چند مسألهٔ جالب دربارهٔ اعداد اول

هانیه شکوه

واژهٔ «اول»، ترجمهٔ کلمهٔ «Prime» است. این کلمه در دو معنای «ساده‌بودن» و «بنیادی‌بودن» به کار برده شده است.

تعریف: عدد طبیعی $p > 1$ را اول گویند، هرگاه تنها مقسوم‌علیه‌های مثبت آن ۱ و p باشند. هر عدد طبیعی بزرگ‌تر از یک را که اول نباشد، «مرکب» گوییم.

مثال. اعداد ۲ و ۳ و ۵ و ۷ و ۱۱ و ۱۳ و ۲۹ اول و ۱۸ و ۱۵ و ۵۱ مرکبند.

تذکر: با توجه به تعریف یاد شده معلوم است که عدد ۱ نه اول است و نه مرکب.

با توجه به تعریف عدد اول، اگر p عددی اول باشد، به طوری که $p = ab$ $(a < b)$، از آن جایی که a و b مقسوم‌علیه‌های عدد p هستند و p اول است، لذا: $a = 1$ و $b = p$ (با فرض $a < b$). بنابراین، هر عدد اول به جز تجزیهٔ بدیهی $1 \times p$ تجزیهٔ دیگری ندارد.

مثال. اگر m و n دو عدد طبیعی باشند، به طوری که $9m^2 - 4n^2 = 5$، مطلوبست تعیین m و n.

حل. با استفاده از اتحاد مزدوج طرف چپ تساوی فوق را تجزیه می‌کنیم:

$$(3m + 2n)(3m - 2n) = 5$$

چون ۵ یک عدد اول است، پس تنها تجزیهٔ آن به صورت

$a\times b=5$ است که در آن: $a=5$ و $b=1$. پس، از تساوی $(3m+2n)(3n-2n)=5\times 1$ داریم: $3n+2n=5$ و $3m-2n=1$ (به وضوح مشخص است که $3m-2n<3m+2n$). حال m و n را به دست می‌آوریم:

$$\begin{cases}3m+2n=5\\3m-2n=1\end{cases}\Rightarrow \begin{matrix}m=1\\n=1\end{matrix}$$

اکنون این سؤال مطرح می‌شود که آیا بزرگ‌ترین عدد اول وجود دارد؟ پاسخ این سؤال را **اقلیدس** ۲۰۰۰ سال پیش به صورت زیر داده است:

قضیهٔ اقلیدس: مجموعهٔ اعداد اول نامتناهی است. به عبارت دیگر، بی‌نهایت عدد اول وجود دارد.

با این که بی‌نهایت عدد اول وجود دارد، توزیع اعداد اول در مجموعهٔ اعداد طبیعی پر رمز و راز است. این اعداد، برخلاف تعریف ساده‌شان، در میان اعداد طبیعی رشد می‌کنند و هیچ کس نمی‌تواند پیش‌بینی کند که عدد اول بعدی در کجا سبز خواهد شد. در عین حال، واقعیت شگفت‌انگیز دیگری هم دربارهٔ این اعداد وجود دارد: این است که به جز کوچک‌ترین دو عدد اول یعنی ۲ و ۳، هیچ دو عدد اول دیگری متوالی نیستند و تنها عدد ۲، عدد اول زوج است. بنابراین، همهٔ اعداد اول به غیر از ۲ فردند و اختلاف دو عدد اول متوالی حداقل برابر ۲ است. اگر اختلاف دو عدد اول برابر ۲ باشد، آن دو عدد اول را «دوقلو» می‌گوییم.

مثال. «۱۱ و ۱۳» و «۱۷ و ۱۹» نمونه‌هایی از اعداد اول دوقلو هستند.

نکته: هر عدد اول به یکی از صورت‌های ۲ یا $4k+1$ یا $4k+3$ $(K\in N)$ است. زیرا تنها عدد اول زوج، عدد ۲ است و سایر اعداد اول فردند و اعداد فرد نیز به یکی از صورت‌های $4k+1$ یا $4k+3$ هستند.

به عنوان مثال، عدد اول ۱۷ به صورت $4\times4+1$ $(k=4)$ یا عدد اول ۲۳ به صورت $4\times5+3$ $(k=5)$ نوشته می‌شود.

توجه کنید که عکس مطلب فوق درست نیست. یعنی نمی‌توان گفت که هر عدد به صورت $4k+1$ یا $4k+3$ اول است. مثلاً به ازای $k=5$، $4k+1$ مساوی ۲۱ است و ۲۱ اول نیست. درواقع $4k+1$ و $4k+3$ به ازای بعضی مقادیر طبیعی k اعداد اول را تولید می‌کنند. با توجه به نامتناهی بودن مجموعهٔ اعداد اول می‌توان نتیجه گرفت که بی‌نهایت عدد اول از نوع $4k+1$ یا $4k+3$ وجود دارد.

دیریکله[1] (۱۸۵۹ـ۱۸۰۵م) ثابت کرد، اگر a و b نسبت به هم اول باشند، $a+kb$ بی‌نهایت عدد اول تولید می‌کند. البته این نکته بدین معنی نیست که $a+kb$ فقط اعداد اول تولید می‌کند.

اعداد مرسن[2] (۱۶۴۸ـ۱۵۸۸م): اعداد به صورت $M_n=2^n-1$ را به افتخار کشیش فرانسوی، **مارین مرسن**، اعداد مرسن نامیده‌اند. ولی مرسن در زمینهٔ اول‌بودن این نوع اعداد اظهارنظر نادرستی ارائه کرد. در سال ۱۶۴۴، مرسن اظهار داشت که $M_n=2^n-1$، به ازای اعداد اول $n=2,3,5,7,13,17,19,31,67,127,257$ عددی اول است و به ازای سایر عددهای طبیعی کوچک‌تر از ۲۵۷ عددی مرکب است.

به اعدادی به شکل 2^n-1 که در آن n اول است، اعداد اول مرسن می‌گویند.

مرسن چند اشتباه داشت. اولاً او به خطا تصور کرد $M_{67}=2^{67}-1$ و $M_{257}=2^{257}-1$ اول هستند. ثانیاً M_{61},M_{89},M_{107} را در زمرهٔ اعداد اول در نظر نگرفته بود. بعدها در سال ۱۹۵۲، اعداد اول مرسن بزرگ‌تری نیز به دست آمدند که عبارتند از:

$M_{521},M_{607},M_{1279},M_{2203},M_{2281}$. همچنین، در سال ۲۰۰۱ بزرگ‌ترین عدد اول مرسن به صورت $M_{13466917}$ به دست آمده است.[3]

حال در مسألهٔ زیر می‌بینیم که شرط لازم برای اول‌بودن 2^n-1 چیست.

مسأله. اگر 2^n-1 اول باشد، نشان دهید n اول است.

اثبات. (برهان خلف) فرض می‌کنیم n اول نباشد، بنابراین می‌توان آن را به صورت $n=pq$ در نظر گرفت که در آن $1<p,q<n$. حال داریم:

$$2^n-1=2^{pq}-1=(2^p)^q-1=(2^p-1)((2^p)^{q-1}+\dots+1)$$

به وضوح روشن است که هریک از عوامل فوق از ۱ بزرگ‌ترند؛ یعنی 2^n-1 تجزیهٔ غیربدیهی دارد که این خلاف

اول بودن $۲^n - ۱$ است.

البته عکس مسألهٔ فوق درست نیست. به‌عنوان مثال، $۲۰۴۷ = ۲^{۱۱} - ۱$ که بر ۲۳ بخش‌پذیر است، اول نیست.

عدد فرما: [4] (۱۶۶۵ـ۱۶۰۱م)

هر عدد فرما، عددی است به صورت $F_n = ۲^{۲^n} + ۱$ $(n \geq ۰)$. اگر F_n اول باشد، آن را عدد اول فرما می‌گویند.

مسأله. اگر $۲^m + ۱$ اول باشد، نشان دهید: $m = ۲^n$.

اثبات. (برهان خلف) فرض کنید m توانی از ۲ نیست؛ یعنی: $m \neq ۲^n$. لذا m مقسوم‌علیه فردی مانند $۲k + ۱$ دارد که از یک بزرگ‌تر است. بنابراین:

$$M = (۲k + ۱)L; \ (k, L \in \mathbb{N})$$

حال داریم:

$$۲^m + ۱ = ۲^{(۲k+۱)L} + ۱ = (۲^L)^{(۲k+۱)} + ۱$$
$$= (۲^L + ۱)((۲^L)^{(۲k+۱-۱)} - ۲^{L(۲k-۱)} + \ldots + ۱)$$

یعنی $۲^{m+۱}$ تجزیهٔ غیربدیهی دارد، پس اول نیست که این خلاف فرض است. پس نتیجه می‌گیریم که شرط لازم برای اول بودن $۲^m + ۱$، این است که $m = ۲^n$ باشد.

فرما مشاهده کرد که:

$F_۰ = ۲^{۲^۰} + ۱ = ۳$، $F_۱ = ۲^{۲^۱} + ۱ = ۵$، $F_۲ = ۲^{۲^۲} + ۱ = ۱۷$، $F_۳ = ۲^{۲^۳} + ۱ = ۲۵۷$ و $F_۴ = ۲^{۲^۴} + ۱ = ۶۵۵۳۷$ اولند و به خطا تصور کرد که همهٔ F_n ها اولند.

در سال ۱۷۳۲، اولر نشان داد که $F_۵$ بر ۶۴۱ بخش‌پذیر است.

$$F_۵ = ۲^{۲^۵} + ۱ = ۲^{۳۲} + ۱ = ۴۲۹۴۹۶۷۲۹۷$$

بنابراین خط بطلانی بر ادعای فرما کشید. البته ممکن است برای ما چنین عددی بزرگ جلوه نکند، ولی در زمان فرما به علت محدودیت ابزار محاسبه‌های بزرگ، تشخیص اول بودن این عدد کاری بسیار دشوار بود.

اکنون ثابت شده است که به‌ازای همهٔ اعداد طبیعی $۵ \leq n \leq ۲۱$، F_n مرکب است.

ریاضیدانان اعداد اول را مانند بلوک‌های ساختمانی می‌دانند که همهٔ اعداد از آن‌ها ساخته شده‌اند. به همین دلیل، سالیان درازی است که ریاضیدانان را شیفتهٔ خود ساخته و فکر آن‌ها را مشغول کرده‌اند.

اعداد اول بین ۱ و ۱۰۰۰ در جدول زیر آمده‌اند:

	۲	۳	۵	۷	۱۱	۱۳	۱۷	۱۹	۲۳
۲۹	۳۱	۳۷	۴۱	۴۳	۴۷	۵۳	۵۹	۶۱	۶۷
۷۱	۷۳	۷۹	۸۳	۸۹	۹۷	۱۰۱	۱۰۳	۱۰۷	۱۰۹
۱۱۳	۱۲۷	۱۳۱	۱۳۷	۱۳۹	۱۴۹	۱۵۱	۱۵۷	۱۶۳	۱۶۷
۱۷۳	۱۷۹	۱۸۱	۱۹۱	۱۹۳	۱۹۷	۱۹۹	۲۱۱	۲۲۳	۲۲۷
۲۲۹	۲۳۳	۲۳۹	۲۴۱	۲۵۱	۲۵۷	۲۶۳	۲۶۹	۲۷۱	۲۷۷
۲۸۱	۲۸۳	۲۹۳	۳۰۷	۳۱۱	۳۱۳	۳۱۷	۳۳۱	۳۳۷	۳۴۷
۳۴۹	۳۵۳	۳۵۹	۳۶۷	۳۷۳	۳۷۹	۳۸۳	۳۸۹	۳۹۷	۴۰۱
۴۰۹	۴۱۹	۴۲۱	۴۳۱	۴۳۳	۴۳۹	۴۴۳	۴۴۹	۴۵۷	۴۶۱
۴۶۳	۴۶۷	۴۷۹	۴۸۷	۴۹۱	۴۹۹	۵۰۳	۵۰۹	۵۲۱	۵۲۳
۵۴۱	۵۴۷	۵۵۷	۵۶۳	۵۶۹	۵۷۱	۵۷۷	۵۸۷	۵۹۳	۵۹۹
۶۰۱	۶۰۷	۶۱۳	۶۱۷	۶۱۹	۶۳۱	۶۴۱	۶۴۳	۶۴۷	۶۵۳
۶۵۹	۶۶۱	۶۷۳	۶۷۷	۶۸۳	۶۹۱	۷۰۱	۷۰۹	۷۱۹	۷۲۷
۷۳۳	۷۳۹	۷۴۳	۷۵۱	۷۵۷	۷۶۱	۷۶۹	۷۷۳	۷۸۷	۷۹۷
۸۰۹	۸۱۱	۸۲۱	۸۲۳	۸۲۷	۸۲۹	۸۳۹	۸۵۳	۸۵۷	۸۵۹
۸۶۳	۸۷۷	۸۸۱	۸۸۳	۸۸۷	۹۰۷	۹۱۱	۹۱۹	۹۲۹	۹۳۷
۹۴۱	۹۴۷	۹۵۳	۹۶۷	۹۷۱	۹۷۷	۹۸۳	۹۹۱	۹۹۷	(۱۰۰۹)

زیرنویس

1. Dirichlet
2. Mersenne
3. http://www-gap.dcs.St-And.ac.uk/~History/MistTopics/Prime-numbers.html
4. Fermat

منابع

1. Burton, David M. Elementary Number Theory
۲. نظریهٔ اعداد. سیدحسین سید موسوی و شمس‌الدین انوار.