Seminar 10

4 Dec 2024

$\mathbb{Z}_n = \{ \hat{a} \mid a \in \mathbb{Z} \}$
$= \{ \hat{0}, \hat{1}, \dots, \widehat{n-1} \}$

$\hat{k} = \{ m \in \mathbb{Z} \mid m = n \cdot q + k \} \quad \forall\, k = \overline{0, n-1}$

$\hat{k} + \hat{l} \overset{def}{=} \widehat{k+l}$

$\hat{k} \cdot \hat{l} \overset{def}{=} \widehat{k \cdot l}$

$(\mathbb{Z}_n, +)$
↳ grup abelian
(el. neutru este $\hat{0}$
inversul lui $\hat{k}$ este $-\hat{k}$)
$= \widehat{n-k}$

$(\mathbb{Z}_n, \cdot)$
↳ monoid comutativ

$U(\mathbb{Z}_n, \cdot) = \{ \hat{k} \mid \hat{k}$ e inversabil în raport cu "$\cdot$" $\}$

$\overset{dem}{=} \{ \hat{k} \mid 0 \le k \le n-1$ și $(k, n) = 1 \}$

$|U(\mathbb{Z}_n, \cdot)| = \varphi(n)$

ex 1

Fie $a, b \in \mathbb{Z}^*$. Calculați cmmdc (a, b)

<u>Sol</u>:

Algoritmul lui Euclid

$a = b \cdot q_1 + r_1$

$b = r_1 \cdot q_2 + r_2$

$\dots$ $\qquad\qquad r_{k+2} = (a, b)$

$r_k = r_{k+1} \cdot q_{k+2} + \boxed{r_{k+2}}^{\neq 0}$

$r_{k+1} = r_{k+2} \cdot q_{k+3}$

Dacă $d = (a, b) \Rightarrow (\exists)\ t, s \in \mathbb{Z}$ a. î.

$$d = a \cdot t + b \cdot s$$

Exc! $(a, b) = 1 \iff (\exists)\ t, s \in \mathbb{Z}$ a.î. $1 = a \cdot t + b \cdot s$

Temă

$\hat{1} = \hat{b} \cdot \hat{s}$ (modulo a)

$\hat{1} = \hat{a} \cdot \hat{t}$ (modulo b)

Exemplu

$\underline{2} \cdot (-1) + \underline{3} \cdot (1) = 1$

$\underline{2} \cdot (-4) + \underline{3} \cdot 4 = 4$

? T. Lagrange

$(G, \cdot)$ grup finit $(\ |G| = n\ )$

$(\forall)\ x \in G,\quad x^n = e$

î elementul neutru

Th. lui Euler

Lagrange $\Rightarrow$ $(\forall)\ \hat{n} \in U(\mathbb{Z}_n)$ $\qquad \hat{n}^{\varphi(n)} = 1$

$$\hat{n}^{\varphi(n)} \equiv 1 \pmod{n}$$

Alg. lui Euclid

Exc.

$$(137, 250) = 1$$

$\Leftrightarrow$ Calculați inversul lui 137 în $\mathbb{Z}_{250}$

$250 = 137 \cdot 1 + 113 \qquad \Rightarrow 113 = 250 \cdot 1 - 137 \cdot 1$

$137 = 113 \cdot 1 + 24 \qquad \Rightarrow 24 = 137 \cdot 1 - (250 \cdot 1 - 137 \cdot 1)$

$113 = 24 \cdot 4 + 17 \qquad = 137 \cdot 2 - 250 \cdot 1$

$24 = 17 \cdot 1 + 7 \qquad \Rightarrow 17 = 250 \cdot 1 - 137 \cdot 1 - 4(137 \cdot 2 - 250 \cdot 1)$

$17 = 7 \cdot 2 + 3 \qquad = 250 \cdot 5 - 137 \cdot 9$

$7 = 3 \cdot 2 + 1 \qquad \Rightarrow 7 = -250 \cdot 5 + 137 \cdot 9 + 137 \cdot 2 - 250 \cdot 1$

$3 = 1 \cdot 3 + 0 \qquad = 137 \cdot 11 - 250 \cdot 6$

$\Rightarrow 3 = 250 \cdot 5 - 137 \cdot 9 - 2 \cdot (137 \cdot 11 - 250 \cdot 6)$

$= 250 \cdot 17 - 137 \cdot 31$

$\Rightarrow 1 = 137 \cdot 11 - 250 \cdot 6 - 2 \cdot (250 \cdot 17 - 137 \cdot 31)$

$= 137 \cdot 73 - 250 \cdot 40$

$$1 = 137 \cdot 73 - 250 \cdot 40 = 137 \cdot 73 + 250 \cdot (-40)$$

$$\Downarrow$$

$$\overline{1} = \overline{137} \cdot \overline{73} \text{ în } \mathbb{Z}_{250}$$

$$\Rightarrow \overline{137}^{-1} \text{ în } U(\mathbb{Z}_{250}, \cdot) \text{ este } \overline{73}$$

$\square$

$$U(\mathbb{Z}_n, \cdot) = \{ \hat{k} \mid 0 \le k \le n-1, \ (k, n) = 1 \}$$

<u>Dem</u>

"$\supseteq$" $\quad (k, n) \overset{\text{Euclid}}{\Longrightarrow} 1 = k \cdot t + n \cdot s \Rightarrow$

$$\hat{1} = \hat{k} \cdot \hat{t} \text{ în } \mathbb{Z}_n$$

$$\Rightarrow \hat{k} \in U(\mathbb{Z}_n, \cdot)$$

"$\subseteq$" $\quad \hat{k} \in U(\mathbb{Z}_n) \overset{\text{def}}{\Longrightarrow} (\exists)\, \hat{\ell} \in \mathbb{Z}_n$ a.î. $\hat{k} \cdot \hat{\ell} = \hat{1}$

$$\widehat{k \cdot \ell} = \hat{1}$$

$$\hat{a} = \hat{t} \overset{\text{def}}{\underset{\text{rel. de echiv}}{\Longleftrightarrow}} n \mid a - t \Longleftrightarrow a \equiv t \pmod{n}$$

$$\Rightarrow k\ell \equiv 1 \pmod{n} \Rightarrow k\ell - n \cdot q = 1, \text{ pt } q \in \mathbb{Z}$$

Exc!

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

$\square$

$(\mathbb{Z}_n, +, \cdot) \to$ inelul claselor de resturi mod n

Ex

Aflați restul împărțirii lui $1024^{2000^{2001}}$ la 900. (17)

Sol:

$h \equiv l \pmod{n}$

$P(h) \equiv P(l) \pmod{n}$ pt orice P polinom

$\Leftrightarrow \quad \widehat{1024^{2000^{2001}}}$ în $\mathbb{Z}_{900}$

Reducerea bazei

$1024 \equiv 124 \pmod{900} \Rightarrow 1024^{2000^{2001}} \equiv \underline{124^{2000^{2001}} \pmod{900}}$

Reducerea exponentului

$900 = 2^2 \cdot 3^2 \cdot 5^2$ (L.C.R.)

$\varphi(900) = 900 \cdot \left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)$

$= 900 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{3} \cdot \frac{4}{5} = 2^4 \cdot 3 \cdot 5$

$= 240$

In loc de 1024 să zicem că avem un nr. prim

$23^{2000^{2001}}$

$23^{240} \equiv 1 \pmod{900}$

(LCR) $\Rightarrow$ Restul împ lui $124^{2000^{2001}}$ la 900 poate fi determinat din resturile împ lui $124^{2000^{2001}}$ la

la 2^2, 3^2 și 5^2

$\hookrightarrow$ (în mod unic)

$$124^{2000^{2001}} \equiv 0 \pmod{2^2} \quad (1) \qquad 124 = 2^2 \cdot 31$$

Vrem $124^{2000^{2001}} \pmod{3^2}$ și $124^{2000^{2001}} \pmod{5^2}$

$(124, 3^2) = 1$, $(124, 5^2) = 1$

$\hookrightarrow$ Euler ! doar dacă $(a, b) = 1$

$$124^{\varphi(3^2)} \equiv 1 \pmod{3^2} \qquad \varphi(3^2) = 9 \cdot \frac{2}{3} = 6$$

$$2000^{2001} \pmod{\varphi(3^2)} \Leftarrow$$

$$2000^{2001} \pmod 6 \equiv 2^{2001} \pmod 6 \equiv \underline{2 \pmod 6}$$

$$\left\{ \begin{array}{l} x = 2^{2001} \equiv 0 \pmod 2 \\ x = 2^{2001} \equiv (-1)^{2001} \pmod 3 \equiv 2 \pmod 3 \end{array} \right] \overset{LCR}{\Longrightarrow}$$

$$x = \underline{2a} = 3b + 2$$

$$\| $$

$$2(3a_1 + 1) = 6a_1 + 2$$

$$\Rightarrow b = \frac{2a - 2}{3} \in \mathbb{Z} \Rightarrow 2a \equiv 2 \pmod 3$$

$$2(a - 1) \equiv 0 \pmod 3$$

$$\Downarrow \quad (2, 3) = 1$$

$$a - 1 \equiv 0 \pmod 3$$

$$a \equiv 1 \pmod 3$$

$$a = 3a_1 + 1$$

$$124^{2000^{2001}} \equiv 124^{6c+2} \pmod{3^2} \equiv$$

$$\equiv (\underbrace{124^6}_{\substack{\shortparallel \\ 124^{\varphi(3^2)}}})^c \cdot 124^2 \pmod{3^2} \equiv \underline{1} \cdot 124^2 \pmod{3^2}$$

$$\equiv (-2)^2 \pmod{3^2} \equiv 4 \pmod{3^2} \quad (2)$$

$$124^{2000^{2001}} \pmod{5^2} \equiv (-1)^{2000^{2001}} \pmod{5^2}$$

$$\equiv 1 \pmod{5^2} \quad (1)$$

$$\left\{\begin{array}{lll} y = 124^t \equiv 0 \pmod{2^2} & (1) \\ y = 124^t \equiv 4 \pmod{3^2} & (2) \\ y = 124^t \equiv 1 \pmod{5^2} & (3) \end{array}\right.$$

$$\Rightarrow y \overset{(1)}{=} 4d = 9f + 4$$

$$\Rightarrow y = 25t + 1 = 36f_1 + 4$$

$$4d = 9f + 4 = 36f_1 + 4$$

$$4d - 4 \equiv 0 \pmod 9$$

$$9f + 4 \equiv 0 \pmod 4$$

$$f \equiv 0 \pmod 4$$

$$\Rightarrow f = 4f_1$$

$25t+1 = 36 f_1 + 4$

$\Rightarrow \quad 36 f_1 + 4 \equiv 1 \pmod{25}$

$36 f_1 + 3 \equiv 0 \pmod{25}$

$36 f_1 \equiv -3 \pmod{25}$

$\Rightarrow \quad 12 f_1 = -1 \pmod{25}$

Inversul lui 12 in mod 25

$n \mid a-b \iff n \mid k(a-b)$

$(n, k) = 1$

$(2, 25) = 1$

$\iff \quad 24 f_1 \equiv -2 \pmod{25}$

$\quad \; \shortparallel$

$-f_1 \equiv -2 \pmod{25}$

$\iff f_1 \equiv 2 \pmod{25}$

$\Downarrow$

$f_1 = 25 f_2 + 1$

$y = 36(25 f_2 + 1) + 4 = 900 f_2 + 40$

$\Rightarrow \quad 1024^{2000^{2001}} \equiv 40 \pmod{900}$

Rezumat

$a^b \pmod{c} \equiv r^b \pmod{c}$

1) Reduci baza $\Rightarrow a \equiv r \pmod{c}$

2) Reduci exponentul $\rightarrow$ prim cu c $\Rightarrow$ Euler

$\searrow$ nu e prim $\Rightarrow$ LCR