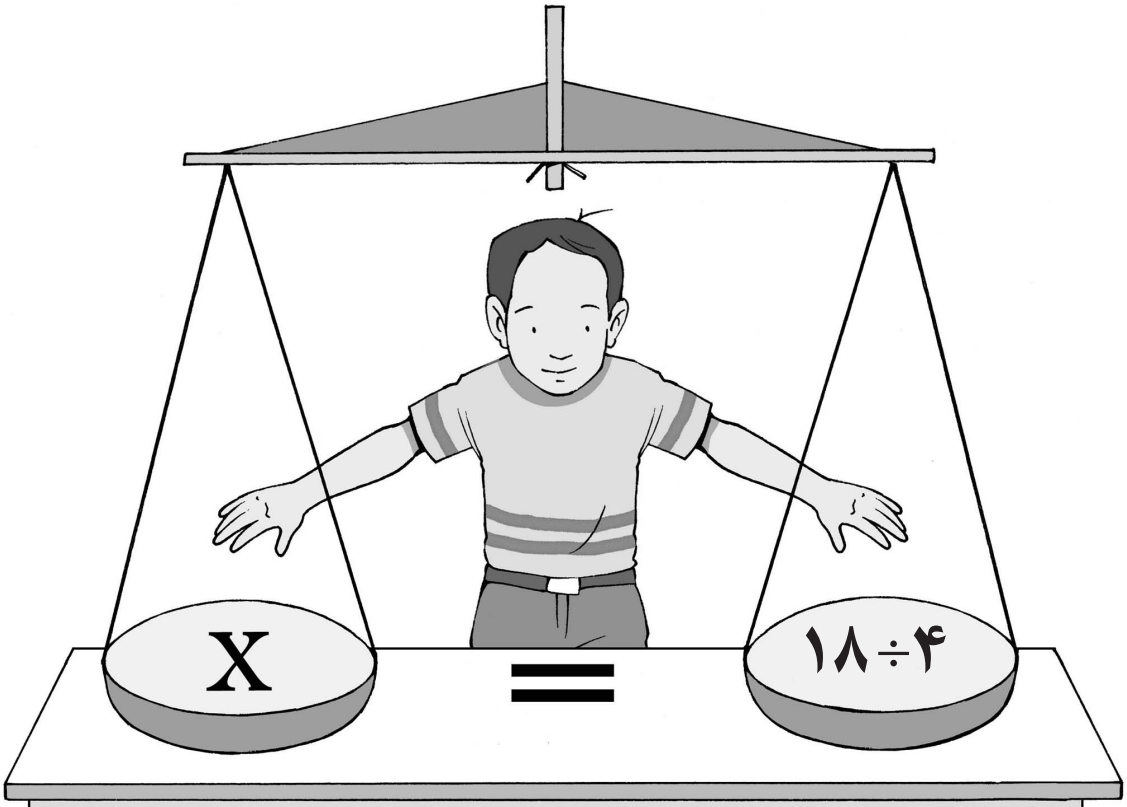
● حمیدرضا امیری

۴

$$a=dq+r$$



کاربردهای قضیه‌ی تقسیم

افراز Z توسط قضیه‌ی تقسیم

در قضیه‌ی تقسیم مشاهده شد که اگر a عددی صحیح و دل‌خواه باشد و $b \in |N$ ، با تقسیم a بر b رابطه‌ی $a=bq+r$ را برای $0 \le r < b$ و در b حالت ممکن، یعنی حالتی که $r = 0$ تا $r = b-1$ باشد، می‌توان نوشت. برای مثال اگر $b = 4$ ، در این صورت باقی‌مانده‌ی تقسیم عدد صحیح a بر ۴، طبق قضیه‌ی تقسیم عبارت است از $r = 0$ یا $r = 1$ یا $r = 2$ یا $r = 3$. به بیان دیگر، هر عدد صحیح مانند a را به یکی از چهار صورت زیر می‌توان نوشت:

$a = 4q$ یا $a = 4q+1$ یا $a = 4q+2$ یا $a = 4q+3$

در واقع می‌توان یک افراز ۴ عضوی برای Z و به‌صورت زیر تعریف کرد:

$$A_1 = \{x \in Z | x = 4k\}$$

$$A_2 = \{x \in Z | x = 4k+1\}$$

$$A_3 = \{x \in Z | x = 4k+2\}$$

$$A_4 = \{x \in Z | x = 4k+3\}$$

در حالت کلی می‌توان یک افراز k عضوی برای Z تعریف کرد؛ یعنی Z را به k زیر مجموعه، افراز یا تقسیم کنیم (منظور از افراز یک مجموعه به n زیر مجموعه‌ی خودش، تقسیم آن مجموعه به n زیر مجموعه است که اول، هیچ‌کدام از زیر مجموعه‌ها تهی نباشند. دوم، دو به دو اشتراکی نداشته باشند و سوم، اجتماع زیرمجموعه‌ها، مجموعه‌ی اصلی را تشکیل دهد):

$$Z = A_1 \cup A_2 \cup \cdots \cup A_k$$

که $A_k = \{x \in Z;\ x = kq + (k-1)\}$

حال می‌خواهیم از این نوع افراز Z، که توسط قضیه‌ی تقسیم صورت گرفت و با استفاده از روشی در استدلال به نام «روش اشباع» چند مسئله در نظریه‌ی اعداد طرح و حل کنیم.

مسئله‌ی ۱: ثابت کنید حاصل‌ضرب هر دو عدد صحیح و متوالی، همواره بر ۲ بخش‌پذیر است.

حل: فرض کنیم $a = n(n-1)$. ثابت می‌کنیم $2|a$. برای این منظور، طبقه قضیه‌ی تقسیم، برای n دو حالت در نظر می‌گیریم. در هر دو حالت ثابت می‌کنیم a بر ۲ بخش‌پذیر است:

الف) $n = 2k \Rightarrow 2|n \Rightarrow 2|n(n-1) \Rightarrow 2|a$

ب) $n = 2k+1 \Rightarrow n-1 = 2k \Rightarrow 2|n-1 \Rightarrow 2|n(n-1) \Rightarrow 2|a$

مسئله‌ی ۲: ثابت کنید حاصل‌ضرب هر سه عدد صحیح و متوالی، همواره بر ۶ بخش‌پذیر است.

حل: فرض کنیم $a = (n-1)n(n+1)$. ثابت می‌کنیم $6|a$. کافی است ثابت شود $2|a$ و $3|a$. برای این منظور، برای n سه حالت در نظر می‌گیریم و از مسئله‌ی ۱ نیز استفاده می‌کنیم:

الف) $n = 3k \Rightarrow 3|n \Rightarrow 3|(n-1)n(n+1) \Rightarrow 3|a$

ب) $n = 3k+1 \Rightarrow n-1 = 3k \Rightarrow 3|n-1$
$\Rightarrow 3|(n-1)n(n+1) = a$

ج) $n = 3k+2 \Rightarrow n+1 = 3k+3 = 3k' \Rightarrow 3|n+1 \Rightarrow 3|(n-1)n(n+1) = a$

ثابت شد که $3|a$. در مسئله‌ی ۱ نیز ثابت کردیم $2|n(n-1)$. بنابراین $2|n(n-1)(n+1) = a$ و در نتیجه $6|a$ (اگر عدد بر ۲ و ۳ بخش‌پذیر باشد، آن‌گاه بر ۶ هم بخش‌پذیر است).

مسئله‌ی ۳: ثابت کنید هر عدد صحیح و فرد را به یکی از دو صورت $(4k+1)$ یا $(4k+3)$ می‌توان نوشت. سپس نشان دهید مربع هر عدد صحیح فرد به‌صورت $(8t+1)$ است.

حل: فرض کنیم a عدد صحیح و دل‌خواه باشد. در این صورت طبق قضیه‌ی تقسیم، a را به یکی از چهار صورت $a = 4k$ یا $a = 4k+1$ یا $a = 4k+2$ یا $a = 4k+3$ می‌توان نوشت. حال اگر a فرد باشد، $a \neq 4k$ و $a \neq 4k+2$. بنابراین، فقط به یکی از دو صورت $a = 4k+1$ یا $a = 4k+3$ نوشته می‌شود:

الف) $a = 4k+1 \Rightarrow a^2 = 16k^2 + 8k + 1 = 8t_1 + 1$

ب) $a = 4k+3 \Rightarrow a^2 = 16k^2 + 24k + 9$
$\Rightarrow a^2 = 16k^2 + 24k + 8 + 1 = 8t_2 + 1$

مسئله‌ی ۴: ثابت کنید برای هر $n \in Z$ عدد $a = n^5 - n$ بر ۳۰ بخش‌پذیر است.

حل: چون $a = n(n-1)(n+1)(n^2+1)$ و قبلاً طبق مسئله‌ی ۲ ثابت کردیم $6|n(n-1)(n+1)$، پس $6|a$. کافی است ثابت کنیم $5|a$. برای این منظور، برای n، پنج حالت در نظر می‌گیریم:

الف) $n = 5k \Rightarrow 5|n \Rightarrow 5|n(n^4-1) \Rightarrow 5|a$

ب) $n = 5k+1 \Rightarrow n-1 = 5k \Rightarrow 5|n-1 \Rightarrow 5|a$

پ) $n = 5k+2 \Rightarrow n^2 = 25k^2 + 20k + 4$
$\Rightarrow n^2+1 = 25k^2 + 20k + 5 = 5t \Rightarrow 5|n^2+1$
$\Rightarrow 5|(n^2-1) \times n \times (n^2+1) = a$

ت) $n = 5k+3 \Rightarrow n^2 = 25k^2 + 30k + 9 \Rightarrow n^2+1$
$\Rightarrow n^2+1 = 25k^2 + 30k + 10 = 5t$
$\Rightarrow 5|n^2+1 \Rightarrow 5|a$

ث) $n = 5k+4 \Rightarrow n+1 = 5k+5 = 5t \Rightarrow 5|n+1 \Rightarrow 5|a$

مسئله‌ی ۵: اگر a عددی فرد و مضرب ۳ نباشد، ثابت کنید (a^2+23) بر ۲۴ بخش‌پذیر است.

حل: کافی است ثابت کنیم (a^2+23) بر ۸ و بر ۳ بخش‌پذیر است.

a فرد است $\Rightarrow a^2 = 8t+1$

$\Rightarrow a^2 + 23 = 8t + 1 + 23 = 8t + 24$

$\Rightarrow a^2 + 23 = 8(\underbrace{t+3}_{t_1}) \Rightarrow 8|a^2+23$

$a \neq 3k \Rightarrow \begin{cases} a = 3k+1 \\ a = 3k+2 \end{cases}$ طبق فرض

اگر $a = 3k+1 \Rightarrow a^2 = 9k^2 + 6k + 1$

$\Rightarrow a^2 + 23 = 9k^2 + 6k + 24 = 3k'$

اگر $a = 3k+2 \Rightarrow a^2 = 9k^2 + 12k + 4$

$\Rightarrow a^2 + 23 = 9k^2 + 12k + 27 = 3k''$

مسئله‌ی ۶: ثابت کنید، اگر $p > ۳$ عددی اول باشد، فقط به یکی از دو صورت $۶k \pm ۱$ نوشته می‌شود.

حل: می‌دانیم عدد $p \in N$ و $p \neq ۱$ اول است، هرگاه هیچ شمارنده یا مقسوم‌علیه مثبتی به جز ۱ و خودش نداشته باشد و می‌دانیم عدد ۲ تنها عدد اول و زوج است. و نیز می‌دانیم هر عدد به‌صورت $۶t + ۵$ همان $۶k - ۱$ است، زیرا:

$$۶t + ۵ = ۶t + ۶ - ۱ = ۶(t + ۱) - ۱ = ۶k - ۱$$

حال اگر p عددی اول باشد، لذا عددی صحیح است و هر عدد صحیح به یکی از ۶ صورت $۶k$ یا $۶k + ۱$ یا $۶k + ۲$ یا $۶k + ۳$ یا $۶k + ۴$ یا $۶k + ۵$ نوشته می‌شود که چون p اول و بزرگ‌تر از ۳ است، پس p زوج نیست و $p \neq ۶k$، $p \neq ۶k + ۲$ و $p \neq ۶k + ۴$ و نیز p، مضرب ۳ نیستند. پس $p \neq ۶k + ۳$. بنابراین فقط می‌تواند به یکی از دو صورت $p = ۶k + ۱$ یا $p = ۶k + ۵$ باشد که همان $۶t - ۱$ است.

نتیجه‌ی متمم از مسئله‌ی ۶: اگر عددی طبیعی و بزرگ‌تر از ۳ را بر ۶ تقسیم کنیم و باقی‌مانده‌ی تقسیم آن عدد با ۱ یا ۵ برابر نباشد، قطعاً آن عدد اول نیست و اگر باقی‌مانده ۱ یا ۵ باشد، دلیل بر اول بودن آن عدد نیست. فقط می‌توان گفت آن عدد می‌تواند اول باشد. مانند عدد ۲۵ که به‌صورت $۶ \times ۴ + ۱$ است، ولی اول نیست.

مسئله‌ی ۷: اگر a عددی فرد و اول باشد، ثابت کنید a را فقط به یک صورت منحصربه‌فرد به شکل تفاضل مربعین دو عدد طبیعی می‌توان نوشت.

حل: می‌دانیم اگر a فرد باشد، اعداد $(\frac{a+۱}{۲})$ و $(\frac{a-۱}{۲})$ اعدادی طبیعی و $a = (\frac{a+۱}{۲})^۲ - (\frac{a-۱}{۲})^۲$.

حال برای اثبات منحصر به فردی فرض کنیم x و y دو عدد طبیعی هستند و $a = x^۲ - y^۲$. در این صورت داریم: $a = (x-y)(x+y)$ که $۰ < x - y < x + y$ و چون a اول است $a = ۱ \times a$، پس $x - y = ۱$ و $x + y = a$ که با حل دستگاه $\begin{cases} x + y = a \\ x - y = ۱ \end{cases}$ داریم:

$$x = \frac{a+۱}{۲} \quad \text{و} \quad y = \frac{a-۱}{۲}.$$

یعنی: $a = x^۲ - y^۲ = (\frac{a+۱}{۲})^۲ - (\frac{a-۱}{۲})^۲$

تمرین: عکس مسئله‌ی ۷ را ثابت کنید. یعنی ثابت کنید: اگر یک عدد طبیعی و فرد که مخالف یک است، فقط یک نمایش به‌صورت تفاضل مربعین دو عدد صحیح و نامنفی داشته باشد، آن‌گاه آن عدد اول است (روش اثبات خود را برای ما بفرستید).

مسئله‌ی ۸: اگر p عددی اول و بزرگ‌تر از ۳ باشد، ثابت کنید $p^۲ - ۱$ بر ۲۴ بخش‌پذیر است.

حل: فرض کنیم: $a = p^۲ - ۱$. ثابت می‌کنیم: $۲۴ | a$. برای این منظور کافی است ثابت کنیم: $۸ | a$ و $۳ | a$.

$$p > ۳ \Rightarrow p \text{ فرد است} \Rightarrow p^۲ = ۸k + ۱ \Rightarrow p^۲ - ۱ = ۸k \text{ اول است}$$

$$\Rightarrow ۸ | p^۲ - ۱ \Rightarrow ۸ | a$$

$$p > ۳ \Rightarrow p \neq ۳k \begin{cases} p = ۳k + ۱ \Rightarrow p - ۱ = ۳k \\ p = ۳k + ۲ \Rightarrow p + ۱ = ۳k' \end{cases} \text{ اول است: بخش‌پذیری ۳}$$

$$\Rightarrow \begin{cases} ۳ | p - ۱ \Rightarrow ۳ | (p-۱)(p+۱) = p^۲ - ۱ = a \\ ۳ | p + ۱ \Rightarrow ۳ | (p+۱)(p-۱) = p^۲ - ۱ = a \end{cases}$$

مسئله‌ی ۹: اگر p عددی اول و بزرگ‌تر از ۵ باشد، ثابت کنید $(p^۴ - ۱)$ بر ۱۲۰ بخش‌پذیر است.

حل: اگر فرض کنیم $a = p^۴ - ۱$، ثابت می‌کنیم $۱۲۰ | p^۴ - ۱$. کافی است ثابت کنیم $(p^۴ - ۱)$ بر ۵ و ۲۴ بخش‌پذیر است.

$$۲۴ | p^۲ - ۱ \Rightarrow ۲۴ | (p^۲ - ۱)(p^۲ + ۱) \Rightarrow ۲۴ | a \text{ ثابت شد: بخش‌پذیری بر ۲۴}$$

$$p > ۵ \text{ اول است: بخش‌پذیری بر ۵}$$

$$\Rightarrow p \neq ۵k \begin{cases} p = ۵k + ۱ \Rightarrow p - ۱ = ۵k \Rightarrow ۵ | p - ۱ \Rightarrow ۵ | a \\ p = ۵k + ۲ \\ p = ۵k + ۳ \\ p = ۵k + ۴ \end{cases}$$

اگر $p = ۵k + ۲ \Rightarrow p^۲ = ۲۵k^۲ + ۲۰k + ۴$

$$\Rightarrow p^۲ + ۱ = ۵k' \Rightarrow ۵ | p^۲ + ۱ \Rightarrow ۵ | a$$

اگر $p = ۵k + ۳ \Rightarrow p^۲ = ۲۵k^۲ + ۳۰k + ۹$

$$\Rightarrow p^۲ + ۱ = ۵k'' \Rightarrow ۵ | p^۲ + ۱ \Rightarrow ۵ | a$$

اگر $p = ۵k + ۴ \Rightarrow p + ۱ = ۵t \Rightarrow ۵ | p + ۱ \Rightarrow ۵ | a$