۴

اعداد اول

● سید محمدرضا هاشمی موسوی *

در این جا می‌خواهیم اعدادی را معرفی کنیم که در واقع سنگ زیربنای همه‌ی اعداد هستند؛ یعنی اعدادی که توسط آن‌ها می‌توان، تمام اعداد طبیعی به جز یک را تولید کرد. این نوع اعداد را در فارسی «اول» و در لاتین «**Prime**» نام نهاده‌اند. Prime در دو معنای «ساده بودن» و «بنیادی بودن» به کار رفته است که اتفاقاً، اعداد اول این هر دو ویژگی را دارند. برای سهولت، اعداد اول را فقط برای اعداد صحیح مثبت تعریف می‌کنند.

این اعداد را شاید به این دلیل اول نامیده‌اند که هم ساده (از نظر تجزیه)، و هم زیربنایی (از نظر تجزیه‌ی اعداد طبیعی به جز یک، به حاصل‌ضرب آن‌ها) هستند. تعداد این نوع اعداد بی‌نهایت است. آن‌ها به طور بسیار نامنظم بین اعداد طبیعی ظهور می‌کنند و همین توزیع نامنظم، سبب به وجود آمدن بسیاری از مسائل حل نشدنی در این باب شده است. امروزه، پس از گذشت چند قرن، مسائل بی‌شماری از این اعداد شگفت‌انگیز، یا به صورت حدس (نه ردّ مسأله و نه اثبات آن) و یا به صورت مسأله‌ای حل نشدنی مطرح هستند که مورد توجه خاص بسیاری از ریاضیدانان حرفه‌ای و غیر حرفه‌ای قرار دارند.

از طرف دیگر، مسائلی در تئوری اعداد وجود دارند که به طور مستقیم و یا غیرمستقیم با این اعداد در ارتباط هستند و بدون آگاهی از ویژگی‌ها و قضیه‌های اعداد اول، به هیچ یک از آن‌ها نمی‌توان پاسخ گفت. به همین دلیل، هر محصل این شاخه از ریاضیات ابتدا باید سیری در اعداد اول داشته باشد و سپس در مورد مباحث دیگر مطالعه کند. همچنین، بحث مستدل در بعضی از این مسائل، موقوف به تسلط کامل بر بعضی دیگر از رشته‌های ریاضیات (مانند: آنالیز حقیقی و تئوری توابع تحلیلی و...) و موضوع شاخه‌های خاص و تخصصی از تئوری اعداد است که برخی از آن‌ها بسیار پهناور و سخت دشوارند. دو مسأله از این مسائل حل نشدنی که همیشه مورد توجه خاص و عام بوده‌اند، یکی «توزیع اعداد اول به توسط یک یا چند ضابطه‌ی معین»، و دیگری «تعداد اعداد اول، در هر فاصله‌ی دلخواه» است.

در این جا، ما فقط به تعریف و بررسی برخی از ویژگی‌های اعداد اول و بیان برخی از قضیه‌های مهم و اساسی می‌پردازیم و به دیگر جنبه‌های بحث‌انگیز و مسدود این نوع اعداد، تنها اشاره خواهیم کرد.

تعریف: هر عدد طبیعی و بزرگ‌تر از یک، مانند p را اول

می‌نامیم، هرگاه هیچ شمارنده یا مقسوم علیه مثبتی به جز یک و خودش نداشته باشد.

می‌دانیم، هر عدد صحیح مانند $a \neq \pm 1$، حداقل دارای چهار شمارنده‌ی ± 1 و $\pm a$ است. برای سهولت، بدون این که از عمومیت مطلب کاسته شود، اعداد اول را فقط برای اعداد صحیح مثبت تعریف می‌کنند. برای مثال، عددهای ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷ و ۱۹ را که جز یک و خودشان هیچ شمارنده‌ی دیگری ندارند، «اول» گوییم و عددهایی مثل ۹، ۱۲، ۱۵، ۲۴، ۲۷، ۳۴، ۹۹ را که جز یک و خودشان دارای عامل یا عامل‌هایی دیگر هستند، «مرکب» گوییم. بنابر تعریف، عددی که اول نباشد، مرکب است.

تذکر: با توجه به تعریف عدد اول، بدیهی است که عدد ۱ نه اول است و نه مرکب. خواهیم دید که پذیرفتن عدد ۱ در زمره‌ی اعداد اول، نه تنها مفید نیست، بلکه در یکتایی تجزیه‌ی هر عدد صحیح به عامل‌های اول، باعث اختلال می‌شود.

با توجه به تعریف عدد اول، اگر p عدد اولی به صورت $p=a.b$ $(a<b)$ باشد، در این صورت $a=1$ و $b=p$؛ زیرا:

(۱) $p=a.b \Rightarrow$ (a و b مقسوم علیه‌های p هستند) و $a=1$ $b=p$

هر عددی مثل n، دارای یک تجزیه‌ی بدیهی $n \times 1$ است. برای مثال، تجزیه‌ی بدیهی عدد ۱۸ به صورت 18×1 (حاصلضرب دو عدد) و تجزیه‌های غیربدیهی و جدی آن به صورت‌های زیر است:

$18=2\times 9=3\times 6(=2\times 3^2=9\times 2=6\times 3)$

نتیجه‌ی ۱. گزاره‌ی (۱) نشان می‌دهد که عدد اول به جز تجزیه‌ی بدیهی $p \times 1$، تجزیه‌ی نابدیهی ندارد. این واقعیت، ساده و بسیط بودن اعداد اول را نشان می‌دهد.

نتیجه‌ی ۲. اگر p عددی اول و k عددی مثبت و $k|p$، آن‌گاه $k=1$ یا $k=p$.

نتیجه‌ی ۳. اگر p و q دو عدد اول و $p|q$ یا $q|p$، آن‌گاه $p=q$؛ زیرا:

$$p|q \Rightarrow p=1 \text{ یا } p=q \xrightarrow{(p\neq 1 \text{ و } q \text{ اول})} p=q$$

تعریف: هر عدد طبیعی بزرگ‌تر از واحد را که اول نباشد (تجزیه‌ی نابدیهی هم داشته باشد)، عدد مرکب می‌نامیم.

مثال: همه‌ی عددهای طبیعی x و y را که در معادله‌ی زیر صدق می‌کنند، بیابید.

$$25y^2-16x^2=-31$$

حل: معادله را به صورت زیر می‌نویسیم:

$$16y^2-25x^2=31 \; ; \; (4y-5x)(4y+5x)=31 \quad (2)$$

از برابری (۲) نتیجه می‌شود:

$$\begin{cases} 4y-5x=1 \\ 4y+5x=31 \end{cases}$$

تنها جواب این دستگاه در مجموعه‌ی اعداد طبیعی $x=3$ و $y=4$ است.

این نتیجه از تجزیه‌ی عدد اول ۳۱ به صورت 31×1 حاصل شده است، زیرا بنابر اول بودن عدد ۳۱، تجزیه‌ی غیربدیهی ندارد و تجزیه‌ی بدیهی آن هم منحصر به فرد است.

قضیه‌ی ۱: با فرض این‌که p عددی طبیعی و به جز یک باشد و a و b دو عدد طبیعی دلخواه باشند، در این صورت اگر p در گزاره‌ی شرطی زیر صدق کند، p اول است:

$$\forall a,b \in |N;\; p|ab \Rightarrow p|a \text{ یا } p|b \quad (3)$$

اثبات (برهان خلف): فرض می‌کنیم p در شرط (۳) صدق کند، ولی اول نباشد. پس p دارای تجزیه‌ی نابدیهی به دو عامل مثبت مثل $n=ab$ است (واضح است که $n>a$ و $n>b$). از طرف دیگر، برابری $n=ab$ رابطه‌ی $n|ab$ را در بردارد

که با توجه به گزاره‌ی شرطی (۳) باید $n|a$ یا $n|b$ که با $n>a$ و $n>b$ متناقض است. بنابراین، فرض خلف نادرست و حکم برقرار است.

۴: عدد اول زوجی به جز ۲ وجود ندارد؛ زیرا اگر $p>2$ عددی زوج باشد، بدیهی است که $2|p$ و این با اول بودن p در تناقض است (p عاملی جز ۱ و خودش ندارد).

۵: هیچ دو عدد اول و متوالی به جز ۲ و ۳ وجود ندارند؛ زیرا به ازای هر عدد اول p که بزرگ‌تر از ۳ باشد، $p+1$ زوج است و با توجه به نتیجه‌ی ۴، هر عدد زوج بزرگ‌تر از ۲ مرکب است.

قضیه‌ی ۲: هر عدد صحیح به جز ± 1، لااقل یک مقسوم علیه اول دارد.

قضیه‌ی ۳: مجموعه‌ی اعداد اول، مجموعه‌ای نامتناهی است (بی‌نهایت عدد اول وجود دارد).

قضیه‌ی ۴: اگر n عددی مرکب باشد، آن‌گاه حداقل یک مقسوم علیه اول و کوچک‌تر یا برابر با $\sqrt{n}$ خواهد داشت.

۶: اگر عدد طبیعی n بزرگ‌تر از ۱ باشد و هیچ مقسوم علیه اول و کوچک‌تر یا برابر $\sqrt{n}$ نداشته باشد، آن‌گاه n عددی اول است.

نتیجه‌ی ۶، در واقع الگوریتمی برای تشخیص اول بودن اعداد طبیعی است. برای مثال، برای تشخیص عدد ۱۲۷، کافی است که این عدد را بر همه‌ی اعداد اول کوچک‌تر از $\sqrt{۱۲۷}$ تقسیم کنیم. چون $\sqrt{۱۲۷} \simeq ۱۱/۲۷$ و $۱۲۷ \not| ۳$، $۱۲۷ \not| ۵$، $۱۲۷ \not| ۷$ و $۱۲۷ \not| ۱۱$، پس ۱۲۷ عددی اول است. می‌دانیم، هر عدد اول p نسبت به همه‌ی اعداد کوچک‌تر از خودش اول است و بنابراین، نسبت به حاصل‌ضربشان نیز اول است. از این‌رو، شرط کافی برای اول بودن p چنین است:

$$(p,\ (p-1)!)=1 \quad (۴)$$

برای سهولت می‌توان حاصل‌ضرب همه‌ی اعداد اول کوچک‌تر از $\sqrt{p}$ را در نظر گرفت. در صورتی که حاصل‌ضرب همه‌ی اعداد اول فرد کوچک‌تر از $\sqrt{p}$ را با نماد $\lfloor \sqrt{p} \rfloor!$ نشان دهیم، شرط کافی برای اول بودن p چنین است:

$$\left(p,\ \lfloor \sqrt{p} \rfloor!\right)=1 \quad (۵)$$

مثال: با توجه به رابطه‌ی (۵)، شرط کافی برای اول بودن عدد ۱۲۷ را بنویسید.

حل: با توجه به $\sqrt{۱۲۷} \simeq ۱۱/۲۷$ و $\lfloor ۱۱/۲۷ \rfloor = ۱۱$ و رابطه‌ی (۵)، می‌توان نوشت:

$$\left(۱۲۷,\ \lfloor \sqrt{۱۲۷} \rfloor!\right)=۱;\ (۱۲۷, ۳\times۵\times۷\times۱۱)=۱$$

نتیجه‌ی ۷: برای تشخیص اول بودن اعداد طبیعی، کافی است با استفاده از روش نردبانی برای محاسبه‌ی ب. م (الگوریتم اقلیدسی) عمل کنیم و $\left(p,\ \lfloor \sqrt{p} \rfloor!\right)=d$ را محاسبه کنیم. در صورتی که $d=۱$، آن‌گاه p عددی اول است.

مثال: با استفاده از الگوریتم اقلیدسی، مشخص کنید که عدد $p=۱۲۷$، اول است.

حل: در واقع باید $\left(۱۲۷, \underbrace{۳\times۵\times۷\times۱۱}_{۱۱۵۵}\right)=d$ را تعیین کنیم:

چون $d=۱$، پس عدد $p=۱۲۷$، اول است.

	۲	۲	۱	۱	۱۰	۹	(خارج قسمت‌ها)
۱=d	۲	۵	۷	۱۲	۱۲۷	۱۱۵۵	
۰	۱	۲	۵	۷	۱۲		(باقی‌مانده)

نتیجه‌ی ۸: اگر a یک عدد طبیعی دلخواه و p عددی اول باشد، در این صورت دو حالت ممکن $(a,p)=۱$ یا $(a,p)=p$ وجود دارد؛ زیرا با فرض $(a,p)=d$، خواهیم داشت:

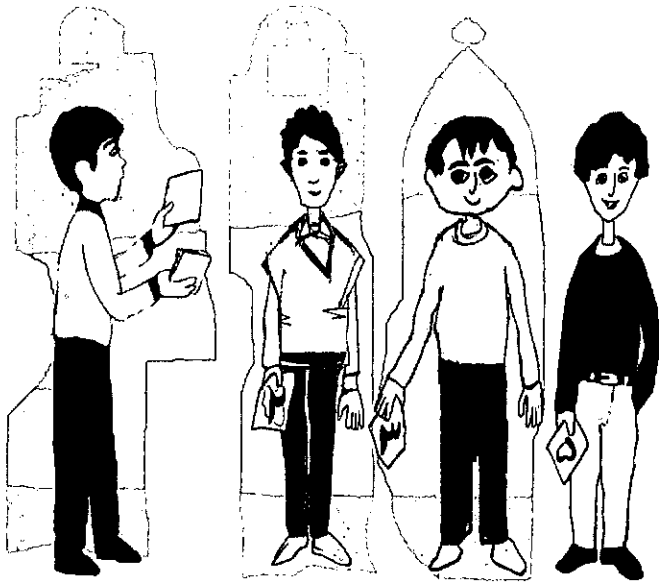
$$d|p \Rightarrow \begin{cases} d=۱ \\ \text{یا} \\ d=p \end{cases} \quad (p \text{ اول است})$$

نتیجه‌ی ۹: اگر p عددی اول باشد، آن‌گاه:

$$p \not| a \Leftrightarrow (p,a)=۱$$

با توجه به نتایج اخیر، واضح است که برای یافتن ب. م. م عدد اول p و یک عدد صحیح دلخواه مانند a، فقط به یک‌بار تقسیم کردن نیاز است؛ زیرا اگر باقی‌مانده‌ی تقسیم a بر p برابر صفر شود، ب. م. م همان p است و اگر باقی‌مانده صفر نشود، ب. م. م برابر ۱ خواهد بود. برای مثال، می‌خواهیم (۲۹ و ۱۳۷۹) را تعیین کنیم. کافی است یک‌بار تقسیم کنیم:

$$۱۳۷۹=۲۹\times۴۷+۱۶$$



چون باقی‌مانده‌ی این تقسیم برابر صفر نشد، بنابراین ب. م. م برابر ۱ خواهد شد (زیرا p=۲۹ عدد اول است):

(۲۹ و ۱۳۷۹) = ۱

نتیجه‌ی ۱۰: اگر p و q دو عدد اول متمایز باشند، در این صورت p و q نسبت به هم اولند.

قضیه‌ی ۵: اگر p عددی اول باشد، آن‌گاه:

$$p|ab \Rightarrow p|a \text{ یا } p|b$$

برهان: اگر p|a، حکم برقرار است. بنابراین، فرض می‌کنیم $p \nmid a$. با توجه به (p,a)=۱ و لم اقلیدس:

$$p|ab \ , \ (b,a)=1 \Rightarrow p|b$$

نتیجه‌ی ۱۱: اگر p عددی اول باشد، آن‌گاه:

$$p|a_1a_2a_3\dots a_k \Rightarrow p|a_1 \text{ یا } p|a_2 \text{ یا } \dots \text{ یا } p|a_k$$

نتیجه‌ی ۱۲: اگر p عددی اول باشد، آن‌گاه:

$$p|a^n \Rightarrow p|a$$: (حالت خاص نتیجه‌ی ۱۱)

مسأله: اگر p عددی اول باشد و داشته باشیم $p|49^n$، نشان دهید: p=۷.

حل:

$$p|49^n;\ p|7^{2n} \Rightarrow p|7$$
$$\Rightarrow p=1 \text{ یا } p=7$$
$$\overset{p \text{ عدد اول}}{\Rightarrow} p=7$$

مسأله: اگر p_1 و p_2، p_3، ... و p_k، اعداد اول باشند و داشته باشیم: $p|p_1p_2\dots p_k$، ثابت کنید به ازای n طبیعی، خواهیم داشت: $p=p_n$.

حل: با توجه به فرض، یعنی $p|p_1p_2\dots p_k$ و نتیجه‌ی (۱)، p حداقل یکی از p_iها مثل p_n را می‌شمارد. بنابراین:

$$p|p_n \Rightarrow p=1 \text{ یا } p=p_n \overset{p \text{ اول است}}{\Rightarrow} p=p_n$$

قضیه‌ی بنیادی حساب

اکنون می‌خواهیم قضیه‌ای را بیان کنیم که یکی از اساسی‌ترین قضیه‌های تئوری اعداد است. این قضیه بیان می‌کند که هر عدد طبیعی بزرگ‌تر از واحد را می‌توان به صورت حاصل‌ضرب اعداد اول نمایش داد و نمایش هر عدد به صورت حاصل‌ضرب این چند عدد اول، بدون در نظر گرفتن ترتیب عوامل ضرب، منحصر به فرد است.

با توجه به این قضیه، نقش بنیادی اعداد اول آشکار می‌شود. یعنی همه‌ی اعداد در واقع از اعداد اول به‌وجود آمده‌اند. در اصطلاح ریاضیدانان، اعداد اول «بلوک‌های ساختمانی» اعداد هستند. پیش از بیان قضیه‌ی بنیادی حساب، لازم است به این تعریف و یک قضیه اشاره شود:

تعریف: با فرض این‌که اعداد اولی مثل p_1، p_2، ... و p_k یافت شوند به‌طوری که $p|p_1p_2\dots p_k$، در این صورت گویند: n به عوامل اول تجزیه شده است. برای مثال، اعداد ۱۸، ۲۴، ۳۶ و ۹۹ را به صورت حاصل‌ضرب عوامل اول به شکل زیر نشان می‌دهیم:

$18=2\times3\times3=2\times3^2$ و $24=2\times2\times2\times3=2^3\times3$

$36=2\times2\times3\times3=2^2\times3^2$ و $99=3\times3\times11=3^2\times11$

تذکر ۱: هیچ‌یک از صورت‌های حاصل‌ضرب ۸×۳، ۶×۴، ۱۲×۲، و ۲۴×۱، یک تجزیه‌ی ۲۴ به عامل‌های اول محسوب نمی‌شود و تنها ۲×۲×۲×۳ و معادل آن $2^3\times3$، تجزیه‌ی ۲۴ به عوامل اول است.

تذکر ۲: صورت حاصل‌ضرب ۱×۷، یک تجزیه‌ی ۷ به عوامل اول نیست و چون ۷ عدد اول است و تنها یک شمارنده به جز ۱ دارد، پس ۷ در واقع یک تجزیه‌ی ۷ به عوامل اول است. بنابراین، اگر p اول باشد، خود p تجزیه‌ی آن به عوامل اول محسوب می‌شود.

قضیه‌ی ۶: هر عدد طبیعی بزرگ‌تر از واحد (n>۱)، حداقل دارای یک شمارنده‌ی اول است.

برهان: اگر مجموعه‌ی تمام شمارنده‌های بزرگ‌تر از واحد عدد طبیعی n را به D نشان دهیم:

$$D=\{k:k>1,\ k|n\}$$

بدیهی است که D تهی نیست $(n \in D)$ و بنابر اصل خوش ترتیبی، دارای عضو ابتدایی مثل p است. کافی است ثابت کنیم، p اول است. می‌دانیم هر شمارنده‌ی p یک شمارنده‌ی

n نیز هست. پس اگر p اول نباشد، در این صورت D عضوی کوچک‌تر از p خواهد داشت که یک تناقض است. بنابراین p اول است.

قضیه‌ی بنیادی حساب: هر عدد طبیعی بزرگ‌تر از واحد ($n>1$) را می‌توان به عوامل اول تجزیه کرد و این تجزیه بدون در نظر گرفتن ترتیب قرار گرفتن عوامل، منحصر به فرد است.

برهان: واضح است که اگر n عددی اول باشد، تجزیه‌ی منحصر به فرد آن به عوامل اول n است. و اگر n مرکب باشد، بر طبق قضیه، دارای حداقل یک شمارنده‌ی اول مثل p_1 خواهد بود:

$$n = p_1 q_1 \quad ; \quad 1 < q_1 < n$$

حال اگر q_1 اول باشد؛ $p_1 q_1$ تجزیه‌ی n به عامل‌های اول است. در غیر این صورت، چون q_1 مرکب است، دارای حداقل یک شمارنده‌ی اول مثل p_2 خواهد بود:

$$q_1 = p_2 q_2 \quad ; \quad 1 < q_2 < q_1$$

اکنون اگر q_2 اول باشد، تجزیه‌ی منحصر به فرد n به عامل‌های اول به صورت زیر خواهد بود:

$$n = p_1 p_2 q_2$$

اگر به همین ترتیب برای q_2، q_3، ... و q_k، عمل کنیم، خواهیم داشت:

$$n = p_1 p_2 p_3 \cdots p_k \cdot q_k$$

با توجه به نابرابری‌های زیر:

$$n > q_1 > q_2 > q_3 > \ldots > q_k > 1$$

بدیهی است که این عمل نمی‌تواند بی‌نهایت بار تکرار شود، یعنی یکی از p_kها عدد اولی مثل p_k خواهد بود. بنابراین، تجزیه‌ی منحصر به فرد n به عوامل اول به این صورت خواهد بود:

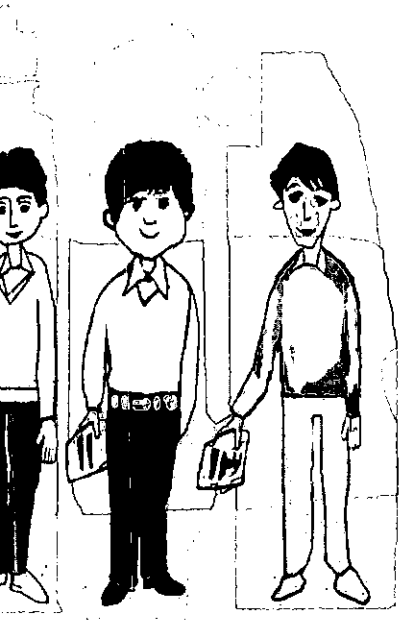
$$n = p_1 p_2 p_3 \cdots p_k$$

توجه: یکتایی این تجزیه را نیز می‌توان اثبات کرد.

تذکر: در صورتی که تعدادی از عامل‌های اول تجزیه با هم برابر باشند، می‌توان هر یک از عامل‌های تکراری را به صورت یک عدد توان‌دار نوشت که در این صورت، هر عدد طبیعی $n>1$ به صورت رابطه‌ی منحصر به فرد زیر تجزیه خواهد شد:

$$n = p_1^k \cdot p_2^s \cdots p_t^r \quad (۶)$$

در رابطه‌ی (۶)، اعداد k، s، ... و r طبیعی و p_iها اعداد



اول متمایزی هستند، با شرط زیر:

$$p_1 < p_2 < \ldots p_t$$

توجه: طریقه‌ی نمایش عدد n را به صورت رابطه‌ی منحصر به فرد (۶)، «تجزیه‌ی استاندارد» یا کانونیک عدد n گویند. برای مثال، تجزیه‌ی استاندارد عدد $n=۱۸۹۰۰$ به صورت زیر است:

$$۱۸۹۰۰ = ۲^۲ \times ۳^۳ \times ۵^۲ \times ۷$$

مسائل حل شده

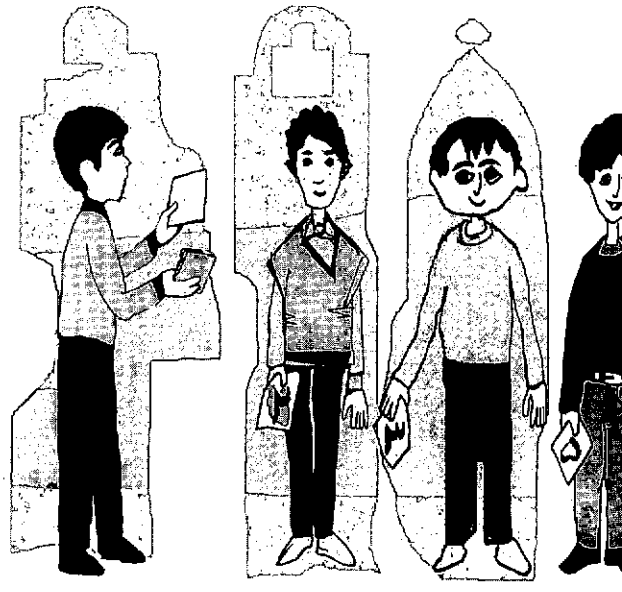
مسأله‌ی ۱: ثابت کنید، هر عدد اول بزرگ‌تر از ۳ به یکی از دو صورت $۶t \pm ۱$ است.

اثبات: طبق الگوریتم تقسیم، هر عدد طبیعی دلخواه به یکی از شش صورت: $۶n$، $۶n+۱$، $۶n+۲$، $۶n+۳$، $۶n+۴$ و $۶n+۵$ نوشته می‌شود. در صورتی که عدد مورد نظر اول و فرد باشد، به صورت $۶n$، $۶n+۲$، $۶n+۳$ یا $۶n+۴$ نمی‌تواند باشد. بنابراین، فقط به یکی از دو صورت $۶n+۱$ و $۶n+۵$ می‌تواند ظاهر شود. بدیهی است که $۶n+۵$ را به صورت $۶(n+۱)-۱$ می‌توان نوشت. پس، هر عدد اول بزرگ‌تر از ۳ به یکی از دو صورت $۶t \pm ۱$ است.

مسأله‌ی ۲: ثابت کنید، هر عدد اول و فرد به یکی از دو صورت $۴t \pm ۱$ است.

اثبات: طبق الگوریتم تقسیم، هر عدد طبیعی دلخواه به یکی از چهار صورت: $۴k$، $۴k+۱$، $۴k+۲$ و $۴k+۳$ نوشته می‌شود. در صورتی که عدد مورد نظر اول و فرد باشد، به صورت‌های $۴k$ و $۴k+۲$ نمی‌تواند باشد. از طرف دیگر، چون $۴k+۳$ را به صورت $۴(k+۱)-۱$ می‌توان نوشت، پس هر عدد اول و فرد تنها به یکی از دو صورت $۴t \pm ۱$ ظاهر می‌شود.

مسأله‌ی ۳: ثابت کنید، هر عدد طبیعی به صورت $۶t-۱$ یا $۴t-۱$، عامل اولی به همان صورت دارد.



اثبات: با فرض این‌که a عددی طبیعی و به صورت $a = 6t-1$ باشد، بدیهی است که تجزیه‌ای به صورت عامل‌های اول به شکل $a = p_1p_2\dots p_n$ خواهد داشت. چون a عددی فرد است، واضح است که همه‌ی p_iها باید فرد باشند (یکی از p_iها زوج باشد، حاصل‌ضربشان زوج خواهد شد). چون p_iها همگی فرد و اول هستند، پس به یکی از دو صورت $6k\pm1$ خواهند بود.

حال اگر همه‌ی عامل‌ها به صورت $6k+1$ باشند، حاصل‌ضرب آن‌ها، یعنی a، باید به صورت $6s+1$ باشد که با فرض، یعنی $a = 6t-1$، متناقض است. پس حداقل یکی از p_iها باید به صورت $6k-1$ باشد. به همین ترتیب ثابت می‌شود که هر عدد طبیعی به صورت $4t-1$، عامل اولی به شکل $4n-1$ دارد.

مسأله‌ی ۴: ثابت کنید بی‌نهایت عدد اول به صورت $4t-1$ یا $6t-1$ وجود دارد.

اثبات: با فرض این‌که تنها n عدد اول p_1، p_2، ... و p_n به یکی از دو صورت فوق وجود دارد، به تناقض خواهیم رسید. زیرا اعداد $4(p_1p_2\dots p_n)-1$ یا $6(p_1p_2\dots p_n)-1$ اگر اول نباشند، مرکب هستند و هر یک عامل اولی به صورت خودشان دارند که جزو p_iها نیست؛ زیرا اگر این عامل اول که آن را به p نشان می‌دهیم، جزو p_iها باشد، در این صورت خواهیم داشت:

$$\left.\begin{array}{l} p \mid 4(p_1p_2\dots p_n) \\ p \mid 4(p_1p_2\dots p_n)-1 \end{array}\right\} \xrightarrow{\text{(p تفاضل را می‌شمارد)}} p \mid 1$$

نتیجه‌ی $p\mid 1$، با فرض اول بودن p متناقض است. به همین ترتیب، برای عدد $6t-1$ نیز به همین نتیجه خواهیم رسید.

بنابراین p عدد اولی به جز p_iها خواهد بود. در این‌جا حکم ثابت است.

مسأله‌ی ۵: اگر p عددی اول و بزرگ‌تر از ۳ باشد؛ ثابت کنید: p^2-1 مضرب ۲۴ است.

اثبات: چون $8\times3=24$، پس کافی است نشان دهیم: p^2-1 بر ۳ و ۸ بخش‌پذیر است. p فرد است و می‌دانیم مربع هر عدد فرد به صورت $p^2=8k+1$ و یا $p^2-1=8k$ است. از طرف دیگر، p عدد اول و غیر ۳ است، پس p به یکی از صورت‌های $p=3t\pm1$ نوشته می‌شود. بنابراین در هر صورت خواهیم داشت:

$$p = 3t\pm1 \;;\; p^2 = 9t^2 \pm 6t + 1$$
$$\;;\; p^2 - 1 = 3(3t^2 \pm 2t)$$
$$\;;\; p^2 - 1 = 3s$$

در این‌جا ثابت شد که p^2-1 به ازای هر عدد اول بزرگ‌تر از ۳ مضربی از ۳ و ۸ و در نتیجه ۲۴ است.

مسأله‌ی ۶: اگر 2^p-1 اول باشد، ثابت کنید p عددی اول است.

اثبات: اگر 2^p-1 عددی اول و p مرکب باشد به تناقض خواهیم رسید. زیرا اگر p مرکب باشد، تجزیه‌ای نابدیهی به صورت $p=mn$ خواهد داشت که با فرض مسلم $2 \le m < n < p$ خواهیم داشت:

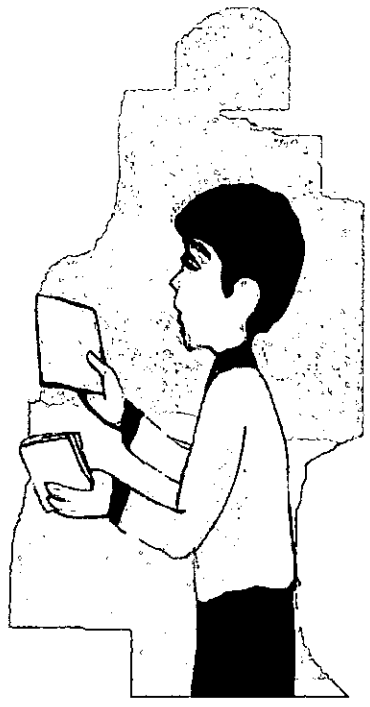
$$p = mn : 2^p - 1 = 2^{mn} - 1 = (2^m)^n - 1$$
$$= (2^m - 1)\left[(2^m)^{n-1} + (2^m)^{n-2} + \dots + 1\right] \quad (*)$$

سمت راست برابری (*)، حاصل‌ضرب دو عامل بزرگ‌تر از واحد و تجزیه‌ای نابدیهی برای 2^p-1 است که با اول بودن آن در تناقض است. پس p اول است.

مسأله‌ی ۷: اگر p عدد اول بزرگ‌تر از ۳ باشد، ثابت کنید: p^2+23 بر ۲۴ بخش‌پذیر است.

اثبات: کافی است نشان دهیم، عدد p^2+23 بر ۳ و ۸ بخش‌پذیر است. از آن‌جا که p عددی اول و بزرگ‌تر از ۳ است، پس به صورت $p=3k\pm1$ می‌باشد. بنابراین:

$$p^2 = 9k^2 \pm 6k + 1 = 9k^2 \pm 6k + 24 - 23$$
$$= 3(3k^2 \pm 2k + 8) - 23$$
$$= 3s - 23 \;\;;\;\; p^2 + 23 = 3s$$



همچنین، چون p عدد اول بزرگ‌تر از ۳ است، بنابراین فرد است و مربع آن به صورت زیر است:

$$p^2 = 8t+1 \; ; \; p^2+23 = 8t+24 = 8(t+3) = 8r$$

در این‌جا ثابت شد که p^2+23 برای هر p اول بزرگ‌تر از ۳، مضربی از ۳ و ۸ و در نتیجه مضربی از ۲۴ است.

مسأله‌ی ۸: ثابت کنید که تنها عدد اول به صورت k^3-1، عدد ۷ است.

اثبات: کافی است ثابت کنیم، عدد k^3-1 به ازای هر عدد طبیعی بزرگ‌تر از ۲ مرکب است. به این منظور عدد k^3-1 را تجزیه می‌کنیم:

$$k^3-1 = (k-1)(k^2+k+1)$$

واضح است که عدد k^3-1 فقط در حالت $k-1=1$ دارای تجزیه‌ی بدیهی است و در حالت $k-1>1$، دارای تجزیه‌ی نابدیهی است. یعنی به ازای $k=2$ $(7=2^3-1)$، عدد k^3-1 اول و به ازای هر $k>2$ مرکب است.

مسأله‌ی ۹: ثابت کنید بی‌نهایت عدد اول وجود دارد.

اثبات: ابتدا برای هر $n \geq 1$، عدد طبیعی $k=n!+1$ را در نظر می‌گیریم، چون $k>1$، پس طبق قضیه، حداقل یک مقسوم علیه اول مثل p خواهد داشت. یعنی عدد اول p وجود دارد، به‌طوری که داشته باشیم:

$$p \mid k=n!+1$$

از طرف دیگر باید: $p>n$. زیرا اگر $p \leq n$، در این صورت خواهیم داشت:

$$p \leq n: \begin{cases} p \mid n! \\ p \mid n!+1 \end{cases} \xrightarrow{\text{(p تفاضل را می‌شمارد)}} p \mid n!+1-n! \Rightarrow p \mid 1 \quad (8)$$

رابطه‌ی (۸) با اول بودن p متناقض است، پس باید: $p>n$.

در این‌جا، به ازای عدد دلخواه $n \geq 1$، به یک عدد اول بزرگ‌تر از n دست یافته‌ایم. پس باید بی‌نهایت عدد اول وجود داشته باشد.

واضح است که به ازای هر $n \geq 1$، به یک عدد اول جدید خواهیم رسید.

تمرین

۱. تعیین کنید کدام یک از اعداد زیر اول است:

الف) ۱۱۸۹ ب) $12!\pm1$

ج) $3\times5\times7\pm2$ د) $2^{132}\pm1$

۲. نشان دهید، عدد $(2^{pq}-1)$ به ازای هر عدد اول p و q همیشه مرکب است و حداقل دارای یک عامل نابدیهی است.

۳. تابع با ضابطه‌ی $f(n) = n^2-n+41$، به ازای $1 \leq n \leq 61$، چند عدد اول تولید می‌کند.

۴. ثابت کنید، اگر (2^m+1) اول باشد، m باید به صورت توانی از ۲ باشد $(m=2^n)$.

۵. اگر p عدد فرد و اول باشد و $p \neq 5$، ثابت کنید: (p^2-1) یا (p^2+1)، همیشه مضربی از ۱۰ است.

۶. ثابت کنید به ازای هر $n \geq 2$، عدد (n^4+4) مرکب است.

۷. حدس می‌زنند که بی‌نهایت عدد اول به صورت n^2-2 و n^2+1 وجود دارد. هفت نمونه از این عددها را بیابید.

۸. ثابت کنید، هر عدد به صورت (8^n+1) مرکب است.

۹. با فرض $(a,b)=p$، حاصل $[a,b]$ و (a^p,b^p)، $(a^{p!},b^{p-1})$ و (a^{p^k},b^p) را در صورتی که p عددی اول باشد، بیابید.

* www.primenumbersformula.com