ و ۳۱» و «$10^{12}+61$ و $10^{12}+63$» نمونه‌هایی از جفت اعداد دوقلو هستند.

تاکنون در مورد نامتناهی یا متناهی بودن جفت‌های دوقلو به نتیجه‌ای دست نیافته‌اند. با استفاده از محاسبه‌گرها، تعداد ۱۵۲۹۸۲ جفت دوقلوی کوچک‌تر از 3×10^{7} و بین 10^{12} و $10^{12}+10000$، ۲۰ جفت عدد دوقلو یافته‌اند که این واقعیت نشانگر رشد افزایشی ولی بسیار کند این اعداد در مجموعه‌ی

اعداد طبیعی است. به‌علاوه، نشان می‌دهند که اعداد اول تا چه حد می‌توانند نزدیک به هم باشند.

از طرف دیگر، در میان اعداد اول شکاف‌های پهناوری وجود دارند؛ شکاف‌هایی به اندازه‌ی دلخواه بزرگ در مجموعه‌ی اعداد اول. به بیان دیگر، برای هر عدد طبیعی n، به تعداد n عدد متوالی وجود دارند که همگی مرکبند؛ زیرا n عدد متوالی زیر همگی مرکبند:

$$(n+1)!+2 = 1\times2\times3\times\ldots\times(n+1)+2 = 2k_1+2 = 2(k_1+1)$$
$$(n+1)!+3 = 1\times2\times3\times\ldots\times(n+1)+3 = 3k_2+3 = 3(k_2+1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(n+1)!+(n+1) = 1\times2\times3\times\ldots\times(n+1)+(n+1) = (n+1)k_n+(n+1) = (n+1)(k_n+1)$$

بنابراین، در این‌جا ثابت شد که به ازای هر k با شرط $2 \le k \le n+1$، عدد $(n+1)!+k$ مرکب و بر k بخش‌پذیر است. پس برای مثال، اگر بخواهیم ۴۰ عدد متوالی نشان دهیم که در میان آن‌ها هیچ عدد اولی موجود نباشد، به‌راحتی می‌توان ۴۰ عدد: ۴۱!+۲، ۴۱!+۳، ... و ۴۱!+۴۱، را پیشنهاد داد. با مشاهده‌ی جدول‌های اعداد اول می‌توان پذیرفت که هیچ دلیل روشنی برای این که چرا عددی اول است و عدد دیگری مرکب، وجود ندارد.

با مشاهده‌ی این اعداد، انسان خود را در برابر یکی از رازهای غیرقابل توضیح آفرینش می‌بیند. تلاش پیگیر ریاضیدانان هم سالیان سال است که نتوانسته است رمز و راز این اعداد مرموز را بشکافد. ریاضیدانان به دنبال اعداد اولی هستند که از اعداد اول شناخته شده‌ی قبلی بزرگ‌تر باشد. برای مثال، در سال ۱۸۷۶، لوکاس ثابت کرد که عدد $(2^{127}-1)$ اول است. مدت ۷۵ سال، این عدد بزرگ‌ترین عدد اول شناخته شده بود. دیدن این عدد ممکن است، این واقعه‌ی تاریخی را برای ما ملموس‌تر کند؛ زیرا این عدد، یک عدد ۳۹ رقمی است:

$$2^{127}-1=\overbrace{170141183460\ldots\ldots\ldots7}^{\text{۳۹ رقم}}$$

از سال ۱۹۴۱، با ظهور ماشین‌های محاسبه‌گر الکترونیکی، اعداد اول بزرگ‌تری کشف شدند. از جمله کسانی که به عددهای اول بزرگ‌تری رسیدند، می‌توان فرید، میلر، ویلر، لمر، رابینسون، ریول، هورویتس، سلفویج، گیلیس، تاکرمن، نول، نیکل، اسلووینسکی، نلسون و دمبارت را نام برد. بزرگ‌ترین عدد اولی که تا سال ۱۹۸۵ شناخته شده بود، عددی ۶۵۰۵۰ رقمی بود که دمبارت آن را چنین $(2^{216091}-1)$ نمایش داد (برای آشنایی با اعداد بزرگ اول، به مقاله‌ی ارزشمند «نخستین ۵۰ میلیون عدد اول» از دان زاگیر رجوع کنید).

در حال حاضر (۲۰۰۶) عدد $(2^{30402457}-1)$ (یعنی مِرسن۴۳) بزرگ‌ترین عدد شناخته شده است.

توابع مولد اعداد اول

هر عدد اول فرد به یکی از صورت‌های $4k \pm 1$ یا $6n \pm 1$ و... می‌تواند ظاهر شود. در واقع، با هریک از این دستورها می‌توان، همه‌ی اعداد اول را تولید کرد. ولی مسأله‌ی اصلی در این‌جا، یافتن دستوری است که به ازای هر عدد طبیعی دلخواه، یک عدد اول تولید کند. یعنی دستوری یا قانونی ارائه دهیم که فقط عدد اول توزیع کند. می‌دانیم تا به حال انسان به چنین دستوری دست نیافته و فقط دستورهای خاصی نظیر: $f(n)=n^2+n+11$، $F(n)=n^2-n+41$ (دستور اویلر) و... را به‌دست آورده است که هیچ‌یک از این دستورها جوابگوی مسأله‌ی «تابع مولد اعداد اول» نخواهد شد. زیرا، اولین دستور به‌ازای $1 \le n \le 9$، و دومین دستور به ازای $1 \le n \le 40$، عددی اول است، ولی $f(10)=11^2$ و $F(41)=41^2$، اعداد اول نیستند و همین یک نمونه برای هریک از این دستورها کافی است تا آن‌ها را از درجه‌ی اعتبار ساقط کند.

دیریکله[2] ثابت کرد، اگر a و b نسبت به هم اول باشند، عبارت $ak+b$ به ازای اعداد طبیعی k، بی‌نهایت عدد اول تولید می‌کند. با این همه، تا به حال هیچ عبارتی به صورت $ak+b$، شناخته نشده است که فقط اعداد اول تولید کند.

مسأله: ثابت کنید، هیچ چندجمله‌ای با ضرایب صحیح وجود ندارد که مولد اعداد اول باشد.

اثبات: فرض می‌کنیم $f(n)$ چندجمله‌ای مولد اعداد اول باشد؛ یعنی به ازای هر n طبیعی، فقط اعداد اول تولید کند:

(a_iها اعداد صحیح و $a_k \neq 0$)

$$f(n)=a_k n^k+\ldots+a_1 n+a_0$$

به ازای عدد ثابتی مثل n_1، $f(n_1)$ عددی اول است:

$$f(n_1)=p$$

حال عبارت $f(n_1+pm)$ را به ازای اعداد صحیح m درنظر می‌گیریم. بنابراین:

$$f(n_1+pm)=a_k(n_1+pm)^k+\ldots+a_1(n_1+pm)+a_0$$

$$= (a_k n_1^k + \dots + a_1 n_1 + a_0) + pT(m)$$
$$= p + pT(m)$$
$$= p(1 + T(m))$$

$T(m)$ یک چندجمله‌ای با ضرایب صحیح است. بنابراین، $f(n)$ به ازای بی‌نهایت عدد صحیح، اعداد مرکب تولید می‌کند و این با فرض مسأله تناقض دارد.

توجه: هر چندجمله‌ای از درجه‌ی k، بیش از k مرتبه (به عدد درجه‌ی خود) نمی‌تواند یک مقدار خاص را به خود اختصاص دهد. بنابراین، $f(n)$ و حالت خاص آن $f(n_1 + pm)$، به ازای همه‌ی اعداد صحیح نمی‌توانند برابر مقدار خاصی مثل صفر یا $\pm p$ شوند.

در سال‌های اخیر، ریاضیدانان به موفقیت‌هایی در زمینه‌ی توابع مولد اعداد اول دست یافته‌اند که از همه‌ی آن‌ها مهم‌تر، قضیه‌ی میلز[3] است که ثابت می‌کند، عدد حقیقی مثبتی مثل r یافت می‌شود که در دستور زیر قرار می‌گیرد و دستور زیر:

$$n \in \mathbb{N}:\ f(n) = \left\lfloor r^{3^n} \right\rfloor \quad (\lfloor\ \rfloor : \text{قسمت درست عدد})$$

به ازای هر n طبیعی، فقط عدد اول تولید می‌کند[4]. بدیهی است که این دستور فقط وقتی ارزش دارد که عدد حقیقی r معلوم شود؛ زیرا با این دستور، حتی یک عدد اول هم نمی‌توان ساخت.

اعداد فرما

در این جا، نوع خاصی از اعداد را معرفی می‌کنیم که محرکی برای پژوهش و تحقیقات فراوان در زمینه‌ی اعداد اول شده است. این نوع اعداد خاص به صورت $(2^m + 1)$ هستند. ابتدا به بررسی مسأله‌ی زیر می‌پردازیم.

مسأله: در صورتی که $(2^m + 1)$ عددی اول باشد، ثابت کنید m باید به صورت توانی از ۲ باشد:

$$\text{عدد اول} = 2^m + 1 \Rightarrow m = 2^n$$

اثبات: با فرض این که m توانی از ۲ نباشد، به تناقض خواهیم رسید. زیرا، اگر m دارای یک شمارنده‌ی فرد مثل $2k + 1\ (k \geq 1)$ باشد:

$$m = (2k+1)s$$

بنابراین، می‌توان نوشت:

$$2^m + 1 = 2^{(2k+1)s} + 1 = (2^s)^{2k+1} + 1$$
$$= (2^s + 1)(2^{2ks} - 2^{(2k-1)s} + \dots + 2^{2s} - 2^s + 1)$$

یعنی $2^m + 1$، در صورتی که m دارای شمارنده‌ی فرد باشد، دارای تجزیه‌ی نابدیهی است و این خلاف اول بودن $2^m + 1$ است.

تعریف: هر عدد به صورت $F_n = 2^{2^n} + 1\ (n \geq 0)$ را «عدد فرما» گویند و اگر F_n اول باشد، آن را عدد اول فرما می‌نامند.

نکته: همه‌ی اعدادی که به صورت $(n^{n^n} + 1)$ هستند، به ازای هر $n > 1$ (طبیعی) وقتی اولند که n به صورت $2^{2^k} (k \geq 0)$ باشد. فرما، که اغلب حدس‌هایش مورد توجه ریاضیدانان بوده است، مشاهده کرد که F_n به ازای $n \in \{0,1,2,3,4\}$، عددی اول است:

$$F_0 = 2^{2^0} + 1 = 3,\quad F_1 = 2^{2^1} + 1 = 5,\quad F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257,\quad F_4 = 2^{2^4} + 1 = 65537$$

بنابراین، تصور کرد که همه‌ی F_nها اولند. فرما در نامه‌ای که به مرسن نوشت، متذکر شد که من اعدادی به صورت $2^{2^n} + 1$ یافته‌ام که همیشه اولند و ریاضیدانان سال‌های بعد درستی آن را خواهند فهمید. در سال ۱۷۳۲، اویلر نشان داد که عدد F_5 مرکب است و عدد F_5 بر ۶۴۱ بخش‌پذیر است:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

در سال‌های بعد، ثابت شد که F_6 و F_7 نیز مرکب است. در مورد عدد F_8 و عددهای بعدی[5] نیز همچنان مبارزه ادامه داشت، تا این که ثابت شد، F_8 نیز مرکب است، ولی مدت‌ها قادر به تجزیه‌ی آن نشده بودند تا سرانجام با عرضه‌ی ماشین‌های محاسبه‌گر جدید، این مشکل هم مرتفع شد.

تا امروز معلوم نشده است که آیا تعداد اعداد اول فرما محدود است یا نامحدود. در خاتمه، درباره‌ی اعداد اول فرما همین بس که تا به حال یک عدد اول بزرگ‌تر از F_4 هم یافت نشده است.

اعداد مرسن

در ریاضیات، اعداد به صورت $M_n = 2^n - 1$ را به نام کشیش فرانسوی، مارین مرسن[6] [۱۶۴۸ـ۱۵۸۸] «اعداد مرسن» نامیده‌اند؛ چرا که مرسن در زمینه‌ی اول بودن این نوع اعداد، اظهارنظری نادرست اما محرک کرده بود که سبب پژوهش‌ها و تحقیقات بسیاری در رابطه با اعداد اول شد.

تعریف: هر عدد به صورت $M_n = 2^n - 1$ که اول باشد را، عدد اول مرسن می‌نامند. در سال ۱۶۴۴، مرسن اظهار داشت که عدد $M_p = 2^p - 1$ به ازای اعداد اول زیر:

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

عددی اول و به ازای سایر اعداد $p < ۲۵۷$ عدد M_p مرکب است.

ریاضیدانان معتقدند که به یقین، مرسن همه‌ی اعدادی را که ادعا کرده بود اول هستند، آزمایش نکرده بود. سال‌ها بعد، اویلر ثابت کرد که عدد $M_{۳۱} = ۲^{۳۱} - ۱$ اول است. ولی نظری روی اعداد $M_{۶۷}$، $M_{۱۲۷}$ و $M_{۲۵۷}$ نداشت، زیرا این اعداد بسیار بزرگ و دور از دسترس او بودند. در حال حاضر می‌دانیم که مرسن ۵ خطا داشته است؛ یعنی $M_{۶۷}$ و $M_{۲۵۷}$ را به خطا تصور کرده بود اول هستند و $M_{۶۱}$، $M_{۸۹}$ و $M_{۱۰۷}$ را از زمره‌ی اعداد اول حذف کرده بود.

در اکتبر سال ۱۹۰۳، ریاضیدانی آمریکایی به نام **نلسون کول**[7] مقاله‌ای تحت عنوان «تجزیه‌ی اعداد بزرگ» به «انجمن ریاضی آمریکا» ارایه داد. پس از آن که او را به جایگاه سخنرانی دعوت کردند، پیش چشم حاضران روی تخته‌ی سیاه، عدد ۲ را ۶۷ بار در خودش ضرب کرد و به دقت یک واحد از آن کم کرد. در واقع عدد $M_{۶۷} = ۲^{۶۷} - ۱$ را حساب کرد. سپس بدون این که کلمه‌ای بگوید در گوشه‌ی دیگر تخته‌ی سیاه، حاصل ضرب زیر را نوشت:

$$۱۹۳۷۰۷۷۲۱ \times ۷۶۱۸۳۸۲۵۷۲۸۷$$

این حاصل ضرب به طور دقیق برابر عددی بود که از محاسبه‌ی $۲^{۶۷} - ۱$ به دست آورده بود. مدت‌ها بعد، به یکی از دوستانش گفته بود که او ۲۰ سال تمام عصر یکشنبه‌های خود را صرف یافتن عوامل عدد $M_{۶۷} = ۲^{۶۷} - ۱$ کرده بود (همان طور که ثابت شد و دیدیم که اگر $۲^p - ۱$ اول باشد، p اول است).

مسأله: ثابت کنید که عدد $M_{۲۳۷} = ۲^{۲۳۷} - ۱$، مرکب است. سپس یکی از عامل‌های نابدیهی آن را بیابید.

اثبات: چون $۳|p = ۲۳۷$، پس $M_{۲۳۷}$ عددی مرکب است. یکی از عامل‌های نابدیهی آن از تجزیه‌ی $M_{۲۳۷}$ به دست می‌آید:

$$\begin{aligned} M_{۲۳۷} &= ۲^{۲۳۷} - ۱ = (۲^۳)^{۷۹} - ۱ \\ &= (۲^۳ - ۱)\underbrace{\left[(۲^۳)^{۷۸} + (۲^۳)^{۷۷} + \dots + (۲^۳) + ۱\right]}_{k} \end{aligned}$$

$$M_{۲۳۷} = ۲^{۲۳۷} - ۱ = ۷k \Rightarrow ۷ \mid M_{۲۳۷} = ۲^{۲۳۷} - ۱$$

پس، عامل نابدیهی آن، عدد ۷ است.

تمرین: یکی از عامل‌های نابدیهی $M_{۲۰۲}$، $M_{۹۱}$ و $M_{۲۱}$ را بیابید و نشان دهید $M_{۱۱}$ و $M_{۲۲}$ اولند.

زیرنویس

۱. خلاصه‌ای از این مقاله، در مجله‌ی نشر ریاضی، سال ۱، شماره‌ی ۳ آذرماه ۱۳۶۷ درج شده است.

2. Dirichlet

3. W.H.Mills

(برهان این قضیه در جلد دوم، قسمت دوم، تئوری اعداد دکتر مصاحب آمده است.)

۴. در حالت کلی قضیه برای $f(n) = \left\lfloor \theta^{c^n} \right\rfloor$، به ازای هر n طبیعی و هر $c > \frac{۶۱}{۲۳}$ (ناکم‌تر از ۳) برقرار است.

۵. هر مقسوم‌علیه عدد $F_n\ (n > ۱)$ به صورت $۲^{n+۲}k + ۱$ است (قضیه‌ی لوکا).

6. Marin Mersenne

7. Nelson Cole

8. Faber

9. Worldwide

۱۰. چنین فرمولی در تاریخ ۱۳۸۲/۵/۱۴ (سال ۲۰۰۳ میلادی) توسط مؤلف کشف شده است که نتایج بسیاری را در بر داشته است. از جمله «حل معادله‌ی زتای ریمان» است (این مسأله یکی از هفت مسأله‌ی لاینحل جهانی است) -. برای اطلاع بیشتر از این اکتشاف بزرگ قرن (مسأله لاینحل ۲۳۰۰ ساله) می‌توانید به کتابی تحت عنوان «کشف فرمول اعداد اول و نتایج آن» که توسط مؤسسه (انتشاراتی) استاندارد بین‌المللی (ISI) به نام Brill/VSP کشور هلند (VSP آمریکا) به چاپ خواهد رسید، رجوع شود.

همچنین می‌توانید به سایت مؤلف نیز رجوع کنید:

www.primenumbersformula.com

سایت‌های انتشارات Brill/VSP:

www.brill.nl

www.vsppub.com

نام کتاب: (این کتاب به توسط انتشارات معراج قلم چاپ شده است).

"The discovery of prime numbers formula and its results"

(ISBN: 964-93227-7-9)

یکی از فرمول‌های اعداد اول که با توجه به قضیه‌ی ویلسن توسط مؤلف ارائه شده است را می‌آوریم:

$$H(m) = ۲\left(\frac{۲m+۱}{۲}\right)\left\lfloor \frac{۲m+۱}{(۲m)!+۱}\left\lfloor \frac{(۲m)!+۱}{۲m+۱} \right\rfloor \right\rfloor$$

$$\begin{aligned} D_H = \mathbb{N}\ ,\ R_H = \mathbb{P} &= \{۳,۵,۷,۲,۱۱,۱۳,۲,۱۷,۱۹,\dots\} \\ &= \{۲,۳,۵,۷,۱۱,۱۳,۱۷,۱۹,\dots\} \\ &= \left\{ n \in \mathbb{N} : H(m) = ۲\left(\frac{۲m+۱}{۲}\right)^{\Delta_m} \right\} \end{aligned}$$

مقاله‌ای تحت عنوان «کشف فرمول اعداد اول و نتایج آن» در ادامه مطالب ارائه خواهد شد و از فرمول‌های اصلی و نتایج آن که در مجله‌ی ISI به نام "Acta Applicandae Mathematicae" به چاپ خواهد رسید با اطلاع خواهید شد.