بخشی از یک کتاب

ورودی به نظریه اعداد
(سری کتابهای کوچک ریاضی)

(برای دانش‌آموزان دورهٔ پیش‌دانشگاهی)

حمیدرضا امیری

بزرگترین مقسوم علیه مشترک (ب م م) یا بزرگترین شمارندهٔ مشترک

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

به عنوان مثال، عدد ۳ یک شمارندهٔ مشترک برای دو عدد ۶ و ۹- است؛ زیرا $3|6$ و $3|-9$.

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 داده و آن عددی است طبیعی چون d، که اولاً مقسوم‌علیه مشترک a و b باشد و دوم این که 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:

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

تعریف: اگر برای دو عدد صحیح a و b داشته باشیم $(a,b)=1$، در این صورت می‌گوییم a و b نسبت به هم اوّل هستند (یا نسبت به هم متباین هستند). به‌عنوان مثال، ۱=(۹، ۴)، ۱=(۵، ۳) و ۱=(۶، ۵).

تذکر: اگر دو عدد صحیح a و b مفروض باشند و مجموعهٔ همهٔ شمارنده‌های مشترک a و b را A بنامیم؛ یعنی فرض کنیم $A=\{c|c|a,\ c|b\}$ واضح است که $A\subseteq Z$ و $A\neq\varnothing$؛ زیرا، $1\in A$. از طرفی اگر فرض کنیم $a>b$، در این صورت $|a|$

$|a|$ یک کران بالا برای مجموعهٔ A است (زیرا عددی بزرگتر از $|a|$ نمی‌تواند a را عاد کند)، پس طبق قضیّه‌های[1] قبل مجموعهٔ A باید دارای عضو انتها باشد که این عضو انتها همان ب‌م‌م است. درواقع ثابت شد که همواره ب‌م‌م دو عدد صحیح که حدّاقل یکی از آنها مخالف صفر باشد، موجود است.

قضیهٔ 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:

$$I)\ a|a, -a|a \Rightarrow |a||a$$

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

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

$$II)\ \text{فرض کنیم } c>0, c|a, c|b$$

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

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

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

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

$$(p,a) = d \overset{\text{اوّل } P}{\rightarrow} \begin{matrix} d|a \\ d|p \end{matrix} \Rightarrow d = 1 \quad \text{یا} \quad d = p \quad (1)$$

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 $d = 1$.

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

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

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

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

(توجه دارید که عددی عضو A است که دو شرط داشته باشد؛ یکی آن که مثبت باشد و دیگر آن که 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 m. و n.ای در Z باشند، به قسمی که $d = m_0a + n_0b$ (۱).

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

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.)

امّا $r \in A$ با توجه به این که $r < d$ و تعریف عضو ابتدا برای d یک تناقض ایجاد می‌کند (زیرا عضوی از عضو ابتدا کوچکتر نمی‌توانیم 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 $c \le d$.

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

نتیجه‌های حاصل از قضیّهٔ بزو

نتیجهٔ ۱: اگر $(a,b) = d$ آن‌گاه اعدادی صحیح و نسبت به هم اوّل 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 قضیهٔ بزو d عضو ابتدای مجموعهٔ ترکیبهای خطی a و b است، پس باید $d \in A$ و هر عضو A ترکیبی خطی از a و b است. اثبات نسبت‌به هم اوّل بودن ضرایب این ترکیب خطی؛ یعنی r و s را درنتیجهٔ (۴) ملاحظه کنید.

نتیجهٔ 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 $a|d$.

$$(b,c)=d \overset{\text{قضیهٔ بزو}}{\Rightarrow} \exists r,s,\ rb+sc=d$$

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

تذکر مهم: عکس قضیهٔ بزو در حالت کلّی برقرار نمی‌باشد؛ یعنی اگر عددی چون d برابر با ترکیب خطی دو عدد صحیح مانند a و b باشد، نمی‌توان نتیجه گرفت که d ب‌م‌م دو عدد a و b است.

به عنوان مثال $۲۷=۳\times۴+۳\times۵$ ولی $(۵,۳)=۱\neq۲۷$.

نتیجهٔ ۳: عکس قضیهٔ 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 اوّل هستند.

$$ra+sb=۱ \Rightarrow (a,b)=۱$$

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

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

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

نتیجهٔ ۴: اگردو عدد صحیح مانند a و b را بر بزرگترین مقسوم‌علیه مشترکشان تقسیم کنیم، آن‌گاه خارج‌قسمتها نسبت‌به هم اوّل خواهند بود؛ یعنی:

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

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

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

$$r\frac{a}{d}+s\frac{b}{d}=\frac{d}{d} \Rightarrow r\frac{a}{d}+s\frac{b}{d}=۱ \overset{\text{نتیجهٔ ۳}}{\Rightarrow} \left(\frac{a}{d},\frac{b}{d}\right)=۱$$

تذکر مهم: 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 قضیهٔ بزو ضرایب ترکیب خطی که d را می‌سازد، همواره نسبت به هم اوّل هستند!

نتیجهٔ ۵ (لم اقلیدس): هرگاه عددی حاصلضرب دو عدد را بشمارد و نسبت به یکی از آن دو، عدد اوّل باشد، آن‌گاه همواره دیگری را می‌شمارد:

$$a|bc, (a,b)=۱ \Rightarrow a|c$$

اثبات: برای اثبات این که $a|c$ کافی است که ثابت کنیم $c=aq$، پس به دنبال یک تساوی هستیم که یک طرف آن c باشد و طرف دیگر مضرب a باشد:

$$(a,b)=۱ \overset{\text{قضیهٔ بزو}}{\Rightarrow} ra+sb=۱ \Rightarrow rac+sbc=c \qquad (۱)$$

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

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

مسألهٔ مهم: ثابت کنید، اگر a، b، c و d اعداد طبیعی بوده

و $\frac{a}{b}=\frac{c}{d}$ و داشته باشیم $(a,b)=(c,d)=1$، 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 در نتیجه $b=d$ حاصل می‌شود:

(۱) طبق فرض: $ad=bc\Rightarrow a|bc,(a,b)=1\overset{\text{لم اقلیدس}}{\Rightarrow}a|c\Rightarrow a\le c$

(۲) طبق فرض: $ad=bc\Rightarrow c|ad,(c,d)=1\overset{\text{لم اقلیدس}}{\Rightarrow}c|a\Rightarrow c\le a$

(۱) و (۲) $a=c, ad=bc\Rightarrow \not{a}d=\not{a}a\Rightarrow b=d$

تست: اگر a و b دو عدد صحیح و $p|ab$ و $37p-29a=1$، کوچکترین عضو مثبت مجموعهٔ $A=\{mp+nb: m,n\in Z\}$ کدام است؟ (سراسری ۷۵)

۱) b ۲) p

۳) ۱ ۴) ۸

حل: گزینهٔ (۲) صحیح است؛ زیرا با توجه به رابطهٔ $37p-29a=1$ و نتیجهٔ (۳) باید $(p,a)=1$ و چون $p|ab$ پس طبق لم اقلیدس باید $p|b$؛ بنابراین $(p,a)=|p|$ که طبق قضیهٔ بزو $\min A=(p,b)$، پس $\min A=|p|$ که البته در گزینه‌ها باید به جای p عدد $|p|$ به کار می‌رفت!

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

$$b|a, c|a, (b,c)=1\Rightarrow bc|a$$

اثبات: برای اثبات این که، $bc|a$ 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:

$$(b,c)=1\overset{\text{قضیهٔ بزو}}{\Rightarrow}rb+sc=1\overset{\text{دو طرف در a ضرب}}{\Rightarrow}rab+sac=a \qquad (1)$$

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

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

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

تست: عدد k بر دو عدد ۹ و t بخش‌پذیر است، اگر k بر $9t$ نیز بخش‌پذیر باشد، در این صورت t کدام می‌تواند باشد؟

۱) ۳ ۲) ۶

۳) ۴ ۴) ۹

حل: گزینهٔ (۳) صحیح است؛ زیرا طبق نتیجهٔ ۶، باید $(9,t)=1$ که در بین گزینه‌ها فقط $(9,4)=1$.

نتیجهٔ ۷: اگر p عددی اوّل 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 قضیهٔ (۲) باید $(p,a)=1$ و

در نتیجه، بنابر لم اقلیدس، باید $p|b$؛ یعنی:

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

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

نتیجهٔ ۸: اگر $(a,b)=d$ و $k\in N$ در این صورت $(ka,kb)=kd$ و بعکس.

اثبات (شرط لازم):

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

دو شرط بم‌م را برای kd بررسی می‌کنیم:

$$\text{I})\ (a,b)=d\begin{cases}\xrightarrow{d|a}kd|ka\\ \xrightarrow{d|b}kd|kb\end{cases}$$

$$\text{II})\ \text{فرض کنیم } c>0, c|kb\overset{\text{باید ثابت کنیم}}{\Rightarrow}c\le kd$$

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

از طرفی فرض $c|ka, c|kb \Rightarrow c|rka, c|skb \Rightarrow c|rka+skb$ کرده‌ایم

$$\Rightarrow^{(1)} c|kd \Rightarrow c \le kd$$

(شرط کافی):

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

حال دو شرط ب‌م‌م را برای d بررسی می‌کنیم :

$$I)(ka,kb)=kd \begin{cases} kd|ka \Rightarrow d|a \\ kd|kb \Rightarrow d|b \end{cases}$$

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

$$(ka,kb)=kd \overset{\text{قضیهٔ بزو}}{\Rightarrow} rka+skb=kd \Rightarrow ra+sb=d \quad (2)$$

از طرفی فرض $c|a, c|b \Rightarrow c|ra, c|sb \Rightarrow c|ra+sb$ کرده‌ایم

$$\Rightarrow^{(2)} c|d \Rightarrow c \le d$$

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

۱) ۱ ۲) ۲

۳) ۱ یا ۲ ۴) ۱ یا ۲ یا ۴

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

$$\begin{cases} d|a+b \\ d|a-b \end{cases} \Rightarrow \begin{cases} \Rightarrow d|(a+b)+(a-b) \Rightarrow d|2a \\ \Rightarrow d|(a+b)-(a-d) \Rightarrow d|2b \end{cases}$$

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

$$\Rightarrow d=1 \text{ یا } d=2$$

نتیجهٔ ۹: اگر عددی نسبت به دو عدد اوّل باشد، آن‌گاه نسبت به حاصلضرب آن دو عدد نیز اوّل است و بعکس :

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

اثبات (شرط لازم):

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

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

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

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

اثبات (شرط کافی):

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

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

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

۱. هر زیر مجموعهٔ ناتهی Z که از بالا کراندار باشد، دارای عضو اتها است.