درس ۲ بخش‌پذیری در اعداد صحیح[۱]

قرار دادن تعدادی شیء در دسته‌های مساوی یا دسته‌بندی کردن تعدادی از چیزها را، بدون آنکه باقی‌مانده‌ای داشته باشیم، «عاد کردن» یا شمارش آن اشیا، توسط شمارنده‌ها می‌گویند. مثلاً، ۱۲ شیء را می‌توان با شمارنده‌های مثبتِ 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 بخش‌پذیر است (باقی‌ماندهٔ تقسیم صفر است).

توجه داشته باشید که دسته‌بندی کردن اشیا در دسته‌های صفرتایی یا شمارش تعدادی شیء خاص به‌صورت صفر تا صفر کار بی‌معنایی است؛ لذا صفر هیچ عدد غیر صفری را نمی‌شمارد و هیچ عدد غیر صفری بر صفر بخش‌پذیر نمی‌باشد در ضمن توجه داشته باشید که هر عدد بر خودش و بر ۱ بخش‌پذیر است؛ یعنی اگر a عددی طبیعی باشد $1|a$ و $a|a$. (عدد ۱ هر عدد صحیح را عاد می‌کند و هر عدد برخودش بخش‌پذیر است).

حال با توجه به اینکه مفهوم بخش‌پذیری 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 بخش‌پذیری را می‌توان برای هر دو عدد صحیح به‌کار برد، مثلاً می‌توان گفت، عدد ۲۸- بر ۴ بخش‌پذیر است (زیرا، (۷-)×۴=۲۸- یا باقی‌مانده تقسیم ۲۸- بر عدد ۴ صفر است) پس در حالت کلّی و با تعمیم مفهوم عاد کردن به مجموعهٔ اعداد صحیح عاد کردن به‌صورت زیر تعریف می‌شود.

عدد صحیح a، که مخالف صفر است[۲]، شمارندهٔ عدد b است ــ یا a، b را می‌شمارد یا $a|b$ یا b بر a بخش‌پذیر است ــ هرگاه عددی صحیح چون q وجود داشته باشد به‌طوری که $b=aq$.

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

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

۲ــ اینکه صفر عدد صفر را می‌شمارد به‌صورت یک قرارداد پذیرفته می‌شود.

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

الف) $۷ \mid ۶۳ \Leftrightarrow ۶۳= \_\_ \times \_\_$

ب) $۹۱=۷\times \_\_ \Leftrightarrow \_\_ \mid ۹۱$ یا $\_\_ \mid \_\_$

پ) $-۶ \mid ۵۴ \Leftrightarrow \_\_ = (-۶) \times \_\_$

ت) $۵ \mid -۳۵ \Leftrightarrow \_\_ = ۵ \times \_\_$

ث) $۰=۱۸\times \_\_ \Leftrightarrow ۱۸ \mid \_\_$

ج) $a \mid ۱ \Rightarrow a= \_\_$ یا $a= \_\_$

چ) $۲۶=۲\times ۱۳ \Rightarrow ۲ \mid \_\_$ و $\_\_ \mid ۲۶$

۲ با استفاده از تعریف عاد کردن و قوانین ضرب و تقسیمِ اعداد توان‌دار با پایه‌های برابر، ابتدا نشان دهید که $۳^۵ \mid ۳^۹$ و سپس ثابت کنید :

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

$(۳^۹ = ۳^۵ \times ۳^۴ \overset{(۳^۴=q)}{\Rightarrow} ۳^۵ \mid \cdots)$

$۳^۹ = ۳^۵ \times ۳^۴ \xrightarrow{q=۳^۴} ۳^۹ = ۳^۵ \times q \to ۳^۵ \mid ۳^۹$

$\begin{cases} a^n = a^m \times a^{n-m} \xrightarrow{a^{n-m}=q} a^n = a^m \times q \to a^m \mid a^n \\ m \le n \end{cases}$

ویژگی‌های رابطهٔ عاد کردن

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

$$\boxed{a \mid b \Rightarrow a \mid mb}$$

مثال: $۳ \mid ۶ \Rightarrow ۳ \mid ۶ \times ۵ \, , \, ۳ \mid ۶ \times ۴ \, , \, ۳ \mid ۶ \times (-۷) \, , \cdots$

نتیجه : اگر عدد a عدد b را بشمارد، آنگاه $b^۲$ را می‌شمارد و در حالت کلّی b^n را می‌شمارد که $n \in \mathbb{N}$ است. یعنی :

$\begin{cases} \text{الف) } a \mid b \Rightarrow a \mid b^۲ \\ \text{ب) } a \mid b \Rightarrow a \mid b^n \end{cases}$

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 $m=b^{n-۱}$ 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) $۳ \mid ۹$ و $۳ \mid ۶$ و $۳ \mid ۶ \times ۹$

ب) $۳ \nmid ۵$ و $۳ \mid ۶$ و $۳ \mid ۶ \times ۵$

ج) $۶ \nmid ۴$ و $۶ \nmid ۳$ و $۶ \mid ۳ \times ۴$

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

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

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

$a \mid b \Leftrightarrow ka \mid kb$

$a \mid b \to b = aq \xrightarrow{\times k} kb = kaq \to ka \mid kb$

$ka \mid kb \to kb = kaq \xrightarrow{\div k} b = aq \to a \mid b$

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

$$\boxed{a|b \wedge b|c \Rightarrow a|c}$$

اثبات: $\begin{cases} a|b \Rightarrow b = aq_1 \ (1) \\ b|c \Rightarrow c = bq_2 \end{cases}$

$$a|b \to b = aq_1\ (1)$$
$$b|c \to c = bq_2\ (2)$$
$$\xrightarrow{(1),(2)} c = aq_1q_2 \xrightarrow{q_1q_2=q} c = aq \to a|c$$

$$c = bq_2 \overset{(1)}{\Rightarrow} c = \cdots q_2 \overset{q_1q_2=q}{\Rightarrow} c = a\cdots \Rightarrow a|c$$

این خاصیّت را «خاصیت تعدّی» برای رابطهٔ عاد کردن می‌نامیم.

سؤال : با استفاده از خاصیت تعدّی برای رابطهٔ عاد کردن، نشان دهید که :

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

اثبات: طبق فرض $a|b$ و می‌دانیم $b|b^n$ $\xRightarrow{\text{تعدی}}$ $a|b^n$

روش دوم:

$$a|b \xrightarrow{m\in\mathbb{Z}} a|mb$$
$$a|b \xrightarrow{m=b^{n-1}} a|b^{n-1}b \to a|b^n$$

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

$$\boxed{a|b \wedge a|c \Rightarrow a|b \pm c}$$

اثبات: $\left.\begin{matrix} a|b \Rightarrow b = a\times q_1 \\ a|c \Rightarrow c = aq_2 \end{matrix}\right\} \Rightarrow b \pm c = a\cdot\underbrace{(q_1 \pm q_2)}_{q} \Rightarrow a|b \pm c$

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

خیر-مثال نقض: $5|3+7 \to 5|3\text{ ،}5|7$

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 :

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

روش دوم: $a|b \to b = aq \to |b| = |a||q| \geq |a|\times 1 \to |b| \geq |a|$

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

اثبات: $\left.\begin{matrix} a|b \overset{(4)}{\Rightarrow} |a| \leq |b| \\ b|a \overset{(4)}{\Rightarrow} |b| \leq |a| \end{matrix}\right\} \Rightarrow |a| = |b| \Rightarrow a = \pm b$

کار در کلاس

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

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

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

می‌دانیم: $\begin{cases} a|1 \to |a| \leq 1 \\ 1|a \to 1 \leq |a| \end{cases} \to |a| = 1 \to a = \pm 1$

$a^n \mid b^n \rightarrow a \mid b$

$a^n \mid b^n \rightarrow b^n = a^n q \rightarrow \frac{b^n}{a^n} = q \in \mathbb{Z} \rightarrow \frac{b^n}{a^n} \in \mathbb{Z} \rightarrow \left(\frac{b}{a}\right)^n \in \mathbb{Z} \rightarrow \frac{b}{a} \in \mathbb{Z} \rightarrow \frac{b}{a} = k \rightarrow b = ak \rightarrow a \mid b$

۲ اگر $a|b$ نشان دهید که $a^n|b^n$.

اثبات: $a \mid b \Rightarrow b = aq \Rightarrow b^n = \cdots \overset{q^n = q'}{\Rightarrow} b^n = a^n q' \Rightarrow a^n \mid b^n$

$a^n q^n$

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

$$\left.\begin{array}{l} a \mid b \Rightarrow b = aq_1 \\ c \mid d \Rightarrow d = cq_2 \end{array}\right\} \Rightarrow b \times d = (a \times c)\underbrace{(q_1 q_2)}_{q}$$

$$\Rightarrow bd = a \times c \times q \Rightarrow ac \mid bd$$

$a \mid b, a \mid c \rightarrow a \mid mb \pm mc$

$a \mid b \rightarrow b = aq \xrightarrow{\times m} mb = maq$

$a \mid c \rightarrow c = aq' \xrightarrow{\times n} nc = naq'$

$\xrightarrow{\pm} mb \pm nc = maq \pm naq' = a\underbrace{(mq \pm nq')}_{q''}$

$\rightarrow mb \pm nc = aq'' \rightarrow a \mid mb \pm nc$

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 اشنا شده‌اید و می‌دانید که هر عدد طبیعی و بزرگ‌تر از یک که هیچ شمارندهٔ مثبتی به‌جز یک و خودش نداشته باشد، عدد اول نامیده می‌شود. مجموعهٔ اعداد اول، که ثابت شده است مجموعه‌ای نامتناهی است، به‌صورت $P = \{2,3,5,7,11,\ldots\}$ نمایش داده می‌شود.

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

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

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

$\Rightarrow a \mid 63k + 49$

$a \mid 7k+6$

$\Rightarrow a \mid 9 \times (7k+6) \Rightarrow a \mid 63k + 54$

$\Rightarrow a \mid (63k + 54) - (63k + 49)$

$\Rightarrow a \mid 5 \Rightarrow a = 1$ یا $a = 5$.

خواندنی

می‌دانیم که هر عدد طبیعی و کوچک‌تر یا مساوی ۱۰ عدد $10!$ را عاد می‌کند (چرا؟) و به‌طور کلّی می‌توان نوشت : $\forall k \leq n, k \mid n!$؛ بنابراین عدد $100!+2$ و همین‌طور عدد $100!+3$ و ... و بالاخره عدد $100!+100$ همه اعدادی غیراول هستند. بنابراین با توجه به اینکه اعداد $(100!+2)$ و $(100!+3)$ 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 : $7 \mid 100!+7 \Rightarrow 7 \mid 7$ و $7 \mid 100!$)

بزرگ‌ترین مقسومٌ‌علیه مشترک و کوچک‌ترین مضرب مشترک دو عدد

می‌خواهیم با توجه به تعریف رابطهٔ عاد کردن، مفاهیم ب م م (بزرگ‌ترین مقسومٌ‌علیه مشترک) و ک 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 شمارندهٔ 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 ب م م دو عدد صحیح a و b می‌نامیم (a و b هر دو با هم صفر نیستند) و می‌نویسیم $d=(a,b)$، هرگاه دو شرط (الف) و (ب) برقرار باشد و اگر دو شرط زیر برقرار باشد آنگاه $d=(a,b)$.

الف) $d|a, d|b$

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

شرط (الف) مقسومٌ‌علیه 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 ک م م دو عدد صحیح و ناصفر a و b می‌نامیم و می‌نویسیم $c=[a,b]$، هرگاه دو شرط (الف) و (ب) برقرار باشد، و اگر این دو شرط برقرار باشد آنگاه $c=[a,b]$

الف) $a|c \ , \ b|c$

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

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

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

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

الف) $a \mid b \rightarrow (a,b) = \mid a \mid$

باید ثابت کنیم $a \mid b$ واگر $m \mid a, m \mid b$ باشد آنگاه $m \leq \mid a \mid$

می دانیم طبق فرض $a \mid b$ طبق خاصیت تعدی. پس شرط اول برقرار است $\mid a \mid \mid a, a \mid b \leftarrow a \mid b$

حال اگر $m \mid a, m \mid b$ باید ثابت کنیم $m \leq \mid a \mid$ پس خواهیم داشت: $m \mid a \xrightarrow{a \mid b \rightarrow a \leq b} m \leq \mid a \mid$

ب) باید ثابت کنیم: $a \mid b \Rightarrow [a,b] = \mid b \mid$ $\quad b \mid\mid b \mid, a \mid\mid b \mid$

می دانیم طبق فرض $a \mid b$ طبق خاصیت تعدی. پس شرط اول برقرار است $a \mid\mid b \mid \leftarrow b \mid\mid b \mid, a \mid b$

حال اگر $b \mid m, a \mid m$ باید ثابت کنیم $\mid b \mid \leq m$ پس خواهیم داشت: $b \mid m \xrightarrow{a \mid b \rightarrow a \leq b} \mid b \mid \leq m$

۲ اگر p عددی اول باشد و $a\in\mathbb{Z}$ و $p\nmid a$ ، ثابت کنید، $(p,a)=۱$

فرض کنیم $(p,a)=d$ $\begin{cases} d\mid p \overset{p\text{ اول}}{\Rightarrow} d=۱ \text{ یا } d=p \\ d\mid a \quad (۱)\end{cases}$

اگر $d=p \overset{(۱)}{\Rightarrow} p\mid a$ (و این با فرض $p\nmid a$ تناقض دارد)

پس فقط $d=۱$ یا $d=۱۰۰$. $(p,a)=۱$

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

مثال: $۴\nmid ۶$ ولی $(۴,۶)=۲\neq ۱$

قضیه تقسیم و کاربردها

ممکن است در تقسیم عدد صحیح a بر عدد طبیعی b، باقی‌مانده صفر نباشد، یعنی a بر b بخش‌پذیر نباشد $(b\nmid a)$. در این‌صورت قضیهٔ تقسیم که به بیان آن خواهیم پرداخت (این قضیه را بدون اثبات می‌پذیریم) کمک می‌کند تا بحث بخش‌پذیری در $\mathbb{Z}$ را کامل کنیم.

قضیه تقسیم : اگر a عددی صحیح و b عددی طبیعی باشد در این‌صورت، اعدادی صحیح و منحصربه‌فرد مانند q و r یافت می‌شوند به قسمی که $a=bq+r$ و $۰\le r<b$.

مثال : اگر ۲۵ را بر ۷ تقسیم کنیم داریم : $q=۳$ و $r=۴$، و به عبارت دیگر $۲۵=(۷\times ۳)+۴$. حال اگر -۲۵ را بر ۷ تقسیم کنیم و $q=-۳$ در نظر بگیریم، در این صورت تساوی $-۲۵=۷\times(-۳)-۴$ حاصل می‌شود که نمی‌توان (-۴) را به عنوان باقی‌مانده معرفی کرد، زیرا طبق قضیه تقسیم باقی‌مانده باید نامنفی و کوچک‌تر از مقسوم‌علیه باشد در این صورت با اضافه و کم کردن مضارب مثبتی از مقسومٌ‌علیه، شرایط قضیه تقسیم را برقرار می‌کنیم :

$$-۲۵=۷\times(-۳)-۴=۷\times(-۳)-۴-۷+۷$$

$$=۷\times(-۳)-۷+۳=۷\underbrace{[(-۳)-۱)]}_{q}+۳=۷q+۳\Rightarrow r=۳$$

تذکر : همان‌طور که از دورهٔ ابتدایی به‌خاطر دارید در تقسیم عدد a بر b، a را مقسوم، b را مقسومٌ‌علیه، q را خارج قسمت و r را باقی‌مانده می‌نامیم.

مثال : اگر باقی‌ماندهٔ تقسیم اعداد m و n بر ۱۷ به‌ترتیب ۵ و ۳ باشد، در این‌صورت باقی‌ماندهٔ تقسیم عدد $(۲m-۵n)$ بر ۱۷ را به‌دست آورید.

حل :

$$\begin{cases} \text{طبق فرض}: m=۱۷q_۱+۵ \\ \text{طبق فرض}: n=۱۷q_۲+۳ \end{cases}\Rightarrow \begin{cases} ۲m=۲\times ۱۷q_۱+۱۰ \\ -۵n=(-۵)\times ۱۷q_۲-۱۵ \end{cases}$$

$$\Rightarrow (۲m-۵n)=۱۷(۲q_۱-۵q_۲)-۵$$

$$= ۱۷(۲q_۱ - ۵q_۲) - ۵ - ۱۷ + ۱۷$$

$$= ۱۷(\underbrace{۲q_۱ - ۵q_۲}_{q_۳} - ۱) + ۱۷ - ۵$$

$$\Rightarrow (۲m - ۵n) = ۱۷(\underbrace{q_۳ - ۱}_{q}) + ۱۲$$

$$= ۱۷q + ۱۲ \Rightarrow r = ۱۲$$

افراز مجموعهٔ $\mathbb{Z}$ به کمک قضیه تقسیم

با توجه به قضیهٔ تقسیم، می‌دانیم که اگر a عددی صحیح و دلخواه باشد، با تقسیم آن بر عدد طبیعی b، و با توجه به اینکه باقی‌ماندهٔ تقسیم یعنی r در رابطهٔ $۰ \leq r < b$ صدق می‌کند، برای a برحسب r دقیقاً b حالت وجود دارد، مثلاً اگر عدد صحیح a را بر ۵ تقسیم کنیم در این صورت یا a بر ۵ بخش‌پذیر است، یعنی $r = ۰$، یا باقی‌مانده تقسیم a بر ۵ عدد ۱ است یا ... یا باقی‌ماندهٔ تقسیم ۴ است؛ به عبارت دیگر، $a = ۵k$ یا $a = ۵k + ۱$ یا $a = \cdots$ یا $a = ۵k + ۳$ یا $a = \cdots$ 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 $۲k$ یا $۲k + ۱$ (زوج یا فرد) می‌توان نوشت.

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

$$m = ۲k + r \ , \ ۰ \leq r < ۲ \Rightarrow m = \cdots \text{ یا } m = \cdots$$

مسئله ۲ : ثابت کنید اگر $p > ۳$ عددی اول باشد، آنگاه به یکی از دو صورت $p = ۶k + ۱$ یا $p = ۶k + ۵$ نوشته می‌شود.

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

$p = ۶k$ (۱)

$p = ۶k + ۱$ (۲)

$p = ۶k + ۲$ (۳)

$p = ۶k + ۳$ (۴)

$p = ۶k + ۴$ (۵)

$p = ۶k + ۵$ (۶)

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

$$p = ۳(۲k + ۱)$$

یا $p = ۳k'$ یا $۳ | p$ 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 کلّی برقرار نیست؛ مثلاً $(۱+۴\times۶ = ۲۵)$ ولی ۲۵ اول نیست.)

مسئله۳ : ابتدا ثابت کنید که هر عدد صحیح و فرد مانند a به یکی از دو صورت $۴k + ۱$ یا $۴k + ۳$ نوشته می‌شود، سپس نشان دهید که مربع هر عدد فرد به شکل $۸t + ۱$ نوشته می‌شود (باقی‌ماندهٔ 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 :

$a=4k$ (۱)

$a=4k+1$ (۲)

$a=4k+2$ (۳)

$a=4k+3$ (۴)

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

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

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

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 می‌کنیم $ab=cd$ (a , b , c و d اعداد صحیح و ناصفرند) در این صورت پنج رابطهٔ عاد کردن از این تساوی نتیجه بگیرید.

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 به‌طوری‌که $5|4k+1$، 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 اول‌اند. ب) هر دو عدد صحیح و فرد متوالی نسبت به هم اول‌اند.

(راهنمایی : فرض کنید $(m\ ,\ m+1)=d$ 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 $a,b\in\mathbb{Z}$ ثابت کنید :

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

۹ اگر باقی‌ماندهٔ تقسیم عدد a بر دو عدد ۷ و۸ به‌ترتیب ۵ و ۷ باشد، باقی‌ماندهٔ تقسیم عدد a را بر ۵۶ بیابید.

۱۰ اگر a عددی صحیح و فرد باشد و $b|a+2$ در این صورت باقی‌ماندهٔ تقسیم عدد (a^2+b^2+3) بر ۸ را 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 ... در نظر بگیرید و در هر حالت ثابت کنید $3|n^3-n$).

حل تمرینات درس دوم فصل اول

تمرین۱:

$$ab = cd \xrightarrow{a,b,c,d\in\mathbb{Z}} ab \mid cd\ ,\ a \mid cd\ ,b \mid cd\ ,\ c \mid ab\ ,\ d \mid ab$$

تمرین۲: الف)

$$a \mid b \xrightarrow{\exists q\in\mathbb{Z}} b = aq \xrightarrow{\times(-1)} -b = a(-q) \to -b = aq' \to a \mid -b$$

ب)

$$a \mid b \xrightarrow{\exists q\in\mathbb{Z}} b = aq \to b = -a(-q) \to b = -aq' \to -a \mid b$$

ج)

$$a \mid b \xrightarrow{\exists q\in\mathbb{Z}} b = aq \xrightarrow{\times(-1)} -b = -aq \to -a \mid -b$$

تمرین۳:

$a \neq ۱ , a \mid ۹k+۴ , a \mid ۵k+۳ \to$ a عدد اول است

$$\begin{cases} a \mid ۹k+۴ \xrightarrow[m\in\mathbb{Z}]{a\mid b\to a\mid mb} a \mid ۵(۹k+۴) \\ a \mid ۵k+۳ \xrightarrow[m\in\mathbb{Z}]{a\mid b\to a\mid mb} a \mid ۹(۵k+۳) \end{cases} \Rightarrow \begin{cases} a \mid ۴۵k+۲۰ \\ a \mid ۴۵k+۲۷ \end{cases} \Rightarrow a \mid (۴۵k+۲۷)-(۴۵k+۲۰) \Rightarrow a \mid ۷$$

$\xrightarrow{a\neq ۱} a = ۷$ عدد اول است

تمرین۴: گروه تلگرامی فقط گسسته مدیر گروه :استاد ایمانلو

$$\begin{cases} ۵ \mid ۴k+۱ \xrightarrow{a\mid b \to a^n \mid b^n} ۲۵ \mid ۱۶k^۲ + ۸k + ۱ \\ ۵ \mid ۴k+۱ \xrightarrow{a\mid b \to ka \mid kb} ۲۵ \mid ۲۰k + ۵ \end{cases}$$

$$\xrightarrow{a\mid b, a\mid c \to a\mid b+c} ۲۵ \mid \left(۱۶k^۲ + ۸k + ۱\right) + \left(۲۰k + ۵\right) \Rightarrow ۲۵ \mid ۱۶k^۲ + ۲۸k + ۶$$

تمرین۵: خیر. مثال نقض:

$$\begin{matrix} ۲ \mid ۸ \\ ۳ \mid ۹ \end{matrix} \to ۲ + ۳ \not\mid ۸ + ۹ \to ۵ \not\mid ۱۷$$

مدیریت بررسی: استاد عربیار محمدی زهـــــــــــــــــرا شمسی

تمرین ۶: الف)

$$\left.\begin{matrix} m, m+1 \\ m, (m+1) \in \mathbb{Z} \end{matrix}\right\} \Rightarrow (m, m+1) = d, d = 1$$

$$\left.\begin{matrix} d \mid m+1 \\ d \mid m \end{matrix}\right\} \Rightarrow d \mid m+1-m \Rightarrow d \mid 1 \xrightarrow{d>0} d = 1$$

ب)

فرد فرد

$$m, (m+2) \in \mathbb{Z} \Rightarrow (m, m+2) = d, d = 1$$

$$\left.\begin{matrix} d \mid m+2 \\ d \mid m \end{matrix}\right\} \Rightarrow d \mid \cancel{m} + 2 - \cancel{m} \Rightarrow d \mid 2 \xrightarrow{d>0} \begin{matrix} d = 1 & \text{ق ق} \\ d = 2 & \text{غ ق ق} \end{matrix}$$

زیرا $m, (m+2)$ هردو فرد هستند

$$p \neq q \rightarrow (p,q) = 1$$

تمرین ۷:

$$(p,q) = d \rightarrow \begin{cases} d \mid p \rightarrow d = 1 \vee d = p \\ d \mid q \rightarrow d = 1 \vee d = q \end{cases} \xrightarrow{p \neq q} d = 1$$

$$m \leq n \, , a \mid b \rightarrow a^m \mid b^n$$

تمرین ۸:

$$a \mid b \rightarrow a^m \mid b^m \xrightarrow[k = b^{n-m}]{a \mid b \rightarrow a \mid kb} a^m \mid b^{n-m} \times b^m \rightarrow a^m \mid b^n$$

تمرین ۹:

$$a = 7q + 5 \xrightarrow{\times 8} 8a = 56q + 40 \xrightarrow{-} a = 56(q - q') + 40 - 49 \rightarrow a = 56q'' - 9$$

$$a = 8q' + 7 \xrightarrow{\times 7} 7a = 56q' + 49$$

$$\rightarrow a = 56q'' - 9 - 56 + 56 \rightarrow a = 56(q'' - 1) + 47 = 56q''' + \boxed{47}$$

باقی مانده a بر ۵۶ برابر ۴۷ است

تمرین ۱۰:

$$\begin{cases} a \in \mathbb{Z}, a = 2k+1 \\ b \mid a+2 \end{cases} \rightarrow \underline{a^2 + b^2 + 3 \quad \vdots 8}$$

$$r = ?$$

a عددی فرد است پس $a+2$ فرد است و b باید فرد باشد پس $a = 2k+1, b = 2k'+1$

$$a^2 + b^2 + 3 = (2k+1)^2 + (2k'+1)^2 + 3 = 4k^2 + 4k + 1 + 4k'^2 + 4k' + 1 + 3 = \underbrace{4k(k+1)}_{2q} + \underbrace{4k'(k'+1)}_{2q'} + 5$$

$$= 8q + 8q' + 5 = 8(q+q') + 5 = 8q'' + 5 \rightarrow a^2 + b^2 + 3 = 8q'' + 5$$

پس باقی‌مانده $a^2 + b^2 + 3$ بر ۸ برابر **۵**

تمرین ۱۱: باقیمانده هر عدد صحیح بر ۳ برابر صفر یا ۱ یا ۲ است پس $n = 3k$ یا $n = 3k+1$ یا $n = 3k+2$

روش اشباع:

$$n^3 - n = n(n-1)(n+1)$$

$$n = 3k \rightarrow 3\underbrace{k(3k-1)(3k+1)}_{k'} = 3k' \rightarrow 3 \mid n^3 - n$$

$$n = 3k+1 \rightarrow (3k+1)(3k)(3k+2) = 3k' \rightarrow 3 \mid n^3 - n$$

$$n = 3k+2 \rightarrow (3k+2)(3k+1)(3k+3) = 3\big((3k+2)(3k+1)(k+1)\big) = 3k' \rightarrow 3 \mid n^3 - n$$

۱۲ اگر در یک تقسیم، مقسوم و مقسومٌ‌علیه، هر دو بر عدد صحیح n بخش‌پذیر باشند، ثابت کنید باقی‌ماندهٔ تقسیم نیز همواره بر n بخش‌پذیر است.

۱۳ اگر a عددی صحیح و دلخواه باشد ثابت کنید همواره یکی از اعداد صحیح a یا $a+۲$ یا $a+۴$ بر ۳ بخش‌پذیر است.

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

۱۵ ثابت کنید حاصل ضرب سه عدد صحیح متوالی همواره بر !۳ بخش‌پذیر است.

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

الف) $\left([m^۲, m], m^۵\right)$

ب) $(۲m, ۶m^۳)$

پ) $(۳m+۱, ۳m+۲)$

ت) $\left[m^۷, (m^۲, m^۳)\right]$

ث) $[(۷۲, ۴۸), ۱۲۰]$

$$\left(\left[m^۲, m\right], m^۵\right) \xrightarrow{\left[m^۲, m\right]=m^۲} \left(m^۲, m^۵\right) = m^۲$$

$$\left(۲m, ۶m^۲\right) = |۲m|$$

$$\left(۳m+۱, ۳m+۲\right) = ۱$$ ب.م.م هردو عدد متوالی برابر یک است

$$\left[m^۷, \left(m^۲, m^۳\right)\right] \xrightarrow{\left(m^۲, m^۳\right)=m^۲} \left[m^۷, m^۲\right] = |m^۷|$$

$$\left[(۷۲, ۴۸), ۱۲۰\right] \xrightarrow{(۷۲, ۴۸)=۲۴} \left[۲۴, ۱۲۰\right] = ۱۲۰$$

$۷۲ = ۲^۳ \times ۳^۲ \quad ۴۸ = ۲^۴ \times ۳ \quad ۱۲۰ = ۲^۳ \times ۳ \times ۵$

تمرین ۱۲:

$$\begin{array}{l|l} kn & tn \\ \hline r & q \end{array}$$

$$kn = tnq + r \rightarrow r = kn - tnq \rightarrow r = n\underbrace{(k - tq)}_{q'} \rightarrow r = nq' \rightarrow n \mid r$$

یعنی r بر n بخش پذیر است

تمرین ۱۳:

$$a \in \mathbb{Z} \rightarrow \begin{cases} a = 3k \\ a = 3k + 1 \\ a = 3k + 2 \end{cases}$$

$$a = 3k \rightarrow 3 \mid a$$

$$a = 3k + 1 \xrightarrow{+2} a + 2 = 3k + 3 \rightarrow a + 2 = 3\underbrace{(k + 1)}_{k'} \rightarrow a + 2 = 3k' \rightarrow 3 \mid a + 2$$

$$a = 3k + 2 \xrightarrow{+4} a + 4 = 3k + 6 \rightarrow a + 4 = 3\underbrace{(k + 2)}_{k'} \rightarrow a + 4 = 3k' \rightarrow 3 \mid a + 4$$

تمرین ۱۴:

$(n+1)^3 - n^3 =$ **فرد**

$$(n+1)^3 - n^3 = n^3 + 3n^2 + 3n + 1 - n^3 = 3n^2 + 3n + 1 = 3\underbrace{n(n+1)}_{2k} + 1 = 6k + 1 = 2\underbrace{(3k)}_{k'} + 1 = 2k' + 1$$

تمرین۱۵: هرعدد صحیح n بصورتهای $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$ است

$$n^3 - n = n(n-1)(n+1)$$

$$n = 6k \rightarrow 6\underbrace{k(6k+1)(6k+2)}_{k'} = 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

$$n = 6k+1 \rightarrow (6k+1)(6k+2)(6k+3) = 2\times 3\underbrace{(6k+1)(3k+1)(2k+1)}_{k'}$$

$$= 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

$$n = 6k+2 \rightarrow (6k+2)(6k+3)(6k+4) = 2\times 3\times 2\underbrace{((3k+1)(2k+1)(3k+2))}_{k'}$$

$$= 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

$$n = 6k+3 \rightarrow (6k+3)(6k+4)(6k+5) = 2\times 3\underbrace{((2k+1)(3k+2)(6k+5))}_{k'}$$

$$= 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

$$n = 6k+4 \rightarrow (6k+4)(6k+5)(6k+6) = 6\times 2\underbrace{((3k+2)(6k+5)(k+1))}_{k'}$$

$$= 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

$$n = 6k+5 \rightarrow (6k+5)(6k+6)(6k+7) = 6\underbrace{((6k+5)(k+1)(6k+7))}_{k'}$$

$$= 6k' \rightarrow 6 \mid n(n+1)(n+2)$$

۱) کدامیک درست وکدامیک نادرست است . درستها را اثبات وبرای نادرستها مثال نقض بیاورید.

$a \mid b \Rightarrow |a| \leq |b|$

$|a| \leq |b| \Rightarrow a \mid b$

$a \mid b \Rightarrow a+c \mid b+c$

$a \mid b+c \Rightarrow a \mid b, a \mid c$

$a \mid b \Rightarrow a \mid 2b$

$3a^2 \mid b \Rightarrow a \mid b$

$a \mid b \Rightarrow 3a \mid b$

$a^2 \mid b^2 \Rightarrow 2a \mid 2b$

$a \mid c, ab \mid c \Rightarrow b \mid c$

$a^2 \mid b+c \Rightarrow a^2 \mid b^3+c^3$

$a^2 \mid b^3 \Rightarrow a \mid b$

$a^3 \mid b^2 \Rightarrow a^4 \mid b^3$

$a^4 \mid b^3 \Rightarrow a^3 \mid b^2$

$a \mid b+c, a \mid 2c \Rightarrow a \mid 2b$

۲-اگر $a \mid ۴m+۳, a \mid ۵m+۴$ آنگاه برای a چند جواب صحیح وجود دارد؟

۳-اگر x,y دو عدد طبیعی باشند بطوریکه $x-y \mid ۳x-۱, x^۲-y^۲ \mid ۳x$ ثابت کنید x,y متوالیند.

۴-بزرگترین عدد طبیعی که $n+۴ \mid n^۳+n+۱$ را بیابید

۵-مجموعه $\{n \in \mathbb{Z}: \quad n+۴ \mid ۴n^۲+۲\}$ چند عضو دارد؟

۶-اگر $(a,b)=۶$ باشد برای $(a^۲,b^۳)$ چند تا جواب می توان نوشت؟

۷- اگر $(a,b)=1$ باشد نشان دهید $(a+b,a^2+b^2)=1$ یا ۲

۸- حاصل عبارتهای زیر را بدست آورید

$[a,(a,b)]+(a,[a,b])$ $\qquad$ $([ac,b^2],c)$

۹- مطلوب است تعیین دو عدد صحیح مثبت که مجموعشان مساوی ۱۶۰ و کوچکترین مضرب مشترکشان ۶۳ برابر بزرگترین مقسوم علیه مشترکشان باشد.

۱۰- نسبت دو عدد صحیح و مثبت برابر $\frac{5}{6}$ است و میدانیم تفاضل حاصلضربشان از کوچکترین مضرب مشترک آن دو عدد برابر ۳۹۶۰ می باشد آن دو عدد را بیابید.

۱۱-درصورتی که. م. م دوعدد m و ب. م. م آنها d باشدو $m - d = ۳۲,۱ < d < ۱۰$ مطلوبست آن دوعدد طبیعی.

۱۲-بزرگترین شمارنده دو عدد طبیعی ۷۲ و عدد بزرگتر ۸۶۴ می باشد کوچکترین عدد را بیابید

۱۳-حاصل ضرب دوعدد ۶۴۸ و بزرگترین شمارنده آنها ۶ است آن دوعدد طبیعی را بیابید.

۱۴-ب. م. م دو عدد طبیعی ۱۵ و ک. م. م آنها ۱۹۰ است آن دوعدد را بیابید.

۱۵-مطلوبست تعیین دوعدد طبیعی که مجموع آنها ۲۶ و ک. م. م آنها ۱۰۵ می باشد

۱۶-ثابت کنید دوعدد $n^۲ + ۲n + ۱, ۲n + ۱$ به ازای هر عدد طبیعی نسبت بهم اولند.

۱۷-ثابت کنید اگر دوعدد نسبت بهم اول باشند حاصل ضرب ومجموع آنها نیز نسبت بهم اولند.

۱۸-ثابت کنید اگر دوعدد نسبت بهم اول باشند حاصل ضرب وتفاضل آنها نیز نسبت بهم اولند.

قبل از شروع به حل مسایل همنشتی نکات زیر را بدانیم :

۱-هر مضرب m به پیمانه m، همنشت صفر است $km \overset{m}{\equiv} 0$

۲-اگر $a \overset{m}{\equiv} b$، در این صورت همه جا در همنشتی ها می توان به جای a، b را قرار داد. $a \overset{9}{\equiv} -1 \Rightarrow a \overset{9}{\equiv} 8$ مثال: $-1 \overset{9}{\equiv} 8$

۳-اگر $0 \leq r < m$ باشد می دانیم باقیمانده r بر m خود r است

مثال: باقیمانده ۲ بر ۵ خود ۲ است. یا باقیمانده ۰ و ۱ و ۲ و ۳ و ۴ بر ۵ خود این اعداد به ترتیب هستند.

۴-دو عدد هم نشت هم باقیمانده اند. پس اگر $a \overset{m}{\equiv} b$ و باقی مانده a بر m معلوم باشد یا بشود به راحتی بدست آورد در این صورت باقیمانده b بر m هم مشخص است

** در حالت کلی اگر $a \overset{m}{\equiv} r$ $0 \le r < m$, در این صورت باقی مانده a بر r مساوی r است.

۵- $a \overset{m}{\equiv} b \Rightarrow a^n \overset{m}{\equiv} b^n$ (در بسیاری از مسائل همنهشتی که در ارتباط با بدست آوردن باقیمانده تقسیم اعداد به صورت a^n است بکار می رود)

** در اغلب موارد بدست آوردن باقیمانده تقسیم اعداد به صورت a^t سعی می کنیم با استفاده از خواص همنهشتی، این اعداد را کاهش دهیم یعنی عددی کوچکتر بیابیم که با a^t هم نهشت باشد برای این کار دو دسته مسائل داریم

دسته اول: توانی از a هم نهشت با ۱ و ۱- است.

دسته دوم: هیچ توانی از a هم نهشت با ۱ یا ۱- نیست و یا اینکه اگر وجود داشته باشد دور از دسترس است. در این صورت با استفاده از خواص هم نهشتی ها عدد مفروض را کاهش میدهیم