

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

$\rightarrow (\mathbb{Z}_n, +)$ grup comutativ
 0 = element neutru

Pf orice $x \in \mathbb{Z}_n$, not $-x$ „simetric” lui x față de $+$
 $-x$ s.a. opusul lui x : $\forall x \in \mathbb{Z}_n, x + (-x) = 0$.

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

Nu pf orice $x \in \mathbb{Z}_n - \{0\}$ există un „simetric”

Dacă există, not. x^{-1} și s.n. inversul lui x .

$$x \cdot (x^{-1}) = 1.$$

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

Teorema: $x \in \mathbb{Z}_n$ unitate (\Rightarrow) $\text{cum.d.c.}(x, n) = 1$

$$\Rightarrow U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cum.d.c.}(x, n) = 1\}$$

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

$$2 + 3 = 5$$

$$2 \cdot 3 = 6$$

$$5 \cdot 6 = 30 = 28 + 2 = 2$$

$$2 = \{x \in \mathbb{Z}_n \mid x \text{ dă restul } 2 \text{ la împ. cu } 7\} = \{7k+2 \mid k \in \mathbb{Z}\}$$

$$= \{2, 9, 16, 23, 30, \dots\}$$

$$\Leftrightarrow 12 \cdot 3k + 2 \text{ este } 2 \text{ în } \mathbb{Z}_7.$$

$$1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$$

$$5 \cdot 6 = 2 \Rightarrow 12 \cdot 34 = 23 \text{ in } \mathbb{Z}_7$$

$$-3 = y \Rightarrow y + 3 = 0 \text{ in } \mathbb{Z}_7 \Rightarrow y = 4 \text{ pt că } 3 + 4 = 7 = 0$$

$$-5 = 2 \text{ pt că } -5 = 0 - 5 = 7 - 5 = 2$$

$$3^{-1} = y \Rightarrow y \cdot 3 = 1 \text{ in } \mathbb{Z}_7 \Rightarrow y = 5 \text{ pt că } 3 \cdot 5 = 15 = 14 + 1 = 1$$

$$5^{-1} = y \Rightarrow y \cdot 5 = 1 \text{ in } \mathbb{Z}_7 \Rightarrow y = 3$$

$$4^{-1} = 2 \text{ pt că } 4 \cdot 2 = 8 = 7 + 1 = 1$$

Obs: Deoarece 7 este prim $\Rightarrow U(\mathbb{Z}_7) = \mathbb{Z}_7^* \setminus \{0\} = \mathbb{Z}_7^*$

pt că cauza $(x, 7) = 1, \forall x \in \mathbb{Z}_7^*$.

Ecuații de gradul I

Ex: $2x + 5 = 1 \text{ in } \mathbb{Z}_7$

$$2x = 1 - 5 = -4 = 3 \mid 2^{-1} = 4$$

$$4 \cdot 2 \cdot x = 4 \cdot 3$$

$$\underline{1} x = 12 = 5 \Rightarrow \underline{\underline{x=5}}$$

Verificare:

$$2 \cdot 5 + 5 = 15 = 1 \text{ in } \mathbb{Z}_7 \quad \checkmark$$

Ex: $5x + 3 = 7 \text{ in } \mathbb{Z}_{11}$

$$5x = 7 - 3 = 4 \mid 5^{-1} = 9$$

$$9 \cdot 5 \cdot x = 9 \cdot 4$$

$$\underline{1} x = 36 = 3 \Rightarrow \underline{\underline{x=3}}$$

Ex: $6x + 1 = 2 \text{ in } \mathbb{Z}_{10}$ $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

$$6x = 1 \mid 6^{-1} \text{ NU EXISTĂ!!}$$

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

Ec. nu are sol.

Ecu. nu are sol.

Obs: Ecu. $6x=1$ este echivalentă cu $x=6^{-1}$ nu se poate!

Ecu. de gradul II

$$\text{Ex: } 2x^2 + 5x - 1 = 0 \text{ în } \mathbb{Z}_9$$

$$\Delta = 25 + 8 = 33 = 6$$

$$\sqrt{\Delta} = \sqrt{6} = y \quad (\Rightarrow) \quad y^2 = 6 \text{ există?}$$

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

$\not\exists y = \sqrt{6}$ nu există în \mathbb{Z}_9 !

\Rightarrow Ecu. nu are soluții.

$$\text{Ex: } x^2 - 5x + 6 = 0 \text{ în } \mathbb{Z}_7$$

$$\Delta = 25 - 24 = 1; \sqrt{1} = 1 \text{ în } \mathbb{Z}_7$$

$$x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 4 = 24 = 3$$

$$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 4 = 16 = 2$$

y	0	1	2	3	4	5	$6 = -1$
y^2	0	1	4	2	2	4	1

$$1 = 1^2 = (-1)^2 = 6^2$$

$$\text{Dacă luăm } \sqrt{1} = 6 \Rightarrow x_1 = (5+6) \cdot 2^{-1} = 4 \cdot 4 = 2$$

$$x_2 = (5-6) \cdot 2^{-1} = 6 \cdot 4 = 3$$

Sisteme liniare (2x2)

$$\text{Ex: } \begin{cases} 2x - y = 3 \\ 5x + 2y = 1 \end{cases} \text{ în } \mathbb{Z}_{11}$$

1 1 1 1 \Rightarrow det matricei săt = 0 sau element neinversabil.

Obs Verifică dacă \det matricei săt = osau element neinversabil.
Dacă da, rezolv prin încercări.

$$A = \begin{pmatrix} 2 & -1 \\ 5 & 2 \end{pmatrix}; \det A = 4 + 5 = 9 \neq 0, \quad g \in U(\mathbb{Z}_{11}) \text{ OK.}$$

$$\text{Substituție: } y = 2x - 3$$

$$\begin{aligned} 5x + 2(2x - 3) &= 1 \\ 9x - 6 &= 1 \Rightarrow 9x = 7 \quad | \cdot 9^{-1} = 5 \\ X &= 7 \cdot 5 = 35 = 2 \\ y &= 2x - 3 = 1. \end{aligned}$$

Inverse matriciale

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

În \mathbb{Z}_n : $A \in M_n(\mathbb{Z}_n)$ este inversabilă dacă $\det A \in U(\mathbb{Z}_n)$.

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

$$\det A = 2 \cdot 15 = -13 = -11 - 2 = -2 = 9 \in U(\mathbb{Z}_{11})$$

$$A \rightarrow A^t = \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 2 & -5 \\ -3 & 1 \end{pmatrix} \quad \begin{matrix} -22-3=-3=8 \\ 11 \end{matrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot \begin{pmatrix} 2 & -5 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 10 & -25 \\ -15 & 5 \end{pmatrix} \quad \begin{matrix} -11-4=-4=7 \\ -11+4=7 \end{matrix}$$

$$= \begin{pmatrix} 10 & 8 \\ 7 & 5 \end{pmatrix}.$$

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

Coduri elementare

Coduri elementare

Setup

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

\Rightarrow Vom lucra în $\mathbb{Z}_{29} = \{0, 1, \dots, 28\}$, 29 prim \Rightarrow
 $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$

Cifrul Caesar

Ecuația de criptare: mesaj + cheie = cod (în \mathbb{Z}_{29})
 $m + k = c$

Ecuația de decriptare: Cod - cheie = mesaj
 $c - k = m$

1) Varianta flux (stream cipher) = aceeași cheie pt tot mesajul

Ex: $m = ASTAZI$, $k = 18$

$$[A, S, T, A, Z, I] \rightarrow [0, 18, 19, 0, 25, 8] \xrightarrow{\begin{matrix} +K \\ +18 \end{matrix}}$$

$$\rightarrow [18, 36, 137, 18, 43, 26] \xrightarrow[\text{mod 29}]{} [18, 7, 8, 18, 14, 26]$$

$\rightarrow \text{SHISO}_{\text{L}}$

$$\text{ASTAZi} \xrightarrow[\text{Caesur}]{+18} \text{SHISO}_{\text{L}}$$

$$\underline{\text{Decriptare}} \quad [\text{S}, \text{H}, \text{i}, \text{s}, \text{o}, \text{L}] \rightarrow [18, 7, 8, 18, 14, 26]$$

$$\xrightarrow[-K]{-18} [0, -11, -10, 0, -4, 8] \xrightarrow[\text{mod 29}]{} [0, 18, 19, 0, 25, 8]$$

$\rightarrow \text{ASTAZi}$

- 2) Varianta pe blocuri
- a) fără padding
 - b) cu padding (random)
- } Împart mesajul în blocuri de lungime fixă și folosesc o cheie pt fiecare bloc.

Ex: $m = \text{ASTAZi}$ blocuri de lungime 3

$$b_1: \text{AST} \quad K_1 = 15$$

$$b_2: \text{AZi} \quad K_2 = 20$$

$$[\text{A}, \text{S}, \text{T}] \rightarrow [0, 18, 19] \xrightarrow[\substack{+K_1 \\ +15}]{} [15, 33, 34] \xrightarrow[\text{mod 29}]{} [15, 4, 5] \rightarrow \text{PEF}$$

$$[\text{A}, \text{Z}, \text{i}] \rightarrow [0, 25, 8] \xrightarrow[\substack{+K_2 \\ +20}]{} [20, 45, 28] \xrightarrow[\text{mod 29}]{} [20, 16, 28]$$

$\rightarrow \text{UQ}?$

ASTAZi \rightarrow **PEFUQ?** (Caesar pe blocuri fără padding)

OBS: Caractere identice în blocuri diferite nu sunt criptate diferit \Rightarrow securitate ++.

Ex: $m = ASTA2i$ blouri de lungime 4 cu padding random

$$b_1 : ASTA \quad K_1 = 15$$

$$b_2 : 2iX. \quad K_2 = 20$$

$$[A, S, T, A] \rightarrow [0, 18, 19, 0] \xrightarrow[\mod 29]{+K_1 \atop +15} [15, 33, 34, 15]$$

$$\xrightarrow[\mod 29]{} [15, 4, 5, 15] \rightarrow PEFP$$

$$[2, i, X, .] \rightarrow [25, 8, 23, 27] \xrightarrow[\mod 29]{+K_2 \atop +20} [45, 28, 43, 57]$$

$$\xrightarrow[\mod 29]{} [16, 28, 19, 18] \rightarrow Q?OS$$

$$ASTA2iX. \rightarrow PEFPQ?OS$$

dec.

OBS: Nu există metodă teoretică de eliminare a padding-ului după decriptare

Cifrul afin

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

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

Varianta flux: același 2 chei pt tot mesajul

$$\text{Ex: } m = TRUMP, K_1 = 6, K_2 = 12 \quad (K_1^{-1} = 6^{-1} = 5)$$

$$[T, R, U, M, P] \rightarrow [19, 17, 20, 12, 15] \xrightarrow[\mod 29]{\cdot K_1 + K_2 \atop \cdot 6 + 12} [126, 114, 132, 84, 102]$$
$$\xrightarrow[\mod 29]{} [10, 27, 16, 26, 15] \rightarrow K \cdot Q \cup P$$

$$\xrightarrow{\text{mod } 29} [10, 27, 16, 26, 15] \rightarrow K \cdot Q \cup P$$

decriptare: $[K, ., Q, \cup, P] \rightarrow [10, 27, 16, 26, 15]$

$$\xrightarrow{-K2 \cdot K1^{-1}} [-10, 75, 20, 70, 15] \xrightarrow{\text{mod } 29} [19, 17, 20, 12, 15]$$

$\rightarrow \text{TRUMP}$

Varianta pc băunii = cite 2 chei pt făcere bloc

Ex: HARRIS = m , blocuri de lungime 5, fără padding

$$b_1: \text{HARRI} \quad | \quad K1=10, K2=13 \quad | \quad K1^{-1}=10^{-1}=3$$

$$b_2: S \quad | \quad K3=15, K4=20 \quad | \quad K3^{-1}=15^{-1}=2$$

$$[H, A, R, R, i] \rightarrow [7, 0, 17, 17, 8] \xrightarrow{\frac{K1+K2}{10+13}}$$

$$[83, 13, 183, 183, 93] \xrightarrow{\text{mod } 29} [25, 13, 9, 9, 6]$$

$\rightarrow ZNJJG$

$$S \rightarrow 18 \xrightarrow{\frac{K3+K4}{15+20}} 290 \xrightarrow{\text{mod } 29} 0 \rightarrow A$$

HARRIS $\rightarrow ZNJJGA$

Cifrul Hill

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

\uparrow
matrice
de criptare

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

Ec. de descriptare: $m = K^{-1} \cdot c$

$$\underline{\text{Ex: } m: 10N \rightarrow \begin{pmatrix} 1 \\ 0 \\ N \end{pmatrix}}$$

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

$$\begin{pmatrix} 1 \\ 0 \\ N \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} ; \quad \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix} \left| \begin{array}{c|c} 8 \\ 14 \\ 13 \end{array} \right. = \begin{pmatrix} -6 \\ 29 \\ -9 \end{pmatrix} \text{ mod } 29$$

$$= \begin{pmatrix} 23 \\ 0 \\ 20 \end{pmatrix} \quad \begin{matrix} X \\ A \\ U \end{matrix}$$

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

$$4 \cdot y = 1 \text{ mod } 29 = \{30, 59, 88, \dots\}$$

$$4^{-1} = 22 \text{ pt că } 4 \cdot 22 \equiv 88 \equiv 87 + 1 = 1$$

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

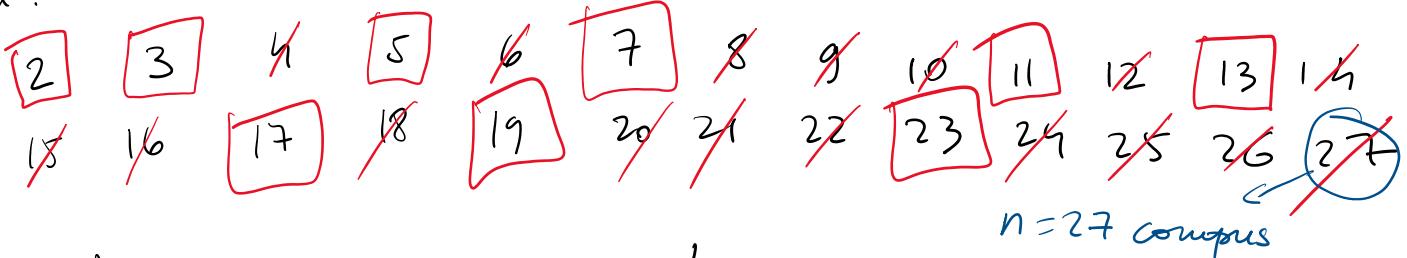
$$K^{-1} = 22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix}$$

$$\text{Descriptarea: } 22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} \text{ (mod 29)}$$

Teste de primalitate

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

Ex: $n = 27$



$$\Rightarrow \{2, 3, 5, 7, 11, 13, 17, 19, 23\} \text{ nr prime } \leq 27$$

2) Testul Fermat (sec. XVII)

Teorema (Mica Teorema a lui Fermat)

Dacă n nr. prim $\Rightarrow \forall a \in \{1, 2, \dots, n-1\}$, $a^{n-1} \equiv 1 \pmod{n}$.

Echivalent: $\forall a \in \mathbb{Z}_n^*, a^{n-1} = 1$.

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

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

$$a = 2 \Rightarrow 2^{10} = (2^3)^3 \cdot 2 = (-3)^3 \cdot 2 = -27 \cdot 2 = -5 \cdot 2 = -10 = 1 \text{ OK}$$

$$a = 3 \Rightarrow 3^{10} = (3^2)^5 = (-2)^5 = (-2)^3 \cdot 2^2 = -8 \cdot 4 = 3 \cdot 4 = 12 = 1 \text{ OK}$$

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

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

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

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

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

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

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

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

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

Ex: $n=15 \xrightarrow{?} \forall a \in \mathbb{Z}_{15}^*, a^{14} = 1 \text{ in } \mathbb{Z}_{15}^*$.

$$a=1 \Rightarrow 1^{14} = 1 \text{ OK}$$

$$a=2 \Rightarrow 2^{14} = (2^4)^3 \cdot 2^2 = 4 \neq 1$$

$\Rightarrow n=15$ compus cf. Fermat ($a=2$ s.v. marfor (witness))

Testul Solovay-Strassen (\sim sec XIX)

Simbolul Jacobi

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

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

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

$$\text{Ex: } \left(\frac{15}{3} \right) = 0 \quad \text{că } 3 \mid 15$$

$$\left(\frac{3}{7} \right) = -1$$

$$\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline x^2 & 1 & 4 & 2 \end{array} \quad \left. \begin{array}{c} (-3) \quad (-2) \quad (-1) \\ 4 \quad 5 \quad 6 \end{array} \right\}$$

$$1 \quad 4 \quad 1 \quad + \quad - \quad . \quad 2 \quad - \quad \rightarrow *$$

$$\left(\frac{4}{19}\right) = 1 \quad \text{pt. } \bar{a}^4 = 2^2 \text{ in } \mathbb{Z}_{19}^*$$

Teorema (Solovay-Strassen)

Leorema (Solovay-Strassen)

Equivalent, that $\in \mathbb{Z}_n^*$, $a^{n-1} = \left(\frac{a}{n}\right) \in \mathbb{Z}_n^*$.

$$\text{Ex: } n=9 \stackrel{?}{\Rightarrow} \forall a \in \mathbb{Z}_9^*, \quad a^4 = \left(\frac{a}{9} \right) \text{ in } \mathbb{Z}_9^*.$$

$$a=1 \Rightarrow 1^4 = 1; \left(\frac{1}{9}\right)^4 = 1 \text{ ist falsch } 1 = 1^2 \quad \checkmark$$

$$a=2 \Rightarrow 2^4 = 2^3 \cdot 2 = (-1) \cdot 2 = -2 = 7 + \left(\frac{2}{9}\right)^{-1}$$

$\Rightarrow n=9$ Compus ($a=2$ märkt)

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

$$a=1 \quad \checkmark \\ a=2 \Rightarrow 2^5 = 32 = -1 : \left| \begin{pmatrix} 2 \\ 11 \end{pmatrix} = -1 \quad \checkmark \right.$$

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

$$a=3 \Rightarrow 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 4 \cdot 3 = 12 = 1$$

$$\left(\frac{3}{11}\right) = 1 \text{ pt } \text{ca } 3 \equiv 5^2$$

$$a=4 \Rightarrow 4^5 = (2^2)^5 = (2^5)^2 = (-1)^2 = 1 \quad ; \quad \left(\frac{4}{11}\right) = 1 \neq \text{ca } 4^2 = 2^2$$

$$-r \cdot r^5 - (r^2)^2 \cdot 5 = 3^2 \cdot 5 = (-2) \cdot 5 = -10 = 1$$

$$a=4 \Rightarrow 4^5 = (-2)^5 = -32 \stackrel{11}{\equiv} -10 \equiv 1$$

$$a=5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = (-2) \cdot 5 \stackrel{11}{\equiv} -10 \equiv 1$$

$$\left(\frac{5}{11}\right) = 1 \text{ pt că } 5 \stackrel{2}{\equiv} 1$$

$$a=6 \Rightarrow 6^5 = 2^5 \cdot 3^5 = (-1) \cdot 1 \stackrel{11}{\equiv} -1 \stackrel{11}{\equiv} 10 \quad ; \quad \left(\frac{6}{11}\right) = -1 \checkmark$$

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

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

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

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

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

Variantele probabilistice

Fermat

Sororay-Strassen

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

Ex: Fermat probabilist, $t=3$, $n=41$

Mostre: $a \in \{23, 36, 40\}$? $\Rightarrow a^{40} = 1$ în \mathbb{Z}_{41}^*

$$23^{40} = (-18)^{40} = 18^{40} = 2^{40} \cdot 3^{80} = 1 \cdot 1 = 1 \checkmark$$

$$3^{80} = (3^4)^{20} = 81^{20} = (-1)^{20} = 1$$

$$9^{40} - (2^5)^8 = 32^8 = (-9)^8 = 9^8 = (9^2)^4 = (-1)^4 = 1$$

$$2^{40} = (2^5)^8 = 32^8 = (-9)^8 = 9^8 = (9^2)^4 = (-1)^4 = 1$$

$$36^{40} = (-5)^{40} = 5^{40} = (5^2)^{20} = (-16)^{20} = 2^{80} = (2^{40})^2 = 1.$$

$$40^{40} = (-1)^{40} = 1.$$

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

Logaritmul discret (in Z_n)

Def: $\log_a b = c \Leftrightarrow a^c = b$ (in R_+ , in Z_n)

Obs: Există valori pt a, b a.t. $\log_a b$ nu există in Z_n .

Ex: $\log_2 3$ in Z_{11} $\log_2 3 = x \Leftrightarrow 2^x = 3$ in Z_{11}

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

$\Rightarrow \text{ord}_2 = 10$
in Z_{11}

$$2^6 = 2^5 \cdot 2 = 10 \cdot 2 = 20 = 9; \quad 2^7 = 2^6 \cdot 2 = 9 \cdot 2 = 18 = 7$$

$$2^8 = 2^7 \cdot 2 = 7 \cdot 2 = 14 = 3$$

$\Rightarrow \log_2 3 = 8$ in Z_{11} . (pt că $2^8 = 3$ in Z_{11}).

Ex: $\log_3 5$ in Z_{13} dacă există

$$\log_3 5 = x \Leftrightarrow 3^x = 5 \text{ in } Z_{13}$$

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

x	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	<u>1</u>

$\Rightarrow \log_3 5$ nu există în \mathbb{Z}_{13} .

Obs: Cf. Fermat, dacă n hr prim $\Rightarrow a^{n-1} = 1$ în \mathbb{Z}_n^* ,
 $\forall a \in \mathbb{Z}_n^*$.

Ex: $\log_3 4$ în $\mathbb{Z}_{17} = x \Leftrightarrow 3^x = 4$ în \mathbb{Z}_{17}

x	1	2	3	4	5	6	7	8	(-8)	(-7)	(-6)	(-5)
3^x	3	9	10	13	5	15	11	16	14	8	7	4

$$3^4 = 3 \cdot 3 = 10 \cdot 3 = 30 = 13 ; 3^5 = 3^4 \cdot 3 = 13 \cdot 3 = 39 = 5$$

$$3^6 = 3^5 \cdot 3 = 5 \cdot 3 = 15 ; 3^7 = 3^6 \cdot 3 = 15 \cdot 3 = (-2) \cdot 3 = -6 = 11$$

$$3^8 = 3^7 \cdot 3 = 11 \cdot 3 = (-6) \cdot 3 = -18 = -1 = 16$$

$$3^9 = 3^8 \cdot 3 = 16 \cdot 3 = (-1) \cdot 3 = -3 = 14$$

$$3^{-8} \text{ în } \mathbb{Z}_{17} = ? \quad 3^{-8} = (3^8)^{-1} = \text{inversele lui } 3^8 = 16 = (-1)$$

$$(-1)^{-1} = -1 \text{ pt că } (-1) \cdot (-1) = 1$$

$$3^{10} = 3^9 \cdot 3 = 14 \cdot 3 = (-3) \cdot 3 = -9 = 8 \quad \left\{ \begin{array}{l} 3^{11} = 3^{10} \cdot 3 = 8 \cdot 3 = 7 \\ 3^{12} = 3^{11} \cdot 3 = 7 \cdot 3 = 21 = 4 \end{array} \right.$$

$$3^{10} = 3^{-7} = (3^7)^{-1} = 11^{-1}$$

$$\Rightarrow 3^{12} \equiv 1 \pmod{17} \text{ și } \log_3 4 = 12 \text{ în } \mathbb{Z}_{17}.$$

Ordinul unui element în \mathbb{Z}_n

Def: $\text{ord}(x \in \mathbb{Z}_n) = t \Leftrightarrow x^t \equiv 1 \pmod{n}$ și t este cea mai mică putere

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

Ex: $3^3 \equiv 1 \pmod{13} \Rightarrow \text{ord}(3) = 3$ în \mathbb{Z}_{13} .

OBS: Dacă n este prim și folosim Fermat $\Rightarrow x^{n-1} \equiv 1$, dar asta nu înseamnă mereu că $\text{ord}(x) = n-1$.

Teorema (Lagrange)

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

Ex: $\text{ord}3=3$ în \mathbb{Z}_{13} (OK)

Ex: \mathbb{Z}_7 :

x	1	2	3	4	5	6	
2^x	2	4	1	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 $\text{ord}(x) = n-1$ în \mathbb{Z}_n , spunem că x este generator pt \mathbb{Z}_n , iar \mathbb{Z}_n s.n. ciclic.

Ex: \mathbb{Z}_7 este ciclic, generat de 3 sau 5

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

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

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

$\Rightarrow \varphi(10) = 4$. ($\#\mathcal{U}(\mathbb{Z}_{10}) = 4$, adică $1, 3, 7, 9$ inversabile în \mathbb{Z}_{10})

Poarbeți: 1) Dacă p prim $\Rightarrow \varphi(p) = p-1$

2) $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

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

\nwarrow Formula generală

Ex: $n=97 \Rightarrow \varphi(97) = 96$.

$$n=582 = 2 \cdot 3 \cdot 97$$

$$\begin{array}{r} 582 \\ 291 \\ 97 \end{array} \Big| \begin{array}{l} 2 \\ 3 \\ 97 \end{array}$$

$$n = 582 = 2 \cdot 3 \cdot 97$$

$$\begin{array}{r} 582 \\ 97 \mid 582 \\ 97 \\ \hline 10 \end{array}$$

$$\begin{aligned}\varphi(582) &= \varphi(2) \cdot \varphi(3) \cdot \varphi(97) \\ &= 1 \cdot 2 \cdot 96 = 192 \quad (\text{proper 18-2})\end{aligned}$$

$$\begin{aligned}\varphi(582) &= 582 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{97}\right) \\ &= 582 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{96}{97} = 192\end{aligned}$$

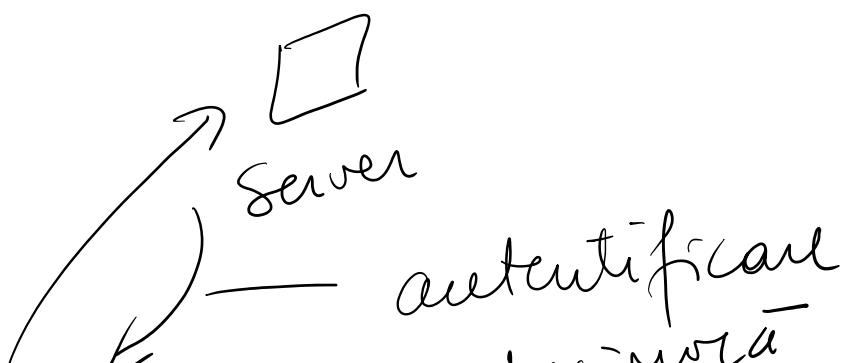
$$\varphi(1000) = 1000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400.$$

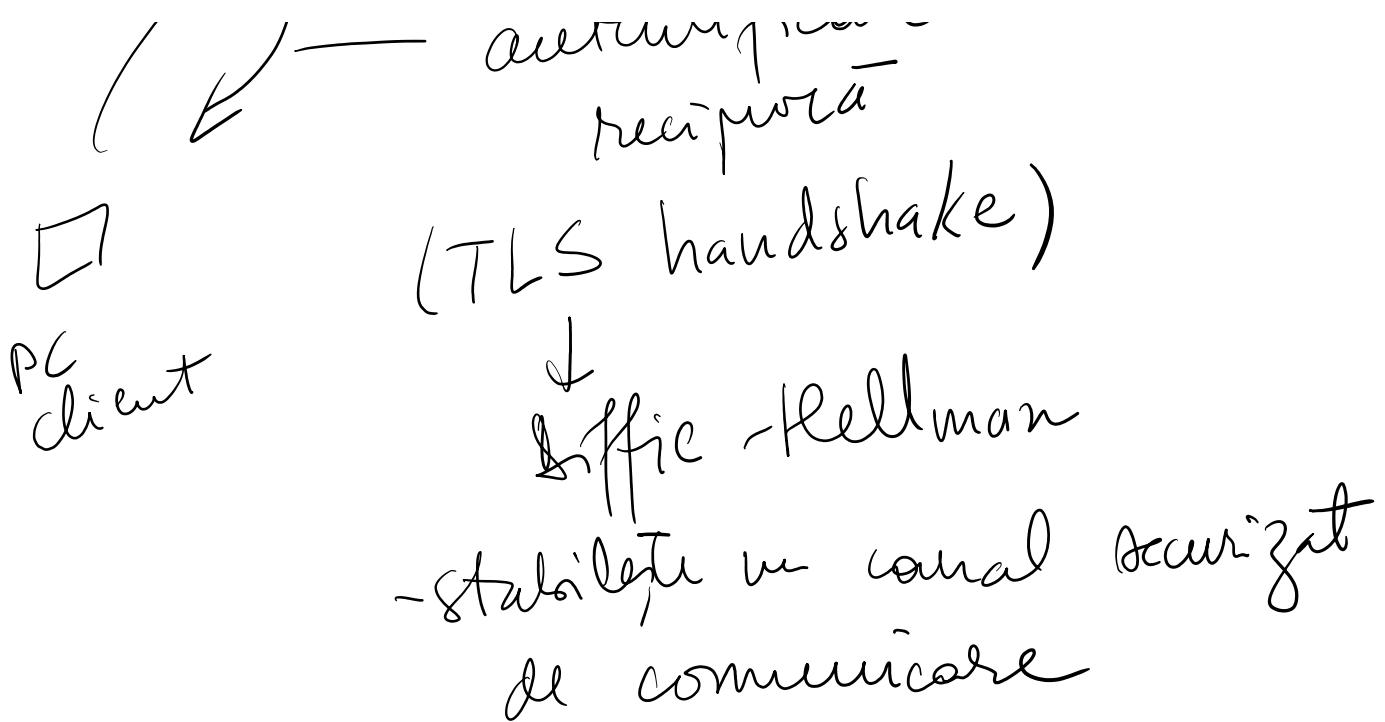
$$1000 = 10^3 = 2^3 \cdot 5^3$$

$$\varphi(2^3) = 2^3 \cdot \left(1 - \frac{1}{2}\right) ; \varphi(5^3) = 5^3 \cdot \left(1 - \frac{1}{5}\right)$$

Diffie-Hellman

- baza matematică: log discret (logaritmă în \mathbb{Z}_q)
- se folosește pt generaarea unei chei,
NU criptază!





Ex :

1. Alice alege cheie pirată $a = 11$
2. Bob alege cheie pirată : $b = 8$
3. p prim = 13 , $\alpha \in \mathbb{N}$, $\alpha = 20$
public

4. Cheia publică $A = \alpha^a \bmod p$

$$A = 20^{11} \bmod 13 = 7^{11} \bmod 13$$

$$- (7^2)^5 \cdot 7 = 49^5 \cdot 7 = 10^5 \cdot 7$$

$$= (7^2)^3 \cdot 7 = 49^3 \cdot 7 = 10^3 \cdot 7$$

$$= (-3)^5 \cdot 7 = -3^3 \cdot 3^2 \cdot 7 = -1 \cdot 9 \cdot 7$$

$$= (-1) \cdot (-2) = 2.$$

5. Cheia publică $B = 2^b \pmod{p}$

$$B = 20^8 \pmod{13} = 7^8 \pmod{13}$$

$$= (7^2)^4 = 10^4 = (-3)^4 = (-3) \cdot -3^3$$

$$= -3 \cdot (-1) = 3.$$

6. Cheie comună (shared key)

$$K = B^a \pmod{p} \quad (\text{Alice})$$

$$\text{II } K = A^b \pmod{p} \quad (\text{Bob})$$

$$B^a \pmod{p} = 3^{11} \pmod{13} = (3^3)^3 \cdot 3^2$$

$$B^k \bmod p = 5 \quad \dots \quad \text{OK}$$

$$= 1^3 \cdot 3^2 = 9 \quad \text{OK.}$$

$$A^b \bmod p = 2^8 \bmod 13 = (2^4)^2$$

$$= 3^2 = 9 \quad \text{OK}$$

OUTPUT: $K = 9$.

El Gamal

- bazat pe generatori ai grupurilor ciclice

Ex.:

I Generarea cheii de criptare

$G = \text{grup ciclic} \quad G = \mathbb{Z}_{11}^*$, $q-1 = 10$

$\Rightarrow q = 11$, $g = \text{generator al lui } G$

$\Rightarrow g = 11$, $g = \text{generator in } \mathbb{Z}_{11}$

$$g = 3$$

$$\begin{array}{c|ccccccccc} \times & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 3^x & 3 & 9 & 5 & 4 & 1 & 6 & 7 & 8 & 9 \end{array}$$

$\Rightarrow \text{ord } 3 = 5$
 $\Rightarrow \mathbb{Z}_{11}^* = \langle 3 \rangle$

$$g = 2$$

$$\begin{array}{c|cccccccc} \times & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 2^x & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \end{array} \boxed{10}$$

$\Rightarrow \mathbb{Z}_{11}^* = \langle 2 \rangle.$

$$e = 1$$

$$\text{Aleg } x \in \{1, 2, 3, \dots, 10\}$$

$$X=5$$

Calanăz: $h = \frac{X}{g} \text{ mod } q = 2 \text{ mod } 11 = 10^5$

Cheia publică: $(\mathbb{Z}_{11}^*, 11, 2, 10)$.

II Criptarea

Mesaj $M \xrightarrow[\text{inversibilitate}]{f} m \in \mathbb{Z}_{11}^*$

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

$$M = 7 \rightarrow f(M) = M = 7$$

Aleg $y \in \{1, 2, \dots, 10\}$

$$y = 7$$

in

$$\text{Calcular } S = h^y \bmod q = 10^7 \bmod 11$$

$$= (-1)^7 = -1 = 10 \quad \underline{\text{public}}$$

Calcular cifral:

$$c_1 = g^y \bmod q = 2^7 \bmod 11 = 7$$

$$c_2 = m \cdot s = 7 \cdot 10 = 70 \bmod 11 = 4$$

$$\text{Cifral } (c_1, c_2) = (7, 4).$$

Mesaj $M = 7 \rightarrow m = 7 \rightarrow (7, 4)$.

III Decifranje:

$$S = c_1^x \bmod q = 7^5 \bmod 11$$

$$r, s, 5 \quad 1, \dots, (-1)^2 \cdot (-1) = 5 \cdot (-1)$$

$$= (-h)^5 \bmod 11 = (-4^2) \cdot (-4) = 5 \cdot (-h)$$

$$= (-100) = -1 = 10,$$

$$s^{-1} \in \mathbb{Z}_{11}^* = 10^{-1} \in \mathbb{Z}_{11}^* = 10$$

Recuperez $m = c_2 \cdot s^{-1} = 4 \cdot 10 = 40 = 7$

$m \xrightarrow{s^{-1}} M = 7$.

RSA

- bazat pe factorizarea nr. m doar 2 divizori, adica $n = p \cdot q$, p, q prime

- în 2024, RSA este considerat sigur
pt $p, q \sim 10^{600}$.

Ex:

I Generarea cheilor de criptare

$$p = 11 \quad \text{prime}$$
$$q = 13$$

$$n = p \cdot q = 143$$

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

Aleg $e \in \{3, 4, 5, \dots, 119\}$ astfel încât

$$\text{cumul}(e, 120) = 1$$

Aleg: $e = 11$.

Calulez exponentul de decifrare

$$d \text{ astfel încât } d \cdot e = 1 \text{ mod } \varphi(n)$$

$$d = 11^{-1} \equiv 11^{120} \pmod{120}$$

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

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

Cheie publică: $(e, n) = (\underline{11}, 143)$

Cheie privată: $(d, n) = (\underline{11}, 143)$.

II Cryptarea

Neraj $m \in \{0, 1, \dots, 142\}$

$$m = 12$$

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

$$= 12^{11} \bmod 143$$

$$= (12^2)^5 \cdot 12 = 12 \cdot$$

Gifel transmis : $c = 12$

III Decipher

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

$$= 12^{11} \bmod 143 = (12^{25} \cdot 12) \bmod 143$$

OK