مقالات کوتاه از مجلات ریاضی معتبر جهان (۱۷)

ترجمه: غلامرضا یاسی‌پور

اعداد اول، تجزیه و رمزهای مخفی

(قسمت سوم)

در همایش اکتبر ۱۹۰۳ی انجمن ریاضی معتبر آمریکایی، نام فردریک *نلسون کول*[1] ریاضیدان در فهرست برنامهٔ انجمن به عنوان ارائه‌دهندهٔ مقاله‌ای با عنوان متواضعانهٔ «راجع به تجزیهٔ اعداد بزرگ[2]» آمده بود. هنگامی که نام *کول* را برای سخنرانی خواندند، وی به طرف تخته سیاه رفت و، بدون اظهار کلمه‌ای، محاسبهٔ ۲ به توان ۶۷ را انجام داد، و بعد از آن ۱ واحد از نتیجه کم کرد، و در حالی که همچنان چیزی نمی‌گفت به طرف قسمت نوشته نشده‌ای از تخته سیاه رفت و اعداد زیر را در هم ضرب کرد

۲۸۷ ۲۵۷ ۸۳۸ ۷۶۱ و ۷۲۱ ۷۰۷ ۱۹۳

پاسخهای دو محاسبه یکسان بودند. *کول* همچنان بی‌آن که کلمه‌ای ادا کند به جایش برگشت، و برای اولین و تنها دفعه جمیع حاضران در جلسهٔ انجمن آمریکایی ریاضی به پا خاسته ابراز احساسات کردند.

کاری که *کول* انجام داده بود (و ظاهراً بیست سال بعدازظهرهای یک‌شنبهٔ خود را صرف آن کرد) یافتن عاملهای اول عدد مرسن $M_{۶۷}$ بود. از ۱۸۷۶ مشخص بود که $M_{۶۷}$ مرکب است. اما این موضوع (توسط خود *ادوارد لوکاس*) با استفاده از آزمون *لوکاس* (اکنون *لوکاس ــ لمر*) کشف شده بود، که در ضمن این که پاسخی به این سؤال نیز می‌داد که عدد مرسن مفروضی اول یا مرکب است، اطلاعاتی در مورد عاملهای اعدادی که مرکب بودنشان را مشخص می‌کرد نمی‌داد. (این مطلب در مورد آزمون ARCL، چنانکه می‌توان از طرح قبلاً داده شدهٔ این روش دریافت، و در واقع در مورد هر تعداد روش سریع آزمون اول بودن اخیراً در دسترس، صادق است.)

اما چگونه می‌توان عاملهای عددی را که مرکب بودنش را می‌دانیم پیدا کرد؟ آزمایش و خطا واضحاً، به همان دلیل که در مورد آزمون اول بودن عملی نیست، کارا نیست. اما در عمل عنصری از تقسیم آزمایشی در جمیع اجراهای جاری روشهای آزمونهای اول بودن و تجزیه موجود است. و به علت سرعت انجام این کار، آغاز کردن عمل با، مثلاً، یک میلیون عدد اول اولیه معقول به نظر می‌رسد. در این صورت اگر مقسوم‌علیهی یافت شود، هر دو مسألهٔ اول بودن و تجزیه حل شده‌اند. و اگر نه، دست کم خواهیم دانست که عدد مورد نظر یا اول است، یا

اگر مرکب است، تنها عاملهای اول بزرگ دارد. کاربرد واقعیت اخیر با روش تجزیهٔ ساده‌ای انجام می‌گیرد که از *فرما* و به صورت زیر است.

فرض می‌کنیم $n = uv$، که در آن u و v هر دو اعداد بزرگ و فرد، با $u \le v$، اند. (این وضعیت، از آنجا که فرضمان بر این است که n تنها عاملهای اول بزرگ دارد، وضعیتی است که هنگامی با آن روبرو می‌شویم که می‌دانیم n مرکب است و مایل به یافتن عاملهای آنیم.) فرض می‌کنیم

$$x = \frac{1}{2}(u+v) \quad \text{و} \quad y = \frac{1}{2}(u-v)$$

دراین‌صورت $0 \le y < x$، $u = x+y$، $v = x-y$، بنابراین

$$n = (x+y)(x-y) = x^2 - y^2$$

که می‌تواند به صورت زیر نوشته شود

$$y^2 = x^2 - n \qquad (1)$$

برعکس، اگر x و y در معادلهٔ (۱) صدق کنند، آنگاه n دارای تجزیهٔ زیر می‌شود

$$n = (x+y)(x-y) \qquad (2)$$

در نتیجه، تجزیهٔ n به حاصلضرب دو عدد هم‌ارز یافتن عددهای x و yی است که در معادلهٔ (۱) صدق کنند، و در این حالت تجزیهٔ حاصل توسط معادلهٔ (۲) داده می‌شود. (توجه داشته باشید که این کار لزوماً تجزیهٔ *اول* n را به دست نمی‌دهد. اما زمانی که عددی به دو عامل تقسیم شود، ممکن است خود آن دو عامل به نوبت خود تجزیه شوند، و این کاری است که بدون استثنا بسیار ساده‌تر است زیرا هر چه عدد کوچکتر باشد تجزیه‌اش آسانتر است.)

برای یافتن x و y، چنان که در معادلهٔ (۱) آمده است، با کوچکترین عدد اول k، چنان که $k \ge \sqrt{n}$، آغاز می‌کنیم، و سپس، به نوبت، به بررسی مقادیر $x = k$، $x = k+1$، $x = k+2$، ... پرداخته ملاحظه می‌کنیم $x^2 - n$ مربع کامل است یا خیر. هنگامی که چنین xی را یافتیم، تجزیه به گونه‌ای مؤثر کامل می‌شود. با این شرط که n دارای دو عامل تقریباً به یک اندازه باشد (و در نتیجه نزدیک به $\sqrt{n}$ که روشمان را از آن آغاز کردیم)، باید جواب را نسبتاً سریع به دست آوریم. (اگر مایل باشید که در این مرحله خودتان به بررسی این روش بپردازید، اعداد ۱۰۳۷۹ و ۹۳۳۴۳ مثالهای مناسبی به دست می‌دهند).

طرق گوناگونی در سرعت بخشیدن به فرایند فوق موجودند. به عنوان نمونه، اگر عمل مورد نظر را بدون استفاده از ابزار انجام می‌دهیم نیاز به محاسبهٔ ریشهٔ دوم $x^2 - n$، برای ملاحظهٔ عدد درست بودن آن، در هر حالت نداریم. از آنجا که هیچ مربع کاملی به یکی از ارقام ۲، ۳، ۷، یا ۸ ختم نمی‌شود، هرگاه مشخص شود $x^2 - n$ به یکی از چنین رقمهایی ختم می‌شود آن مقدار x را می‌توان بلافاصله کنار گذاشت.

خود *فرما* از این روش برای تجزیهٔ زیر استفاده کرد

$$۲۰۲۷۶۵۱۲۸۱ = ۴۴۰۲۱ \times ۴۶۰۶۱$$

اجراهای کامپیوتری برای «حذف بلافاصله» مقادیر غیرممکن x (فرایندی به دلایل آشکار معروف به *غربال کردن*) از روشهایی کاملاً پیچیده استفاده می‌کنند. در ۱۹۷۴، ریاضیدانهای دانشگاه *کالیفرنیا* در *برکلی* SRS ـ ۱۸۱، ابزار الکترونیکی به طور اختصاصی طرح شده‌ای را برای غربال کردن اعداد ساختند، که می‌توانست در هر ثانیه ۲۰ میلیون عدد را بررسی کند.

عددهای فرما

nامین عدد *فرما*[۳] با رساندن ۲ به توان n، سپس با رساندن ۲ به توان این عدد و افزودن ۱ به نتیجه، حاصل می‌شود، یعنی،

$$F_n = ۲^{۲^n} + ۱$$

به این ترتیب $F_0 = ۳$، $F_1 = ۵$، $F_2 = ۱۷$، $F_3 = ۲۵۷$، و (هم‌اکنون نمو سریع این اعداد نظر به کاربرد مکرر تابع نمایی مربوطه آشکار شده است)

$$F_4 = ۲^{۱۶} + ۱ = ۶۵۵۳۷$$

علت توجه به این اعداد ادعایی است که توسط *فرما* در نامه‌ای که به مرسن در ۱۶۴۰ نوشته شده، انجام گرفته است. *فرما*، با توجه به این که هر یک از اعداد F_0 تا F_4 اول است چنین نوشته است: «دریافته‌ام اعداد به صورت $۲^{۲^n} + ۱$ همواره عددهایی اول‌اند» و از آن زمان به بعد صدق این قضیه برای تحلیلگران دارای اهمیت شده است. این موضوع باید به عنوان

اخطاری به تمام کسانی باشد که بر مبنای مبالغ اندکی از اطلاعات به نتیجه‌گیری می‌پردازند. *فرما* با تمام تواناییهایش در مورد اعداد، در این اظهار به خطا رفته بود. این مطلب اولین‌بار به طور قاطع توسط لئونهارد اویلر[۴] ریاضیدان بزرگ سوئیسی در ۱۷۳۲ نشان داده شد: $F_5 = ۴۲۹۴۹۶۷۲۹۷$ اول نیست. شگفت اینجاست که گرچه *اویلر* این نتیجه را با استفاده از تقسیم آزمایشی به دست آورد. نتیجه‌ای مستقیم با استفاده از خود آزمون فرما موجود است که غیر اول بودن F_5 را مبرهن می‌کند. به یاد بیاورید که آزمون مزبور بر این است که اگر P اول باشد در این صورت $۳^{P-1} \bmod P = ۱$، اما در مورد $P = F_5$ به دست می‌آوریم

$$۳^{P-1} \bmod P = ۳۰۲۹۰۲۶۱۶۰$$

بنابراین F_5 نمی‌تواند اول باشد.

کارهای بعدی نشان داده که فرما تا چه حد به خطا بوده است. اکنون می‌دانیم F_n به ازای جمیع مقادیر n از ۵ تا ۱۶، نیز به ازای مقادیر گوناگون دیگر، مرکب است، و حدس فعلی این است که F_n به ازای جمیع مقادیر n بزرگتر از ۴ مرکب است.

اعداد فرما مثالی دیگر از عددهایی را به دست می‌دهند که صورت خاص آنها آزمون اول بودنشان را به طریقی کارا امکانپذیر می‌کند ــ یکی از روشهای معروف در این مورد قضیهٔ پروث[۵] است: عدد فرمای F_n اول است اگر، و تنها اگر

$$۳^{\frac{(F_n-1)}{۲}} \bmod F_n = -۱$$

این دستاورد آزمون بسیار کارایی برای اول بودن اعداد فرما به دست می‌دهد. (این آزمون، همانگونه که ممکن است حدس زده باشید، رابطهٔ تنگاتنگی با آزمون *فرمای* قبلاً بحث شده دارد.) اما علاقهٔ ما در این مرحله به آزمون اول بودن اعداد فرما نیست، بلکه به تجزیهٔ اعدادی است که مرکب بودنشان مشخص است، زیرا در این زمینه است که در سالهای اخیر گسترشهای قابل توجهی انجام گرفته است، گسترشهایی که بدون کاربردهایی خارج از قلمرو ریاضیات نیستند. (بعداً بخش مربوط به رمزهای محرمانه را در این فصل ملاحظه کنید.)

همانطور که قبلاً توجه کردیم مرکب بودن عدد فرمای F_5 توسط *اویلر* به اثبات رسید. وی یک عامل اول آن، یعنی ۶۴۱، را نیز محاسبه کرد. مرکب بودن F_6 در ۱۸۸۰ توسط *لندری*[۶] ثابت شد، و بار دیگر عاملی اول به دست آمد: ۲۷۴۱۷۷. F_7 ماجرایی دگرگونه داشت. مرکب بودن آن در ۱۹۰۵ توسط مورهد[۷] و وسترن[۸] به اثبات رسید، اما تجزیهٔ آن تا سال ۱۹۷۱ زمانی که *بریلهارت*[۹] و موریسون[۱۰] (مجهز با کامپیوتر IBM.360-91) تجزیهٔ زیر را به دست آوردند میسر نشد

$$F_۷ = ۲^{۱۲۸} + ۱$$
$$= ۳۴۰\ ۲۸۲\ ۳۶۶\ ۹۲۰\ ۹۳۸\ ۴۶۳\ ۴۶۳\ ۳۷۴\ ۶۰۷\ ۴۳۱\ ۷۶۸\ ۲۱۱\ ۴۵۷$$
$$= ۵۹\ ۶۴۹\ ۵۸۹\ ۱۲۷\ ۴۹۷\ ۲۱۷ \times ۵\ ۷۰۴\ ۶۸۹\ ۲۰۰\ ۶۸۵\ ۱۲۹\ ۰۵۴\ ۷۲۱$$

آنها برای انجام این کار از روشی استفاده کردند که مدتها قبل توسط *لمر* و پاورز[۱۱] مطرح و شامل کسرهای مسلسل بود. محاسبه ده ساعت و نیم طول کشید. نمونه‌های اصلاح شدهٔ روش کسر *مسلسل*[۱۲] (آن طور که امروزه نامیده می‌شود) بعضی از روشهای تجزیهٔ اخیراً در دسترس را به دست می‌دهند.

دو نفری که در ۱۹۰۵ مرکب بودن F_7 را نشان دادند، یعنی مورهد و وسترن، مرکب بودن F_8 را نیز در ۱۹۰۹ پیدا کردند. و تنها در ۱۹۸۱ بود که برنت[۱۳] و پولار[۱۴] تجزیهٔ آن را یافتند. محاسبهٔ این کار دو ساعت بر کامپیوتر یونیواک[۱۵] ۱۱۰۰/۲ طول کشید. روش محاسبه، که توسط خود پولار اختراع شده بود، در آن زمان از این لحاظ غیرمعمول بود که، برخلاف اغلب روشهای ریاضیات، به دست دادن نتیجه را تضمین نمی‌کرد، و تنها چیزی که می‌توانست از ریاضیات زمینهٔ آن به دست آید این بود که اگر محاسبهٔ مشخصی انجام می‌گرفت، در این صورت احتمال بسیار وجود داشت که تجزیهٔ عدد طی طول معقولی از زمان به دست آید، اما امکان اندکی هم وجود داشت که این واقعه اتفاق نیفتد. بنابراین روش مزبور شبیه تقسیم آزمایشی نبود، که در آن شانس به دست آوردن پاسخ طی یک میلیارد سال اندک است. و گرچه همچنان عنصری از تصادف در روش پولار وجود دارد اما هوشمندانه بودن آن در این است که در آن شانس به مقدار زیادی به نفع تجزیه شدن

است.

در سالهای اخیر تعدادی از روشهای موسوم به روشهای مونت کارلو[۱۶]، از قبیل روش تجزیهٔ پولار موجود شده‌اند که ایقان یک نتیجه را با احتمال بالای نتیجه‌ای در زمانی بسیار کمتر تعویض کرده‌اند.

دو عامل اول F_8 (که دارای ۷۸ رقم است) عبارت‌اند از

۱ ۲۳۸ ۹۲۶ ۳۶۱ ۵۵۲ ۸۹۷

و

۹۳ ۴۶۱ ۶۳۹ ۷۱۵ ۳۵۷ ۹۷۷ ۷۶۹ ۱۶۳ ۵۵۸

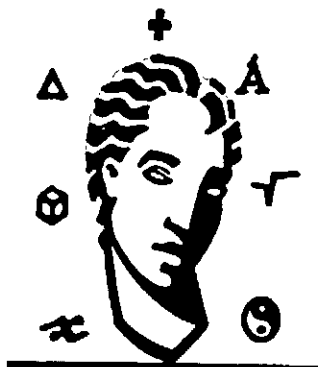
۱۹۹ ۶۰۶ ۸۹۶ ۵۸۴ ۰ ۵۱ ۲۳۷ ۵۴۱ ۶۳۸

۱۸۸ ۵۸۰ ۲۸۰ ۳۲۱

از هنگام نوشتن F_9 کسی توانایی تجزیهٔ آن را نداشته است. شاید *کارل فردریش گاوس*[۱۷]، در صورتی که زنده بود، اکنون که کامپیوترهای سریع در دسترس‌اند، می‌توانست در این مورد کمک کند. وی محققاً شگفت‌آورترین نتیجه‌ها را در مورد اعداد فرما به دست داد، یعنی نتیجه‌ای که آنها را به مسأله‌ای کلاسیک از هندسهٔ یونان متصل می‌کند، این دستاورد، همان‌گونه که بسیاری از کشفیات گاوس، شایستگی ورودی استثنائی به یکی از حیرت‌انگیزترین ذهنهای ریاضی‌ای را دارند که دنیا تاکنون شناخته است.

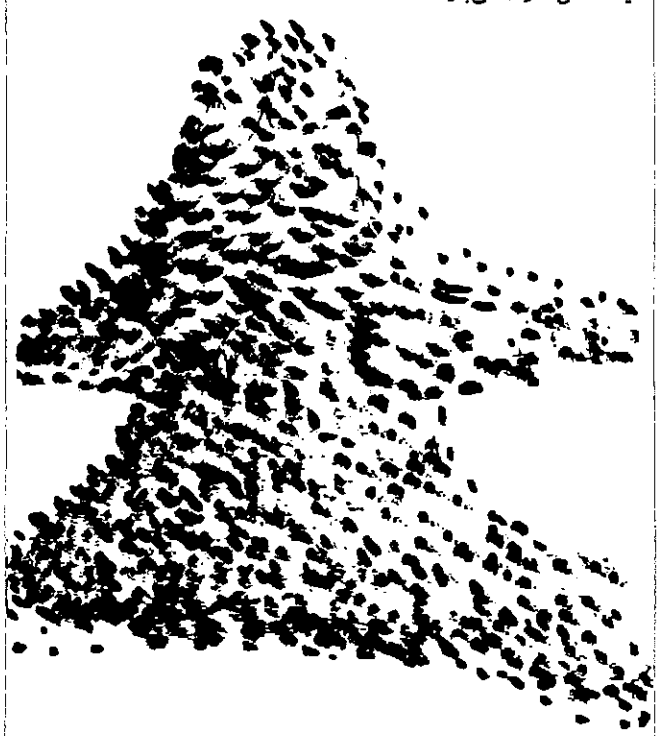
یادداشتها :

1– Fredrick Nelson Cole
2– On the factorization of large numbers
3– Fermat numbers
4– Leonhard Euler
5– Proth's theorem
6– Landry
7– Morehead
8– Western
9– Brillhart
10– Morrison
11– Powers
12– Continued fraction method
13– Brent
14– Pollard
15– Univac
16– Mont Carlo methods
17– Karl Friedrich Causs



تفریح اندیشهٔ ۵

دو توده شن داریم. دو بازیکن به نوبت (۱) یکی از توده‌ها را از محل بازی برمی‌دارد و (۲) تودهٔ باقی‌مانده را به دو تودهٔ تقسیم می‌کند. بازیکنی که نتواند توده‌ای را تقسیم کند (زیرا تودهٔ مزبور تنها یک شن دارد) می‌بازد.



جواب در صفحه ۸۸