

Aritmetică în \mathbb{Z}_n

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

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

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

\hookrightarrow nu orice element este inv. față de \cdot

\mathbb{Z}_n = resturile posibile la împărțirea cu n

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

Ex: $(\mathbb{Z}_7, +, \cdot)$, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ reprezentanți

$$2+4=6 \Leftrightarrow 16+11=6 \Leftrightarrow 23+25=13 \text{ etc}$$

$$2 = \{7k+2 \mid k \in \mathbb{Z}\} = \{2, 9, 16, 23, \dots\}$$

$$4 = \{7k+4 \mid k \in \mathbb{Z}\} = \{4, 11, 18, 25, \dots\}$$

$$6 = \{7k+6 \mid k \in \mathbb{Z}\} = \{6, 13, 20, 27, 34, \dots\}$$

Pt $x \in \mathbb{Z}_n$, notez cu $-x$ simetricul față de $+$ = oposul lui x

Def: $-x = y \Leftrightarrow x+y=0$, elem. neutr.

Ex: în \mathbb{Z}_7 , $-3 = y \Leftrightarrow 3+y=0 \Rightarrow y=4$

$$\underline{\text{Stu}}: -3 = 0-3 = 7-3 = 4.$$

Notez cu x^{-1} simetricul față de \cdot = inversel lui x .

Pt cîn (\mathbb{Z}_n, \cdot) monoid $\Rightarrow x^{-1}$ nu există pt orice x .

Def: $x^{-1} = y \Leftrightarrow x \cdot y = 1$, elem. neutr.

Ex: în \mathbb{Z}_7 , $3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = 5$ pt că $3 \cdot 5 = 15 = 14 + 1 = 1$.
 $6^{-1} = y \Leftrightarrow 6 \cdot y = 1 \Rightarrow y = 6$ pt că $6 \cdot 6 = 36 = 35 + 1 = 1$

$$6 \equiv y \ (\Rightarrow) 6 \cdot y = 1 \Rightarrow y = 6 \text{ pt că } 6 \cdot 6 = 36 = 35 + 1 = 1$$

Not. $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1}\} = \underline{\text{unități}}$

Teorema: În \mathbb{Z}_n , x este unitate ($\Leftrightarrow \text{cumndc}(x, n) = 1$)

$$\Rightarrow U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cumndc}(x, n) = 1\}$$

În particular, dacă n este prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{0\} = \mathbb{Z}_n^*$

$$\text{De ex, } U(\mathbb{Z}_7) = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

Ecuții de gradul I în \mathbb{Z}_n

$$1) 5x + 1 = 3 \text{ în } \mathbb{Z}_{11}$$

$$5x = 3 - 1 = 2 \quad | \cdot 5^{-1} = 9$$

$$9 \cdot 5 \cdot x = 2 \cdot 9 \\ 1 \cdot x = 18 = 7 \quad \Rightarrow \underline{x = 7}$$

$$2) 6x + 5 = 2 \text{ în } \mathbb{Z}_{10}$$

$$6x = 2 - 5 = -3 = 7 \quad | \cdot 6^{-1}$$

NU EXISTĂ

pt că $\text{cumndc}(6, 10) = 2 \neq 1$

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9
6x	0	6	2	8	4	0	6	2	8	4

\Rightarrow ec. nu are sol.

$$3) hx + 7 = 2 \text{ în } \mathbb{Z}_{10}$$

$$hx = 2 - 7 = -5 = 5 \quad | \cdot 4^{-1} \text{ NU EXISTĂ}$$

x	0	1	2	3	4	5	6	7	8	9
hx	0	4	8	2	6	0	4	8	2	6

\Rightarrow nu are sol.

Ec. de gradul al II-lea

Ecu. de gradul al II-lea

Ex: 1) $2x^2 - 5x + 1 = 0 \text{ în } \mathbb{Z}_7$

$$\Delta = (-5)^2 - 4 \cdot 1 \cdot 2 = 25 - 8 = 17 = 3$$

Există $\sqrt{3}$? Dacă $\sqrt{3} = y \Rightarrow 3 = y^2$

y	0	1	2	3	4	5	6	
y^2	0	1	4	2	2	4	1	

\Rightarrow ec. nu are sol.

2) $x^2 - 5x + 6 = 0 \text{ în } \mathbb{Z}_9$

$$\Delta = 25 - 24 = 1$$

y	0	1	2	3	4	5	6	7	8
y^2	0	1	4	0	7	7	0	4	1

$$\Rightarrow \sqrt{1} \in \{1, 8\} \quad 8 = -1$$

$$\text{Dacă } \sqrt{1} = 1 \Rightarrow x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 5 = 30 = 3$$

$$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 5 = 20 = 2$$

$$\text{Dacă luăm } \sqrt{1} = 8 \Rightarrow x_1 = (5+8) \cdot 2^{-1} = 13 \cdot 5 = 65 = 20 = 2$$

$$x_2 = (5-8) \cdot 2^{-1} = (-3) \cdot 5 = -15 = -9 - 6 \\ = -6 = 3$$

Ex: $4x^2 + x + 5 = 2 \text{ în } \mathbb{Z}_{10}$

$$4x^2 + x + 3 = 0 \text{ în } \mathbb{Z}_{10}$$

$$\Delta = 1 - 4 \cdot 3 \cdot 4 = -47 = -40 - 7 = -7 = 3$$

$\exists \sqrt{3} \text{ în } \mathbb{Z}_{10}$? Nu. \Rightarrow nu are sol.

$\exists \sqrt{3} \in \mathbb{Z}_{10}$? NU \Rightarrow nu are sol.

Sisteme liniare (2x2)

sunt neînverzibile

| obs: Dacă $\det(\text{mat. sist.}) = 0 \Rightarrow$ rezolv puin incertă

• Altfel, pot aplica reducere sau substituții.

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

$$A = \begin{pmatrix} 3 & 1 \\ 2 & -5 \end{pmatrix}; \det A = -15 - 2 = -17 = -14 - 3 = -3 = 4 \text{ OK.}$$

Reducere:

$$\begin{cases} 3x+y=2 | \cdot 5 \\ 2x-5y=1 \end{cases} \Rightarrow \begin{cases} 15x+5y=10 \\ 2x-5y=1 \end{cases} \quad (+) \\ 17x=11 \Rightarrow 3x=4 | \cdot 3^{-1}=5$$

$$\begin{aligned} 2 \cdot 6 - 5y &= 1 \\ 5y &= 11 = 4 | \cdot 5^{-1}=3 \\ y &= 12 = 5 \end{aligned} \quad x = 20 = 6.$$

Substituție:

$$\begin{cases} 3x+y=2 \Rightarrow y=2-3x \\ 2x-5y=1 \end{cases}$$

$$2x - 5(2-3x) = 1$$

$$2x - 10 + 15x = 1$$

$$17x = 11 \Rightarrow 3x = 4 \Rightarrow \begin{aligned} x &= 6 \\ y &= 2-3 \cdot 6 = -16 \\ &= -14 - 2 = -2 = 5 \end{aligned}$$

Inverse matriciale

În \mathbb{R} , matricea M este inversabilă ($\Leftrightarrow \det M \neq 0$).

În \mathbb{Z}_n , matricea M este inversabilă (\Leftrightarrow există $(\det M)^{-1}$)

$\Gamma_n \mathbb{Z}_n$, matricea M este inversabilă (\Leftrightarrow există A^{-1})

Ex: $A = \begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_5)$

$\det A = 8 + 3 = 11 = 1 \text{ or } \Rightarrow \text{există } A^{-1}$ $(-1)^{\text{linii} + \text{col.}}$

$$A \rightarrow A^t = \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 4 & -3 \\ +1 & 2 \end{pmatrix}$$

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

Verificare: $A \cdot A^{-1} = A^{-1} \cdot A = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Coduri elementare

Setup:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	g
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	?	.	.	?
20	21	22	23	24	25	26	27	28	

Alfabetul englezesc conduce la lucrul în $\mathbb{Z}_{26} = \{0, \dots, 25\}$

DAR: $U(\mathbb{Z}_{26}) = \{x \in \mathbb{Z}_{26} \mid \text{cmmdc}(x, 26) = 1\} \neq \text{nr. par}$
 \Rightarrow unele litere vor fi indescifrabile

\Rightarrow Comparam alfabetul cu 3 simboluri $\Rightarrow \mathbb{Z}_{29}$, 29 prim
 $\Rightarrow (1/\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$

\Rightarrow Comptăm altădată cu \sim numărul $-1 \in \mathbb{Z}_{29}$ și \sim primul
 $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$

Cifrul Caesar

Varianta flux (stream cipher)

\hookrightarrow aceeași cheie pt tot mesajul

Ecuția de criptare: mesaj + cheie = cod
 $m + k = c$

Ecuția de decriptare: $c - k = m$
 $\text{cod} - \text{cheie} = \text{mesaj}$

Ex: mesaj: CIFRU, cheie: 19

$$[C, I, F, R, U] \xrightarrow{\substack{+ \text{cheie} \\ + 19}} [21, 27, 24, 36, 39]$$
$$\xrightarrow{\substack{\text{mod } 29 \\ }} [21, 27, 24, 7, 10] \rightarrow V. YHK$$

CIFRU \rightarrow V. YHK (Caesar)

Decriptare: $[V, Y, H, K] \xrightarrow{-K} [21, 27, 24, 7, 10] \xrightarrow{-19}$

$$\rightarrow [2, 8, 5, -12, -9] \xrightarrow{\text{mod } 29} [2, 8, 5, 17, 20] \rightarrow \text{CIFRU.}$$

Varianta pe blocuri (block cipher): cite o cheie pt fiecare bloc

a) fără padding

b) cu padding

Ex: $m = STICLA$, blocuri de lungime 4

$$\Rightarrow b_1 : STIC \quad K_1 = 10$$
$$b_2 : LA?S \leftarrow \text{padding random} \quad K_2 = 20$$

$\Rightarrow b_1 = \text{padding}$ $K_2 = 20$
 $b_2 : L A ? S \leftarrow \text{padding random}$

$$\begin{aligned} [S, T, i, c] &\rightarrow [18, 19, 8, 2] \xrightarrow[\substack{+K_1 \\ +10}]{} [28, 29, 18, 12] \xrightarrow[\substack{\text{mod } 29}]{} \\ &\rightarrow [28, 0, 18, 12] \rightarrow [?, A, S, M] \\ [L, A, ?, S] &\rightarrow [11, 0, 28, 18] \xrightarrow[\substack{+K_2 \\ +20}]{} [31, 20, 48, 38] \\ &\xrightarrow[\substack{\text{mod } 29}]{} [2, 20, 19, 9] \rightarrow [c, U, T, J] \end{aligned}$$

STICLA?S + ? ASMCUTJ (Caesar pe slovuri cu padding)

- Obs 1) Două caractere identice în slovuri diferite se criptază diferit
 \Rightarrow securitate++
- 2) Nu există metode de a separa padding-ul de mesaj
 (după decriptare).

Cifrat afin

Varianta flux:

Ec. de criptare: $m \cdot K_1 + K_2 = c$

Ec. de decriptare: $(c - K_2) K_1^{-1} = m$

Ex: $m = \text{AFIN}$, $K_1 = 3$, $K_2 = 17$

$$\begin{aligned} [A, F, i, N] &\rightarrow [0, 5, 8, 13] \xrightarrow[\substack{\cdot K_1 + K_2 \\ \cdot 3 + 17}]{} [17, 32, 41, 56] \\ &\xrightarrow[\substack{\text{mod } 29}]{} [17, 3, 12, 27] \rightarrow \text{RDM.} \end{aligned}$$

$\text{AFIN} \rightarrow \text{RDM. (afin)}$

$$\dots \rightarrow R \rightarrow M \cdot 7 \rightarrow R_{17} \oplus 12 \oplus 27 \xrightarrow{-K_2 \cdot K_1^{-1}}$$

$$\text{Decriptarea} : [R, A, M, \cdot] \rightarrow [17, 3, 12, 27]$$

$\xrightarrow{-K_2 \cdot K_1^{-1}}$
 $-17 \cdot 3^{-1}$
 $-17 \cdot 10$
 \uparrow
 $+12$

↓
-2

$$\rightarrow [0, -140, -50, 100]$$

$$\xrightarrow[\text{mod } 29]{} [0, 5, 8, 13] \rightarrow \text{AFIN}$$

$$-140 = -146 - 29 = -24 \equiv 5 \pmod{29}$$

$$29 \cdot 4 = 116$$

$$-50 = -29 - 21 = -21 \equiv 8 \pmod{29}$$

$$100 = 87 + 13 \equiv 13 \pmod{29}$$

Varianta pe blocuri

- cite 2 chei pt fiecare bloc

etc

Cifrul Hill

$$\text{Ecuatia de criptare : } \underset{\substack{\uparrow \\ \text{matrice}}}{\text{cheie} \cdot \text{mesaj}} = \underset{\substack{\uparrow \\ \text{vector}}} {\text{cod}}$$

$$\text{Ecuatia de decriptare : } \text{mesaj} = \text{cheie}^{-1} \cdot \text{cod}$$

$$\text{Ex : mesaj : ROZ} \rightarrow \begin{pmatrix} R \\ O \\ Z \end{pmatrix} \rightarrow \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix}$$

$$\text{cheie} \in M_3(\mathbb{Z}_{29}) \quad K = \begin{pmatrix} 1 & -1 & 0 \\ 2 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix}$$

$$\det K = -2 + 1 + 2 = 1 \Rightarrow K \text{ inversabil}$$

$$\text{Criptarea : } \begin{pmatrix} 1 & -1 & 0 \\ 2 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} = \begin{pmatrix} 3 \\ 31 \\ 2 \end{pmatrix} \text{ mod } 29 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} D \\ C \\ B \end{pmatrix}$$

$$\text{Criptarea : } \begin{pmatrix} 1 & -1 & 0 \\ 2 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} = \begin{pmatrix} 3 \\ 31 \\ 11 \end{pmatrix} \bmod 29 = \begin{pmatrix} 3 \\ 2 \\ 11 \end{pmatrix} = \begin{pmatrix} D \\ c \\ L \end{pmatrix}$$

R02 → DCL (Hill)

Decriptarea $\det K = 1 \Rightarrow (\det K)^{-1} = 1$

$$K \rightarrow K^t = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -2 & -1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} -1 & +1 & -1 \\ -2 & 1 & -1 \\ -2 & +1 & 0 \end{pmatrix}$$

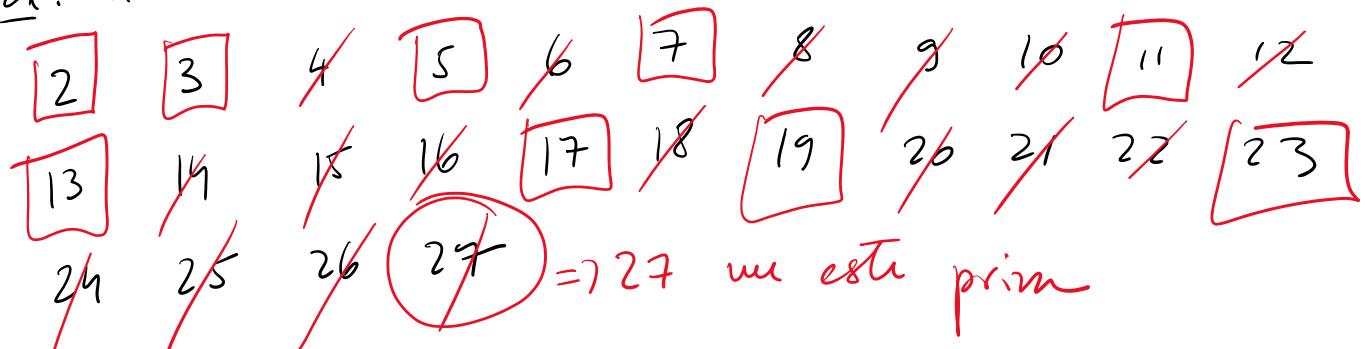
$$K^{-1} = (\det K)^{-1} \cdot K^* = \begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 11 \end{pmatrix} = \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} = \begin{matrix} R \\ O \\ Z \end{matrix}$$

Teste de primalitate

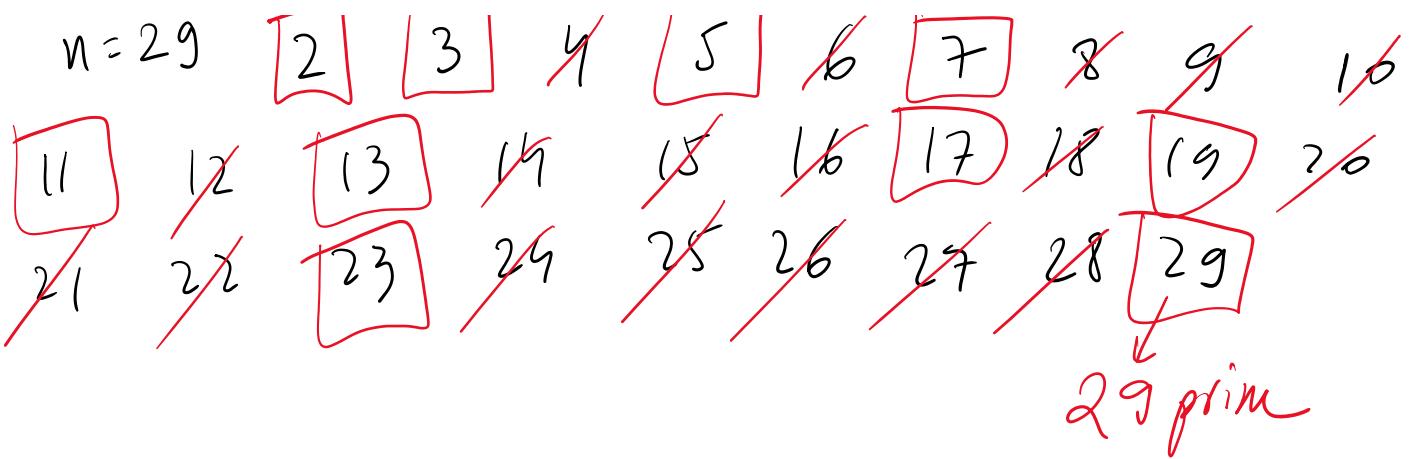
i) Ciurul (sita) lui Eratostene (~ Greaca antică)

Ex: $n = 27$



\Rightarrow lista de nr prime $\leq n$

$$n = 29 \quad \boxed{2} \quad \boxed{3} \quad \cancel{4} \quad \boxed{5} \quad \cancel{6} \quad \boxed{7} \quad \cancel{8} \quad \cancel{9} \quad \cancel{10}$$



Testul Fermat

Teorema (Mica teorema Fermat) (\sim sec XVII)

Dacă n este prim $\Rightarrow \forall 0 < a < n$, $a^{n-1} \equiv 1$ mod n
 Echivalent: $\forall a \in \mathbb{Z}_n^*$, $a^{n-1} \equiv 1$ în \mathbb{Z}_n^* .

Să se arate că: $n = 11 \stackrel{?}{\Rightarrow} \forall a \in \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
 $a^{10} \equiv 1$ în \mathbb{Z}_{11}^* .

$$a=1 \Rightarrow 1^{10} \equiv 1 \text{ OK}$$

$$a=2 \Rightarrow 2^{10} = (2^4)^2 \cdot 2^2 = 5^2 \cdot 2^2 = 10^2 = (-1)^2 = 1 \text{ OK}$$

$$a=3 \Rightarrow 3^{10} = (3^2)^5 = 9^5 = (-2)^5 = -32 = -33 + 1 = 1 \text{ OK.}$$

$$a=4 \Rightarrow 4^{10} = (2^2)^{10} = (2^{10})^2 = 1^2 = 1 \text{ OK}$$

$$a=5 \Rightarrow 5^{10} = (5^2)^5 = 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 4 \cdot 3 = 12 = 1 \text{ OK}$$

$$a=6 \Rightarrow 6^{10} = 2^{10} \cdot 3^{10} = 1 \cdot 1 = 1 \text{ OK}$$

$$a=7 \Rightarrow 7^{10} = (-1)^{10} = 1^{10} = 1 \text{ OK}$$

$$a=8 \Rightarrow 8^{10} = 2^{10} \cdot 4^{10} = 1 \cdot 1 = 1 \text{ OK}$$

$$a=9 \Rightarrow 9^{10} = (3^2)^{10} = (3^{10})^2 = 1 \text{ OK}$$

.....

$$a \equiv g \Rightarrow g^{14} = (3^{-})^{14} = (5^{-})^{14} = 1 \text{ OK}$$

$$a \geq 10 \Rightarrow 10^{10} = 2^{10} \cdot 5^{10} \geq 1 \cdot 1 = 1 \text{ OK}$$

$\Rightarrow n=11$ prim (cf. Fermat)

$$n=15 \Rightarrow \forall a \in \mathbb{Z}_{15}^* = \{1, \dots, 14\} \quad a^{14} \equiv 1 \pmod{15}$$

$$\begin{aligned} a &= 1 \text{ OK} \\ a &= 2 \Rightarrow 2^{14} = (2^4)^3 \cdot 2^2 = 16^3 \cdot 2^2 = 1 \cdot 2^2 = 4 \neq 1 \text{ STOP} \end{aligned}$$

$\Rightarrow n=15$ compus ($a=2$ martor [witness] = contrarevenire la Fermat)

Varianta probabilistica: Aleg doar t măști ($a \in \mathbb{Z}_n^*$)

și verific doar pt ele \Rightarrow răspunsul va avea prob = $\frac{t}{n-1}$.

$$\text{Ex: } n=41, t=3, a \in \{5, 11, 23\}$$

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

$$5^{40} = (5^2)^{20} = 25^{20} = (-16)^{20} = 16^{20} = 2^{80} = (2^5)^{16}$$

$$= (32)^{16} = (-9)^{16} = 9^{16} = 3^{32} = (3^4)^8 = 81^8 = (-1)^8 = 1 \text{ OK}$$

$$11^{40} = (11^2)^{20} = (121)^{20} = (-2)^{20} = 2^{20} = (2^5)^4 = (-9)^4 = 81$$

$$= 81 \cdot 81 = (-1) \cdot (-1) = 1 \text{ OK.}$$

$$23^{40} = (-18)^{40} = 18^{40} = 2^{40} \cdot 3^{80} = (2^{20})^2 \cdot (3^4)^{20} = 81^{20}$$

$$= (-1)^{20} = 1 \text{ OK.} \quad (\text{fără deja})$$

$$\Rightarrow n=41 \text{ probabil prim, cu prob} = \frac{3}{40}.$$

$\Rightarrow n=41$ probabil prim, cu prob = $\frac{1}{40}$.

Testul Solovay-Strassen (sec XX)

Simbolul Jacobi

Def $b, n \in \mathbb{N}^*$, n impar

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

\Updownarrow
există $\sqrt{b \bmod n}$ în \mathbb{Z}_n

Ex: $\left(\frac{4}{11}\right) = ?$ $4 = 2^2$ în $\mathbb{Z}_{11} \Rightarrow \left(\frac{4}{11}\right) = 1$.

$$\left(\frac{6}{3}\right) = 0 \text{ pt că } 3 \mid 6$$

$$\left(\frac{3}{9}\right) = -1$$

x	1	2	3	4	5	6	7	8
	1	4	0	7	7	0	4	1

Teorema (Solovay-Strassen)

Dacă n prim $\Rightarrow \forall a \in \mathbb{Z}_n^*, a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$ în \mathbb{Z}_n^* .

?

*

?

| a |

*

Ex: $n=15 \Rightarrow \forall a \in \mathbb{Z}_{15}^*, a^7 = \left(\frac{a}{15}\right) \in \mathbb{Z}_{15}^*$

$$a=1: 1^7 = 1; \quad \left(\frac{1}{15}\right) = 1 \text{ OK}$$

$a=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 16 \cdot 2^3 = 8 \neq \left(\frac{2}{15}\right) \Rightarrow n=15 \text{ counterexample}$
 $a=2 \text{ is a divisor}$

Ex: $n=17 \Rightarrow \forall a \in \mathbb{Z}_{17}^*, a^8 = \left(\frac{a}{17}\right)$

$$a=1 \text{ OK}$$

$$a=2: 2^8 = (2^4)^2 = (-1)^2 = 1; \quad \left(\frac{2}{17}\right) = 1 \text{ pt. } \bar{a} = 2 = 6^2 \checkmark$$

x	1	2	3	4	5	6	7	8	-8	-7	9	10
x^2	1	4	9	16	8	2	15	13				

$$a=3: 3^8 = (3^2)^2 \cdot 3^2 = 10^2 \cdot 3^2 = 30^2 = (-1)^2 = 1 = 16 = -1$$

$$\left(\frac{3}{17}\right) = -1$$

$$a=4: 4^8 = (2^4)^2 = 1 \quad ; \quad \left(\frac{4}{17}\right) = 1 \text{ pt. } \bar{a} = 4 = 2^2 \checkmark$$

$$a=5: 5^8 = (5^2)^4 = 8^4 = 2^{12} = 2^8 \cdot 2^4 = 2^4 = 16 = -1$$

$$\left(\frac{5}{17}\right) = -1$$

$$a=6: 6^8 = 2^8 \cdot 3^8 = 1 \cdot (-1) = -1 \quad ; \quad \left(\frac{6}{17}\right) = -1 \checkmark$$

$$\dots \quad 2^8 - (-10)^8 = 10^8 = 2^8 \cdot 5^8 = 1 \cdot (-1) = -1 \quad ; \quad \left(\frac{2}{17}\right) = -1 \checkmark$$

$$a=7 : 7^8 = (-10)^8 = 10^8 = 2^8 \cdot 5^8 = 1 \cdot (-1) = -1 ; \left(\frac{2}{17}\right) = -1 \checkmark$$

$$a=8 : 8^8 = 2^8 \cdot 4^8 = 1 ; \left(\frac{8}{17}\right) = 1 \text{ pt că } 8=5^2 \checkmark$$

$$a=9 : 9^8 = (3^8)^2 = 1 ; \left(\frac{9}{17}\right) = 1 \text{ pt că } 9=3^2 \checkmark$$

$$a=10 : 10^8 = 2^8 \cdot 5^8 = 1 \cdot (-1) = -1 ; \left(\frac{10}{17}\right) = -1 \checkmark$$

$$a=11 : 11^8 = (-6)^8 = 6^8 = 2^8 \cdot 3^8 = -1 ; \left(\frac{11}{17}\right) = -1 \checkmark$$

$$a=12 : 12^8 = 2^8 \cdot 6^8 = 1 \cdot (-1) = -1 ; \left(\frac{12}{17}\right) = -1 \checkmark$$

$$a=13 : 13^8 = (-4)^8 = 4^8 = 1 ; \left(\frac{13}{17}\right) = 1 \text{ pt că } 13=8^2 \checkmark$$

$$a=14 : 14^8 = (-3)^8 = 3^8 = -1 ; \left(\frac{14}{17}\right) = -1 \checkmark$$

$$a=15 : 15^8 = 3^8 \cdot 5^8 = 1 ; \left(\frac{15}{17}\right) = 1 \text{ pt că } 15=7^2 \checkmark$$

$$a=16 : 16^8 = (2^8)^4 = 1 ; \left(\frac{16}{17}\right) = 1 \text{ pt că } 16=4^2 \checkmark$$

$\Rightarrow n=17$ prim cf. Solovay-Strassen.

Obs: Testul Solovay-Strassen are și o variantă probabilistică.

Logaritmul discret

Logaritmul discret

Def: $\log_a b = c \Leftrightarrow a^c = b$ (în \mathbb{R} , în \mathbb{Z}_n)

Obs: În \mathbb{Z}_n , $\log_a b$ poate să nu existe.

Ex: $\log_3 7$ în \mathbb{Z}_{11} dacă există

$\log_3 7 = x \Leftrightarrow 3^x = 7$ în \mathbb{Z}_{11} .

x	1	2	3	4	5	6	7	8	9	10
3^x	3	9	5	4	1	3	9	5	4	1

p^{-1}

Obs: Fermat: $a^{p-1} = 1$, dacă p prim

$$3^4 = 3^3 \cdot 3 = 5 \cdot 3 = 15 = 4$$

$\Rightarrow \log_3 7$ nu există în \mathbb{Z}_{11} .

Ex: $\log_5 2$ în $\mathbb{Z}_{13} = x \Rightarrow 5^x = 2$ în \mathbb{Z}_{13}

x	1	2	3	4	5	6	7	8	9	10	11	12
5^x	5	12	8	1								1

$\Rightarrow \log_5 2$ nu există în \mathbb{Z}_{13} .

$$\log_5 8 = 3 \text{ in } \mathbb{Z}_{13}.$$

Ordinal unui element într-un grup (\mathbb{Z}_n^*)

Def 1) Ordinal unui grup = nr. de elemente ale grupului

[ordinalul lui \mathbb{Z}_p^* este $p-1$, p prim]

2) Fie $x \in \mathbb{Z}_p^*$. $\text{ord } x = t \Leftrightarrow x^t = 1$ și t este cel mai mic cu această proprietate.

Dacă nu există ($x^t \neq 1$, $\forall t$), punem $\text{ord } x = \infty$.

Ex: $\text{ord } 3 = 5$ în \mathbb{Z}_{11} și $\text{ord } 5 = 4$ în \mathbb{Z}_{13} (rezultatul anterior)

Teorema (Lagrange)

În \mathbb{Z}_p^* , ordinalul oricărui element divide $p-1$.
 $(\text{ord } x \mid p-1, \forall x \in \mathbb{Z}_p^*, p \text{ prim})$

Def: Dacă în \mathbb{Z}_p^* există (cel puțin) un element de ordin $p-1$, atunci \mathbb{Z}_p^* este un grup ciclic, iar elementul = generator.

Ex: Este \mathbb{Z}_7^* ciclic? $\rightarrow \text{ord}(2) = 3$

$$\begin{array}{ccccccccc} & & & & & & & & \\ \sqrt{+} & 1 & 2 & 3 & 4 & 5 & 6 & & \end{array}$$

x	1	2	3	4	5	6
2^x	2	4	1			
3^x	3	2	6	4	5	1
4^x	4	1				
5^x	5	4	6	2	3	1

$\Rightarrow \text{ord } 3 = 6$

$\Rightarrow \mathbb{Z}_7^* \text{ cyclic, 3 generator}$

$\mathbb{Z}_7^* = \langle 3 \rangle$

Obs: Dacă există generatori
nu este unic.

$\mathbb{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$

Indicatorul lui Euler (Euler's TOTIENT function)

Def: $n \in \mathbb{N}$, $\varphi(n) = \#\{1 \leq x \leq n \mid \text{cmmdc}(x, n) = 1\}$

Ex: $\varphi(10) = ?$ $\{1 \leq x \leq 10 \mid \text{cmmdc}(x, 10) = 1\} \Rightarrow \{1, 3, 7, 9\}$

$$\Rightarrow \varphi(10) = 4.$$

Obs: $\varphi(n) = \# U(\mathbb{Z}_n)$

$$U(\mathbb{Z}_n) = \left\{ x \in \mathbb{Z}_n \mid \text{exists } x^{-1} \right\}$$

Proprietăți 1) Dacă p prim $\Rightarrow \varphi(p) = p - 1$.

$$2) \varphi(xy) = \varphi(x) \cdot \varphi(y)$$

În particular, dacă p, q prime și $n = pq$

$$\Rightarrow \varphi(n) = (p-1)(q-1).$$

$$\Rightarrow n, \dots, \overbrace{11}, 1, 1$$

$$3) \varphi(n) = n \cdot \prod_{\substack{p \text{ prim} \\ p \mid n}} \left(1 - \frac{1}{p}\right).$$

$$\text{Ex: } n = 342 \quad \varphi(342) = ?$$

$$\begin{array}{c|c} 342 & 2 \\ 171 & 3 \\ 57 & 3 \\ 19 & 19 \end{array}$$

$$342 = 2 \cdot 3^2 \cdot 19$$

$$\varphi(342) = 342 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{19}\right)$$

$$= 342 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{18}{19} = 6 \cdot 18 = 108$$