

تابع حسابی اوایلر و قضیه ی اوایلر و نتایج حاصل از آن ها

● جمیدرضا امیری

$$\sum_{i=1}^k \varphi(d_i) = m$$

مثال ۱. مطلوب است محاسبه ی:

$$\varphi(120) \quad (\text{الف})$$

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) \quad (\text{ب})$$

حل. الف)

$$\varphi(120) = \varphi(2^3 \times 3 \times 5) = \varphi(2^3) \times \varphi(3) \times \varphi(5) = \varphi(8 \times 3) \times \varphi(5)$$

$$= \varphi(8) \times \varphi(3) \times \varphi(5) = \varphi(2^3) \times 2 \times 4$$

$$= 2^2 \times (1 - \frac{1}{2}) \times 2 \times 4 = 4 \times 2 \times 4 = 32$$

ب)

$$\varphi(1) + \dots + \varphi(9) + \varphi(18) = 18 \quad (\text{طبق قضیه ی ۳})$$

(اعداد ۱ و ۲ و ۳ و ۶ و ۹ و ۱۸ شماره های مثبت عدد ۱۸ هستند.)

تمرین: ثابت کنید:

$$I) \varphi(10^n) = 10^{n-1} \times 4$$

$$II) \varphi(2n) = \begin{cases} 2\varphi(n) & \text{زوج } n \\ \varphi(n) & \text{فرد } n \end{cases}$$

$$III) \varphi(3n) = 2\varphi(n) \Leftrightarrow 3 \nmid n$$

$$IV) \varphi(3n) = 2\varphi(n) \Leftrightarrow 3 \mid n$$

$$V) \varphi(n) = \frac{n}{2} \Leftrightarrow n = 2^\alpha \quad (\alpha \geq 1)$$

$$VI) \varphi(n^2) = n\varphi(n) \quad (\forall n \in \mathbb{N})$$

اثبات:

$$I) \varphi(10^n) = \varphi(2^n \times 5^n) = 10^{n-1} \times \frac{1}{2} \times \frac{4}{5} = 10^{n-1} \times 4$$

$$II) \begin{cases} \text{زوج } n \Rightarrow (n, 2) = 2 \Rightarrow \varphi(2n) = \varphi(2) \times \varphi(n) \times \frac{2}{\varphi(2)} = 2\varphi(n) \\ \text{فرد } n \Rightarrow (n, 2) = 1 \Rightarrow \varphi(2n) = \varphi(2) \times \varphi(n) = 1 \times \varphi(n) = \varphi(n) \end{cases}$$

در کتاب ریاضیات گسسته ی پیش دانشگاهی، در بخش ترکیبات، با استفاده از اصل شمول و عدم شمول ثابت شده است که اگر $m = p_1 \times p_2 \times p_3$ به صورت m عددی طبیعی باشد و به صورت حاصل ضرب سه عدد اول تجزیه شود، در این صورت تعداد اعداد طبیعی و کوچک تر از m که نسبت به m اول هستند، از رابطه ی

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3})$$

رابطه در حالت کلی و برای هر عدد طبیعی مانند m که به صورت

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$$

شود و به تابع حسابی اوایلر معروف است؛ یعنی:

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$$

برای مثال، عدد $60 = 2^2 \times 3 \times 5$ را در نظر می گیریم. در

این صورت:

$$\varphi(60) = 60 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3}) \times (1 - \frac{1}{5}) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}$$

$$\Rightarrow \varphi(60) = 16$$

قبل از هر چیز، برای تسریع در محاسبه ی $\varphi(m)$ در حالت های

گوناگون، برای m چند قضیه را بیان می کنیم^۱:

قضیه ی ۱. اگر p عددی اول و α عددی طبیعی باشد:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$$

نتیجه: اگر p عددی اول باشد، همواره:

$$\varphi(p) = p(1 - \frac{1}{p}) = (p-1)$$

قضیه ی ۲. به ازای هر دو عدد طبیعی مانند m و n که

$$(m, n) = d$$

$$\varphi(mn) = \varphi(m) \times \varphi(n) \times \frac{d}{\varphi(d)}$$

نتیجه (حالت خاص قضیه ی ۲): اگر m و n دو عدد طبیعی و

$$(m, n) = 1$$

$$\varphi(mn) = \varphi(m) \times \varphi(n)$$

(توجه داریم که: $\varphi(1) = 1$.)

قضیه ی ۳. اگر $d_k, \dots, d_2, d_1$ همه ی شماره های مثبت عدد

m متباین بوده و هر دو تا از آن‌ها به پیمانه‌ی m ، ناهم‌نهشت باشند.

اثبات: با توجه به تعریف، اثبات واضح و بدیهی است.

قضیه: اگر مجموعه‌ی $\varphi(m)$ عدد $r_1, r_2, \dots, r_{\varphi(m)}$ ، یک د.م.م. به پیمانه‌ی m و $(a, m) = 1$ باشد، در این صورت مجموعه‌ی $A = \{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ نیز یک د.م.م. به پیمانه‌ی m است.

اثبات: تعداد اعضای A برابر است با $\varphi(m)$. از طرف دیگر برای هر r_i که $1 \leq i \leq \varphi(m)$ ، همواره: $(r_i, m) = 1$ (طبق تعریف د.م.م.) و طبق فرض: $(a, m) = 1$ و لذا: $(ar_i, m) = 1$ و همواره: $ar_i \not\equiv ar_j \pmod{m}$ زیرا اگر $ar_i \equiv ar_j \pmod{m}$ باشد، چون:

$(a, m) = 1$ ، پس: $r_i \equiv r_j \pmod{m}$ که با تعریف د.م.م. تناقض دارد. بنابراین، مجموعه‌ی A یک د.م.م. به پیمانه‌ی m است. حال به اثبات قضیه‌ی اوایلر می‌پردازیم.

اثبات قضیه‌ی اوایلر: فرض کنیم $k = (\varphi)m$ و $A = \{r_1, r_2, \dots, r_k\}$ یک د.م.م. به پیمانه‌ی m باشد. بنابر قضیه‌ی قبل و این‌که: $(a, m) = 1$ ، مجموعه‌ی $B = \{ar_1, ar_2, \dots, ar_k\}$ نیز یک د.م.م. به پیمانه‌ی m است.

بنابراین، هر یک از اعضای A با یکی و فقط یکی از اعضای B به پیمانه‌ی m هم‌نهشت است که اگر طرفین این k هم‌نهشتی را در هم ضرب کنیم، خواهیم داشت:

$$(ar_1)(ar_2)\dots(ar_k) \equiv r_1 r_2 \dots r_k \pmod{m}$$

$$\Rightarrow (r_1 r_2 \dots r_k) a^k \equiv r_1 r_2 \dots r_k \pmod{m}$$

از طرف دیگر: $(r_1, m) = 1$ و $(r_2, m) = 1, \dots, (r_k, m) = 1$ (طبق تعریف د.م.م.)، پس: $(r_1 r_2 \dots r_k, m) = 1$. یعنی می‌توان طرفین رابطه‌ی (۱) را بر $(r_1 r_2 \dots r_k)$ تقسیم کرد که پس از تقسیم نتیجه می‌شود: $a^k \equiv 1 \pmod{m}$ یا $a^{\varphi(m)} \equiv 1 \pmod{m}$.

نتیجه‌ی ۱: (قضیه‌ی فرما) اگر p عددی اول و a عددی صحیح و $p \nmid a$ ، $((p, a) = 1)$ باشد، در این صورت:

$$a^{p-1} \equiv 1 \pmod{p}$$

اثبات: اگر p اول باشد، $\varphi(p) = p-1$ و طبق قضیه‌ی اوایلر حکم ثابت می‌شود.

تذکر: فرما قضیه‌ی خود را حدود ۸۰ سال قبل از اوایلر بیان کرد! نتیجه‌ی ۲: اگر p عددی اول و a عددی صحیح باشند، در این صورت:

$$a^p \equiv a \pmod{p}$$

اثبات: اگر $p \nmid a$ باشد، پس طبق نتیجه‌ی ۱ داریم: $a^{p-1} \equiv 1 \pmod{p}$ و با ضرب طرفین هم‌نهشتی در a حکم به دست می‌آید. و اگر $p \mid a$ ،

$$IV, III) \quad \varphi(\varphi n) = \varphi(\varphi) \times \varphi(n) \times \frac{(\varphi, n)}{\varphi[(\varphi, n)]}$$

حال اگر $\varphi \nmid n$ باشد، پس: $\varphi[(\varphi, n)] = \varphi(\varphi)$ و $\varphi(\varphi) = \varphi$ و تمرین (III) ثابت می‌شود. و اگر $\varphi \mid n$ باشد، پس: $(\varphi, n) = \varphi$ ، $\varphi[(\varphi, n)] = \varphi(1)$ و $\varphi(1) = 1$ ، و تمرین (IV) اثبات می‌شود.

$$V) \quad \varphi(n) = \varphi(\varphi^\alpha) = \varphi^\alpha \times (1 - \frac{1}{\varphi}) = \varphi^\alpha \times \frac{\varphi-1}{\varphi} = \frac{\varphi^\alpha}{\varphi} = \frac{n}{\varphi}$$

$$VI) \quad \varphi(n') = \varphi(n \times n) = \varphi(n) \times \varphi(n) \times \frac{(n, n)}{\varphi[(n, n)]}$$

$$= \varphi(n) \times \varphi(n) \times \frac{(n)}{\varphi(n)} = n\varphi(n)$$

قضیه‌ی ۴: اگر a و b دو عدد طبیعی و $(a, b) = d$ و $[a, b] = c$ باشند، در این صورت داریم:

$$\varphi(a)\varphi(b) = \varphi(d)\varphi(c)$$

تذکر: در قضیه‌ی (۴)، اگر $d = 1$ باشد، خواهیم داشت: $(c=ab)$:

$$\varphi(ab) = \varphi(a) \times \varphi(b)$$

که همان نتیجه‌ی قضیه‌ی ۲ است.

تمرین: ثابت کنید:

$$I) \quad \forall n \in \mathbb{N}, \quad \varphi(n) \mid n!$$

$$II) \quad \text{اگر } k, n \in \mathbb{N}, d \mid n \text{ ثابت کنید: } \varphi(nd^k) = d^k \varphi(n)$$

(راه‌حل‌های خود را برای ما ارسال کنید. از بین بهترین‌ها، به دو نفر جایزه می‌دهیم!)

قضیه‌ی اوایلر در هم‌نهشتی‌ها و کاربردهای آن

قضیه‌ی اوایلر: اگر m عددی طبیعی و a عددی صحیح باشد و $(m, a) = 1$ ، در این صورت:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

برای اثبات قضیه‌ی اوایلر، به بیان یک تعریف و دو قضیه‌ی مربوط به آن نیاز داریم که شاید مفید باشد!

تعریف دستگاه مخفف مانده‌ها به پیمانه‌ی m (د.م.د)

مجموعه‌ی شامل $\varphi(m)$ عدد $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ را یک د.م.م. به پیمانه‌ی m می‌نامیم، هرگاه هریک از کلاس‌های هم‌ارزی به پیمانه‌ی m متباین با m ، دقیقاً با یک عضو این مجموعه هم‌نهشت باشند:

برای مثال، مجموعه‌ی $\{1, 3, 5, 7\}$ یک د.م.م. به پیمانه‌ی ۸ است.

قضیه: شرط لازم و کافی برای آن‌که مجموعه‌ی شامل $\varphi(m)$ عدد صحیح یک د.م.م. به پیمانه‌ی m باشد آن است که هریک از این اعداد با

پس: $p|a(a^{p-1}-1)$ و لذا: $p|a^p - a$.

در نتیجه: $a^p \equiv a$
 نتیجه ۳. اگر a عددی صحیح و فرد و k عددی طبیعی باشد،
 همواره داریم:

$$a^{2k-1} \cdot 2^k \equiv 1$$

اثبات: چون a فرد است، پس: $(a, 2) = 1$ و لذا طبق قضیه ی اوایلر داریم:

$$a^{\varphi(2^k)} \equiv 1 \xrightarrow{\text{(تمرین V)}} a^{2^{k-1}} \equiv 1 \Rightarrow a^{2k-1} \equiv 1$$

نتیجه ی ۴. اگر p و q دو عدد اول و متمایز باشند، همواره داریم:

$$p^{q-1} + q^{p-1} \equiv 1$$

اثبات: می دانیم $(p, q) = 1$ ، لذا طبق قضیه ی فرما داریم:

$$p^{q-1} \equiv 1 \Rightarrow p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \quad (1)$$

$$q^{p-1} \equiv 1 \Rightarrow p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \quad (2)$$

$$(p, q) = 1 \xrightarrow{(1), (2)} p^{q-1} + q^{p-1} \equiv 1$$

نتیجه ی ۵. اگر p عددی اول و a و b اعدادی صحیح باشند،
 همواره داریم:

$$(a+b)^p \equiv a^p + b^p$$

اثبات: طبق نتیجه ی ۲ داریم:

$$a^p \equiv a \pmod{b^p} \Rightarrow a^p + b^p \equiv a + b \pmod{b^p} \quad (1)$$

$$(a+b)^p \equiv (a+b) \pmod{b^p} \quad (2)$$

$$(1), (2) \Rightarrow (a+b)^p \equiv a^p + b^p$$

نتیجه ی ۶. اگر p و q دو عدد اول و متمایز باشند و:

$$a^p \equiv a \pmod{a^q}, \quad a^q \equiv a \pmod{a^p}$$

$$(a^p)^q \equiv a^p \pmod{a^q}, \quad (a^q)^p \equiv a^q \pmod{a^p}$$

از طرف دیگر طبق فرض: $a^q \equiv a$ و $a^p \equiv a$ و بنابه خاصیت تعدی داریم:

$$a^{pq} \equiv a \pmod{a^p}, \quad a^{pq} \equiv a \pmod{a^q} \xrightarrow{(p,q)=1} a^{pq} \equiv a$$

نتیجه ی ۷. مجموعه ی اعداد اولی که به صورت $4k+1$ هستند، نامتناهی است.

اثبات: ثابت می کنیم به ازای هر عدد طبیعی مانند $n \neq 1$ ، عدد اولی چون p به صورت $p = 4k+1$ وجود دارد که: $p > n$. برای اثبات، فرض کنیم: $n > 1$ و $a = n!$.

چون $a = n!$ عددی زوج است، پس عدد $a^2 + 1$ فرد است. و چون $a^2 + 1 > 1$ عامل اولی چون p دارد که p به یکی از دو صورت $4k+1$ یا $4k+3$ است و واضح است که: $p > n$ (زیرا اگر $p \leq n$ باشد، همواره: $p|n!$ یا $p|a$. پس $p|a^2$ و چون $p|a^2 + 1$ باید $p|1$ که تناقض است). حال کافی است ثابت کنیم به صورت $(4k+1)$ است. فرض کنیم چنین نباشد (فرض خلف)، یعنی: $p = 4k+3$. طبق ویژگی ها و خواص رابطه ی عا کردن داریم:

$$p|a^2 + 1, \quad a^2 + 1 | (a^2)^{2k+1} + 1 \quad ((a^2)^{2k+1} + 1 = (a^2 + 1) \times Q) \\ \Rightarrow p|(a^2)^{2k+1} + 1 \Rightarrow p|a^{4k+2} + 1 \xrightarrow{p=4k+3} p|a^{p-1} + 1 \\ \Rightarrow p|a(a^{p-1} + 1) \Rightarrow p|a^p + a \quad (1)$$

$$a^p \equiv a \pmod{p} \Rightarrow p|a^p - a \quad (2)$$

$$(1), (2) \Rightarrow p|2a = 2 \times n!$$

و چون p بزرگ تر از n و فرد است، عبارت $p|2 \times n!$ یک تناقض است و لذا باید $p = 4k+1$ و حکم به اثبات می رسد.

نتیجه ی ۸ (تعمیم نتیجه ی ۴): اگر m و n اعدادی طبیعی باشند و $(m, n) = 1$ ، در این صورت:

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$$

(اثبات به عهده ی شما)

کاربرد قضیه های اوایلر و فرما در حل مسائل عددی و

غیر عددی و پیدا کردن باقی مانده ی تقسیم

۱. باقی مانده ی تقسیم عدد $A = 3^{256} \times (-5)$ را بر ۱۰۰ بیابید.

$$(3, 100) = 1, \quad \varphi(100) = \varphi(10^2) = 10^2 \times 4 = 40$$

در نتیجه بنابر قضیه ی اوایلر داریم:

$$3^{40} \equiv 1 \pmod{100} \Rightarrow (3^{40})^6 \times 3^{16} \equiv 3^{16} \pmod{100}$$

$$3^{16} = (81)^4 \equiv (-19)^4 = (-19^2)^2 = (361)^2 \equiv 61^2 = 3721 \equiv 21 \pmod{100}$$

$$\Rightarrow 3^{256} \equiv 21 \pmod{100} \Rightarrow 3^{256} \times (-5) \equiv -105 \equiv 95 \pmod{100}$$

پس باقی مانده ی عدد A بر ۱۰۰ عدد ۹۵ است، یا عدد A از سمت راست به ۹۵ ختم می شود.

۲. باقی مانده ی تقسیم عدد $12 \times (12^{24} + 35^4)$ را بر ۴۲۰ بیابید.

می دانیم:

$$(12, 25) = 1, \quad \varphi(12) = 4, \quad \varphi(35) = \varphi(7 \times 5) = \varphi(7) \times \varphi(5)$$

$$\Rightarrow \varphi(35) = 6 \times 4 = 24$$

از طرف دیگر، بنابر یکی از تمرین‌های قبل داریم:

$$(m, n) = 1 \Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1$$

$$\Rightarrow 12^{\varphi(35)} + 35^{\varphi(12)} \equiv 1 \Rightarrow 12^{24} + 35^{12} \equiv 1$$

$$\Rightarrow A = (12^{24} + 35^{12}) \times 12 \equiv 12 \Rightarrow r = 12$$

۳. ثابت کنید، اگر: $(a, v) = (b, v) = 1$ ، آنگاه:
 $49 | a^{42} - b^{42}$

اولیتر

$$(a, v) = 1 \Rightarrow (a, 49) = 1 \Rightarrow a^{\varphi(49)} \equiv 1, \varphi(49) = 42$$

$$\Rightarrow a^{42} \equiv 1, b^{42} \equiv 1 \Rightarrow a^{42} - b^{42} \equiv 0 \Rightarrow 49 | a^{42} - b^{42}$$

۴. باقی مانده‌ی تقسیم عدد $A = \sum_{k=1}^{\infty} k^{16}$ را بر ۱۷ بیابید.

از بین اعداد ۱ تا ۴۰ فقط دو عدد ۱۷ و ۳۴ نسبت به ۱۷ اول نیستند و در مورد بقیه‌ی اعداد می‌توان از قضیه‌ی فرما استفاده کرد:

$$A = 1^{16} + 2^{16} + \dots + 17^{16} + 18^{16} + \dots + 34^{16} + 35^{16} + \dots + 40^{16}$$

$$\Rightarrow A \equiv \underbrace{1+1+\dots+1}_{16 \text{ تا}} + \underbrace{1+\dots+1}_{16 \text{ تا}} + \underbrace{1+\dots+1}_{16 \text{ تا}}$$

$$\Rightarrow A \equiv 16 + 16 + 16 = 48 \equiv 14 \Rightarrow r = 14$$

۵. باقی مانده‌ی تقسیم عدد $A = \sum_{k=1}^{\infty} k^{12}$ را بر عدد ۱۳ بیابید.

$$A = 1^{12} + \dots + 12^{12} + 13^{12} + \dots + 40^{12}$$

بنابر نتیجه ۲ داریم:

$$A \equiv 1 + 2 + \dots + 40 = \frac{40 \times 41}{2} = 20 \times 41 \equiv 7 \times 2 = 14 \equiv 1$$

$$\Rightarrow r = 1$$

$$(20 \equiv 7, 41 \equiv 2)$$

۶. باقی مانده‌ی تقسیم عدد $A = 35^{2008} \times 50$ را بر ۲۴ بیابید.

$$(35, 24) = 1 \Rightarrow 35^{\varphi(24)} \equiv 1 \Rightarrow 35^{24} \equiv 1$$

$$2008 = 251 \times 8 \Rightarrow (35^8)^{251} \equiv 1 \Rightarrow 35^{2008} \times 50 \equiv 1 \times 50 \equiv 2$$

۷. اگر عدد a نسبت به ۲، ۳، ۱۹ و ۳۷ اول باشد، ثابت کنید

$$a^{36} - 1 \text{ بر } 33744 \text{ بخش پذیر است.}$$

$$33744 = 2^4 \times 3 \times 19 \times 37,$$

$$a^{36} - 1 = (a^{18} + 1)(a^9 + 1)(a^9 - 1)$$

$$(a, 37) = 1 \Rightarrow a^{36} \equiv 1 \Rightarrow 37 | a^{36} - 1 \quad (1)$$

از طرف دیگر، چون $(a, 2) = 1$ ، پس a فرد است و هر یک از

سه عدد $(a^9 - 1)$ ، $(a^9 + 1)$ و $(a^{18} + 1)$ زوج هستند. و چون

$(a^9 + 1)$ و $(a^9 - 1)$ دو عدد زوج متوالی هستند، پس یکی از آنها

بر ۴ بخش پذیر است. بنابراین:

$$(a^{36} - 1) = (a^{18} + 1)(a^9 + 1)(a^9 - 1) \\ = 2k_1 \times 2k_2 \times 4k_3 = 16k \Rightarrow 2^4 | a^{36} - 1 \quad (2)$$

$$(a, 19) = 1 \Rightarrow a^{18} \equiv 1 \Rightarrow 19 | a^{18} - 1 \Rightarrow 19 | a^{36} - 1 \quad (3)$$

$$(a, 3) = 1 \Rightarrow a^2 \equiv 1 \Rightarrow 3 | a^2 - 1 \Rightarrow 3 | a^{36} - 1 \quad (4)$$

$$[a^{36} - 1 = (a^2)^{18} - 1 = (a^2 - 1)Q]$$

$$(1), (2), (3), (4) \Rightarrow [2^4, 3, 19, 37] | a^{36} - 1$$

$$\Rightarrow 2^4 \times 3 \times 19 \times 37 | a^{36} - 1 \Rightarrow 33744 | a^{36} - 1$$

۸. ثابت کنید: $11 | 5^{28} - 4$.

$$(5, 11) = 1 \Rightarrow 5^{10} \equiv 1 \Rightarrow (5^{10})^2 \times 5^8 \equiv 5^8$$

$$5^8 = 25^4, 25 \equiv 3 \Rightarrow 25^4 \equiv 3^4 = 81 \equiv 4$$

$$\Rightarrow 5^8 \equiv 4 \Rightarrow 5^{28} \equiv 4 \Rightarrow 11 | 5^{28} - 4$$

کاربرد قضیه‌های اوایلر و فرما در حل معادلات سیاله‌ی

خطی و هم‌نهشتی

می‌دانیم، هر معادله‌ی سیاله‌ی خطی و دو مجهولی به صورت

$$a'x + b'y = c' \text{ که } (a', b') | c', \text{ دارای بی شمار جواب صحیح}$$

است که با تقسیم طرفین تساوی بر (a', b') ، به معادله‌ی سیاله‌ی

$$ax + by = c \text{ می‌رسیم و همواره } (a, b) = 1 \text{ است. از طرف}$$

دیگر، شرط لازم و کافی برای آن که زوج مرتب (x, y) یک جواب

معادله‌ی اخیر باشد، آن است که:

$$y = \frac{c - ax}{b} \in \mathbb{Z} \text{ یا } b | ax - c \text{ یا } ax \equiv c \text{ به علاوه، بنابر}$$

قضیه‌ی اوایلر: $a^{\varphi(b)} \equiv 1$. بنابراین:

$$aa^{\varphi(b)-1} \equiv 1 \Rightarrow a(ca^{\varphi(b)-1})^b \equiv c$$

یعنی، هر عدد مانند x که $x \equiv ca^{\varphi(b)-1}$ در معادله‌ی

هم‌نهشتی $ax \equiv c$ و در نتیجه در معادله‌ی سیاله‌ی $ax + by = c$

صدق می‌کند (می‌توان x را مساوی با $ca^{\varphi(b)-1}$ فرض کرد).

برای مثال، معادله‌ی $13x + 12y = 17$ را حل می‌کنیم:

$$\varphi(12) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4 \Rightarrow x \equiv 17 \times 13^3$$

$$I) \Delta|a \Rightarrow (\Delta, a) = 1 \Rightarrow (\Delta^r, a) = 1 \Rightarrow a^{100 \cdot 125} \equiv 1$$

$$II) \Delta|a \Rightarrow \Delta^r|a^r \Rightarrow \Delta^r|a^{100} \Rightarrow a^{100 \cdot 125} \equiv 0$$

۱۲. اگر $(a, 10) = 1$ باشد، ثابت کنید سه رقم سمت راست a^{100} و a با هم برابرند.

برای اثبات می‌باید نشان دهیم: $a^{100} \equiv a$ که چون $\varphi(8) = 4$ و $\varphi(125) = 100$ طبق قضیه ی اویلر: $a^{100} \equiv 1$ و $a^{125} \equiv 1$ پس: $a^{100} \equiv 1$ و چون $(8, 125) = 1$ ، لذا: $a^{100 \cdot 125} \equiv 1$ یا $a^{12500} \equiv 1$ یا ضرب طرفین در a داریم: $a^{12500} \equiv a$

۱۳. اگر $(a, 90) = 1$ باشد، ثابت کنید: $a^{12} \equiv 1$.
 $\varphi(9) = 6$, $\varphi(10) = 4$

$$\left. \begin{aligned} (a, 10) = 1 &\Rightarrow a^4 \equiv 1 \Rightarrow (a^4)^3 \equiv 1 \Rightarrow a^{12} \equiv 1 \\ (a, 9) = 1 &\Rightarrow a^6 \equiv 1 \Rightarrow (a^6)^2 \equiv 1 \Rightarrow a^{12} \equiv 1 \end{aligned} \right\} \Rightarrow a^{12} \equiv 1$$

۱۴. به کمک قضیه ی اویلر دو رقم سمت راست $A = 7^{4001} \times 9$ را بیابید.

$$\begin{aligned} \varphi(100) &= 40, (7, 100) = 1 \Rightarrow 7^{40} \equiv 1 \\ \Rightarrow 7^{400} \equiv 1 &\Rightarrow (7^{40})^{10} \times 7 \equiv 7 \Rightarrow 7^{4001} \times 9 \equiv 7 \times 9 \\ \Rightarrow 7^{4001} \times 9 &\equiv 63 \Rightarrow \text{دو رقم سمت راست عدد } A, \text{ } 63 \text{ است.} \\ 15. \text{ اگر } p \text{ و } q \text{ اعداد اول و متمایز باشند، به طوری که } (p-1)|(q-1), \text{ ثابت کنید:} \end{aligned}$$

$$(a, pq) = 1 \Rightarrow a^{q-1} \equiv 1$$

$$((a, pq) = 1 \Rightarrow (a, p) = (a, q) = 1) \quad \text{حل:}$$

$$(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \quad (1)$$

$$(a, q) = 1 \Rightarrow a^{q-1} \equiv 1 \quad (2)$$

$$(p-1)|(q-1) \Rightarrow (q-1) = (p-1) \times k$$

$$(1) \Rightarrow a^{q-1} = (a^{p-1})^k \equiv 1^k \Rightarrow a^{q-1} \equiv 1 \quad (3)$$

$$(2), (3) \xrightarrow{(p,q)=1} a^{q-1} \equiv 1$$

$$17 \equiv 5, 13 \equiv 1 \Rightarrow x \equiv 5 \times 1^4 = 5, y = \frac{17-13x}{12}$$

$$\Rightarrow y = \frac{17-65}{12} \Rightarrow y = \frac{-48}{12} = -4$$

$$\Rightarrow \begin{cases} x = x_0 + \frac{b}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases}, d = (a, b) = 1 \Rightarrow \begin{cases} x = 5 + 12k \\ y = -4 - 13k \end{cases}$$

۹. جواب‌های عمومی معادله ی هم‌نهشتی $x^7 + x^6 + 5x \equiv 19$ را بیابید.

کلاس‌های هم‌ارزی رابطه ی هم‌نهشتی به پیمانه ی ۷ عبارت‌اند از: [۰] و [۱] و ... و [۶]. و چون این کلاس‌های هم‌ارزی یک افراز برای Z هستند، لذا جواب معادله ی هم‌نهشتی فوق، یعنی x، به یکی از این کلاس‌ها تعلق دارد. هم‌چنین، چون $x = 0$ در معادله صدق نمی‌کند، پس x در یکی از کلاس‌های هم‌ارزی [۱] تا [۶] است و همواره $(x, 7) = 1$.

$$(x, 7) = 1 \xrightarrow{\text{فرما}} x^6 \equiv 1, x^7 \equiv x$$

$$\Rightarrow x^7 + x^6 + 5x \equiv x + 1 + 5x \Rightarrow x + 1 + 5x \equiv 19, 19 \equiv -2$$

$$\Rightarrow 6x \equiv -3 \Rightarrow 6x \equiv -3 + 21 \Rightarrow 6x \equiv 18 \Rightarrow x \equiv 3$$

$$\Rightarrow x = 7k + 3$$

(توجه دارید که اگر $a \equiv b$ باشد، آن‌گاه $a \equiv b + mk$ که $k \in Z$ و از این نکته استفاده شد.)

۱۰. جواب‌های عمومی معادله ی زیر را بیابید.

$$x^{15} + 18x^4 + 9x^3 + 37x \equiv 17$$

چون $x = 0$ در معادله صدق نمی‌کند، مطابق آن‌چه در مسئله ی قبل بیان شد، باید: $(x, 5) = 1$.

$$(x, 5) = 1 \xrightarrow{\text{فرما}} x^4 \equiv 1, x^5 \equiv x$$

$$\Rightarrow 18x^4 \equiv 18 \equiv 3, (x^5)^3 \equiv x^3 \Rightarrow x^{15} \equiv x^3$$

$$9 \equiv -1 \Rightarrow 9x^3 \equiv -x^3, 37 \equiv 2, 17 \equiv 2$$

$$\Rightarrow x^{15} + 18x^4 + 9x^3 + 37x \equiv x^3 + 3 + (-x^3) + 2x \equiv 2$$

$$\Rightarrow 2x \equiv -1 \Rightarrow 2x \equiv -1 + 5 \Rightarrow 2x \equiv 4$$

$$(2, 5) = 1 \xrightarrow{\text{فرما}} x \equiv 2 \Rightarrow x = 5k + 2$$

۱۱. اگر a عددی صحیح و دل‌خواه باشد، باقی‌مانده ی تقسیم a^{100} را بر ۱۲۵ بیابید.

$$\varphi(125) = 100$$

۱. برای آشنایی با اثبات رابطه ی اویلر و قضایای بیان شده، به جلد دوم، قسمت اول کتاب تئوری مقدماتی اعداد، نوشته ی مرحوم دکتر غلامحسین مصاحب (انتشارات امیرکبیر) مراجعه فرمایید.