Aritmetică în $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$$

$\hat{a} = \{$ nr. întregi care dau restul a la împărțirea cu $n\}$

$$\hat{a} = \{nk + a, k \in \mathbb{Z}\}$$

Ex: $\mathbb{Z}_7 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\}$

$\hat{0}$ = multipli de 7 $= \{0, 7, 14, 21, 28, \dots\}$

$\cup \{-7, -14, -21, -28, \dots\}$

$$\hat{1} = \{7k + 1 \mid k \in \mathbb{Z}\} = \{1, 8, 15, 22, 29, \dots\}$$

$$2 \in \mathbb{Z}_7 = \{2, 9, 16, 23, \dots\}$$

Structura algebrică a $\mathbb{Z}_n$:

$(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$\rightarrow (\mathbb{Z}_n, +)$ grup com.

el. neutru : 0

simetricul lui $a \in \mathbb{Z}_n$ este $-a$

= opusul lui a

$\rightarrow (\mathbb{Z}_n - \{0\}, \cdot)$ monoid comutativ

el. neutru 1

nu orice element este simetrizabil față de „$\cdot$"

$$U(\mathbb{Z}_n) = \{ x \in \mathbb{Z}_n \mid x \text{ este simetrizabil față de } \cdot \}$$

Dacă $x \in U(\mathbb{Z}_n)$, x s.n. unitate

Simetricul lui x f. de „$\cdot$" se notează x^{-1} (inversul)

Teoremă: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cmmdc}(x, n) = 1\}$

Ex: $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(\mathbb{Z}_8, +)$ grup comutativ

$(\mathbb{Z}_8 - \{0\}, \cdot)$ monoid comutativ.

$\hat{2} + \hat{3} = \widehat{2+3} = \hat{5}$

$\hat{5} + \hat{7} = \hat{12} = \hat{4}$

$-3 = ?$ opusul lui 3 = simetricul față de +

$-3 = a \Leftrightarrow a + 3 = 0 \Rightarrow a = 5$

$U(\mathbb{Z}_8) = \{x \in \mathbb{Z}_8 \mid \text{cmmdc}(x, 8) = 1\}$

$= \{1, 3, 5, 7\}$

$3^{-1} = ?$ inversul lui 3 = simetricul față de $\cdot$

$3^{-1} = a \Leftrightarrow a \cdot 3 = 1 \Rightarrow a = 3$

$\bar{1}^{-1} = \bar{1}$; $\bar{5}^{-1} = \bar{5}$ pt că $\bar{5}\cdot\bar{5} = \bar{25} = \bar{1}$ în Z_8

$\bar{7}^{-1} = \bar{7}$ pt că $\bar{7}\cdot\bar{7} = \bar{49} = \bar{1}$ în Z_8

Ecuații de gradul I în Z_n

1. $\bar{2}x + \bar{5} = \bar{3}$ în $Z_{11} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{10}\}$

$\bar{2}x = \bar{3} - \bar{5} = \bar{-2}$

$\bar{x} = \bar{-1} = \bar{10}$ SAU $\bar{2}x = \bar{9} \mid \cdot \bar{2}^{-1} = \bar{6}$

$\bar{6}\cdot\bar{2}\cdot x = \bar{9}\cdot\bar{6}$

$\bar{1}x = \bar{54} = \underbrace{\bar{44}}_{\bar{0}} + \bar{10} = \bar{10} = x$

2. $\bar{5}x + \bar{3} = \bar{1}$ în Z_{13}

$\bar{5}x = \bar{-2} = \bar{11} \mid \cdot \bar{5}^{-1}$ $\quad$ $\bar{e}$

$x = \bar{11}\cdot\bar{5}^{-1} = \bar{11}\cdot\bar{8} = \bar{88} = \bar{78} + \bar{10} = \bar{10}$

$= (\bar{-2})\cdot(\bar{-5}) = \bar{10}$

3. $3x+5=1$ în $\mathbb{Z}_{17}$

$3x=-4 \mid \cdot 3^{-1} \Rightarrow x=-4\cdot 3^{-1}=-4\cdot 6$

$\Rightarrow x=-24=\underbrace{-17}_{0}-7=-7=10$

4. $6x+3=1$ în $\mathbb{Z}_{10}$

$6x=-2=8 \mid \cdot 6^{-1}$ ~~$\cdot 6^{-1}$~~ nu există în $\mathbb{Z}_{10}$

$U(\mathbb{Z}_{10})=\{1,3,7,9\}$

$\text{cmmdc}(6,10)=2\neq 1$

$6x=8$ rezolv prin încercări

Obs. $x=3 \Rightarrow 6\cdot 3=18=8 \Rightarrow x=3$ soluție

Ec. de gradul al 2-lea în $\mathbb{Z}_n$

1) $x^2-3x+1=0$ în $\mathbb{Z}_7$

$\Delta=9-4=5$

$\sqrt{5}$ în $\mathbb{Z}_7=?$

$\sqrt{5} = a \Rightarrow a^2 = 5$ în $\mathbb{Z}_7$

$1^2 = 1;\ 2^2 = 4;\ 3^2 = 2;\ 4^2 = 2;\ 5^2 = 4;\ 6^2 = 1;\ 0^2 = 0$

$\Rightarrow \sqrt{5}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol. în $\mathbb{Z}_7$

2) $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{13}$

$\Delta = 25 - 24 = 1$

$\sqrt{\Delta} = \sqrt{1} = \{1, 12\} = \{1, -1\}$

$x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 7 = 42 = \overset{\parallel}{39} + 3 = 3$

$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 7 = 28 = 26 + 2 = 2$

$\overset{\parallel}{0}$

~~$x_3 = (5-1) \cdot 2^{-1}$~~

~~$x_4 = (5+1) \cdot 2^{-1}$~~

Inverse matriceale

$A \in \mathcal{M}_3(\mathbb{Z}_n)$ este inversabilă $\Leftrightarrow$

$\det A \in U(\mathbb{Z}_n) \Leftrightarrow \text{cmmdc}(\det A, \mathbb{Z}_n) = 1$

În $\mathbb{R}$: $A^{-1} = \frac{1}{\det A} \cdot A^*$ | În $\mathbb{Z}_n$: $A^{-1} = (\det A)^{-1} \cdot A^*$

Ex: $A = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 2 & 0 \\ -1 & 2 & 3 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

$A^{-1} = ?$ dacă există

$$\det A = \begin{vmatrix} 2 & 1 & -1 \\ 0 & 2 & 0 \\ -1 & 2 & 3 \end{vmatrix} = 12 - 2 = 10 = 3 \text{ în } \mathbb{Z}_7$$

3^{-1} în $\mathbb{Z}_7 = 5$

$(-1)^{\text{lin+col}}$

$$A \to A^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 2 & 2 \\ -1 & 0 & 3 \end{pmatrix} \to A^* = \begin{pmatrix} 6 & -5 & 2 \\ 0 & 5 & 0 \\ 2 & -5 & 4 \end{pmatrix}$$

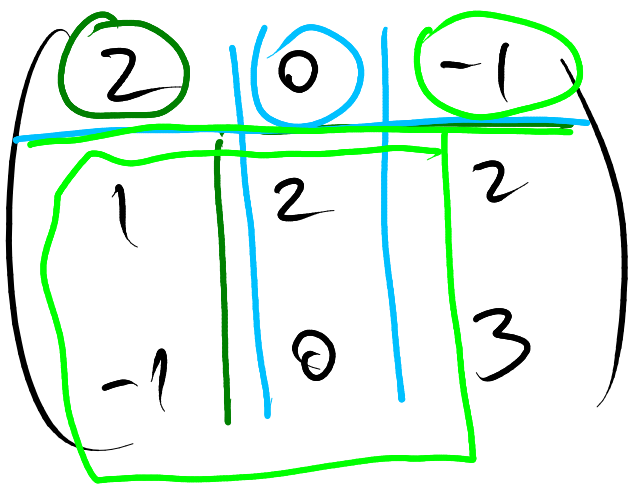
$$A^* = \begin{pmatrix} -1 & 2 & 2 \\ 0 & -2 & 0 \\ 2 & 2 & -3 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot A^* =$$

$$= 5 \cdot \begin{pmatrix} -1 & 2 & 2 \\ 0 & -2 & 0 \\ 2 & 2 & -3 \end{pmatrix} = \begin{pmatrix} -5 & 10 & 10 \\ 0 & -10 & 0 \\ 10 & 10 & -15 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 3 \\ 0 & 4 & 0 \\ 3 & 3 & 6 \end{pmatrix} = A^{-1}$$

Obs: $A \cdot A^{-1} = A^{-1} \cdot A = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$



$$2 \to \begin{vmatrix} 2 & 2 \\ 0 & 3 \end{vmatrix} = 6$$

$$0 \to \begin{vmatrix} 1 & 2 \\ -1 & 3 \end{vmatrix} = 5$$

$$-1 \to \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} = 2$$

Sisteme liniare

1) $\begin{cases} 3x + 2y = 1 \\ 5x - y = 3 \end{cases}$ în $\mathbb{Z}_7$

$\Leftrightarrow$

$y = 5x - 3$

$\Rightarrow 3x + 2(5x - 3) = 1$

$3x + 10x - 6 = 1$

$13x = 7 \Rightarrow 0 \Rightarrow 1x = 0$

$y = 5 \cdot 0 - 3 = -3 = 4$

$\Rightarrow S = \{(0, 4)\}$

2) $\begin{cases} 5x + 2y = 3 \\ -2x + 2y = 5 \end{cases}$ în $\mathbb{Z}_7$

$A = \begin{pmatrix} 5 & 2 \\ -2 & 2 \end{pmatrix}$

$\det A = 14 = 0$

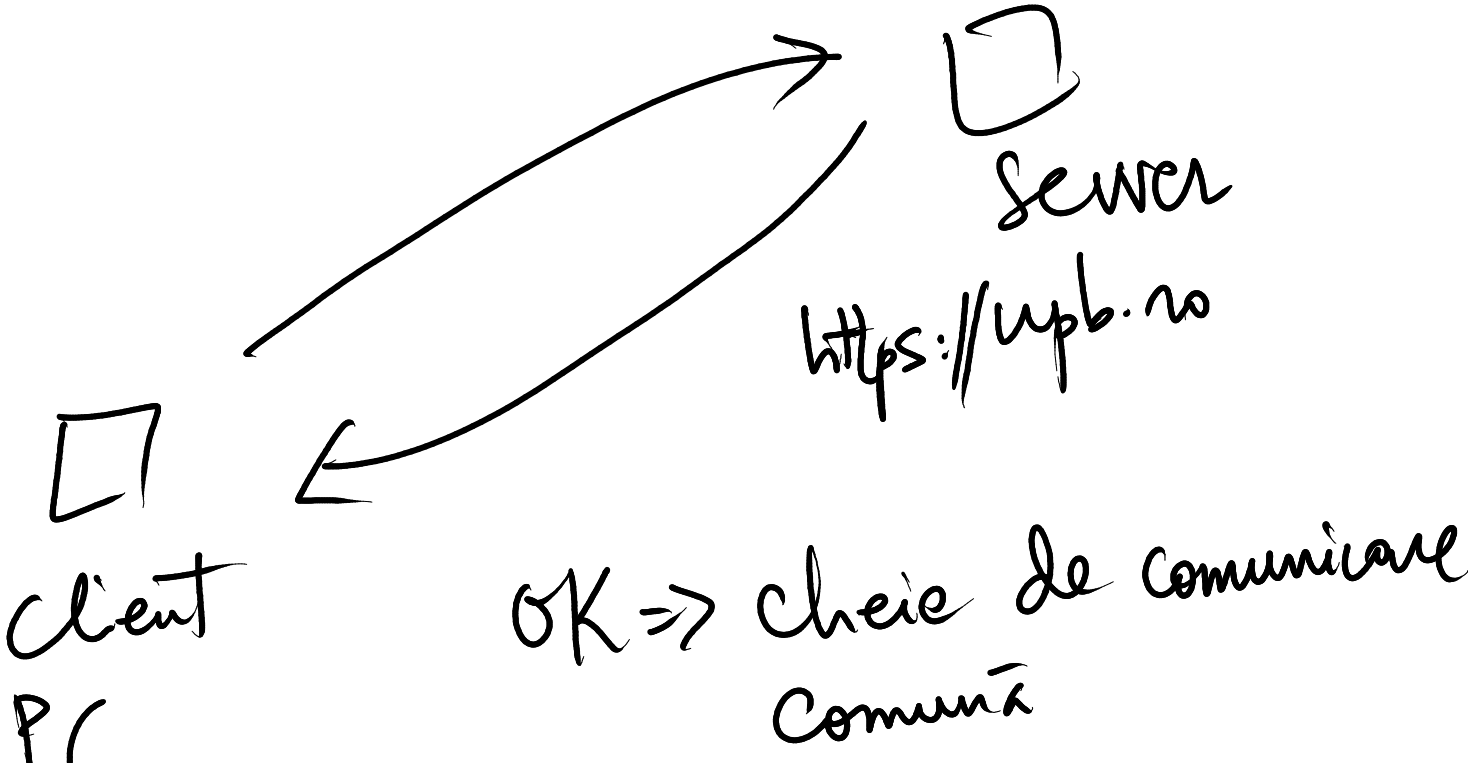
=) Sist. nu mai are sol. unică

=) { are Sol. cu parametri sau
nu are sol.

Teste de primalitate

Securitate practică vs. matematică

Ex: Alg. Diffie-Hellman
-pt. schimb de chei



$n = 20 = 2^2 \cdot 5$

$2 \quad 5$

$n = 13517329$

Nu există:

INPUT $\longrightarrow$ [???] $\longrightarrow$ nr. prim

Ref: Ipoteza lui Riemann (~ 1850)

$\pi : \mathbb{N} \to \mathbb{N}$, $\pi(x) =$ al x-lea nr. prim

$$\lim_{n \to \infty} \frac{\pi(n)}{\ln n} = 1$$

Teste de primalitate

1) Sigure = Deterministe: ineficiente
dpdv computațional

2) Probabiliste: eficiente

T1. Verificare directă:

n prim $\Leftrightarrow \forall d \in \{2, 3, \dots, n-1\}$, $d \nmid n$.

$\left[\frac{n}{2}\right]+1$

$[\sqrt{n}]+1$

↑

Varianta deterministă

Varianta probabilistă: Aleg t mostre $d_1, d_2, d_3, \dots, d_t \in \{2, \dots, n-1\}$ și verific dacă $d_i \mid n$.

Dacă $d_i \nmid n, \forall i \in \{1, \dots, t\} \Rightarrow n$ PROBABIL prim,

prob: $\frac{t}{n-2}$

T2: Ciurul (Sita) lui Eratostene

Ex: $n = 23$

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

~~20~~ ~~21~~ ~~22~~ 23

Ex: $n=25$

2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18

19 20 21 22 23 24 25

STOP $\Rightarrow$ 25 compus

T3: Fermat

Teoremă: $\forall a \in \mathbb{Z}_n^*$ dacă n prim $\Rightarrow$

$$\Rightarrow a^{n-1} = 1 \text{ în } \mathbb{Z}_n^*$$

$$(a^{n-1} = 1 \mod n)$$

Ex: $n=7 \Rightarrow \mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

? $\forall a \in \mathbb{Z}_7^*, a^6 = 1 \mod 7$

$a=1 \Rightarrow 1^6 = 1$ OK

$a=2 \Rightarrow 2^6 = 64 = 63+1$ OK

$a=3 \Rightarrow 3^6 = (3^2)^3 = 2^3 = 8 = 7+1 = 1$ OK

$a=4 \Rightarrow 4^6 = (2^2)^6 = (2^6)^2 = 1$ ok

$a=5 \Rightarrow 5^6 = (-2)^6 = 2^6 = 1$ ok

$a=6 \Rightarrow 6^6 = 2^6 \cdot 3^6 = 1 \cdot 1 = 1$ ok

$\Rightarrow \forall a \in \mathbb{Z}_7^*, a^6 = 1 \bmod 7 \Rightarrow$ n=7 prim.
TF

Ex: $n=9 \Rightarrow \mathbb{Z}_9^* = \{1,2,3,4,5,6,7,8\}$

? $a^8 = 1 \bmod 9, \forall a \in \mathbb{Z}_9^*$

$a=1 \Rightarrow 1^8 = 1$ ok

$a=2 \Rightarrow 2^8 = (2^3)^2 \cdot 2^2 = (-1)^2 \cdot 2^2 = 4 \neq 1 \Rightarrow$

$\Rightarrow n=9$ compus, martor = 2

↑

Varianta deterministă (sigură)

Varianta probabilistă: Alg t mostre

$a_1, a_2, \dots, a_t \in \mathbb{Z}_n^*$ a.i. testez

$a_i^{n-1} = 1 \bmod n$

Simbolul Jacobi

$a, b \in \mathbb{N}$, n impar

$$\left(\frac{b}{n}\right) = \begin{cases} 0 \text{ dacă } n \mid b \\ 1 \text{ dacă } b \text{ este pătrat în } \mathbb{Z}_n \\ -1 \text{ în rest} \end{cases}$$

Ex: $\left(\frac{3}{7}\right) = ?$ $b = 3$, $n = 7$

$7 \nmid 3 \Rightarrow \left(\frac{3}{7}\right) \neq 0$

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$PP(\mathbb{Z}_7^*) = \{1, 4, 2\} \not\ni 3 \Rightarrow \left(\frac{3}{7}\right) = -1$

Ex: $\left(\frac{20}{5}\right)$ $b = 20$, $n = 5$ $\quad 5 \mid 20 \Rightarrow \left(\frac{20}{5}\right) = 0$

Ex: $\left(\frac{71}{7}\right)$ $b = 71$, $n = 7$ $\quad 7 \nmid 71 \Rightarrow \left(\frac{71}{7}\right) \neq 0$

$PP(\mathbb{Z}_7^*) = \{1, 2, 4\}$

$\left(\frac{7!}{7}\right) = \left(\frac{1}{7}\right) = 1$. pt că $1 = 1^2 \in \mathbb{Z}_7^*$

Ex: $\left(\frac{27}{5}\right) = \left(\frac{2}{5}\right) = -1$

$PP(\mathbb{Z}_5^*) = \{1, 4\} \neq 2$

T4: Solovay - Strassen

Teoremă: n prim $\Rightarrow \forall b \in \mathbb{Z}_n^*$,

$$b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \bmod n$$

Ex: $n = 7 \Rightarrow \forall b \in \{1, 2, 3, 4, 5, 6\}$,

$b^{\frac{7-1}{2}} = \left(\frac{b}{7}\right) \bmod 7$?

$b^3 = \left(\frac{b}{7}\right) \bmod 7$

$PP(\mathbb{Z}_7^*) = \{1, 2, 4\}$

$b=1 \Rightarrow b^3=1$

$\left(\frac{1}{7}\right)=1$ p.t că $1 \in PP(\mathbb{Z}_7^*)$] OK

$b=2 \Rightarrow 2^3=1$

$\left(\frac{2}{7}\right)=1$ p.t că $2 \in PP(\mathbb{Z}_7^*)$] OK

$b=3 \Rightarrow 3^3=27=-1=6$

$\left(\frac{3}{7}\right)=-1$ p.t că $3 \notin PP(\mathbb{Z}_7^*)$] OK

$b=4 \Rightarrow 4^3=(2^2)^3=(2^3)^2=1$

$\left(\frac{4}{7}\right)=1$ p.t că $4 \in PP(\mathbb{Z}_7^*)$] OK

$b=5 \Rightarrow 5^3=5^2\cdot 5=25\cdot 5=4\cdot 5=20=-1$

$\left(\frac{5}{7}\right)=-1$ p.t că $5 \notin PP(\mathbb{Z}_7^*)$] OK

$7 \nmid 5$

$b=6 \Rightarrow 6^3=2^3\cdot 3^3=1\cdot(-1)=-1$

$\left(\frac{6}{7}\right)=-1$ p.t că $7 \nmid 6$, $6 \notin PP(\mathbb{Z}_7^*)$] OK

$\Rightarrow 17$ prim

Ex: $n=9 \Rightarrow \forall b \in \mathbb{Z}_9^*$,

$$b^{\frac{9-1}{2}} = \left(\frac{b}{9}\right) ?$$

$$b^4 = \left(\frac{b}{9}\right) \bmod 9$$

$b=1 \Rightarrow 1^4 = 1 \; ; \left(\frac{1}{4}\right) = 1$ OK

$PP(\mathbb{Z}_9^*) = \{1, 4, 0, 7\}$

$b=2 \Rightarrow 2^4 = 16 = 7$

$\left(\frac{2}{9}\right) \in \{0, 1, -1\} = \{0, 1, 8\}$] NU

$\Rightarrow n=9$ compus, 2 martori

Varianta deterministă

Var. probabilistă: Alegi mai multi $b_1, \dots, b_t \in \mathbb{Z}_n^*$ și testez

$$b_i^{\frac{n-1}{2}} = \left(\frac{b_i}{n}\right) \bmod n \; , \forall i \in \{1, \dots, t\}$$