

هم نهشتی و

کاربردهای آن

قسمت ۱

● سید محمدرضا هاشمی موسوی
hashemi - moosavi@yahoo.com

صورتی که هر دو ظرف A و B پر از شیر باشند و بخواهیم با پیمانه ی C شیر برداریم، واضح است که پس از ۸ بار برداشت از ظرف A و پس از ۳ بار برداشت از ظرف B، ۲ لیتر شیر در هر یک از ظرف ها باقی مانده به اصطلاح می گوییم دو ظرف A و B به پیمانه ی ۵ هم پیمانه و یا به بیان دیگر هم نهشت اند. این مطلب را با بیان ریاضی به این صورت نشان می دهند:

واژه ی «هم نهشتی» برگردان کلمه ی «Congruence» است. این کلمه به معنای سازگاری، موافقت و مطابقت شیئی با شیء دیگر به کار رفته است. برای مثال، در هندسه دو شکل را که قابل انطباق باشند، هم نهشت گویند. در این جا، برای درک بیشتر این واژه مثالی می آوریم. مثال: فرض کنید دو ظرف شیر با گنجایش های $A = 42$ و $B = 17$ و یک پیمانه ی $C = 5$ لیتری در دسترس داشته باشیم. در

$$A \overset{\circ}{\equiv} B$$

مفهوم هم پیمانی یا هم نهشتی را که بین ظرف ها برقرار است، می توان در Z تعمیم داد و در حالت کلی، این مفهوم را به صورت زیر تعریف کرد:

تعریف

اگر m عددی طبیعی و a و b دو عدد صحیح باشند، a و b را به پیمانه m (سج) «هم نهشت» گوئیم، هرگاه $(a-b)$ یا $(b-a)$ مضربی صحیح از m (پیمانه) باشد. به بیان دیگر، عبارت $(a-b)$ یا $(b-a)$ بر m بخش پذیر باشد، در این صورت می نویسیم:

$$a \overset{m}{\equiv} b \quad (۱)$$

بیان ریاضی این تعریف چنین است:

$$\forall a, b \in Z, m \in \mathbb{N}; a \overset{m}{\equiv} b \Leftrightarrow a - b = km \text{ یا } m | (a - b)$$

قضیه ۱: رابطه ی هم نهشتی به پیمانه m ($\overset{m}{\equiv}$) روی Z (مجموعه ی اعداد صحیح) یک رابطه ی هم ارزی است.

اثبات: باید ثابت کرد که رابطه ی $\overset{m}{\equiv}$ دارای سه خاصیت انعکاسی، تقارنی و تعدی است:

$$\text{(انعکاسی)} \quad \forall a \in Z, a - a = (0)m \Rightarrow a \overset{m}{\equiv} a$$

$$\text{(ب)} \quad \forall a, b \in Z, a \overset{m}{\equiv} b \Rightarrow m | a - b \Rightarrow m | -(a - b)$$

$$\Rightarrow m | (b - a) \Rightarrow b \overset{m}{\equiv} a \quad \text{(تقارنی)}$$

$$\text{(ج)} \quad \forall a, b, c \in Z, a \overset{m}{\equiv} b, b \overset{m}{\equiv} c \Rightarrow m | (a - b), m | (b - c)$$

$$\Rightarrow m | (a - b) + (b - c) \Rightarrow m | (a - c) \Rightarrow a \overset{m}{\equiv} c \quad \text{(تعدی)}$$

در این جا، ثابت شد که رابطه ی $\overset{m}{\equiv}$ ، یک رابطه ی هم ارزی است و چون هر رابطه ی هم ارزی، هر مجموعه ی تعریف شده روی آن را افراز می کند، بنابراین، رابطه ی $\overset{m}{\equiv}$ مجموعه ی Z را افراز می کند و بنا به تعریف کلاس های هم ارزی، برای هر عضو Z ، کلاس هم ارزی یا دسته ی هم نهشتی، به صورت زیر تعریف می شود:

$$\forall a \in Z, [a] = \left\{ x \in Z \mid x \overset{m}{\equiv} a \right\}$$

برای مثال، اگر $m=2$ ، آن گاه خواهیم داشت:

$$[0] = \left\{ x \in Z \mid x \overset{2}{\equiv} 0 \right\} = \{ x \in Z \mid x = 2k \}$$

$$= \{ \dots, -4, -2, 0, 2, 4, \dots \}$$

$$[1] = \left\{ x \in Z \mid x \overset{2}{\equiv} 1 \right\} = \{ x \in Z \mid x = 2k + 1 \}$$

$$= \{ \dots, -3, -1, 1, 3, \dots \}$$

بدیهی است که $2 \in [0]$ ، پس $[2] = [0]$ و هم چنین $3 \in [1]$ ، پس $[3] = [1]$. به همین ترتیب، برای هر عضو دل خواه مثل a که $a \in [0]$ داریم $[a] = [0]$ و برای هر عضو دل خواه مثل b که $b \in [1]$ ، خواهیم داشت $[b] = [1]$. بنابراین رابطه ی $\overset{2}{\equiv}$ ، فقط دو کلاس یا دسته ی هم نهشتی دارد که این دو مجموعه، Z را افراز می کنند:

$$\text{(زیرا: } 1 \in [1], 0 \in [0]) \quad [1] \neq \emptyset, [0] \neq \emptyset$$

$$[0] \cap [1] = \emptyset$$

$$[0] \cup [1] = Z$$

تذکره ۱: رابطه ی $\overset{m}{\equiv}$ ، دارای m دسته ی هم نهشتی $[0], [1], \dots, [m-1]$ است. در حالت کلی، دسته ی هم نهشتی عدد مفروض a به پیمانه m را با نماد $[a]_m$ نشان می دهیم.

تذکره ۲: شرط لازم و کافی برای آن که $x \in [a]_m$ ، آن است که داشته باشیم: $x \overset{m}{\equiv} a$.

قضیه ۲: اگر عددی مثل a بر m تقسیم کنیم و باقی مانده ی تقسیم را به r نشان دهیم $(a = mq + r)$ ، آن گاه خواهیم داشت:

$$a \overset{m}{\equiv} r$$

اثبات: با توجه به فرض قضیه، یعنی $a = mq + r$ ، می توان نوشت $a - r = mq$ یا $m | a - r$. پس:

$$a \overset{m}{\equiv} r$$

نتیجه: با استفاده از قضیه ۲، می توان عدد هم نهشت با عدد مفروض به پیمانه ی دل خواه را محاسبه کرد. یعنی کافی است عدد مورد نظر را به پیمانه تقسیم کنیم و باقی مانده ی تقسیم را به دست آوریم.

مثال: عدد هم نهشت با ۳۳۴ به پیمانه ی ۱۷ را بیابید.

حل: با توجه به تقسیم ۳۳۴ بر ۱۷، خواهیم داشت:

$$334 = 17 \times 19 + 11 \Rightarrow 334 \overset{17}{\equiv} 11$$

قضیه ۳: برای عددهای صحیح k و s ، اگر $a \overset{m}{\equiv} b$ ، آن گاه:

$$a + km \overset{m}{\equiv} b + sm$$

اثبات: با توجه به فرض $a \overset{m}{\equiv} b$ ، می توان نوشت:

$$a - b = t, m$$

هم چنین:

$$(a + km) - (b + sm) = (a - b) + m(\underbrace{k-s}_{t_1}) = t_1 m + t_2 m$$

$$= (\underbrace{t_1 + t_2}_q) m = qm$$

پس:

$$(a + km) - (b + sm) = qm \Rightarrow a + km \equiv b + sm^m$$

نتیجه: اگر به دو طرف یک رابطه‌ی هم‌نهشتی، هر مضرب صحیحی از پیمانه را اضافه کنیم، همیشه به یک هم‌نهشتی معادل خواهیم رسید. در حالت خاص، با فرض $k = 0$ ، خواهیم داشت:

$$a \equiv b + sm^m$$

بنابراین، همیشه دو طرف یا یک طرف هر رابطه‌ی هم‌نهشتی را می‌توان به اندازه‌ی هر مضرب پیمانه تغییر داد. برای مثال، هم‌نهشتی $a \equiv -3$ ، معادل هم‌نهشتی $a \equiv 5 - 3$ یا $a \equiv 2$ است.

مسئله: در صورتی که a عددی صحیح باشد، ثابت کنید:

$$a \equiv 1^2 \text{ یا } a \equiv 0^2$$

حل: رابطه‌ی $a \equiv 1^2$ ، مجموعه‌ی Z را به دو مجموعه‌ی $[0]$ و $[1]$ افراز می‌کند و با توجه به تعریف افراز، باید $[0] \cup [1] = Z$. پس اگر

a عدد صحیح دل‌خواهی باشد، باید $a \in [0]$ یا $a \in [1]$. بنابراین، بر طبق تعریف دسته‌های هم‌نهشتی خواهیم داشت:

$$a \in [0] \Rightarrow a \equiv 0^2 ; a \in [1] \Rightarrow a \equiv 1^2$$

تذکره ۱: گزاره‌ی « a و b به پیمانه‌ی m هم‌نهشت‌اند» را با یکی از نمادهای زیر نشان می‌دهند:

$$1) a \equiv b^m \quad 2) a \equiv b \text{ (پیمانه‌ی } m)$$

$$3) a \equiv b \text{ (هنگ } m) \quad 4) a \equiv b \pmod{m}$$

در صورتی که $(a-b)$ مضرب m نباشد، a و b به پیمانه‌ی m ناهم‌نهشت‌اند. در این صورت می‌نویسیم:

$$a \not\equiv b \text{ (پیمانه‌ی } m)$$

تذکره ۲: می‌دانیم هر عددی بر ۱ بخش پذیر است. بنابراین، هر دو عدد صحیح به پیمانه‌ی ۱ هم‌نهشت‌اند. به همین دلیل در عمل، همیشه پیمانه‌هایی غیر از ۱ مورد نظر ما خواهند بود.

قضیه‌ی ۴: دو عدد صحیح a و b به پیمانه‌ی m هم‌نهشت‌اند، اگر و تنها اگر باقی‌مانده‌ی a بر m برابر باقی‌مانده‌ی b بر m باشد. اثبات: با فرض این که a و b به پیمانه‌ی m هم‌نهشت‌اند، می‌توان نوشت:

$$a \equiv b \Rightarrow a - b = km ; a = b + km \quad (1)$$

اگر باقی‌مانده‌ی b بر m برابر r باشد:

$$b = sm + r ; 0 \leq r < m \quad (2)$$

از رابطه‌های ۱ و ۲ نتیجه می‌شود:

$$a = (sm + r) + km ; a = (k + s)m + r , 0 \leq r < m$$

این برابری نشان می‌دهد که r باقی‌مانده‌ی a بر m است. یعنی a و b هم باقی‌مانده‌اند.

به عکس: با فرض این که باقی‌مانده‌ی a و b بر m برابر باشد:

$$\begin{cases} a = km + r \\ b = k'm + r \end{cases} \Rightarrow a - b = m(k - k') ; a \equiv b^m$$

توجه: هم‌نهشتی در واقع تعمیم برابری است و رفتار آن در ارتباط با جمع و ضرب، مانند جمع و ضرب معمولی است. برخی از این خواص را در قضیه‌ی زیر آورده‌ایم.

قضیه‌ی ۵: اگر m عدد طبیعی ثابت و a ، b و c اعداد صحیح دل‌خواه باشند، در این صورت خواص زیر برقرار است:

$$1) a \equiv a^m$$

$$2) a \equiv b \Rightarrow b \equiv a^m$$

$$3) a \equiv b , b \equiv c \Rightarrow a \equiv c^m$$

$$4) a \equiv b , c \equiv d \Rightarrow a + c \equiv b + d^m$$

$$5) a \equiv b , c \equiv d \Rightarrow ac \equiv bd^m$$

$$6) a \equiv b \Rightarrow a^k \equiv b^k \text{ (} k \in \mathbb{N} \text{)}$$

$$7) a \equiv b , a \equiv b \Rightarrow a \equiv b^{[m,n]}$$

$$8) a \equiv b , b \equiv c \Rightarrow a \equiv c^{(m,n)}$$

$$9) a \equiv b \Rightarrow (a, m) = (b, m)$$

$$10) ac \equiv bc^m , (m, c) = d \Rightarrow a \equiv b^{\frac{m}{d}}$$

$$11) a \equiv 1 \Leftrightarrow (a, m) = 1$$

در این جا، هر قسمت را به طور خلاصه و مختصر اثبات می‌کنیم:

۱. می‌دانیم برای هر a داریم $a - a = (0)m$ ، پس می‌توان نوشت:

$$a \equiv a^m$$

۲. اگر $a \equiv b^m$ ، در این صورت $a - b = km$ و یا

$$b - a = (-k)m \text{ ، پس : } b \equiv a^m$$

$$a_1 a_2 \cdots a_k \equiv^m b_1 b_2 \cdots b_k$$

۶. اگر در نتیجه ی ۲ فرض کنیم:

$$a_1 = a_2 = \cdots = a_k = a, \quad b_1 = b_2 = \cdots = b_k = b$$

خواهیم داشت:

$$a^m \equiv b \Rightarrow a^k \equiv^m b^k$$

۷. با فرض $a \equiv^m b$ و $a \equiv^n b$ ، به ترتیب می توان نوشت

$$ml(a-b), \quad nl(a-b) \text{ . پس:}$$

$$[m, n](a-b) \Rightarrow a^{[m, n]} \equiv b$$

نتیجه: اگر $a \equiv^m b$ و $a \equiv^n b$ و $(m, n) = 1$ ، بدیهی است که

$$[m, n] = mn \text{ . پس:}$$

$$a^{mn} \equiv b$$

۸. با فرض $(m, n) = d$ ، خواهیم داشت $d|m$ و $d|n$. پس:

$$\begin{cases} d|m \\ m|(a-b) \end{cases} \Rightarrow d|(a-b)(\frac{m}{d}) \text{ , } \begin{cases} d|n \\ n|(b-c) \end{cases} \Rightarrow$$

$$d|(b-c)(\frac{n}{d}) \Rightarrow d|(a-b) + (b-c) \Rightarrow d|(a-c) \Rightarrow a^d \equiv c$$

۹. با فرض $(a, m) = d_1$ و $(b, m) = d_2$ ، ثابت می کنیم

$$d_1 = d_2$$

با توجه به فرض، یعنی $a \equiv^m b$ ، داریم $a - b = km$. پس:

$$(a, m) = d_1 \Rightarrow \begin{cases} d_1|a \\ d_1|m; d_1|km \end{cases} \Rightarrow d_1|a - km = b$$

می دانیم اگر $d_1|b$ و $d_1|m$ ، آن گاه $d_1|(b, m) = d_2$ و در

$$نتیجه خواهیم داشت: $d_1 \leq d_2$$$

به همین ترتیب، می توان ثابت کرد که $d_2|d_1$ یا $d_2 \leq d_1$.

بنابراین در کل ثابت می شود: $d_1 = d_2$.

۱۰. با فرض $ac \equiv^m bc$ ، خواهیم داشت $m|(ac - bc)$ یا

$$m|c(a - b) \text{ . پس:}$$

$$c(a - b) = km \xrightarrow{\text{(تقسیم بر } d)} \frac{c}{d}(a - b) = \frac{m}{d}k$$

$$\Rightarrow \frac{m}{d} \left| \frac{c}{d}(a - b) \right.$$

$$\xrightarrow{\substack{(\frac{m}{d} \cdot \frac{c}{d})=1 \\ \text{(لم اقلیدس)}}} \frac{m}{d} | (a - b) \Rightarrow a \equiv^m b$$

نتیجه: اگر $ac \equiv^m bc$ و $(m, c) = 1$ ، آن گاه $a \equiv^m b$.

۳. با فرض $a \equiv^m b$ و $b \equiv^m c$ ، خواهیم داشت:

$$\begin{cases} a - b = km \\ b - c = k'm \end{cases} \Rightarrow a - c = (k + k')m \Rightarrow a \equiv^m c$$

۴. با فرض $a \equiv^m b$ و $c \equiv^m d$ ، خواهیم داشت:

$$\begin{cases} a - b = km \\ c - d = k'm \end{cases} \Rightarrow (a + c) - (b + d) = (k + k')m$$

$$\Rightarrow a + c \equiv^m b + d$$

نتیجه ی ۱: در حالت خاص خواهیم داشت:

$$a \equiv^m b \Rightarrow a \pm c \equiv^m b \pm c$$

نتیجه ی ۲: به استقرا می توان نشان داد که اگر داشته باشیم:

$$\begin{matrix} a_1 & \equiv^m & b_1 \\ a_2 & \equiv^m & b_2 \\ \dots & \dots & \dots \\ & \vdots & \\ \dots & \dots & \dots \\ a_k & \equiv^m & b_k \end{matrix}$$

آن گاه:

$$a_1 + a_2 + \cdots + a_k \equiv^m b_1 + b_2 + \cdots + b_k$$

۵. با فرض $a \equiv^m b$ و $c \equiv^m d$ ، خواهیم داشت:

$$\begin{cases} a - b = km \\ c - d = k'm \end{cases} ; \quad \begin{cases} a = b + km \\ c = d + k'm \end{cases}$$

از ضرب دو رابطه ی فوق خواهیم داشت:

$$ac = bd + (bk' + dk + kk'm)m \Rightarrow ac \equiv^m bd$$

نتیجه ی ۱: در حالت خاص خواهیم داشت:

$$a \equiv^m b \Rightarrow ac \equiv^m bc$$

نتیجه ی ۲: به استقرا می توان نشان داد که اگر داشته باشیم:

$$\begin{matrix} a_1 & \equiv^m & b_1 \\ a_2 & \equiv^m & b_2 \\ \dots & \dots & \dots \\ & \vdots & \\ \dots & \dots & \dots \\ a_k & \equiv^m & b_k \end{matrix}$$

آن گاه:

۱۱. با فرض $a \equiv 1^m$ ، خواهیم داشت $a - 1 = km$ یا $a = km + 1$. پس: $(a, m) = 1$ و به عکس، اگر $(a, m) = 1$ ، خواهیم داشت $a = km + 1$ یا $a - 1 = km$. پس: $a \equiv 1^m$. نتیجه: با فرض $(a, m) = 1$ ، خواهیم داشت:

$$(n \in \mathbb{N}) \quad a^n \equiv 1^m$$

نکته: به طور کلی، اگر $a \equiv r^m$ و $0 \leq r < m$ ، در این صورت باقی مانده‌ی a بر m برابر r است.

مسائل حل شده

۱. عدد ۱۳۴ به پیمانه‌ی ۷، با چه عددی بین صفر و ۷ هم‌نهشت است؟

حل: ابتدا عدد ۱۳۴ را بر ۷ تقسیم می‌کنیم:

$$134 = 19(7) + 1$$

بدیهی است، باقی مانده‌ی این تقسیم، جواب مسئله است:

$$(19(7) \equiv 0 \pmod{7}) \quad 134 \equiv 1 \pmod{7}$$

۲. با فرض $a \equiv 2$ ، نشان دهید $a \equiv 3$.

حل: با توجه به $a \equiv 2$ ، می‌توان به طرف دوم فرض، صفر را افزود:

$$a \equiv 2 \Rightarrow a \equiv 3$$

۳. با فرض $a \equiv 7^9$ ، باقی مانده‌ی a بر ۹ را به دست آورید.

$$(7^9 \equiv 0 \pmod{9}) \quad a \equiv 7^9 \Rightarrow a \equiv 7$$

۴. باقی مانده‌ی تقسیم 2^7 ، 4^7 ، 2^{21} را بر ۲۹ بیابید.

حل:

$$2^7 = 128 = 4(29) + 12 \Rightarrow 2^7 \equiv 12$$

$$4^7 = 2^{14} = (2^7)^2 \equiv (12)^2 \equiv 144 \equiv 28$$

$$2^{21} = (2^7)^3 \equiv (12)^3 \equiv 1728 \equiv 59(29) + 17 \equiv 17$$

۵. باقی مانده‌ی تقسیم $[(5 \times (41)^{83})^{1379}]$ بر ۹ را به دست

آورید.

حل:

$$41 \equiv 5 \pmod{9}, \quad 5^3 \equiv 125 \equiv 8 \equiv -1 \Rightarrow 5^9 \equiv -1$$

$$(5^3)^{27} \equiv (-1)^{27} \equiv -1 \Rightarrow 5^{81} \times 5^{29} \equiv (-1) \times 5^2 \Rightarrow 5^{83} \equiv -25$$

$$(41)^{83} \equiv 5^{83} \equiv -25 \equiv 27 - 25 \equiv 2 \Rightarrow 5 \times (41)^{83} \equiv 10 \equiv 1$$

$$\Rightarrow [5 \times (41)^{83}]^{1379} \equiv 1$$

۶. باقی مانده‌ی تقسیم $31 + (32)^{802}$ بر ۱۵ را بیابید.

حل:

$$2^5 = 32 \equiv 2 \pmod{15}, \quad 2^4 \equiv 1 \pmod{15}, \quad (2^4)^{200} \equiv 1 \pmod{15}; \quad 2^{800} \times 2^2 \equiv 2^2$$

$$2^{802} \equiv 4 \pmod{15}, \quad 32^{802} \equiv 2^{802} \Rightarrow 32^{802} \equiv 4 \pmod{15}; \quad 32^{802} + 31 \equiv 4 + 31$$

$$32^{802} + 31 \equiv 35 \equiv 5 \pmod{15} \Rightarrow r = 5$$

۷. باقی مانده‌ی تقسیم $9 \times (7006)^{2001}$ بر ۷ را بیابید.

حل:

$$7006 \equiv 6 \pmod{7}; \quad (7006)^{2001} \equiv (-1)^{2001} \equiv -1 \pmod{7}; \quad 9 \times 6 \equiv 6 \pmod{7}$$

$$9 \times (7006)^{2001} \equiv -9 \equiv 5 \pmod{7}; \quad 9 \times (7006)^{2001} \equiv 5 \pmod{7} \Rightarrow r = 5$$

۸. باقی مانده‌ی تقسیم $(2^{13} - 4)$ بر ۲۳ را بیابید.

حل:

$$2^6 \equiv 18 \equiv -5 \pmod{23}, \quad 2^5 \equiv 9 \Rightarrow 2^6 \times 2^5 \equiv -45 \equiv 1$$

$$2^{11} \equiv 1 \pmod{23}; \quad 2^2 \times 2^{11} \equiv 2^2 \pmod{23}; \quad 2^{13} \equiv 4 \pmod{23}; \quad 2^{13} - 4 \equiv 0 \pmod{23} \Rightarrow r = 0$$

تمرین

۱. اگر $x \equiv 37$ ، باقی مانده‌ی x بر ۵ چه عددی است؟

۲. اگر x بر ۱۳ باقی مانده‌ی ۷ دهد، $8x - 1$ بر ۱۳ چه

باقی مانده‌ای می‌دهد؟

۳. اگر n بر ۷ باقی مانده‌ی ۴ دهد و

$x = n^3 + 3n^2 + 4n + 1$ ، باقی مانده‌ی x بر ۷ چه عددی است؟

۴. اگر باقی مانده‌های تقسیم x بر ۷ و ۸ به ترتیب برابر ۳ و ۵

باشند، باقی مانده‌ی تقسیم x بر ۵۶ چه عددی است؟

۵. باقی مانده‌ی تقسیم 13^{1377} بر ۱۳ چه عددی است؟

۶. باقی مانده‌ی تقسیم $65^{1377} + 66^{1377}$ بر ۱۳ چه

عددی است؟

۷. باقی مانده‌ی تقسیم $s = (67 \times 68)^{1377}$ بر ۱۳ چه عددی

است؟

۸. باقی مانده‌ی تقسیم 7^{1382} بر عدد ۱۹ چه عددی است؟

۹. باقی مانده‌ی تقسیم 11^{1383} بر عدد ۶۱ چه عددی است؟

۱۰. باقی مانده‌ی تقسیم 13^{581} بر عدد ۴۱ را تعیین کنید.

۱۱. باقی مانده‌ی تقسیم $N = 19^{57} + 13^{75}$ بر عدد ۱۷ را

تعیین کنید.

۱۲. باقی مانده‌ی تقسیم $5(7006)^{2005}$ بر عدد ۷ را بیابید.

ادامه دارد...