نظریه اعداد

اصل خوش ترتیبی: هر زیرمجموعه‌ی غیرتهی از اعداد طبیعی دارای کوچکترین عضو است. این کوچکترین عضو را عضو ابتدا نیز می‌گوییم.

مثال. فرض کنید $S=\{n^2 \mid n\in\mathbb{N}\}$. در این صورت عضو ابتدای S برابر است با ۱. در واقع $S\subseteq\mathbb{N}$ و $S=\{1,4,9,\dots\}\neq\emptyset$.

شهود.

تعریف. فرض کنید $a,b\in\mathbb{Z}$. در این صورت گوییم a عدد b را می‌شمارد (عاد می‌کند) هرگاه $q\in\mathbb{Z}$ چنان موجود باشد که $b=aq$، در چنین حالتی می‌نویسیم $a\mid b$.

و اگر a عدد b را عاد نکند می‌نویسیم $a\nmid b$.

مثال. $-6\mid 3$ چون $3=(-2)(-6)$

$4\nmid 5$ زیرا برای هر $q\in\mathbb{Z}$، $5\neq 4q$.

قضیه. فرض کنید a، b و c اعداد صحیح باشند. در این صورت

الف. اگر $a\mid b$ آنگاه $\pm a\mid \pm b$.

ب. اگر $a\mid b$ و $a\mid c$ آنگاه برای هر $x,y\in\mathbb{Z}$، $a\mid bx+cy$.

ج. همواره $a\mid 0$ و $1\mid b$.

اثبات. (ب)

$$a\mid b \longrightarrow \exists q_1,\ b=aq_1 \longrightarrow bx=axq_1$$

$$a\mid c \longrightarrow \exists q_2,\ c=aq_2 \longrightarrow cy=ayq_2$$

ج: $bx+cy=a(\underbrace{xq_1+yq_2}_{q'\in\mathbb{Z}})=aq'$

بنابراین $a \mid bx+cy$.

اثبات بقیه نیز به سادگی حاصل می‌شود.

تعریف. اگر $x, y \in \mathbb{Z}$ و c و b آنگاه $bx+cy$ یک ترکیب خطی b و c نامیده می‌شود.

قسمت (ب) قضیه‌ی بالا بیان می‌کند که اگر $a \mid b$ و $a \mid c$ آنگاه a هر ترکیب خطی b و c را می‌شمارد.

الگوریتم تقسیم:

قضیه: فرض کنید a و b اعدادی صحیح بوده و $b > 0$. در این صورت اعداد صحیح و یکتای q و r چنان موجودند که $a = bq + r$ و $0 \leqslant r < b$.

اثبات: حالت اول. $b \mid a$. در این صورت $q \in \mathbb{Z}$ موجود است که $a = bq$ بنابراین $a = bq + 0$. یعنی در این قسمت $r = 0$ انتخاب شده است.

حالت دوم. $b \nmid a$. در این صورت برای هر $q \in \mathbb{Z}$، $a - bq \neq 0$. قرار می‌دهیم

$$S = \{a - bq \geqslant 0 \mid q \in \mathbb{Z}\}$$

بوضوح برای هر q صحیح، $a - bq \in \mathbb{Z}$ و بنا به آنچه بیان شد $a - bq \neq 0$. پس اگر $a - bq \in S$ آنگاه لازم است $a - bq > 0$. یعنی $S \subseteq \mathbb{N}$.

می‌خواهیم نشان دهیم $S \neq \emptyset$. برای این منظور قرار می‌دهیم $q = -|a| - 1$. در این صورت:

$$a - bq = a - b(-|a| - 1) = a + |a|b + b \geqslant a + |a| + b > 0$$

بنابراین $S \ni a-bq$ و لذا $S \neq \emptyset$. پس بنا به اصل خوش ترتیبی، S دارای عضو ابتدایی مانند r_0 است.

فرض کنید $r_0 = a-bq_0$. در این صورت $a = bq_0 + r_0$.

واضح است که $r_0 \geq 0$. می خواهیم نشان دهیم $r_0 < b$.

فرض کنید $r_0 \geq b$. در این صورت $r_0 - b \geq 0$ و

$$0 \leq r_0 - b = (a-bq_0) - b = a - b(q_0+1) = a - bq' \in S$$

که q'

از این که r_0 عضو ابتدایی S است لذا $r_0 - b < r_0$. بنابراین $b > 0$ ✗

پس $0 \leq r_0 < b$.

اثبات یکتایی.

فرض کنید $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ چنان موجود باشند که $a = bq_1 + r_1$, $a = bq_2 + r_2$

و $0 \leq r_1 < b$ و $0 \leq r_2 < b$، در این صورت $|r_2 - r_1| < b$.

$a = bq_1 + r_1 = bq_2 + r_2$ بنابراین $bq_2 + r_2 = bq_1 + r_1$ و لذا

$r_1 - r_2 = b(q_1 - q_2)$.

فرض کنید (فرض خلف) $r_2 \neq r_1$. در این صورت $r_1 - r_2 \neq 0$.

از این که $r_1 - r_2 = b(q_1 - q_2)$ نتیجه می شود $b \mid r_1 - r_2$ و لذا $|b| \leq |r_1 - r_2|$

و این تناقض است، پس $r_2 = r_1$ و با جایگذاری در رابطه $bq_2 + r_2 = bq_1 + r_1$

نتیجه می شود $q_1 = q_2$. □

توجه کنید درستی ی قضیه ی بالا از قضیه ی زیر استفاده کرده ایم.

قضیه: اگر $a|b$ و $b\neq 0$ آنگاه $|a|\leq|b|$.

اثبات: زیرا $a|b$ لذا $q\in\mathbb{Z}$ موجود است که $b=aq$ و لذا $|b|=|a||q|$

چنانچه $q=0$ آنگاه $b=aq=0$ که خلف. بنابراین $q\neq 0$ و لذا $|q|\geq 1$

اکنون $|b|=|a||q|\geq|a|$.

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

اثبات: اگر $b=0$ آنگاه از این که $b|a$ نتیجه می شود $a=0$.

مشابه $a=0$ ایجاب می کند $b=0$. که در این حالت $a=\pm b$ برقرار است.

بنابراین فرض می کنیم $a,b\neq 0$، در این صورت:

$$\left.\begin{array}{l} a|b \xrightarrow{b\neq 0} |a|\leq|b| \\ b|a \xrightarrow{a\neq 0} |b|\leq|a| \end{array}\right\} \Rightarrow |a|=|b| \longrightarrow a=\pm b.$$

اعداد صحیح زوج و فرد:

چنانچه در قضیه ی الگوریتم تقسیم قرار دهیم $b=2$ آنگاه برای هر عدد صحیح a، عدد صحیح q چنان موجود است که $a=2q+r$ و $0\leq r<2$ یعنی $r=0$ یا $r=1$

اگر $r=0$ آنگاه $a=2q$ و چنانچه $r=1$ آنگاه $a=2q+1$.

تعریف: هر عدد صحیح به صورت $a=2q$ عددی زوج و هر عدد به شکل $a=2q+1$ عدد فرد نامیده می شود.

مثال: $0=2(0)$. بنابراین صفر عددی زوج است.

مثال. نشان دهید حاصلضرب هر دو عدد متوالی زوج است.

حل. حاصلضرب دو عدد متوالی همواره به صورت $a(a+1)$ است.

دو حالت اتفاق می‌افتد.

الف. $a=2q$، در این حالت

$$a(a+1) = 2q(2q+1) = 2(q(2q+1)) = 2q'$$

زوج

ب. $a=2q+1$، در این حالت q'

$$a(a+1) = (2q+1)(2q+2) = 2(2q+1)(q+1) = 2q''$$

زوج

پس $a(a+1)$ همواره q'' عددی زوج است.

مثال. مربع هر عدد فرد به شکل $8t+1$ است.

حل. فرض کنید a عدد فرد باشد. بنابراین $a=2q+1$، اکنون

$$a^2 = (2q+1)^2 = 4q^2+4q+1 = 4q(q+1)+1 = 8t+1$$

$2t$

توجه کنید $q(q+1)$ حاصلضرب دو عدد متوالی است و بنابه مثال قبل عددی زوج است.

مثال. نشان دهید هر عدد فرد قابل تقسیم به یکی از دو صورت $4q+1$ یا $4q+3$ است.

حل. ابتدا فرض کنید a عددی صحیح باشد. در این صورت بنابه الگوریتم تقسیم

$a=4q+r$ که $0 \le r < 4$. پس a قابل تقسیم به یکی از چهار شکل زیر است،

الف. $a=4q$ ب. $a=4q+1$ ج. $a=4q+2$ د. $a=4q+3$

به راحتی می‌توان دید در حالتهای الف، ج، a عددی زوج و در حالتهای ب و د

a عددی فرد است. بنابراین اگر a فرد باشد یکی از نمایشهای $4q+1$ یا $4q+3$

را خواهد داشت.

مثال، از مجموعه‌ی $A=\{11, 111, 1111, \ldots\}$ چند عدد مربع کامل هستند؟

حل، اعداد 11، 1111، ... را در نظر می‌گیریم و نشان می‌دهیم هیچکدام مربع کامل نیستند، زیرا فرض کنید (فرض خلف) عددی بصورت $11\ldots111$ مربع کامل باشد چون این عدد فرد است، باید بصورت $8t+1$ باشد. یعنی $11\ldots111 = 8t+1$ ولذا $11\ldots110 = 8t$. پس $11\ldots110$ در نتیجه سه رقم سمت راست آن یعنی 110 باید مضربی از 8 باشد که این چنین نیست. پس از اعداد 11، 1111 و ... هیچکدام مربع کامل نیستند. از 2 عدد باقیمانده‌ی مجموعه‌ی A، 1 مربع کامل است و 11 مربع کامل نیست. پس تنها یک عضو از مجموعه‌ی A مربع کامل است.

بزرگترین مقسوم علیه مشترک دو عدد

مثال، بزرگترین مقسوم علیه مشترک 24 و 18 را بدست آورید.

حل.

مقسوم علیه‌های 24 $= \{1, 2, 3, 4, 6, 8, 12, 24\}$

مقسوم علیه‌های 18 $= \{1, 2, 3, 6, 9, 18\}$

مقسوم علیه‌های مشترک 18 و 24 $= \{1, 2, 3, 6\}$

پس بزرگترین مقسوم علیه مشترک 24 و 18 برابر است با 6.

تعریف. فرض کنید a و b دو عدد صحیح و نه هر دو صفر باشند. در این صورت $d \geq 1$ را بزرگترین مقسوم علیه مشترک a و b می‌گوییم هرگاه:

الف. $d|a$ و $d|b$

ب. اگر $e|a$ و $e|b$ آنگاه $e \leq d$.

در چنین حالتی می‌نویسیم $d = (a, b)$.

مثال. نشان دهید مربع هر عدد فرد به شکل $8t+1$ است.

حل. این مثال را قبلاً حل کردیم. اکنون آن را به روشی دیگر حل می‌کنیم.

فرض کنید a عددی فرد باشد، بنابراین مثال قبل a دارای یکی از دو حالت زیر است:

الف. $a=4q+1$ یا ب) $a=4q+3$.

چنانچه حالت الف رخ دهد:

$$a^2=(4q+1)^2=\underbrace{16q^2+8q}_{8t}+1=8t+1$$

و اگر حالت ب اتفاق بیفتد:

$$a^2=(4q+3)^2=16q^2+24q+9=\underbrace{16q^2+24q+8}_{8t}+1=8t+1$$

مثال. نشان دهید $8t$ اعدادی بر ۴ بخش پذیرند که دو رقم سمت راست آنها بر ۴ بخش پذیر باشد.

حل. قرارداد می‌کنیم که اگر a و b دو عدد صحیح نامنفی باشند آنگاه منظور از $\overline{ab}$ عددی است دو رقمی که رقم یکان آن b و رقم دهگان آن a است.

اینک فرض کنید x عددی بصورت $x=\overline{a\cdots bcd}$ باشد. در این صورت:

$$x=\overline{a\cdots bcd}=\overline{a\cdots boo}+\overline{cd}$$
$$=100\,\overline{a\cdots b}+\overline{cd}$$

حال از این که $100\,\overline{a\cdots b}$ بر ۴ بخش پذیر است لذا $x=\overline{a\cdots bcd}$ بر ۴ بخش پذیر است اگر و تنها اگر $\overline{cd}$ بر ۴ بخش پذیر باشد.

تمرین. نشان دهید اعدادی بر ۸ بخش پذیرند که سه رقم سمت راست آنها بر ۸ بخش پذیر باشد.

قضیه. اگر a و b هر دو هم‌زمان صفر نباشند، آنگاه بزرگترین مقسوم علیه مشترک a و b موجود و یکتاست.

اثبات. قرار می‌دهیم $S=\{ax+by>0 \mid x,y\in\mathbb{Z}\}$

با انتخاب $x=a$ و $y=b$ داریم $ax+by=a^2+b^2>0$ و چون a و b هم‌زمان صفر نیستند لذا $S\neq\emptyset$، یعنی $ax+by=a^2+b^2>0$. بوضوح $S\subseteq\mathbb{N}$ و بنا به اصل خوش‌ترتیبی، S دارای عضو ابتداست، عضو ابتدای S را d می‌گیریم و نشان می‌دهیم $d=(a,b)$.

از این‌که $d\in S$ لذا x_0 و y_0 صحیح موجودند که $d=ax_0+by_0$.

الف. $d\mid a$. برای اثبات فرض کنید $a=dq+r$ که $r=0$ یا $0<r<d$. می‌خواهیم نشان دهیم $r=0$. فرض کنید چنین نباشد. بنابراین $0<r<d$. اکنون

$$0<r=a-dq=a-(ax_0+by_0)q$$
$$=a\underbrace{(1-x_0q)}_{x'}+b\underbrace{(-y_0q)}_{y'}=ax'+by'\in S$$

حال از این‌که d عضو ابتدای S است و $r\in S$ لذا $r\geq d$ که $r<d$ پس $r=0$ و لذا $a=dq$. یعنی $d\mid a$، بطور مشابه $d\mid b$.

ب. حال فرض کنید $e\mid a$ و $e\mid b$. در این صورت با استفاده از قضیه‌ای از قبل، $e\mid ax_0+by_0=d$ و لذا $e\leq d$.

پس $d=(a,b)$.

اثبات یکتایی. فرض کنید d و d'، بزرگترین مقسوم علیه‌های مشترک a و b باشند

d بزرگترین مقسوم علیه مشترک a و b است، $d' \mid a$ ، $d' \mid b$ و لذا بنابه تعریف، $d' \le d$.

حال اگر d' را بزرگترین مقسوم علیه مشترک a و b بگیریم از اینکه $d \mid a$ و $d \mid b$ بطور مشابه نتیجه میشود $d \le d'$، پس $d = d'$ و لذا ب.م.م یکتاست.

نتیجه. اگر $d = (a,b)$ آنگاه $x_0, y_0 \in \mathbb{Z}$ چنان موجودند که $d = ax_0 + by_0$.

اثبات. از اینکه $d = \min S \in S$ لذا $x_0, y_0 \in \mathbb{Z}$ موجودند که $d = ax_0 + by_0$.

مسأله. فرض کنید $d = (a,b)$. در اینصورت:

الف. اگر $m > 0$، در اینصورت $(ma, mb) = md$.

ب. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

اثبات. الف. از اینکه $d = (a,b)$ لذا $x_0, y_0 \in \mathbb{Z}$ موجودند که $d = ax_0 + by_0$،

$d \mid a$ بنابراین $md \mid ma$. مشابها $md \mid mb$،

اکنون فرض کنید $e \mid ma$، $e \mid mb$ در اینصورت e هر ترکیب خطی ma و mb را میگیرد بخصوص $e \mid max_0 + mby_0 = m(ax_0 + by_0) = md$

بنابراین $e \le md$ و لذا $(ma, mb) = md$!

ب) $ax_0 + by_0 = d \rightarrow \frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$

چنانچه $d' = \left(\frac{a}{d}, \frac{b}{d}\right)$ آنگاه

$$\left.\begin{matrix} d' \mid \frac{a}{d} \\ d' \mid \frac{b}{d} \end{matrix}\right\} \rightarrow d' \mid \frac{a}{d}x_0 + \frac{b}{d}y_0 = 1 \longrightarrow d' = 1$$

بنابراین $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

تعریف: اعداد a و b را نسبت به هم اول گوییم هرگاه $(a,b)=1$.

توجه۱: اگر $(a,b)=d$ آنگاه $x_0, y_0 \in \mathbb{Z}$ چنان موجودند که $ax_0+by_0=d$. اما عکس این حکم لزوماً برقرار نیست، بعنوان مثال، $2(5)+3(10)=40$ درحالیکه $(2,3)\neq 40$.

اما صحیح $ax_0+by_0=1$ آنگاه $(a,b)=1$.

زیرا اگر $(a,b)=d'$ آنگاه از این که $d'|a$ و $d'|b$، لذا $d'|ax_0+by_0=1$ و بنابراین $d'=1$.

توجه۲. چنانچه $(a,b)=d$ و $x_0,y_0\in\mathbb{Z}$ چنان باشند که $ax_0+by_0=d$ آنگاه $(x_0,y_0)=1$. زیرا از $ax_0+by_0=d$ نتیجه می‌شود $\frac{a}{d}x_0+\frac{b}{d}y_0=1$. حال از این که ترکیبی خطی از x_0 و y_0 برابر ۱ شده است لذا $(x_0,y_0)=1$.

کوچکترین مضرب مشترک دو عدد

تعریف: فرض کنید a و b دو عدد غیرصفر باشند. در این صورت c را کوچکترین مضرب مشترک a و b گوییم هرگاه

الف. $a|c$ و $b|c$.

ب. اگر $a|x$ و $b|x$ آنگاه $c\leq x$.

در چنین حالتی می‌نویسیم $c=[a,b]$.

توجه: اگر $A=\{$مضرب $a\}$ و $B=\{$مضرب $b\}$ و $C=A\cap B$ آنگاه بوضوح $C\subseteq\mathbb{N}$. از طرفی $ab\in A\cap B=C$ بنابراین $C\neq\emptyset$.

لذا بنابر اصل خوش‌ترتیبی C دارای عضو ابتدا مانند c است. واضح است که $c=[a,b]$،

قضیه: اگر $a,b\in\mathbb{N}$، $d=(a,b)$ و $c=[a,b]$ آنگاه $c=\frac{ab}{d}$.

اثبات: کافی است ثابت کنیم $[a,b]=\frac{ab}{d}$. برای این منظور:

$$①\begin{cases}\frac{ab}{d}=a\left(\frac{b}{d}\right)\longrightarrow a\mid\frac{ab}{d}\\ \frac{ab}{d}=b\left(\frac{a}{d}\right)\longrightarrow b\mid\frac{ab}{d}\end{cases}\quad \left(\frac{b}{d},\frac{a}{d}\in\mathbb{Z}\right)$$

اکنون فرض کنید $a\mid x$ و $b\mid x$ در این صورت $\frac{a}{d}\mid\frac{x}{d}$ و $\frac{b}{d}\mid\frac{x}{d}$.

حال از این که $\left(\frac{a}{d},\frac{b}{d}\right)=1$ لذا $\frac{a}{d}\frac{b}{d}\mid\frac{x}{d}$. با ضرب طرفین رابطه‌ی اخیر در d خواهیم داشت $\frac{ab}{d}\mid x$ یعنی $\frac{ab}{d}\le x$. ②

روابط ① و ② نتیجه می‌دهند $[a,b]=\frac{ab}{d}$.

روشی برای محاسبه‌ی ب.م.م دو عدد.

قضیه: فرض کنید $a,b\in\mathbb{N}$، اگر $a=bq+r$ آنگاه $(a,b)=(b,r)$.

اثبات: فرض کنید $d=(a,b)$ و $d'=(b,r)$.

$$(a,b)=d\longrightarrow\begin{cases}d\mid a\\ d\mid b\end{cases}\Rightarrow d\mid a-bq=r$$

از این که $d\mid b$ و $d\mid r$ لذا $d\mid(b,r)=d'$. ①

$$(b,r)=d'\longrightarrow\begin{cases}d'\mid b\\ d'\mid r\end{cases}\Rightarrow d'\mid bq+r=a$$

از اینکه $d'\mid a$ و $d'\mid b$ لذا $d'\mid(a,b)=d$ ②

از روابط ① و ② نتیجه می‌شود $d'=d$ یعنی $(a,b)=(b,r)$.

توجه: با استفاده از قضیه‌ی بالا و با تقسیمات متوالی می‌توان بزرگترین مقسوم علیه مشترک دو عدد a و b را محاسبه کرد. بدین صورت که:

$$a = bq_0 + r_0 \qquad 0 \le r_0 < b$$
$$b = r_0 q_1 + r_1 \qquad 0 \le r_1 < r_0$$
$$r_0 = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

باتوجه به این که $b > r_0 > r_1 > r_2 > \cdots \ge 0$ لذا n ای موجود است که $r_n = 0$. آنگاه:

$$(a,b) = (b,r_0) = (r_0,r_1) = \cdots = (r_{n-1},r_n) = r_{n-1}$$

این روش را در دوره ی راهنمایی به روش تزیانی می شناختیم.

لم اقلیدس:

قضیه: فرض کنید a و b و c سه عدد صحیح باشند. اگر $a \mid bc$ و $(a,b)=1$ آنگاه $a \mid c$.

اثبات: $(a,b)=1$ بنابراین $x,y \in \mathbb{Z}$ موجودند که $ax+by=1$. بنابراین $acx+bcy=c$. از این که $a \mid acx$ و $a \mid bcy$ لذا $a \mid acx+bcy=c$.

حل معادله ی سیاله ی $ax+by=c$

یک معادله ی سیاله، معادله ای است با ضرایب صحیح و هدف از حل معادله ی سیاله، یافتن جواب یا جواب های صحیح آن است.

مثال: $2x+3y=7$ یک معادله ی سیاله و $(x,y)=(2,1)$ یک جواب آن است.

قضیه. معادله‌ی سیاله‌ای $ax+by=c$ دارای جواب است، اگر و تنها اگر $(a,b) \mid c$.

اثبات. ابتدا فرض می‌کنیم معادله‌ی $ax+by=c$ دارای جواب (x_0,y_0) باشد. $d=(a,b)$ قرار می‌دهیم. $ax_0+by_0=c$. در این صورت

$$\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Longrightarrow d \mid ax_0+by_0=c$$

برعکس: فرض کنید $d=(a,b) \mid c$. در این صورت $q \in \mathbb{Z}$ موجود است که $c=dq$. از آن‌جا که $d=(a,b)$ لذا $x',y' \in \mathbb{Z}$ موجودند که $d=ax'+by'$، بنابراین $c=dq=ax'q+by'q$. پس معادله‌ی $ax+by=c$ دارای جواب $(x'q,y'q)$ است. □

برای بدست آوردن جوابی از معادله‌ی $ax+by=c$ کافی است ابتدا جوابی از $ax+by=d$ را بدست آوریم و سپس طرفین معادله را در مقدار مناسب ضرب کرده و جوابی برای $ax+by=c$ بدست آوریم.

برای محاسبه‌ی جواب $ax+by=d$ می‌توان از تقسیمات متوالی استفاده کرد.

مثال. جوابی برای معادله‌ی $۲۹۵x+۷۸۹y=۴$ بدست آورید.

حل. ابتدا جوابی برای $۲۹۵x+۷۸۹y=۱$ بدست می‌آوریم. توجه کنید $(۷۸۹,۲۹۵)=۱$

		۱	۷	۲	۱	۱	۵	۱	۲	
۷۸۹	۴۹۵	۹۴	۳۷	۲۰	۱۷	۳	۲	۱	۰	
۴۹۵	۹۵۸	۷۴	۲۰	۱۷	۱۸	۲	۲			

$$۷۸۹ = ۴۹۵(۱) + ۹۴ \rightarrow ۹۴ = ۷۸۹ + ۴۹۵(-۱)$$

$$۳۷ = ۹۴(۷) + ۲۰ \rightarrow ۲۰ = ۳۷ + ۹۴(-۷)$$

$$= ۷۸۹(-۷) + ۴۹۵(۸)$$

۹۴ = ۳۷(۲) + ۲۰ ⟶ ۲۰ = ۹۴ + ۳۷(−۲)

= (۷۸۹ + ۶۹۵(−۱)) + (۷۸۹(−۷) + ۶۹۵(۸))(−۲)

= ۷۸۹(۱۵) + ۶۹۵(−۱۷)

۳۷ = ۲۰(۱) + ۱۷ ⟶ ۱۷ = ۳۷ + ۲۰(−۱)

= (۷۸۹(−۷) + ۶۹۵(۸)) + (۷۸۹(۱۵) + ۶۹۵(−۱۷))(−۱)

= ۷۸۹(−۲۲) + ۶۹۵(۲۵)

۲۰ = ۱۷(۱) + ۳ ⟶ ۳ = ۲۰ + ۱۷(−۱)

= (۷۸۹(۱۵) + ۶۹۵(−۱۷)) + (۷۸۹(−۲۲) + ۶۹۵(۲۵))(−۱)

= ۷۸۹(۳۷) + ۶۹۵(−۴۲)

۱۷ = ۳(۵) + ۲ ⟶ ۲ = ۱۷ + ۳(−۵)

= (۷۸۹(−۲۲) + ۶۹۵(۲۵)) + (۷۸۹(۳۷) + ۶۹۵(−۴۲))(−۵)

= ۷۸۹(−۲۰۷) + ۶۹۵(۲۳۵)

۳ = ۲(۱) + ۱ ⟶ ۱ = ۳ + ۲(−۱)

= (۷۸۹(۳۷) + ۶۹۵(−۴۲)) + (۷۸۹(−۲۰۷) + ۶۹۵(۲۳۵))(−۱)

= ۷۸۹(۲۴۴) + ۶۹۵(−۲۷۷)

پس: ۷۸۹(۲۴۴) + ۶۹۵(−۲۷۷) = ۱

و با ضرب طرفین در ۴، ۷۸۹(۹۷۶) + ۶۹۵(−۱۱۰۸) = ۴

(۹۷۶ ↓ y ، −۱۱۰۸ ↓ x)

در قضیه زیر نشان می‌دهیم که با داشتن جوابی خاص از معادله‌ی $ax+by=c$ ، می‌توان تمام جواب‌ها را به دست آورد.

قضیه. فرض کنید (x_0, y_0) جوابی خاص از معادله‌ی $ax+by=c$ باشد. در این صورت

الف. جوابی از معادله است به صورت $\begin{cases} x = x_0 + \frac{kb}{d} \\ y = y_0 - \frac{ka}{d} \end{cases}$ $(k \in \mathbb{Z})$ که در آن $d = (a, b)$.

ب. هر جواب معادله به صورت جواب ارائه شده در قسمت الف است.

اثبات. الف) کافی است x و y را جایگذاری کنیم. در این صورت

$$ax+by = a\left(x_0 + \frac{kb}{d}\right) + b\left(y_0 - \frac{ka}{d}\right)$$
$$= ax_0 + by_0 = c$$

ب) فرض کنید (x, y) جوابی دلخواه از معادله باشد. در این صورت

$$ax+by = c = ax_0 + by_0$$
$$\rightarrow ax+by = ax_0 + by_0$$
$$\rightarrow a(x - x_0) = b(y_0 - y)$$
$$\rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

چون $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$ لذا $\frac{b}{d} \mid (y_0 - y)$. اما $(\frac{a}{d}, \frac{b}{d}) = 1$ لذا بنا به لم اقلیدس $\frac{b}{d} \mid x - x_0$ و بنابراین $k \in \mathbb{Z}$ موجود است که $x - x_0 = \frac{kb}{d}$ و در نتیجه $x = x_0 + \frac{kb}{d}$.

با جایگذاری $x = x_0 + \frac{kb}{d}$ در رابطه‌ی $ax+by=ax_0+by_0$ به دست می‌آید $y = y_0 - \frac{ka}{d}$.

پس جواب معادله به شکل $\begin{cases} x = x_0 + \frac{kb}{d} \\ y = y_0 - \frac{ka}{d} \end{cases}$ $(k \in \mathbb{Z})$ است.

مسأله. فرض کنید قیمت یک گاو ۵ تومان، یک گوسفند ۲ تومان و یک بزغاله ۱ ریال باشد. اگر با ۱۰۰ تومان دقیقاً ۱۰۰ حیوان از حیوانات بالا خریداری کنیم، حساب کنید از هر حیوان به چه تعداد خریده ایم.

حل. تمرین

مسأله (نارگیل‌ها) ۵ دزد در جزیره‌ای تعدادی نارگیل چیدند. هنگام تقسیم شب یکی از دزدها نارگیل‌ها را به ۵ قسمت مساوی تقسیم کرد و یک نارگیل اضافی را دور انداخت و سهم خود را برداشت. نفر دوم نیز با تمام نارگیل‌ها چنین کاری را انجام داد و به همین صورت نفرات سوم، چهارم و پنجم این روند را انجام دادند. تعداد نارگیل‌ها حداقل چقدر بوده است؟

اعداد اول

تعریف، عدد صحیح $p>1$ را اول گوئیم هرگاه تنها مقسوم علیه‌های مثبت آن ۱ و p باشند.

مثال، تنها عوامل مثبت ۳۷، ۱ و خود ۳۷ می‌باشد. پس ۳۷ عددی اول است.

مسأله، اگر p عددی اول باشد و $p\nmid a$ آنگاه $(p,a)=1$.

حل. قرار می‌دهیم $(p,a)=d$،

اگر $d\neq 1$ (فرض خلف) بنا به تعریف، $d\mid p$ و $d\mid a$. از اینکه p اول است و $d\neq 1$ لذا $d=p$. اینک از $d\mid a$ نتیجه می‌شود $p\mid a$ ✗.

بنابراین $d=1$. یعنی $(p,a)=1$.

لم. اگر p عددی اول باشد بطوریکه $p\mid ab$ در اینصورت $p\mid a$ یا $p\mid b$.

اثبات، اگر $p\mid a$ که مسأله حل است. در غیر اینصورت $(p\nmid a)$ بنا به مسأله‌ی بالا $(p,a)=1$ و لذا بنا به لم اقلیدس، $p\mid b$.

نتیجه. اگر p عددی اول باشد و $p\mid a_1a_2\cdots a_n$ آنگاه $p\mid a_i$ برای یک i.

قضیه. هر عدد صحیح $n>1$، بطور یکتا، قابل نمایش بصورت حاصلضرب اعداد اول است.

اثبات. فرض کنید چنین نباشد. (فرض خلف) بنابراین $n>1$ موجود است که قابل نمایش بصورت حاصلضرب اعداد اول نیست. قرار می‌دهیم

$S = \{n>1 \mid n$ قابل نمایش بصورت حاصلضرب اعداد اول نیست$\}$

بنابه فرض $S \neq \emptyset$ و بوضوح $S \subseteq \mathbb{N}$ ولذا بنابه اصل خوش ترتیبی دارای عضو ابتدائی مانند n_0 است. پس $n_0>1$. از طرفی چون هر عدد اول در واقع نمایشی از حاصلضرب اعداد اول است و $n_0 \in S$، لذا n_0 اول نیست. بنابراین $1<a,b<n_0$ چنان موجودند که $n_0=ab$.

از اینکه $1<a,b<n_0$ لذا $a,b \notin S$ و بنابه تعریف S، اعداد اول $p_1, \dots, p_r$ و $p'_1, \dots, p'_s$ چنان موجودند که

$$a = p_1 p_2 \cdots p_r$$
$$b = p'_1 p'_2 \cdots p'_s$$

و در نتیجه $n_0 = ab = p_1 \cdots p_r p'_1 \cdots p'_s$ که یک تناقض است.

پس هر عدد طبیعی $n>1$، قابل نمایش بصورت حاصلضرب اعداد اول است.

اثبات یکتایی. فرض کنید $n = p_1 p_2 \cdots p_r$ و $n = q_1 q_2 \cdots q_s$ نمایشهای n بصورت حاصلضرب اعداد اول باشند. بنابراین $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

و لذا $p_1 \mid q_1 q_2 \cdots q_s$ و بنابه نتیجه‌ی قضیه‌ی قبل، $p_1 \mid q_1$ یا $p_1 \mid q_2 \cdots q_s$. با یک تجدید اندیس گذاری می‌توان فرض کرد $p_1 \mid q_1$ و چون q_1 اول است لذا $p_1 = 1$ یا $p_1 = q_1$. اما p_1 نیز اول است. پس $p_1 \neq 1$ و لذا $p_1 = q_1$.

حال با حذف $p_1 = q_1$ از طرفین تساوی $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ و ادامه‌ی این روند،

نتیجه می‌شود $p_1 = q_1$ ، ... ، و $p_r = q_s$. (توجه کنید که $r=s$ نیز نتیجه می‌شود)

تعریف. عدد صحیح $n>1$ را مرکب گوییم هرگاه اول نباشد.

مثال. ۶ عددی مرکب است.

رخنه در اعداد اول.

مسأله. برای هر عدد طبیعی n ، n عدد متوالی مرکب موجود است.

اثبات. به راحتی می‌توان دید n عدد زیر همگی مرکب اند.

$$(n+1)!+2,\ (n+1)!+3,\ \dots,\ (n+1)!+(n+1)$$

قضیه. اگر n عددی مرکب باشد آنگاه شامل عاملی نابیشتر از $\sqrt{n}$ است.

اثبات. فرض کنید n مرکب باشد. در این صورت $1<a,b<n$ موجودند که $n=ab$. می‌توان فرض کرد $a \leqslant b$. در این صورت

$$a^2 \leqslant ab = n \longrightarrow a \leqslant \sqrt{n}. \ \square$$

نتیجه. اگر $n>1$ شامل هیچ مقسوم علیه کوچکتر یا مساوی $\sqrt{n}$ نباشد، اول خواهد بود.

مثال. ۱۲۷ اول است یا مرکب؟

حل. کافی است در بین اعداد اول نابیشتر از $11 = [\sqrt{127}]$ جستجو کنیم. به راحتی می‌توان دید هیچکدام از اعداد ۲، ۳، ۵، ۷ و ۱۱ عدد ۱۲۷ را نمی‌شمارند. پس ۱۲۷ عددی اول است.

قضیه. مجموعه‌ی اعداد اول نامتناهی است.

اثبات. فرض کنید مجموعه‌ی اعداد اول متناهی باشد و آن را $\{p_1, p_2, \dots, p_k\}$ بگیرید. قرار می‌دهیم $a = p_1p_2\dots p_k + 1$. در این صورت بنا به قضیه‌ی اساسی، a دارای عاملی اول است و لذا برای یک j ، $p_j \mid a$. اکنون

$p_j \mid a = p_1 p_2 \cdots p_k + 1$

از طرفی $p_j \mid p_1 \cdots p_j \cdots p_k \Rightarrow p_j \mid$ تفاضل $= 1 \longrightarrow p_j = 1$ ✗

پس مجموعه اعداد اول نامتناهی است.

تمرین. نشان دهید مجموعه‌ی اعداد اول به صورت $4k+3$ نامتناهی است.

همنهشتی

تعریف. گوئیم a و b در پیمانه‌ی n همنهشت‌اند هرگاه $n \mid a-b$. در این صورت می‌نویسیم $a \overset{n}{\equiv} b$ یا $a \equiv b \pmod{n}$.

مثال. $23 \overset{7}{\equiv} 9$ چون $7 \mid 14 = 23 - 9$.

قضیه. فرض کنید n عددی صحیح باشد. در این صورت:

الف. برای هر a، $a \overset{n}{\equiv} a$.

ب. اگر $a \overset{n}{\equiv} b$ آنگاه $b \overset{n}{\equiv} a$.

ج. اگر $a \overset{n}{\equiv} b$، $b \overset{n}{\equiv} c$، آنگاه $a \overset{n}{\equiv} c$.

اثبات ج)

$$a \overset{n}{\equiv} b \longrightarrow n \mid a-b$$
$$b \overset{n}{\equiv} c \longrightarrow n \mid b-c$$
$$\Rightarrow n \mid \text{مجموع} = a-c$$
$$\longrightarrow a \overset{n}{\equiv} c$$

اثبات دو مورد دیگر به عنوان آسان‌ترین واگذار می‌شود.

توجه کنید، قضیه بالا بیان می‌کند که رابطه‌ی همنهشتی در پیمانه‌ی n، یک رابطه‌ی هم‌ارزی است.

خواص مقدماتی همنهشتی.

الف. اگر $a \overset{n}{\equiv} b$ آنگاه برای هر c، $a+c \overset{n}{\equiv} b+c$.

دلیل:

$$a \overset{n}{\equiv} b \longrightarrow n \mid a-b \longrightarrow n \mid (a+c)-(b+c) \longrightarrow a+c \overset{n}{\equiv} b+c$$

ب. اگر $a \overset{n}{\equiv} b$ آنگاه برای هر c، $ac \overset{n}{\equiv} bc$.

دلیل. $a \overset{n}{\equiv} b \to n \mid a-b \to n \mid (a-b)c = ac-bc \to ac \overset{n}{\equiv} bc$

ج. اگر $a \overset{n}{\equiv} b$ و $c \overset{n}{\equiv} d$ آنگاه $a+c \overset{n}{\equiv} b+d$.

دلیل.
$$\left.\begin{array}{l} a \overset{n}{\equiv} b \to n \mid a-b \\ c \overset{n}{\equiv} d \to n \mid c-d \end{array}\right\} \Rightarrow n \mid \text{مجموع} = (a+c)-(b+d)$$
$$\to a+c \overset{n}{\equiv} b+d$$

د. اگر $a \overset{n}{\equiv} b$ ، $c \overset{d}{\equiv} n$ آنگاه $ac \overset{n}{\equiv} bd$،

دلیل.
$$\left.\begin{array}{l} a \overset{n}{\equiv} b \xrightarrow{\times c} ac \overset{n}{\equiv} bc \\ c \overset{n}{\equiv} d \xrightarrow{\times b} bc \overset{n}{\equiv} bd \end{array}\right\} \xrightarrow{\text{تعدی}} ac \overset{n}{\equiv} bd$$

با استفاده از قسمت قبل و با استقرا می‌توان نشان داد:

هـ. اگر $a_1 \overset{n}{\equiv} b_1$، ... و $a_k \overset{n}{\equiv} b_k$ آنگاه $a_1 \dots a_k \overset{n}{\equiv} b_1 \dots b_k$،

همچنین به عنوان نتیجه‌ای از هـ. ثابت می‌شود:

و. اگر $a \overset{n}{\equiv} b$ آنگاه برای هر عدد طبیعی k، $a^k \overset{n}{\equiv} b^k$. □

نکته. فرض کنید a عددی صحیح و b عددی طبیعی باشد. در این صورت بنا به الگوریتم تقسیم، q و r موجودند که $a = bq + r$ که در آن $0 \le r < b$. بنابراین $b \mid bq = a - r$ و لذا $a \overset{b}{\equiv} r$.

پس برای محاسبه‌ی باقیمانده‌ی تقسیم a بر b، عدد r با $0 \le r < b$ را چنان یافت که $a \overset{b}{\equiv} r$.

مثال. باقیمانده‌ی تقسیم 30^{50} بر ۱۳ را به دست آورید.

حل. (روش اول) توجه کنید که توان‌های ۳ در پیمانه‌ی ۱۳ می‌باشند:

$$3^2 = 9 \equiv -4 \xrightarrow{\uparrow 2} 3^4 \equiv (-4)^2 = 16 \equiv 3$$

$\xrightarrow{\uparrow 2} 3^8 \equiv 3^2 = 9 \equiv -4 \xrightarrow{\uparrow 2} 3^{16} \equiv (-4)^2 = 16 \equiv 3$

$\xrightarrow{\uparrow 2} 3^{32} \equiv 3^2 = 9 \equiv -4$

اکنون: $3^{50} = 3^{32} \times 3^{16} \times 3^2 \equiv (-4)(3)(-4) = 48 \equiv 9$

بنابراین باقیمانده‌ی تقسیم 3^{50} بر 13 برابر است با 9.

(روش دوم) $3^4 = 27 \equiv 1 \xrightarrow{\uparrow 16} 3^{48} \equiv 1 \xrightarrow{\times 3^2} 3^{50} = 9$

دستگاه کامل مانده‌ها

همان طور که قبلاً نیز بیان شد، برای هر عدد صحیح a و هر عدد طبیعی n، $0 \le r < n$ چنان موجود است که $a = nq + r$ و در نتیجه $a \equiv r$.

به عبارت دیگر هر عدد صحیح a در پیمانه‌ی n، دقیقاً با یکی از اعداد $\{0, 1, \dots, n-1\}$ همنهشت است. مجموعه‌ی $\{0, 1, \dots, n-1\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی n است.

تعریف. فرض کنید $n \in \mathbb{N}$. مجموعه‌ی $\{r_1, r_2, \dots, r_n\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی n نامیده می‌شود هرگاه هر عدد صحیح دقیقاً به یکی از r_i ها در پیمانه‌ی n همنهشت باشد.

مثال: $\{9, \dots, 0\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی 10 می‌باشد.

همچنین $\{10, 9, -2, 7, 16, 35, 6, -7, 21, 2, 0\}$ نیز یک دستگاه کامل مانده‌ها در پیمانه‌ی 10 است.

مثال. اگر $n = 2k+1$ آنگاه $\{k, \dots, -k\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی n است و اگر $n = 2k$ آنگاه $\{k, \dots, -k+1\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی n است.

در بسیاری مواقع استفاده از دستگاه مختصات انتخابی، محاسبات را ساده‌تر می‌کند.

قضیه: فرض کنید $\{r_1, \dots, r_k\}$ و $\{s_1, \dots, s_t\}$ دو دستگاه کامل مانده‌ها در پیمانه‌ی n باشند. در این صورت $k=t$.

اثبات: با در نظر گرفتن r_i به عنوان عددی صحیح، دقیقاً با یکی از s_jها، مثلاً s_j، همنهشت است. می‌توان فرض کرد $j=1$، پس $r_1 \equiv_n s_1$.

به همین صورت با یکی از s_2ها همنهشت است. واضح است که $s_1 \neq s_2$. زیرا اگر $r_1 \equiv_n s_1$ با توجه به این که $s_1 \equiv_n r_1$، آنگاه عدد صحیح r_1 با r_2 در پیمانه‌ی n همنهشت است که تناقض است. پس $s_1 \neq s_2$.

به همین شکل برای هر $1 \leq i \leq k$، دقیقاً یک $1 \leq j \leq t$ موجود است که $r_i \equiv_n s_j$ و این بدین معنی است که $k \leq t$.

به طور مشابه $t \leq k$، لذا $k=t$.

نتیجه: در هفتمین پیمانه‌ی n، هر دستگاه کامل مانده‌ای دقیقاً از مرتبه‌ی n است.

اثبات: فرض کنید $\{r_1, \dots, r_k\}$ یک دستگاه کامل مانده‌ای در پیمانه‌ی n باشد. همچنین می‌دانیم $\{1-n, \dots, 0\}$ یک دستگاه کامل مانده‌ای (با مرتبه‌ی n) است. پس $k=n$.

وجود یا عدم وجود جواب‌های معادله‌ی $f(x,y)=0$.

$f(x,y)$ را چندجمله‌ای با ضرایب صحیح و متغیرهای x و y در نظر می‌گیریم. منظور از حل معادله‌ی $f(x,y)=0$، یافتن مقادیر صحیح x_0 و y_0 است که در آن $f(x_0,y_0)=0$.

قضیه: اگر $f(x,y)=0$ دارای جواب باشد آنگاه برای هر n، $f(x,y) \equiv_n 0$ نیز دارای جواب است.

اثبات: فرض کنید (x_0, y_0) جوابی برای $f(x,y)=0$ باشد. بنابراین $f(x_0,y_0)=0$.

اکنون برای هر n، $n|0=f(x_0,y_0)$ و لذا $f(x_0,y_0) \overset{n}{\equiv} 0$. پس (x_0,y_0) جواب معادله‌ی همنهشتی $f(x,y) \overset{n}{\equiv} 0$ است.

نتیجه. اگر برای یک n، $f(x,y) \overset{n}{\equiv} 0$ دارای جواب نباشد آنگاه $f(x,y)=0$ جواب ندارد.

مثال. معادله‌ی $x^2-4y^2-2=0$ را حل کنید.

حل. قرار می‌دهیم $f(x,y)=x^2-4y^2-2$ و پیمانه‌ی ۴ را در نظر می‌گیریم.

$$f(x,y)=x^2-4y^2-2 \overset{4}{\equiv} x^2-2$$

با انتخاب دستگاه کامل مانده‌ی $\{0,1,2,3\}$ در پیمانه‌ی ۴ می‌توان دید $x^2-2 \overset{4}{\equiv} 0$ دارای جواب نیست و لذا بنا به نتیجه‌ی قضیه‌ی بالا، $x^2-4y^2-2=0$ جواب ندارد.

عکس حسابی در یک پیمانه

تعریف. a^* را وارون حسابی a در پیمانه‌ی n گوئیم هرگاه $a^*a \overset{n}{\equiv} 1$.

مثال. در پیمانه‌ی ۷، $2\times4 \overset{7}{\equiv} 1$. بنابراین ۴ وارون حسابی ۲ در پیمانه‌ی ۷ است.

قضیه. فرض کنید n عددی طبیعی باشد. در این صورت عکس حسابی a به پیمانه‌ی n موجود است اگر و تنها اگر $(a,n)=1$. بعلاوه اگر عکس حسابی موجود باشد آنگاه این عکس در حد همنهشتی یکتاست.

اثبات. ابتدا فرض کنید عکس حسابی a در پیمانه‌ی n موجود باشد. اگر عکس a را a' بگیریم آنگاه $aa' \overset{n}{\equiv} 1$ و لذا $n|aa'-1$ و در نتیجه عدد صحیح q موجود است که $aa'-1=nq$. بنابراین $aa'-nq=1$ و لذا $(a,n)=1$.

برعکس. فرض کنید $(a,n)=1$. در این صورت $x,y\in\mathbb{Z}$ موجودند که $ax+ny=1$. بنابراین $n|ax-1$ و لذا $ax \overset{n}{\equiv} 1$. بنابراین x عکس حسابی a در پیمانه‌ی n است.

حال فرض کنید a' و a'' عکس های a در پیمانه‌ی n باشند.

در این صورت $aa' \overset{n}{\equiv} 1$ و $aa'' \overset{n}{\equiv} 1$.

$aa' \equiv 1 \times a'' \rightarrow a''aa' \overset{n}{\equiv} a'' \rightarrow a' \overset{n}{\equiv} a''$.

از این پس عکس های a در پیمانه‌ی n (در صورت وجود) با a^{-1} نشان داده می‌شود.

سئوال. آیا طرفین یک رابطه همنهشتی را می‌توان بر عددی ثابت تقسیم کرد؟

جواب. مثال نقض $6 \overset{4}{\equiv} 2 \xrightarrow{\div 2} 3 \overset{4}{\equiv} 1$

قضیه. فرض کنید $ax \overset{n}{\equiv} ay$. در این صورت $x \overset{\frac{n}{d}}{\equiv} y$ که در آن $d=(a,n)$.

اثبات. $ax \overset{n}{\equiv} ay \rightarrow n \mid a(x-y) \rightarrow \frac{n}{d} \mid \frac{a}{d}(x-y)$

اکنون از این که $1=(\frac{a}{d}, \frac{n}{d})$ بنا به لم اقلیدس $\frac{n}{d} \mid x-y$. بنا بر این $x \overset{\frac{n}{d}}{\equiv} y$.

حل معادله‌ی همنهشتی $ax \overset{b}{\equiv} c$.

فرض کنید $ax \overset{b}{\equiv} c$ دارای جواب باشد. اگر x_0 جوابی برای این معادله همنهشتی باشد آنگاه $ax_0 \overset{b}{\equiv} c$ و لذا $b \mid ax_0 - c$. پس y_0 موجود است که $by_0 = ax_0 - c$. بنا بر این $ax_0 - by_0 = c$. یعنی معادله‌ی سیاله‌ی $ax+by=c$ دارای جواب $(x_0, -y_0)$ است. برعکس اگر معادله‌ی سیاله‌ی $ax+by=c$ دارای جواب باشد آنگاه معادله همنهشتی $ax \overset{b}{\equiv} c$ دارای جواب است.

پس می‌توان با تبدیل معادله‌ی همنهشتی $ax \overset{b}{\equiv} c$ به معادله سیاله‌ی $ax+by=c$ آن را حل کرد. همچنین از آنچه گفته شد نتیجه می‌شود

قضیه. معادله‌ی همنهشتی $ax \overset{b}{\equiv} c$ دارای جواب است اگر و تنها اگر $(a,b) \mid c$.

روش دیگر برای حل معادلاتی هم نهشتی $ax \overset{n}{\equiv} b$، استفاده از عکس ضرب است.

مثال. معادله ی هم نهشتی $6x \overset{9}{\equiv} 6$ را حل کنید.

حل. $(6,9) = 3 \mid 6$. بنابراین معادله دارای جواب است.

از این که $(6,9) = 3$ لذا عکس ضربی هم در پیمانه ی 9 وجود دارد. در واقع عکس ضربی هم در پیمانه ی 9 برابر است با 7. چون $7 \times 4 = 28 \overset{9}{\equiv} 1$. اکنون

$$6x \overset{9}{\equiv} 6 \xrightarrow{\times 7} 42x \overset{9}{\equiv} 42 \longrightarrow 14x \overset{9}{\equiv} 6 \longrightarrow x \overset{9}{\equiv} 6$$

مثال. معادله ی هم نهشتی $10x \overset{15}{\equiv} 35$ را حل کنید.

حل. $10x \overset{15}{\equiv} 35 \xrightarrow{\div 5} 2x \overset{3}{\equiv} 7 \xrightarrow{\times 2} 4x \overset{3}{\equiv} 14 \longrightarrow x \overset{3}{\equiv} 2$

قضیه. نشان دهید اگر $a \overset{n}{\equiv} b$ آنگاه $(a,n) = (b,n)$.

حل. قرار می دهیم $d = (a,n)$ و $d' = (b,n)$. از این که $a \overset{n}{\equiv} b$ لذا $n \mid a-b$ و در نتیجه به ازای عدد صحیح q، $a-b = nq$.

$$(a,n) = d \begin{cases} d \mid a \\ d \mid n \longrightarrow d \mid nq = a-b \end{cases} \longrightarrow d \mid a-(a-b) = b$$

حال از این که $n \mid d$ و $d \mid b$ لذا $d \mid (b,n) = d'$.

مشابها $d' \mid d$ و در نتیجه $d = d'$.

دستگاه مختف مانده ها

می دانیم در پیمانه ی 10، اعداد $0, 1, 2, 3, \ldots, 9$ یک دستگاه کامل مانده ها می باشند. در این میان اعداد $1, 3, 7, 9$ با 10 متباین اند.

این دسته از اعداد یک دستگاه مختف مانده ها در پیمانه ی 10 می باشد.

در نیز دستگاه مختف مانده ها تعریف می شود.

تعریف: $a_1, a_2, \dots, a_t$ یک دستگاه مختصر مانده‌ای در پیمانه‌ی n نامیده می‌شود هرگاه هر عدد متباین با n، دقیقاً با یکی از a_i ها همنهشت باشد. (در پیمانه‌ی n)

مثال: $1, 2, \dots, 6$ یک دستگاه مختصر مانده‌ای در پیمانه‌ی 7 می‌باشد.

در حالت کلی اگر p عددی اول باشد آنگاه $1, 2, \dots, p-1$ یک دستگاه مختصر مانده‌ای در پیمانه‌ی p می‌باشد.

چند نکته: فرض کنید $a_1, a_2, \dots, a_t$ یک دستگاه مختصر مانده‌ای در پیمانه‌ی n باشد در این صورت:

الف) برای هر $1 \le i \le t$، عدد متباین a با n چنان موجود است که $a \overset{n}{\equiv} a_i$.

زیرا در غیر اینصورت برای هر عدد a متباین با n، $a \overset{n}{\not\equiv} a_i$ و لذا a_i را می‌توان از دستگاه مختصر مانده‌ای $a_1, \dots, a_t$ حذف کرد که تناقض است.

ب) برای هر $1 \le i \le t$، $(a_i, n) = 1$.

بنابه قسمت الف) عدد a متباین با n موجود است که $a \overset{n}{\equiv} a_i$، اکنون بنابه مسأله‌ی قبل، $(a_i, n) = (a, n) = 1$.

ج) برای هر $1 \le i, j \le t$، اگر $i \neq j$ آنگاه $a_i \overset{n}{\not\equiv} a_j$.

فرض کنید $a_i \overset{n}{\equiv} a_j$. در اینصورت $a_i \overset{n}{\equiv} a_j$ و البته $a_i \overset{n}{\equiv} a_i$. پس a_i با دو عدد از دستگاه مختصر بالا هم‌نهشت است که تناقض است. پس $a_i \overset{n}{\not\equiv} a_j$.

قضیه: فرض کنید $a_1, \dots, a_t$ و $b_1, \dots, b_s$ دو دستگاه مختصر مانده‌ای در پیمانه‌ی n باشند. در اینصورت $t = s$.

اثبات: از این که $(a_1, n) = 1$ و $b_1, \dots, b_s$ یک دستگاه مختصر مانده‌ای است لذا به ازای یک $1 \le j \le s$، $a_1 \overset{n}{\equiv} b_j$. مثلاً (با تعویض اندیس گذاری) $a_1 \overset{n}{\equiv} b_1$

مشابهاً a_2 با عضوی از b_jها هم‌نهشت است. اما $a_2 \not\equiv_n b_1$ زیرا در غیر این صورت $a_2 \equiv_n b_1$ و $a_1 \equiv_n b_1$ و لذا $a_1 \equiv a_2$ که تناقض است. پس در هر مرحله برای هر $1 \le i \le t$ یک j وجود دارد که $a_i \equiv_n b_j$ و این نشان می‌دهد $s \le t$.

مشابهاً $t \le s$ و لذا $s=t$.

یادآوری. فرض کنید n عددی طبیعی باشد. در این صورت تعداد اعداد طبیعی متباین با n و نابیشتر از n را $\varphi(n)$ می‌نامیم. به عبارت دیگر

$$\varphi(n) = |\{1 \le a \le n \mid (a,n)=1\}|$$

مثال. $\varphi(10)=4$ چون اعداد طبیعی نابیشتر از ۱۰ و متباین با ۱۰ عبارتند از ۱، ۳، ۷ و ۹.

مثال. اگر p عددی اول باشد آنگاه برای هر $1 \le i < p$، $(i,p)=1$. پس $\varphi(p)=p-1$.

بعداً ثابت می‌کنیم:

الف) اگر p عددی اول باشد آنگاه $\varphi(p^n)=p^n-p^{n-1}$.

ب) اگر $(m,n)=1$ آنگاه $\varphi(mn)=\varphi(m)\varphi(n)$.

مثال. $\varphi(144)=?$

$$144 = 2^4 \times 3^2 \longrightarrow \varphi(144) = \varphi(2^4 \times 3^2)$$
$$= \varphi(2^4)\,\varphi(3^2) = (2^4-2^3)(3^2-3^1) = 48$$

و در حالت کلی اگر $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ آنگاه:

$$\varphi(n)=\varphi(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$$
$$=(p_1^{\alpha_1}-p_1^{\alpha_1-1})\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1})$$

با توجه به آنچه بین شد یک دستگاه مخفف مانده‌ای در پیمانه‌ی n مانند $\varphi(n)$ عضو دارد، زیرا اگر $a_1, a_2, \dots, a_{\varphi(n)}$ یک دستگاه مخفف مانده‌ای باشد، با توجه به این که $\{1 \le a \le n \mid (a,n)=1\}$ نیز یک دستگاه مخفف مانده‌ای در پیمانه‌ی n با $\varphi(n)$ عضو است لذا $t=\varphi(n)$.

مسأله. فرض کنید $a_{\varphi(n)}, \dots, a_2, a_1$ چنان باشند که

الف) برای هر i, j، $a_i \not\equiv a_j \pmod n$.

ب) برای هر i، $(a_i, n)=1$.

در این صورت $a_{\varphi(n)}, \dots, a_2, a_1$ یک دستگاه مخفف مانده‌ای در پیمانه‌ی n است.

حل. دستگاه مخفف مانده‌ای $b_{\varphi(n)}, \dots, b_2, b_1$ را در نظر می‌گیریم، از این که $(a_1, n)=1$ لذا i ای موجود است که $a_1 \equiv b_i \pmod n$. مثلاً فرض کنید $a_1 \equiv b_1 \pmod n$. مشابهاً $(a_2, n)=1$ لذا a_2 نیز در پیمانه‌ی n با یکی از b_j ها همنهشت است. مسلماً این عدد b_1 نیست. چون اگر $a_2 \equiv b_1 \pmod n$، با توجه به این که $a_1 \equiv b_1 \pmod n$ خواهیم داشت $a_1 \equiv a_2 \pmod n$ که تناقض است. پس j ای موجود است که $a_2 \equiv b_j \pmod n$. مثلاً فرض کنید $a_2 \equiv b_2 \pmod n$. با ادامه‌ی این روند، احتمالاً با تعویض اندیس گذاری، $a_3 \equiv b_3 \pmod n$، و $a_{\varphi(n)} \equiv b_{\varphi(n)} \pmod n$. اکنون با توجه به این که $b_{\varphi(n)}, \dots, b_2, b_1$ یک دستگاه مخفف مانده‌ای در پیمانه‌ی n است لذا $a_{\varphi(n)}, \dots, a_2, a_1$ نیز چنین است.

لم. فرض کنید $(a,b)=1$ و $(a,c)=1$. در این صورت $(a,bc)=1$.

اثبات. روش اول) فرض کنید $(a,bc)=d \neq 1$. در این صورت عدد اول p

چنان موجود است که $p|d$. بنابراین $p|a$ و $p|bc$ و لذا بنا به نتیجه‌ای از لم اقلیدس $p|b$ یا $p|c$.

- اگر $p|b$ آنگاه با توجه به این که $p|a$، لذا $p|(a,b)=1$ که غیر ممکن است.
- اگر $p|c$ مشابها $p|(a,c)=1$ که غیر ممکن است.

پس $d=(a,bc)=1$.

روش دوم:

$(a,b)=1 \rightarrow \exists x,y \quad ax+by=1$

$(a,c)=1 \rightarrow \exists x',y' \quad ax'+cy'=1$

با ضرب طرفین در رابطه اخیر خواهیم داشت:

$$a(\underbrace{axx'+cxy'+bx'y}_{x''}) + bc(\underbrace{yy'}_{y''}) = 1$$

بنابراین $(a,bc)=1$.

نتیجه. اگر $(a,b_1)=1$، ... و $(a,b_n)=1$ آنگاه $(a,b_1b_2\cdots b_n)=1$.

مسأله. اگر $a_1, \ldots, a_{\varphi(n)}$ یک دستگاه مختصف مانده‌ای در پیمانه‌ی n باشد و $(a,n)=1$ آنگاه $aa_1, \ldots, aa_{\varphi(n)}$ نیز یک دستگاه مختصف مانده‌ای در پیمانه n است.

اثبات. برای هر i، $(a_i,n)=1$، بعلاوه $(a,n)=1$ و لذا بنا به لم قبل، $(aa_i,n)=1$.

حال نشان می‌دهیم دو به دو در پیمانه‌ی n غیر هم‌نهشت‌اند. برای فرض کنید برای $i \neq j$، $aa_i \overset{n}{\equiv} aa_j$. از این که $(a,n)=1$ لذا $a_i \overset{n}{\equiv} a_j$ که ...

بنابراین با استفاده از مثال قبل، $aa_1, \dots, aa_{\varphi(n)}$ یک دستگاه مختصف مانده کامل است.

قضیه اویلر، فرض کنید $(a,n)=1$. در این صورت $a^{\varphi(n)} \overset{n}{\equiv} 1$.

اثبات. فرض کنید $a_1, \dots, a_{\varphi(n)}$ یک دستگاه مختصف مانده کامل در پیمانه‌ی n باشد. در این صورت بنابه‌مثال قبل، $aa_1, \dots, aa_{\varphi(n)}$ نیز یک دستگاه مختصف مانده کامل در پیمانه‌ی n است و لذا هر aa_i با یکی از a_j ها هم‌نهشت است.

در هر حال
$$(aa_1)\cdots(aa_{\varphi(n)}) \overset{n}{\equiv} a_1 \cdots a_{\varphi(n)}$$
$$\rightarrow a^{\varphi(n)}(a_1 \cdots a_{\varphi(n)}) \overset{n}{\equiv} a_1 \cdots a_{\varphi(n)}$$

از این که $(a_1 \cdots a_{\varphi(n)}, n) = 1$ با تقسیم طرفین رابطه‌ی اخیر بر $a_1 \cdots a_{\varphi(n)}$ خواهیم داشت $a^{\varphi(n)} \overset{n}{\equiv} 1$.

نتیجه ۱. (قضیه کوچک فرما) اگر p عددی اول باشد آنگاه $a^{p-1} \overset{p}{\equiv} 1$.

اثبات. می‌دانیم $\varphi(p) = p-1$. بنابراین $a^{p-1} \overset{p}{\equiv} 1$.

نتیجه ۲. اگر $(a,n)=1$ آنگاه $a^{\varphi(n)-1}$ یک عکس حسابی a در پیمانه‌ی n است.

اثبات. از این که $a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \overset{n}{\equiv} 1$

لذا $a^{\varphi(n)-1}$ عکس حسابی a در پیمانه‌ی n است.

مثال. یک عکس حسابی ۵۰۳ در پیمانه‌ی ۹۰۰ را بیابید.

$$\varphi(900) = \varphi(2^2 \times 3^2 \times 5^2) = (2^2-2)(3^2-3)(5^2-5) = 240$$

5^{239} ولذا $5^{240} \equiv_{900} 1$ بنابراین $(5, 900) = 1$ زیرا

یک عکس حسابی 5^3 در پیمانه‌ی ۹۰۰ است.

قضیه‌ی ویلسون. اگر p عددی اول باشد آنگاه $(p-1)! \overset{p}{\equiv} -1$.

قبل از اثبات، طرح اثبات را برای $p = 13$ در زیر می‌آوریم.

$$(p-1)! = 12! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12$$

به راحتی می‌توان دید که زوج‌های $\{2, 7\}$، $\{3, 9\}$، $\{4, 10\}$، $\{5, 8\}$، $\{6, 11\}$ عکس‌های حسابی یکدیگرند و لذا حاصل‌ضرب آن‌ها برابر 1 (در پیمانه‌ی ۱۳) است.

پس $(p-1)! = 12! \equiv_{13} 12 \equiv -1$.

اثبات. $(p-1)! = 1 \times 2 \times \cdots \times (p-2)(p-1)$. نشان می‌دهیم هر عدد در عاصله‌ی 2 تا $p-2$ دارای عکس حسابی درون خودش است.

برای این منظور فرض کنید $2 \leq k \leq p-2$. در این صورت $(k, p) = 1$ و لذا k دارای عکس حسابی به پیمانه‌ی p است که آن را با k^* نشان می‌دهیم.

می‌توان فرض کرد $k^* \in \{0, 1, \cdots, p-1\}$.

از این که $(k^*, p) = 1$ لذا $k^* \neq 0$.

همچنین از این که $k^* \overset{p}{\equiv} 1$ و $(p-1)^2 = p^2 - 2p + 1 \overset{p}{\equiv} 1$ بنابراین $k^* \neq 1, p-1$.

عکس حسابی 1 و $p-1$ خودشان می‌باشد و لذا $k^* \in \{2, \cdots, p-2\}$.

اکنون با قرار دادن هر k و k^* کنار یکدیگر خواهیم داشت $1 \overset{p}{\equiv} (2 \times \cdots \times (p-2)) \times 1$

و در نتیجه: $(p-1)! = 1 \times (2 \times \cdots \times (p-2)) \times (p-1) \equiv 1 \times 1 \times (-1) \equiv -1$

سؤال. در چه پیمانه‌ای ۱− مربع است؟

مثال. در پیمانه‌ی ۵، $-1 \overset{5}{\equiv} 4 = 2^2$. پس ۱− در پیمانه‌ی ۵ مربع است.

می‌خواهیم بررسی کنیم که آیا در پیمانه‌ی ۷، نظیر ۱− یک مربع است؟

$0^2=0$ ، $1^2=1$ و $2^2=4$ و $3^2=9 \overset{7}{\equiv} 2$ و $4^2=16 \overset{7}{\equiv} 2$ ، $5^2=25 \overset{7}{\equiv} 4$

$6^2=36 \overset{7}{\equiv} 1$

همان طور که ملاحظه می‌شود، ۱− در پیمانه‌ی ۷ یک مربع نیست.

در قضیه زیر به سؤال بالا پاسخ داده می‌شود.

قضیه. فرض کنید p عددی اول باشد. در این صورت معادله‌ی $x^2 \overset{p}{\equiv} -1$ دارای جواب است اگر و تنها اگر $p=2$ یا $p=4k+1$.

اثبات. واضح است که در پیمانه‌ی ۲، $-1 \overset{2}{\equiv} 1 = 1^2$.

حال فرض کنید p عدد اول فردی به صورت $4k+1$ باشد. در این صورت $\frac{p-1}{2}=2k$

و بنا به قضیه‌ی ویلسون، $(p-1)! \overset{p}{\equiv} -1$. بنابراین:

$$1\times 2\times \cdots \times \left(\frac{p-1}{2}\right)\times \underbrace{\left(\frac{p+1}{2}\right)}_{\equiv -\frac{p-1}{2}}\times \cdots \times \underbrace{(p-2)}_{\equiv -2}\underbrace{(p-1)}_{\equiv -1} \overset{p}{\equiv} -1$$

$$(-1)^{\frac{p-1}{2}}\left(1\times 2\times \cdots \times \frac{p-1}{2}\right)^2 \overset{p}{\equiv} -1$$

اما از این که $\frac{p-1}{2}$ زوج است لذا

$$\left(1\times 2\times \cdots \times \frac{p-1}{2}\right)^2 \overset{p}{\equiv} -1 ،$$

یعنی معادله‌ی $x^2 \overset{p}{\equiv} -1$ دارای جواب $x=\left(\frac{p-1}{2}\right)!$ است.

برعکس فرض کنید $x^2 \overset{p}{\equiv} -1$ دارای جواب باشد. همچنین فرض کنید $p \neq 2$،

در این صورت بنا به قضیه‌ی فرما،

$$1 \overset{p}{\equiv} x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}$$

بنابراین $1 \overset{p}{\equiv} (-1)^{\frac{p-1}{2}}$ ولذا $\frac{p-1}{2}$ عددی زوج است. اگر $\frac{p-1}{2} = 2k$

آنگاه $p = 4k+1$.

توجه کنید: اگر $p \mid x$ آنگاه $x^2 \overset{p}{\equiv} 0$ ∴ $(x,p) = 1$

ولذا قضیه‌ی فرما برقرار است.

نتیجه: اگر عدد اول p عددی صحیح بشکل x^2+1 را عاد کند آنگاه $p = 4k+1$.

اثبات. $p \mid x^2+1 \longrightarrow x^2+1 \overset{p}{\equiv} 0 \longrightarrow x^2 \overset{p}{\equiv} -1 \longrightarrow p = 4k+1$

ترین. ثابت کنید مجموعه‌ی اعداد اول بشکل $4k+1$ نامتناهی است.

مرتبه‌ی یک عدد در یک دستگاه

تعریف. فرض کنید n عددی طبیعی باشد و $(a,n) = 1$.

در این صورت مرتبه‌ی a را کوچکترین توان k می‌گیریم که $a^k \overset{n}{\equiv} 1$. در این صورت می‌نویسیم $o_n(a) = k$

مثال. در دستگاه ۶، $o_6(5) = ?$

$5^1 = 5$، $5^2 = 25 \overset{6}{\equiv} 1 \longrightarrow o_6(5) = 2$

توجه کنید اگر $(a,n) = 1$ آنگاه بنا به قضیه‌ی اویلر $a^{\varphi(n)} \overset{n}{\equiv} 1$. بنابراین

$o_n(a)$ موجود است و بعلاوه

$$1 \leq o_n(a) \leq \varphi(n)$$

قضیه. فرض کنید $o_n(a)=k$. در این صورت $a^h \overset{n}{\equiv} 1$ اگر و تنها اگر $k \mid h$.

اثبات. ابتدا فرض کنید $k \mid h$. در این صورت $q \in \mathbb{Z}$ موجود است که $h=kq$.

حال از این که $o_n(a)=k$ لذا $a^k \overset{n}{\equiv} 1$ ، اکنون

$$a^h = a^{kq} = (a^k)^q \overset{n}{\equiv} 1^q = 1 .$$

برعکس فرض کنید $a^h \overset{n}{\equiv} 1$. بنابه الگوریتم تقسیم q, r موجودند بطوری که

$h = kq + r$ که در آن $0 \le r < k$ ،

ادعا می کنیم $r=0$ ، فرض کنید (فرض خلف) خیلی نباشد. بنابراین $0 < r < k$.

اکنون $a^h = a^{kq+r} = (a^k)^q a^r \overset{n}{\equiv} 1^q a^r = a^r \overset{n}{\equiv} 1$.

بنابراین $a^r \overset{n}{\equiv} 1$ که تناقض با کوچکترین بودن k است، پس $r=0$ ولذا

$h=kq$. یعنی $k \mid h$.

نتیجه. اگر $(a,n)=1$ آنگاه $o_n(a) \mid \varphi(n)$ ،

اثبات. بنا به قضیه اویلر، $a^{\varphi(n)} \overset{n}{\equiv} 1$ و بنا به قضیه‌ی بالا، $o_n(a) \mid \varphi(n)$.

قضیه. فرض کنید $o_n(a)=k$. در این صورت $a^i \overset{n}{\equiv} a^j$ اگر و تنها اگر $i \overset{k}{\equiv} j$.

اثبات. فرض می کنیم $i \ge j$ ، در این صورت:

$$a^i \overset{n}{\equiv} a^j \longleftrightarrow a^{i-j} \overset{n}{\equiv} 1 \longleftrightarrow k \mid i-j \longleftrightarrow i \overset{k}{\equiv} j$$

نتیجه. اگر $(a,n)=1$ و $o_n(a)=k$ آنگاه a^k ، ... ، a^2 ، a دو به دو

در باقیمانده‌ی n غیر هم نهشت اند.

اثبات. اگر برای $i \ge j$ ، $a^i \overset{n}{\equiv} a^j$ آنگاه بنا به قضیه‌ی قبل $i \overset{k}{\equiv} j$ ⊗

توجه کنید: اگر $o_n(a)=k$ آنگاه $a^k \overset{n}{\equiv} 1=a^0$. بنابراین a^{k-1} و ... و a^0, a^1 در پیمانه‌ی n، دو به دو غیرهم‌نهشت‌اند.

قضیه، فرض کنید $(a,n)=1$. در این صورت $o_n(a^h)=\frac{o_n(a)}{(o_n(a),h)}$.

اثبات. قرار می‌دهیم $o(a)=k$، $(k,h)=d$، $o(a^h)=t$، می‌خواهیم ثابت کنیم $t=\frac{k}{d}$.

① $(a^h)^{\frac{k}{d}} = a^{\frac{kh}{d}} = (a^k)^{\frac{h}{d}} \overset{n}{\equiv} 1 \longrightarrow t=o(a^h) \mid \frac{k}{d}$

همچنین $o(a^h)=t$. بنابراین $(a^h)^t \overset{n}{\equiv} 1$ و لذا $a^{ht} \overset{n}{\equiv} 1$. بنابه یکی از قضیه‌های قبل، $k=o(a) \mid ht$ و در نتیجه $\frac{k}{d} \mid \frac{h}{d} t$.

حال از این که $(\frac{k}{d}, \frac{h}{d})=1$، بنابه لم اقلیدس، ② $\frac{k}{d} \mid t$.

روابط ① و ② نتیجه می‌دهند $t=\frac{k}{d}$ و حکم ثابت می‌شود.

نتیجه: اگر $(a,n)=1$ آنگاه $o(a)=o(a^h)$ اگر و تنها اگر $(h,o(a))=1$.

قبلاً بیان شد که اگر $(a,n)=1$ آنگاه $1 \leq o(a) \leq \varphi(n)$. اکنون:

تعریف. اگر $(a,n)=1$، a را یک ریشه‌ی اولیه‌ی n (یا یک ریشه‌ی اولیه در پیمانه‌ی n) می‌گوییم هرگاه $o(a)=\varphi(n)$، در چنین حالتی می‌گوییم n دارای ریشه‌ی اولیه است.

سؤال، چه اعدادی دارای ریشه‌ی اولیه هستند.

مثال، نشان دهید ۷ دارای ریشه‌ی اولیه است.

حل، باید عدد صحیح a را چنان بیابیم که $o(a)=\varphi(7)=6$.

برای این منظور باید در بین اعداد $\{1,2,3,4,5,6\}$ عدد a با خاصیت خواسته شده را بیابیم.

$1^1 \equiv 1 \longrightarrow o(1)=1$

$2^1=2,\ 2^2=4,\ 2^3=8\equiv 1 \longrightarrow o(2)=3$

$3^1=3,\ 3^2=9\equiv 2,\ 3^3=27\equiv -1 \longrightarrow o_7(3)=6$

پس ۳ یک ریشه‌ی اولیه در پیمانه‌ی ۷ است.

توجه: بنا به نتیجه‌ای از قبل، $o_h(a) \mid \varphi(h)$. پس $6=\varphi(7) \mid o_7(3)$

بنابراین $o(3)=1$ یا ۲ یا ۳ یا ۶. از این که $3^1 \neq 1$ ، $3^2 \neq 1$ و $3^3 \neq 1$ لذا $o(3) \neq 1,2,3$ و در نتیجه $o_7(3)=6$.

می‌دانیم $\varphi(1)=1$ و $\varphi(2)=1$.

مساله: فرض کنید $n \geq 3$. ثابت دهید $\varphi(n)$ عددی زوج است.

حل: عوامل n همگی ۲ هستند با این که n شامل یک عامل فرد مثل p است.

- اگر همه‌ی عوامل n، ۲ باشند آنگاه $n=2^k$ و چون $n \geq 3$ لذا $k \geq 2$،

$$\varphi(n)=\varphi(2^k)=2^k-2^{k-1}=2^{k-1}$$ زوج

- اگر n شامل عامل فردی مانند p باشد و توان p برابر با k باشد،

$$n=p^k \times m \longrightarrow \varphi(n)=\varphi(p^k)\varphi(m)$$

$$=\underbrace{(p^k-p^{k-1})}_{\text{زوج}}\varphi(m)=\text{زوج}$$

بنابراین برای هر $n \geq 3$، $\varphi(n)$ زوج است. (توجه کنید $\varphi(1)=\varphi(2)=1$)

مساله: فرض کنید n عددی طبیعی بوده و $d|n$. در این صورت تعداد اعداد نامنفی نشت با n که با n دارای ب.م.م d است برابر است با $\varphi(\frac{n}{d})$.

حل: قرار میدهیم $A_d=\{1\leq a\leq n \mid (a,n)=d\}$.

میخواهیم ثابت کنیم $|A_d|=\varphi(\frac{n}{d})$.

برای این منظور قرار می‌دهیم $B=\{1\leq b\leq \frac{n}{d} \mid (b,\frac{n}{d})=1\}$.

واضح است که $|B|=\varphi(\frac{n}{d})$.

آنگاه تعریف می‌کنیم $f: A_d \longrightarrow B$, $a \longmapsto \frac{a}{d}$

الف. f خوش تعریف است.

برای این منظور فرض کنید $a\in A_d$ در این صورت $1\leq a\leq n$ و بعلاوه $(a,n)=d$. در این صورت $d|a$ و لذا $\frac{a}{d}$ عددی صحیح است.

همچنین از این که $1\leq a\leq n$ لذا $1\leq \frac{a}{d}\leq \frac{n}{d}$ و بعلاوه از $(a,n)=d$ نتیجه می‌شود $(\frac{a}{d},\frac{n}{d})=1$. پس $\frac{a}{d}\in B$، پس f خوش تعریف است.

ب. f یک به یک است، واضح است.

ج. f پوشاست. فرض کنید $b\in B$ دلخواه باشد. در این صورت $1\leq b\leq \frac{n}{d}$ و $(b,\frac{n}{d})=1$. در این صورت $1\leq bd\leq n$ و $(bd,n)=d$.

پس $bd\in A_d$ و البته $f(bd)=\frac{bd}{d}=b$. پس f پوشاست.

بنابراین f دوسویی است و لذا $|A_d|=|B|=\varphi(\frac{n}{d})$.

گزاره. فرض کنید n عددی طبیعی باشد. در این صورت $\sum_{d|n}\varphi(d)=n$.

اثبات. قرار می‌دهیم $A_d=\{1\le a\le n \mid (a,n)=d\}$. در این صورت از تعریف ب.م.م نتیجه می‌شود A_d ها دوبه‌دو متمایزند. از طرفی $\bigcup_{d|n}A_d=\{1,2,\dots,n\}$. بنابراین A_d ها مجموعه $\{1,\dots,n\}$ را افراز می‌کنند و لذا $\sum_{d|n}|A_d|=|\{1,2,\dots,n\}|=n$. یعنی $\sum_{d|n}\varphi(\frac{n}{d})=n$. اما $\sum_{d|n}\varphi(\frac{n}{d})=\sum_{d|n}\varphi(d)$. بنابراین $\sum_{d|n}\varphi(d)=n$.

حکم اخیر را با مثالی نشان می‌دهیم.

اگر $n=12$ آنگاه مقسوم‌علیه‌های 12 عبارتند از $\{1,2,3,4,6,12\}$ و بنابراین

$$\sum_{d|n}\varphi(\tfrac{n}{d})=\varphi(\tfrac{12}{1})+\varphi(\tfrac{12}{2})+\varphi(\tfrac{12}{3})+\varphi(\tfrac{12}{4})+\varphi(\tfrac{12}{6})+\varphi(\tfrac{12}{12})$$
$$=\varphi(12)+\varphi(6)+\varphi(4)+\varphi(3)+\varphi(2)+\varphi(1)$$
$$=\sum_{d|n}\varphi(d)$$

مسئله. فرض کنید n عددی طبیعی، $(a,n)=1$ و a^* یک عکس ضربی a به پیمانه n باشد. در این صورت $o_n(a^*)=o_n(a)$.

حل. فرض کنید $o(a)=r$ و $o(a^*)=s$. در این صورت $a^r\overset{n}{\equiv}1$ و $a^{*s}\overset{n}{\equiv}1$.

اکنون: $a^s=1\cdot a^s\overset{n}{\equiv}a^{*s}a^s=(a^*a)^s\overset{n}{\equiv}1^s=1$

بنابراین $r=o(a)\mid s$. مشابهاً $s\mid r$ و لذا $s=r$.

مسأله. فرض کنید n عددی طبیعی باشد و $(a,n)=(b,n)=1$. در این صورت اگر $(o_n(a),o_n(b))=1$ آنگاه $o_n(ab)=o_n(a)\,o_n(b)$.

حل. قرار می دهیم $o(a)=r$، $o(b)=s$ و $o(ab)=t$.

$$(ab)^{rs}=a^{rs}b^{rs}=(a^r)^s(b^s)^r \overset{n}{\equiv} 1^s.1^r=1$$

پس $t=o(ab)\mid rs$.

از این که $a^t b^t=(ab)^t \overset{n}{\equiv} 1$ لذا $o(ab)=t$ یعنی a^t و b^t عکس حاصل ضرب هم در پیمانه‌ی n می باشند و بنابه مسأله‌ی قبل $o(a^t)=o(b^t)$.

$$o(a^t)=o(b^t) \longrightarrow \frac{o(a)}{(o(a),t)}=\frac{o(b)}{(o(b),t)}$$

فرض کنید که مقدار اخیر برابر k باشند

$$k=\frac{o(a)}{(o(a),t)} \longrightarrow k \mid o(a)$$

از طرفی $k \mid o(b)$ و لذا $k \mid (o(a),o(b))=1$. بنابراین $k=1$.

پس $\frac{o(a)}{(o(a),t)}=1$ در نتیجه $(o(a),t)=o(a)$ یعنی $o(a)\mid t$.

از طرفی $o(b)\mid t$ و چون $(o(a),o(b))=1$ لذا $rs=o(a)o(b)\mid t$

پس $t=rs$ و حکم بدست می آید.

مسأله. فرض کنید n عددی طبیعی و $(a,n)=1$. اگر a یک ریشه‌ی اولیه‌ی n باشد، آنگاه $a, a^2, \ldots, a^{\varphi(n)}$ یک دستگاه مخفف مانده‌ی اویلری n است.

اثبات: در قضیه‌ای از قبل بیان کردیم که اگر $o_n(a)=k$ آنگاه $a, a^2, \dots, a^k$ دو به دو غیر هم‌نهشت (در پیمانه‌ی n) می‌باشند.

حال از این که a یک ریشه‌ی اولیه‌ی n است لذا $o_n(a)=\varphi(n)$ و بنابه آنچه هم اکنون بیان شد، $a, a^2, \dots, a^{\varphi(n)}$ دو به دو در پیمانه‌ی n غیر هم‌نهشت‌اند. از طرفی از این که $(a,n)=1$ لذا برای هر i، $(a^i,n)=1$ و بعلاوه تعداد مجموعه‌ی $a, a^2, \dots, a^{\varphi(n)}$ برابر است با $\varphi(n)$.

حال بنابه قضیه‌ای از قبل، $a, a^2, \dots, a^{\varphi(n)}$ یک دستگاه مخفف مانده‌ی در پیمانه‌ی n است.

مسأله: فرض کنید عدد طبیعی n دارای ریشه‌ی اولیه است. در این صورت n دقیقاً $\varphi(\varphi(n))$ ریشه‌ی اولیه دارد.

اثبات: فرض کنید a یک ریشه‌ی اولیه‌ی n باشد. در این صورت بنابه مسأله‌ی قبل، $a, a^2, \dots, a^{\varphi(n)}$ یک دستگاه مخفف مانده‌ی در پیمانه‌ی n است. تمام ریشه‌های اولیه‌ی n باید با n نسبت اول باشند. بنابراین برای یافتن تمام ریشه‌های اولیه در یک دستگاه مخفف مانده‌ای جستجو می‌کنیم. برای این منظور دستگاه مخفف مانده‌ای $a, a^2, \dots, a^{\varphi(n)}$ را در نظر می‌گیریم. a^i یک ریشه‌ی اولیه‌ی n است هرگاه $o(a^i)=\varphi(n)$ از طرفی $o(a)=\varphi(n)$. پس لازم است $o(a^i)=o(a)$. یعنی $o(a)=\frac{o(a)}{(o(a),i)}$. و این برقرار است هرگاه $(o(a),i)=1=(\varphi(n),i)$

پس :

$|\{i \mid 1 \le i \le \varphi(n) \ , \ (\varphi(n), i) = 1\}|$ = تعداد دسته‌های اولیه‌ی n

$= \varphi(\varphi(n))$.

لم. اگر $n \ge 3$ و a عددی فرد باشد آنگاه $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.

اثبات. (بطریق استقرا)

اگر $n = 3$ باید ثابت کنیم $a^2 \equiv 1 \pmod{8}$.

اما حکم اخیر برقرار است، زیرا قبلاً ثابت دادیم که اگر a عددی فرد باشد آنگاه $a^2 \equiv 1 \pmod{8}$ ،

a^2 بصورت $8t+1$ است، بنابراین

حال فرض کنید برای $k \ge 3$ ، $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. می‌خواهیم ثابت کنیم

$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

بنابه فرض استقرا، $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ و در نتیجه ① $2^k \mid a^{2^{k-2}} - 1$.

همچنین a عددی فرد است، بنابراین $a^{2^{k-2}} + 1$ زوج است ولذا ② $2 \mid a^{2^{k-2}} + 1$

①, ② $\longrightarrow 2^k \times 2 \mid (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1) = a^{2^{k-1}} - 1$

پس $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

قضیه. اگر عدد طبیعی n دارای ریشه‌ی اولیه باشد آنگاه باید به یکی از صورتهای زیر باشد:

$2, 4, p^k, 2p^k$ (p فرد)

اثبات، فرض کنید n بصورت $2p^k$، p^k، 4، 2 (هر فرد) نباشد.

بنابراین n یا بصورت 2^r است که $r \geq 3$ و یا این که n را می‌توان بشکل $n = n_1 n_2$ بیان کرد که $(n_1, n_2) = 1$ و $n_1 n_2 > 2$،

بررسی می‌کنیم.

الف، $n = 2^r$ که در آن $r \geq 3$،

در این حالت اگر a برای ریشه‌ی اولیه‌ی a باشد آنگاه $(a, 2^r) = 1$ ولذا a عددی فرد است.

از این که a ریشه‌ی اولیه‌ی $n = 2^r$ است لذا

$$o_{2^r}(a) = \varphi(2^r) = 2^r - 2^{r-1} = 2^{r-1}(2-1) = 2^{r-1}$$

اما بنا به لم قبل، برای $r \geq 3$، $a^{2^{r-2}} \equiv 1 \pmod{2^r}$ و در نتیجه

$$2^{r-1} = o_{2^r}(a) \mid 2^{r-2} \quad \text{!!}$$

ب. $n = n_1 n_2$ که در آن $(n_1, n_2) = 1$ ، $n_1, n_2 > 2$،

در این حالت $\varphi(n_1)$ و $\varphi(n_2)$ بنا به یکی از لم‌های قبل، هر دو زوج‌اند.

اکنون بنا به قضیه‌ی اویلر $a^{\varphi(n_1)} \equiv 1 \pmod{n_1}$ ولذا

$$a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} = \left(a^{\varphi(n_1)}\right)^{\frac{\varphi(n_2)}{2}} \equiv 1 \pmod{n_1}$$

وبنابراین $n_1 \mid a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} - 1$.

مشابهاً $n_2 \mid a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} - 1$ و چون $(n_1, n_2) = 1$ حاصل ضرب آنها هم عاد می‌کند پس

$n = n_1 n_2 \mid a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} - 1$ ولذا $a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} \overset{n}{\equiv} 1$،

چنانچه a ریشه‌ی اولیه‌ی n باشد، $o_n(a) = \varphi(n)$ و از این که $a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} \overset{n}{\equiv} 1$ لذا $\varphi(n) = o_n(a) \mid \frac{\varphi(n_1)\varphi(n_2)}{2}$.

یعنی $\varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2) \mid \frac{\varphi(n_1)\varphi(n_2)}{2}$ که این غلط است.

بنابراین در هر حلقه n نمی‌تواند ریشه‌ی اولیه داشته باشد.

قضیه لاگرانژ. فرض کنید $f(x) = a_n x^n + \cdots + a_0$ یک چندجمله‌ای با ضرایب صحیح باشد و p عددی اول باشد طوری که $p \nmid a_n$، در این صورت $f(x) \overset{p}{\equiv} 0$ حداکثر n ریشه دارد.

اثبات. به طریق استقرا اگر $n=1$ آنگاه $f(x) = a_1 x + a_0$ که در آن $p \nmid a_1$. واضح است که $a_1 x + a_0 \overset{p}{\equiv} 0$ دارای جواب $a_1^*(-a_0)$ است. چون $a_1 x + a_0 \overset{p}{\equiv} 0 \to a_1 x \overset{p}{\equiv} -a_0 \to x \overset{p}{\equiv} a_1^*(-a_0)$،

توجه کنید از این که $(p, a_1) = 1$ لذا وارون ضربی a_1 در پایه‌ی کامل وجود است. این وارون ضربی را a_1^* گرفته‌ایم.

اکنون فرض کنید $f(x)$ یک چند جمله‌ای با درجه‌ی k باشد.

همچنین $f(x) \overset{p}{\equiv} 0$ جواب نداشته باشد حکم ثابت شده است. پس فرض کنیم

این معادله هم‌نهشتی دارای جواب a باشد، یعنی $f(a) \overset{p}{\equiv} 0$،

بنا به الگوریتم تقسیم $f(x) = (x-a)g(x) + r$ که در آن باقی‌مانده $x=a$

در طرفین تساوی اخیر جوهیم داشت: $f(a) = r$،

پس $f(x) = (x-a)g(x) + f(a)$ و چون $f(a) \overset{p}{\equiv} 0$ لذا $f(x) \overset{p}{\equiv} 0$.

یا $(x-a)g(x) \overset{p}{\equiv} 0$ تبدیل می‌شود،

بوضوح $\deg(g(x)) \leq k-1$ و لذا بنا به فرض استقرا $g(x) \overset{p}{\equiv} 0$ حداکثر

$k-1$ جواب دارد و لذا $f(x) \overset{p}{\equiv} 0$ حداکثر k جواب خواهد داشت.

نتیجه. اگر p عددی اول باشد و $d \mid p-1$ آنگاه $x^d - 1 \overset{p}{\equiv} 0$ دقیقاً دارای

d جواب متمایز است،

اثبات. از این که $d \mid p-1$ لذا t صحیح موجود است که $p-1 = td$، اکنون

$$x^{p-1} - 1 = x^{dt} - 1 = (x^d - 1)(x^{dt-d} + \cdots) = (x^d - 1)g(x)$$

بنا به قضیه‌ی فرما اگر $(x,p) = 1$ آنگاه $x^{p-1} \overset{p}{\equiv} 1$. بنابراین $x^{p-1} - 1 \overset{p}{\equiv} 0$

دارای جواب‌های $1, 2, \ldots, p-1$ است و لذا $x^{p-1} - 1 \overset{p}{\equiv} 0$ دقیقاً $p-1$ جواب دارد

و از این که $x^{p-1}-1=(x^d-1)g(x)$ لذا $(x^d-1)g(x)$ نیز دقیقاً $p-1$ جواب متمایز دارد.

اما بنا به قضیه‌ی قبل $g(x)\overset{p}{\equiv}0$ حداکثر به اندازه‌ی $\deg g(x)=p-1-d$ جواب دارد. بنابراین $x^d-1\overset{p}{\equiv}0$ حداقل d جواب دارد.

از طرفی بنا به قضیه قبل $x^d-1\overset{p}{\equiv}0$ حداکثر d جواب دارد و در نتیجه x^d-1 دقیقاً d جواب متمایز دارد.

در مباحث پیش رو نشان می‌دهیم هر عدد به صورت ۲، ۴، p^k و $2p^k$ (p فرد) دارای ریشه‌ی اولیه است.

قضیه. اگر p عددی اول باشد آنگاه ریشه‌ی اولیه در پیمانه‌ی p موجود است.

اثبات. اگر $p=2$ آنگاه 1 یک ریشه‌ی اولیه در پیمانه‌ی p است. پس می‌توان فرض کرد $p\geq 3$. یعنی p را یک عدد اول فرد می‌گیریم.

فرض کنید $p-1=p_1^{q_1}\cdots p_k^{q_k}$ تجزیه به عوامل اول باشد.

از این که $p_1^{q_1}\mid p-1$ لذا بنا به قضیه‌ی قبل $x^{p_1^{q_1}}\overset{p}{\equiv}1$ دقیقاً $p_1^{q_1}$ جواب دارد.

مشابهاً $x^{p_1^{q_1-1}}\overset{p}{\equiv}1$ نیز دقیقاً $p_1^{q_1-1}$ جواب دارد. از این که $p_1^{q_1}>p_1^{q_1-1}$ می‌توان a_1 را چنان انتخاب کرد که a_1 جواب $x^{p_1^{q_1}}\overset{p}{\equiv}1$ باشد ولی جواب $x^{p_1^{q_1-1}}\overset{p}{\equiv}1$ نباشد. پس

$a_1^{p_1^{\alpha_1}} \overset{p}{\equiv} 1$ و $a_1^{p_1^{\alpha_1-1}} \overset{p}{\not\equiv} 1$ ،

ادعا می‌کنیم $o_p(a_1) = p_1^{\alpha_1}$.

از این که $a_1^{p_1^{\alpha_1}} \overset{p}{\equiv} 1$ لذا $o_p(a_1) \mid p_1^{\alpha_1}$ و در نتیجه $t \leq \alpha_1$ موجود است

که $o_p(a_1) = p_1^t$. کافی است نشان دهیم $t = \alpha_1$.

فرض کنید $t \neq \alpha_1$ بنابراین $t < \alpha_1$ و یا $t \leq \alpha_1 - 1$.

$$o_p(a_1) = p_1^t \rightarrow a_1^{p_1^t} \overset{p}{\equiv} 1 \rightarrow (a_1^{p_1^t})^{p_1^{\alpha_1-1-t}} \overset{p}{\equiv} 1$$

$$\rightarrow a_1^{p_1^{\alpha_1-1}} \overset{p}{\equiv} 1 \quad \text{!!}$$

پس $t = \alpha_1$ و در نتیجه $o_p(a_1) = p_1^{\alpha_1}$.

مشابهاً عدد صحیح a_2 چنان موجود است که $o_p(a_2) = p_2^{\alpha_2}$ و ... a_k وجود

دارد که $o_p(a_k) = p_k^{\alpha_k}$. اگر قرار دهیم $b = a_1 \cdots a_k$ آنگاه

$$o_p(b) = o_p(a_1) \cdots o_p(a_k) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = p-1 = \varphi(p)$$

پس b یک ریشه‌ی اولیه در پیمانه‌ی p است .

مسأله. یک ریشه‌ی اولیه در پیمانه‌ی ۷ بیابید .

حل. $p = 7 \rightarrow p-1 = 6 = 2^1 \times 3^1$

ابتدا a_1 را چنان می‌یابیم که همزمان در روابط $\begin{cases} x^{\frac{7}{2}} \overset{7}{\equiv} 1 \\ x \overset{7}{\neq} 1 \end{cases}$ صدق کند .

به راحتی می‌توان دید $a_1 = 6$ دارای این خاصیت است .

همچنین a_2 را چنان می‌یابیم که همزمان در خواص $\begin{cases} x^3 \overset{7}{\equiv} 1 \\ x \overset{7}{\not\equiv} 1 \end{cases}$ صدق کند. می‌توان دید $a_2 = 2$ این خاصیت را دارد.

حال بنا به قضیه‌ی قبل، $b = a_1 a_2 = 6 \times 2 = 12 \overset{7}{\equiv} 5$ یک ریشه‌ی اولیه‌ی ۷ می‌باشد.

لم ۱ فرض کنید p عددی اول فرد باشد. در این صورت ریشه‌ی اولیه‌ای مانند b موجود است که $b^{p-1} \overset{p^2}{\not\equiv} 1$.

اثبات. فرض کنید a یک ریشه‌ی اولیه‌ی پیمانه‌ی p باشد. (بنا به قضیه قبل چنین a موجود است) چنانچه $a^{p-1} \overset{p^2}{\not\equiv} 1$ حکم ثابت شده است. پس فرض می‌کنیم $a^{p-1} \overset{p^2}{\equiv} 1$. قرار می‌دهیم $b = a + p$. واضح است که $a \overset{p}{\equiv} b$ و لذا b نیز یک ریشه‌ی اولیه‌ی p است.

ادعا می‌کنیم $b^{p-1} \overset{p^2}{\not\equiv} 1$.

فرض کنید (فرض خلف) $b^{p-1} \overset{p^2}{\equiv} 1$. در این صورت

$$1 \overset{p^2}{\equiv} b^{p-1} = (a+p)^{p-1} = a^{p-1} + (p-1)p\,a^{p-2} + p^2 \overset{p^2}{\equiv} 1 + (p-1)p\,a^{p-2} + 0$$

بنابراین $(p-1)p\,a^{p-2} \overset{p^2}{\equiv} 0$ و لذا $p^2 \mid (p-1)p\,a^{p-2}$ و بنابراین $p \mid a^{p-2}(p-1)$. از این که a ریشه‌ی اولیه‌ی p است لذا $(p, a) = 1$ و در نتیجه $(p, a^{p-2}) = 1$.

حال از لم اقلیدس نتیجه می‌شود $p \mid p-1$ که خلف. بنابراین $b^{p-1} \overset{p^2}{\not\equiv} 1$.

قضیه: فرض کنید p عدد اول فرد و b یک ریشه‌ی اولیه‌ی p باشد بطوری که $b^{p-1} \not\equiv 1 \pmod{p^2}$.
در این صورت b یک ریشه‌ی اولیه در پیمانه‌ی p^2 است.

اثبات: فرض کنید $o_{p^2}(b) = h$ در این صورت $b^h \equiv 1 \pmod{p^2}$. بنابراین
$b^h - 1 \mid p^2$ ولذا $p \mid b^h - 1$. پس $b^h \equiv 1 \pmod{p}$ ولذا $h \mid o_p(b)$
آنگاه b یک ریشه‌ی اولیه‌ی p است. بنابراین $o_p(b) = p-1$. پس $p-1 \mid h$ ①
همچنین از این که $o_{p^2}(b) = h$ لذا $h \mid \varphi(p^2) = p(p-1)$ ②
از روابط ① و ② داریم $p-1 \mid h \mid p(p-1)$. بنابراین
$h = p-1$ یا $h = p(p-1)$.
اگر $h = p-1$ آنگاه $o_{p^2}(b) = p-1$ ولذا $b^{p-1} \equiv 1 \pmod{p^2}$ ×
پس $h = p(p-1) = \varphi(p^2)$. پس b یک ریشه‌ی اولیه در پیمانه‌ی p^2 است.

لم۲: فرض کنید p یک عدد اول فرد و b یک ریشه‌ی اولیه‌ی p باشد به طوری که
$b^{p-1} \not\equiv 1 \pmod{p^2}$. در این صورت برای هر $k \geq 2$، $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.

اثبات: (بطریق استقرا) اگر $k=2$ آنگاه حکم است $b^{p^0(p-1)} \not\equiv 1 \pmod{p^2}$
یعنی $b^{p-1} \not\equiv 1 \pmod{p^2}$ که بنا به فرض لم برقرار است.
اینک فرض کنید رابطه برای k برقرار باشد و آن را برای $k+1$ ثابت می‌کنیم.
پس $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. از طرفی بنا به قضیه‌ی اویلر $b^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$. آنا

$\varphi(p^{k-1}) = p^{k-1} - p^{k-2} = p^{k-2}(p-1)$

$b^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$ پس $p^{k-1} \mid b^{p^{k-2}(p-1)} - 1$ ولذا b و p نسبت اول هستند. بنابراین عدد صحیح t موجود است که $b^{p^{k-2}(p-1)} - 1 = tp^{k-1}$

و ادعا می‌کنیم $p \nmid t$. زیرا اگر $p \mid t$ آنگاه $p^k \mid tp^{k-1} = b^{p^{k-2}(p-1)} - 1$

ولذا $b^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$ که تناقض با فرض استقرا است. پس $p \nmid t$.

حال:

$$b^{p^{k-2}(p-1)} = 1 + p^{k-1}t$$

$$\xrightarrow{\text{به توان } p} b^{p^{k-1}(p-1)} = (1 + p^{k-1}t)^p = 1 + p^k t + p^{k+1}\cdot(\cdots)$$

$$\equiv 1 + p^k t \pmod{p^{k+1}}$$

واضح است که $b^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$ زیرا اگر $b^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{k+1}}$ آنگاه $p^{k+1} \mid b^{p^{k-1}(p-1)} - 1$ و درنتیجه $p^{k+1} \mid p^k t$ که تناقض است. پس $p \mid t$ که تناقض است. بنابراین $b^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$ که حکم استقرا را ثابت می‌کند.

قضیه. اگر p عدد اول فرد و b یک ریشه‌ی اولیه‌ی p باشد به طوری که $b^{p-1} \not\equiv 1 \pmod{p^2}$ در این صورت برای هر $k \geq 1$، b یک ریشه‌ی اولیه‌ی p^k است.

اثبات. فرض کنید $o_{p^k}(b) = h$. در این صورت:

① $b^h \equiv 1 \pmod{p^k} \longrightarrow p^k \mid b^h - 1 \longrightarrow p \mid b^h - 1 \longrightarrow b^h \equiv 1 \pmod{p} \longrightarrow p-1 = o_p(b) \mid h$

همچنین از این که $o_{p^k}(b)=h$ نتیجه می‌شود ② $h \mid \varphi(p^k)=p^{k-1}(p-1)$

①، ② $\longrightarrow$ $h=p^{\alpha}(p-1)$ $\quad 0 \le \alpha \le k-1$

ادعا: $\alpha=k-1$

فرض کنید (فرض خلف) چنین نباشد. در این صورت $\alpha \le k-2$. اکنون:

$$b^{h} \overset{p^k}{\equiv} 1 \longrightarrow b^{p^{\alpha}(p-1)} \overset{p^k}{\equiv} 1 \xrightarrow{\uparrow p^{k-2-\alpha}} b^{p^{k-2}(p-1)} \overset{p^k}{\equiv} 1$$

که با نتیجه‌ی لم ۲ تناقض است. پس برای این $\alpha=k-1$ و لذا $o(b)=p^{k-1}(p-1)$

پس b یک ریشه‌ی اولیه در پیمانه‌ی p^k است.

قضیه. اگر p عدد اول فرد باشد، آنگاه ریشه‌ی اولیه در پیمانه‌ی $2p^k$ موجود است.

اثبات. فرض کنید b ریشه‌ی اولیه در پیمانه‌ی p^k باشد. در این حالت، مطلوب، b فرد است. چنانچه b زوج باشد، قرار می‌دهیم $b'=b+p^k$. واضح است که b' فرد است، و از این که $b' \overset{p^k}{\equiv} b$ و b یک ریشه‌ی اولیه‌ی p^k است نتیجه b' نیز یک ریشه‌ی اولیه‌ی p^k است (و البته عددی فرد است)

پس از ابتدا می‌توانستیم فرض کنیم b عددی فرد است. نشان می‌دهیم b یک ریشه‌ی اولیه‌ی $2p^k$ نیز می‌باشد. برای این منظور فرض کنید $h=o_{2p^k}(b)$، در این صورت

$$b^{h} \overset{2p^k}{\equiv} 1 \longrightarrow b^{h} \overset{p^k}{\equiv} 1 \longrightarrow \varphi(p^k)=o_{p^k}(b) \mid h \quad ①$$

بعلاوه از این که $h = o(b) \mid \varphi(2p^k)$ خواهیم داشت $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ (۲)

$$\textcircled{1},\textcircled{2} \longrightarrow \quad \varphi(p^k) \mid h \mid \varphi(p^k)$$

بنابراین $h = \varphi(p^k) = \varphi(2p^k)$ و لذا b یک ریشه‌ی اولیه‌ی $2p^k$ است.

توجه کنید $2p^k$ عددی زوج است و از این که ریشه‌ی اولیه در پیمانه‌ی $2p^k$ عدد فرد است با $2p^k$ متباین باشد، لذا باید عددی فرد باشد.

از آنچه در وقت‌های قبل بیان شد در مراحل زیر می‌توان ریشه‌ی اولیه در پیمانه‌های p^k و $2p^k$ یا 2 را عدد اول فرد p یافت.

فرض کنید p عدد اول فرد باشد

مرحله ① ابتدا ریشه‌ی اولیه‌ای در پیمانه‌ی p می‌یابیم، و آن را a می‌نامیم.

دو حالت ممکن است رخ دهد.

الف. $a^{p-1} \neq 1 \pmod{p^2}$ ب. $a^{p-1} \equiv 1 \pmod{p^2}$

همانگونه که حالت دوم رخ دهد با جایگزین کردن $b = a + p$ به جای a خواهیم داشت $b^{p-1} \not\equiv 1 \pmod{p^2}$. پس می‌توان b را چنان یافت که b یک ریشه‌ی اولیه در پیمانه‌ی p بوده و $b^{p-1} \not\equiv 1 \pmod{p^2}$. در این صورت

مرحله ② b یک ریشه‌ی اولیه در پیمانه‌ی p^2 و

مرحله ③ b یک ریشه‌ی اولیه در پیمانه‌ی p^k (با ازای هر $k \geq 2$) می‌باشد.

اکنون اگر b فرد نباشد آنگاه

مرحله ۲ b یک ریشه‌ی اولیه در پیمانه‌ی p^k خواهد بود.

وچنانچه b زوج باشد، $b' = b + p^k$ این خاصیت را دارد.

قضیه‌ی زیر محکی گویا در تشخیص ریشه‌ی اولیه در پیمانه‌ی p است.

قضیه. اگر p یک عدد اول فرد بوده و a یک ریشه‌ی اولیه‌ی p باشد. در این صورت

$$a^{\frac{p-1}{2}} \overset{p}{\equiv} -1$$

اثبات. فرض کنید a یک ریشه‌ی اولیه در پیمانه‌ی p باشد. در این صورت:

$$a^{p-1} \overset{p}{\equiv} 1 \longrightarrow p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$$

$$\rightarrow \begin{cases} p \mid a^{\frac{p-1}{2}} - 1 \longrightarrow a^{\frac{p-1}{2}} \overset{p}{\equiv} 1 \longrightarrow p-1 = o_p(a) < \frac{p-1}{2} \quad \text{ناممکن} \\ \text{یا} \\ p \mid a^{\frac{p-1}{2}} + 1 \longrightarrow a^{\frac{p-1}{2}} \overset{p}{\equiv} -1 \end{cases}$$

مثال: نشان دهید ۳ یک ریشه‌ی اولیه در پیمانه‌ی ۷ است و ریشه‌ی اولیه‌ای برای 7^2 و 2×7^k بیابید.

حل. $\frac{p-1}{2} = 3$ و $3^3 = 27 \overset{7}{\equiv} -1$. لذا ۳ یک ریشه‌ی اولیه در پیمانه‌ی ۷ است.

اکنون باید بررسی کنیم که $3^{p-1} = 3^6 \overset{7^2}{\equiv} ?$ ،

$3^2 = 9$ ، $3^4 = 9^2 = 81 \overset{49}{\equiv} -17$

$3^6 = 3^2 \times 3^4 \overset{49}{\equiv} 9 \times (-17) = -153 \overset{49}{\equiv} -6 \not\equiv 1$

بنابراین ۳ یک ریشه‌ی اولیه در پیمانه‌ی $49 = p^2$ و 7^k برای هر $k \geq 2$ است.

واز این که ۳ عددی فرد است لذا ۳ یک ریشه‌ی اولیه‌ی 17^k و 2×17^k (برای هر $k\in\mathbb{Z}^+$) نیز هست.

مثال. نشان دهید ۳ یک ریشه‌ی اولیه در پیمانه‌ی ۱۷ است و با استفاده از آن ریشه‌ی اولیه‌ای در پیمانه‌های 17^k و 2×17^k بیابید.

حل: $\frac{p-1}{2}=8$ و

$$3^2=9\ ,\ 3^4=81\overset{17}{\equiv}-4\ ,\ 3^8\overset{17}{\equiv}(-4)^2=16\overset{17}{\equiv}-1$$

بنابراین ۳ یک ریشه‌ی اولیه در پیمانه‌ی ۱۷ است.

اکنون باید بررسی کنیم که $3^{p-1}=3^{16}\overset{17^2}{\equiv}1$ ؟ $(17^2=289)$

$$3^2=9\ ,\ 3^4=81\ ,\ 3^8=6561\overset{17^2}{\equiv}203\ ,\ 3^{12}=4120\overset{17^2}{\equiv}171\neq 1$$

بنابراین ۳ یک ریشه‌ی اولیه در پیمانه‌ی 17^2، 17^k و 2×17^k برای هر $k\in\mathbb{Z}^+$ می‌باشد.

یادآوری: اگر a یک ریشه‌ی اولیه در پیمانه‌ی p باشد آنگاه $\{a^1,a^2,\dots,a^{p-1}\}$ یک دستگاه مخفف مانده‌ها در پیمانه‌ی p است، از این حکم استفاده کرده سوال بعد را حل می‌کنیم.

مسأله ۱: نشان دهید معادله‌ی همنشتی $x^4\overset{11}{\equiv}6$ دارای جواب نیست.

حل: به راحتی می‌توان دید ۲ یک ریشه‌ی اولیه‌ی ۱۱ است. چون $2^5=32\overset{11}{\equiv}-1$.

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

از این که $6 \overset{11}{\equiv} x^4$ لذا $(x,11)=1$. اگر معادله‌ی $6 \overset{11}{\equiv} x^6$ دارای جواب باشد آنگاه y موجود است که $x \overset{11}{\equiv} 2^y$. همچنین از جدول بالا می‌توان دید $6 \overset{11}{\equiv} 2^9$

$$x^6 \overset{11}{\equiv} 6 \longrightarrow (2^y)^4 \overset{11}{\equiv} 2^9 \longrightarrow 2^{4y} \overset{11}{\equiv} 2^9 \xrightarrow{\times 9} 4y \overset{10}{\equiv} 9 \cdot 9 \equiv 1$$

پس معادله‌ی $x^6 \overset{11}{\equiv} 6$ دارای جواب نیست.

مسأله. نشان دهید $x^4 \overset{11}{\equiv} 3$ دارای جواب است و جواب‌های آن را بیابید.

حل. از جدول بالا می‌توان دید $3 \overset{11}{\equiv} 2^8$. اگر $x \overset{11}{\equiv} 2^y$ آنگاه:

$$x^4 \overset{11}{\equiv} 3 \longrightarrow (2^y)^4 \overset{11}{\equiv} 2^8 \longrightarrow 2^{4y} \overset{11}{\equiv} 2^8 \longrightarrow 4y \overset{10}{\equiv} 8$$

$$\xrightarrow{\div 4} y \overset{5}{\equiv} 2 \longrightarrow y = 5k+2$$

بنابراین: $x \overset{11}{\equiv} 2^y = 2^{5k+2} = 4(2^5)^k \equiv 4(-1)^k = \pm 4$

قانون تعادل مربعی

مثال. معادله‌ی همنهشتی $5x^2+9x+11 \overset{13}{\equiv} 0$ را حل کنید.

$$5x^2+9x+11 \overset{13}{\equiv} 0 \longrightarrow 5x^2+9x \overset{13}{\equiv} -11 \equiv 2$$

$$\xrightarrow{\times 5^*} x^2+72x \overset{13}{\equiv} 16 \longrightarrow x^2-6x \overset{13}{\equiv} 3$$

$$\longrightarrow x^2-6x+9 \overset{13}{\equiv} 9+3 \longrightarrow (x-3)^2 \overset{13}{\equiv} -1$$

اگر قرار دهیم $x-3=y$، کافی است $y^2 \overset{13}{\equiv} -1$ را حل کنیم.

معادله‌ی همنشتی انجر به دو روش قابل حل است.

روش اول استفاده از یک دستگاه کامل مانده‌ای در پیمانه‌ی ۱۳ است. برای این منظور

دستگاه کامل مانده‌گی $\{0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6\}$

$0^2 \overset{13}{\equiv} 0 \not\equiv -1$

$(\pm1)^2 \overset{13}{\equiv} 1 \not\equiv -1$

$(\pm2)^2 \equiv 4 \not\overset{13}{\equiv} -1$

$(\pm3)^2 \equiv 9 \not\overset{13}{\equiv} -1$

$(\pm4)^2 \equiv 16 \not\overset{13}{\equiv} -1$

$(\pm5)^2 \equiv 25 \overset{13}{\equiv} -1$

$(\pm6)^2 \equiv 36 \not\overset{13}{\equiv} -1$

بنابراین تنها جواب‌های $y^2 \overset{13}{\equiv} -1$ عبارتند از $y \equiv \pm5$. اما $y = x-3$. بنابراین:

$x = y+3 = \pm5+3 \rightarrow x_1 \equiv -2$

$\rightarrow x_2 \equiv 8$

جواب‌های معادله‌ی همنشتی $5x^2+9x+11 \overset{13}{\equiv} 0$ می‌شوند.

روش دوم استفاده از یک ریشه‌ی اولیه در پیمانه‌ی ۱۳ است.

۲ یک ریشه‌ی اولیه‌ی ۱۳ است، چون: $2^6 = 64 \overset{13}{\equiv} -1$

k	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
2^k	۲	۴	۸	۳	۶	۱۲	۱۱	۹	۵	۱۰	۷	۱

(۱-)

می‌خواهیم معادله‌ی $y^2 \overset{13}{\equiv} -1$ را حل کنیم. توضیح $1 = \text{ind}_2(13)$. فرض کنید

از طرفی، $y \overset{13}{\equiv} 2^z$ ، $-1 \overset{13}{\equiv} 2^6$

$$y^2 \overset{13}{\equiv} -1 \longrightarrow (2^z)^2 \overset{13}{\equiv} 2^6 \longrightarrow 2^{2z} \overset{13}{\equiv} 2^6$$

$$\longrightarrow 2z \overset{12}{\equiv} 6 \xrightarrow{\div 2} z \overset{6}{\equiv} 3 \longrightarrow z = 6k+3$$

$$\longrightarrow y = 2^z = 2^{6k+3} = (2^6)^k \times 2^3$$

$$= (-1)^k \times 8 = \pm 8 = \mp 5$$

که همان جواب‌های قسمت قبل می‌باشند.

در حالت کلی معادله‌ی همنهشتی درجه دوم $ax^2+bx+c \overset{p}{\equiv} 0$ را در نظر بگیرید که در آن p عددی اول و فرد است و $(a,p)=1$. فرض کنید a^* عکس حسابی a در پیمانه‌ی p باشد.

$$ax^2+bx \overset{p}{\equiv} -c \xrightarrow{\times a^*} x^2 + a^*bx \overset{p}{\equiv} -a^*c$$

چون p فرد است لذا وارون حسابی ۲ موجود است. ($2^* = \frac{p+1}{2}$)

بنابراین:

$$x^2 + a^*bx + (2^*a^*b)^2 \overset{p}{\equiv} (2^*a^*b)^2 - a^*c$$

$$\longrightarrow (x + 2^*a^*b)^2 \overset{p}{\equiv} (2^*a^*b)^2 - a^*c$$

چنانچه قرار دهیم $y = x + 2^*a^*b$ و $d = (2^*a^*b)^2 - a^*c$ ، آنگاه معادله‌ی اخیر به شکل $y^2 \overset{p}{\equiv} d$ ساده خواهد شد.

هدف از این بخش، حل معادلاتی همنهشتی $x^2 \overset{p}{\equiv} a$ است که p عددی اول و فرد است.

تعریف. فرض کنید p عددی اول و فرد باشد و $(a,p)=1$، در این صورت a را مانده‌ی مربعی در پیمانه‌ی p گوئیم هرگاه معادله‌ی همنهشتی $x^2 \overset{p}{\equiv} a$ دارای جواب باشد. در غیر این صورت آن را نامانده‌ی مربعی می‌نامیم.

مثال. $p=11$ را در نظر بگیرید. $\{\pm 5, \ldots, \pm 1, 0\}$ یک دستگاه کامل مانده‌ها است.

$$1^2 = (\pm 1)^2 \equiv 12 \equiv (\pm 2)^2 \equiv 9 = (\pm 3)^2 \equiv 4 = (\pm 2)^2 \equiv 5 \equiv (\pm 4)^2 \pmod{11}$$

بنابراین مانده‌های مربعی در پیمانه‌ی ۱۱ عبارتند از ۱، ۳، ۴، ۵ و ۹

و نامانده‌های مربعی در پیمانه‌ی ۱۱ عبارتند از ۲، ۶، ۷، ۸ و ۱۰.

در حالت کلی اگر p عددی اول و فرد باشد آنگاه $\{\pm(\frac{p-1}{2}), \ldots, \pm 1, 0\}$ یک دستگاه کامل مانده‌ها در پیمانه‌ی p است و لذا مانده‌های مربعی عبارتند از

$$0^2, (\tfrac{p-1}{2})^2, \ldots, 3^2, 2^2, 1^2$$

بنابراین در پیمانه‌ی p، دقیقاً $\frac{p-1}{2}$ مانده و $\frac{p-1}{2}$ نامانده‌ی مربعی وجود دارند.

قضیه. فرض کنید p عددی اول و فرد باشد و $(a,p)=1$. در این صورت معادله‌ی همنهشتی $x^2 \overset{p}{\equiv} a$ دارای جواب است اگر و تنها اگر $a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$.

اثبات. ابتدا فرض کنید $x^2 \overset{p}{\equiv} a$ دارای جواب x_0 باشد.

پس $x_0^2 \overset{p}{\equiv} a$، اکنون بنابه قضیه‌ی فرما،

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \overset{p}{\equiv} 1$$

پس $a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$،

برعکس: فرض کنید $a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$، اگر g یک ریشه‌ی اولیه (پیمانه‌ی p) باشد آنگاه

b موجود است طوری که $a = g^b$. اکنون:

$$a^{\frac{p-1}{2}} \overset{p}{\equiv} 1 \longrightarrow (g^b)^{\frac{p-1}{2}} \overset{p}{\equiv} 1 \longrightarrow g^{\frac{b(p-1)}{2}} \overset{p}{\equiv} 1$$

پس $p-1 = o_p(g) \mid \frac{b(p-1)}{2}$.

با حذف $p-1$ از طرفین داریم $\frac{b}{2} \mid 1$ و لذا b زوج است. اگر $b=2k$

با قرار دادن $x = g^k$ جواب است:

$$x^2 = (g^k)^2 = g^{2k} = g^b \overset{p}{\equiv} a$$

یعنی $x^2 \overset{p}{\equiv} a$ دارای جواب است،

با توجه به تعریف مانده‌ی مربعی و قضیه قبل، می‌توان نتیجه‌ی زیر را بیان کرد:

نتیجه: فرض کنید p عددی اول و فرد باشد و $(a,p)=1$. در این صورت a مانده‌ی

مربعی (پیمانه‌ی p) است اگر و تنها اگر $a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$، □

حال با توجه به این که p فرد است، $p-1$ زوج است. بنابراین:

$$a^{p-1} \overset{p}{\equiv} 1 \rightarrow p \mid a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)$$ قضیه فرما

لم اقلیدس $\rightarrow$
$$\begin{cases} p \mid a^{\frac{p-1}{2}}-1 \rightarrow a^{\frac{p-1}{2}} \overset{p}{\equiv} 1 \\ p \mid a^{\frac{p-1}{2}}+1 \rightarrow a^{\frac{p-1}{2}} \overset{p}{\equiv} -1 \end{cases}$$

پس اگر $(a,p)=1$ آنگاه همواره $a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$ یا $a^{\frac{p-1}{2}} \overset{p}{\equiv} -1$.

بنابراین اگر $a^{\frac{p-1}{2}} \not\overset{p}{\equiv} 1$ آنگاه $a^{\frac{p-1}{2}} \overset{p}{\equiv} -1$. بنابراین ثابت کرده‌ایم:

نتیجه: اگر p عدد اول فرد بوده و $(a,p)=1$ بعلاوه a نامانده‌ی مربعی باشد آنگاه

$a^{\frac{p-1}{2}} \overset{p}{\equiv} 1$.

نماد لژاندر

فرض کنید p یک عدد اول فرد باشد و $(a,p)=1$. در این صورت نماد $(\frac{a}{p})$ را بصورت زیر تعریف می‌کنیم:

$$(\frac{a}{p})=\begin{cases} 1 & a \text{ نامانده‌ی مربعی به پیمانه‌ی } p \text{ باشد} \\ -1 & \text{در غیر این صورت} \end{cases}$$

مثال: $x^2 \overset{5}{\equiv} -1$ دارای جواب $x=2$ است. پس -1 نامانده‌ی مربعی به پیمانه‌ی 5 است. بنابراین $(\frac{-1}{5})=1$.

مثال. به راحتی می‌توان دید $x^2 \equiv -1 \pmod 3$ دارای جواب نیست. بنابراین $\left(\frac{-1}{3}\right) = -1$.

قضیه. فرض کنید p یک عدد اول فرد بوده و a و b اعداد صحیح نسبت به p باشند، $(p \nmid a, p \nmid b)$. در این صورت:

الف) $\left(\frac{a^2}{p}\right) = 1$

ب) $\left(\frac{1}{p}\right) = 1$

ج) اگر $a \equiv b \pmod p$ آنگاه $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

اثبات. الف) بوضوح $x^2 \equiv a^2 \pmod p$ دارای جواب $x = a$ است. پس $\left(\frac{a^2}{p}\right) = 1$.

ب) از رابطه الف) نتیجه می‌شود.

ج) فرض کنید $b \equiv a \pmod p$. اگر $\left(\frac{a}{p}\right) = 1$ آنگاه $x^2 \equiv a \pmod p$ دارای جواب x_0 است. بنابراین $x_0^2 \equiv a \pmod p$. از طرفی $a \equiv b \pmod p$. بنابراین $x_0^2 \equiv b \pmod p$ و لذا $\left(\frac{b}{p}\right) = 1$.

حال اگر $\left(\frac{a}{p}\right) = -1$ آنگاه $\left(\frac{b}{p}\right) \neq 1$. زیرا در غیر اینصورت $\left(\frac{b}{p}\right) = 1$ و لذا بنا به حالت قبل، $\left(\frac{a}{p}\right) = 1$ که تناقض است. پس در هر حال $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$.

قضیه (محک اویلر) فرض کنید p یک عدد اول فرد بوده و $(a,p) = 1$. در این صورت $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

اثبات. از قبل می‌دانیم:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{اگر } a \text{ مانده‌ی مربعی به پیمانه‌ی } p \text{ باشد.} \\ -1 & \text{اگر } a \text{ ناماندهٔ مربعی به پیمانه‌ی } p \text{ باشد} \end{cases}$$

همچنین نیز به تعریف:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{اگر } a \text{ مانده‌ی مربعی به پیمانه‌ی } p \text{ باشد.} \\ -1 & \text{اگر } a \text{ ناماندهٔ مربعی به پیمانه‌ی } p \text{ باشد} \end{cases}$$

اکنون با مقایسه‌ی دو رابطه‌ی اخیر خواهیم داشت: $\left(\frac{a}{p}\right) \overset{p}{\equiv} a^{\frac{p-1}{2}}$.

نتیجه ۱. اگر $(a,p)=1$ و $(b,p)=1$ آنگاه $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

اثبات:

$$\left(\frac{ab}{p}\right) \overset{p}{\equiv} (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \overset{p}{\equiv} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

بنابراین $\left(\frac{ab}{p}\right) \overset{p}{\equiv} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

حال از این که p عددی فرد است لذا $1 \neq -1 \pmod{p}$. از طرفی طرفین رابطه‌ی هم‌نشتی بالا یا 1 یا -1 می‌باشند، پس هر دو طرف همزمان 1 یا هر دو طرف -1 می‌باشند، در واقع $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

نتیجه ۲. برای هر عدد اول فرد p، $(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$،

اثبات. بنا به محک اویلر $(-1)^{\frac{p-1}{2}} \overset{p}{\equiv} \left(\frac{-1}{p}\right)$. و چون طرفین رابطه‌ی هم‌نشتی

اخیر ۱ یا ۱- می‌باشند لذا همیشه نتیجه‌ی ۱، دو طرف برابرند. یعنی $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

مثال. بررسی کنید معادله‌ی همنهشتی $x^2 \overset{47}{\equiv} 38$ دارای جواب است یا خیر؟

حل. باید $(\frac{38}{47})$ را محاسبه کنیم.

از آنجا که $38 \overset{47}{\equiv} -9$، بنابراین $(\frac{38}{47}) = (\frac{-9}{47})$ است.

$$(\frac{-9}{47}) = (\frac{-1}{47})(\frac{9}{47})$$

از طرفی $(\frac{9}{47}) = 1$ (چون $9 = 3^2$).

همچنین $(\frac{-1}{47}) = (-1)^{\frac{47-1}{2}} = (-1)^{23} = -1$. پس

$$(\frac{38}{47}) = (\frac{-9}{47}) = (\frac{-1}{47})(\frac{9}{47}) = (-1)(1) = -1$$

بنابراین $x^2 \overset{47}{\equiv} 38$ دارای جواب نیست.

در حالت کلی اگر a یک عدد صحیح باشد و $a = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

آنگاه $(\frac{a}{p}) = (\frac{\pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}}{p}) = (\frac{\pm 1}{p})(\frac{p_1}{p})^{\alpha_1} \cdots (\frac{p_k}{p})^{\alpha_k}$

بنابراین برای محاسبه‌ی $(\frac{a}{p})$ کافی است برای هر i، $(\frac{p_i}{p})$ محاسبه شود.

بعداً (در بحث قانون تقابل مربعی) برای هر p و q اول، $(\frac{p}{q})$ را محاسبه می‌کنیم.

لم زیر موسوم به لم گاوس یکی از احکام کاربردی این بخش است. این لم را بدون اثبات می‌پذیریم

لم گاوس: فرض کنید p یک عدد اول فرد بوده و $(a,p)=1$، اعداد

$$a\times 1,\ a\times 2,\ \dots,\ a\times\frac{p-1}{2}$$

را در نظر گرفته و به جای هر کدام، عدد هم نهشت با آن را در فاصله‌ی $-\frac{p-1}{2}$ و $\frac{p-1}{2}$ قرار می‌دهیم. اگر n تعداد اعداد منفی در دنباله‌ی اخیر n باشد، آنگاه $\left(\frac{a}{p}\right)=(-1)^n$.

مثال: با استفاده از لم گاوس $\left(\frac{3}{7}\right)$ را محاسبه می‌کنیم، $p=7$ و $a=3$.

$$a\times 1=3\overset{7}{\equiv}3 \qquad a\times 2=6\overset{7}{\equiv}-1 \qquad a\times 3=9\overset{7}{\equiv}2$$

$n=1$ و لذا $\left(\frac{3}{7}\right)=(-1)^1=-1$.

مثال: $\left(\frac{8}{17}\right)$ را محاسبه کنید. $p=17$ و $a=8$

$$a\times 1=8\overset{17}{\equiv}8 \qquad a\times 2=16\overset{17}{\equiv}-1$$

$$a\times 3=24\overset{17}{\equiv}7 \qquad a\times 4=32\overset{17}{\equiv}-2$$

$$a\times 5=40\overset{17}{\equiv}6 \qquad a\times 6=48\overset{17}{\equiv}-3$$

$$a\times 7=56\overset{17}{\equiv}5 \qquad a\times 8=64\overset{17}{\equiv}-4$$

(در واقع دستگاه کامل مانده‌ای $\{8,7,\dots,-8\}$ را در نظر گرفته‌ایم.)

پس $n=4$ و لذا $\left(\frac{8}{17}\right)=(-1)^4=1$.

توجه: $\left(\frac{2}{17}\right)=1\times\left(\frac{2}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{2}{17}\right)^2=\left(\frac{2}{17}\right)^3=\left(\frac{2}{17}\right)^4=\left(\frac{8}{17}\right)$

بنابراین از این به بعد می‌توانیم $\left(\frac{2}{17}\right)$ را محاسبه کنیم.

تمرین: $\left(\frac{2}{17}\right)$ را محاسبه کرده و حل خود را با حل بالا مقایسه کنید.

مثال. فرض کنید p یک عدد اول فرد باشد و با استفاده از لم گاوس، $\left(\frac{-1}{p}\right)$ را محاسبه کنید.

حل. اعداد

$$(-1),\ (-1)\times 2,\ (-1)\times 3,\ \dots,\ (-1)\frac{p-1}{2}$$

را در نظر می‌گیریم. اگر دستگاه کامل مانده‌های $\left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}$ را در نظر بگیریم، اعداد دنباله‌ی بالا در هم‌نهشتی با یکی از اعداد دستگاه کامل مانده‌های اینجا عبارتند از:

$$-1,\ -2,\ -3,\ \dots,\ -\frac{p-1}{2}$$

که همگی منفی هستند. پس $v = \frac{p-1}{2}$ و لذا بنا به لم گاوس،

$$\left(\frac{-1}{p}\right) = (-1)^{v} = (-1)^{\frac{p-1}{2}}.$$

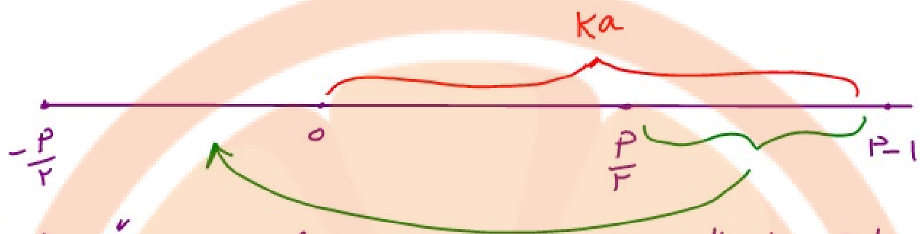
مسأله. فرض کنید p یک عدد اول فرد است و $\left(\frac{2}{p}\right)$ را محاسبه کنید.

حل. مجموعه‌ی

$$S = \left\{2,\ 2\times 2,\ \dots,\ 2\frac{p-1}{2}\right\} = \{2, 4, \dots, p-1\}$$

را در نظر می‌گیریم. برای استفاده از لم گاوس، باید اعداد هم‌نهشت با هر کدام از اعداد مجموعه‌ی بالا در پیمانه‌ی p و در دستگاه کامل مانده‌های $\left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}$ را محاسبه کنیم و تعداد اعداد منفی را بشماریم.

واضح است که برای $1 \le k \le \frac{p-1}{2}$، $2 \le ka \le p-1$. ($a = 2$)



برای انجام فرایند لم گاوس، اعداد فاصله‌ی $[0, \frac{p}{2}]$ در جایگاه خود باقی می‌مانند ولی اعداد فاصله‌ی $[\frac{p}{2}, p-1]$ به فاصله‌ی $[-\frac{p}{2}, 0]$ منتقل می‌شوند. و بنابراین برای شمارش تعداد اعداد منفی کافی است تعداد ka هایی را بشماریم که در فاصله‌ی $[\frac{p}{2}, p-1]$ قرار می‌گیرند. به عبارت دیگر

$$\frac{p}{2} < ka < p$$

و چون $a = 2$ لذا باید تعداد k هایی را بشماریم که $\frac{p}{2} < 2k < p$ یا

$$\frac{p}{4} < k < \frac{p}{2}$$

فرض کنید $p = 8m + r$ که $0 \leq r < 8$. واضح است که به ازای $r = 0, 2, 4, 6$ مقدار p زوج خواهد بود که تناقض است. پس $r = 1$ یا 3 یا 5 یا 7.

الف) بررسی حالت $p = 8m + 1$:

$$\frac{p}{4} < k < \frac{p}{2} \longrightarrow \frac{8m+1}{4} < k < \frac{8m+1}{2} \longrightarrow 2m + \frac{1}{4} < k < 4m + \frac{1}{2}$$

$$\longrightarrow 2m+1 \leq k \leq 4m \longrightarrow v = \text{تعداد } k \text{ ها} = (4m) - (2m+1) + 1 = 2m$$

و در این حالت $(\frac{2}{p}) = (-1)^{v} = (-1)^{2m} = 1$.

ب) بررسی حالت $p = 8m + 3$:

$$\frac{p}{4} < k < \frac{p}{2} \longrightarrow \frac{8m+3}{4} < k < \frac{8m+3}{2} \longrightarrow 2m + \frac{3}{4} < k < 4m + \frac{3}{2}$$

$$\longrightarrow 2m+1 \leq k \leq 4m+1 \longrightarrow \text{تعداد } k \text{ ها } v = (4m+1) - (2m+1) + 1 = 2m+1$$

و در این حالت $\left(\frac{2}{p}\right) = (-1)^{v} = (-1)^{2m+1} = -1$.

ج) بررسی حالت $p = 8m+5$.

$$\frac{p}{4} < k < \frac{p}{2} \rightarrow \frac{8m+5}{4} < k < \frac{8m+5}{2} \rightarrow 2m + \frac{5}{4} < k < 4m + \frac{5}{2}$$

$$\rightarrow 2m+2 \leq k \leq 4m+2 \rightarrow \text{تعداد } k\text{ ها } \; v = (4m+2) - (2m+2) + 1 = 2m+1$$

و در این حالت $\left(\frac{2}{p}\right) = (-1)^{v} = (-1)^{2m+1} = -1$

د) بررسی حالت $p = 8m+7$.

$$\frac{p}{4} < k < \frac{p}{2} \rightarrow \frac{8m+7}{4} < k < \frac{8m+7}{2} \rightarrow 2m + \frac{7}{4} < k < 4m + \frac{7}{2}$$

$$\rightarrow 2m+2 \leq k \leq 4m+3 \rightarrow \text{تعداد } k\text{ ها } \; v = (4m+3) - (2m+2) + 1 = 2m+2$$

و در این حالت $\left(\frac{2}{p}\right) = (-1)^{v} = (-1)^{2m+2} = 1$.

از آنچه در بالا محاسبه شد، به طور خلاصه می‌توان گفت

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p = 8m+1 \text{ یا } 8m+7 \\ -1 & p = 8m+3 \text{ یا } 8m+5 \end{cases}$$

یا :

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \overset{8}{\equiv} 1 \text{ یا } 7 \\ -1 & p \overset{8}{\equiv} 3 \text{ یا } 5 \end{cases}$$

یا :

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \overset{8}{\equiv} \pm 1 \\ -1 & p \overset{8}{\equiv} \pm 3 \end{cases}$$

در زیر با بیانی ساده محکی ساده‌تر برای $\left(\frac{2}{p}\right)$ به دست می‌آوریم .

چنانچه $p \overset{8}{\equiv} \pm 1$ به راحتی می‌توان دید $\frac{p^2-1}{8}$ عددی صحیح و زوج است

و اگر $p \overset{8}{\equiv} \pm 3$ آنگاه $\frac{p^2-1}{8}$ عددی صحیح و فرد است. بنابراین:

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \overset{8}{\equiv} \pm 1 \\ -1 & p \overset{8}{\equiv} \pm 3 \end{cases}$$

با مقایسه‌ی رابطه‌ی اخیر با آخرین مقدار برای $(\frac{2}{p})$ می‌توان دید:

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

مثال: $(\frac{2}{17}) = ?$

روش اول: $17 \overset{8}{\equiv} 1 \leftarrow (\frac{2}{17}) = 1$

روش دوم: $(\frac{2}{17}) = (-1)^{\frac{17^2-1}{8}} = (-1)^{36} = 1$

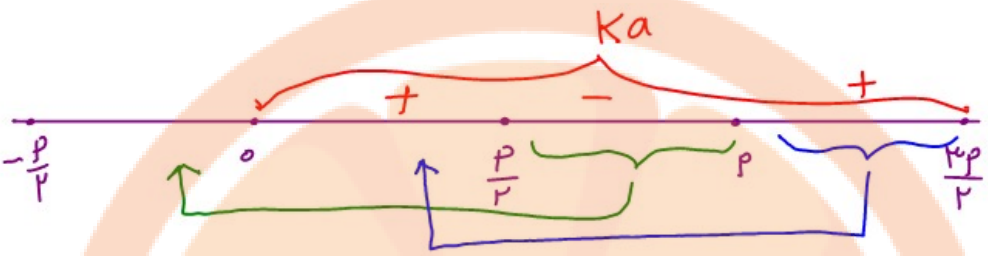
مسأله: مقدار $(\frac{3}{p})$ را به ازای عدد اول فرد p محاسبه کنید.

حل: برای آشنایی با لم گاوس،

$$S = \{3, 6, \dots, 3\frac{p-1}{2}\}$$

را در نظر می‌گیریم، اعداد این مجموعه در فاصله‌ی $]0, \frac{3p}{2}[$ قرار دارند.

برای شمارش تعداد k هایی که پس از محاسبه‌ی $\pmod p$ در دسته‌ی کامل مانده‌های $\{\frac{p-1}{2}, \dots, -\frac{p-1}{2}\}$ مقداری منفی دارند، کافی است تعداد k هایی را بشماریم که $p < 3k < \frac{p}{2}$. (شکل زیر)



$\frac{p}{2} < ka < p$ و چون $a=3$ لذا کافی است مقدار k هایی را بشماریم

که $\frac{p}{2} < 3k < p$. یعنی $\frac{p}{6} < k < \frac{p}{3}$.

برای این منظور فرض می کنیم $p = 12m + r$ که در آن $0 \le r < 12$.

به راحتی می توان دید مقادیر $r = 0, 2, 3, 4, 6, 8, 9, 10$ قابل قبول نیستند .

بنابراین $r = 1$ یا 5 یا 7 یا 11 .

استدلالی مشابه حالت $a=2$ نشان می دهد :

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p = 12m+1 \text{ یا } 12m+11 \\ -1 & p = 12m+5 \text{ یا } 12m+7 \end{cases}$$

و بطور خلاصه

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \overset{12}{\equiv} \pm 1 \\ -1 & p \overset{12}{\equiv} \pm 5 \end{cases}$$

تمرین . $\left(\frac{5}{p}\right)$ را به ازای عدد اول فرد p محاسبه کنید.

قانون تقابل مربعی

فرض کنید p و q دو عدد اول فرد باشند. سئوالی که مطرح است این است که آیا معادله تطابقی

$x^2 \equiv p \pmod{q}$ ، $x^2 \equiv q \pmod{p}$ ارتباطی دارند؟

قانون تقابل مربعی به این سئوال پاسخ می دهد.

لم، فرض کنید p یک عدد اول فرد و a یک عدد صحیح فرد متباین با p باشد، در این صورت

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}$$

که در آن $[\ ]$ نشانگر تابع جزء صحیح است.

اثبات. برای اثبات از لم گاوس استفاده می کنیم، برای این منظور فرض کنید

$$S = \left\{a, 2a, \dots, \frac{p-1}{2}a\right\}$$

باقیمانده هر کدام از اعداد مجموعه ی S را در دستگاه کامل مانده ای $\left\{\frac{p-1}{2}, \dots, -\frac{p-1}{2}\right\}$ محاسبه کنیم،

بنا به الگوریتم تقسیم

$$ka = h_k p + t_k \qquad 0 \le t_k < p$$

توجه کنید در این صورت

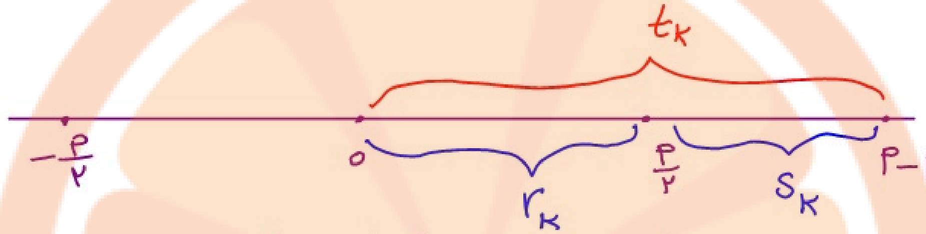
$$\frac{ka}{p} = h_k + \frac{t_k}{p}$$

و چون $0 \le \frac{t_k}{p} < 1$ بنابراین $\left[\frac{ka}{p}\right] = h_k$ پس می توان نوشت:

$$ka = \left[\frac{ka}{p}\right] p + t_k$$

برای استفاده از لم گاوس، بجای ka با t_k کار می کنیم و هفتشت آنها را در دستگاه کامل مانده ی $\left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}$ محاسبه می کنیم،

فرض کنید پس از این فرایند w مقدار منفی و v مقدار مثبت ایجاد شود ،

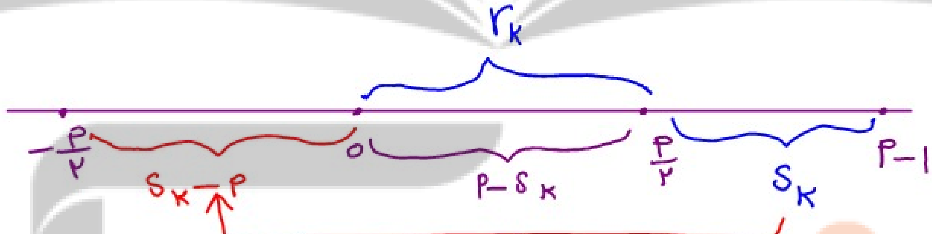


مجموعه‌ی $\{t_1, t_2, \dots, t_{\frac{p-1}{2}}\}$ را به دو مجموعه‌ی $\{r_1, \dots, r_w\}$ و $\{s_1, \dots, s_v\}$ افراز می‌کنیم ،

به عبارت دیگر $r_1, \dots, r_w < \frac{p}{2}$ و $s_1, \dots, s_v > \frac{p}{2}$.

به وضوح برای هر i ، $\frac{p}{2} < s_i < p$ بنابراین $-\frac{p}{2} < s_i - p < 0$

و لذا $0 < p - s_i < \frac{p}{2}$.



حال اولین سوالی که مطرح است این است که آیا r_k ها و $p-s_k$ ها می‌توانند بر هم منطبق شوند؟ نشان می‌دهیم این اتفاق رخ نمی‌دهد. برای این منظور،

فرض کنید (فرض خلف) به ازای یک i و یک j ، $p - s_j = r_i$.

می‌دانیم $r_i = t_i \overset{p}{\equiv} ia$ و $s_j = t_j \overset{p}{\equiv} ja$. اکنون

$$p - s_j = r_i \longrightarrow -s_j \overset{p}{\equiv} r_i \longrightarrow -ja \overset{p}{\equiv} ia \xrightarrow{\div a} -j \overset{p}{\equiv} i$$

$$\longrightarrow i + j \overset{p}{\equiv} 0 \longrightarrow p \mid i + j$$

در حالی که $\frac{p-1}{2} > r_i > 0$ و در نتیجه $p > r_i + r_j > 0$ که $i \neq j$ است،
حال از این که r_iها و $p - s_j$ها همگی $\frac{p-1}{2}$ تا هستند لذا این اعداد دقیقاً
$1, \dots, \frac{p-1}{2}$ می‌باشند.

$$ka = \left[\frac{ka}{p}\right]p + t_k \longrightarrow \sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left(\left[\frac{ka}{p}\right]p + t_k\right)$$

$$\longrightarrow \sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]p + \sum_{i=1}^{3} r_i + \sum_{j=1}^{7} s_j \qquad (1)$$

از طرفی از این که $\{r_1, r_2, r_3\} \cup \{p - s_1, \dots, p - s_7\} = \{1, 2, \dots, \frac{p-1}{2}\}$

لذا

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{3} r_i + \sum_{j=1}^{7} (p - s_j)$$

$$= \sum_{i=1}^{3} r_i + 7p - \sum_{j=1}^{7} s_j \qquad (2)$$

از تفاضل روابط (1) و (2) بدست می‌آوریم:

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]p + 2\sum_{j=1}^{7} s_j - 7p$$

اکنون با توجه به این که a فرد است لذا $a - 1 \overset{2}{\equiv} 0$ همچنین $p \overset{2}{\equiv} 1$

لذا پس از بازنویسی معادله‌ی اخیر در هشتک به پیمانه‌ی 2 خواهیم داشت:

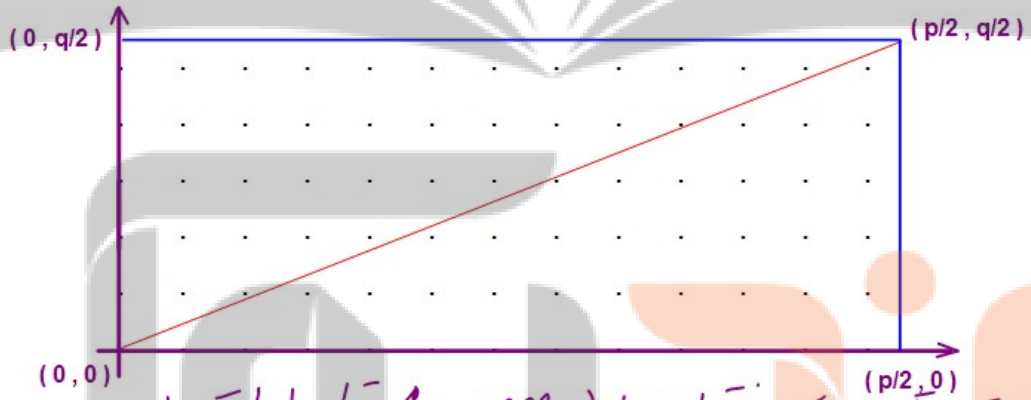
$$-7 \overset{2}{\equiv} 0 \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] - 7$$

پس $(\frac{a}{p}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}]} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}]} = (-1)^{v}$. بنابراین $v = \sum_{k=1}^{\frac{p-1}{2}} [\frac{ka}{p}]$

قضیه . (قانون تقابل مربعی) فرض کنید p و q دو عدد اول فرد و متمایز باشند. در این صورت :

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

اثبات . مستطیلی با رئوس $(0,0)$ ، $(\frac{p}{2},0)$ ، $(0,\frac{q}{2})$ و $(\frac{p}{2},\frac{q}{2})$ در نظر می‌گیریم . همچنین نقاط با مولفه‌های صحیح درون این مستطیل را به دو روش می‌شماریم .



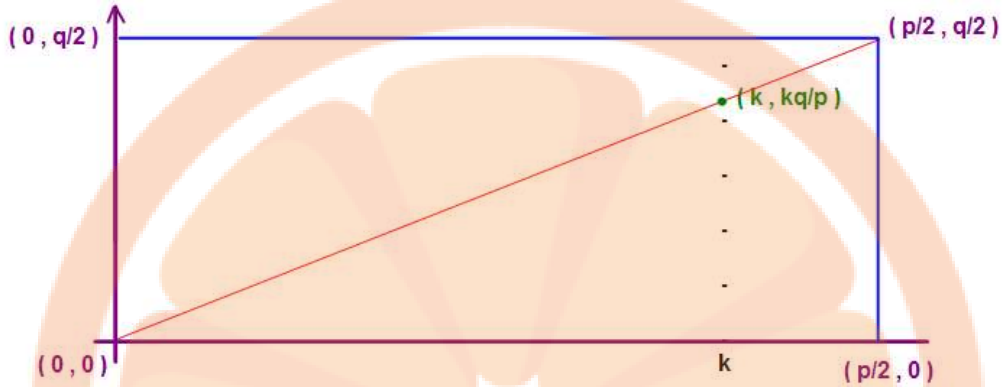
به راحتی می‌توان دید تعداد نقاط با مولفه‌های صحیح درون مستطیل برابر است با

$$\frac{p-1}{2}\ \frac{q-1}{2} .$$

روش دوم این است که تعداد نقاط درون هر کدام از مثلث‌ها را شمرده و آنها را با هم جمع کنیم .

ابتدا می‌توان دید معادله‌ی قطر مستطیل عبارت است از

$$y = \frac{q}{p}x .$$



برای شمارش نقاط درون مثلث پاسخ نقطه‌ی طبیعی k را در نظر می‌گیریم. واضح است که محل تلاقی خطوط $x=k$ و قطر مستطیل، نقطه‌ی $(k, \frac{kq}{p})$ می‌باشد. تعداد نقاط با مولفه‌های صحیح که زیر این نقطه قرار دارند برابر است با $[\frac{kq}{p}]$ و لذا تعداد نقاط درون مثلث پاسخ $\sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}]$ می‌باشد.

با تغییر نقش p و q، تعداد نقاط با مولفه‌های صحیح که درون مثلث بالایی باشند نیز $\sum_{k=1}^{\frac{q-1}{2}} [\frac{kp}{q}]$ است. بنابراین

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}] + \sum_{k=1}^{\frac{q-1}{2}} [\frac{kp}{q}]$$

حال بنا به لم قبل:

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}]} \cdot (-1)^{\sum_{k=1}^{\frac{q-1}{2}} [\frac{kp}{q}]}$$

$$= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}] + \sum_{k=1}^{\frac{q-1}{2}} [\frac{kp}{q}]} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

نتیجه: اگر p و q اعداد اول فرد متمایز باشند آنگاه

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

مثال: $\left(\frac{12}{17}\right)$ را محاسبه کنید.

حل:

$$12=2^2\times 3 \longrightarrow \left(\frac{12}{17}\right)=\left(\frac{2}{17}\right)^2\left(\frac{3}{17}\right)=\left(\frac{3}{17}\right)$$

$$\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)(-1)^{\frac{3-1}{2}\frac{17-1}{2}}=\left(\frac{17}{3}\right)$$

و چون $17\equiv -1 \pmod 3$ لذا

$$\left(\frac{17}{3}\right)=\left(\frac{-1}{3}\right)(-1)^{\frac{3-1}{2}}=-1$$

پس

$$\left(\frac{12}{17}\right)=\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=-1$$

در حالت کلی برای محاسبه‌ی $\left(\frac{a}{p}\right)$ می‌توان از قانون تفکیک بررسی استفاده کرد.

همچنین با توجه به این که $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ و $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$، برای هر مقدار صحیح a، متناظر این بامه می‌توان $\left(\frac{a}{p}\right)$ را محاسبه کرد.

مثال: آیا معادله‌ی $x^2\equiv 330 \pmod{17}$ دارای جواب است؟

حل:

$$330=2\times 3\times 5\times 11 \longrightarrow \left(\frac{330}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)\left(\frac{5}{17}\right)\left(\frac{11}{17}\right)$$

بنابراین کافی است هر کدام از عوامل سمت راست تساوی اخیر را محاسبه کنیم.

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{36} = 1$$

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{17}{3}\right)(-1)^{8} = \left(\frac{17}{3}\right)$$

و چون $17 \overset{3}{\equiv} -1$ لذا $\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$. پس

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = -1$$

$$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{17}{5}\right)(-1)^{16} = \left(\frac{17}{5}\right)$$

و چون $17 \overset{5}{\equiv} 2$. بنابراین

$$\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^{3} = -1$$

ولذا $\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = -1$

$$\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right)(-1)^{\frac{11-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{17}{11}\right)(-1)^{40} = \left(\frac{17}{11}\right)$$

اما $17 \overset{11}{\equiv} 6 = 2\times 3$. بنابراین

$$\left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)(1) = -1$$

چون :

$$\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$$

$$\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}} = \left(\frac{11}{3}\right)(-1)^{5} = \left(\frac{11}{3}\right)(-1)$$

و چون $11 \overset{3}{\equiv} -1$ لذا $\left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = (-1)$. پس $\left(\frac{3}{11}\right) = 1$

بنابراین

$$1=(1)(-1)(-1)(1)=\left(\frac{11}{17}\right)\left(\frac{5}{17}\right)\left(\frac{3}{17}\right)\left(\frac{2}{17}\right)=\left(\frac{330}{17}\right)$$

و این بدین معنی است که معادله‌ی هم‌نهشتی $x^2 \overset{17}{\equiv} 330$ دارای جواب است.

مسأله. فرض کنید a و b دو عدد صحیح دلخواه باشند، نشان دهید برای هر عدد اول p

$$(x^2-a)(x^2-b)(x^2-ab) \overset{p}{\equiv} 0$$

دارای جواب است.

حل. برای استفاده از عدد لژاندر مجبور به درنظرگرفتن دو حالت هستیم،

حالت اول) $p=2$. در این حالت باید نشان دهیم

$$(x^2-a)(x^2-b)(x^2-ab) \overset{2}{\equiv} 0 \quad (1)$$

دارای جواب است. و این بدیهی است. چون اگر a فرد باشد آنگاه به ازای $x=1$، $x^2-a=1-a$ عددی زوج است. لذا طرف چپ رابطه‌ی (1) عددی زوج بوده و بنابراین معادله‌ی هم‌نهشتی (1) دارای جواب است.

و چنانچه a عددی زوج باشد آنگاه به ازای $x=0$، $x^2-a=-a$ عددی زوج است و لذا هم‌نهشتی قبل معادله‌ی هم‌نهشتی رابطه (1) دارای جواب است.

حالت (دوم) p یک عدد اول فرد است.

- اگر $x^2 \overset{p}{\equiv} a$ دارای جواب x_0 باشد آنگاه $x_0^2 \overset{p}{\equiv} a$. بنابراین

$$p \mid x_0^2 - a \longrightarrow p \mid (x_0^2 - a)(x_0^2 - b)(x_0^2 - ab)$$

یعنی x_0 جواب معادله‌ی هم نهشتی

$$(x^2 - a)(x^2 - b)(x^2 - ab) \overset{p}{\equiv} 0 \qquad (2)$$

می‌باشد.

- اگر $x^2 \overset{p}{\equiv} b$ نیز جواب داشته باشد، مشابه حالت قبل، معادله‌ی هم نهشتی (2) دارای جواب است.

بنابراین فرض می‌کنیم $x^2 \overset{p}{\equiv} a$ و $x^2 \overset{p}{\equiv} b$ هیچکدام دارای جواب نباشند.

در این صورت $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. و در نتیجه $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$

پس $x^2 \overset{p}{\equiv} ab$ دارای جواب است و لذا همانند حالتهای قبل، معادله‌ی هم نهشتی (2) دارای جواب است.

مسأله. عدد صحیح x را چنان بیابید که باقیمانده‌ی تقسیم آن بر ۲ برابر ۱، باقیمانده‌ی تقسیم آن بر ۳ برابر با ۲، باقیمانده‌ی تقسیم آن بر ۴ برابر ۳ و باقیمانده‌ی تقسیم آن بر ۵، برابر با ۴ باشد.

حل:

لازم است:

$$\begin{array}{r|l} x & 2 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} x & 3 \\ \hline 2 & \end{array} \qquad \begin{array}{r|l} x & 4 \\ \hline 3 & \end{array} \qquad \begin{array}{r|l} x & 5 \\ \hline 4 & \end{array}$$

بنابراین

$$\begin{array}{r|l} x+1 & 2 \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} x+1 & 3 \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} x+1 & 4 \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} x+1 & 5 \\ \hline 0 & \end{array}$$

پس کافی است x را چنان اختیار کنیم که $x+1$ بر تمام اعداد ۲، ۳، ۴ و ۵ بخش‌پذیر باشد. تعداد جوابها نامتناهی است. یکی از این جوابها $60 = [2,3,4,5] = x+1$ است

بنابراین $x = 59$.

مسأله: عدد صحیح x را چنان بیابید که باقیمانده‌ی تقسیم آن بر ۳، برابر ۲ باشد. باقیمانده‌ی تقسیم آن بر ۴ برابر با ۱ و باقیمانده‌ی تقسیم آن بر ۵، برابر با ۳ باشد.

حل. در واقع می‌خواهیم x جواب همزمان معادلات همنهشتی زیر باشد:

$$\begin{cases} x \overset{3}{\equiv} 2 \\ x \overset{4}{\equiv} 1 \\ x \overset{5}{\equiv} 3 \end{cases}$$

این مسأله را نمی‌توان همانند مسأله‌ی بالا حل کرد.

قضیه‌ی زیر موسوم به قضیه‌ی باقیمانده‌های چینی این مسأله را حل می‌کند.

قضیه‌ی باقیمانده‌ی چینی: فرض کنید $m_1, m_2, \dots, m_k$ اعداد طبیعی دو به دو متباین و $b_1, b_2, \dots, b_k$ اعداد صحیح دلخواه باشند. در این صورت دستگاه معادلات هم‌نشتی

$$\begin{cases} x \overset{m_1}{\equiv} b_1 \\ x \overset{m_2}{\equiv} b_2 \\ \vdots \\ x \overset{m_k}{\equiv} b_k \end{cases} \quad *$$

دارای جواب است. به‌علاوه این جواب در پیمانه‌ی $m_1 m_2 \dots m_k$ یکتاست.

بدین معنی که اگر x و y جواب‌های دستگاه معادلات هم‌نشتی $*$ باشند، آنگاه

$$x \overset{m_1 \dots m_k}{\equiv} y$$

اثبات: تعریف می‌کنیم $n_i = \dfrac{m_1 m_2 \dots m_k}{m_i} = m_1 \dots m_{i-1} m_{i+1} \dots m_k$.

یعنی مقدماتی بیان می‌کند، اگر $(a,b)=1$ و $(a,c)=1$ آنگاه $(a,bc)=1$،

تعمیم این لم را بکار می‌گیریم، در این صورت:

$$\left.\begin{matrix} (m_1, m_2)=1 \\ (m_1, m_3)=1 \\ \vdots \\ (m_1, m_k)=1 \end{matrix}\right\} \longrightarrow (m_1, \underbrace{m_2 m_3 \dots m_k}_{n_1}) = 1 \longrightarrow (m_1, n_1) = 1$$

به طور مشابه برای هر i، $(m_i, n_i)=1$. در چنین حالتی n_i در پیمانه‌ی m_i دارای وارون ضربی است که آن را با n_i^* نشان می‌دهیم.

همچنین از این که $m_k \cdots$ لذا اگر $n_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ آن‌گاه $m_j \mid n_i$ $i \neq j$

اکنون قرار می‌دهیم $x = n_1 n_1^* b_1 + \cdots + n_k n_k^* b_k$.

$x \overset{m_1}{\equiv} ?$.

از این که n_1^* وارون جمعی n_1 در پیمانه‌ی m_1 است لذا $n_1 n_1^* \overset{m_1}{\equiv} 1$.

از طرفی برای هر $j \neq 1$، $m_1 \mid n_j$. بنابراین $n_j \overset{m_1}{\equiv} 0$ $\forall j \neq 1$.

حال :

$$x = \underbrace{n_1 n_1^* b_1}_{\overset{m_1}{\equiv} 1} + \underbrace{n_2 n_2^* b_2}_{\overset{m_1}{\equiv} 0} + \cdots + \underbrace{n_k n_k^* b_k}_{\overset{m_1}{\equiv} 0}$$

$$\overset{m_1}{\equiv} b_1 + 0 + \cdots + 0 = b_1$$

و به‌طور کلی برای هر i ، $x \overset{m_i}{\equiv} b_i$.

اثبات یکتایی، فرض کنید x و y جواب‌های دستگاه معادلات هم‌نهشتی $*$ باشند.

یعنی $\begin{cases} x \overset{m_1}{\equiv} b_1 \\ x \overset{m_2}{\equiv} b_2 \\ \vdots \\ x \overset{m_k}{\equiv} b_k \end{cases}$ و $\begin{cases} y \overset{m_1}{\equiv} b_1 \\ y \overset{m_2}{\equiv} b_2 \\ \vdots \\ y \overset{m_k}{\equiv} b_k \end{cases}$. در این صورت $\begin{cases} x \overset{m_1}{\equiv} y \\ x \overset{m_2}{\equiv} y \\ \vdots \\ x \overset{m_k}{\equiv} y \end{cases}$.

بنابراین برای هر i ، $m_i \mid x - y$ و چون m_i ها دو به دو متباین اند لذا

$m_1 m_2 \cdots m_k \mid x - y$. بنابراین $x \overset{m_1 \cdots m_k}{\equiv\equiv} y$.

مثال . دستگاه معادلات همنهشتی زیر را حل کنید .

$$\begin{cases} x \overset{۳}{\equiv} ۲ \\ x \overset{۴}{\equiv} ۱ \\ x \overset{۵}{\equiv} ۳ \end{cases}$$

حل .

i	m_i	n_i	n_i^*	b_i	$n_i n_i^* b_i$
۱	۳	۲۰	۲	۲	۸۰
۲	۴	۱۵	۳	۱	۴۵
۳	۵	۱۲	۳	۳	۱۰۸

$$x = n_1 n_1^* b_1 + n_2 n_2^* b_2 + n_3 n_3^* b_3$$

$$= ۸۰ + ۴۵ + ۱۰۸ = ۲۳۳ \overset{۶۰}{\equiv} ۵۳$$

توابع حسابی.

تعریف. هر تابع $f: \mathbb{N} \to \mathbb{R}$ یک تابع حسابی نامیده می‌شود.

مثال. $f(n)=\frac{1}{n}$، $f(n)=\sqrt{n}$، $f(n)=1$، ... توابع حسابی‌اند.

معرفی چند تابع حسابی در نظریه‌ی اعداد.

اگر n عددی طبیعی باشد آنگاه تعریف می‌کنیم:

$d(n)=$ تعداد مقسوم علیه‌های مثبت n

$\sigma(n)=$ مجموع مقسوم علیه‌های مثبت n

$\sigma_k(n)=$ مجموع توان k ام مقسوم علیه‌های مثبت n

مثال. اگر $n=6$ آنگاه مقسوم علیه‌های مثبت آن عبارتند از $\{1,2,3,6\}$. بنابراین

$$d(6)=4$$

$$\sigma(6)=1+2+3+6=12$$

$$\sigma_2(6)=1^2+2^2+3^2+6^2=50$$

$$\sigma_0(6)=1^0+2^0+3^0+6^0=4=d(6)$$

$$\sigma_1(6)=1^1+2^1+3^1+6^1=12=\sigma(6)$$

در حالت کلی: $\sigma_0(n)=d(n)$ و $\sigma_1(n)=\sigma(n)$.

لم. فرض کنید m و n دو عدد طبیعی متباین باشند. اگر $\alpha \mid mn$ آنگاه $\alpha = ef$ که در آن $e \mid m$ و $f \mid n$ و $(e,f) = 1$.

اثبات. فرض کنید

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$
$$n = q_1^{\beta_1} \cdots q_r^{\beta_r}$$

که در آن p_i ها و q_j ها اعداد اول متمایزند. (توجه کنید $(m,n) = 1$)

حال از این که $\alpha \mid mn = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_r^{\beta_r}$ لذا $\alpha = p_1^{\alpha_1'} \cdots p_k^{\alpha_k'} q_1^{\beta_1'} \cdots q_r^{\beta_r'}$ که در آن برای هر i و j، $0 \le \alpha_i' \le \alpha_i$ و $0 \le \beta_j' \le \beta_j$. اکنون با قرار دادن $e = p_1^{\alpha_1'} \cdots p_k^{\alpha_k'}$ و $f = q_1^{\beta_1'} \cdots q_r^{\beta_r'}$ حکم بدست می آید.

مسأله. فرض کنید m و n دو عدد طبیعی متباین باشند. نشان دهید

$$d(mn) = d(m)d(n).$$

حل. فرض کنید $d(m) = r$ و $d(n) = s$. همچنین $A = \{a_1, \ldots, a_r\}$ را مجموعه ی مقسوم علیه های مثبت m، $B = \{b_1, \ldots, b_s\}$ را مجموعه ی مقسوم علیه های مثبت n می گیریم.

ادعا می‌کنیم مجموعه‌ی مقسوم علیه‌های مثبت mn عبارتند از:

$$D = \{a_i b_j \mid 1 \le i \le r ,\ 1 \le j \le s\}$$

$$= \{a_1 b_1, a_1 b_2, \dots, a_1 b_s, a_2 b_1, \dots, a_r b_s\}$$

برای این منظور فرض کنید

$$C = \{c_1, \dots, c_t\}$$

مجموعه‌ی مقسوم علیه‌های مثبت mn باشد،

ثابت می‌کنیم $D = C$.

فرض کنید $x \in D$. در این صورت به ازای یک i و j، $x = a_i b_j$.

$$\left.\begin{array}{l} a_i \in A \longrightarrow a_i \mid m \\ b_j \in B \longrightarrow b_j \mid n \end{array}\right\} \longrightarrow a_i b_j \mid mn \longrightarrow x = a_i b_j \in C$$

برعکس، فرض کنید $\alpha \in C$ در این صورت $\alpha \mid mn$. بنا به لم قبل اعداد طبیعی و مثبت e و f چنان موجودند که $\alpha = ef$، $e \mid m$ و $f \mid n$،

از این که $e \mid m$ لذا به ازای یک i، $e = a_i$ و از این که $f \mid n$ لذا به ازای یک j، $f = b_j$. اکنون $\alpha = ef = a_i b_j \in D$.

بنابراین $D = C$. پس $d(mn) = |C| = |D| = rs = d(m)d(n)$.

با استفاده از مسئله‌ی بالا می‌توان $d(n)$ را برای هر عدد طبیعی n محاسبه کرد.

اگر $n=1$، بوضوح $d(n)=1$.

فرض کنید $n\neq 1$. در این صورت n قابل تجزیه به صورت

$$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

می‌باشد و بنا به مسئله‌ی قبل:

$$d(n)=d(p_1^{\alpha_1}\cdots p_k^{\alpha_k})=d(p_1^{\alpha_1})\cdots d(p_k^{\alpha_k})$$

پس کافی است برای هر i، $d(p_i^{\alpha_i})$ را محاسبه کنیم.

اما براحتی می‌توان دید مجموعه‌ی مقسوم علیه‌های مثبت $p_i^{\alpha_i}$ عبارتند از:

$$\{1, p_i, p_i^2, \ldots, p_i^{\alpha_i}\}.$$

بنابراین $d(p_i^{\alpha_i})=\alpha_i+1$ و در نتیجه

$$d(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$$

مثال: تعداد مقسوم علیه‌های مثبت ۱۴۴ را به دست آورید.

$$144=2^4\times 3^2 \longrightarrow d(144)=(4+1)(2+1)=15$$

مثال: حاصل $d(30)$ چیست؟

$$30=2\times 3\times 5 \longrightarrow d(30)=(1+1)(1+1)(1+1)=8$$

مسأله ۱. اگر n خالی از مربع باشد آنگاه $d(n)$ توانی از ۲ است.

حل. $n = p_1^1 p_2^1 \cdots p_k^1 \longrightarrow d(n) = (1+1)(1+1)\cdots(1+1) = 2^k$

توجه کنید عکس مسأله بالا برقرار نمی باشد. برای مثال $d(8) = 2^2$ درحالی که 8 خالی از مربع نیست.

مسأله ۲. نشان دهید n مربع کامل است اگر و تنها اگر $d(n)$ فرد باشد.

حل. برای $n=1$ حکم واضح است.

فرض کنید $n \neq 1$. در این صورت

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad d(n) = (\alpha_1+1)\cdots(\alpha_k+1)$$

حال اگر n مربع کامل باشد آنگاه برای هر i، α_i زوج و لذا α_i+1 فرد است.

بنابراین $d(n) = \prod_{i=1}^{k}(\alpha_i+1)$ نیز عددی فرد است.

برعکس اگر $d(n) = \prod (\alpha_i+1)$ فرد باشد، برای هر i، α_i+1 فرد است و لذا α_i زوج است. بنابراین n مربع کامل است.

تعریف. فرض کنید $f(n)$ یک تابع حسابی باشد. در این صورت $f(n)$ را ضربی گوییم هرگاه برای هر m, n مثبت داشته باشیم $f(mn) = f(m)f(n)$. به عبارت دیگر

$$(m,n)=1 \longrightarrow f(mn) = f(m)f(n)$$

مثال، بنابه قضیه اساسی شمارش، برای هر m و n متباین، $d(mn)=d(m)\,d(n)$.

بنابراین تابع $d(n)$ یک تابع ضربی است.

مثال. $f(n)=n$ یک تابع ضربی است. چون برای هر m و n،

$$f(mn)=mn=f(m)\,f(n)$$

توجه کنید در مثال اخیر، شرط $(m,n)=1$ برای برقراری تساوی لازم نیست.

تعریف. تابع حسابی $f(n)$ را ضربی قوی می‌نامیم هرگاه، برای هر m و n،

$$f(mn)=f(m)\,f(n)$$

مثال. توابع زیر، ضربی قوی هستند.

$$f(n)=n,\quad f(n)=n^2,\quad f(n)=\sqrt{n},\quad f(n)=\frac{1}{n},\quad f(n)=1$$

توجه کنید که توابع ضربی قوی، ضربی هستند درحالیکه عکس آن برقرار نیست.

مثال، قبلاً ثابت کردیم تابع $d(n)$ ضربی است. درحالیکه ضربی قوی نیست. برای این منظور قرار دهید $n=4$ و $m=6$. در این صورت

$$\left.\begin{array}{l} d(4)=3 \longrightarrow \{1,2,4\}=\text{مجموعه مقسوم علیه‌های } 4 \\ d(6)=4 \longrightarrow \{1,2,3,6\}=\text{مجموعه مقسوم علیه‌های } 6 \end{array}\right\} \longrightarrow d(4)\,d(6)=12$$

$$d(24)=8 \longrightarrow \{1,2,3,4,6,8,12,24\}=\text{مجموعه مقسوم علیه‌های } 24$$

$$12\neq 8$$

قضیه. فرض کنید $g(n)$ یک تابع حسابی ضربی باشد. در این صورت

$$f(n)=\sum_{d\mid n} g(d)$$

نیز حسابی ضربی است.

اثبات. فرض کنید $(m,n)=1$. در این صورت:

$$f(m)f(n)=\sum_{d\mid m} g(d)\sum_{e\mid n} g(e)=\sum_{d\mid m}\sum_{e\mid n} g(d)g(e)$$

اکنون توجه کنید:

الف. زیرا $d\mid m$ و $e\mid n$ و $(m,n)=1$ لذا $(e,d)=1$. بنابراین

$$g(d)g(e)=g(de).$$

ب. اگر $d\mid m$ و $e\mid n$ آنگاه $de\mid mn$.

برعکس، اگر $\alpha\mid mn$ آنگاه بنا به یکی از لم‌های قبل، α قابل نمایش به صورت $\alpha=de$ است که $d\mid m$ و $e\mid n$، به عبارت دیگر:

$$\begin{cases} d\mid m \\ e\mid n \end{cases} \equiv de\mid mn$$

بنابراین مجموع به دست آمده در تساوی بالا عبارت است از:

$$\sum_{de\mid mn} g(de)=\sum_{c\mid mn} g(c)=f(mn)$$

بنابراین $f(m)f(n)=f(mn)$ و لذا f ضربی است.

مثال. ① اگر $g(n)=1$ آنگاه به وضوح g ضربی است و لذا

$$\sum_{d\mid n} g(d) = \sum_{d\mid n} 1 = d(n)$$

نیز ضربی است.

② با فرض $g(n)=n$ ، g ضربی است و بنابراین

$$\sum_{d\mid n} g(d) = \sum_{d\mid n} d = \sigma(n)$$

نیز ضربی است.

③ قرار می‌دهیم $g(n)=n^k$. در این صورت g ضربی است و لذا

$$\sum_{d\mid n} g(d) = \sum_{d\mid n} d^k = \sigma_k(n)$$

نیز ضربی است.

محاسبه‌ی فرمول $\sigma(n)$.

فرض کنید p عددی اول باشد. در این صورت

$$\{1, p, \dots, p^\alpha\} = \text{مجموعه‌ی تقسیم‌های مثبت } p^\alpha$$

بنابراین

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$$

اکنون اگر $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ آنگاه $n+1$ و در نتیجه

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \overset{\sigma \text{ ضربی}}{=} \sigma(p_1^{\alpha_1}) \cdots \sigma(p_k^{\alpha_k})$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \times \cdots \times \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

مثال.

$$\sigma(12) = \sigma(2^2 \times 3^1) = \sigma(2^2)\sigma(3^1)$$

$$= \frac{2^3-1}{2-1} \times \frac{3^2-1}{3-1} = 7 \times 13 = 91$$

بحث.

تعریف. فرض کنید f و g دو تابع حسابی باشند. در این صورت برای هر n تعریف می‌کنیم:

$$f*g(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

لم. فرض کنید n عددی طبیعی باشد. در این صورت:

$$d|n \text{ و } c|\frac{n}{d} \equiv c|n \text{ و } d|\frac{n}{c}$$

اثبات. فرض کنید $d|n$ و $c|\frac{n}{d}$. در این صورت $cd|n$.

برعکس. فرض کنید $cd|n$. در این صورت از آنجا که $d|cd$ نتیجه می‌شود $d|n$. حال از این که $cd|n$ با تقسیم طرفین رابطه اخیر بر d داریم $c|\frac{n}{d}$. بنابراین ثابت کرده‌ایم:

$$\left.\begin{matrix} d \mid n \\ c \mid \frac{n}{d} \end{matrix}\right\} \equiv dc \mid n$$

می‌دانیم:

$$\left.\begin{matrix} c \mid n \\ d \mid \frac{n}{c} \end{matrix}\right\} \equiv cd \mid n$$

بنابراین:

$$\left.\begin{matrix} d \mid n \\ c \mid \frac{n}{d} \end{matrix}\right\} \equiv \begin{cases} c \mid n \\ d \mid \frac{n}{c} \end{cases}$$

قضیه. فرض کنید f و g توابع حسابی ضربی باشند. در این صورت $f*g$ نیز ضربی است.

اثبات. فرض کنید m و n دو عدد طبیعی متباین باشند و قرار می‌دهیم $h=f*g$. در این صورت:

$$h(m)h(n) = \sum_{d \mid m} f(d)\, g\left(\frac{m}{d}\right) \sum_{c \mid n} f(c)\, g\left(\frac{n}{c}\right)$$

$$= \sum_{d \mid m} \sum_{c \mid n} f(d) f(c)\, g\left(\frac{m}{d}\right) g\left(\frac{n}{c}\right)$$

$$= \sum_{cd \mid mn} f(cd)\, g\left(\frac{mn}{cd}\right)$$

$$= \sum_{\alpha \mid mn} f(\alpha)\, g\left(\frac{mn}{\alpha}\right) = h(mn)$$

بنابراین $h=f*g$ نیز ضربی است.

نتیجه. اگر g یک تابع ضربی باشد، آنگاه تابع f که به صورت زیر تعریف می‌شود

$$f(n) = \sum_{d|n} g(d)$$

نیز ضربی است.

اثبات. تابع $g(n)$ ضربی است، از طرفی تابع $I(n)=1$ نیز ضربی است. بنابراین $g * I$ نیز ضربی است، اما

$$g*I = \sum_{d|n} g(d) I\left(\frac{n}{d}\right) = \sum_{d|n} g(d) \times 1 = \sum_{d|n} g(d) = f(n)$$

پس f نیز ضربی است.

تلاشی در مسیر موفقیت

ترنج بوک

- دانلود گام به گام تمام دروس
- دانلود آزمون های قلم چی و گاج + پاسخنامه
- دانلود جزوه های آموزشی و شب امتحانی
- دانلود نمونه سوالات امتحانی
- مشاوره کنکور
- فیلم های انگیزشی