

هم‌نهشتی

تعریف: اگر a و b دو عدد صحیح و m عددی طبیعی باشد، در این صورت می‌گوییم a و b به پیمانه m با یکدیگر هم‌نهشت‌اند و می‌نویسیم $a \equiv b \pmod{m}$ هرگاه، $(a-b)$ بر m بخش‌پذیر باشد یا $m \mid (a-b)$ ، یعنی:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \text{ یا } a - b = mk \quad (k \in \mathbb{Z})$$

مثال: دو عدد ۶۵ و ۳۷ به پیمانه ۷ با یکدیگر هم‌نهشت‌اند، زیرا $۷ \mid (۶۵ - ۳۷) = ۲۸$.

مثال: اگر $۱۲ \equiv ۷۲ \pmod{p}$ و p عددی اول باشد، در این صورت داریم:

$$۱۲ \equiv ۷۲ \pmod{p} \rightarrow p \mid ۱۲ - ۷۲ \rightarrow p \mid -۶۰ \rightarrow p = ۲ \text{ یا } p = ۳ \text{ یا } p = ۵$$

قضیه: رابطه $\equiv \pmod{m}$ روی \mathbb{Z} یک رابطه هم‌ارزی است.

این قضیه گویای این مطلب است که رابطه هم‌نهشتی به پیمانه m سه خاصیت انعکاسی، تقارنی و تعدی (تراپایی) دارد:

$$\text{I) } \forall a \in \mathbb{Z}, m \mid a - a \rightarrow a \equiv a \pmod{m}$$

اثبات:

$$\text{II) } \forall a, b \in \mathbb{Z}, a \equiv b \pmod{m} \rightarrow m \mid a - b \rightarrow m \mid b - a \rightarrow b \equiv a \pmod{m}$$

$$\text{III) } \forall a, b, c \in \mathbb{Z}, a \equiv b \pmod{m}, b \equiv c \pmod{m} \rightarrow m \mid b - a, m \mid b - c \rightarrow m \mid (a - b) + (b - c) \rightarrow m \mid a - c \rightarrow a \equiv c \pmod{m}$$

تذکر مهم: چون رابطه $\equiv \pmod{m}$ روی \mathbb{Z} یک رابطه هم‌ارزی است، لذا این رابطه \mathbb{Z} را به m کلاس هم‌ارزی به صورت زیر افراز می‌کند.

$$[0]_m = \{x \in \mathbb{Z} \mid x \equiv 0\} = \{x \in \mathbb{Z} \mid x = mk\}$$

$$[1]_m = \{x \in \mathbb{Z} \mid x \equiv 1\} = \{x \in \mathbb{Z} \mid x = mk + 1\}$$

⋮

$$[m-1]_m = \{x \in \mathbb{Z} \mid x \equiv m-1\} = \{x \in \mathbb{Z} \mid x = mk + (m-1)\}$$

توجه داریم که از تعریف کلاس‌های هم‌ارزی و خواص آن‌ها و نیز تعریف افراز نتیجه می‌شود که:

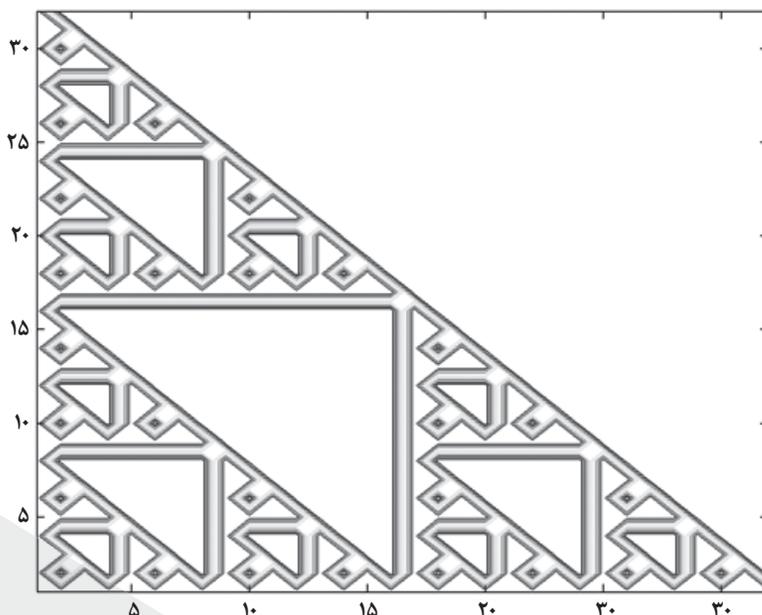
(I) هیچ دو کلاس هم‌ارزی عضو مشترک ندارند.

(II) هر دو عضو یک کلاس هم‌ارزی به پیمانه m با یکدیگر هم‌نهشت‌اند و به عکس، اگر دو عدد صحیح به پیمانه m با یکدیگر هم‌نهشت باشند این دو عدد در یک کلاس هم‌ارزی قرار دارند و باقی‌مانده‌های تقسیم آن‌ها بر m مساوی‌اند.

$$\text{(III) } [a]_m = [a + mk]_m \quad (k \in \mathbb{Z})$$

کلیدواژه‌ها:

پیمانه، رابطه هم‌ارزی، کلاس هم‌ارزی، انعکاسی، تقارنی، تعدی، معادله سیاله، معادله هم‌نهشتی.



۱. عدد ۱۳۹۱ به کدام دسته یا کلاس هم‌ارزی به پیمانه ۷ تعلق دارد؟

- ۴۴ (۱)
- ۱۲۲ (۲)
- ۲۹۶ (۳)
- ۱۰۱ (۴)

حل: گزینه (۳)

$$\left. \begin{aligned} -296 &= 7(-43) + 5 \\ 1391 &= 7(198) + 5 \end{aligned} \right\} \Rightarrow 1391 \equiv -296 \pmod{7}$$

۲. در صورتی که داشته باشیم $[7x + 2]_7 = [6x - 3]_7$ ، کدام گزینه درست است؟

- (۱) $x = 5k + 1$
- (۲) $x = 4k + 1$
- (۳) $x = 4k + 2$
- (۴) $x = 4k + 3$

حل: گزینه (۴)

$$[7x + 2]_7 = [6x - 3]_7 \rightarrow 7x + 2 \equiv 6x - 3 \pmod{7} \rightarrow 7x - 6x \equiv -3 - 2 \pmod{7} \rightarrow x \equiv -5 \equiv 2 \pmod{7} \rightarrow x = 4k + 3$$

ویژگی‌های رابطه هم‌نهشتی

- ۱) $a \equiv b \Leftrightarrow a \pm c \equiv b \pm c$
- ۲) $a \equiv b \Leftrightarrow ka \equiv kb$ ($k|m$)
- ۳) $a \equiv b \rightarrow ac \equiv bc$
- ۴) $a \equiv b \rightarrow a^n \equiv b^n$ ($n \in \mathbb{N}$)
- ۵) $a \equiv b, n|m \rightarrow a^n \equiv b^n$
- ۶) $a \equiv b, c \equiv d \rightarrow a \pm c \equiv b \pm d, a \pm d \equiv b \pm c$
- ۷) $a \equiv b, c \equiv d \rightarrow ac \equiv bd, ad \equiv bc$
- ۸) $a \equiv b, a \equiv c \rightarrow a \equiv b \equiv c$ ($[m, n]$)
- ۹) $a \equiv b, b \equiv c \rightarrow a \equiv c$ ((m, n))

اگر a را بر m تقسیم کنیم و باقی‌مانده تقسیم r باشد، در این صورت (a)، یعنی مقسوم، با باقی‌مانده، به پیمانه مقسوم‌علیه، یعنی m هم‌نهشت است.

$$۱۱) a \equiv b \rightarrow a \pm mt \equiv b \pm mk$$

(به دو طرف یک رابطه هم‌نهشتی می‌توان هر مضربی از پیمانه را اضافه یا از دو طرف کم کرد).

$$(۱۱) a \equiv b \xrightarrow{t \cdot} a \equiv b \pm mk$$

(می‌توانیم فقط به یک طرف رابطه \equiv هر مضربی از پیمانه را اضافه یا کم کنیم).

$$۱۲) a \equiv b \rightarrow (a, m) \equiv (b, m)$$

$$۱۳) ab \equiv ac, (a, m) = d \rightarrow b \equiv c \pmod{\frac{m}{d}}$$

$$۱۴) ab \equiv ac, (a, m) = 1 \rightarrow b \equiv c$$

قضیه اصلی هم‌نهشتی‌ها: شرط لازم و کافی برای این که $a \equiv b$ باشد آن است که باقی‌مانده‌های تقسیم a و b بر m مساوی باشند، یعنی:

$$a \equiv b \Leftrightarrow \begin{cases} a = mq_1 + r \\ b = mq_2 + r \end{cases}$$

مثال‌ها و مسائل مهم

مثال ۱: عدد ۱۳۹۲ به پیمانه ۱۴ با کدام عدد هم‌نهشت است؟

حل: کافی است عدد ۱۳۹۲ را بر ۱۴ تقسیم کنیم. طبق ویژگی ۱۰ باقی‌مانده تقسیم جواب مسئله ماست.

$$۱۳۹۲ = ۱۴ \times ۹۹ + ۶ \rightarrow ۱۳۹۲ \equiv ۶$$

مثال ۲: اگر $a \equiv -۱۱$ در این صورت باقی‌مانده تقسیم a بر ۷ را بیابید.

حل: طبق ویژگی ۱۱ و حالت خاص آن کافی است دو برابر پیمانه را به ۱۱ اضافه کنیم، خواهیم داشت:

$$a \equiv -۱۱ \rightarrow a \equiv -۱۱ + ۱۴ \rightarrow a \equiv ۳ \rightarrow ۷ | a - ۳ \rightarrow a - ۳ = ۷k \rightarrow a = ۷k + ۳ \rightarrow r = ۳$$

مسئله ۱: باقی‌مانده تقسیم عدد $A = ۴۹^{۱۳۹۱} \times ۱۰۲$ را بر ۲۴ بیابید.

$$۴۹ \equiv ۱ \rightarrow ۴۹^{۱۳۹۱} \equiv ۱ \rightarrow ۴۹^{۱۳۹۱} \times ۱۰۲ \equiv ۱۰۲ \equiv ۶ \rightarrow r = ۶$$

مسئله ۲: باقی‌مانده تقسیم عدد $A = ۵۹^{۱۳۹۱} \times ۷ - ۲۹۰$ را بر ۲۸ بیابید.

$$\begin{aligned} ۵۹ \equiv ۳ \rightarrow ۵۹^{۱۳۹۱} \equiv ۳^{۱۳۹۱}, ۳^۳ \equiv -۱, ۱۳۹۱ = ۳ \times ۴۶۳ + ۲ \rightarrow (۳^۳)^{۴۶۳} \times ۳^۲ \equiv (-۱)^{۴۶۳} \times ۳^۲ \rightarrow ۳^{۱۳۹۱} \equiv -۹ \\ \rightarrow ۳^{۱۳۹۱} \times ۷ \equiv -۹ \times ۷ = -۶۳ \equiv ۲۱ \rightarrow ۳^{۱۳۹۱} \times ۷ - ۲۹۰ \equiv ۲۱ - ۲۹۰ \equiv -۲۶۹ \equiv ۱۱ \rightarrow r = ۱۱ \end{aligned}$$

مسئله ۳: باقی‌مانده تقسیم عدد $A = ۵۳^{۲۰۱۳} \times ۴۸ - ۵۲^{۲۰۱۱} \times ۹$ را بر ۱۷ بیابید.

$$\begin{aligned} ۵۳ \equiv ۲, ۲^۲ \equiv -۱, ۲۰۱۳ = ۵۰۳ \times ۴ + ۱ \rightarrow (۲^۲)^{۵۰۳} \times ۲^۱ \equiv (-۱)^{۵۰۳} \times ۲ = -۲, ۴۸ \equiv ۱۴ \equiv -۳ \rightarrow ۲^{۲۰۱۳} \times ۴۸ \equiv (-۲) \times (-۳) = ۶ \\ ۵۲ \equiv ۱ \rightarrow ۵۲^{۲۰۱۱} \equiv ۱^{۲۰۱۱} \rightarrow ۵۲^{۲۰۱۱} \times ۹ \equiv ۱ \times ۹ = ۹ \rightarrow A \equiv ۶ - ۹ = -۳ \equiv ۱۴ \rightarrow r = ۱۴ \end{aligned}$$

قضیه‌های مهم و کاربردی

قضیهٔ اویلر: اگر a عددی صحیح و $(a, m) = ۱, m \in \mathbb{N}$ در این صورت $a^{\varphi(m)} \equiv ۱$

یادآوری: $\varphi(m)$ همان تعداد اعداد طبیعی و کوچک‌تر یا مساوی m است که نسبت به m اول اند و اگر $m = p_1^{k_1} \times p_2^{k_2} \times \dots \times p_n^{k_n}$

تجزیه‌ای استاندارد برای m باشد، در این صورت $\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$.

مسئله ۴: باقی‌مانده تقسیم عدد $A = ۱۷^{۱۲۰۲} \times ۹$ را بر ۳۶ بیابید.

قضیهٔ فرما: اگر p عددی اول باشد و $(a, p) = ۱, a \in \mathbb{Z}$ در این صورت، $a^{p-1} \equiv ۱$.

(اگر در قضیهٔ اویلر به جای m عدد p قرار دهیم با توجه به این که اگر p اول باشد $\varphi(p) = p - ۱$ حکم به دست می‌آید)

نتیجهٔ قضیهٔ فرما: اگر p عددی اول باشد و $a \in \mathbb{Z}$ در این صورت $a^p \equiv a$

مسئله ۵: باقی‌مانده تقسیم عدد $A = ۱۷^{۲۰۰۱} - ۱۹^{۲۰۰۲}$ را بر ۱۰۱ بیابید.

$$۱۷^{۲۰۰۱} \equiv ۱, ۱۹^{۲۰۰۲} \equiv ۱ \rightarrow (۱۷^{۲۰۰})^{۱۰} \times ۱۷ \equiv ۱^{۱۰} \times ۱۷ = ۱۷$$

$$(۱۹^{۲۰۰})^{۱۰} \times ۱۹^۲ \equiv ۱^{۱۰} \times ۱۹^۲, ۱۹^۲ = ۳۶۱ \equiv ۵۸ \rightarrow A \equiv ۱۷ - ۵۸ = -۴۱ \equiv ۶۰ \rightarrow r = ۶۰$$

مسئله ۶: باقی‌مانده تقسیم عدد $A = \sum_{k=1}^{۶۶} k^{۱۶} + \sum_{k=1}^{۳۹} k^{۱۷}$ را بر ۱۷ بیابید.

$$\sum_{k=1}^{۶۶} k^{۱۶} = ۱^{۱۶} + ۲^{۱۶} + \dots + ۱۷^{۱۶} + \dots + ۳۴^{۱۶} + \dots + ۵۱^{۱۶} + \dots + ۶۶^{۱۶}$$

(چون ۱۷ اول است، هر عددی که مضرب ۱۷ نباشد نسبت به ۱۷ اول است.)

$$\sum_{k=1}^{۶۶} k^{۱۶} \equiv \underbrace{۱+۱+\dots+۱}_{۱۶} + \underbrace{۰+۰+\dots+۰}_{۱۶} + \underbrace{۰+۰+\dots+۰}_{۱۶} + \underbrace{۰+۰+\dots+۰}_{۱۵} \equiv -۱ - ۱ - ۱ - ۲ = -۵$$

$$\sum_{k=1}^{۳۹} k^{۱۷} = ۱^{۱۷} + ۲^{۱۷} + \dots + ۳۹^{۱۷} \equiv ۱ + ۲ + \dots + ۳۹ = \frac{۳۹ \times ۴۰}{۲} = ۳۹ \times ۲۰ \equiv ۵ \times ۳ = ۱۵ (۳۹ \equiv ۵, ۲۰ \equiv ۳)$$

$$\rightarrow A \equiv -۵ + ۱۵ = ۱۰ \rightarrow r = ۱۰$$

مسئله ۷: اگر a, b و c مضرب γ نباشند باقی مانده تقسیم عدد $A = a^{1392} + 2b^{1392} - 2c^{1392}$ را بر γ بیابید.
 و به همین ترتیب $b^{1392} \equiv 1$ و $c^{1392} \equiv 1$ ؛ بنابراین:

$$A \equiv 1 + 2 \times 1 - 4 \times 1 = -1 \equiv 6 \rightarrow r = 6$$

قضیه ویلسون: اگر p عددی اول باشد، در این صورت، $(p-1)! \equiv (-1) \pmod{p}$.

مسئله ۸: باقی مانده تقسیم عدد $A = 18! \times 90$ را بر 19 بیابید.
 قوانین یافتن باقی مانده تقسیم اعداد طبیعی بر $2, 3, 4, 5, \dots$

$$19 \equiv 1 \rightarrow 18! \equiv (-1) \pmod{19} \rightarrow 18! \times 90 \equiv (-1) \times 14 = -14 \equiv 5 \pmod{19} \rightarrow r = 5$$

اگر $A = a_{n-1}a_{n-2}\dots a_2a_1a_0$ عددی n رقمی و بسط عدد A در مبنای 10 به شکل زیر مفروض باشد، داریم:

$$A = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \dots + 10^2a_2 + 10a_1 + a_0$$

(I) بخش پذیری و باقی مانده تقسیم بر 3 و 9

$$10^k \equiv 1 \pmod{9} \rightarrow A \equiv 1 \times a_{n-1} + 1 \times a_{n-2} + \dots + 1 \times a_2 + 1 \times a_1 + a_0 \rightarrow A \equiv (a_{n-1} + a_{n-2} + \dots + a_2 + a_1 + a_0) \pmod{9}$$

یعنی باقی مانده تقسیم هر عدد طبیعی مانند A بر 3 و 9 با باقی مانده تقسیم مجموع ارقامش بر 3 و 9 برابر است.

(II) بخش پذیری بر $4, 8, 16, \dots$ و 2^k

$$10^k \equiv 0 \pmod{2^k} \rightarrow A \equiv a_0 \pmod{2^k}$$

به همین ترتیب ثابت می شود که باقی مانده تقسیم عدد A بر 2^k با باقی مانده تقسیم k رقم سمت راست A بر 2^k برابر است، یعنی:

$$A \equiv (a_{k-1}a_{k-2}\dots a_2a_1a_0) \pmod{2^k}$$

(III) بخش پذیری بر 11

$$10^k \equiv (-1)^k \pmod{11} \rightarrow A \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^{n-1}a_{n-1} \pmod{11}$$

تمرین: باقی مانده تقسیم عدد $A = 9498324256$ را بر 11 بیابید.

$$10^k \equiv (-1)^k \pmod{11} \rightarrow A \equiv 9 - 4 + 9 - 8 + 3 - 2 + 4 - 2 + 5 - 6 = 1 \pmod{11}$$

(IV) بخش پذیری بر 10 و یافتن رقم یکان اعداد توان دار
 یعنی باقی مانده تقسیم هر عدد بر 10 برابر است با رقم یکانش).
قضیه: شرط لازم و کافی برای $A \equiv B \pmod{m}$ آن است که رقم یکان A و B برابر باشد.
 ۳. اگر دو عدد $(2a+3)$ و $(2a+4)$ رقم یکان برابر داشته باشند، رقم یکان عدد $(2a+2)$ کدام است؟

(۱)	(۲)	(۳)	(۴)
۱	۲	۳	۴

حل: گزینه (۱)؛ زیرا طبق قضیه قبل، این دو عدد به پیمانه 10 با یکدیگر هم نهشت اند و داریم:
 رقم یکان $a, 7$ است $a \equiv 7 \rightarrow -3 \equiv 7 \rightarrow a \equiv -3, -3 \equiv 7 \rightarrow a \equiv -3$

$$a \equiv 7 \rightarrow 2a + 2 \equiv 2 \times 7 + 2 = 16 \equiv 6 \pmod{10}$$

(پس رقم یکان عدد $2a+2$ همان 6 است).

رقم یکان اعداد توان دار به صورت A^n

(I) اگر عدد A به ۰ یا ۱ یا ۵ یا ۶ ختم شود، در این صورت A^n نیز متناظراً به صفر یا ۱ یا ۵ یا ۶ ختم می‌شود.

(II) اگر عدد A به ۴ ختم شود، در این صورت برای هر n زوج عدد A^n به ۶ و برای هر n فرد به ۴ ختم می‌شود.

(III) اگر عدد A به ۹ ختم شود، آن‌گاه برای هر n زوج عدد A^n به ۱ و برای هر n فرد به ۹ ختم می‌شود.

(IV) برای یافتن رقم یکان اعدادی به صورت A^n که در آن‌ها عدد A به ۲ یا ۳ یا ۷ یا ۸ ختم می‌شود از قضیه زیر استفاده می‌کنیم:

قضیه: رقم یکان توان‌های متوالی اعداد طبیعی هر ۴ بار یک مرتبه تکرار می‌شود، یعنی: $A^n \equiv A^{n+4}$ ($n \in \mathbb{N}$)

با توجه به قضیه قبل برای یافتن رقم یکان عدد A^n کافی است n را بر ۴ تقسیم کنیم. اگر $n = 4k + r$ و $r \neq 0$ در این صورت $A^n = A^{4k+r} \equiv A^r \equiv a^r$ (رقم یکان A است).
 اگر $n = 4k$ (است) و $r = 0$ در این صورت $A^n = A^{4k} \equiv a^4$ (رقم یکان A است).

مثال: مطلوب است رقم یکان عدد $1392^{1393} \times 7$.

$$1393 = 4 \times (348) + 1 \rightarrow 1392^{1393} \equiv 2^1 \rightarrow 1392^{1393} \times 7 \equiv 2 \times 7 = 14 \equiv 4 \rightarrow \text{رقم یکان} = 4$$

مثال: مطلوب است رقم یکان عدد $A = 499^{1342} \times 6 + 853^{1392} \times 8$.

$$1342 = 2k \rightarrow 499^{1342} \equiv 1 \rightarrow 499^{1342} \times 6 \equiv 6$$

$$1392 = 4 \times 348 \rightarrow 853^{1392} \equiv 3^4 \equiv 81 \equiv 1 \rightarrow 853^{1392} \times 8 \equiv 1 \times 8 = 8 \rightarrow A \equiv 6 + 8 = 14 \equiv 4$$

مثال: رقم یکان اعداد زیر را بیابید:

$$D) A = 216^{612} - 519^{915} \times 7 + 1393^{3931} \times 4 - 594^{7^9} \times 3$$

$$II) B = \sum_{k=1}^{1392} k!$$

$$III) C = [1 + 3^{1392} + 9^{1392} + 27^{1392}]^{1392}$$

$$IV) D = 453^{2 \cdot 13 + 3} + 599^{10!} \times 4 - 807^{807! + 20!}$$

حل:

$$D) 216^{612} \equiv 6 \text{ و } 915 \text{ فرد است} \Rightarrow 519^{915} \equiv 9 \Rightarrow 519^{915} \times 7 \equiv 9 \times 7 = 63 \equiv 3$$

$$\Rightarrow 519^{915} \times 7 \equiv 3, 3931 = 4k + 3$$

$$\Rightarrow 1393^{3931} \equiv 3^3 \equiv 27 \equiv 7 \Rightarrow 1393^{3931} \times 4 \equiv 7 \times 4 \equiv 8$$

$$7^9 = 2k + 1 \text{ (فرد است)} \Rightarrow 594^{7^9} \equiv 4 \Rightarrow 594^{7^9} \times 3 \equiv 4 \times 3 \equiv 2$$

$$\Rightarrow A \equiv 6 - 3 + 8 - 2 = 9 \Rightarrow \text{رقم یکان } A, 9 \text{ است}$$

$$II) B = \sum_{k=1}^{1392} k! = 1! + 2! + 3! + 4! + 5! + \dots + 1392!$$

$$\Rightarrow B \equiv 1 + 2 + 6 + 4 + 0 + \dots + 0 = 13 \equiv 3 \rightarrow B \text{ رقم یکان } 3$$

(توجه دارید که $4! = 24$ و $24 \equiv 4$ و $4! = 24$ برای هر $n \geq 5$ همواره $n! \equiv 0$ است).

$$III) 2^{1392} = 2^{4k} \equiv 2^4 \equiv 6 \Rightarrow C \equiv [1 + 1 + 1 + 6]^{1392} \equiv 9^{1392} \equiv 1$$

$$IV) n! \equiv 0 \text{ (برای هر } n \geq 4 \text{ و } k! = 2n \text{ (برای هر } n \geq 2 \text{))}$$

$$\Rightarrow 453^{2 \cdot 13 + 3} = 453^{4k+3} \equiv 3^3 \equiv 27 \equiv 7, 599^{10!} = 599^{2n} \equiv 1 \text{ (زوج است)}$$

$$\Rightarrow 599^{10!} \times 4 \equiv 4, 807^{807! + 20!} = 807^{4k}, 20! = 4k'$$

$$\Rightarrow 807^{807! + 20!} = 807^{4m} \equiv 7^4 \equiv 1$$

$$\Rightarrow D \equiv 7 + 4 - 1 = 10 \equiv 0 \rightarrow \text{رقم یکان}$$