

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

Pf 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 „ \cdot ”

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

$$7 + 8 = 15 = \overset{1}{11} + 4 = 4,$$

$$4 \cdot 7 = 28 = \underset{11}{2} 2 + 6 = 6.$$

reprezentanți

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

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

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

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

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

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

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

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

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

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

$$5^{-1} = y \text{ pt că } 5y \equiv 1 \pmod{11} \Rightarrow y = 9 \text{ pt că } 5 \cdot 9 = 45 \stackrel{\text{mod } 11}{=} 1$$

$$7^{-1} = y \text{ pt că } 7y \equiv 1 \pmod{11} \Rightarrow y = 8 \text{ pt că } 7 \cdot 8 = 56 \stackrel{\text{mod } 11}{=} 1$$

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

Ecuații de gradul I

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

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

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

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

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

$$\text{Ex: } 7x + 3 = 1 \text{ în } \mathbb{Z}_9$$

Ex: $7x+3=1$ în \mathbb{Z}_9

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

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}

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

$\sqrt{1} = 1$ OK.

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

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

\therefore soluțiile sunt $\sqrt{1} \cdot y \mid 0 \quad 1 \quad 2 \quad 3 \quad 4 \dots \quad 12$

Dacă calculăm $\sqrt{1}$:	$y \mid 0 \quad 1 \quad 2 \quad 3 \quad 4, \dots \quad 12$
	$y^2 \mid 0 \quad 1 \quad 4 \quad 9 \quad 3 \quad \dots \quad 1$

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

$$12 = -1 \text{ și } (-1)^2 = 1$$

$$\begin{aligned} \text{În plus, } x_1 &= (5+12) \cdot 2^{-1} = 17 \cdot 7 = 4 \cdot 7 = 28 = 2 \\ x_2 &= (5-12) \cdot 2^{-1} = (-7) \cdot 7 = -49 = -39-10 = -10 = 3. \end{aligned}$$

Sisteme liniare (2x2)

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

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

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

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

$$11x - 9 = 1$$

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

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

Inversă matricială

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

În \mathbb{Z}_n : $A \in M_n(\mathbb{Z}_n)$ este invertibilă $\Leftrightarrow \det A \in U(\mathbb{Z}_n)$

$\forall n \in \mathbb{Z}_n$: $A \in M_2(\mathbb{Z}_n)$ 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						

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 numerice la pasul 1 sunt invadabile.

niciun numar par \Rightarrow Codurile care folosesc elemente neînversabile vor fi îndesifrabile.

\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) : aceasi cheie pt tot mesajul

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

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

Ex: $m: C O L E G$, $K = 21$

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

$$\xrightarrow{\text{mod } 29} [23, 6, 3, 25, 27] \rightarrow X G D Z .$$

$C O L E G \rightarrow X G D Z .$ (Caesar, $K=21$)

Decriptare: $[X, G, D, Z, .] \rightarrow [23, 6, 3, 25, 27] \xrightarrow{-K} [-21]$
 $\rightarrow [2, -15, -18, 4, 6] \xrightarrow{\text{mod } 29} [2, 14, 11, 4, 6] \rightarrow C O L E G$

Varianta pe blocuri (block cipher)

a) fără padding

b) cu padding (random)

{ Împărțim textul în blocuri de lungime fixă și folosim
aceeași cheie pt fiecare bloc.

Ex: $m: M I E R C U R I$ blocuri de lungime 5
..... " "

Ex: m: MIERCURI Slovuri de lungime 5

b₁: MIERC K₁ = 11

b₂: URIRS K₂ = 15

$$[M, I, E, R, C] \rightarrow [12, 8, 4, 17, 2] \xrightarrow{+K1 \atop +11} [23, 19, 15, 28, 13]$$

→ XTP?N

$$[U, R, I, R, S] \rightarrow [20, 17, 8, 17, 18] \xrightarrow{+K2 \atop +15}$$

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

→ GDXDE

M_ER_CU_RI_S → XTP?N_{GDXDE} (Coresar pe slovuri)

OBS: 1) Caractere identice in slovuri difrente te cripțează diferent
→ securitate ++

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

Cifrul afin

Ec. de criptare: $m \cdot K1 + K2 = C$

Ec. de decriptare: $(C - K2) \cdot K1^{-1} = m$

Varianta flux: 2 chei pt tot mesajul

Ex: m: MESAJ K₁ = 6 K₂ = 12

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

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

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

MESAJ \rightarrow HEMI (afin)

$$\text{Descriptarea: } [\text{H, E, M, I}] \rightarrow [26, 7, 4, 12, 8] \xrightarrow[\substack{-K_2 \cdot K_1 \\ -12 \cdot 6 \\ 5}]{\substack{+K_1 \\ +1}} [12, 4, 18, 0, 9]$$

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

Varianta pe blocuri: cite 2 chei pt fiecare bloc

Cifrul Hill

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

matrice
(de criptare)

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

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

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

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

ORI \longrightarrow OM C (Hill flux)

$$\text{Decriptarea: } V \sim D^{-1} \cdot \begin{pmatrix} 1 & 2 & -1 \\ -1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & +2 & -1 \\ -5 & 2 & -1 \end{pmatrix}$$

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

$$K^{-1} = (\det K)^{-1} \cdot K^* = 4^{-1} \cdot K^* = 22 \cdot K^*$$

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

$$22 \cdot \begin{pmatrix} -1 & 2 & -1 \\ -5 & 2 & -1 \\ 11 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 12 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix} = \begin{matrix} C \\ R \\ i \end{matrix}$$

Varianta pe blocuri - cînd o matrice de criptare pt fiecare bloc.

* Hill afin: Ec. de criptare: $K1 \cdot M + K2 = C$

Ec. de designture : $k_1^{-1} \cdot (C - k_2) = m$

$$Ex: m = R\circ Z$$

$$M = K \cup L$$

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

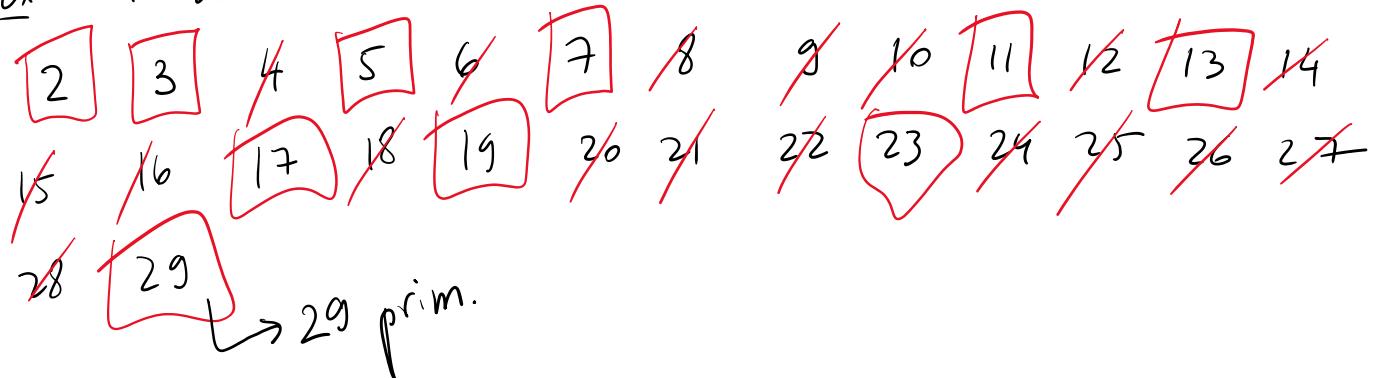
Trans

Teste de primalitate

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

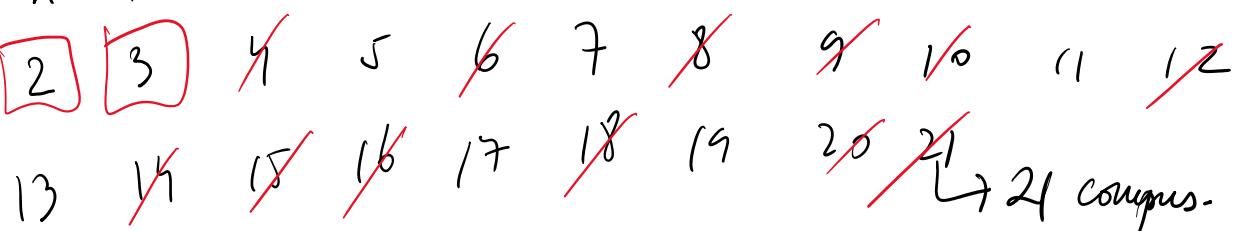
Ex: $n = 29$

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

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

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

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

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

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

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

$$\begin{aligned}
 a=4 \Rightarrow 4^{10} &= (2^2)^{10} = (2^1)^2 = 1^2 = 1 \quad \checkmark \\
 a=5 \Rightarrow 5^{10} &= (5^2)^5 = 4^5 = 2^{10} = 1 \quad \checkmark \\
 a=6 \Rightarrow 6^{10} &= 2^{10} \cdot 3^{10} = 1 \cdot 1 = 1 \quad \checkmark \\
 a=7 \Rightarrow 7^{10} &= (-4)^{10} = 4^{10} = 1 \quad \checkmark \\
 a=8 \Rightarrow 8^{10} &= (2^3)^{10} = (2^1)^3 = 1 \quad \checkmark \\
 a=9 \Rightarrow 9^{10} &= (3^2)^{10} = (3^1)^2 = 1 \quad \checkmark \\
 a=10 \Rightarrow 10^{10} &= 2^{10} \cdot 5^{10} = 1 \cdot 1 = 1 \quad \checkmark
 \end{aligned}$$

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

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

$a=1$ OK.

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

$$\begin{aligned}
 2^7 &= 128 = 102 + 26 & & = 26 \cdot 13^7 \cdot 2 = 13^8 \cdot 2^2 = (13^2)^4 \cdot 2^2 \\
 128 &= 26 \text{ in } \mathbb{Z}_{51}^* & & = 169^4 \cdot 2^2 = 16^4 \cdot 2^2 = 2^{16} \cdot 2^2 = 2^{18} \\
 51 \cdot 3 &= 153 & & = 2^7 \cdot 2^7 \cdot 2^4 = 26 \cdot 26 \cdot 2^4 \\
 169 - 153 &= 16 & & = 2 \cdot 13 \cdot 2 \cdot 13 \cdot 2^4 = 2^6 \cdot 13^2 = 64 \cdot 169 \\
 && & = 13 \cdot 16 = 13 \cdot 4 \cdot 4 = 52 \cdot 4 = 1 \cdot 4 = 4 \\
 && & \neq 1
 \end{aligned}$$

$\Rightarrow n=51$ composite (Fermat)

$a=2$ Martha (Witness).

3) Testul Solovay-Strassen

Simbolul Jacobi

Simbolul Jacobi

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

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

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

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
x^2	1	4	9	16	25	36	49	64	81	100	11	12

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

Teorema (Solovay-Strassen)

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

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

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

$$a=2 \Rightarrow 2 = 2 - 1 \quad | \quad (11) - -$$

$$\begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 \\ \hline x^2 & 1 & 4 & 9 & 16 & 25 \end{array}$$

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

$$\left(\frac{3}{11}\right) = 1 \text{ f.t. } 3 = 5^2 \quad \checkmark$$

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

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

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

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

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

$$a=9 \Rightarrow 9^5 = (-2)^5 = -2^5 = 1 ; \quad \left(\frac{9}{11}\right) = 1 \text{ f.t. } 9 = 3^2 \quad \checkmark$$

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

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

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

$$a=1 \quad \checkmark$$

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

$\Rightarrow n=15$ composite.

Variante probabilistică

Fermat
Solovay-Strassen

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

\exists : Solovay-Strassen, $n = 2^9$, $t = 3$,
mostre $a \in \{13, 5, 10\}$

$$a^{14} = \left(\frac{a}{2^9}\right)$$

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

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

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

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

$$(\overline{29})^{\pm}$$

$\Rightarrow n=29$ 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 îl dinamică -

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

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

$$\begin{array}{c|ccccccccc} x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 2^x & 2 & 4 & 8 & 5 & 6 & 7 & 8 & 9 & 10 & 1 \end{array} \Rightarrow \log_2 5 = 4 \text{ in } \mathbb{Z}_{11}.$$

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

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

$$\begin{array}{c|ccccccccccccc} x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \hline 3^x & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 \end{array}$$

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

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

Ordinul unui element în \mathbb{Z}_n

Def: $\text{ord}(a) = t \Leftrightarrow \left\{ \begin{array}{l} a^t = 1 \\ t \text{ este cea mai mică putere} \end{array} \right.$

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

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

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

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

d) ca în cazul anterior, \mathbb{Z}_7^* ciclic, cu generator 3 și 5.
Not. $\mathbb{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$

Indicatormul lui Euler (TOTIENT function)

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

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

$$\begin{aligned} \text{Ex: } n=10, \quad & \{x \mid 1 \leq x \leq 10 \text{ și } \text{cmmdc}(x, 10) = 1\} \Rightarrow \{1, 3, 7, 9\} \\ & \Rightarrow \varphi(10) = 4 \text{ și } U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\} \quad 7^{-1} = 3, 9^{-1} = 9 \end{aligned}$$

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

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

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

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

$$\begin{array}{r}
 1218 \Big| 2 \\
 609 \Big| 3 \\
 203 \Big| 7 \\
 29 \Big| 29
 \end{array}
 \quad - \text{ " } 23 \neq 28 \\
 = 2 \cdot 6 \cdot 8 \cdot 28 = 2688$$

Soluție: $\varphi(9744) = \varphi(2^4 \cdot 3 \cdot 7 \cdot 29) = \varphi(2^4) \cdot \varphi(3) \cdot \varphi(7) \cdot \varphi(29)$

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

Diffie-Hellman

- bazat pe logaritmul discret ($\log_a b \in \mathbb{Z}_n$)
- Nu criptază, doar generează o cheie

Ex:

- Aliu alegă o cheie pirată, $a = 15$
- Bob alegă o cheie pirată, $b = 12$
- $p = \text{prim}$ $p = 13$ } publice
 $\lambda \in \mathbb{N}$ $\lambda = 10$ } pirată

$$15 \wedge \sim^a \text{ mod } 13 = 15 \text{ mod } 13$$

$$4. \underline{A = \alpha^a \bmod p} = 10^{10} \bmod 13$$

$$= (-3)^{15} = (-3^3)^5 = (-27)^5 = (-1)^5 = (-1) = 12$$

$$5. \underline{B = \alpha^b \bmod p} = 10^{12} \bmod 13$$

$$= (-3)^{12} = (3^3)^4 = 27^4 = 1^4 = 1.$$

A si B publice $\rightarrow b = \log_{\alpha} B$

6. Cheia comună (shared Key)

$$\underline{K = B^a \bmod p} \quad (\text{Alice}) \rightarrow a = \log_B K$$

$$11 = 1^{15} \bmod 13 = 1$$

$$\underline{K = A^b \bmod p} \quad (\text{Bob})$$

$$= 12^{12} \bmod 13 = (-1)^{12} = 1$$

OK

OUTPUT: $K = 1$. public

El Gamal

- bazat pe generatori în grupuri ciclice

I Generez cheia de criptare

$$G \text{ grup cíclic} = \mathbb{Z}_{13}^*$$

$$q-1=12 \Rightarrow q=13$$

generator $g=3$?

Validarea datelor:

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

$\Rightarrow \text{ord}(3) \geq 3$

$$g=2 \quad \text{OK}$$

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

$$\Rightarrow \mathbb{Z}_{13}^* = \langle 2 \rangle.$$

$$e=1$$

$$x \in \{1, 2, \dots, 12\} \quad x = 7$$

$$\text{Calculus: } h = \frac{x}{g} \bmod q = 2 \bmod 13 \\ = 11$$

$$\underline{\text{Pustice: }} G = \mathbb{Z}_{13}^* ; q = 13 ; g = 2 ; h = 11$$

$$\underline{\text{Pivot: }} x = 7.$$

↓
11 chia 11

II Criptarea

$$M = 5 \xrightarrow[\text{inversitate}]{f} m = f(M)$$

Cel mai simplu: $f = \text{id}$, $f(x) = x$

$$m = M = 5.$$

Aleg $y \in \{1, 2, \dots, 12\}$ $y = 8$

Calulez: $s = h^y \bmod q$ public

$$s = 11^8 \bmod 13 = (-2)^8 = 2^8$$

$$= (2^4)^2 = 3^2 = 9$$

Calulez: $c_1 = g^y \bmod q = 2^8 \bmod 13$

$$c_1 = 9$$

$$c_2 = m \cdot s = 5 \cdot 9 = 45 \pmod{13} = 6.$$

Cifru: $(c_1, c_2) = (9, 6)$ public

$$m = 5 \longmapsto (9, 6).$$

Decryption

$$s = c_1^x \pmod{q} = 9^7 \pmod{13}$$

$$= (-4)^7 = (4^2)^3 \cdot (-4) = 3^3 \cdot (-4)$$

$$= 27 \cdot (-4) = -4 = 9.$$

$$s^{-1} \text{ in } \mathbb{Z}_{13}^* = 9^{-1} = 3$$

$$m = c_2 \cdot s^{-1} = 6 \cdot 3 = 18 = 5.$$

$$m = \overline{z}^e$$

RSA

- se bazează pe factorizarea nr. cu două 2 divizori, $n = p \cdot q$, p, q prime mari
- în 2024, se consideră sigur RSA cu $p, q \approx 10^{600}$.

Ex :

I) Generarea cheii

$$p = 11$$

$$q = 13$$

prime | private

$$n = p \cdot q = 143 \quad \cancel{\text{public}}$$

$$\varphi(n) = \varphi(pq) = (p-1)(q-1) = 120$$

Exponent de mărire

Exponent de criptare

$e \in \{3, 4, 5, \dots, 119\}$ ai.

$$\text{ammd}(e, \varphi(n)) = 1$$

$$e = 11.$$

Exponent de decriptare de $\{3, \dots, 119\}$

$$a_i \cdot d \cdot e \equiv 1 \pmod{\varphi(n)}$$

$$\Rightarrow d = e^{-1} \text{ in } \mathbb{Z}_{\varphi(n)}$$

$$d = 11^{-1} \text{ in } \mathbb{Z}_{120} = 11$$

Public: e ; Privat: d

II Criptarea:

UCiptarea:

Aleg mesaj $m \in \{0, 1, \dots, 162\}$

$$m = 15$$

Gfuzul: $c = m^e \bmod n$

$$c = 15^{11} \bmod 163$$

$$= 3^{11} \cdot 5^{11} = (3^5)^2 \cdot 3 \left(\frac{3}{5}\right)^3 \cdot 5^2$$

$$= 100^2 \cdot 3 \cdot (-18)^3 \cdot 5^2$$

$$= 2^4 \cdot 5^4 \cdot 3 \left((-2) \cdot 3^2\right)^3 \cdot 5^2$$

$$= -2^7 \cdot 3^7 \cdot 5^6 = -128 \cdot 243 \cdot 9 \cdot (5^3)^2$$

$$= 15 \cdot 100 \cdot 9 \cdot (-18)^2$$

$$= 3 \cdot 5 \cdot 2^2 \cdot 5^2 \cdot 3^2 \cdot 2 \cdot 3^2$$

$\underbrace{}_{(-18)} \quad \underbrace{}_{100}$

100

$$= (-18) \cdot 100 \cdot 2^3 = -144 \cdot 100$$

$$= -1 \cdot 100 = -1 \cdot (-43) = 43 -$$

$$m = 15 \xrightarrow{\text{RSA}} 43.$$

III Deciphering:

$$m' = c^d \bmod n \stackrel{?}{=} m$$

$$= 43^{11} \bmod 143$$

$$= (-100)^{11} = -(2^2 \cdot 5^2)^{11}$$

$$= -2^{22} \cdot 5^{22} = -(2^7)^3 \cdot 2 \cdot (5^3)^7 \cdot 5$$

$$= + (415^3 \cdot 2 \cdot (-18)^7 \cdot 5$$

$$= + (-1)^{15} \cdot (-1)^{-10}$$

$$= -3^3 \cdot 5^3 \cdot 2 \cdot 2^7 \cdot 3^{14} \cdot 5$$

$$= -2^8 \cdot 3^{17} \cdot 5^4 = 30 \cdot \left(3^5\right)^3 \cdot 3^2 \cdot 5^3 \cdot 5$$

$$= \underline{\underline{30}} \cdot 100^3 \cdot 9 \cdot (-18) \cdot \underline{\underline{5}}$$

$$= 7 \cdot (-162) \cdot 2^6 \cdot 5^6 =$$

$$= 7 \cdot 2^6 \cdot 5^6 \cdot (-19)$$

$$= -133 \cdot 64 \cdot (5^3)^2$$

$$= 10 \cdot 64 \cdot (-18)^2$$

$$= 10 \cdot 18 \cdot 64 \cdot 18 = 37 \cdot 64 \cdot 18$$

$$= 15 (?)$$