

# بخش پذیری و هم نهستی

۲

- ۱ بخش پذیری در اعداد صحیح
- ۲ رابطه هم نهستی روی  $Z$  و کاربردهای آن

قرار دادن تعدادی شیء در دسته‌های مساوی یا دسته‌بندی کردن تعدادی شیء، بدون آنکه باقیمانده‌ای داشته باشیم، یعنی شمارش آن اشیا توسط شمارنده‌ها، مثلاً، ۱۲ شیء را می‌توان توسط شمارنده‌های ۱۲ یعنی ۱، ۲، ۳، ۴، ۵، ۶ و ۱۲ شمارش کرد.

به عبارت دیگر شمارنده‌های هر عدد مانند ۱۲ می‌توانند آن عدد را بشمارند. در این فصل برای نمایش این مفهوم از نماد « $\mid$ » استفاده کرده می‌نویسیم  $2 \mid 12$  و می‌خوانیم ۲ می‌شمارد ۱۲ را یا ۲ عاد می‌کند عدد ۱۲ را (عاد کردن یعنی همان شمردن) و یا عدد ۱۲ بر ۲ بخش پذیر است (باقیمانده تقسیم صفر است).

توجه داشته باشید که شمارش تعدادی شیء خاص به صورت صفر تا صفر کار بیهوده‌ای است و لذا صفر هیچ عدد غیر صفری را نمی‌شمارد یا هیچ عدد غیر صفری بر صفر بخش پذیر نمی‌باشد و نیز توجه دارید که هر عدد بر خودش و ۱ بخش پذیر است؛ یعنی اگر  $a$  عددی طبیعی باشد  $1 \mid a$  و  $a \mid a$ . (عدد ۱، هر عدد صحیح را عاد می‌کند و هر عدد بر خودش بخش پذیر است).

حال با توجه به اینکه مفهوم بخش پذیری  $a$  بر  $b$  معادل است با اینکه بنویسیم  $b \mid a$  (را می‌شمارد  $a$  بر  $b$  یا  $a$ ،  $b$  را عاد می‌کند) مفهوم بخش پذیری را می‌توان برای هر دو عدد صحیح به کار برد مثلاً می‌توان گفت، عدد  $28 - 4$  بر ۴ بخش پذیر است (زیرا،  $28 = 4 \times (-7)$  یا باقیمانده تقسیم  $28 - 4$  بر عدد ۴، صفر است) پس در حالت کلی و با تعمیم مفهوم عاد کردن به مجموعه اعداد صحیح مفهوم عاد کردن به صورت زیر تعریف می‌شود.

عدد صحیح  $a$  که مخالف صفر است<sup>۲</sup> شمارنده عدد  $b$  است یا  $a$ ،  $b$  را می‌شمارد یا  $b$  بر  $a$  بخش پذیر است یا  $a \mid b$  هرگاه عددی صحیح چون  $q$  وجود داشته باشد به طوری که  $b = aq$ .

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 رابطهٔ 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 تقسیم اعداد توان دار با پایه‌های برابر ابتدا نشان دهید  $3^5 \mid 3^9$  و سپس ثابت کنید:

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

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

## خواص رابطهٔ عاد کردن

۱ اگر عدد  $a$  عدد  $b$  را بشمارد، آنگاه هر مضرب 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 خاصیت ۱ استفاده کرده و  $m$  را مساوی با  $b$  فرض کنیم و برای اثبات (ب) کافی است

$$m = b^{n-1} \text{ فرض شود.}$$

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 سؤال را بیان کنید.

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  $ka \mid kb$ ؟ آیا از  $ka \mid kb$  می‌توان نتیجه گرفت  $a \mid b$ ؟

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

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

۲ اگر عدد  $a$ ، عدد  $b$  را بشمارد و  $b$  نیز  $c$  را بشمارد آنگاه  $a$ ، 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 و کار در کلاس قبل (شماره ۳) نشان دهید:

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

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

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

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

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

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

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: 
$$\left. \begin{cases} a|b \Rightarrow |a| \leq \dots \text{ (۴)} \\ b|a \Rightarrow \dots \leq |a| \text{ (۴)} \end{cases} \right\} |a| = |b| \Rightarrow a = \pm b$$

## 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  $a = \pm 1$ .

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

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

۲ اگر  $a|b$  نشان دهید که  $a^n|b^n$ .

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

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 خاصیت ۱ و خاصیت ۳ استفاده کنید).

در سال‌های قبل با تعریف و مفهوم اعداد اول آشنا شده‌اید (هر عدد طبیعی و بزرگ‌تر از یک که هیچ شمارندهٔ مثبتی به جز یک و خودش نداشته باشد، عدد اول نامیده می‌شود) این مجموعه که 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  $a$  عددی طبیعی باشد و دو عدد  $(9k+7)$  و  $(7k+6)$  را عا د کند، ثابت کنید  $a=1$  یا  $a=5$ .

$$a | 9k+7 \Rightarrow a | 7 \times (9k+7) \Rightarrow a | 63k + \dots$$

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

$$\Rightarrow a | (\dots + 54) - (63k + \dots) \Rightarrow a | 54 \Rightarrow a = \dots \text{ یا } a = \dots$$

## خواندنی

می‌دانیم هر عدد طبیعی و کوچک‌تر یا مساوی  $10!$  عدد  $10!$  را عا د می‌کند (چرا؟) و به‌طور کلی می‌توان نوشت:  $\forall k \leq n, k! | n!$  بنابراین عدد  $100!+2$  عددی اول/ غیر اول است و همین‌طور عدد  $100!+3$  عددی اول/ غیر اول است و بالاخره عدد  $100!+100$  نیز عددی ... است. بنابراین با توجه به اینکه اعداد  $(100!+2)$  و  $(100!+3)$  و  $(100!+100)$  ...  $(100!+99)$  عدد طبیعی و متوالی‌اند ما توانسته‌ایم  $99$  عدد طبیعی متوالی بیابیم که هیچ‌کدام ... نباشند.

آیا شما می‌توانید  $15$  عدد طبیعی متوالی بیابید که هیچ‌کدام اول نباشند؟

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

$$\text{فاکتور بگیریم یا با استفاده از خواص عا د کردن بنویسیم } 7 | 100! + 7 \Rightarrow 7 | 7 \text{ و } 7 | 100!$$

حال می‌خواهیم با توجه به تعریف رابطهٔ عا د کردن، مفاهیم  $b$  م (بزرگ‌ترین مقسوم‌علیهٔ مشترک) و  $k$  م (کوچک‌ترین مضرب مشترک) دو عدد را معرفی کنیم.

توجه دارید که مقسوم‌علیهٔ همان شمارنده است اگر بنویسیم  $a|b$  یعنی  $a$  شمارندهٔ  $b$  است یا  $b$  بر  $a$  بخش‌پذیر است و این یعنی

$$a \text{ مقسوم‌علیهٔ } b \text{ است و نیز توجه دارید که } b \text{ مضرب } a \text{ است یعنی } b = aq \text{ یا } a|b.$$

**تعریف:** عدد طبیعی  $d$  را ب م م دو عدد صحیح  $a$  و  $b$  می نامیم ( $a$  و  $b$  هر دو با هم صفر نیستند) و می نویسیم  $(a,b)=d$  هرگاه دو شرط (الف) و (ب) برقرار باشند و اگر دو شرط زیر برقرار باشند آنگاه  $(a,b)=d$ .

الف)  $d|a, d|b$

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

شرط (الف) مقسوم علیه مشترک بودن را برای  $d$  تأمین می کند و شرط (ب) نشان می دهد از هر مقسوم علیه مشترک دلخواهی چون  $m$ ، بزرگ تر است.

به خاطر دارید که اگر  $(a,b)=1$  در این صورت می گوئیم  $a$  و  $b$  نسبت به هم اولند.

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

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

**تعریف:** عدد طبیعی  $c$  را ک م م دو عدد ناصفر  $a$  و  $b$  می نامیم و می نویسیم  $[a,b]=c$  هرگاه دو شرط (الف) و (ب) برقرار باشند و اگر دو شرط (الف) و (ب) برقرار باشند آنگاه  $[a,b]=c$

الف)  $a|c$  ,  $b|c$

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

توضیح دهید که شرط های (الف) و (ب) هر یک چه ویژگی را تأمین می کنند؟

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

### کار در کلاس

۱ با توجه به تعاریف ب م م و ک م 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 ب م م را برای  $|a|$  بررسی کنیم یعنی نشان دهیم  $|a||a|$  و ... و نیز برای هر  $m > 0$  که  $m|a$  و  $m|b$  نشان دهیم  $d \leq \dots$  و همین طور برای اثبات (ب) ...

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

... یا  $d|p \Rightarrow d=1$  اول  $d|p$  فرض کنیم  $(p,a)=d$   $d|a$  ①

و این با فرض  $p \nmid a$  تناقض دارد)  $d=p \Rightarrow p|a$  اگر 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:

$4 \nmid 6$  ولی  $(4,6)=2 \neq 1$

## قضیه تقسیم و کاربردها

ممکن است در تقسیم عدد صحیح  $a$  بر عدد طبیعی  $b$  باقیمانده صفر نباشد یا به بیان دیگر  $a$  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، (با تقسیم  $a$  بر  $b$ ) اعدادی صحیح و منحصر به فرد مانند  $q$  و  $r$  یافت می شوند به قسمی که  $a = bq + r$  و  $0 \leq r < b$ .

تذکر: همان طور که از مقطع ابتدایی به خاطر دارید در یک تقسیم وقتی  $a$  را بر  $b$  تقسیم می کنیم،  $a$  را مقسوم،  $b$  را مقسوم علیه،  $q$  را خارج قسمت و  $r$  را باقیمانده می نامیم.

مثال: اگر باقیمانده تقسیم اعداد  $m$  و  $n$  بر  $17$  به ترتیب  $5$  و  $3$  باشد، در این صورت باقیمانده تقسیم عدد  $(2m - 5n)$  را بر  $17$  به دست آورید.

حل:

$$\begin{aligned} \text{فرض فرض: } m &= 17q_1 + 5 & \Rightarrow & \begin{cases} 2m = 2 \times 17q_1 + 10 \\ -5n = (-5) \times 17q_2 - 15 \end{cases} \\ \text{فرض فرض: } n &= 17q_2 + 3 & & \\ \Rightarrow (2m - 5n) &= 17(2q_1 - 5q_2) - 5 = 17(2q_1 - 5q_2 + 1 - 1) - 5 = 17(\underbrace{2q_1 - 5q_2}_{q_r} - 1) + 17 - 5 \\ \Rightarrow (2m - 5n) &= 17(\underbrace{q_r - 1}_q) + 12 = 17q + 12 \Rightarrow \text{باقیمانده} = r = 12 \end{aligned}$$

## افراز مجموعه $\mathbb{Z}$ به کمک قضیه تقسیم

با توجه به قضیه تقسیم می دانیم 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 می کند، برای  $a$  بر حسب  $r$  دقیقاً  $b$  حالت وجود دارد، مثلاً اگر عدد صحیح  $a$  را بر  $5$  تقسیم کنیم در این صورت یا  $a$  بر  $5$  بخش پذیر است یعنی  $r = 0$  یا باقیمانده تقسیم  $a$  بر  $5$  عدد  $1$  است یا  $\dots$  یا باقیمانده تقسیم  $4$  است به عبارت دیگر،  $a = \dots$  یا  $a = 5k + 3$  یا  $a = \dots$  یا  $a = 5k + 1$  یا  $a = 5k$  یا  $a = 5k$  پس می توان گفت هر عدد صحیح مانند  $a$  را می توان 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) می توان نوشت.

حل: کافی است  $m$  را بر  $2$  تقسیم کنیم که 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 می شود.

حل: کافی است  $P$  را بر  $6$  تقسیم کنیم در این صورت طبق قضیه تقسیم خواهیم داشت:

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

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

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

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

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

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

$P$  در حالت (۱)، (۳) و (۵) زوج است و لذا با اول بودن آن تناقض دارد. در حالت (۴) و با فاکتورگیری از  $P = 3(k+1)$  یا  $P = 3k$  یا  $P = 3|P$  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 هر عدد صحیح و فرد مانند  $a$  به یکی از دو صورت  $4k+1$  یا  $4k+3$  نوشته می‌شود و سپس نشان دهید که مربع هر عدد فرد به شکل  $(4t+1)$  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  $A_4 = \{a \in \mathbb{Z} | a = 4k + 3\}$  مجموعه  $\mathbb{Z}$  را افزای می‌کنند.)  
 حالت‌های ... 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 اگر فرض کنیم  $ab = cd$  ( $a, b, c, d$  اعداد صحیح و ناصفرند) در این صورت پنج رابطه عاد کردن از این تساوی نتیجه بگیرید.

۲ اگر  $a|b$  ثابت کنید  $a|-b$  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  $k$  ای در  $\mathbb{Z}$  باشد که داشته باشیم،  $5|4k+1$  ثابت کنید:  $25|16k^2 + 28k + 6$

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

۶ ثابت کنید: الف) هر دو عدد صحیح و متوالی نسبت به هم اولند. ب) هر دو عدد صحیح و فرد متوالی نسبت به هم اولند. (راهنمایی: فرض کنید  $d = (m, m+1)$  و ثابت کنید  $d|1$  و نتیجه بگیرید  $d=1$ ).

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

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

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

۹ اگر باقیمانده تقسیم عدد  $a$  بر دو عدد ۷ و ۸ به ترتیب ۵ و ۷ باشد، باقیمانده تقسیم عدد  $a$  را بر ۵۶ بیابید.

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

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

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

۱۲ اگر در یک تقسیم، مقسوم و مقسوم علیه، هر دو بر عدد صحیح  $n$  بخش پذیر باشند، ثابت کنید باقیمانده 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 مکعب های دو عدد صحیح متوالی، عددی فرد است.

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

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 نماینده مجموعه‌ای در نظر بگیریم که باقیمانده تقسیم هر عضو آن مجموعه بر عدد ۴، به ترتیب صفر، ۱، ۲ و ۳ باشد داریم:

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

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

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

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

۱ دو عضو (به صورت دلخواه) از مجموعه  $A_0$  در نظر بگیرید، آیا تفاضل این دو عدد مضرب ۴ است؟

۲ از مجموعه  $A_1$  دو عضو دلخواه در نظر گرفته و تفاضل آنها را حساب کنید، آیا عدد حاصل مضرب ۴ است؟

۳ نتیجه‌ای که از ۱ و ۲ گرفتید را 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 بگوییم اعضای مجموعه  $A_3$  همگی بر عدد ۴، باقیمانده یکسان دارند؟ در مورد مجموعه  $A_3$  چه می‌توان گفت؟

می‌دانیم مجموعه‌های  $A_0, A_1, A_2, A_3$  یک افزاز برای مجموعه  $\mathbb{Z}$  بوده و بنابراین هر دو عدد صحیح مانند  $a$  و  $b$  یا هر دو به یکی از این چهار مجموعه تعلق دارند یا هر کدام در یک مجموعه واقع هستند ( $A_0, A_1, A_2, A_3$  اشتراکی با هم ندارند. چرا؟) و لذا اگر  $a$  و  $b$  هر دو در یک مجموعه از

این چهار مجموعه باشند (باقیمانده تقسیم  $a$  بر  $b$  مساوی باشد یا اصطلاحاً  $a$  و  $b$  بر  $4$  هم باقیمانده باشند) همواره  $4 \mid a - b$  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  $m \mid a - b$  (و  $b$  بر  $a$  بر  $m$  هم باقیمانده باشند) می‌گوییم « $a$  هم‌نهشت با  $b$  است به سنج یا پیمانه  $m$ » و می‌نویسیم  $a \equiv b^m$ . تعریف رابطه هم‌نهشتی به پیمانه  $m$ ، به زبان ریاضی عبارت است از:

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

قرارداد: مجموعه همه اعداد صحیح که با باقیمانده تقسیم آنها بر عدد طبیعی  $m$  برابر با  $r$  می‌باشد یعنی،  $[r]_m = \{x \in \mathbb{Z} \mid x = mk + r\}$  را کلاس یا دسته هم‌نهشتی  $r$  به پیمانه  $m$  می‌نامیم. 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.

$$a \equiv b^m \Rightarrow a \pm c \equiv b \pm c^m \quad \text{ویژگی ۱:}$$

(به دو طرف یک رابطه هم‌نهشتی می‌توان عددی صحیح را اضافه یا کم کرد.)

$$a \equiv b^m \Rightarrow m \mid a - b \Rightarrow m \mid a + c - b - c \quad \text{اثبات:}$$

$$\Rightarrow m \mid (a + c) - (\dots + \dots) \Rightarrow (\dots + \dots) \equiv (b + c)^m$$

مثال: با توجه به فعالیت قبل فرض کنیم  $7 \equiv -1$  یا  $7 \in A_7$  و  $7$  یا  $7 \equiv (-1)$  در این صورت اگر  $5$  واحد به دو طرف این هم‌نهشتی اضافه کنیم فاصله این دو عدد یا تفاضل آنها همچنان حفظ شده و همان  $8$  که مضرب  $4$  است باقی می‌ماند به عبارت دیگر اعداد حاصل یعنی  $7 + 5 = 12$  و  $7 + 5 = 4 + 8$  نیز در  $A_7$  قرار خواهند گرفت.

$$a \equiv b^m \Rightarrow ac \equiv bc^m \quad \text{ویژگی ۲:}$$

(دو طرف یک رابطه هم‌نهشتی را می‌توان در عددی صحیح ضرب کرد.)

اثبات:

$$a \equiv b^m \Rightarrow m \mid \dots - \dots \Rightarrow m \mid \dots \times (a - b) \Rightarrow m \mid ac - \dots$$

$$\Rightarrow \dots \equiv bc^m$$

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

$$a \equiv b^m \Rightarrow a^n \equiv b^n^m \quad \text{ویژگی ۳:}$$

(دو طرف یک رابطه هم‌نهشتی را می‌توانیم به توان  $n$  برسانیم.) ( $n \in \mathbb{N}$ )

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

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  $5^4 \equiv 3^4$  ولی  $5 \not\equiv 3$  بنابراین نتیجه می‌گیریم که ...

**ویژگی ۴:**  $a \equiv b, c \equiv d \Rightarrow ac \equiv bd$  (۱)  $a \pm c \equiv b \pm d$  (۲)

(دو طرف دو رابطه هم‌نهستی که پیمانه‌های یکسان داشته باشند را می‌توان با هم جمع یا منها کرده یا در هم ضرب کرد.)

$$(15 \equiv 10, 7 \equiv 2 \Rightarrow 15 \times 7 \equiv 10 \times 2, 15 \times 2 \equiv 10 \times 7)$$

$$\Rightarrow 15 + 7 \equiv 10 + 2 \Rightarrow 22 \equiv 12$$

اثبات:

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

$$\Rightarrow m | ac - \dots \dots \dots \xrightarrow{m} \dots \equiv bd$$

اثبات (۲) به عهده شما

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

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

$$(279 = 11 \times 16 + 3 \Rightarrow 279 \equiv 3)$$

اثبات:

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

نتیجه ۱: هرگاه بخواهیم هم‌نهشت عدد  $a$  را به پیمانه  $m$ ، مشخص کنیم کافی است عدد  $a$  را بر  $m$  تقسیم کرده و باقیمانده را به دست آوریم.

نتیجه ۲: اگر  $a$  و  $b$  بر عدد طبیعی  $m$ ، هم باقیمانده باشند (باقیمانده‌های تقسیم  $a$  و  $b$  بر  $m$ ، برابر باشد) در این صورت  $a \equiv b$

مثال: باقیمانده تقسیم عدد  $A = (27)^7 + 19$  را بر ۱۳ بیابید.

$$27 = 13 \times 2 + 1 \Rightarrow 27 \equiv 1 \Rightarrow (27)^7 \equiv 1^7 = 1, 19 = 13 \times 1 + 6$$

$$\Rightarrow \underbrace{19}_{\text{①}} \equiv \underbrace{6}_{\text{①}} \Rightarrow (27)^7 + 19 \equiv 1 + 6 \Rightarrow A \equiv 7 \Rightarrow r = 7$$

پس باقیمانده  $A$  بر ۱۳، برابر با ۷ می‌باشد.

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

$$1000 = 7 \times 142 + 6 \Rightarrow 1000 \equiv 6, 6 \equiv -1 \Rightarrow 1000 \equiv -1$$

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

$$\Rightarrow (1000)^{13} \times 12 + 10 \equiv (-12) + 10 = -2, -2 \equiv 5$$

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

$$a \equiv b \Rightarrow a \pm mt \equiv b \pm mk \quad \text{ویژگی ۶:}$$

(می‌توان به دو طرف یک رابطه هم‌نهستی هر مضربی از پیمانه را اضافه یا کم کرد.)

$$\begin{aligned} \text{طبق فرض: } a &\equiv b \pmod{m} \\ \Rightarrow a \pm mt &\equiv b \pm mk \\ \text{می‌دانیم: } mt &\equiv mk \pmod{m} \end{aligned}$$

مثال: می‌دانیم  $7 \equiv 2 \pmod{5}$  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.

$$ac \equiv bc \pmod{m}, (c, m) = d \Rightarrow a \equiv b \pmod{\frac{m}{d}} \quad \text{ویژگی ۷:}$$

(اگر بخواهیم دو طرف یک رابطه هم‌نهستی را بر عددی تقسیم کنیم می‌بایست پیمانه آن هم‌نهستی را بر م م آن عدد و پیمانه تقسیم کنیم.)

(این ویژگی را بدون اثبات می‌پذیریم)

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

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

## فعالیت

همان‌طور که در مقطع ابتدایی آموختید عدد نویسی ما، در مبنای ۱۰ انجام می‌شود به عبارت دیگر ارزش مکانی ارقام، ده تا ده تا در نظر گرفته می‌شود (ده تا یکی می‌شود ده تا و ده تا ده تا می‌شود صد تا و ده تا صد تا می‌شود هزار تا و ...) بنابراین به راحتی می‌توانیم یک عدد را در مبنای ده، بسط بدهیم. به عنوان مثال عدد ۱۳۹۷ 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 شما هر یک از اعداد زیر را در مبنای ده بسط بدهید:

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

$$13571122 =$$

۲ باقیمانده تقسیم عدد  $A = 1358112$  را بر عدد ۹ بیابید.

می‌دانیم  $1^{\circ} \equiv 1$  و بنا بر ویژگی‌های رابطه هم‌نهستی  $1^{\circ n} \equiv 1$  بنابراین:

$$A = 1 \times 1^{\circ 6} + 3 \times 1^{\circ 5} + \dots + \dots + \dots + 1 \times 1^{\circ} + 2$$

$$1^{\circ 6} \equiv 1 \Rightarrow 1 \times 1^{\circ 6} \equiv 1$$

$$1^{\circ 5} \equiv 1 \Rightarrow 3 \times 1^{\circ 5} \equiv 3$$

$$1^{\circ 4} \equiv 1 \Rightarrow \dots \equiv \dots$$

$$1^{\circ 3} \equiv 1 \Rightarrow \dots \times 1^{\circ 3} \equiv \dots$$

$$1^{\circ 2} \equiv 1 \Rightarrow 1 \times 1^{\circ 2} \equiv \dots$$

$$1^{\circ} \equiv 1 \Rightarrow 1 \times 1^{\circ} \equiv \dots$$

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

با جمع طرفین هم‌نهستی‌ها داریم:

اگر دقت کنید سمت راست هم‌نهستی‌ها، مجموع ارقام  $A$  است بنابراین می‌توان گفت «باقیمانده تقسیم هر عدد بر ۹ برابر است با باقیمانده مجموع ارقام آن عدد بر ۹»

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

$$A = 1^{\circ n-1} \times a_{n-1} + \dots + \dots + \dots + 1^{\circ 2} a_2 + 1^{\circ} a_1 + 1^{\circ} a_0$$

$$\Rightarrow A \equiv 1 \times a_{n-1} + \dots + 1 \times a_1 + a_0$$

$$\Rightarrow A \equiv \dots$$

## کار در کلاس

۱ با توجه به اینکه  $1^{\circ} \equiv 1$ ، نتیجه می‌گیریم،  $\forall k \in W, 1^{\circ k} \equiv 1$  بنابراین مشابه فعالیت قبل باقیمانده تقسیم عدد  $A = 598348$  را بر ۳ بیابید و سپس یک قاعده کلی برای یافتن باقیمانده تقسیم و بخش‌پذیری اعداد  $n$  رقمی بر ۳ بیان کنید.

۲ واضح است که  $1^{\circ} \equiv -1$  بنابراین برای هر  $n$  زوج،  $1^{\circ n} \equiv 1$  و برای هر  $n$  فرد،  $1^{\circ n} \equiv -1$ . حال اگر در هم‌نهستی به پیمانه ۱۱ و در بسط عدد  $A = 4985327$  به جای توان‌های زوج عدد  $1^{\circ}$ ، عدد یک و به جای توان‌های فرد عدد  $1^{\circ}$ ، عدد  $(-1)$  قرار دهیم باقیمانده عدد  $A$  را بر ۱۱ بیابید.

$$A = 4 \times 1^{\circ 6} + 9 \times 1^{\circ 5} + 8 \times 1^{\circ 4} + \dots + 2 \times 1^{\circ} + 7$$

$$\Rightarrow A \equiv 4 \times \dots + \dots \times (-1) + \dots \times 1 + \dots + 2 \times (-1) + 7$$

$$\Rightarrow A \equiv 7 - 2 + 3 - 5 + 8 - 9 + 4 = 6 \Rightarrow r = \dots$$

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

$$\forall k \in \mathbb{N}; 10^k \equiv \dots^2 \text{ و } 10^k \equiv \dots^5 \text{ و } 10^k \equiv \dots^1$$

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  $10$  (در هم‌نهمی‌های به پیمانه  $2$  و  $5$  و  $10$ ) صفر قرار دهیم خواهیم داشت:

$$A = 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10^2 a_2 + 10^1 a_1 + a_0$$

$$\Rightarrow A \equiv 0 \times a_{n-1} + \dots + \dots + \dots \times a_2 + \dots + a_0$$

$$\Rightarrow A \equiv \dots^2 \text{ و } A \equiv \dots^5 \text{ و } A \equiv a_0$$

نتیجه حاصل را برای یافتن باقیمانده تقسیم اعداد  $n$  رقمی بر  $2$  و  $5$  و  $10$  و شرط بخش‌پذیری بر این اعداد را بیان کنید.

یکی از کاربردهای هم‌نهمی در تقویم‌نگاری و محاسبه روزهای هفته برحسب تاریخ داده شده یا مشخص شده است. به‌عنوان مثال اگر اول مهر ماه در یک سال یکشنبه باشد، در این صورت ۲۲ بهمن در همان سال چند شنبه است؟ برای پاسخ دادن به سؤالاتی شبیه سؤال بالا فعالیت زیر را انجام دهید.

### فعالیت

می‌دانیم هر روز از هفته مانند 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. حتماً در بحث تقویم و روزهای هفته دقت داریم که شش ماه اول سال همگی ۳۱ روزه و شش ماه دوم سال غیر از اسفند (که ۲۹ روز است) همگی ۳۰ روزه می‌باشند. البته هر چهار سال یک‌بار (سال کبیسه) اسفند نیز ۳۰ روزه است. 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 ... می‌رسیم.

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

ی	د	س	چ	پ	ج	ش
۰	۱	۲	۳	۴	۵	۶

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

ش	ی	د	س	چ	پ	ج
۰	۱	۲	۳	۴	۵	۶

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

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  $d = 29 + 3 \times 30 + 12 = 131$

۱-۹ دی ماه روز بصیرت نام‌گذاری شده است.

از طرفی  $131 \equiv 0 \pmod{7}$  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 ۲۲ بهمن در سال جاری چه روزی از هفته است؟ درستی پاسخ خود را از روی تقویم نیز بررسی کنید.

## معادله هم‌نهستی

یک رابطه هم‌نهستی همراه با مجهولی چون  $x$  به فرم  $ax \equiv b \pmod{m}$  را یک معادله هم‌نهستی می‌نامیم و منظور از حل یک معادله هم‌نهستی پیدا کردن همه جواب‌هایی چون  $x_0 \in \mathbb{Z}$  است که در معادله فوق صدق کنند یعنی  $ax_0 \equiv b \pmod{m}$  ( $a, b \in \mathbb{Z}$ ).  
 به‌عنوان مثال، معادله  $x \equiv 2 \pmod{3}$  را در نظر بگیرید،  $x$  می‌تواند ۲ باشد و نیز می‌تواند ۵ باشد. عدد بعدی که می‌تواند به جای  $x$  قرار بگیرد و در معادله صدق کند عدد ۸ است و اگر بخواهیم می‌توان تمام جواب‌های این معادله یا جواب‌های عمومی آن را داشته باشیم کافی است از تعریف هم‌نهستی 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 جواب‌های  $x_0 = 2$  و  $x_0 = 5$  و  $x_0 = 8$  را به دست می‌آوریم و برای هر  $k \in \mathbb{Z}$ ، جوابی برای معادله به دست می‌آید. در معادله فوق ضریب  $x$  عدد یک است و اگر ضریب  $x$  عددی غیر از یک باشد برای دست‌یابی به جواب‌های عمومی معادله، ضریب  $x$  را باید حذف کنیم که ویژگی‌های ۵ و ۶ و نتیجه ویژگی ۶ به ما کمک می‌کنند.  
 مثال: جواب‌های عمومی معادله  $4x \equiv 17 \pmod{5}$  را به دست آورید.

$$\begin{aligned} 4x \equiv 17 \pmod{5}, 17 \equiv 2 \pmod{5} &\Rightarrow 4x \equiv 2 \pmod{5} \xrightarrow{\text{ویژگی ۵}} 4x \equiv 2 + (2 \times 5) \\ \Rightarrow 4x \equiv 12 \pmod{5} &\xrightarrow{(4,5)=1} x \equiv 3 \pmod{5} \Rightarrow x = 5k + 3 \\ (5 \mid x - 3) &\Rightarrow x - 3 = 5k \Rightarrow x = 5k + 3 \end{aligned}$$

مثال: همه اعداد صحیح 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  $3x \equiv 13 \pmod{7}$

$$3x \equiv 13 \pmod{7} \Rightarrow 3x \equiv 13 - 7 = 6 \pmod{7} \xrightarrow{(3,7)=1} x \equiv 2 \pmod{7} \Rightarrow x = 7k + 2$$

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

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

معادله را حل کنید:

$$\begin{aligned} 4x \equiv 18 \pmod{6} &\Rightarrow 2 \times 2x \equiv 2 \times 9 \pmod{6}, (2, 6) = 2 \xrightarrow{\text{ویژگی ۶}} 2x \equiv 9 \\ \Rightarrow 2x \equiv 9 \pmod{6} &\Rightarrow 2x \equiv 9 + 3 = 12 \pmod{6} \Rightarrow x \equiv 3 \pmod{6} \Rightarrow x = 6k + 3 \end{aligned}$$

## 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  $x, y \in W$  و  $x$  و  $y$  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.

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 هم‌نهشتی

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

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

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

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

و به طریق مشابه می‌توان نوشت:

### کار در کلاسی

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

$$4x + 5y = 9 \Rightarrow 4x \equiv \dots \pmod{5} \Rightarrow 4x \equiv 9 - \dots \pmod{5} \Rightarrow 4x \equiv 4 \pmod{5}$$

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

$$\Rightarrow 4(5k + 1) + 5y = 9 \Rightarrow 20k + 4 + 5y = 9 \Rightarrow 20k + 5y = 5$$

$$\Rightarrow 4k + y = 1 \Rightarrow y = \dots k + 1$$

۲ در قسمت ۱ فعالیت قبل مشخص کنید به چند طریق می توان عمل وزن کردن را انجام داد؟

کافی است جواب های عمومی معادله  $4x + 3y = 19$  را (بر حسب  $k$ ) بیابیم و به ازای هر  $k \in \mathbb{Z}$  که  $x$  و  $y$  منفی نباشند تعداد حالت ها را شمارش کنیم :

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

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

به ازای  $k=2$  و بیشتر از آن  $y < 0$  و به ازای  $k=-1$  و کمتر از آن  $x < 0$  که قابل قبول نمی باشند و لذا به دو صورت فوق می توان این کیسه ۱۹ کیلویی را وزن کرد.

مثال : به چند طریق می توان ۱۷۰۰۰ تومان را به اسکناس های ۲۰۰۰ و ۵۰۰۰ تومانی خرد کرد؟

حل : اگر  $x$  و  $y$  را به ترتیب تعداد اسکناس های ۲۰۰۰ و ۵۰۰۰ تومانی فرض کنیم حل این مثال معادل است با تعداد جواب های نامنفی  $2000x + 5000y = 17000$

$$\begin{aligned} 2000x + 5000y = 17000 &\Rightarrow 2x + 5y = \dots \Rightarrow 2x \equiv 17, 17 \equiv \dots \\ &\Rightarrow \cancel{2}x \equiv \cancel{2} \times 1 \Rightarrow x \equiv \dots \Rightarrow \underline{x = 5k + 1} \Rightarrow 2(5k + 1) + 5y = 17 \\ &\Rightarrow 10k + 2 + 5y = 17 \Rightarrow 10k + 5y = 15 \Rightarrow \underline{y = -2k + 3} \end{aligned}$$

$$k = 0 \Rightarrow \begin{cases} x = 1 \\ y = 3 \end{cases}, k = 1 \Rightarrow \begin{cases} x = 6 \\ y = 1 \end{cases} \quad (\text{فقط به ازای } 1 \text{ و } 0 \text{ برای } x \text{ و } y \text{ جواب ها نامنفی هستند})$$

پس به دو طریق امکان خرد کردن ۱۷۰۰۰ تومان به اسکناس های ۲۰۰۰ و ۵۰۰۰ تومانی، وجود دارد.

مثال : در یک رستوران فقط دو نوع غذای قورمه سبزی و قیمه وجود دارد. اگر ۵ نفر وارد این رستوران شوند به چند طریق می توانند سفارش غذا بدهند؟ (هر نفر فقط یک پرس غذا میل می کند)

حل : اگر تعداد قورمه سبزی و قیمه سفارش داده را به ترتیب با  $x$  و  $y$  نشان دهیم خواهیم داشت :

$$\begin{aligned} x + y = 5 &\Rightarrow x \equiv 5 \Rightarrow \underline{x = k + \dots} \\ &\Rightarrow k + \cancel{1} + y = \cancel{1} \Rightarrow \underline{y = \dots} \end{aligned}$$

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

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

حل: اگر  $x$  و  $y$  را به ترتیب تعداد اصابت‌ها به دایره کوچک‌تر و بزرگ‌تر فرض کنیم، داریم:

$$5x + 3y = 42 \Rightarrow 5x \equiv 42 \Rightarrow 5x \equiv 42 + 3 \Rightarrow 5x \equiv 45 \Rightarrow x \equiv 9$$

$$\Rightarrow x = 3k + 9, \quad 5(3k + 9) + 3y = 42 \Rightarrow 15k + 45 + 3y = 42$$

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

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

( $x = 6$  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 هم‌نهشتی به پیمانه ۹ تعلق دارد؟

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

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

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

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

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

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

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، برای هر  $n \in \mathbb{N}$  و  $a, b \in \mathbb{Z}$  همواره  $(a+b)^n \equiv a^n + b^n$ .

۸ با توجه به تمرین ۷ ثابت کنید عدد  $12^{51} - 11^{51} - 33^{51}$  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  $500! + 499! + 498! + \dots + 2! + 1!$  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 توسط اسکناس‌های ۲۰۰۰ و ۵۰۰۰ تومانی خرد کرد؟

۱۴ معادله‌های هم‌نهستی 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 گل به دلخواه انتخاب کرد؟

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

کسب کرده است (پاسخ به هر سؤال یا امتیاز کامل دارد و یا امتیازی ندارد) در این صورت این شخص به چه صورت‌هایی

می‌توانسته این امتیاز را به دست آورده باشد؟