گردو گردو است، ولی هر گردی گردو نیست

«اسرار عددهای اول»

محمدحسن بیژن‌زاده
استاد تمام ریاضی دانشگاه خوارزمی تهران

ما در ریاضیات با قضیه‌ها سر و کار داریم. قضیه‌ها حقایق ریاضیات را بیان می‌کنند. به جز احکام اولیهٔ هر رشته از ریاضیات که آن‌ها را «بنداشت» یا «اصل موضوع» می‌نامیم، بقیهٔ احکام که آن‌ها را قضیه می‌نامیم باید دارای برهان باشند. در واقع، آنچه ریاضیات را از سایر علوم بشری متمایز می‌سازد، برهان است. در واقع اگر برهانی در کار نباشد، ریاضیاتی وجود ندارد.

بیشتر قضیه‌های ریاضیات در واقع گزاره‌های شرطی هستند که از مدل «اگر p، آن‌گاه q» پیروی می‌کنند:

- اگر مثلث ABC قائم‌الزاویه باشد، آن‌گاه رابطهٔ **فیثاغورث** در آن برقرار است.
- اگر دو زاویهٔ یک مثلث برابر باشند، دو ضلع مجاور این زاویه‌ها برابرند.

در منطق وقتی گزارهٔ

$$p \Rightarrow q \qquad (1)$$

نادرست است که p درست و q نادرست باشد. به ازای سایر ارزش‌دهی‌های p و q این گزارهٔ شرطی، درست است.

از گزاره (۱) گزارهٔ

$$q \Rightarrow p \qquad (2)$$

را می‌توان ساخت که آن را عکس گزارهٔ (۱) می‌نامیم.

ممکن است یک گزاره شرطی درست باشد، اما عکس آن درست نباشد:

(۳) اگر عددی بر ۴ قابل قسمت باشد، بر ۲ هم قابل قسمت است.

اما به وضوح پیداست که عکس این گزاره درست نیست:

اگر عددی بر ۲ قابل‌قسمت باشد، بر ۴ نیز قابل قسمت است.

پس ممکن است عکس یک گزارهٔ شرطی در مواردی درست و در مواردی نادرست باشد.

با این مقدمه به یک مسئلهٔ تاریخی در خصوص عددهای اول می‌پردازیم:

اگر p عددی اول باشد، برای هر عدد طبیعی a داریم:

$$a^p \equiv a \pmod{p} \qquad (\alpha)$$

این قضیهٔ را «قضیهٔ کوچک فرما» می‌نامند. این قضیه در درس جبر ۱ در مبحث گروه‌های متناهی اثبات می‌شود. معنی این قضیه آن است که باقی‌ماندهٔ تقسیم a^p بر p، با باقی‌ماندهٔ تقسیم a بر p برابر است. برای مثال 185^{37} را امتحان کنید!

عدد 185^{37} بر ۳۷ قابل قسمت است.

ما این عدد را نمی‌شناسیم و شاید روزها یا ماه‌ها وقت بگیرد تا ارقام آن به دست آید. لیکن این قدرت برهان ریاضیات است که نداشتن تجربه را جبران می‌کند. این عدد بر ۳۷ قابل قسمت است، زیرا ۱۸۵ بر ۳۷ قابل‌قسمت است.

حالا این سؤال پیش می‌آید که آیا عکس قضیهٔ کوچک فرما قضیه است؟

یک‌بار دیگر رابطهٔ (α) را دقیق‌تر شرح می‌دهیم تا بهتر بتوانیم عکس آن را بیان کنیم:

اگر p عددی اول باشد، آن‌گاه برای هر عدد طبیعی a داریم:

$a^p \equiv a(\text{mod } p)$ (α رابطهٔ)

پس عکس آن چنین است:

(حکم γ) اگر برای هر عدد طبیعی a داشته باشیم: $a^p \equiv a(\text{mod } p)$**، آن‌گاه p عددی اول است.**

جالب است بدانید، تا این اواخر کسی از ریاضی‌دانان به این فکر نیفتاده بود که عکس قضیهٔ فرما را صورت‌بندی کند و به فکر اثبات یا رد آن باشد. اگر قادر باشیم حکم (γ) را اثبات کنیم، یعنی برای آن برهانی ارائه دهیم، خود این حکم یک قضیهٔ ریاضی است و در این صورت ثابت کرده‌ایم که عکس قضیهٔ کوچک فرما یک قضیه است.

چنانچه نتوانیم برهانی برای آن اقامه کنیم، به این حدس نائل می‌شویم که این حکم درست نیست و لذا نقیض آن درست است.

با آنکه قضیهٔ کوچک فرما در سال‌های ۱۶۳۴ م، یعنی حدود چهار قرن قبل اثبات شده است، بررسی و تعیین تکلیف حکم (γ) به دههٔ اول قرن بیستم میلادی برمی‌گردد. سه نفر از جبردانان دانشگاه «جورجیا» به نام‌های **آلفرد، گرانویل**، و **پومرفس**، پس از سال‌ها تلاش و با استفاده از برنامه‌ریزی‌های رایانه‌ای پیشرفته توانستند حکم (γ) را نقض کنند.

می‌دانیم که یک گزاره شرطی، مثل اگر p آن‌گاه q، فقط وقتی نادرست است که p (مقدم‌گزاره) درست و q (تالی‌گزاره) نادرست باشد. لذا برای رد حکم (γ) باید عددی غیراول بیابیم که برای هر عدد طبیعی a در رابطهٔ

$a^p \equiv a(\text{mod } p)$

صدق کند.

کار تیم سه‌نفرهٔ دانشگاه جورجیا کاری خارق‌العاده در مبحث نظریهٔ اعداد محسوب می‌شود. چرا که وجود چنین عددهایی که در واقع خاصیت عددهای اول را دارند، اما اول نیستند، ظاهراً بسیار نادر و کمیاب هستند. *به عبارت دیگر، عددهای مرکبی وجود دارند که خاصیت‌های عددهای اول را دارا هستند؛* یعنی در (رابطهٔ α) برای هر عدد طبیعی a صدق می‌کنند!

کوچک‌ترین این عددها که توسط **کار میشل**[1] کشف شده، عدد ۵۶۱ است که عددی مرکب است:

$۵۶۱=۳\times۱۱\times۱۷$

این عدد در سال ۱۹۱۰ توسط کار میشل کشف شد. از این‌رو، این‌گونه عددهای مرکب را که در رابطهٔ α صدق می‌کنند، «عددهای کار میشل» نیز می‌نامند. به قدرت ریاضیات توجه کنید:

$۲۵۶۳^{۵۶۱} \equiv ۲۵۶۳ \pmod{۵۶۱}$

این هم‌نهشتی را به زبان ساده بیان کنید. به جای a عددهای دیگری قرار دهید. نتیجه آنکه هر عدد اول در رابطهٔ

$a^p \equiv a(\text{mod } p)$

صدق می‌کند، لیکن هر عدد m که در

$a^m \equiv a(\text{mod } m)$

برای هر a صدق کند (آزمایش قضیهٔ کوچک‌فرما)، لزوماً اول نیست. هر گردو گرد است، اما هر گردی گردو نیست.

امروزه یافتن عددهای اول بزرگ و کار با «ترکیبیات»[2] آن‌ها در حوزه‌های علمی رمزنگاری و سیستم‌های امنیت رایانه‌ای کاربرد فراوانی دارد.

پی‌نوشت‌ها

1. Car micheal

۲. متخصصان علوم رایانه، به‌ویژه متخصصان امنیت رایانه و سیستم‌های امنیتی رویه‌های فنی خاصی را با استفاده از عددهای اول اعمال می‌کنند.

منابع

1. W.k.Nicholson: (Abstruct Algebra)
PWS, Boston, Publishing Company. 1997.
2.What,s Happening in the mathematical Sciences, American Mathematical Society. Vol 1,1993.