

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. neutru

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 neutru

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

Dacă există, notez cu x^{-1} acest „simetric”, numit inverse 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: $(\mathbb{Z}_{11}, +, \cdot)$; $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

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

reprenzentanți

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

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

... punctuală

$7 = \{$ toate nr. întregi care dau restul 7 la împ. cu 11 $\}$

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

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

$$\mathbb{Z}_{11}: 4 \cdot 7=6 \Leftrightarrow 40 \cdot 15=17$$

$$-2=y \Leftrightarrow y+2=0 \Rightarrow y=9 \text{ pt că } 9+2 \equiv 11 \equiv 0.$$

$$-7=u \text{ pt că } 7+u \equiv 11 \equiv 0.$$

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

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

$$2^{-1}=y \Leftrightarrow 2y=1 \Rightarrow y=6 \text{ pt că } 2 \cdot 6 = 12 = 11 + 1 = 1$$

$$5^{-1}=g \text{ pt că } 5 \cdot g = 1 \Leftrightarrow 5 \cdot 5 = 25 = 11 + 1 = 1$$

$$7^{-1}=8 \text{ pt că } 7 \cdot 8 = 56 = 55 + 1 = 1.$$

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

Ecuații de gradul I

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

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

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

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

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

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

Ex: $7x + 3 = 1$ în \mathbb{Z}_9

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

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

Rezolv prin încercări

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}

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

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

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

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

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

Dacă calculăm $\sqrt{1}$:

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

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

$$42 = -1 \text{ și } (-1)^2 = 1$$

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)

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

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

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

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

$$11x - 9 = 1$$

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

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

Inversă matricială

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						

γ \leftarrow \rightarrow \cdot $:$
 24 25 26 27 28

Ar 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 neinvertibile vor fi îndesifrabile.

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

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

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, $K=21$)

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

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

Variantă pe blocuri (block cipher) { Împărțim textul în blocuri de lungime dată și folosim
a) fără padding
b) cu padding (random)

Ex: $m: MIERCURI$ blocuri de lungime 5

$b_1: MIERC$ $K_1 = 11$

$b_2: URIRS$ $K_2 = 15$

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

$\rightarrow XTP?N$

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

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

$\rightarrow GDXDE$

$M \overset{!}{\text{I}} \overset{!}{\text{E}} \overset{!}{\text{R}} \overset{!}{\text{C}} \overset{!}{\text{U}} \overset{!}{\text{R}} \overset{!}{\text{I}} \overset{!}{\text{R}} \overset{!}{\text{S}} \rightarrow X \overset{!}{\text{T}} \overset{!}{\text{P}} \overset{!}{\text{?}} N \overset{!}{\text{G}} \overset{!}{\text{D}} \overset{!}{\text{X}} \overset{!}{\text{D}} \overset{!}{\text{E}}$ (Caesar pe blocuri)

(Obs: 1) Caractere identice în blocuri diferite \rightarrow criptarea diferențială
 \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: $(c - K_2) \cdot K_1^{-1} = m$

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

Varianta flux: 2 chei pt făt mesajul

$$\text{Ex.: } m: \text{MESAJ} \quad K_1 = 6 \quad K_2 = 12$$

$$[M, E, S, A, J] \rightarrow [12, 4, 18, 0, 9] \xrightarrow[\mod 29]{\begin{matrix} \cdot K_1 + K_2 \\ \cdot 6 + 12 \end{matrix}} [84, 36, 120, 12, 66]$$

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

$$\text{MESAJ} \rightarrow \text{HEMI} \text{ (afin)}$$

$$\text{Decriptarea: } [\text{H, E, M, I}] \rightarrow [26, 7, 4, 12, 8] \xrightarrow[-12 \cdot 6^{-1}]{\begin{matrix} \cdot K_2 \cdot K_1^{-1} \\ \mod 29 \end{matrix}}$$

$$[70, -25, -40, 0, -20] \xrightarrow[\mod 29]{\begin{matrix} \cdot 5 \\ \mod 29 \end{matrix}} [12, 4, 18, 0, 9] \rightarrow \text{MESAJ}$$

Varianta pe blocuri: cite 2 chei pt fiecare bloc

Cifrul Hill

vectorii-coloană

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

matrice
(de criptare)

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

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

$$K \in U_3(\mathbb{Z}_{29}) = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \quad \det K = 4 \in U(\mathbb{Z}_{29})$$

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

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

ORI \longrightarrow OM C (Hill flux)

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

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

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

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

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

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

$\downarrow \quad \downarrow \quad \swarrow$
matrice vector-coborâr

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

Ex: $m = ROZ$

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

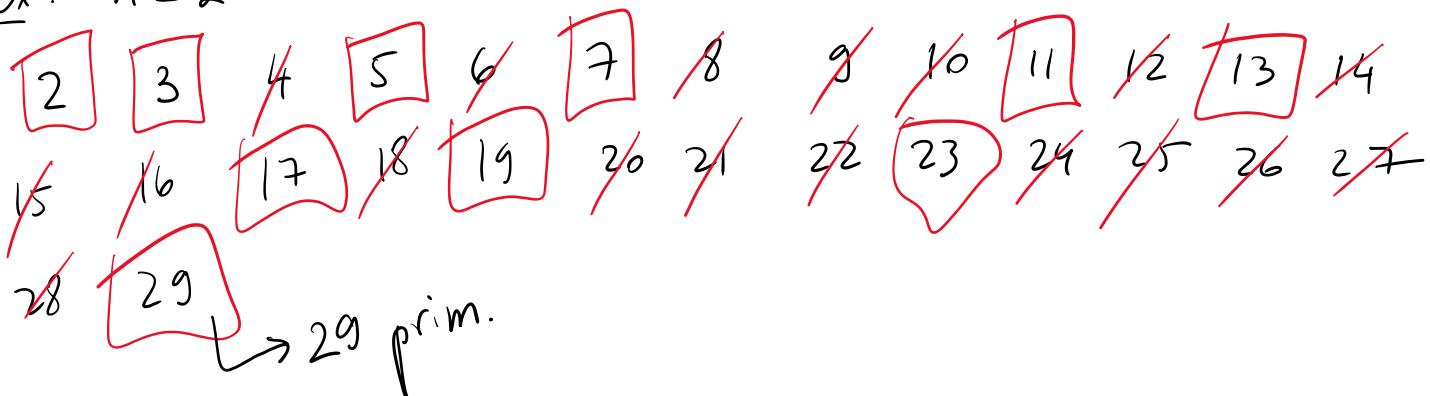
$$K_1 = \begin{pmatrix} -1 & 1 & 0 \\ 2 & 1 & 0 \\ -1 & -1 & -2 \end{pmatrix}; K_2 = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$$

Tinus \xrightarrow{n}
II

Teste de primalitate

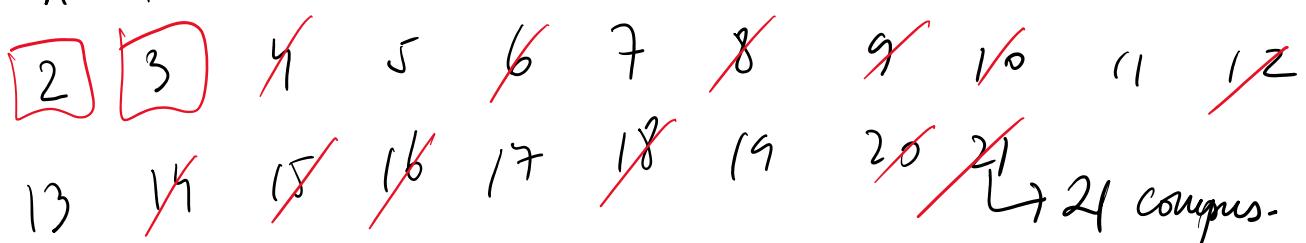
1) Ciurul (sita) lui Eratostene (Grecia antică)

Ex: $n = 29$



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

Ex: $n = 21$



2. Testul Fermat (sec XVII)

Teorema (Mica Teorema Fermat)

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

Equivalent: $\forall a \in \mathbb{Z}_n^* \Rightarrow a^{n-1} = 1 \text{ in } \mathbb{Z}_n^*$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} 2^7 &= 128 = 102 + 26 \\ 128 &= 26 \text{ in } \mathbb{Z}_{51}^* \end{aligned} \quad \left| \begin{aligned} &= 26 \cdot 13^7 \cdot 2 = 13^8 \cdot 2^2 = (13^2)^4 \cdot 2^2 \\ &- 16 \cdot 9^4 \cdot 7^2 = 16^4 \cdot 2^2 = 2^{16} \cdot 2^2 = 2^{18} \end{aligned} \right.$$

$$\begin{aligned}
 128 &= 2^6 \in \mathbb{Z}_{51} \\
 51 \cdot 3 &= 153 \\
 169 - 153 &= 16
 \end{aligned}
 \quad
 \begin{aligned}
 &= 16^4 \cdot 2^2 = 16^4 \cdot 2^2 = 2^{16} \cdot 2^2 = 2^{18} \\
 &= 2^7 \cdot 2^7 \cdot 2^4 = 26 \cdot 26 \cdot 2^4 \\
 &= 2 \cdot 13 \cdot 2 \cdot 13 \cdot 2^4 = 2^6 \cdot 13^2 = 64 \cdot 169 \\
 &= 13 \cdot 16 = 13 \cdot 4 \cdot 4 = 52 \cdot 4 = 1 \cdot 4 = 4 \neq 1
 \end{aligned}$$

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

3) Testul Solovay - Strassen

Simbolul Jacobi

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

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

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

Ex: $\left(\frac{18}{3} \right) = 0$ 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
$\sqrt{2}$	1	4	9	16	6	17	11	7	5	10	11	12

$$\begin{array}{c|cccccccccc} x & 1 & - & - & & & & & & & \\ \hline x^2 & 1 & 4 & 9 & 16 & 6 & 17 & 11 & 7 & 5 & \end{array}$$

$$\left(\frac{3}{11} \right) = -1$$

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

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

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

$$\begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 \\ \hline x^2 & 1 & 4 & 9 & 5 & 3 \end{array} \quad \left. \right\}$$

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

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

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

$$a=5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = 45 = 44 + 1 = 1 ; \quad \left(\frac{5}{11} \right) = 1 \text{ pt că } 5 = 4^2 \quad \checkmark$$

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

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

$$\dots , 8^5 = 7^5 \cdot 6^5 = (-1) \cdot 1 = 1 \quad \checkmark$$

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

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

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

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

$$\text{Ex: } n=15 \xrightarrow{?} \nexists a \in \mathbb{Z}_{15}^*, a^7 = \left(\frac{a}{15} \right).$$

$$a=1 \checkmark$$

$$a=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 1 \cdot 2^3 = 8 \neq \left(\frac{2}{15} \right)$$

$\Rightarrow n=15$ compus.

Variante probabilistică

Fermat
Sororay-Strassen

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

Ex: Sororay-Strassen, $n=29$, $t=3$,

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

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

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

x^2	1	4	9	16	25	7	20	6	23	13	5	28	24	22
-------	---	---	---	----	----	---	----	---	----	----	---	----	----	----

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

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

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

$$\Rightarrow n=29 \text{ probabil prim } 1 \text{ prob} = \frac{3}{28}.$$