

قرار دادن تعدادی شیء در دسته‌های مساوی یا دسته‌بندی کردن تعدادی از چیزها را، بدون آنکه باقی مانده‌ای داشته باشیم، «عاد کردن» یا شمارش آن اشیا، توسط شمارنده‌ها می‌گویند. مثلاً، ۱۲ شیء را می‌توان با شمارنده‌های مثبت عدد ۱۲ یعنی ۱، ۲، ۳، ۴، ۶ و ۱۲ دسته‌بندی یا شمارش کرد. در این فصل برای نمایش این مفهوم از نماد « $|$ » استفاده کرده و مثلاً می‌نویسیم $۲|۱۲$ و می‌خوانیم عدد ۲ عدد ۱۲ را می‌شمارد یا عاد می‌کند. بیان دیگر این مفهوم آن است که بگوییم عدد ۱۲ بر عدد ۲ بخش پذیر است (باقی مانده تقسیم صفر است).

توجه داشته باشید که دسته‌بندی کردن اشیا در دسته‌های صفرتایی یا شمارش تعدادی شیء خاص به صورت صفر تا صفر تا کار بی‌معنایی است؛ لذا صفر هیچ عدد غیر صفری را نمی‌شمارد و هیچ عدد غیر صفری بر صفر بخش پذیر نمی‌باشد در ضمن توجه داشته باشید که هر عدد بر خودش و بر ۱ بخش پذیر است؛ یعنی اگر a عددی طبیعی باشد $۱|a$ و $a|a$. (عدد ۱ هر عدد صحیح را عاد می‌کند و هر عدد بر خودش بخش پذیر است).

حال با توجه به اینکه مفهوم بخش پذیری b بر a معادل است با اینکه بنویسیم $a|b$ (عدد a ، عدد b را می‌شمارد یا عدد a ، عدد b را عاد می‌کند) مفهوم بخش پذیری را می‌توان برای هر دو عدد صحیح به کار برد، مثلاً می‌توان گفت، عدد $۲۸ - ۴$ بر ۴ بخش پذیر است (زیرا، $۲۸ = ۴ \times (-۷)$ یا باقی مانده تقسیم $۲۸ - ۴$ بر عدد ۴ صفر است) پس در حالت کلی و با تعمیم مفهوم عاد کردن به مجموعه اعداد صحیح عاد کردن به صورت زیر تعریف می‌شود.

عدد صحیح a ، که مخالف صفر است^۲، شمارنده عدد b است - یا a ، b را می‌شمارد یا $a|b$ یا b بر a بخش پذیر است - هرگاه عددی صحیح چون q وجود داشته باشد به طوری که $b = aq$.

اگر عدد b بر عدد a بخش پذیر نباشد یا عدد a عدد b را عاد نکند می‌نویسیم، $a \nmid b$

۱- در سراسر این فصل منظور از عدد، عدد صحیح است.

۲- اینکه صفر عدد صفر را می‌شمارد به صورت یک قرارداد پذیرفته می‌شود.

۱ با توجه به تعریف رابطه عاد کردن جاهای خالی را پر کنید.

الف) $7 \mid 63 \Leftrightarrow 63 = \dots \times \dots$

ب) $91 = 7 \times \dots \Leftrightarrow \dots \mid 91$

پ) $-6 \mid 54 \Leftrightarrow \dots = \dots \times (-6)$

ت) $5 \mid -35 \Leftrightarrow \dots = 5 \times \dots$

ث) $0 = 18 \times \dots \Leftrightarrow 18 \mid \dots$

ج) $a \mid 1 \Rightarrow a = \dots$ یا $a = \dots$

چ) $26 = 2 \times 13 \Rightarrow 2 \mid \dots$ و $\dots \mid 26$

۲ با استفاده از تعریف عاد کردن و قوانین ضرب و تقسیم اعداد توان دار با پایه‌های برابر، ابتدا نشان دهید که $3^5 \mid 3^9$ و

سپس ثابت کنید:

$$\forall m, n \in \mathbb{N}; m \leq n \Rightarrow a^m \mid a^n$$

$$(3^9 = 3^5 \times 3^4 \Rightarrow 3^5 \mid \dots)$$

ویژگی‌های رابطه عاد کردن

ویژگی ۱: اگر عدد a عدد b را بشمارد، آنگاه هر مضرب صحیح عدد b را نیز می‌شمارد؛ یعنی:

$$a \mid b \Rightarrow a \mid mb$$

مثال: $3 \mid 6 \Rightarrow 3 \mid 6 \times 5, 3 \mid 6 \times 4, 3 \mid 6 \times (-7), \dots$

نتیجه: اگر عدد a عدد b را بشمارد، آنگاه b^n را می‌شمارد و در حالت کلی b^n را می‌شمارد که $n \in \mathbb{N}$ است. یعنی:

$$\begin{cases} \text{الف) } a \mid b \Rightarrow a \mid b^2 \\ \text{ب) } a \mid b \Rightarrow a \mid b^n \end{cases}$$

برای اثبات (الف) کافی است از ویژگی ۱ استفاده کرده و m را مساوی با b فرض کنیم؛ و برای اثبات (ب) نیز کافی است $m = b^{n-1}$ فرض شود.

سؤال: آیا از اینکه $a \mid bc$ می‌توان نتیجه گرفت که a حداقل یکی از دو عدد b و c را عاد می‌کند؟ به گزاره‌های زیر دقت کنید و پس از آن پاسخ دهید:

الف) $3 \mid 9$ و $3 \mid 6$ و $3 \mid 6 \times 9$

ب) $3 \mid 5$ و $3 \mid 6$ و $3 \mid 6 \times 5$

ج) $6 \mid 4$ و $6 \mid 3$ و $6 \mid 3 \times 4$

سؤال: آیا از اینکه $a \mid b$ می‌توان نتیجه گرفت که $ka \mid kb$ ؟ آیا از $ka \mid kb$ می‌توان نتیجه گرفت $a \mid b$ ؟ ($k \in \mathbb{Z}$)

$$a \mid b \Rightarrow b = \overset{\text{در } k \text{ ضرب}}{\dots} \Rightarrow kb = \dots \Rightarrow \dots$$

$$ka \mid kb \Rightarrow kb = \overset{\text{بر } k \text{ تقسیم}}{\dots} \Rightarrow b = \dots \Rightarrow \dots$$

ویژگی ۲: اگر عدد a عدد b را بشمارد و عدد b نیز عدد c را بشمارد آنگاه عدد a عدد c را می‌شمارد.

$$a|b \wedge b|c \Rightarrow a|c$$

اثبات: $\begin{cases} a|b \Rightarrow b = aq_1 \text{ (۱)} \\ b|c \Rightarrow c = bq_2 \end{cases}$

$$c = bq_2 \stackrel{(۱)}{\Rightarrow} c = \dots q_2 \stackrel{q_1 q_2 = q}{\Rightarrow} c = a \dots \Rightarrow a|c$$

این خاصیت را «خاصیت تعدی» برای رابطه عاد کردن می‌نامیم.

سؤال: با استفاده از خاصیت تعدی برای رابطه عاد کردن، نشان دهید که:

$$a|b \Rightarrow a|b^n$$

اثبات: $a|b$ تعدی فرض: $a|b \Rightarrow \dots | \dots$
 $b|b^n$ و می‌دانیم:

ویژگی ۳: هرگاه عددی دو عدد را بشمارد آنگاه مجموع و تفاضل آن دو عدد را نیز می‌شمارد.

$$a|b \wedge a|c \Rightarrow a|b \pm c$$

اثبات: $\left. \begin{array}{l} a|b \Rightarrow b = \dots \times q_1 \\ a|c \Rightarrow \dots = aq_2 \end{array} \right\} \Rightarrow b \pm c = \dots \underbrace{(q_1 \pm q_2)}_q \Rightarrow a | \dots$

سؤال: آیا از اینکه $a|b + c$ همواره می‌توان نتیجه گرفت که $a|b$ یا $a|c$ ؟

ویژگی ۴: اگر $a|b$ و $b \neq 0$ در این صورت $|a| \leq |b|$.

اثبات: چون $a|b$ پس $b = aq$ و چون $b \neq 0$ پس $q \neq 0$ و چون $q \in \mathbb{Z}$ لذا $|q| \geq 1$. حال اگر طرفین نامساوی اخیر را

در $|a|$ ضرب کنیم خواهیم داشت:

$$1 \leq |q| \Rightarrow |a| \times 1 \leq |a| |q| \Rightarrow |a| \leq |aq| \Rightarrow |a| \leq \dots$$

نتیجه: اگر $a|b$ و $b|a$ آنگاه $a = \pm b$.

اثبات: $\left. \begin{array}{l} a|b \stackrel{(۴)}{\Rightarrow} |a| \leq \dots \\ b|a \stackrel{(۴)}{\Rightarrow} \dots \leq |a| \end{array} \right\} \Rightarrow |a| = |b| \Rightarrow a = \pm b$

کار در کلاس

۱ اگر $a \neq 0$ عددی صحیح و دو عدد $(7m+6)$ و $(6m+5)$ بر a بخش پذیر باشند ثابت کنید $a = \pm 1$.

$$\left. \begin{array}{l} a|7m+6 \Rightarrow a|42m+\dots \\ a|6m+5 \Rightarrow \dots|42m+\dots \end{array} \right\} \Rightarrow a|(42m+36) - (42m+35)$$

$$\Rightarrow a|1 \Rightarrow a = \pm 1 \text{ (چرا؟)}$$

۲ اگر $a|b$ نشان دهید که $a^n|b^n$.

$$\text{اثبات: } a|b \Rightarrow b = aq \Rightarrow b^n = \dots \Rightarrow b^n = \dots q^n \Rightarrow a^n | b^n$$

۳ اگر $a|b$ و $c|d$ نشان دهید که $ac|bd$.

$$\left. \begin{array}{l} a|b \Rightarrow b = aq_1 \\ c|d \Rightarrow \dots = \dots \end{array} \right\} \Rightarrow b \times d = (a \times c) \underbrace{(q_1 q_2)}_q$$

$$\Rightarrow \dots = a \times c \times q \Rightarrow \dots | bd$$

۴ اگر $a|b$ و $a|c$ نشان دهید که $a|mb \pm nc$.

(از ویژگی ۱ و ویژگی ۳ استفاده کنید).

شما در سال‌های قبل با تعریف و مفهوم اعداد اول آشنا شده‌اید و می‌دانید که هر عدد طبیعی و بزرگ‌تر از یک که هیچ شمارندهٔ مثبتی به جز یک و خودش نداشته باشد، عدد اول نامیده می‌شود. مجموعهٔ اعداد اول، که ثابت شده است مجموعه‌ای نامتناهی است، به صورت $P = \{2, 3, 5, 7, 11, \dots\}$ نمایش داده می‌شود.

تذکر: با توجه به تعریف عدد اول، اگر p عددی اول باشد و a عددی طبیعی و $a|p$ در این صورت $a=1$ یا $a=p$.

مثال: اگر عدد طبیعی a دو عدد $(9k+7)$ و $(7k+6)$ را عاد کند، ثابت کنید $a=1$ یا $a=5$.

$$a | 9k+7 \Rightarrow a | 7 \times (9k+7)$$

$$\Rightarrow a | 63k + \dots$$

$$a | 7k+6$$

$$\Rightarrow a | 9 \times (7k+6) \Rightarrow a | \dots + 54$$

$$\Rightarrow a | (\dots + 54) - (63k + \dots)$$

$$\Rightarrow a | 5 \Rightarrow a = \dots \text{ یا } a = \dots$$

خواندنی

می‌دانیم که هر عدد طبیعی و کوچک‌تر یا مساوی $10!$ عدد $10!$ را عاد می‌کند (چرا؟) و به طور کلی می‌توان نوشت: $\forall k \leq n, k | n!$ ؛ بنابراین عدد $100!+2$ و همین‌طور عدد $100!+3$ و \dots و بالاخره عدد $100!+100$ همه اعدادی غیر اول هستند. بنابراین با توجه به اینکه اعداد $(100!+2)$ و $(100!+3)$ و \dots و $(100!+100)$ ، تعداد ۹۹ عدد طبیعی و متوالی‌اند ما توانسته‌ایم ۹۹ عدد طبیعی متوالی بیابیم که هیچ‌کدام اول نباشند.

آیا شما می‌توانید ۱۵ عدد طبیعی متوالی بیابید که هیچ‌کدام اول نباشند؟

(برای اینکه نشان دهیم عدد $100!+7$ بر ۷ بخش‌پذیر است، کافی است از عدد ۷ در دو عدد $100!$ و ۷،

فاکتور بگیریم یا با استفاده از خواص عاد کردن بنویسیم: $7 | 100!+7 \Rightarrow 7 | 7$ و $7 | 100!$)

بزرگ‌ترین مقسوم‌علیه مشترک و کوچک‌ترین مضرب مشترک دو عدد

می‌خواهیم با توجه به تعریف رابطه عادی کردن، مفاهیم m م (بزرگ‌ترین مقسوم‌علیه مشترک) و k م م (کوچک‌ترین مضرب مشترک) دو عدد را معرفی کنیم.

توجه دارید که مقسوم‌علیه همان شمارنده است. به عبارت دیگر، اگر بنویسیم $a|b$ ، یعنی a شمارنده b است یا b بر a بخش‌پذیر است و این یعنی a مقسوم‌علیه b است؛ و نیز توجه دارید که b مضرب a است، یعنی $b = aq$ یا $a|b$.

تعریف: عدد طبیعی d را m م دو عدد صحیح a و b می‌نامیم (a و b هر دو با هم صفر نیستند) و می‌نویسیم $(a, b) = d$ ، هرگاه دو شرط (الف) و (ب) برقرار باشند و اگر دو شرط زیر برقرار باشد آنگاه $(a, b) = d$.

(الف) $d|a, d|b$

(ب) $\forall m > 0; m|a, m|b \Rightarrow m \leq d$

شرط (الف) مقسوم‌علیه مشترک بودن را برای d تأمین می‌کند و شرط (ب) نشان می‌دهد که d از هر مقسوم‌علیه مشترک دلخواهی چون m بزرگ‌تر است.

اگر داشته باشیم $(a, b) = 1$ در این صورت می‌گوییم، a و b نسبت به هم اول‌اند.

مثال: $(1, 12) = 1$, $(7, 11) = 1$, $(4, 9) = 1$, $(3, 4) = 1$

$(4, -6) = 2$, $(0, 6) = 6$, $(8, 16) = 8$, $(6, 9) = 3$

تعریف: عدد طبیعی c را k م دو عدد صحیح و ناصفر a و b می‌نامیم و می‌نویسیم $[a, b] = c$ ، هرگاه دو شرط

(الف) و (ب) برقرار باشند، و اگر این دو شرط برقرار باشد آنگاه $[a, b] = c$

(الف) $a|c, b|c$

(ب) $\forall m > 0, a|m, b|m \Rightarrow c \leq m$

توضیح دهید که هریک از شرط‌های (الف) و (ب) کدام ویژگی را تأمین می‌کنند؟

مثال: $[3, 4] = 12$, $[6, 4] = 12$, $[1, 8] = 8$, $[-4, 16] = 16$

کاردرکلاس

۱ با توجه به تعاریف m م و k م ثابت کنید:

(الف) $a|b \Rightarrow (a, b) = |a|$

(ب) $a|b \Rightarrow [a, b] = |b|$

راهنمایی: برای اثبات (الف) باید دو شرط موجود در تعریف m م را برای $|a|$ بررسی کنیم، یعنی نشان دهیم که $|a| | a|$

و... و نیز برای هر $m > 0$ که $m|a$ و $m|b$ نشان دهیم $m \leq \dots$ و همین‌طور برای اثبات (ب) ...

۲ اگر p عددی اول باشد و $a \in \mathbb{Z}$ و $p \nmid a$ ، ثابت کنید، $(p, a) = 1$

$$(p, a) = d \begin{cases} d \mid p \Rightarrow d = 1 \text{ یا } \dots \\ d \mid a \quad (1) \end{cases}$$

و این با فرض $p \nmid a$ تناقض دارد) $d = p \Rightarrow p \mid \dots$

پس فقط $d = \dots$ یا $(p, a) = \dots$.

تذکر: توجه دارید که در مورد اعدادی که اول نباشند، مطلب کار در کلاس ۲ ممکن است برقرار نباشد:

$$\text{مثال: } (4, 6) = 2 \neq 1 \text{ ولی } 4 \nmid 6$$

قضیه تقسیم و کاربردها

ممکن است در تقسیم عدد صحیح a بر عدد طبیعی b ، باقی مانده صفر نباشد، یعنی a بر b بخش پذیر نباشد $(b \nmid a)$. در این صورت قضیه تقسیم که به بیان آن خواهیم پرداخت (این قضیه را بدون اثبات می پذیریم) کمک می کند تا بحث بخش پذیری در \mathbb{Z} را کامل کنیم.

قضیه تقسیم: اگر a عددی صحیح و b عددی طبیعی باشد در این صورت، اعدادی صحیح و منحصر به فرد مانند q و r یافت می شوند به قسمی که $a = bq + r$ و $0 \leq r < b$.

مثال: اگر ۲۵ را بر ۷ تقسیم کنیم داریم: $q = 3$ و $r = 4$ ، و به عبارت دیگر $25 = (7 \times 3) + 4$. حال اگر ۲۵ را بر ۷ تقسیم کنیم و $q = -3$ در نظر بگیریم، در این صورت تساوی $25 = 7 \times (-3) - 4$ حاصل می شود که نمی توان (-4) را به عنوان باقی مانده معرفی کرد، زیرا طبق قضیه تقسیم باقی مانده باید نامنفی و کوچک تر از مقسوم علیه باشد در این صورت با اضافه و کم کردن مضارب مثبتی از مقسوم علیه، شرایط قضیه تقسیم را برقرار می کنیم:

$$\begin{aligned} -25 &= 7 \times (-3) - 4 = 7 \times (-3) - 4 - 7 + 7 \\ &= 7 \times (-3) - 7 + 3 = 7 \underbrace{[(-3) - 1]}_q + 3 = 7q + 3 \Rightarrow r = 3 \end{aligned}$$

تذکر: همان طور که از دوره ابتدایی به خاطر دارید در تقسیم عدد a بر b ، a را مقسوم، b را مقسوم علیه، q را خارج قسمت و r را باقی مانده می نامیم.

مثال: اگر باقی مانده تقسیم اعداد m و n بر ۱۷ به ترتیب ۵ و ۳ باشد، در این صورت باقی مانده تقسیم عدد $(2m - 5n)$ بر ۱۷ را به دست آورید.

حل:

$$\begin{aligned} \text{طبق فرض: } m &= 17q_1 + 5 \\ \text{طبق فرض: } n &= 17q_2 + 3 \end{aligned} \Rightarrow \begin{cases} 2m = 2 \times 17q_1 + 10 \\ -5n = (-5) \times 17q_2 - 15 \end{cases}$$

$$\Rightarrow (2m - 5n) = 17(2q_1 - 5q_2) - 5$$

$$\begin{aligned}
&= 17(2q_1 - 5q_2) - 5 - 17 + 17 \\
&= 17(\underbrace{2q_1 - 5q_2}_{q_r} - 1) + 17 - 5 \\
&\Rightarrow (2m - 5n) = 17(\underbrace{q_r - 1}_q) + 12 \\
&= 17q + 12 \Rightarrow r = 12
\end{aligned}$$

افراز مجموعه \mathbb{Z} به کمک قضیه تقسیم

با توجه به قضیه تقسیم، می‌دانیم که اگر a عددی صحیح و دلخواه باشد، با تقسیم آن بر عدد طبیعی b ، و با توجه به اینکه باقی‌مانده تقسیم یعنی r در رابطه $0 \leq r < b$ صدق می‌کند، برای a بر حسب r دقیقاً b حالت وجود دارد، مثلاً اگر عدد صحیح a را بر ۵ تقسیم کنیم در این صورت یا a بر ۵ بخش پذیر است، یعنی $r = 0$ ، یا باقی‌مانده تقسیم a بر ۵ عدد ۱ است یا ... یا باقی‌مانده تقسیم ۴ است؛ به عبارت دیگر، $a = 0 \dots$ یا $a = 5k + 3$ یا $a = 0 \dots$ یا $a = 5k + 1$ یا $a = 5k$ پس می‌توان گفت هر عدد صحیح مانند a را می‌توان به یکی از پنج صورت فوق نوشت.

مسئله ۱: اگر $m \in \mathbb{Z}$ نشان دهید که m را به یکی از دو صورت $2k$ یا $2k + 1$ (زوج یا فرد) می‌توان نوشت.

حل: کافی است m را بر ۲ تقسیم کنیم؛ در این صورت طبق قضیه تقسیم خواهیم داشت:

$$m = 2k + r, \quad 0 \leq r < 2 \Rightarrow m = \dots \text{ یا } m = \dots$$

مسئله ۲: ثابت کنید اگر $p > 3$ عددی اول باشد، آنگاه به یکی از دو صورت $p = 6k + 1$ یا $p = 6k + 5$ نوشته می‌شود.

حل: کافی است p را بر ۶ تقسیم کنیم، در این صورت طبق قضیه تقسیم خواهیم داشت:

$$p = 6k \quad (1)$$

$$p = 6k + 1 \quad (2)$$

$$p = 6k + 2 \quad (3)$$

$$p = 6k + 3 \quad (4)$$

$$p = 6k + 4 \quad (5)$$

$$p = 6k + 5 \quad (6)$$

در حالت (۱)، (۳) و (۵) زوج است و لذا با اول بودن آن تناقض دارد. در حالت (۴) و با فاکتورگیری از ۳ داریم:

$$p = 3(2k + 1)$$

یا $p = 3k'$ یا $3|p$ که با اول بودن p در تناقض است و لذا فقط حالت‌های (۲) و (۶) باقی می‌ماند و حکم اثبات می‌شود.

(توجه دارید که عکس مطلب فوق در حالت کلی برقرار نیست؛ مثلاً $(25 = 6 \times 4 + 1)$ ولی ۲۵ اول نیست.)

مسئله ۳: ابتدا ثابت کنید که هر عدد صحیح و فرد مانند a به یکی از دو صورت $4k + 1$ یا $4k + 3$ نوشته می‌شود، سپس

نشان دهید که مربع هر عدد فرد به شکل $(8t + 1)$ نوشته می‌شود (باقی‌مانده تقسیم مربع هر عدد فرد بر ۸، مساوی با ۱

است.)

حل : فرض کنیم $a \in \mathbb{Z}$ و a فرد باشد، اگر a را بر ۴ تقسیم کنیم خواهیم داشت :

$$a=4k \quad (1)$$

$$a=4k+1 \quad (2)$$

$$a=4k+2 \quad (3)$$

$$a=4k+3 \quad (4)$$

(چهار مجموعه $A_1=\{a \in \mathbb{Z} | a=4k\}$ و $A_2=\{a \in \mathbb{Z} | a=4k+1\}$ و $A_3=\{a \in \mathbb{Z} | a=4k+2\}$ و $A_4=\{a \in \mathbb{Z} | a=4k+3\}$ را افراز می کنند.)

حالت های ... و ... زوج بوده و لذا $a=4k+1$ یا $a=4k+3$

$$\text{اگر } a=4k+1 \Rightarrow a^2=16k^2+8k+1=8(\underbrace{2k^2+k}_{k'})+1=8k'+1$$

$$\text{اگر } a=4k+3 \Rightarrow a^2=16k^2+24k+9=16k^2+24k+8+1$$

$$\Rightarrow a^2=8(\underbrace{2k^2+3k+1}_t)+1=8t+1$$

تمرین

۱ فرض می کنیم $ab=cd$ (a, b, c, d اعداد صحیح و ناصفرند) در این صورت پنج رابطه عاد کردن از این تساوی نتیجه بگیرد.

۲ ثابت کنید: اگر $a|b$ آنگاه $a|-b$ و $-a|b$ و $-a|-b$.

۳ اگر $a > 1$ و $a|9k+4$ و $a|5k+3$ ، ثابت کنید a عددی اول است.

۴ اگر عددی مانند k در \mathbb{Z} باشد به طوری که $5|4k+1$ ، ثابت کنید: $25|16k^2+28k+6$

۵ آیا از اینکه $a|b$ و $c|d$ ، همواره می توان نتیجه گرفت که $a+c|b+d$ ؟

۶ ثابت کنید: الف) هر دو عدد صحیح و متوالی نسبت به هم اول اند. ب) هر دو عدد صحیح و فرد متوالی نسبت به هم اول اند.

راهنمایی: فرض کنید $(m, m+1)=d$ و ثابت کنید $d|1$ و نتیجه بگیرید $d=1$.

۷ اگر $p \neq q$ و هر دو عدد اول باشند ثابت کنید $(p, q)=1$.

۸ اگر $m, n \in \mathbb{N}$ و $a, b \in \mathbb{Z}$ ثابت کنید:

$$m \leq n, a|b \Rightarrow a^m|b^n$$

۹ اگر باقی مانده تقسیم عدد a بر دو عدد ۷ و ۸ به ترتیب ۵ و ۷ باشد، باقی مانده تقسیم عدد a بر ۵۶ بیاید.

۱۰ اگر a عددی صحیح و فرد باشد و $2|a+b$ در این صورت باقی مانده تقسیم عدد (a^2+b^2+3) بر ۸ را بیاید.

۱۱ اگر n عددی صحیح باشد ثابت کنید $3|n^2-n$

راهنمایی: برای n سه حالت $n=3k$ و $n=3k+1$ و $n=3k+2$ در نظر بگیرید و در هر حالت ثابت کنید $3|n^2-n$.

۱۲ اگر در یک تقسیم، مقسوم و مقسوم‌علیه، هر دو بر عدد صحیح n بخش پذیر باشند، ثابت کنید باقی مانده تقسیم نیز همواره بر n بخش پذیر است.

۱۳ اگر a عددی صحیح و دلخواه باشد ثابت کنید همواره یکی از اعداد صحیح a یا $a+2$ یا $a+4$ بر ۳ بخش پذیر است.

۱۴ ثابت کنید تفاضل مکعب‌های دو عدد صحیح متوالی عددی فرد است.

۱۵ ثابت کنید حاصل ضرب سه عدد صحیح متوالی همواره بر $3!$ بخش پذیر است.

۱۶ حاصل هر یک را به دست آورید: $(m \in \mathbb{Z})$

الف) $([m^2, m], m^5)$

ب) $(2m, 6m^2)$

پ) $(3m+1, 3m+2)$

ت) $[m^4, (m^2, m^3)]$

ث) $[(72, 48), 120]$

فعالیت

در درس قبل دیدیم که باقی‌مانده‌های تقسیم اعداد بر ۴ عبارت‌اند از ۰، ۱، ۲ و ۳. حال اگر هر کدام از این باقی‌مانده‌ها را نمایندهٔ یک مجموعه از اعداد در نظر بگیریم که باقی‌ماندهٔ تقسیم هر عضو آن مجموعه بر عدد ۴، به ترتیب ۰، ۱، ۲ و ۳ باشد، داریم:

(مجموعهٔ اعدادی را که باقی‌ماندهٔ تقسیم آنها بر عدد m ، مساوی با عدد r باشد با نماد $[r]_m$ نشان می‌دهیم)

$$A_0 = \{x \in \mathbb{Z} \mid x = 4k\} = \{\dots, -8, -4, 0, 4, 8, \dots, 16, \dots\} = [0]_4$$

$$A_1 = \{x \in \mathbb{Z} \mid x = 4k + 1\} = \{\dots, -7, -3, 1, 5, \dots, 13, \dots, 21, \dots\} = [1]_4$$

$$A_2 = \{x \in \mathbb{Z} \mid x = 4k + 2\} = \{\dots, -6, \dots, 2, 6, 10, \dots\} = [2]_4$$

$$A_3 = \{x \in \mathbb{Z} \mid x = 4k + 3\} = \{\dots, -13, \dots, -5, -1, 3, 7, 11, \dots\} = [3]_4$$

- ۱ دو عضو دلخواه از مجموعهٔ A را در نظر بگیرید. آیا تفاضل این دو عدد مضرب ۴ است؟
- ۲ از مجموعهٔ A_1 دو عضو دلخواه را در نظر بگیرید و تفاضل آنها را حساب کنید. آیا عدد حاصل مضرب ۴ است؟
- ۳ نتیجه‌ای را که از ۱ و ۲ گرفتید در حالت کلی برای هر دو عضو دلخواه از A_1 اثبات کنید.

$$a, b \in A_1 \Rightarrow \begin{cases} a = 4k_1 + 1 \\ b = \dots \end{cases} \Rightarrow a - b = (\dots) - (4k_1 + 1)$$

$$\Rightarrow a - b = 4 \underbrace{(k_1 - k_2)}_{k_3} \Rightarrow 4 \mid \dots$$

- ۴ آیا درست است که بگویم اعضای مجموعهٔ A_2 همگی بر عدد ۴، باقی‌ماندهٔ یکسان دارند؟ در مورد مجموعهٔ A_3 چه می‌توان گفت؟

می‌دانیم مجموعه‌های A_0, A_1, A_2, A_3 یک‌افراز برای مجموعهٔ \mathbb{Z} هستند و بنابراین هر دو عدد صحیح، مانند a و b ، یا هر دو به یکی از این چهار مجموعه تعلق دارند و یا هر کدام در یک مجموعه

واقع اند (A_1, A_2, A_3, A_4 اشتراکی با هم ندارند. چرا؟) و لذا اگر a و b هر دو در یک مجموعه از این چهار مجموعه باشند (باقی مانده تقسیم a بر b مساوی باشد یا اصطلاحاً a بر b ۴ هم باقی مانده باشند) همواره $a - b$ بر ۴ و اگر این طور نباشد $4 \nmid a - b$.

تعریف: برای هر عدد طبیعی مانند m و هر دو عدد صحیح مانند a و b ، اگر $m \mid a - b$ ، می‌گوییم « a هم‌نهشت با b است به‌سنج یا پیمانه m »؛ و می‌نویسیم $a \equiv b \pmod{m}$. تعریف رابطه هم‌نهشتی به پیمانه m ، به زبان ریاضی عبارت است از:

$$\forall a, b \in \mathbb{Z}, a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \quad (m \in \mathbb{N})$$

مثال:
$$\begin{cases} 12 \equiv 2 \pmod{5}, -11 \equiv 1 \pmod{6} \\ -295 \equiv -5 \pmod{10}, 23 \equiv -7 \pmod{3} \end{cases}$$

قرارداد: مجموعه همه اعداد صحیح که باقی مانده تقسیم آنها بر عدد طبیعی m برابر با r می‌باشد، یعنی $A_r = \{x \in \mathbb{Z} \mid x = mk + r\}$ را کلاس یا دسته هم‌نهشتی r به پیمانه m می‌نامیم و با نماد $[r]_m$ نمایش می‌دهیم. برای استفاده از رابطه هم‌نهشتی، ابتدا خواص و ویژگی‌های این رابطه را بررسی می‌کنیم که با توجه به تعریف این رابطه و خواص رابطه عادی کردن، ویژگی‌های رابطه هم‌نهشتی به راحتی اثبات می‌شوند. شما در کامل کردن اثبات‌ها شرکت کنید.

$$a \equiv b \pmod{m} \Rightarrow \begin{cases} a + c \equiv b + c \pmod{m} \\ a - c \equiv b - c \pmod{m} \end{cases}$$

ویژگی ۱: به دو طرف یک رابطه هم‌نهشتی می‌توان عددی صحیح را اضافه یا از آن کم کرد.

اثبات:
$$a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid a + c - b - c$$

$$\Rightarrow m \mid (a + c) - (\dots + \dots) \Rightarrow (\dots + \dots) \equiv (b + c) \pmod{m}$$

مثال: با توجه به فعالیت قبل فرض کنیم، $7 \equiv -1 \pmod{4}$ یا $(-1, 7) \in A_1$ در این صورت اگر ۵ واحد به دو طرف این هم‌نهشتی اضافه کنیم فاصله این دو عدد یا تفاضل آنها همچنان حفظ شده و همان ۸ که مضرب ۴ است باقی می‌ماند. به عبارت دیگر، اعداد حاصل یعنی $7 + 5 = 12$ و $-1 + 5 = 4$ نیز در A_1 قرار خواهند گرفت.

$$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$$

ویژگی ۲: دو طرف یک رابطه هم‌نهشتی را می‌توان در عددی صحیح ضرب کرد.

اثبات:
$$a \equiv b \pmod{m} \Rightarrow m \mid \dots - \dots \Rightarrow m \mid \dots \times (a - b) \Rightarrow m \mid ac - \dots$$

$$\Rightarrow \dots \equiv bc \pmod{m}$$

تذکر: عکس ویژگی ۲ برقرار نیست، یعنی اگر $ac \equiv b^m$ ، لزوماً نمی‌توان نتیجه گرفت که $a \equiv b^m$ (قانون حذف برای رابطه هم‌نهستی در حالت کلی برقرار نیست) برای این مطلب یک مثال نقض بزنید.

$$a \equiv b \Rightarrow a^n \equiv b^n$$

ویژگی ۳: (دو طرف یک رابطه هم‌نهستی را می‌توان به توان n رساند.) ($n \in \mathbb{N}$)

مثال: $(5 \equiv 2 \Rightarrow 5^3 \equiv 2^3)$

اثبات: (از اتحاد $(a^n - b^n) = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ استفاده می‌کنیم)

$$a \equiv b \Rightarrow m | a - b \Rightarrow m | (a-b) \underbrace{(a^{n-1} + a^{n-2}b + \dots + b^{n-1})}_c \quad (\equiv \Rightarrow \equiv)$$

$$\Rightarrow m | a^n - b^n \Rightarrow \dots \equiv \dots$$

تذکر: می‌دانیم $5^2 \equiv 3^2$ ولی $5 \not\equiv 3$ بنابراین نتیجه می‌گیریم که ...

$$a \equiv b, c \equiv d \Rightarrow \begin{cases} ac \equiv bd & (1) \\ a+c \equiv b+d & (2) \\ a-c \equiv b-d & (3) \end{cases}$$

ویژگی ۴: دو طرف دو رابطه هم‌نهستی را که پیمانه‌های یکسان داشته باشند می‌توان با هم جمع یا از هم منها و یا

در هم ضرب کرد.

$$(15 \equiv 10, 7 \equiv 2 \Rightarrow 15 \times 7 \equiv 10 \times 2 \text{ و } 15 \times 2 \equiv 10 \times 7)$$

$$\text{و } 15 + 7 \equiv 10 + 2 \Rightarrow 22 \equiv 12$$

اثبات ①:

$$\left. \begin{array}{l} a \equiv b \Rightarrow m | \dots \xrightarrow{\times c} \dots \Rightarrow m | ac - bc \\ c \equiv d \Rightarrow m | \dots \xrightarrow{\times b} \dots \Rightarrow m | bc - \dots \end{array} \right\} + \Rightarrow m | (ac - bc) + (\dots - bd)$$

$$\Rightarrow m | ac - \dots \Rightarrow \dots \equiv bd$$

اثبات ② به عهده شما

تذکر مهم: اگر باقی‌مانده تقسیم a بر m مساوی با r باشد در این صورت $a \equiv r^m$

$$a = mq + r \Rightarrow a \equiv r^m$$

$$(179 = 11 \times 16 + 3 \Rightarrow 179 \equiv 3^{11})$$

اثبات :

$$a = mq + r \Rightarrow a - r = mq \Rightarrow m \mid a - r \Rightarrow \dots \equiv \dots$$

نتیجه ۱ : هرگاه بخواهیم کوچک ترین عدد نامنفی و هم نهشت با عدد a به پیمانۀ m را مشخص کنیم، کافی است عدد a را بر m تقسیم کرده و باقی مانده را به دست آوریم.

مثال: $296 \equiv ? \pmod{11} \rightarrow \dots$

نتیجه ۲ : اگر دو عدد a و b تقسیم بر عدد طبیعی m ، هم باقی مانده باشند در این صورت $a \equiv b \pmod{m}$.
مثال : باقی مانده تقسیم عدد $A = (27)^7 + 19$ را بر ۱۳ بیابید.

$$27 = 13 \times 2 + 1 \Rightarrow 27 \equiv 1 \pmod{13} \Rightarrow (27)^7 \equiv 1^7 \pmod{13} = 1 \quad \text{و} \quad 19 = 13 \times 1 + 6$$

$$\Rightarrow \underbrace{19}_{\equiv 6 \pmod{13}} \xrightarrow{\text{با توجه به ① و ②}} (27)^7 + 19 \equiv 1 + 6 \pmod{13} \xrightarrow{\text{با توجه به ①}} A \equiv 7 \pmod{13} \Rightarrow r = 7$$

پس باقی مانده A بر ۱۳، برابر با ۷ می باشد.

مثال : باقی مانده تقسیم عدد $A = (1000)^{13} \times 12 + 10$ را بر ۷ بیابید.

$$1000 = 7 \times 142 + 6 \Rightarrow 1000 \equiv 6 \pmod{7} \quad \text{و} \quad 6 \equiv -1 \pmod{7} \Rightarrow 1000 \equiv -1 \pmod{7}$$

$$\Rightarrow (1000)^{13} \equiv (-1)^{13} = -1 \pmod{7}$$

$$\Rightarrow (1000)^{13} \times 12 \equiv (-1) \times 12 = -12 \pmod{7}$$

$$\Rightarrow (1000)^{13} \times 12 + 10 \equiv (-12) + 10 = -2 \pmod{7} \quad \text{و} \quad -2 \equiv 5 \pmod{7}$$

$$\Rightarrow (1000)^{13} \times 12 + 10 \equiv 5 \pmod{7} \Rightarrow r = 5$$

$$a \equiv b \pmod{m} \Rightarrow \begin{cases} a + mt \equiv b + mk \\ a - mt \equiv b - mk \end{cases}$$

ویژگی ۵ : می توان به دو طرف یا یک طرف یک رابطه هم نهشتی هر مضربی از پیمانۀ را اضافه یا از آن کم کرد.

$$\begin{array}{l} \text{طبق فرض: } a \equiv b \pmod{m} \\ \text{می دانیم: } mt \equiv mk \pmod{m} \\ \hline \Rightarrow a \pm mt \equiv b \pm mk \pmod{m} \end{array}$$

مثال : می دانیم $7 \equiv 2 \pmod{5}$ اگر به سمت چپ رابطه $3 \times 5 = 15$ و به سمت راست آن $5 \times 5 = 25$ واحد اضافه کنیم خواهیم داشت $7 + 15 \equiv 2 + 25 \pmod{5}$ یا $22 \equiv 27 \pmod{5}$ که این رابطه برقرار است.

$$ac \equiv bc, (c, m) = d \Rightarrow a \equiv b \pmod{\frac{m}{d}}$$

ویژگی ۶: اگر بخواهیم دو طرف یک رابطه هم‌نهشتی را بر عددی تقسیم کنیم، باید پیمانه آن هم‌نهشتی را بر م‌م آن عدد و پیمانه تقسیم کنیم. (این ویژگی را بدون اثبات می‌پذیریم)

نتیجه مهم: اگر $ac \equiv bc$ و $(c, m) = 1$ در این صورت $a \equiv b \pmod{m}$ در واقع قاعده حذف در هم‌نهشتی‌ها، برای هر عدد که نسبت به پیمانه اول باشد، برقرار است.

مثال: واضح است که $4 \times 6 \equiv 4 \times 3$ و چون $(4, 3) = 1$ پس $6 \equiv 3$.

فعالیت

همان‌طور که در دوره ابتدایی آموختید عددنویسی در مبنای 10 انجام می‌شود؛ که در آن ارزش مکانی ارقام، ده تا ده تا در نظر گرفته می‌شود (ده تا یکی می‌شود ده تا و ده تا ده تا یکی می‌شود صد تا و ده تا صد تا یکی می‌شود هزار تا و ...). بنابراین به راحتی می‌توانیم هر عدد را در مبنای ده بسط بدهیم. به عنوان مثال عدد 1397 را می‌توان به صورت زیر بسط داد:

$$1397 = 1 \times 1000 + 3 \times 100 + 9 \times 10 + 7$$

$$\Rightarrow 1397 = 1 \times 10^3 + 3 \times 10^2 + 9 \times 10 + 7$$

۱ هر یک از دو عدد زیر را در مبنای ده بسط بدهید:

$$1388109 = 1 \times 10^6 + \dots$$

$$13571122 =$$

۲ باقی‌مانده تقسیم عدد $A = 1358112$ را بر عدد 9 بیابید.

می‌دانیم $10 \equiv 1$ و بنابر ویژگی‌های رابطه هم‌نهشتی $10^n \equiv 1$ بنابراین:

$$A = 1 \times 10^6 + 3 \times 10^5 + \dots + \dots + \dots + 1 \times 10 + 2$$

$$10^6 \equiv 1 \Rightarrow 1 \times 10^6 \equiv 1$$

$$10^5 \equiv 1 \Rightarrow 3 \times 10^5 \equiv 3$$

$$10^4 \equiv 1 \Rightarrow \dots \equiv \dots$$

$$10^3 \equiv 1 \Rightarrow \dots \times 10^3 \equiv \dots$$

$$10^2 \equiv 1 \Rightarrow 1 \times 10^2 \equiv \dots$$

$$10 \equiv 1 \Rightarrow 1 \times 10 \equiv \dots$$

$$\begin{array}{r} 2 \equiv 2 \\ \hline A \equiv 1 + 3 + 5 + 8 + 1 + 1 + 2 \end{array}$$

با جمع طرفین هم‌نهشتی‌ها داریم:

اگر دقت کنید سمت راست هم نهشتیِ اخیر مجموع ارقام A است. بنابراین می‌توان گفت «باقی‌مانده تقسیم هر عدد بر ۹ برابر است با باقی‌مانده تقسیم مجموع ارقام آن عدد بر ۹»

عدد n رقمی $A = \overline{a_{n-1} a_{n-2} a_{n-3} \dots a_2 a_1 a_0}$ را بسط دهید و در هم‌نهشتی به پیمانه ۹ به جای هر توان 10^k عدد ۱ را قرار دهید، سپس همین نتیجه‌گیری را در حالت کلی بررسی کنید.

$$\begin{aligned} A &= 10^{n-1} \times a_{n-1} + \dots + \dots + \dots + 10^2 a_2 + 10^1 a_1 + 10^0 a_0 \\ &\Rightarrow A \equiv 1 \times a_{n-1} + \dots + \dots + 1 \times a_1 + a_0 \\ &\Rightarrow A \equiv \dots \end{aligned}$$

کار در کلاس

۱ با توجه به اینکه $10^3 \equiv 1$ ، نتیجه می‌گیریم، $\forall k \in \mathbb{N}, 10^k \equiv 1$ ، بنابراین، مشابه فعالیت قبل، باقی‌مانده تقسیم عدد $A = 5983248$ را بر ۳ بیابید و سپس یک قاعده کلی برای یافتن باقی‌مانده تقسیم و بخش‌پذیری اعداد n رقمی بر ۳ بیان کنید.

۲ می‌دانیم که $10^{11} \equiv -1$ ؛ بنابراین برای هر n زوج، $10^n \equiv 1$ و برای هر n فرد، $10^n \equiv -1$. حال اگر در هم‌نهشتی به پیمانه ۱۱ و در بسط عدد $A = 4985327$ به جای توان‌های زوج عدد 10^k ، عدد یک و به جای توان‌های فرد عدد 10^k ، عدد (-1) قرار دهیم باقی‌مانده تقسیم عدد A را بر ۱۱ بیابید.

$$\begin{aligned} A &= 4 \times 10^6 + 9 \times 10^5 + 8 \times 10^4 + \dots + 2 \times 10 + 7 \\ &\Rightarrow A \equiv 4 \times \dots + \dots \times (-1) + \dots \times 1 + \dots + 2 \times (-1) + 7 \\ &\Rightarrow A \equiv 7 - 2 + 3 - 5 + 8 - 9 + 4 = 6 \Rightarrow r = \dots \end{aligned}$$

۳ می‌دانیم $10^2 \equiv 0$ و $10^5 \equiv 0$ و $10^8 \equiv 0$ در این صورت:

$$\forall k \in \mathbb{N}; 10^k \equiv \dots \text{ و } 10^k \equiv \dots \text{ و } 10^k \equiv 0$$

بنابراین اگر در بسط هر عدد n رقمی مانند $A = \overline{a_{n-1} a_{n-2} \dots a_2 a_1 a_0}$ به جای توان‌های عدد 10^k (در هم‌نهشتی‌های به پیمانه ۲ و ۵ و 10^8) صفر قرار دهیم خواهیم داشت:

$$\begin{aligned} A &= 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\Rightarrow A \equiv 0 \times a_{n-1} + \dots + \dots + \dots \times a_2 + \dots + a_0 \\ &\Rightarrow A \equiv \dots \text{ و } A \equiv \dots \text{ و } A \equiv a_0 \end{aligned}$$

نتیجه حاصل را برای یافتن باقی‌مانده تقسیم اعداد n رقمی بر ۲ و ۵ و 10^8 و شرط بخش‌پذیری بر این اعداد را بیان کنید.

یکی از کاربردهای هم‌نهستی در تقویم‌نگاری و محاسبه روزهای هفته برحسب تاریخ داده شده، مشخص شده است. به‌عنوان مثال: اگر اول مهر ماه در یک سال یکشنبه باشد، ۲۲ بهمن در همان سال چه روزی از هفته خواهد بود؟ برای پاسخ دادن به سؤالاتی شبیه این سؤال فعالیت زیر را انجام دهید.

فعالیت

می‌دانیم هر روز از روزهای هفته، مثلاً شنبه، پس از گذشت ۷ روز دوباره تکرار می‌شود. به‌عنوان مثال اگر ۱۲ فروردین در یک سال یکشنبه باشد در این صورت $19 = 12 + 7$ فروردین و $26 = 19 + 7$ فروردین نیز یکشنبه می‌باشد. در بحث تقویم و روزهای هفته دقت دارید که شش ماه اول سال همگی ۳۱ روزه و شش ماه دوم سال غیر از اسفند (که، به‌جز سال کبیسه، ۲۹ روزه است) همگی ۳۰ روزه می‌باشند.

حال فرض کنید در یک سال ۹ دی ماه یکشنبه باشد، در همان سال ۲۸ دی ماه چند شنبه است؟ با توجه به مطالب مذکور ۱۶ دی و ۲۳ دی یکشنبه بوده و کافی است از ۲۳ دی تا ۲۸ دی ۵ روز بعد را حساب کنیم که به روز ۰۰۰ می‌رسیم.

حال اگر فاصله ۹ دی تا ۲۸ دی را حساب کنیم ($19 = 9 - 28$) مشاهده می‌شود که ۱۹ روز فاصله داریم و چون $19 \equiv 5^7$

ی	د	س	چ	پ	ج	ش
۰	۱	۲	۳	۴	۵	۶

لذا کافی است یکشنبه را مطابق جدول مقابل مبدأ فرض کرده و مشخص کنیم که ۵ روز بعد چه روزی از هفته است یا عدد ۵ متناظر با کدام روز است.

۱ اگر در یک سال، اول مهر شنبه باشد در این صورت ۱۲ بهمن در همان سال چه روزی است؟

ش	ی	د	س	چ	پ	ج
۰	۱	۲	۳	۴	۵	۶

۲۹ روز در مهر ماه و سه ماه آبان، آذر و دی و ۱۲ روز تا ۱۲ بهمن، فاصله ۱ مهر است تا ۱۲ بهمن؛ یعنی $d = 29 + 3 \times 30 + 12 = 131$

از طرفی $131 \equiv 000^7$ و با توجه به جدول فوق روز متناظر با عدد ... پنجشنبه است، یعنی ۱۲ بهمن در آن سال پنجشنبه است.

۲ از روی تقویم سال جاری روز هفته را برای هفتم تیر مشخص کنید و با توجه به آن و به روش فوق مشخص کنید که ۲۲ بهمن در سال جاری چه روزی از هفته خواهد بود. درستی پاسخ خود را از روی تقویم نیز بررسی کنید.

معادله هم‌نهستی

تعریف: یک رابطه هم‌نهستی همراه با مجهولی چون x به فرم $ax \equiv b^m$ را یک معادله هم‌نهستی می‌نامیم؛ و منظور از حل معادله هم‌نهستی پیدا کردن همه جواب‌هایی چون $x \in \mathbb{Z}$ است که در این معادله صدق کنند، یعنی $ax \equiv b^m$. ($a, b \in \mathbb{Z}$)

۱- ۹ دی ماه روز بصیرت نام‌گذاری شده است.

به عنوان مثال، معادله $x \equiv 2 \pmod{3}$ را در نظر بگیرید. در این معادله x می تواند ۲ یا ۵ باشد. عدد بعدی که می تواند به جای x قرار بگیرد و در معادله صدق کند عدد ۸ است و اگر بخواهیم تمام جواب های این معادله یا جواب های عمومی آن را داشته باشیم کافی است از تعریف هم نهستی استفاده کنیم،

$$x \equiv 2 \pmod{3} \Rightarrow 3 \mid x - 2 \Rightarrow (x - 2) = 3k \Rightarrow x = 3k + 2$$

که اگر k را به ترتیب صفر و ۱ و ۲ قرار بدهیم همان جواب های $x_0 = 2$ و $x_1 = 5$ و $x_2 = 8$ را به دست می آوریم و برای هر $k \in \mathbb{Z}$ ، جوابی برای معادله به دست می آید. در معادله فوق ضریب x عدد یک است و اگر ضریب x عددی غیر از یک باشد برای دست یابی به جواب های عمومی معادله باید ضریب x را حذف کنیم که ویژگی های ۵ و ۶ و نتیجه ویژگی ۶ به ما کمک می کنند.

مثال: جواب های عمومی معادله $4x \equiv 17 \pmod{5}$ را به دست آورید.

$$4x \equiv 17, 17 \equiv 2 \pmod{5} \Rightarrow 4x \equiv 2 \pmod{5}$$

$$\begin{array}{l} \text{ویژگی ۵} \\ \Rightarrow 4x \equiv 2 + (2 \times 5) \end{array}$$

$$\Rightarrow 4x \equiv 12 \pmod{5} \Rightarrow \cancel{4}x \equiv \cancel{4} \times 3 \pmod{5}$$

$$\Rightarrow x \equiv 3 \pmod{5} \Rightarrow x = 5k + 3$$

$$(5 \mid x - 3) \Rightarrow x - 3 = 5k \Rightarrow x = 5k + 3$$

مثال: همه اعداد صحیحی را بیابید که سه برابر آنها منهای ۱۳ بر ۷ بخش پذیر باشند.

حل: اگر آن عدد را x فرض کنیم باید $7 \mid 3x - 13$ یا $3x \equiv 13 \pmod{7}$

$$3x \equiv 13 \pmod{7} \Rightarrow 3x \equiv 13 - 7 = 6 \pmod{7}$$

$$\begin{array}{l} (3, 7) = 1 \\ \Rightarrow \cancel{3}x \equiv \cancel{3} \times 2 \pmod{7} \Rightarrow x = 7k + 2 \end{array}$$

قضیه: معادله هم نهستی $ax \equiv b \pmod{m}$ دارای جواب است اگر و فقط اگر $(a, m) \mid b$. این قضیه را بدون اثبات می پذیریم.

نتیجه: اگر $(a, m) = 1$ چون برای هر b ، همواره $b \mid b$ پس معادله $ax \equiv b \pmod{m}$ همواره دارای جواب است.

مثال: معادله $6x \equiv 11 \pmod{9}$ دارای جواب نیست زیرا، $3 = (6, 9) \nmid 11$ و $3 \nmid 11$ و معادله $4x \equiv 18 \pmod{6}$ دارای جواب است. چرا؟

این معادله را حل کنید:

$$4x \equiv 18 \pmod{6} \Rightarrow 2 \times 2x \equiv 2 \times 9, (2, 6) = 2$$

$$\begin{array}{l} \text{ویژگی ۶} \\ \Rightarrow 2x \equiv 9 \pmod{6} \end{array}$$

$$\Rightarrow 2x \equiv 9 \pmod{6}$$

$$\Rightarrow 2x \equiv 9 + 3 = 12 \pmod{6}$$

$$\Rightarrow \cancel{2}x \equiv \cancel{2} \times 6 \pmod{6} \Rightarrow x = 3k + 6$$

حل معادلات سیاله و کاربردهای آن

فعالیت

۱ آیا می‌توانید یک کیسه ۱۹ کیلویی را با وزنه‌های ۳ و ۴ کیلویی وزن کنید؟ (می‌توانید از یکی از دو وزنه یا هر دو باهم استفاده کنید و از هر وزنه به تعداد کافی در اختیار داریم)
یک جواب مسئله استفاده از ۴ وزنه ۴ کیلویی و یک وزنه ۳ کیلویی است.

$$4 \times \dots + 1 \times 3 = \dots$$

آیا برای این مسئله می‌توانید یک جواب دیگر بیابید؟

$$1 \times \dots + \dots \times 5 = 19$$

در واقع شما به دنبال جواب‌های حسابی (صحیح و نامنفی) برای معادله $4x + 3y = 19$ هستید.

(x تعداد وزنه‌های ۴ کیلویی به کار رفته و y تعداد وزنه‌های ۳ کیلویی به کار رفته است)

۲ اگر در قسمت قبل بخواهیم فقط از وزنه‌های ۲ و ۴ کیلویی استفاده کنیم آیا عمل توزین امکان‌پذیر است؟

باید جواب‌هایی چون $y \in W$ و x بیابیم که $\dots \times x + \dots \times y = \dots$ چون مجموع دو عدد زوج همواره ... است پس چنین x و y ای در W وجود ندارد.

تعریف: هرگاه بخواهیم جواب‌های معادله $ax + by = c$ یعنی x و y را در اعداد صحیح بیابیم و $c \in \mathbb{Z}$ و b و a در این صورت معادله مذکور ($ax + by = c$) را یک معادله سیاله درجه اول یا خطی می‌نامیم.

تبدیل یک معادله سیاله به معادله هم‌نهستی

معادله سیاله $ax + by = c$ دارای دو مجهول است و به دو صورت می‌تواند به یک معادله هم‌نهستی (با مجهول x یا y) تبدیل

شود:

$$ax + by = c \Rightarrow ax - c = (-b)y \Rightarrow -b|ax - c \Rightarrow b|ax - c$$

$$\Rightarrow ax \equiv c \pmod{b} \quad (b > 0) \quad \text{یا} \quad ax \equiv c \pmod{-b} \quad (b < 0) \quad \text{یا} \quad ax \equiv c \pmod{|b|}$$

$$by \equiv c \pmod{-a} \quad \text{و} \quad by \equiv c \pmod{a}$$

و به طریق مشابه می‌توان نوشت:

تذکر: با توجه به قضیه قبل نتیجه می‌گیریم که «شرط لازم و کافی برای آنکه معادله سیاله $ax + by = c$ دارای جواب

باشد آن است که، $c \in (a, b)$

۱ با تبدیل معادله سیاله $4x + 5y = 9$ به معادله هم‌نهشتی و حل آن، جواب‌های عمومی این معادله سیاله را بیابید.

$$\begin{aligned} 4x + 5y = 9 &\Rightarrow 4x \equiv \dots \\ &\Rightarrow 4x \equiv 9 - \dots \Rightarrow 4x \equiv 4 \\ &\Rightarrow x \equiv \dots \Rightarrow x = 5k + \dots \\ &\Rightarrow 4(5k + 1) + 5y = 9 \\ &\Rightarrow 20k + 4 + 5y = 9 \\ &\Rightarrow 20k + 5y = 5 \\ &\Rightarrow 4k + y = 1 \Rightarrow y = \dots k + 1 \end{aligned}$$

۲ در قسمت ۱ فعالیت قبل مشخص کنید به چند طریق می‌توان عمل وزن کردن را انجام داد.

کافی است جواب‌های عمومی معادله $4x + 3y = 19$ را (برحسب k) بیابیم و به‌ازای هر $k \in \mathbb{Z}$ که x و y منفی نباشند تعداد حالت‌ها را شمارش کنیم:

$$\begin{aligned} 4x + 3y = 19 &\Rightarrow 4x \equiv \dots \\ &\Rightarrow 4x \equiv 1 \Rightarrow 4x \equiv 1 + \dots \\ &\Rightarrow x \equiv \dots \times 1 \Rightarrow x = 3k + 1 \\ &\Rightarrow 4(3k + 1) + 3y = 19 \\ &\Rightarrow 12k + 4 + 3y = 19 \\ &\Rightarrow 12k + 3y = \dots \Rightarrow \dots + y = 5 \\ &\Rightarrow y = -4k + 5 \end{aligned}$$

$$k = 0 \Rightarrow \begin{cases} x = 1 \\ y = 5 \end{cases} \text{ و } k = \dots \Rightarrow \begin{cases} x = 4 \\ y = 1 \end{cases}$$

به‌ازای $k=2$ و بیشتر از آن $y < 0$ و به‌ازای $k=-1$ و کمتر از آن $x < 0$ که قابل قبول نمی‌باشند و لذا به دو صورت فوق می‌توان این کیسه ۱۹ کیلویی را وزن کرد.

مثال: به چند طریق می‌توان ۱۸۰۰۰ تومان را به اسکناس‌های ۲۰۰۰ و ۵۰۰۰ تومانی تبدیل کرد؟

حل: اگر x و y را به ترتیب تعداد اسکناس‌های ۲۰۰۰ و ۵۰۰۰ تومانی فرض کنیم حل این مثال معادل است با تعداد

$$2000x + 5000y = 18000$$

$$2000x + 5000y = 18000$$

$$\Rightarrow 2x + 5y = \dots$$

$$\Rightarrow 2x \equiv 18 \text{ و } 18 \equiv \dots$$

$$\Rightarrow x \equiv 9 \times 4$$

$$\Rightarrow x \equiv \dots \Rightarrow x = 5k + 4$$

$$\Rightarrow 2(5k + 4) + 5y = 18$$

$$\Rightarrow 10k + 8 + 5y = 18$$

$$\Rightarrow 10k + 5y = 10 \Rightarrow y = -2k + 2$$

$$k = 0 \Rightarrow \begin{cases} x = 4 \\ y = 2 \end{cases} \text{ و } k = 1 \Rightarrow \begin{cases} x = 9 \\ y = 0 \end{cases} \quad (\text{فقط به ازای } 1 \text{ و } 0 \text{ برای } x \text{ و } y \text{ جواب‌ها نامنفی هستند})$$

پس به دو طریق امکان تبدیل کردن ۱۸۰۰۰ تومان به اسکناس‌های ۲۰۰۰ و ۵۰۰۰ تومانی، وجود دارد.

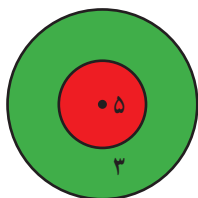
مثال: در یک رستوران فقط دو نوع خورش قورمه‌سبزی و قیمه وجود دارد. اگر ۵ نفر وارد این رستوران شوند به چند طریق می‌توانند سفارش غذا بدهند؟ (هر نفر فقط یک پرس غذا میل می‌کند)

حل: اگر تعداد چلو خورش قورمه‌سبزی و چلو خورش قیمه سفارش داده شده را به ترتیب با x و y نشان دهیم خواهیم داشت:

$$x + y = 5 \Rightarrow x \equiv 5 \Rightarrow x = k + \dots$$

$$\Rightarrow k + \cancel{x} + y = \cancel{x} \Rightarrow y = \dots$$

چون x و y اعدادی نامنفی هستند پس باید $k \in \{0, -1, -2, -3, -4, -5\}$ و لذا به ۶ طریق می‌توانند سفارش غذا بدهند.



مثال: تیراندازی به سمت یک هدف، شامل دو دایره هم مرکز، تیراندازی می‌کند. اگر او تیر را به دایره با شعاع کوچک تر بزند ۵ امتیاز و اگر به دایره بزرگ تر و خارج دایره کوچک تر بزند ۳ امتیاز می‌گیرد. اگر او کمتر از ۱۵ تیر انداخته و همه تیرها به داخل دایره بزرگ تر اصابت کرده باشد و در پایان ۴۲ امتیاز گرفته باشد چند حالت برای او در این تیراندازی می‌تواند ثبت شود؟

حل: اگر x و y را به ترتیب تعداد اصابت‌ها به دایره کوچک تر و بزرگ تر فرض کنیم، داریم:

$$5x + 3y = 42 \Rightarrow 5x \equiv 42$$

$$\Rightarrow 5x \equiv 42 + 3 \Rightarrow x \equiv 9 \times 9$$

$$\Rightarrow x = 3k + 9$$

$$5(3k + 9) + 3y = 42$$

$$\Rightarrow 15k + 45 + 3y = 42$$

$$\Rightarrow 15k + 3y = -3 \Rightarrow y = -5k - 1$$

$$x, y \in W \Rightarrow k \in \{-1, -2, -3\} \Rightarrow \begin{cases} x=6 \\ y=4 \end{cases}, \begin{cases} x=3 \\ y=9 \end{cases}, \begin{cases} x=0 \\ y=14 \end{cases}$$

($x=6$ و $y=4$ یعنی تیرانداز ۶ تیر را به دایره کوچک‌تر و ۴ تیر را به دایره بزرگ‌تر زده است).

تمرین

۱ عدد ۱۳۹۸ به کدام دسته هم‌نهستی به پیمانه ۹ تعلق دارد؟

۲ اگر $k \in \mathbb{Z}$ ، ثابت کنید فقط یکی از سه حالت زیر امکان‌پذیر است

$$k \equiv 0 \pmod{3} \text{ یا } k \equiv 1 \pmod{3} \text{ یا } k \equiv 2 \pmod{3}$$

(به عبارت دیگر، $k \in [0]_3$ یا $k \in [1]_3$ یا $k \in [2]_3$)

۳ اگر $a \equiv b \pmod{m}$ و $n | m$ ثابت کنید $a \equiv b \pmod{n}$.

۴ فرض کنیم، $a \equiv b \pmod{m}$ و $b \equiv c \pmod{n}$ و $(m, n) = d$ در این صورت ثابت کنید $a \equiv c \pmod{d}$.

۵ ثابت کنید: اگر باقی‌مانده‌های تقسیم دو عدد a و b بر m مساوی باشند آن‌گاه $a \equiv b \pmod{m}$.

۶ عکس تمرین ۵ را بیان و اثبات کنید.

۷ با استفاده از بسط دو جمله‌ای ختام یعنی،

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \binom{n}{3} a^{n-3}b^3 + \dots + \binom{n}{n} b^n$$

ثابت کنید که برای هر $n \in \mathbb{N}$ و $a, b \in \mathbb{Z}$ همواره $(a+b)^n \equiv a^n + b^n \pmod{ab}$.

۸ با توجه به تمرین ۷ ثابت کنید عدد $12^{51} - 11^{51} - 23^{51}$ بر عدد ۱۳۲ بخش‌پذیر است.

۹ باقی‌مانده تقسیم عدد $A = (2^{11} + 7) \times 9$ را بر ۲۳ بیابید.

۱۰ اگر دو عدد $(3a - 5)$ و $(4a - 7)$ رقم یکان برابر داشته باشند رقم یکان عدد $(9a + 6)$ را به دست آورید.

۱۱ باقی‌مانده تقسیم عدد $1! + 2! + 3! + \dots + 500!$ را بر ۱۰ به دست آورید (رقم یکان A را بیابید)

۱۲ جواب‌های عمومی معادله سیاله خطی $7x + 5y = 11$ را به دست آورید.

۱۳ به چند طریق می‌توان ۲۹۰۰۰ تومان را به اسکناس‌های ۲۰۰۰ و ۵۰۰۰ تومانی تبدیل کرد؟

۱۴ معادله‌های هم‌نهشتی زیر را در صورت امکان حل کرده و جواب‌های عمومی آنها را به دست آورید.

الف) $423x \equiv 79 \pmod{11}$

ب) $8x \equiv 20 \pmod{12}$

ج) $51x \equiv 11 \pmod{6}$

۱۵ اگر اول مهر ماه در یک سال روز یکشنبه باشد، ۷ اسفندماه در همان سال چه روزی از هفته است؟

۱۶ اگر ۱۲ بهمن در یک سال جمعه باشد، ۳۱ مرداد ماه در همان سال چه روزی از هفته است؟

۱۷ همه اعداد صحیح چون a را بیابید که ۵ برابر آنها به علاوه ۹ بر ۱۱ بخش پذیر باشد.

۱۸ به چند طریق می‌توان یک کیسه ۲۳ کیلویی را با وزنه‌های ۳ و ۵ کیلویی وزن کرد؟

۱۹ به چند طریق می‌توان از بین دو نوع گل یک دسته گل شامل ۹ شاخه به دلخواه انتخاب کرد؟

۲۰ شخصی در یک مسابقه علمی شرکت کرده است. او به سؤالات ۷ امتیازی و ۹ امتیازی پاسخ داده و مجموعاً ۷۳ امتیاز

کسب کرده است. این شخص به چه صورت‌هایی توانسته این امتیاز را به دست آورد؟ (پاسخ به هر سؤال یا امتیاز کامل دارد

و یا امتیازی ندارد)