

Aritmetică în \mathbb{Z}_n

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ → clase de resturi modulo n
 = resturi posibile la împărțirea cu n

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

→ $(\mathbb{Z}_n, +)$ grup comutativ:

0 = el. neutrul

Pt orice $x \in \mathbb{Z}_n$, notez $-x$ „simetric” lui x față de „+”
 $-x$ s.n. opusul lui x .

Adică: $x + (-x) = 0$.

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

1 = element neutrul

Nu orice $x \in \mathbb{Z}_n$ are „simetric” față de „·”

Dacă există, notez cu x^{-1} acest „simetric”, numit inversul lui x .

Adică: $x \cdot (x^{-1}) = 1$.

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1}\}$; $x \in U(\mathbb{Z}_n)$ s.n. unitate.

Teorema $x \in U(\mathbb{Z}_n) \Leftrightarrow \text{cmmdc}(x, n) = 1$.

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

Corolar: Dacă n este nr. prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n^*$.

Ex: $(\mathbb{Z}_{11}, +, \cdot)$; $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$7 + 8 = 15 = \overset{10}{11} + 4 = 4,$$

reprenzentanți

$$7+8=15=11+4=4,$$

$$4 \cdot 7=28=\underset{0}{\underset{\parallel}{2}}2+6=6.$$

$\exists = \{$ toate nr. intregi care dau restul 7 la imp. cu 11 $\}$

$$= \{ 11k+7 \mid k \in \mathbb{Z} \} = \{ 18, 29, 40, \dots \}$$

$$4 = \{ 11k+4 \mid k \in \mathbb{Z} \} = \{ 4, 15, 26, 37, \dots \}$$

$$\mathbb{Z}_{11}: 4 \cdot 7=6 \quad (\Rightarrow 40 \cdot 15=17)$$

$$-2=y \quad (\Rightarrow) \quad y+2=0 \Rightarrow y=9 \quad \text{pt că } 9+2 \underset{11}{=} 0.$$

$$-7=4 \quad \text{pt că } 7+4=11=0.$$

$$-7=0-7=11-7=4$$

$$11 \text{ nr prim} \Rightarrow U(\mathbb{Z}_{11}) = \mathbb{Z}_{11}^* = \{ 1, 2, 3, \dots, 10 \}$$

$$2^{-1}=y \quad (\Rightarrow) \quad 2y=1 \Rightarrow y=6 \quad \text{pt că } 2 \cdot 6=12 \underset{11}{=} 1$$

$$5^{-1}=9 \quad \text{pt că } 5 \cdot 9=45 \underset{11}{=} 4+1=1.$$

$$7^{-1}=8 \quad \text{pt că } 7 \cdot 8=56 \underset{11}{=} 5+1=1.$$

$$6^{-1}=2 \quad \text{și} \quad 9^{-1}=5 \quad \text{și} \quad 8^{-1}=7.$$

Ecuații de gradul I

$$Ex: 5x+7=2 \quad \text{în } \mathbb{Z}_{13}$$

$$5x=2-7=-5=8 \quad | \cdot 5^{-1}=8 \quad \left(\text{pt că } 5 \cdot 8=40 \underset{13}{=} 39+1 \right)$$

$$8 \cdot 5 \cdot x=8 \cdot 8$$

$$x=64=12 \quad \Rightarrow x=\underline{12}.$$

$$\text{Verificare: } 5 \cdot 12+7=60+7=(52+8)+7=15=2 \cdot \underline{12}.$$

Verificare: $5 \cdot 12 + 7 = 60 + 7 = (52+8) + 7 = 15 = 2 \cdot \underline{OK}$.

Ex: $7x + 3 = 1$ în \mathbb{Z}_9

$$\underbrace{7x}_{\sim} = 1 - 3 = -2 = \underline{7} \Rightarrow 7x = 1.$$

Ex: $3x + 5 = 4$ în \mathbb{Z}_{12} $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} \not\ni 3$
 $\underline{3x} = -1 = \underline{11} \mid \cdot 3^{-1}$ **Nu există!**

Rezolv prin inlocuire

x	0	1	2	3	4	5	6	7	8	9	10	11
$3x$	0	3	6	9	0	3	6	9	0	3	6	9

Ec. nu are soluții.

Ec. de gradul II

Ex: $3x^2 - 5x + 1 = 0$ în \mathbb{Z}_7 .

$$\Delta = 25 - 4 \cdot 3 = 25 - 12 = 13 = 6.$$

Există rădăcini? Dacă da, $\sqrt{6} = y \Rightarrow y^2 = 6$

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

\Rightarrow Ec. nu are soluții.

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

$$\Delta = 25 - 4 \cdot 6 = 1$$

$$\sqrt{1} = 1 \text{ OK.}$$

$$-1 \quad , \quad 1 \quad , \quad 12 = 39 + 3 = 3$$

$$\lceil \sqrt{1} = 1 \text{ sfk.}$$

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

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

Dacă calculăm $\lceil \sqrt{1} :$

y	0	1	2	3	4	\dots	12
y^2	0	1	4	9	3	\dots	1

$$\Rightarrow \lceil \sqrt{1} \in \{1, 12\}$$

$$12 = -1 \text{ și } (-1)^2 = 1$$

în plus,

$$x_1 = (5+12) \cdot 2^{-1} = 17 \cdot 7 = 4 \cdot 7 = 28 = 2$$

$$x_2 = (5-12) \cdot 2^{-1} = (-7) \cdot 7 = -49 = -39 - 10 = -10 = 3.$$

Sisteme liniare (2x2)

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

Calcați \det matricei sist. Dacă $= 0$ sau neinvertibil \Rightarrow rezolv prin încercări.

$$A = \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix}; \det A = 11 = 4 \text{ sfk.}$$

$$\text{Substituție: } y = 2x - 3 \Rightarrow 5x + 3(2x - 3) = 1$$

$$11x - 9 = 1$$

$$4x - 2 = 1 \Rightarrow 4x = 3 \mid \cdot 4^{-1} = 2$$

$$\begin{array}{r} x = 6 \\ \hline y = 2 \cdot 6 - 3 = 9 = 2 \end{array}$$

inverse matriciale

În \mathbb{R} : $A \in M_n(\mathbb{R})$ este inversabilă ($\Leftrightarrow \det A \neq 0$).

În \mathbb{Z}_n : $A \in M_t(\mathbb{Z}_n)$ este inversabilă ($\Leftrightarrow \det A \in U(\mathbb{Z}_n)$
(ca să existe $(\det A)^{-1}$)).

Ex: $A = \begin{pmatrix} 2 & -5 \\ 3 & 1 \end{pmatrix} \in M_2(\mathbb{Z}_{11})$

$$\det A = 17 = 6 \in U(\mathbb{Z}_{11}); \quad 6^{-1} = 2 \Rightarrow (\det A)^{-1} = 2$$

$$A \rightarrow A^t = \begin{pmatrix} 2 & 3 \\ -5 & 1 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 1 & +5 \\ -3 & 2 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 2 \cdot \begin{pmatrix} 1 & 5 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 10 \\ -6 & 4 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 2 & 10 \\ 5 & 4 \end{pmatrix}$$

Verificare: $A \cdot A^{-1} = A^{-1} \cdot A = I_2$.

Cifruri elementare

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11
M	N	O	P	Q	R	S	T	U	V	W	X
12	13	14	15	16	17	18	19	20	21	22	23
Y	Z	25	26	27	28						

Y < 25 26 27 28

A trebui să lucrăm în $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$.

DAR 26 nu este prim $\Rightarrow U(\mathbb{Z}_{26})$ nu conține (de ex)

niciun număr par \Rightarrow Codurile care folosesc elemente inversibile vor fi îndesifofabile.

\Rightarrow Vom lucra în $\mathbb{Z}_{29} = \{0, 1, 2, \dots, 28\}$

29 prim $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$.

Cifrul Caesar

Varianta flux (stream cipher) : aceeași cheie pt tot mesajul

Ec. de criptare: mesaj + cheie = cod
 $m + K = c$

Ec. de decriptare: $c - K = m$

Ex: $m: COLEG, K=21$

$$[C, O, L, E, G] \rightarrow [2, 14, 11, 4, 6] \xrightarrow{+K} [23, 35, 32, 25, 27]$$

$$\xrightarrow{\text{mod } 29} [23, 6, 3, 25, 27] \rightarrow XGDZ.$$

COLEG \rightarrow XGDZ. (Caesar, $K=21$)

$$\text{Decriptare: } [X, G, D, Z, .] \rightarrow [23, 6, 3, 25, 27] \xrightarrow{-K} [23, 6, 3, 25, 27] \xrightarrow{-21}$$

$$\rightarrow [2, -15, -18, 4, 6] \xrightarrow{\text{mod } 29} [2, 14, 11, 4, 6] \rightarrow COLEG$$

Variantă pe blocuri (block cipher)

- a) fără padding
- b) cu padding (random)

Împărțim textul în blocuri de lungime dată și folosim cote ocheie pt fiecare bloc.

Ex: $m: MIERCURI$ blocuri de lungime 5

$b_1: MIERC \quad K_1 = 11$

$b_2: URIRS \quad K_2 = 15$

$$[M, I, E, R, C] \rightarrow [12, 8, 4, 17, 2] \xrightarrow{+K_1 \atop +11} [23, 19, 15, 28, 13]$$

$\rightarrow XTP?N$

$$[U, R, I, R, S] \rightarrow [20, 17, 8, 17, 18] \xrightarrow{+K_2 \atop +15}$$

$$\rightarrow [35, 32, 23, 32, 33] \xrightarrow{\text{mod } 29} [6, 3, 23, 3, 4]$$

$\rightarrow GDXDE$

$M \underline{IERCURIS} \rightarrow X \underline{TP?N} \underline{GDXDE}$ (Caesar pe blocuri)

OBS: 1) Caractere identice în blocuri diferite \rightarrow criptarea difert
 \rightarrow securitate ++

2) Nu există nicio metodă teoretică de a separa padding-ul de textul decriptat.

Cifrul afin

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

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

Varianta flux: 2 chei pt tot mesajul

Ex: m: MESAj K1 = 6 K2 = 12

$$[M, E, S, A, J] \rightarrow [12, 4, 18, 0, 9] \xrightarrow[\cdot 6 + 12]{\cdot K1 + K2} [84, 36, 120, 12, 66]$$

$$\xrightarrow[\text{mod } 29]{} [26, 7, 4, 12, 8] \rightarrow \leftarrow \text{HEMi}$$

MESAj \rightarrow \leftarrow HEMi (afin)

$$\text{Decriptare: } [\leftarrow, H, E, M, i] \rightarrow [26, 7, 4, 12, 8] \xrightarrow[-12 \cdot 6]{-K2 \cdot K1} [5, 12, 4, 0, 9]$$

$$[70, -25, -40, 0, -20] \xrightarrow[\text{mod } 29]{} [12, 4, 18, 0, 9] \rightarrow \text{MESAj}$$

Varianta pe blocuri: cu 2 chei pt fiecare bloc

Cifrul Hill

vectori-colonă

$$\text{Ec. de criptare: } K \cdot M = C$$

matrice
(de criptare)

$$\text{Ec. de decriptare: } M = K^{-1} \cdot C$$

$$\text{Ex: } M = \begin{pmatrix} C \\ R \\ I \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix}$$

$$K \in M_3(\mathbb{Z}_{29}) = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \quad \det K = 4 \in U(\mathbb{Z}_{29})$$

$$\text{Puncte: } (1 \quad -1 \quad 0 \backslash \quad 2 \quad -15) \quad (17) \quad 0$$

$$\text{Criptarea: } \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix} = \begin{pmatrix} -15 \\ 12 \\ 31 \end{pmatrix} \pmod{29} = \begin{pmatrix} 14 \\ 12 \\ 2 \end{pmatrix} \begin{matrix} O \\ M \\ C \end{matrix}$$

CRI \longrightarrow OMC (Hill flux)

$$\text{Descriptarea: } K \rightarrow K^t = \begin{pmatrix} 1 & 2 & -1 \\ -1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} -1 & +2 & -1 \\ -5 & 2 & -1 \\ 2 & 0 & 2 \end{pmatrix}$$

$$K^{-1} = (\det K)^{-1} \cdot K^* = h^{-1} \cdot K^* = 22 \cdot K^*$$

$$h^{-1} = y \Rightarrow hy = 1 \pmod{29} = \{30, 59, 88, \dots\}$$

$$22 \cdot \begin{pmatrix} -1 & 2 & -1 \\ -5 & 2 & -1 \\ 2 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 12 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix} = \begin{matrix} C \\ R \\ I \end{matrix}$$

Varianta pe blocuri: cîte o matrice de criptare pt fiecare bloc.

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

\downarrow \downarrow \swarrow
matrice vector-colonă

$$\text{Ec. de descriptare: } K_1^{-1} \cdot (c - K_2) = m$$

Ex: $m = ROZ$

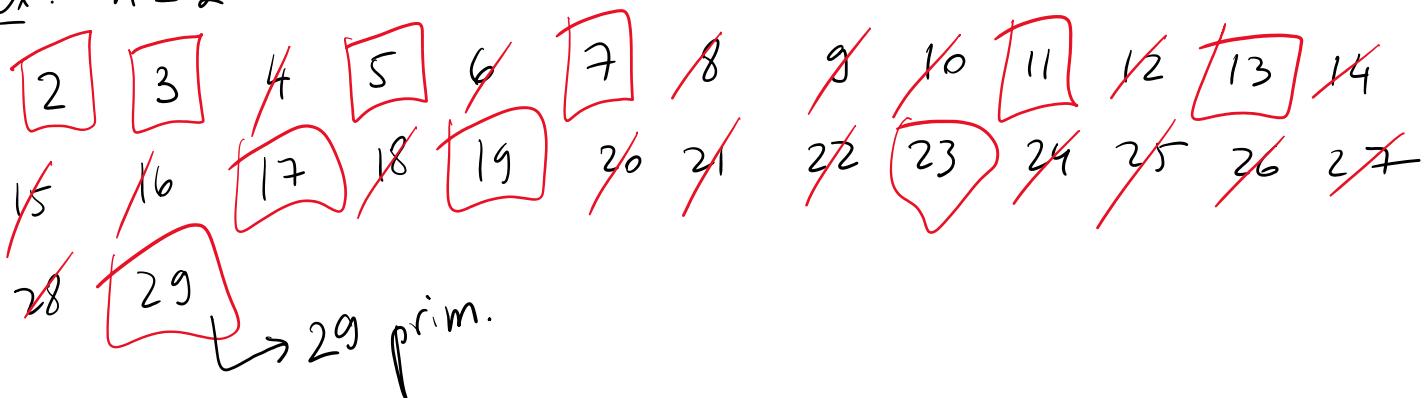
$$K_1 = \begin{pmatrix} -1 & 1 & 0 \\ 2 & 1 & 0 \\ -1 & -1 & -2 \end{pmatrix} ; K_2 = \begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix}$$

$$\begin{array}{c|ccc|cc} & -1 & -2 & & 1 & +1 \\ \hline & & & 4 \\ & & & 11 \\ & & & 11 \\ \hline \end{array}$$

Teste de primalitate

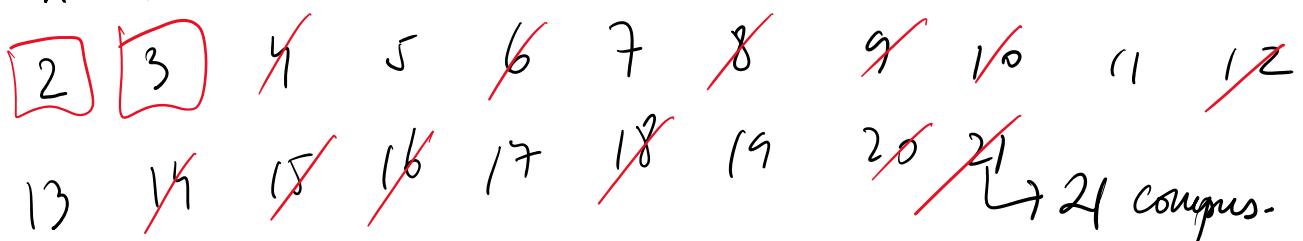
1) Ciurul (sita) lui Eratostene (Grecia antică)

Ex: $n = 29$



$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\} \text{ prime } \leq 29.$$

Ex: $n = 21$



2. Testul Fermat (sec XVII)

Teorema (Mica Teorema Fermat)

Dacă n prim $\Rightarrow \forall a \in \{1, \dots, n-1\}$, $a^{n-1} \equiv 1 \pmod{n}$.

Equivalezent: $\forall a \in \mathbb{Z}_n^* \Rightarrow a^{n-1} \equiv 1 \in \mathbb{Z}_n^*$.

?

×

...

..

Euclidean - von $\leftarrow n \cdot u = 1 \text{ in } \mathbb{Z}_n$.

Ex: $n=11 \Rightarrow \forall a \in \mathbb{Z}_{11}^*, a^{10} = 1 \text{ in } \mathbb{Z}_{11}^*$

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

$$a=2 \Rightarrow 2^{10} = (2^3)^3 \cdot 2 = (-3)^3 \cdot 2 = (-3)^2 \cdot (-3) \cdot 2$$

$$= (-2) \cdot (-3) \cdot 2 = 12 = 1 \text{ OK.}$$

$$a=3 \Rightarrow 3^{10} = (3^2)^5 = (-2)^5 = -32 = -33 + 1 = 1 \checkmark$$

$$a=4 \Rightarrow 4^{10} = (2^2)^{10} = (2^5)^2 = 1^2 = 1 \checkmark$$

$$a=5 \Rightarrow 5^{10} = (5^2)^5 = 4^5 = 2^{10} = 1 \checkmark$$

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

$$a=7 \Rightarrow 7^{10} = (-4)^{10} = 4^{10} = 1 \checkmark$$

$$a=8 \Rightarrow 8^{10} = (2^3)^{10} = (2^5)^3 = 1 \checkmark$$

$$a=9 \Rightarrow 9^{10} = (3^2)^{10} = (3^5)^2 = 1 \checkmark$$

$$a=10 \Rightarrow 10^{10} = 2^{10} \cdot 5^{10} = 1 \cdot 1 = 1 \checkmark$$

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

Ex: $n=51 \Rightarrow \forall a \in \mathbb{Z}_{51}^*, a^{50} = 1 \text{ in } \mathbb{Z}_{51}^*$

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

$$a=2 \Rightarrow 2^{50} = (2^7)^7 \cdot 2 = (2^6)^7 \cdot 2 = 2^7 \cdot 13^7 \cdot 2$$

$$2^7 = 128 = 102 + 26 \\ 128 = 26 \text{ in } \mathbb{Z}_{51}^*$$

$$51 \cdot 3 = 153 \\ 169 - 153 = 16$$

$$\begin{aligned} &= 26 \cdot 13^7 \cdot 2 = 13^8 \cdot 2^2 = (13^2)^4 \cdot 2^2 \\ &= 169^4 \cdot 2^2 = 16^4 \cdot 2^2 = 2^{16} \cdot 2^2 = 2^{18} \\ &= 2^7 \cdot 2^7 \cdot 2^4 = 26 \cdot 26 \cdot 2^4 \end{aligned}$$

$$\begin{aligned}
 51 \cdot 3 &= 153 \\
 169 - 153 &= 16 \\
 &= 2^7 \cdot 2^7 \cdot 2^7 = 26 \cdot 26 \cdot 2^7 \\
 &= 2 \cdot 13 \cdot 2 \cdot 13 \cdot 2^7 = 2^6 \cdot 13^2 = 64 \cdot 169 \\
 &= 13 \cdot 16 = 13 \cdot 4 \cdot 4 = 52 \cdot 4 = 1 \cdot 4 = 4 \\
 &\neq 1
 \end{aligned}$$

$\Rightarrow n=51$ compus (Fermat)
 $a=2$ martor (Witness).

3) Testul Solovay-Strassen

Simbolul Jacobi

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

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

$\exists \sqrt{b \bmod n} \in \mathbb{Z}_n^*$

$$\text{Ex: } \left(\frac{18}{3} \right) = 0 \text{ pt că } 3 \mid 18$$

$$\left(\frac{4}{23} \right) = 1 \text{ pt că } 4 = 2^2$$

$$\left(\frac{7}{19} \right) = 1 \text{ pt că } 7 = 8^2$$

x	1	2	3	4	5	6	7	8	9	-9	-8	-7
x^2	1	4	9	16	6	17	11	7	5	10	11	12
r_3	1	-	-1									

$$\left(\frac{3}{19} \right) = -1$$

)

Teorema (Solvay - Strassu)

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

Ex: $n=11 \stackrel{?}{\Rightarrow} \forall a \in \mathbb{Z}_{11}^*, a^5 = \left(\frac{a}{11} \right)$

$a=1$ OK

$$a=2 \Rightarrow 2^5 = 32 = -1 ; \quad \left(\frac{2}{11} \right) = -1 \quad \checkmark$$

x	1	2	3	4	5	{}
x^2	1	4	9	5	3	

$$a=3 \Rightarrow 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 12 = 1 ;$$

$$\left(\frac{3}{11} \right) = 1 \text{ pt că } 3 = 5^2 \quad \checkmark$$

$$a=4 \Rightarrow 4^5 = (2^2)^5 = (2^5)^2 = 1 ; \quad \left(\frac{4}{11} \right) = 1 \text{ pt că } 4 = 2^2 \quad \checkmark$$

$$a=5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = 45 = 44 + 1 = 1 ; \quad \left(\frac{5}{11} \right) = 1 \text{ pt că } 5 = 3^2 \quad \checkmark$$

$$a=6 \Rightarrow 6^5 = 2^5 \cdot 3^5 = (-1) \cdot 1 = -1 ; \quad \left(\frac{6}{11} \right) = -1 \quad \checkmark$$

$$a=7 \Rightarrow 7^5 = (-4)^5 = -4^5 = -1 ; \quad \left(\frac{7}{11} \right) = -1 \quad \checkmark$$

$$a=8 \Rightarrow 8^5 = 2^5 \cdot 4^5 = (-1) \cdot 1 = -1 ; \quad \left(\frac{8}{11} \right) = -1 \quad \checkmark$$

$$\dots a \quad a^5 = (-2)^5 = -2^5 = 1 \quad , \quad \left(\frac{9}{11} \right) \quad \dots - \dots - 2,$$

$$a=9 \Rightarrow 9^5 = (-2)^5 = -2^5 = 1 \quad ; \quad \left(\frac{9}{11}\right) = 1 \text{ pt că } 9 \equiv 3^2 \pmod{11}$$

$$a=10 \Rightarrow 10^5 = 2^5 \cdot 5^5 = (-1) \cdot 1 = -1 \quad ; \quad \left(\frac{10}{11}\right) = -1 \quad \checkmark$$

$\Rightarrow n=11$ prim (Sororay-Strassen)

$$\exists: n=15 \xrightarrow{?} \nexists a \in \mathbb{Z}_{15}^*, \quad a^{\frac{n-1}{2}} = \left(\frac{a}{15}\right).$$

$$a=1 \quad \checkmark$$

$$a=2 \Rightarrow 2^{\frac{14}{2}} = 2^4 \cdot 2^3 = 1 \cdot 2^3 = 8 \neq \left(\frac{2}{15}\right)$$

$\Rightarrow n=15$ compus.

Variante probabilistică

Fermat
Sororay-Strassen

Aleg t mostre (ele. din \mathbb{Z}_n^*) și verific teoremele drar pt ele.
Rezultatul va avea prob = $\frac{t}{n-1}$.

$\exists:$ Sororay-Strassen, $n=29$, $t=3$,

mostre $a \in \{13, 5, 10\}$

$$a^{\frac{14}{2}} = \left(\frac{a}{29}\right)$$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	1	4	9	16	25	7	20	6	23	13	5	28	24	22

$$\therefore _ _ _ , 14, 1, 11, 14, 14, 1, 4, 14, 7^{56}, 15, 11, 2$$

$$\begin{aligned}
 a=13 \Rightarrow 13^{14} &= (-16)^{14} = 16^{14} = (2^4)^{14} = 2^{56} = (2^5)^{11} \cdot 2 \\
 &= 3^{11} \cdot 2 = (3^3)^3 \cdot 3^2 \cdot 2 = (-2)^3 \cdot 3^2 \cdot 2 = -16 \cdot 9 \\
 &= -4 \cdot 4 \cdot 9 = -4 \cdot 7 = -28 = 1 \quad ; \quad \left(\frac{13}{29}\right) = 1 \text{ pt } \bar{a} \mid 13 = 10^2 \checkmark
 \end{aligned}$$

$$\begin{aligned}
 a=5 \Rightarrow 5^{14} &= (5^2)^7 = (-4)^7 = -2^{14} = -(2^5)^2 \cdot 2^4 \\
 &= -3^2 \cdot 2^4 = -9 \cdot 16 = 1 \quad ; \quad \left(\frac{5}{29}\right) = 1 \text{ pt } \bar{a} \mid 5 = 11^2
 \end{aligned}$$

$$\begin{aligned}
 a=10 \Rightarrow 10^{14} &= 2^{14} \cdot 5^{14} = (2^5)^2 \cdot 2^4 \cdot 1 = 3^2 \cdot 2^4 \cdot 1 = 9 \cdot 16 = -1 \\
 &\left(\frac{10}{29}\right) = -1
 \end{aligned}$$

$$\Rightarrow n=29 \text{ probabil prim, prob} = \frac{3}{28}.$$

Logaritmul discret (in \mathbb{Z}_n)

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

Obs: $\log_a b$ poate să nu existe în \mathbb{Z}_n și nu putem să-l calculăm.

Ex: $\log_2 5$ in $\mathbb{Z}_{11} = ?$ dacă există

$$\log_2 5 = x \Leftrightarrow 2^x = 5 \text{ in } \mathbb{Z}_{11}$$

$$\begin{array}{r}
 x \mid 1 \ 2 \ 3 \boxed{4} \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \\
 \hline
 \end{array}$$

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

$\Rightarrow \log_2 5 = 4 \in \mathbb{Z}_{11}$.

Ex: $\log_3 7 \in \mathbb{Z}_{13} \Rightarrow$ dacă există

$$\log_3 7 = x \Leftrightarrow 3^x = 7 \in \mathbb{Z}_{13}$$

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

$\Rightarrow \log_3 7$ nu există în \mathbb{Z}_{13} .

Obs: Cf Fermat, dacă n este prim, $a^{n-1} = 1 \wedge a \in \mathbb{Z}_n^*$.

Ordinul unui element în \mathbb{Z}_n

Def: $\text{ord}(a) = t \Leftrightarrow a^t = 1$

t este cea mai mică putere

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

Ex: Cf calculilor anterioare, $\text{ord } 2 = 10$ în \mathbb{Z}_{11} , $\text{ord } 3 = 3$ în \mathbb{Z}_{13}

$2^{10} = 1$ în \mathbb{Z}_{11} } 10, 3 cele mai mici puteri
 $3^3 = 1$ în \mathbb{Z}_{13} } cu această proprietate

$$3^3 = 1 \text{ în } \mathbb{Z}_3 \mid \text{în această proprietate}$$

Teorema (Lagrange)

Ordinul oricărui element din \mathbb{Z}_n^* este divizor al lui $n-1$.

Ex: \mathbb{Z}_7

x	1	2	3	4	5	6	
1^x	1						$\Rightarrow \text{ord } 1 = 1$
2^x	2	4	1				$\Rightarrow \text{ord } 2 = 3$
3^x	3	2	6	4	5	1	$\Rightarrow \text{ord } 3 = 6$
4^x	4	2	1				$\Rightarrow \text{ord } 4 = 3$
5^x	5	4	6	2	3	1	$\Rightarrow \text{ord } 5 = 6$
6^x	6	1					$\Rightarrow \text{ord } 6 = 2$

Def: Dacă $\text{ord } a = n-1$ în \mathbb{Z}_n^* , a s.n. generator, iar \mathbb{Z}_n^* s.n. grup ciclic

din calculor anterioare, \mathbb{Z}_7^* ciclic, cu generatorii 3 și 5.
Not. $\mathbb{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$

Indicatormul lui Euler (TOTIENT function)

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

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

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

$$\text{Ex: } n=10, \{x \mid 1 \leq x \leq 10 \text{ and } \gcd(x, 10) = 1\} \rightarrow \{1, 3, 7, 9\}$$

$$\Rightarrow \varphi(10) = 4 \text{ și } \cup(\mathbb{Z}_{10}) = \{1, 3, 7, 9\} \quad 7^{-1} = 3, 9^{-1} = 9$$

- Proprietăți:
- 1) Dacă p prim $\Rightarrow \varphi(p) = p - 1$
 - 2) $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, $m, n \in \mathbb{N}^*$
 - 3) Formula generală: $\varphi(n) = n \cdot \prod_{\substack{\text{p|n} \\ \text{p prim}}} \left(1 - \frac{1}{p}\right)$.

$$\text{Ex: } n = 1231 \text{ prim} \Rightarrow \varphi(1231) = 1230.$$

$$n = 9744 = 2^4 \cdot 3 \cdot 7 \cdot 29$$

$$\begin{array}{c|c} 9744 & 2 \\ 4872 & 2 \\ 2436 & 2 \\ 1218 & 2 \\ 609 & 3 \\ 203 & 7 \\ 29 & 29 \end{array} \quad \begin{aligned} \varphi(9744) &= 9744 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{29}\right) \\ &= 9744 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{28}{29} \\ &= 2 \cdot 6 \cdot 8 \cdot 28 = 2688 \end{aligned}$$

$$\text{Sau: } \varphi(9744) = \varphi(2^4 \cdot 3 \cdot 7 \cdot 29) = \varphi(2^4) \cdot \varphi(3) \cdot \varphi(7) \cdot \varphi(29)$$

$$= 2^4 \cdot \left(1 - \frac{1}{2}\right) \cdot 2 \cdot 6 \cdot 28 = 2^4 \cdot \frac{1}{2} \cdot 2 \cdot 6 \cdot 28 = 2688.$$