بزرگ‌ترین مقسوم علیه مشترک (ب‌م‌م) یا بزرگ‌ترین شمارنده‌ی مشترک

● حمیدرضا امیری

عدد صحیح c را مقسوم‌علیه مشترک یا شمارنده‌ی مشترک دو عدد صحیح a و b می‌نامیم، در صورتی که هر دو را بشمارد؛ یعنی c|a و c|b .

برای مثال، عدد ۳ یک شمارنده‌ی مشترک برای دو عدد ۶ و ۹- است؛ زیرا ۳|۶ و ۳|-۹ .

تعریف: اگر a و b دو عدد صحیح باشند، به طوری که حداقل یکی از آن‌ها صفر نباشد، بزرگ‌ترین مقسوم‌علیه مشترک (ب‌م‌م) a و b را با نماد (a,b) نمایش می‌دهیم و آن عددی است طبیعی چون d، که اولاً مقسوم‌علیه مشترک a و b باشد و دوم این‌که هر مقسوم‌علیه مشترک a و b از d کوچک‌تر باشد .

اگر بخواهیم معادل تعریف فوق را با نمادهای ریاضی بیان کنیم، خواهیم داشت:

$$(a,b)=d \Leftrightarrow \begin{cases} I)\ d|a, d|b \\ II)\ \forall c>0, c|a, c|b \Rightarrow c \le d \end{cases}$$

به مثال‌های زیر توجه کنید:

$(6,8)=2$, $(4,9)=1$, $(-6,3)=3$

تعریف: اگر برای دو عدد صحیح a و b داشته باشیم $(a,b)=1$ ، در این صورت می‌گوییم a و b نسبت به هم اول (یا متباین) هستند. برای مثال، $(4,9)=1$ ، $(5,3)=1$ و $(6,5)=1$.

تذکر: اگر دو عدد صحیح a و b مفروض باشند و مجموعه‌ی همه‌ی شمارنده‌های مشترک a و b را A بنامیم، یعنی فرض کنیم $A=\{c|c|a, c|b\}$ واضح است که $A \subseteq Z$ و $A \neq \emptyset$ ؛ زیرا $1 \in A$. از طرف دیگر، اگر فرض کنیم $a<b$ ، در این صورت $|a|$ یک کران بالا برای مجموعه‌ی A است (زیرا عددی بزرگ‌تر از $|a|$ نمی‌تواند a را عاد کند)، پس طبق قضیه[1]، مجموعه‌ی A باید دارای عضو انتها باشد که این عضو انتها همان ب‌م‌م است. در واقع ثابت شد که همواره ب‌م‌م دو عدد صحیح که حداقل یکی

از آن‌ها مخالف صفر باشد، موجود است.

قضیه‌ی ۱: اگر a و b دو عدد صحیح و $a|b$ $(a \neq 0)$، در این صورت $(a,b) = |a|$.

اثبات: باید ثابت کنیم که $|a|$ هر دو شرط ب‌م‌م را دارد:

۱) $a|a \ , \ -a|a \Rightarrow |a||a$

$a|b \Rightarrow -a|b \Rightarrow |a||b$: طبق فرض

(یعنی $|a|$ یک مقسوم‌علیه مشترک a و b است.)

۲) فرض کنیم $c > 0 \ , \ c|a \ , \ c|b$

$c|a \Rightarrow |c| \leq |a| \overset{c>0}{\Rightarrow} c \leq |a|$

(یعنی $|a|$ از هر مقسوم‌علیه مشترک a و b بزرگ‌تر است.)

قضیه‌ی ۲: اگر p عددی اول باشد و a عددی صحیح؛ به‌طوری که $p \nmid a$، در این صورت همواره $(p,a) = 1$ (عدد اول p نسبت به هر عددی که مضرب p نباشد، اول است.)

اثبات: فرض کنیم $(p,a) = d$، ثابت می‌کنیم $d = 1$.

$$(p,a) = d \begin{cases} \nearrow d|a \\ \searrow d|p \overset{p\text{اول}}{\Rightarrow} d = 1 \text{ یا } d = p \end{cases} \overset{(1)}{}$$

اگر $d = p$ باشد، در این صورت، با توجه به (۱) باید $p|a$ (به جای d قرار می‌دهیم p) که با فرض $p \nmid a$ تناقض دارد؛ پس باید $d = 1$.

قضیه‌ی ۳ (قضیه‌ی بزو): اگر a و b دو عدد صحیح و حداقل یکی از آن‌ها مخالف صفر باشد، در این صورت، عضو ابتدای مجموعه‌ی $A = \{ma + nb > 0 | m,n \in Z\}$، بزرگ‌ترین مقسوم‌علیه مشترک a و b است؛ یعنی: $\min A = (a,b)$.

اثبات: واضح است که $A \subseteq N$، از طرفی حداقل یکی از دو عدد a و b ناصفر است. بنابراین حداقل یکی از دو عدد $|a|$ یا $|b|$ عضو A است و $A \neq \varnothing$؛ زیرا:

۱) $a \neq 0 \Rightarrow |a| > 0 \Rightarrow |a| = \pm a + 0b \Rightarrow |a| \in A$

۲) $b \neq 0 \Rightarrow |b| > 0 \Rightarrow |b| = 0a \pm b \Rightarrow |b| \in A$

(توجه دارید که عددی عضو A است که دو شرط داشته باشد؛ یکی آن‌که مثبت باشد و دیگر آن‌که به صورت ترکیبی خطی و صحیح از a و b نوشته شود.)

پس ثابت شد که A زیرمجموعه‌ای ناتهی از N است. بنابراین طبق اصل خوش‌ترتیبی، باید دارای عضو ابتدا باشد. اگر عضو ابتدای A را d بنامیم، کافی است ثابت کنیم $d = (a,b)$. البته توجه دارید که چون فرض شده $d = \min A$، پس باید $d \in A$؛ یعنی باید m_0 و n_0 ای در Z باشند، به قسمی که $d = m_0a + n_0b$ (۱).

برای اثبات این‌که $d = (a,b)$، دو شرط ب‌م‌م را برای d بررسی کنیم، شرط اول آن است که $d|a$ و $d|b$. پس a را بر d تقسیم می‌کنیم. طبق قضیه‌ی تقسیم داریم: $a = dq + r$ که $0 \leq r < d$

اگر $0 < r < d$، در این صورت داریم:

$$0 < r = a - dq \overset{(1)}{=} a - (m_0a + n_0b)q = \underbrace{(1 - m_0q)}_{m}a + \underbrace{n_0q}_{n}b$$

$\Rightarrow r \in A$ (r هر دو شرط را برای عضو A بودن داراست.)

اما $r \in A$ با توجه به این‌که $r < d$ و تعریف عضو ابتدا برای d یک تناقض ایجاد می‌کند (زیرا نمی‌توانیم عضوی کوچک‌تر از عضو ابتدا در مجموعه داشته باشیم) پس باید $r = 0$؛ یعنی $a = dq$ یا $d|a$ و به همین طریق ثابت می‌شود $d|b$.

حال فرض کنیم $c > 0$ و $c|a$ و $c|b$. ثابت می‌کنیم که $c \leq d$.

$$\left.\begin{matrix} c|a \Rightarrow c|m_0a \\ c|b \Rightarrow c|n_0b \end{matrix}\right\} \Rightarrow c|m_0a + n_0b \overset{(1)}{\Rightarrow} c|d \Rightarrow c \leq d$$

نتیجه‌های حاصل از قضیه‌ی بزو

نتیجه‌ی ۱: اگر $(a,b) = d$ آن‌گاه اعدادی صحیح و نسبت به هم اول، مانند r و s وجود دارند؛ به قسمی که $ra + sb = d$ (ب‌م‌م دو عدد را بر حسب ترکیب خطی آن دو عدد می‌توان نوشت).

اثبات: طبق قضیه‌ی بزو d عضو ابتدای مجموعه‌ی ترکیب‌های خطی a و b است. پس باید $d \in A$ و هر عضو A ترکیبی خطی از a و b است. اثبات نسبت به هم اول بودن ضرایب این ترکیب خطی، یعنی r و s را درنتیجه‌ی ۴ ملاحظه کنید.

نتیجه‌ی ۲: هرگاه عددی دو عدد را بشمارد، آن‌گاه همواره ب‌م‌م آن‌ها را نیز می‌شمارد؛ یعنی:

$a|b \ , \ a|c \Rightarrow a|(b,c)$

اثبات: فرض کنیم $(b,c)=d$ ثابت می‌کنیم که $a|d$.

$$(b,c)=d \xrightarrow{\text{قضیه‌ی بزو}} \exists r,s \ , \ rb+sc=d$$

$a|b, a|c \Rightarrow a|rb, a|sc \Rightarrow a|rb+sc=d \Rightarrow a|d$ از طرف دیگر

تذکر ۱: عکس قضیه‌ی بزو در حالت کلی برقرار نیست. یعنی اگر عددی چون d برابر با ترکیب خطی دو عدد صحیح مانند a و b باشد، نمی‌توان نتیجه گرفت که d ب م م دو عدد a و b است.

برای مثال $۲۷=۳\times۴+۵\times۳$ ولی $۲۷\neq۱=(۵,۳)$.

نتیجه‌ی ۳: عکس قضیه‌ی بزو در حالت $d=۱$ برقرار است؛ یعنی اگر ترکیب خطی دو عدد صحیح، مساوی با یک باشد، آن‌گاه آن دو عدد نسبت به هم اول هستند.

$ra+sb=۱ \Rightarrow (a,b)=۱$

اثبات: فرض کنیم $(a,b)=d$ و ثابت می‌کنیم که $d=۱$.

$$(a,b)=d \begin{matrix} d|a \Rightarrow d|ra \\ d|b \Rightarrow d|sb \end{matrix} \Rightarrow d|ra+sb$$

و چون طبق فرض $ra+sb=۱$ ، بنابراین باید $d|۱$ که نتیجه می‌شود $d=۱$.

تذکر ۲: اگر p عددی اول باشد و $ra+sb=p$ در این صورت $(a,b)=۱$ یا $(a,b)=p$. (مشابه اثبات نتیجه ۳، فقط به‌جای ۱ قرار دهید p)

نتیجه‌ی ۴: اگر دو عدد صحیح مانند a و b را بر بزرگ‌ترین مقسوم‌علیه مشترکشان تقسیم کنیم، آن‌گاه خارج قسمت‌ها نسبت به هم اول خواهند بود؛ یعنی:

$$(a,b)=d \Rightarrow (\frac{a}{d},\frac{b}{d})=۱$$

اثبات: کافی است ثابت کنیم یک ترکیب خطی از $\frac{a}{d}$ و $\frac{b}{d}$ مساوی با عدد یک است و طبق نتیجه‌ی ۳ ثابت می‌شود $\frac{a}{d}$ و $\frac{b}{d}$ نسبت به هم اول هستند.

$$(a,b)=d \xrightarrow{\text{قضیه‌ی بزو}} \exists r,s\in Z \ , \ ra+sb=d \xrightarrow{\text{دو طرف بر d تقسیم}}$$

$$r\frac{a}{d}+s\frac{b}{d}=\frac{d}{d} \Rightarrow r\frac{a}{d}+s\frac{b}{d}=۱ \xrightarrow{\text{نتیجه‌ی ۳}} (\frac{a}{d},\frac{b}{d})=۱$$

تذکر ۳: تساوی $r\frac{a}{d}+s\frac{b}{d}=۱$ ترکیبی خطی از r و s نیز هست که در این صورت ثابت می‌شود $(r,s)=۱$ ؛ یعنی در قضیه‌ی بزو ضرایب ترکیب خطی که d را می‌سازد، همواره نسبت به هم اول هستند!

نتیجه‌ی ۵ (لم اقلیدس): هر گاه عددی حاصل‌ضرب دو عدد را بشمارد و نسبت به یکی از آن دو عدد، اول باشد، آن‌گاه همواره دیگری را می‌شمارد:

$a|bc \ , \ (a,b)=۱ \Rightarrow a|c$

اثبات: برای اثبات این‌که $a|c$ کافی است ثابت کنیم $c=aq$. پس به‌دنبال یک تساوی هستیم که یک طرف آن c و طرف دیگر مضرب a باشد:

$$(a,b)=۱ \xrightarrow{\text{قضیه‌ی بزو}} ra+sb=۱ \Rightarrow rac+sbc=c \quad (۱)$$

از طرف دیگر طبق فرض: $a|bc \Rightarrow bc-aq_۱ \overset{(۱)}{\Rightarrow} rac+s(aq_۱)=c$

$$\Rightarrow c=a\underbrace{(rc+sq_۱)}_{q} \Rightarrow c=aq \Rightarrow a|c$$

مسئله‌ی مهم: ثابت کنید، اگر a، b، c و d اعداد طبیعی باشند و $\frac{a}{b}=\frac{c}{d}$ و داشته باشیم $(a,b)=(c,d)=۱$ ، آن‌گاه $a=c$ و $b=d$.

اثبات: کافی است ثابت کنیم $a\le c$ و $c\le a$ که در این صورت $a=c$ و درنتیجه $b=d$ حاصل می‌شود:

$$ad=bc \Rightarrow a|bc \ , \ (a,b)=۱ \overset{\text{لم اقلیدس}}{\Rightarrow} a|c \Rightarrow a\le c \quad (۱)$$ طبق فرض:

$$ad=bc \Rightarrow c|ad \ , \ (c,d)=۱ \overset{\text{لم اقلیدس}}{\Rightarrow} c|a \Rightarrow c\le a \quad (۲)$$ طبق فرض:

$(۱),(۲) \Rightarrow a=c \ , \ ad=bc \Rightarrow ad=ba \Rightarrow b=d$

تست: اگر a و b دو عدد صحیح و $p|ab$ و $۳۷p-۲۹a=۱$ ، کوچک‌ترین عضو مثبت مجموعه‌ی $A=\{mp+nb:m,n\in z\}$ کدام است؟ (کنکور سراسری ۷۵)

۱) b ۲) p ۳) ۱ ۴) ۸

حل: گزینه‌ی (۲) صحیح است؛ زیرا با توجه به رابطه‌ی $۳۷p-۲۹a=۱$ و نتیجه‌ی (۳) باید $(p,a)=۱$ و چون $p|ab$ پس طبق لم اقلیدس باید $p|b$. بنابراین $(p,a)=|p|$ که طبق قضیه‌ی بزو $\min A=(p,b)$ ، پس $\min A=|p|$ که البته در گزینه‌ها باید به جای p عدد $|p|$ به‌کار می‌رفت!

نتیجه‌ی ۶: اگر عددی بر دو عدد بخش‌پذیر باشد و آن دو عدد نسبت به هم اول باشند، آن‌گاه بر حاصل‌ضرب آن دو عدد نیز بخش‌پذیر است:

$b|a \ , \ c|a \ , \ (b,c)=۱ \Rightarrow bc|a$

اثبات: برای اثبات این‌که $bc|a$ کافی است ثابت کنیم $a=bcq$ که به یک تساوی نیازمندیم؛ طوری که در یک طرف آن a و طرف دیگر آن مضرب bc باشد:

$$(b,c)=۱ \xrightarrow{\text{قضیه‌ی بزو}} rb+sc=۱ \xrightarrow{\text{دو طرف در a ضرب}} rab+sac=a \quad (۱)$$

$b|a \ , \ c|a \Rightarrow a = bq_1 \ , \ a = cq_2$: از طرف دیگر طبق فرض

$$\overset{(1)}{\Rightarrow} r(cq_2)b + s(bq_1)c = a \Rightarrow a = bc\underbrace{(rq_2 + sq_1)}_{q}$$

$$\Rightarrow a = bcq \Rightarrow bc|a$$

نتیجه‌ی ۷: اگر p عددی اول و $p|ab$ ، آن‌گاه $p|a$ یا $p|b$ (p حداقل یکی از a یا b را عاد می‌کند).

اثبات: اگر $p|a$ حکم ثابت است و اگر $p\not|a$ طبق قضیه‌ی ۲ باید $(p,a) = 1$ و در نتیجه، بنابر لم اقلیدس، باید $p|b$ ؛ یعنی:

$$p\not|a \Rightarrow (p,a) = 1 \ , \ p|ab \Rightarrow p|b$$

در این صورت نیز حکم به اثبات رسید؛ یعنی همواره $p|a$ یا $p|b$.

نتیجه‌ی ۸: اگر $(a,b) = d$ و $k \in N$ در این صورت $(ka,kb) = kd$ و برعکس. (اگر $k \in Z$ ، $(ka,kb) = |k|d$)

اثبات (شرط لازم):

$$\overbrace{(a,b) = d}^{\text{فرض}} \Rightarrow \overbrace{(ka,kb) = kd = k(a,b)}^{\text{حکم}}$$

دو شرط ب‌م‌م را برای kd بررسی می‌کنیم:

۱) $(a,b) = d$ $\quad d|a \Rightarrow kd|ka$ ، $d|b \Rightarrow kd|kb$

۲) فرض کنیم $c > 0$ ، $c|ka$ ، $c|kb \overset{\text{باید ثابت کنیم}}{\Rightarrow} c \le kd$

$(a,b) = d \overset{\text{قضیه‌ی بزو}}{\Rightarrow} ra + sb = d \Rightarrow rka + skb = kd$ (۱) طبق فرض

از طرف دیگر فرض کرده‌ایم : $c|ka$ ، $c|kb$

$$\Rightarrow c|rka \ , \ c|skb \Rightarrow c|rka + skb \overset{(1)}{\Rightarrow} c|kb \Rightarrow c \le kd$$

(شرط کافی):

$$\overbrace{(ka,kb) = kd}^{\text{فرض}} \Rightarrow \overbrace{(a,b) = d}^{\text{حکم}}$$

حال دو شرط ب‌م‌م را برای d بررسی می‌کنیم:

۱) $(ka,kb) = kd$ $\quad kd|ka \Rightarrow d|a$ ، $kd|kb \Rightarrow d|b$

۲) فرض کنیم $c > 0$ ، $c|a$ ، $c|b \overset{\text{باید ثابت کنیم}}{\Rightarrow} c \le d$

$(ka,kb) = kd \overset{\text{قضیه‌ی بزو}}{\Rightarrow} rka + skb = kd \Rightarrow ra + sb = d$ (۲)

از طرف دیگر فرض کرده‌ایم : $c|a$ ، $c|b \Rightarrow c|ra$ ، $c|sb$

$$\Rightarrow c|ra + sb \overset{(2)}{\Rightarrow} c|d \Rightarrow c \le d$$

تست: اگر $(a,b) = 1$ ، در این صورت $(a+b, a-b)$ کدام است؟

۱) ۱ ۲) ۲ ۳) ۱ یا ۲ ۴) ۱ یا ۲ یا ۴

حل: گزینه‌ی ۳ صحیح است، زیرا اگر فرض کنیم $(a+b, a-b) = d$ در این صورت داریم:

$$\left.\begin{matrix} d|a+b \\ d|a-b \end{matrix}\right\} \Rightarrow \begin{matrix} d|(a+b)+(a-b) \Rightarrow d|2a \\ d|(a+b)-(a-b) \Rightarrow d|2b \end{matrix}$$

$$d|2a, d|2b \overset{\text{نتیجه‌ی ۲}}{\Rightarrow} d|(2a,2b) \overset{\text{نتیجه‌ی ۸}}{\Rightarrow} d|2(a,b) \Rightarrow d|2\times 1 = 2$$

$$\Rightarrow d = 1 \text{ یا } d = 2$$

نتیجه‌ی ۹: اگر عددی نسبت به دو عدد اول باشد، آن‌گاه نسبت به حاصل ضرب آن دو عدد نیز اول است و برعکس:

$$(a,b) = 1, \ (a,c) = 1 \Leftrightarrow (a,bc) = 1$$

اثبات (شرط لازم):

$$\left.\begin{matrix} (a,b) = 1 \overset{\text{قضیه‌ی بزو}}{\Rightarrow} r_1a + s_1b = 1 \\ (a,c) = 1 \Rightarrow r_2a + s_2c = 1 \end{matrix}\right\} \overset{\text{دو طرف تساوی‌ها در هم ضرب}}{\Rightarrow}$$

$$r_1r_2a^2 + r_1s_2ac + r_2s_1ab + s_1s_2bc = 1$$

$$\Rightarrow \underbrace{(r_1r_2a + r_1s_2c + r_2s_1b)}_{r}a + \underbrace{(s_1s_2)}_{s}bc = 1$$

$$\Rightarrow ra + sbc = 1 \overset{\text{نتیجه‌ی ۳}}{\Rightarrow} (a,bc) = 1$$

اثبات (شرط کافی):

$$(a,bc) = 1 \overset{\text{قضیه‌ی بزو}}{\Rightarrow} ra + sbc = 1 \qquad (1)$$

$$(1) \Rightarrow ra + (sb)c = 1 \overset{\text{نتیجه‌ی ۳}}{\Rightarrow} (a,c) = 1$$

$$(1) \Rightarrow ra + (sc)b = 1 \overset{\text{نتیجه‌ی ۳}}{\Rightarrow} (a,b) = 1$$

مسائل حل شده

مسئله‌ی ۱: ثابت کنید اگر $(a,b) = 1$ ، آن‌گاه $(k \in Z).(ka \pm d, a) = 1$

حل: فرض می‌کنیم $(ka \pm b, a) = d$ و ثابت می‌کنیم $d = 1$.

$$(ka \pm b, a) = d \begin{matrix} \nearrow d|ka \pm b \\ \searrow d|a \end{matrix} \Rightarrow d|ka \Rightarrow d|b$$

$$d|a, d|b \Rightarrow d|(a,b) = 1 \Rightarrow d = 1$$

تذکر: مسئله در حالت کلی یعنی برای $(a,b) = d$ نیز برقرار

است به عبارت دیگر:

$(a,b)=d \Rightarrow (a,ka\pm b)=d$

نتیجه: اگر در مسئله‌ی (۱) قرار دهیم $k=1$، در این صورت خواهیم داشت:

$(a,b)=1 \Rightarrow (a,a\pm b)=1$

مسئله‌ی ۲: ثابت کنید:

$(a,b)=(-a,b)=(a,-b)=(-a,-b)$

حل: فرض کنیم $(a,b)=d_1, (-a,b)=d_2$، ثابت می‌کنیم $d_1=d_2$.

$$(a,b)=d_1 \begin{cases} \nearrow d_1|a \Rightarrow d_1|-a & (1) \\ \searrow d_1|b & (2) \end{cases}$$

$(1),(2) \Rightarrow d_1|(-a,b)=d_2 \Rightarrow d_1 \le d_2$

و به طریق مشابه ثابت می‌شود $d_1 \le d_2$ که نتیجه می‌گیریم $d_1=d_2$ و در بقیه‌ی حالت‌ها نیز مطابق حل فوق عمل می‌کنیم.

مسئله‌ی ۳: اگر $(a,b)=1$، ثابت کنید

$(m,n\in N).(a^n,b^m)=1$

حل: ابتدا به استقرا روی n ثابت می‌کنیم، اگر $(a,b)=1$، آن‌گاه $(a^n,b)=1$.

(برقرار است) $p(1):(a,b)=1 \Rightarrow (a^1,b)=1 \Rightarrow p(1)\equiv T$

فرض استقرا $p(k)\equiv T \Rightarrow (a,b)=1 \Rightarrow (a^k,b)=1$

حکم استقرا $p(k+1):(a,b)=1 \Rightarrow (a^{k+1},b)=1$

$$(a,b)=1 \nearrow (a,b)=1 \searrow (a^k,b)=1 \Big\} \overset{\text{نتیجه‌ی ۹}}{\Rightarrow} (a.a^k,b)=1$$

$\Rightarrow (a^{k+1},b)=1$

ثابت کردیم که اگر دو عدد نسبت به هم اول باشند، آن‌گاه هر توان یکی از آن دو عدد و عدد دیگر نیز نسبت به هم اول خواهند بود که با توجه به این مطلب، برای حالت $(a^n,b^m)=1$ نیازی به استفاده از استقرا روی m نداریم و می‌نویسیم:

$(a,b)=1 \overset{\text{ثابت شد}}{\Rightarrow} (b,a^n)=1 \overset{\text{جابه‌جایی}}{\Rightarrow} (b^m,a^n)=1 \overset{\text{ثابت شد}}{\Rightarrow} (a^n,b^m)=1$

$\overset{\text{جابه‌جایی}}{\Rightarrow}$

مسئله‌ی ۴: عکس مسئله‌ی ۳ را ثابت کنید.

حل: با فرض $(a^n,b^m)=1$ می‌خواهیم ثابت کنیم $(a,b)=1$.

$(a^n,b^m)=1 \overset{\text{قضیه‌ی بزو}}{\Rightarrow} ra^n+sb^m=1$

$\Rightarrow \underbrace{(ra^{n-1})}_{r_1}a+\underbrace{(sb^{n-1})}_{s_1}b=1 \overset{\text{نتیجه‌ی ۳}}{\Rightarrow} (a,b)=1$

مسئله‌ی ۵: ثابت کنید، اگر دو عدد نسبت به هم اول باشند، آن‌گاه حاصل ضرب و مجموع آن‌ها و همین‌طور حاصل ضرب و تفاضل آن‌ها نیز نسبت به هم اول هستند و برعکس؛ یعنی:

$(a,b)=1 \Leftrightarrow (ab,a\pm b)=1$

حل:

$$\left.\begin{matrix}(a,b)=1 \overset{\text{مسئله‌ی ۱}}{\Rightarrow} (a\pm b,a)=1 \\ (a,b)=1 \Rightarrow (a\pm b,b)=1\end{matrix}\right\} \overset{\text{نتیجه‌ی ۹}}{\Rightarrow} (a\pm b,ab)=1$$

مسئله‌ی ۶: اگر $(a,b)=1$، $(a,c)=1$ و $(b,c)=1$، ثابت کنید $(abc,ab+ac+bc)$.

حل: از مسئله‌ی (۱) استفاده می‌کنیم:

$$\left.\begin{matrix}(a,b)=1 \\ (a,c)=1\end{matrix}\right\} \Rightarrow (a,bc)=1 \overset{\text{مسئله‌ی ۱}}{\Rightarrow} (a,\overbrace{ab+ac}^{ka}+bc)=1 \quad (1)$$

$$\left.\begin{matrix}(a,b)=1 \\ (c,b)=1\end{matrix}\right\} \Rightarrow (ac,b)=1 \overset{\text{مسئله‌ی ۱}}{\Rightarrow} (b,\overbrace{ab+bc}^{kb}+ac)=1 \quad (2)$$

$$\left.\begin{matrix}(a,c)=1 \\ (b,c)=1\end{matrix}\right\} \Rightarrow (c,ab)=1 \Rightarrow (c,\overbrace{ac+bc}^{kc}+ab)=1 \quad (3)$$

$$(1) \text{ و } (2) \overset{\text{نتیجه‌ی ۹}}{\Rightarrow} (ab,ab+ac+bc)=1 \quad (4)$$

$$(3) \text{ و } (4) \overset{\text{نتیجه‌ی ۹}}{\Rightarrow} (abc,ab+ac+bc)=1$$

مسئله‌ی ۷: اگر $(a,b)=1$، ثابت کنید

$(a^5+b^2,2a^5+5b^2)$ ۳ یا ۱.

حل: فرض کنیم $(a^5+b^2,2a^5+5b^2)=d$، ثابت می‌کنیم $d=3$ یا $d=1$.

$(a^5+b^2,2a^5+5b^2)=d$

$$\Rightarrow \begin{cases} d|a^5+b^2 \Rightarrow \begin{cases} d|2a^5+2b^2 & (1) \\ d|5a^5+5b^2 & (2) \end{cases} \\ d|2a^5+5b^2 \quad (3) \end{cases}$$

$$\left.\begin{matrix}(1),(3) \Rightarrow d|3b^2 \\ (2),(3) \Rightarrow d|3a^5\end{matrix}\right\} \overset{\text{نتیجه‌ی ۲}}{\Rightarrow} d|(3a^5,3b^2)$$

$d=3$ یا $d=1 \Rightarrow d|(3a^5,b^2) \overset{\text{نتیجه‌ی ۸}}{\Rightarrow} d|3\times 1=3$

(توجه دارید که اگر $(a,b)=1$ ، آن‌گاه $(a^5,b^2)=1$.)

مسئله‌ی ۸ : اگر $(a,b)=d$ ، ثابت کنید $(a^n,b^n)=d^n$.

حل:

$$(a,b)=d \Rightarrow (\frac{a}{d},\frac{b}{d})=1 \Rightarrow \left((\frac{a}{d})^n,(\frac{b}{d})^n\right)=1$$

$$\Rightarrow (\frac{a^n}{d^n},\frac{b^n}{d^n})=1 \Rightarrow d^n(\frac{a^n}{d^n},\frac{b^n}{d^n})=d^n$$

$$\overset{\text{نتیجه‌ی ۸}}{\Rightarrow} (a^n,b^n)=d^n$$

(توجه دارید که از $d|a$ نتیجه می‌شود که $d^n|a^n$ و از این رابطه در تساوی $(\frac{a}{d})^n=\frac{a^n}{d^n}$ استفاده شده است.)

مسئله‌ی ۹ : ثابت کنید اگر $a^n|b^n$ ، آن‌گاه $a|b$.

حل : کافی است ثابت کنیم $(a,b)=a$ که در این صورت، رابطه‌ی $a|b$ نتیجه می‌شود. حال فرض می‌کنیم $(a,b)=d$ و ثابت می‌کنیم $d=a$.

(۱) $(a,b)=d \overset{\text{مسئله‌ی ۸}}{\Rightarrow} (a^n,b^n)=d^n$

(۲) طبق فرض : $a^n|b^n \Rightarrow (a^n,b^n)=a^n$

$(1),(2) \Rightarrow a^n=d^n \Rightarrow a=d \Rightarrow (a,b)=a \Rightarrow a|b$

مسئله‌ی ۱۰ : ثابت کنید اگر $(a^n,b^n)=d^n$ ، آن‌گاه $(a,b)=d$. (عکس مسئله‌ی ۸)

حل:

(۱) $(a^n,b^n)=d^n \Rightarrow (\frac{a^n}{d^n},\frac{b^n}{d^n})=1$

حال با توجه به مسئله‌ی ۹ ، از این‌که $\frac{a^n}{d^n}$ عددی صحیح است یا از این‌که $d^n|a^n$ ، نتیجه می‌گیریم $d|a$ ، که در این صورت تساوی $(\frac{a^n}{d^n})=(\frac{a}{d})^n$ برقرار است:

$$(1) \Rightarrow \left((\frac{a}{d})^n,(\frac{b}{d})^n\right)=1 \Rightarrow (\frac{a}{d},\frac{b}{d})=1$$

$$\Rightarrow d(\frac{a}{d},\frac{b}{d})=d \Rightarrow (a,b)=d$$

مسئله‌ی ۱۱ : اگر $(a,4)=2$ و $(b,4)=2$ ، ثابت کنید $(a+b,4)=4$.

حل:

$(a,4)=2 \Rightarrow (\frac{a}{2},2)=1 \Rightarrow \frac{a}{2}$ فرد است $\Rightarrow \frac{a}{2}=2k+1$

$(b,4)=2 \Rightarrow (\frac{b}{2},2)=1 \Rightarrow \frac{b}{2}$ فرد است $\Rightarrow \frac{b}{2}=2k'+1$

$$\left.\begin{array}{l}\frac{a}{2}=2k+1 \Rightarrow a=4k+2\\ \frac{b}{2}=2k'+1 \Rightarrow b=4k'+2\end{array}\right\} \Rightarrow a+b=4(k+k')+4$$

$$\Rightarrow a+b=4(k+k'+1)=4q \Rightarrow 4|a+b \Rightarrow (a+b,4)=4$$

مسئله‌ی ۱۲ : اگر $(b,d)=1$ ، $d\neq 1$ و $(a-2b,3a-b)=d$ ، ثابت کنید $d=5$.

حل:

$$(a-2b,3a-b)=d \begin{cases} \nearrow d|a-2b \Rightarrow d|-3a+6b & (1)\\ \searrow d|3a-b & (2)\end{cases}$$

$$(1),(2) \Rightarrow d|5b \overset{(d,b)=1}{\underset{\text{لم اقلیدس}}{\Rightarrow}} d|5 \overset{d\neq 1}{\Rightarrow} d=5$$

قضیه‌ی الگوریتم اقلیدسی : اگر $a=bq+r$ ، آن‌گاه $(a,b)=(b,r)$.

(اگر a را بر b تقسیم کنیم و q خارج قسمت و r باقی‌مانده‌ی تقسیم باشد، در این صورت ب.م.م مقسوم و مقسوم‌علیه برابر است با ب.م.م مقسوم‌علیه و باقی‌مانده.)

اثبات : فرض کنیم $(a,b)=d_1$ و $(b,r)=d_2$ ، ثابت می‌کنیم : $d_1=d_2$.

$$(a,b)=d_1 \begin{array}{l} d_1|a\\ d_1|b \Rightarrow d_1|bq\end{array} \Rightarrow d_1|a-bq=r$$

$$d_1|b, d_1|r \Rightarrow d_1|(b,r)=d_2 \Rightarrow d_1\leq d_2 \qquad (1)$$

$$(b,r)=d_2 \begin{array}{l} d_2|b \Rightarrow d_2|bq\\ d_2|r\end{array} \Rightarrow d_2|bq+r=a$$

$$d_2|a, d_2|b \Rightarrow d_2|(a,b)=d_1 \Rightarrow d_2\leq d_1 \qquad (2)$$

(1) و $(2) \Rightarrow d_1=d_2$

زیرنویس

۱. هر زیرمجموعه‌ی ناتهی Z که از بالا کران‌دار باشد، دارای عضو انتهاست.