Congruențe

Fie $x, y, n \in \mathbb{Z}$, $n \notin \{0, 1\}$

$$x \equiv y \pmod{n} \iff n \mid x - y$$

Notație: $x \overset{n}{\equiv} y$

Operații:

$$\left.\begin{aligned} x_1 &\equiv y_1 \pmod{n} \\ x_2 &\equiv y_2 \pmod{n} \end{aligned}\right| \Rightarrow x_1 + x_2 \overset{n}{\equiv} y_1 + y_2$$

$$x_1 \cdot x_2 \overset{n}{\equiv} y_1 \cdot y_2$$

$$x_1^m \equiv y_1^m \pmod{n}$$

$$\left.\begin{aligned} ax &\equiv ay \pmod{n} \\ (a, n) &= 1 \end{aligned}\right| \Rightarrow x \equiv y \pmod{n}$$

$$ax \equiv ay \pmod{n} \Rightarrow x \equiv y \left(\mod \frac{n}{(a, n)}\right)$$

Inversul modulo n

Fie $x \in \mathbb{Z}$. $y \in \mathbb{Z}$ s.n. invers pt. x mod n dacă $x \cdot y \equiv 1 \pmod{n}$

Exemplu:

$5 \cdot 3 \equiv 1 \pmod 7$, deci 3 e inversul lui 5 mod 7.

Condiție necesară și suficientă de existență a inversului mod n.

$x \cdot y \equiv 1 \pmod n \Rightarrow$

$\Rightarrow n \mid x \cdot y - 1 \Rightarrow \underline{(n, x) = 1}$

Arătăm că $(n, x) = 1 \Rightarrow x$ e inversabil modulo n

Algoritmul lui Euclid pt. determinarea c.m.m.d.c:

$a, b \in \mathbb{Z} \setminus \{0\}$

$a = b \cdot c_1 + r_1 \qquad 0 < r_1 < b$

$b = r_1 \cdot c_2 + r_2 \qquad 0 < r_2 < r_1$

$\vdots \qquad\qquad \vdots$

$r_n = r_{n+1} \cdot c_{n+2} + r_{n+2}$

$r_{n+1} = r_{n+2} \cdot c_{n+3}$

Le va ajunge la un rest egal cu 0, pt. că

$b > r_1 > r_2 > \dots$

$r_{n+2} = d = \text{cmmdc}(a, b)$

Dem: $d = r_{n+2} \mid r_{n+1}$

$r_n = r_{n+1} \cdot c_{n+2} + r_{n+2}$ $\Big| \Rightarrow$

$\Rightarrow d \mid r_n$

$d \mid r_{n+1}$ $\Big| \Rightarrow d \mid r_{n-1}$

$d \mid r_n$

În final, $d \mid a$ și $d \mid b$

$$r_{n+2} = r_n - r_{n+1} \cdot c_{n+2}$$

$$= r_n - \left(r_{n-1} - r_n \cdot c_{n+1} \right) \cdot c_{n+2}$$

$$= \underline{r_n} \cdot \left(1 + c_{n+1} \cdot c_{n+2} \right) - \underline{r_{n-1}} \cdot c_{n+2}$$

Continuând tot așa

$$r_{n+2} = r_{n-1} \cdot \underbrace{(\dots)}_{\in \mathbb{Z}} + r_{n-2} \cdot \underbrace{(\dots)}_{\in \mathbb{Z}}$$

În final, $d = a \cdot \alpha + b \cdot \beta$,

$\alpha, \beta \in \mathbb{Z}$

Rezultă că, dacă $\left.\begin{matrix} m \mid a \\ m \mid b \end{matrix}\right| \Rightarrow m \mid d$

$d = \text{cmmdc}(a, b)$

Revenind la a demonstra suficienta

$(x, \gamma) = 1 \Rightarrow 1 = \gamma \cdot \alpha + x \cdot \beta \Rightarrow$

$\Rightarrow \gamma \cdot \alpha \equiv 1 \pmod{x}$

Exemplu:

$(16, 9) = 1$

Calculați inversul lui 9 mod 16

Clase de resturi și operații

Altă metodă de calcul pt. invers.

T Mica teoremă a lui Fermat:

Dacă p e prim, $(a, p) = 1$

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

Dem: $1, a, a^2, \dots a^{p-1}$ dau resturi posibile

$1, 2, \dots (p-1)$ la împărțirea prin p

$(\exists)\ a^i, a^j$ a.î. $a^i \equiv a^j \pmod p$
$i<j$ (i.e. $\hat a^i = \hat a^j$)
$i,j \in \{1,2,\dots p-1\}$

$(a,p)=1 \Rightarrow a^{j-i} \equiv 1 \pmod p$
$\hat a^{j-i} = 1$

Deci $(\exists)\ o \in \{1,2\dots p-1\}$ a.î.
$a^o \equiv 1 \pmod p$

Considerăm o minim cu această proprietate

[o s.n. ordinul lui a modulo p]

Notăm
$\langle \hat a \rangle = \{\hat 1, \hat a, \hat a^2, \dots \hat a^{o-1}\}$

$\hat a^o = 1$
$\hat a^{-1} = \widehat{a^{o-1}} = \hat a^{o-1}$
$\hat a^{-k} = \widehat{a^{o-k}} = \hat a^{o-k}$

Fie $\hat r \in \{\hat 1, \hat 2, \dots \hat{p-1}\} = \mathbb{Z}_p \setminus \{\hat 0\}$

Vom demonstra că, dacă $\hat r \notin \langle a \rangle$
atunci $\widehat{r \cdot a^i} \in \langle \hat a \rangle$

Dacă $\hat r \cdot \hat a^i = \hat a^j \Rightarrow \hat r = \hat a^{j-i}$

Contradicție cu $\hat{r} \notin \langle \hat{a} \rangle$

Notăm $r \cdot \langle \hat{a} \rangle = \{ \hat{r}, \widehat{r \cdot a}, \widehat{r \cdot a^2}, \ldots, \widehat{r \cdot a^{n-1}} \}$

Am arătat $(r \cdot \langle \hat{a} \rangle) \cap \langle \hat{a} \rangle = \emptyset$.

Dacă $\hat{r}_2 \notin r_1 \cdot \langle \hat{a} \rangle$, atunci

$$(\hat{r}_2 \cdot \langle \hat{a} \rangle) \cap (\hat{r}_1 \cdot \langle \hat{a} \rangle) = \emptyset$$

Dacă $\hat{r}_2 \cdot \hat{a}^i = \hat{r}_1 \cdot \hat{a}^j \Rightarrow$

$r_2 = \hat{r}_1 \cdot \hat{a}^{j-i}$ Fals!

Vom scrie acum $\mathbb{Z}_p \setminus \{\hat{0}\}$ ca o reuniune de mulțimi disjuncte de forma

$r \cdot \langle \hat{a} \rangle$.

$A_1 = \langle \hat{a} \rangle$

Dacă $A_1 = \mathbb{Z}_p^*$, gata

Dacă nu, fie $\hat{r}_1 \notin \langle \hat{a} \rangle$

$A_2 = \hat{r}_1 \cdot \langle a \rangle \quad A_2 \cap A_1 = \emptyset$

Dacă $A_1 \cup A_2 = \mathbb{Z}_p^*$ Gata

Altfel fie $\hat{r}_1 \in \mathbb{Z}_p^* \setminus (A_1 \cup A_2)$

$A_3 = \hat{r}_2 \cdot \langle \hat{a} \rangle$ ş.a.m.d.

Fiecare A_i are exact o element $\Rightarrow$

$\Rightarrow o \mid p-1$

$\hat{a}^o = 1 \Rightarrow \hat{a}^{p-1} = 1^{p-1} = 1$

□

Altă demonstrație:

$$\mathbb{Z}_p^* = \{\hat{1}, \hat{2}, \dots, \widehat{p-1}\}$$

$$a \cdot \mathbb{Z}_p^* = \{a \cdot \hat{1}, a \cdot \hat{2}, \dots a \cdot \widehat{p-1}\}$$

Arătăm că $a \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$

I $a \cdot \mathbb{Z}_p^* \subseteq \mathbb{Z}_p^*$ clar, căci $(a, p) = 1$

II Fie $a \cdot \hat{i} = a \cdot \hat{j} \Big/ \Rightarrow \hat{i} = \hat{j}$

$(a, p) = 1$

Deci $a \cdot \hat{1}, a \cdot \hat{2}, \dots, a \cdot \widehat{p-1}$ sunt distincte două câte două. $\square$

$a \cdot U_p^* = U_p^*$, deci

$$\hat{1} \cdot \hat{2} \cdot \ldots \cdot \widehat{(p-1)} = \hat{a}^{p-1} \cdot \hat{1} \cdot \hat{2} \cdot \ldots \widehat{(p-1)}$$

$$\widehat{(p-1)!} = \hat{a}^{p-1} \cdot \widehat{(p-1)!} \quad \Big/ \Rightarrow$$

$$\big((p-1)!, p\big) = 1 \quad \Big/$$

$$\Rightarrow \hat{a}^{p-1} = \hat{1}.$$

În cazul în care n nu e prim, definim

$$U(\mathbb{Z}_n) = \{ \hat{x} \in \mathbb{Z}_n \mid (x, n) = 1 \}$$ elementele inversabile din $\mathbb{Z}_n$

Dacă $\hat{x}_1, \hat{x}_2 \in U(\mathbb{Z}_n)$,

$$\hat{x}_1^{-1} \in U(\mathbb{Z}_n)$$

$$\hat{x}_1 \cdot \hat{x}_2 \in U(\mathbb{Z}_n)$$

Notăm $\varphi(n) = \text{card}\left(U(\mathbb{Z}_n)\right)$

Înlocuind $\mathbb{Z}_p^*$ cu $U(\mathbb{Z}_n)$ în

oricare dintre demonstrațiile anterioare,

obținem

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

(Teorema lui Euler)

Observații: • $\hat{a}^{-1} = \hat{a}^{p-2}$, $(\forall)\ a \in \mathbb{Z}_p^*$

• $\hat{a}^{-1} = \hat{a}^{\varphi(n)-1}$, $(\forall)\ a \in U(\mathbb{Z}_n)$

Câteva proprietăți ale lui φ

- $\sum_{d \mid n} \varphi(d) = n$

Dem: Exemplu pt. $n = 12$

$\varphi(12)$ $\frac{1}{12}$ $\frac{2}{12}$ $\frac{3}{12}$ $\frac{4}{12}$ $\frac{5}{12}$ $\frac{6}{12}$ $\frac{7}{12}$ $\frac{8}{12}$ $\frac{9}{12}$ $\frac{10}{12}$ $\frac{11}{12}$ $\frac{12}{12}$

$\varphi(6)$ $\frac{1}{6}$ $\frac{5}{6}$

$\varphi(4)$ $\frac{1}{4}$ $\frac{3}{4}$

$\varphi(3)$ $\frac{1}{3}$ $\frac{2}{3}$

$\varphi(2)$ $\frac{1}{2}$

$\varphi(1)$ $\frac{1}{1}$

$(m, n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Inducție după $m \cdot n$.

Pt. $m \cdot n = 1$ clar $(\varphi(1) = 1)$

Pp. că $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

$(\forall)\ a, b \in \mathbb{N}^*$ cu $(a, b) = 1$ și $a \cdot b < mn$

$$m \cdot n = \sum_{d \mid m \cdot n} \varphi(d)$$

Dacă $d = m \cdot n$ și $(m, n) = 1$ atunci

$(\exists)!\ d_1, d_2$ a.î. $d_1 \mid m$

$d_2 \mid n$

$d = d_1 \cdot d_2$

$(m, n) = 1 \Rightarrow (d_1, d_2) = 1$

$$m \cdot n = \varphi(m \cdot n) + \sum_{\substack{d_1 \mid m \\ d_1 \neq m}} \varphi(d_1 \cdot n) +$$

$$+ \sum_{\substack{d_2 \mid n \\ d_2 \neq n}} \varphi(m \cdot d_2) + \sum_{\substack{d_1 \mid m \\ d_2 \mid n \\ d_1 \neq m \\ d_2 \neq n}} \varphi(d_1 \cdot d_2)$$

$$= \varphi(m \cdot n) + \varphi(n) \cdot \sum_{\substack{d_1 \mid m \\ d_1 \neq n}} \varphi(d_1) +$$

$$+ \varphi(m) \cdot \sum_{\substack{d_2 \mid n \\ d_2 \neq n}} \varphi(d_2) + \left(\sum_{\substack{d_1 \mid m \\ d_1 \neq m}} \varphi(d_1) \right) \cdot \left(\sum_{\substack{d_2 \mid n \\ d_2 \neq n}} \varphi(d_2) \right)$$

$$mn = \varphi(mn) + \varphi(n)\cdot(m-\varphi(m)) +$$

$$+ \varphi(m)\cdot(n-\varphi(n)) +$$

$$+ (m-\varphi(m))\cdot(n-\varphi(n))$$

Desfăcând parantezele,

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

- p prim, $k \in \mathbb{N}^*$

$$\varphi(p^k) = p^k - p^{k-1} = p^k\cdot\left(1-\frac{1}{p}\right)$$

Dem: Numerele care NU sunt prime cu p^k, mai mici sau egale cu p^k sunt:

$$p,\ 2\cdot p,\ \ldots,\ p^{k-1}\cdot p,$$

adică p^{k-1} numere.

- Dacă $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_n^{k_n}$,

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \dots \cdot \varphi(p_n^{k_n})$$

$$= p_1^{k_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdots p_n^{k_n} \left(1 - \frac{1}{p_n}\right)$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

(1) Fie $a \in \mathbb{N}^*$ prim cu 10.
Arătați că a^{41} are ultimele două cifre egale cu cele ale lui a.

Lol:

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$$= 40$$

$$a^{40} \equiv 1 \pmod{100} \Rightarrow a^{41} \equiv a \pmod{100}$$

② Fie n nr. impar

Arătați că $n \mid 2^{n!}-1$

$(n,2)=1$ $\quad n \mid 2^{\varphi(n)}-1 \Rightarrow 2^{\varphi(n)} \equiv 1 \pmod n$

$\varphi(n) \leq n \Rightarrow \varphi(n) \mid n!$ $\Rightarrow$

$\Rightarrow 2^{n!} \equiv 1 \pmod n$

③ Să se arate că

$1982 \mid \underbrace{222\ldots2}_{1980 \text{ cifre}}$

Lol: $1982 = 2 \cdot 991$ ← prim

Clar $2 \mid 222\ldots2$

$$\underbrace{111\ldots1}_{1980\text{ de }1} = \frac{\overbrace{99\ldots9}^{1980\text{ de }9}}{9}$$

$$= \frac{10^{1980} - 1}{9}$$

$$= \frac{(10^{990} - 1)(10^{990} + 1)}{9}$$

Mica T. Fermat:

$$991 \mid 10^{990} - 1 \Rightarrow$$

$$\Rightarrow 991 \mid \underbrace{111\ldots1}_{\text{de } 1980 \text{ de } 1}$$

④ Orice nr. n prim cu 10 admite un multiplu scris doar cu cifre de 1

Lol:

$(n, 10) = 1 \Rightarrow n \mid 10^{\varphi(n)} - 1$

$n \mid \underbrace{99\ldots9}_{\varphi(n) \text{ ori}}$

Nu e suficient

Observăm că $(9n, 10) = 1$,

deci $(9n) \mid 10^{\varphi(9n)} - 1 \Rightarrow$

$\Rightarrow (9n) \mid \underbrace{99\ldots9}_{\varphi(9n) \text{ ori}}$

$n \mid \underbrace{11\ldots1}_{\varphi(9n) \text{ ori}}$

(5) Să se det. restul împărțirii numărului

$N = 4444^{4444^{4444}}$ prin 13.

(Viitori Olimpici. ro)

Sol:

Din Mica T. Fermat, $13 \nmid 4444$

$$4444^{12} \equiv 1 \mod (13)$$

Dorim să determinăm restul împărțirii lui 4444^{4444} la 12

$$4444 = 12 \cdot 370 + 4$$

$$M = 4444^{4444} \equiv 4^{4444} \pmod{12}$$

$$P = 4^{4444} \equiv 1^{4444} \pmod 3$$

$$1^{11} = 1$$

Deci $p \equiv 1 \pmod 3$

$p \equiv 0 \pmod 4$

$p = 4k$

$3 \mid 4k - 1 \Rightarrow 3 \mid 4k - 4 \Rightarrow$

$\Rightarrow 12 \mid 4k - 4 \Rightarrow$

$\Rightarrow p \equiv 4 \pmod{12}$

Deci $n = 12l + 4$

$N = 4444^{12l+4} = (4444^{12})^{l} \cdot 4444^{4} \equiv$

$\equiv 4444^{4} \pmod{13} \equiv (-2)^{4} \pmod{13}$

$4444 = 13 \cdot 342 - 2$

$(-2)^{4} = 16 \equiv 3 \pmod{13}$

Răspuns: 3

Am fost puși mai sus în situația de a rezolva sistemul de congruențe:

$$x \equiv 1 \pmod 3$$

$$x \equiv 0 \pmod 4$$

O putem face sistematic / algoritmic pe caz general.

Teorema chineză a resturilor

Fie $m_1, m_2 \dots m_n \in \mathbb{N}^* \setminus \{1\}$ prime între ele două câte două.

Fie $a_1, a_2 \dots a_n \in \mathbb{Z}$

Atunci sistemul:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

are în $\{0, 1, \dots, m_1 m_2 \dots m_n - 1\}$ soluție unică

Dem:

Existența:

Căutăm pt. orice $i = \overline{1,n}$ $y_i \in \mathbb{Z}$ a.î.

$$y_i \equiv 1 \pmod{m_i}$$

$$y_i \equiv 0 \pmod{m_j}, \ (\forall)\ j \neq i$$

Adică, dacă notăm $M_i = \frac{m_1 m_2 \dots m_n}{m_i}$,

atunci $y_i = M_i \cdot k_i$ și vrem să alegem $k_i \in \mathbb{Z}$ a.î.

$$M_i \cdot k_i \equiv 1 \pmod{m_i}$$

$(M_i, m_i) = 1$, deci alegem k_i inversul lui M_i modulo m_i.

Deci $y_i = M_i \cdot M_i^{-1 \pmod{m_i}}$

Acum notăm

$z = a_1 \cdot y_1 + a_2 \cdot y_2 + \dots + a_n \cdot y_n$

z e soluție a sistemului de congruențe.

La fel și x = restul împărțirii lui z la $m_1 \cdot m_2 \cdot \dots \cdot m_n$ e soluție a sistemului în $\{0, 1, \dots m_1 \cdot m_2 \cdot \dots \cdot m_n - 1\}$

Unicitatea:

Fie x_1, x_2 soluții în $\mathbb{Z}$ ale sistemului.

Rezultă că $m_1 \mid x_1 - x_2$

$m_2 \mid x_1 - x_2$

$\vdots$

$m_n \mid x_1 - x_2$

Deci $m_1 \cdot m_2 \cdot \dots \cdot m_n \mid x_1 - x_2$

Rezultă că nu pot fi două astfel de soluții diferite în $\{0, 1, \dots, n_1 n_2 \dots n_m - 1\}$.

Mai mult, dacă x este o soluție, mulțimea soluțiilor este

$$S = \{ x + \alpha \cdot n_1 \cdot n_2 \cdot \dots \cdot n_m \mid \alpha \in \mathbb{Z} \}$$

Exemplu: $x \in \mathbb{Z}$

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

$$x \equiv ? \pmod{30}$$

⑥ Arătați că

$n^{12} - 5n^6$ dă rest constant la împărțirea prin 252, independent de valoarea lui $n \geq 2$ a.î. $(n, 252) = 1$

$$A = n^{12} - 5n^6 = n^6(n^6 - 5)$$

$$252 = 4 \cdot 9 \cdot 7$$

Dacă n par $\Rightarrow 4 \mid n^6$

n impar $\Rightarrow n^6 \equiv 1 \pmod 4$ ← pătrat perfect $\Rightarrow$

$\Rightarrow 4 \mid n^6(n^6 - 5)$

Deci $4 \mid A$

$(3, n) = 1 \Rightarrow (9, n) = 1$

T. Euler $\Rightarrow 9 \mid n^{\varphi(9)} - 1 = n^6 - 1$

$$n^6 \equiv 1 \pmod 9$$

$\Rightarrow$

$(7, n) = 1 \Rightarrow (7, n) = 1$

$$n^6 \equiv 1 \pmod 7$$

$\Rightarrow$ Din Teorema chineză a resturilor,

$$n^6 \equiv 1 \pmod{9 \cdot 7},$$

deci $n^6(n^6 - 5) \equiv -4 \pmod{9 \cdot 7}$

$$n^6(n^6 - 5) \equiv 0 \pmod 4$$

Din Teorema chineză a resturilor,

$$A = n^6(n^6 - 5) \equiv -4 \pmod{252}$$

(Din Teorema chineză am folosit practic doar partea de unicitate)

Teorema lui Wilson

Un nr. $n \in \mathbb{N}^* \setminus \{1\}$ este prim dacă și numai dacă

$$n \mid (n-1)! + 1$$

$\Rightarrow$ "

Dem: "Dacă $n \mid (n-1)! + 1$

Presupunem căci n nu e prim

$n = a \cdot b$, cu $1 < a, b \leq (n-1)$

Deci $a \mid n \mid (n-1)! + 1$ și

$a \mid (n-1)!$

Obținem $a \mid 1$ Fals!

$\Leftarrow$ " Dacă p e prim, lucrăm în $\mathbb{Z}_p$

Dacă $p = 2$, clar. Presupunem $p \geq 3$

Elementele

$\hat{1}, \hat{2}, \ldots \widehat{p-1}$ sunt inversabile în $\mathbb{Z}_p$

Le grupăm în perechi de forma

$\left(\hat{x}, \hat{x}^{-1}\right)$

Produsul unei astfel de grupe este $\hat{1}$.

Singura problemă este când

$\hat{x} = \hat{x}^{-1}$, adică atunci când

$\hat{x}^2 = \hat{1}$

Căutăm acele elemente $\hat{x} \in \mathbb{Z}_p^*$ a.î.

$$\hat{x}^2 = \hat{1}$$

$$p \mid x^2 - 1 = (x-1)(x+1) \Rightarrow$$

$$\Rightarrow \begin{cases} p \mid x-1 \\ \text{sau} \\ p \mid x+1 \end{cases}$$

Adică $\hat{x} = \hat{1}$ sau $\hat{x} = -\hat{1}$

Restul elementelor pot fi grupate în perechi de produs $\hat{1}$.

Rezultă că

$$\widehat{(p-1)!} = \hat{1} \cdot \hat{2} \cdot \ldots \cdot \widehat{(p-1)}$$

$$= \hat{1} \cdot \widehat{-1} \cdot \left(\hat{x}_1 \cdot \hat{x}_1^{-1}\right) \cdot \ldots$$

$$\ldots \cdot \left(\hat{x}_{\frac{p-3}{2}} \cdot \hat{x}_{\frac{p-3}{2}}^{-1}\right)$$

$$= -\hat{1}$$

□