



قسمت ۶ هم نهشتی و کاربردهای آن

● سید محمدرضا هاشمی موسوی

اشاره

تعیین باقی مانده‌ی تقسیم و دیگر مسئله‌های خلاق می‌پردازیم. در آخر مبحث، تمرین‌هایی هدف‌دار طراحی شده‌اند که با مشاهده‌ی مثال‌های متن درس می‌توانید، آن‌ها را حل کنید. برای فراگیری بهتر مطالب، بکشید مثال‌هایی

در قسمت قبل، به برخی از کاربردهای هم‌نهشتی اشاره شد. در این قسمت نیز به ادامه‌ی مطلب با عنوان قضیه‌ی اوایلر، تعمیمی از قضیه‌ی کوچک فرما و کاربردهای آن در حل مسئله‌ها و معادله‌های سیاله‌ی خطی و درجه‌ی m و

نظیر و یا در تعمیم مسئله‌ها طراحی و حل کنید.

قضیه‌ی اوایلر و کاربردهای آن

قضیه‌ی اوایلر که می‌توان آن را به عنوان یک قضیه‌ی مستقل معرفی کرد، در واقع تعمیمی از قضیه‌ی فرماست. ابتدا به عنوان این قضیه‌ی بسیار مهم و اثبات آن می‌پردازیم. توجه به این نکته لازم است که فرما قضیه‌ی کوچک خود را حدود ۸۰ سال قبل از اوایلر بیان کرد.

قضیه‌ی اوایلر: اگر m عددی طبیعی و a عددی صحیح باشد و $(m, a) = 1$ ، آن‌گاه: $a^{\varphi(m)} \equiv 1$ تبصره‌ی ۱: تابع φ تابع حسابی اوایلر می‌نامند و این یک تابع ضربی است که برای $m > 1$ در واقع برابر تعداد اعداد طبیعی و کوچک‌تر از m است که نسبت به m اول‌اند و به صورت زیر تعریف می‌شود:

$$m = p_1 \cdot p_2 \cdot p_3 \dots p_n$$

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

در این رابطه، p_1, p_2, \dots, p_n اعداد اول هستند که m به حاصل ضرب n عدد اول تجزیه شده است. بدیهی است، اگر m برابر عددی اول باشد:

$$m = p : \varphi(m) = \varphi(p) = p \left(1 - \frac{1}{p}\right) = p - 1$$

برای مثال، $\varphi(1)$ ، $\varphi(2)$ ، $\varphi(6)$ ، $\varphi(60)$ و $\varphi(2003)$ را تعیین می‌کنیم:

$$\varphi(1) = 1, \varphi(2) = 1, \varphi(6) = 6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 2$$

$$\varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 16,$$

$$\varphi(2003) = 2003 - 1 = 2002$$

(عدد $p = 2003$ اول است و $60 = 2^2 \times 3 \times 5$)

تبصره‌ی ۲. چون φ یک تابع ضربی است، از تعریف $\varphi(m)$ داریم:

$$1) m, n \in \mathbb{N}, (m, n) = d: \varphi(mn) = \varphi(m) \cdot \varphi(n) \times \frac{d}{\varphi(d)} (*)$$

(d : بزرگ‌ترین مقسوم‌علیه مشترک دو عدد طبیعی m و n)

اگر m و n نسبت به هم اول باشند، یعنی

$$\varphi(mn) = \varphi(m) \cdot \varphi(n) : (m, n) = 1$$

$$m = 1, n = p(\quad); (p, 1) = 1$$

$$\varphi(1 \times p) = \varphi(1) \cdot \varphi(p) = 1 \cdot \varphi(p) = p - 1$$

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

$$3) \varphi(2^n) = \begin{cases} 2\varphi(n) & \text{زوج } n \\ \varphi(n) & \text{فرد } n \end{cases}$$

$$4) \varphi(3^n) = \begin{cases} 3\varphi(n) & 3 \mid n \\ 2\varphi(n) & 3 \nmid n \end{cases}$$

$$5) n = 2^k : \varphi(n) = \varphi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = \frac{2^k}{2} = \frac{n}{2}$$

$$6) n \in \mathbb{N} : \varphi(n^2) = \varphi(n, n) = \varphi(n) \cdot \varphi(n) \cdot \frac{(n, n)}{\varphi(n, n)} = n\varphi(n)$$

$$7) (a, b) = d, [a, b] = c : \varphi(a)\varphi(b) = \varphi(c)\varphi(d)$$

$$(d = 1; c = ab : \varphi(ab) = \varphi(a) \cdot \varphi(b))$$

$$8) \sum_{i=1}^k \varphi(d_i) = m(d_1, d_2, \dots, d_k) : m \text{ شمارنده‌های مثبت}$$

اثبات قضیه‌ی اوایلر

اگر $(a, m) = 1$ و فرض کنیم x_1, x_2, \dots, x_n که در آن

$n = \varphi(m)$ ، دسته‌ی ساده‌ی باقی‌مانده، به پیمانه‌ی m باشند،

واضح است که عددهای ax_1, ax_2, \dots, ax_n نیز دسته‌ی

باقی‌مانده‌ها، به پیمانه‌ی m هستند؛ زیرا:

$$(a, m) = 1, n = \varphi(m) : ax_1 \equiv x_1$$

$$ax_2 \equiv x_2$$

$$\dots$$

$$ax_n \equiv x_n$$

از ضرب هم‌نهشتی‌ها:

$$a^n x_1 \cdot x_2 \cdot \dots \cdot x_n \equiv x_1 \cdot x_2 \cdot \dots \cdot x_n \pmod{m}$$

چون $(m, x_1 x_2 \dots x_n) = 1$ ، پس از اختصار لازم خواهیم داشت:

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

بدیهی است، اگر m عدد اولی مثل p باشد، قضیه‌ی اوایلر به حالت خاص، یعنی قضیه‌ی کوچک فرما تبدیل می‌شود:

$$m = p : \varphi(p) = p - 1; a^{p-1} \equiv 1 \pmod{p}$$

تذکر: در قسمت‌های قبل ثابت شد، قضیه‌ی لاینیتز حالت خاصی از قضیه‌ی ویلسن و قضیه‌ی ویلسن نیز نتیجه‌ای از قضیه‌ی کوچک فرماست. بنابراین، در این جا ثابت می‌شود، از قضیه‌ی اوایلر، قضیه‌های لاینیتز، ویلسن و فرما نتیجه خواهد شد:

$$(قضیه‌ی ویلسن) \quad (p-1)! \equiv -1 \pmod{p}, \quad (p-2)! \equiv 1 \pmod{p} \text{ (قضیه‌ی لاینیتز)}$$

هم‌چنین می‌توان ثابت کرد، قضایای فرما و ویلسن جمعاً با این حکم معادل‌اند که به ازای هر عدد اول p و هر عدد صحیح a ، عبارت عددی $a^p + a^{p-1} = M$ را می‌شمارد:

$$p | M$$

مثال: باقی مانده‌ی تقسیم عدد 7^{8^2} بر 3^0 را بیابید.

حل: با توجه به قضیه‌ی اوایلر و برابری $3^0 = 2 \times 3 \times 5$ ، می‌توان نوشت:

$$7^{\varphi(3^0)} \equiv 1; \varphi(3^0) = 3^0 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 8;$$

$$7^8 \equiv 1; 7^{8^2} \equiv 1; 7^{8^2} \equiv 7^{2^3} = 7(7^2) \equiv 7(19) \equiv 13$$

مثال: باقی مانده‌ی تقسیم عدد $N = 87 \times 47^{2008}$ بر 12 را بیابید.

$$\text{حل: } (47, 12) = 1, 47^{\varphi(12)} \equiv 1; 47^4 \equiv 1; (47^4)^{502} \equiv 1$$

$$(باقی مانده‌ی تقسیم) \quad 47^{2008} \equiv 1; 87 \equiv 3; 87 \times 47^{2008} \equiv 3$$

$$(\varphi(12) = \varphi(2^2 \times 3) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4)$$

مثال: تعداد اعداد طبیعی کوچک‌تر از 390 را که نسبت به

60 و 36 اول‌اند تعیین کنید.

حل:

$$390 = 2 \times 3 \times 5 \times 13, (a, 60) = 1; (a, 2^2 \times 3 \times 5) = 1 \quad (1)$$

$$(a, 36) = 1; (a, 2^2 \times 3^2) = 1 \quad (2) \xrightarrow{(1),(2)} (a, 2 \times 3 \times 5) = 1$$

$$390 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 390 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 104$$

104 عدد طبیعی وجود دارد که نسبت به دو عدد 36 و 60 اول‌اند.

مثال: دورقم سمت راست عدد N را بیابید:

$$N = 3^{1367} \times 2^{008}$$

حل:

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

با توجه به قضیه‌ی اوایلر:

$$3^{\varphi(100)} \equiv 1; 3^{40} \equiv 1; (3^{40})^{34} \equiv 1; 3^{1360} \equiv 1$$

$$3^{1360} \times 2^{008} \equiv 2^{008} \equiv 8$$

$$N = 3^{1367} \times 2^{008} \equiv 8 \times 2^{008} = 696 \equiv 96$$

(دورقم سمت راست N)

مثال: اگر $(m, n) = 1$ ، نشان دهید:

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

حل: با توجه به قضیه‌ی اوایلر می‌توان نوشت:

$$(m, n) = 1; m^{\varphi(n)} \equiv 1 \quad (1), n^{\varphi(m)} \equiv 1 \quad (2)$$

از طرفی، هم‌نهشتی‌های زیر بدیهی است:

$$m^{\varphi(n)} \equiv 0 \quad (3), n^{\varphi(m)} \equiv 0 \quad (4)$$

از جمع هم‌نهشتی‌ها

$$(1) + (4): m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \quad (5),$$

$$(2) + (3): n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \quad (6)$$

از جمع (5) و (6) هم‌نهشتی مورد نظر حاصل می‌شود:

$$(5) + (6): m^{\varphi(n)} + n^{\varphi(m)} \equiv 1$$

مثال: باقی مانده‌ی تقسیم عدد k را بر 960 بیابید:

$$k = 25^{48} + 168^{20}$$

حل: با توجه به برابری‌های $168 = 2^3 \times 3 \times 7$ و $25 = 5^2$ و

قضیه‌ی اوایلر و مثال قبل:

مثال: دورقم سمت راست عدد N را بیابید.

$$N = 1388 \times 7^{3001}$$

حل: با توجه به قضیه ی اویلر:

$$\varphi(100) = \varphi(2^2 \times 5^2) = 100 \cdot (1 - \frac{1}{2}) (1 - \frac{1}{5}) = 40$$

$$(7, 100) = 1; \quad 7^{\varphi(100)} \equiv 1; \quad 7^{40} \equiv 1; \quad (7^{20})^{20} \equiv 1$$

$$7^{3000} \times 7 \equiv 7; \quad N = 1388 \times 7^{3001} \equiv 1388 \times 7 = 9716$$

$$N \equiv 9716 \pmod{100}$$

(دورقم سمت راست عدد N برابر ۱۶ است)

مثال: معادله ی سیاله ی خطی عمومی $ax+by=c$ را با استفاده

از قضیه ی اویلر حل کنید.

حل: ابتدا معادله را به یک معادله ی هم نهستی تحویل

می دهیم:

$$ax + by = c; \quad ax \equiv c \pmod{b} \quad \text{یا} \quad by \equiv c \pmod{a}$$

می دانیم شرط جواب برای معادله ی سیاله ی مورد نظر

$(a, b) | c$ است. پس برای حل معادله ی مورد نظر، همیشه باید

داشته باشیم $(a, b) = 1$ که با این فرض خواهیم داشت:

$$(a, b) = 1; \quad x \equiv ca^{\varphi(b)-1} \pmod{b} \quad \text{یا} \quad y \equiv cb^{\varphi(a)-1} \pmod{a}$$

مثال: معادله ی سیاله ی $3x + 4y = 19$ را حل کنید.

حل: با توجه به $(3, 4) = 1$ و قضیه ی اویلر می توان نوشت:

$$\varphi(4) = 4(1 - \frac{1}{2}) = 2; \quad x \equiv 19 \times 3^{\varphi(4)-1} = 19 \times 3 = 57 \pmod{4}$$

k	0	1	2	...
x = 4k + 1	1	5	9	...
y	4	1	3	...

$$3(4k+1) + 4y = 19; \quad y = 4 - 3k$$

مثال: اگر $(m, n) = 1$ ، آن گاه یک سلسله جواب عمومی

معادله ی زیر را با استفاده از قضیه ی اویلر تعیین کنید.

$$x^n + y^n = z^m \quad (1)$$

حل: برای تعیین یک سلسله از جواب های معادله ی ۱، ابتدا

یک سلسله از جواب های معادله ی زیر را تعیین می کنیم:

$$k > 1, \quad k \in \mathbb{N} : x_1^{k-1} + x_2^{k-1} = x_3^k \quad (2)$$

$$25^{\varphi(168)} + 168^{\varphi(25)} = 25^{48} + 168^{20} \equiv 1;$$

$$k \equiv 1 \pmod{960} \quad (\text{باقی مانده ی تقسیم})$$

مثال: نشان دهید اگر $(m, 5) = (n, 5) = 1$ ، آن گاه:

$$25 | (m^{20} - n^{20})$$

حل: با توجه به برابری $25 = 5^2$ و قضیه ی اویلر می توان نوشت:

$$(m, 5) = 1; \quad (m, 25) = 1; \quad m^{\varphi(25)} \equiv 1$$

$$\varphi(25) = 25(1 - \frac{1}{5}) = 20$$

$$m^{20} \equiv 1, \quad (n, 25) = 1; \quad n^{\varphi(25)} \equiv 1; \quad n^{20} \equiv 1$$

بنابراین:

$$m^{20} - n^{20} \equiv 0; \quad 25 | m^{20} - n^{20}$$

مثال: اگر عددی صحیح باشد، باقی مانده ی تقسیم k^{54}

بر ۸۱ را بیابید.

حل: با توجه به برابری $81 = 3^4$ و قضیه ی اویلر:

$$\varphi(81) = 81(1 - \frac{1}{3}) = 54; \quad 3 | k \quad \text{یا} \quad (3, k) = 1$$

$$(3^4, k) = 1; \quad k^{\varphi(81)} \equiv 1; \quad k^{54} \equiv 1 \quad (3, k) = 1$$

بدیهی است که در حالت $3 | k$ یا $3^2 | k$:

$$3^2 | k^{54}; \quad k^{54} \equiv 0$$

مثال: نشان دهید اگر $(10, m) = 1$ ، آن گاه سه رقم سمت

راست m و m^{101} با هم برابرند.

حل: برای اثبات حکم، باید نشان دهیم: $m^{101} \equiv m$

با توجه به برابری $1000 = 8 \times 125$ و قضیه ی اویلر،

می توان نوشت:

$$\varphi(8) = \varphi(2^3) = 8(1 - \frac{1}{2}) = 4, \quad \varphi(125) = \varphi(5^3)$$

$$= 125(1 - \frac{1}{5}) = 100$$

$$m^{\varphi(125)} \equiv 1; \quad m^{100} \equiv 1 \quad (1), \quad \varphi(8) | \varphi(125); \quad m^{100} \equiv 1 \quad (2)$$

از روابط ۱ و ۲ خواهیم داشت:

$$m^{100 \times 125} \equiv 1; \quad m^{1000} \equiv 1; \quad m^{101} \equiv m$$

$$x = 7k + 2, y = 17s + 5$$

k	0	1	2	...
x	2	9	16	...
y	5	683263	651914373	...

تمرین

۱. حاصل $\varphi(2^k)$ و $\varphi(kn)$ ، $\varphi(2008)$ ، $\varphi(10^{1387})$ را

بیابید.

۲. از قضیه‌ی اوایلر، قضیه‌های فرما، لاینیتز و ویلسن را

نتیجه بگیرید.

۳. باقی مانده‌ی تقسیم عدد 7^{87} بر ۲۰ را بیابید.

۴. تعداد اعداد طبیعی کوچک‌تر از ۴۰۰ را که نسبت به اعداد

۳۰ و ۱۸ اول‌اند، بیابید.

۵. دو رقم سمت راست عدد N را بیابید.

$$N = 3^{1364} \times 2009$$

۶. اگر m و n نسبت به هم اول باشند، نشان دهید:

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

۷. باقی مانده‌ی تقسیم عدد k بر ۶۳ را بیابید.

$$k = 13^7 + 78^9$$

۸. نشان دهید، اگر $(k, 3) = (s, 3) = 1$ ، آن‌گاه:

$$9 \mid (m^k - n^s)$$

۹. اگر k عددی صحیح باشد، باقی مانده‌ی تقسیم N^{294} بر

۳۴۳ را بیابید.

۱۰. نشان دهید اگر $(1, n) = 1$ ، آن‌گاه چهار رقم سمت

راست 10^m و 10^{m+1} با هم برابرند.

۱۱. دو رقم سمت راست عدد M را بیابید:

$$M = 1389 \times 7^{2001}$$

۱۲. معادله‌ی سیاله‌ی $13x + 17y = 74$ را با استفاده از

قضیه‌ی اوایلر حل کنید.

۱۳. یک سلسله جواب عمومی $z^{2003} = x^{1387} + y^{1387}$

را با استفاده از قضیه‌ی اوایلر تعیین کنید.

۱۴. اگر $(m, n) = 1$ ، مضرب k را در برابری زیر تعیین

کنید:

$$m^{\varphi(n)} \geq kn + 1$$

برای تعیین یک سلسله از جواب‌های معادله‌ی ۲، کافی است آن را با اتحاد زیر مقایسه کنیم:

$$a, b \in \mathbb{Z} : (a^k + ab^{k-1})^{k-1} + (ba^{k-1} + b^k)^{k-1} \\ = (a^{k-1} + b^{k-1})^k \quad (3)$$

از مقایسه‌ی معادله‌ی ۲ و اتحاد ۳، بلافاصله یک سلسله جواب معادله‌ی ۲ به دست می‌آید:

$$(x_1, x_2, x_3) = (a^k + ab^{k-1}, ba^{k-1} + b^k, a^{k-1} + b^{k-1})$$

در این جا، با فرض $k = m^{\varphi(n)}$ ، معادله‌ی ۲ به معادله‌ی زیر تحول می‌شود:

$$(x_1, x_2, x_3) = (a^k + ab^{k-1}, ba^{k-1} + b^k, a^{k-1} + b^{k-1}) \quad (4)$$

طبق قضیه‌ی اوایلر، اگر $(m, n) = 1$ ، آن‌گاه $(m^{\varphi(n)} - 1)$ بر n بخش پذیر است:

$$(m, n) = 1 ; m^{\varphi(n)} - 1 = n \left(1 + 2 \left[\frac{m^{\varphi(n)} - 1}{2n} \right] \right) \quad (5)$$

([] : قسمت درست عدد)

با توجه به رابطه‌ی ۵ بلافاصله یک سلسله از جواب‌های معادله‌ی ۱ حاصل می‌شود:

$$\begin{cases} x = (a^{m^{\varphi(n)}} + ab^{m^{\varphi(n)-1})^{1+2 \left[\frac{m^{\varphi(n)} - 1}{2n} \right]} \\ y = (ba^{m^{\varphi(n)-1} + b^{m^{\varphi(n)}})^{1+2 \left[\frac{m^{\varphi(n)} - 1}{2n} \right]} \\ z = (a^{m^{\varphi(n)-1} + b^{m^{\varphi(n)-1}})^{m^{\varphi(n)-1}} \end{cases} \quad (6)$$

$$(m = p^k \cdot q^s \cdot r^t \dots, \varphi(m) = m(1 - \frac{1}{p}) \dots)$$

مثال: معادله‌ی سیاله‌ی درجه‌ی هفتم زیر را حل کنید.

$$34x^7 - 14y = 4282$$

حل: معادله را به صورت زیر می‌نویسیم:

$$17x^7 \equiv 2141; 17x^7 \equiv 3x^7 \equiv 6; x^7 \equiv 2$$

$$x = 2; y = \frac{17(2)^7 - 2141}{7} = 5;$$