

Aritmetika in \mathbb{Z}_n

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

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

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

↳ un si ce element este inv. făcă de .."

Z_n = resturile posibile la împărțirea cu n

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

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

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

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

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

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

Pf $x \in \mathbb{Z}_n$, notiz $m - x$ simetricul față de $+$ = oposul lui x

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

$$\text{Ex: } \ln 27 - 3 = y \Leftrightarrow 3 + y = 0 \Rightarrow y = 4$$

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

Notez că x^{-1} este simetricul față de „ \circ ” = inverseul lui x .

pf cù $(\mathbb{Z}_{n_1}, \cdot)$ monoid \Rightarrow x' mu exist' p' rice x.

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

$$\text{Ex: } \exists n \geq 7, \quad 3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = \frac{1}{3} \quad \text{per ca } 3 \cdot 5 = 15 = 14 + 1 = 1.$$

$$6^{-1} = y \Rightarrow 6 \cdot y = 1 \Rightarrow y = 6^{-1} \text{ mit } 6 \cdot 6 = 36 = 35 + 1 = 1$$

11(2) 1971-1972

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 ($\Leftrightarrow \text{cmmdc}(x, n) = 1$)

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

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

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

Ecuatii 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 $\text{cmmdc}(6, 10) = 2 \neq 1$

rezolvu prin incercări

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.

$$3) 4x + 7 = 2 \text{ în } \mathbb{Z}_{10}$$

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

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

\Rightarrow nu are sol.

Ecuatii de gradul al II-lea

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

Sisteme liniare (2x2)

nu se înverzabil

Sisteme liniare (2x2)

| obs: Dacă $\det(\text{matr. sist.}) = 0 \Rightarrow$ rezolv prin incercări

Altfel, pot aplica reducere sau substituții.

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

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

Reducere:

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

$$17x=11 \Rightarrow 3x=4 | \cdot 3^{-1}=5$$

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

Substituție:

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

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

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

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

Inversă matricială

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

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

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

$$\det A = 8+3=11=1 \text{ OK} \Rightarrow \text{există } A^{-1}$$

$$\det A = 8 + 3 - 11 = 1 \text{ or } \Rightarrow \text{exists } A^{-1}$$

(-1) linie + col.

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

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

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

Coduri elementare

Setup:

A	B	C	D	E	F	G	H	I	J
O	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 in $\mathbb{Z}_{26} = \{0, \dots, 25\}$

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 indecifrabile

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

Cifrul Caesar

Varianta flux (stream cipher)

Varianta flux (stream cipher)

↳ aceasi cheie pt tot mesajul

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

Ecuatia de decriptare: $c - K = m$
cod - cheie = mesaj

Ex: mesaj: CIFRU, cheia: 19

$$[c, i, F, R, U] \rightarrow [2, 8, 5, 17, 20] \xrightarrow{\begin{array}{l} \text{+cheie} \\ +19 \end{array}} [21, 27, 24, 36, 39]$$

$\xrightarrow{\text{mod } 29} [21, 27, 24, 7, 10] \rightarrow V. YHK$

CIFRU \rightarrow V. YHK (Caesar)

Decriptare: $[V, Y, H, K] \rightarrow [21, 27, 24, 7, 10] \xrightarrow{\begin{array}{l} -K \\ -19 \end{array}} [2, 8, 5, -12, -9] \xrightarrow{\text{mod } 29} [2, 8, 5, 17, 20] \rightarrow$ CIFRU.

Varianta pe blouri (block cipher): cate o cheie pt fiecare bloc

a) fara padding

b) cu padding

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

$$\Rightarrow b_1 : STIC \quad K_1 = 10$$

$$b_2 : LA?S \leftarrow \text{padding random} \quad K_2 = 20$$

$$[S, T, I, C] \rightarrow [18, 19, 8, 2] \xrightarrow{\begin{array}{l} +K_1 \\ +10 \end{array}} [28, 29, 18, 12] \xrightarrow{\text{mod } 29}$$

$$\rightarrow [28, 0, 18, 12] \rightarrow [?, A, S, M]$$

? - - - ? \rightarrow 107 $+ K_2$ \rightarrow 107

$$\begin{array}{c}
 \text{[L, A, ?, S]} \rightarrow [11, 0, 28, 18] \xrightarrow[\substack{\mod 29 \\ + K_2 \\ + K_0}]{} [31, 20, 48, 38] \\
 \xrightarrow{\mod 29} [2, 20, 19, 9] \rightarrow [C, U, T, J]
 \end{array}$$

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

- Ohs 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).

Cifrul afin

Varianta flux:

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

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

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

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

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

$$\begin{array}{c}
 \text{Decriptarea: } [R, D, M, \cdot] \rightarrow [17, 3, 12, 27] \xrightarrow[\substack{-K_2 \cdot K_1^{-1} \\ -17 \cdot 3^{-1} \\ -17 \cdot 10 \\ +12}]{} [0, -140, -50, 100] \\
 \rightarrow [0, 5, 8, 13] \rightarrow \text{AFIN}
 \end{array}$$

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

$$-140 = -116 - 29 = -29 = 5 \quad -50 = -29 - 21 = -21 = 8$$

$$29 \cdot 5 = 145 \quad 100 = 87 + 13 = 13$$

Varianta pe lăzuri

- cite 2 chei pt fiecare lăz
etc

Cifrul Hill

Ecuția de criptare : $\begin{matrix} \text{cheie} \\ \uparrow \\ \text{matrice} \end{matrix} \cdot \begin{matrix} \text{mesaj} \\ \uparrow \\ \text{vector} \end{matrix} = \text{cod}$

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

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

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

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

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

ROZ \rightarrow DCL (Hill)

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

$$\dots, t \begin{pmatrix} 1 & 2 & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 & -1 \end{pmatrix}$$

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

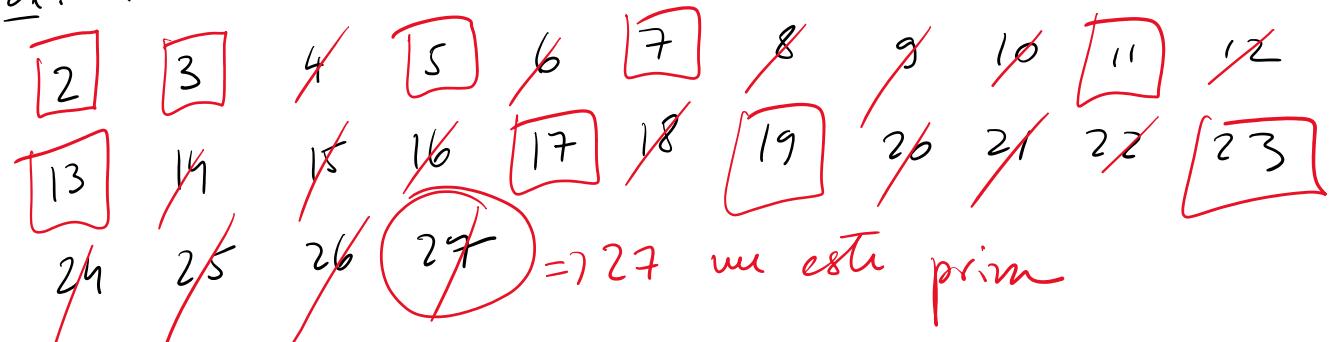
$$K^{-1} = (\det K)^{-1} \cdot K^* = \begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 11 \end{pmatrix} = \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} \pmod{2}$$

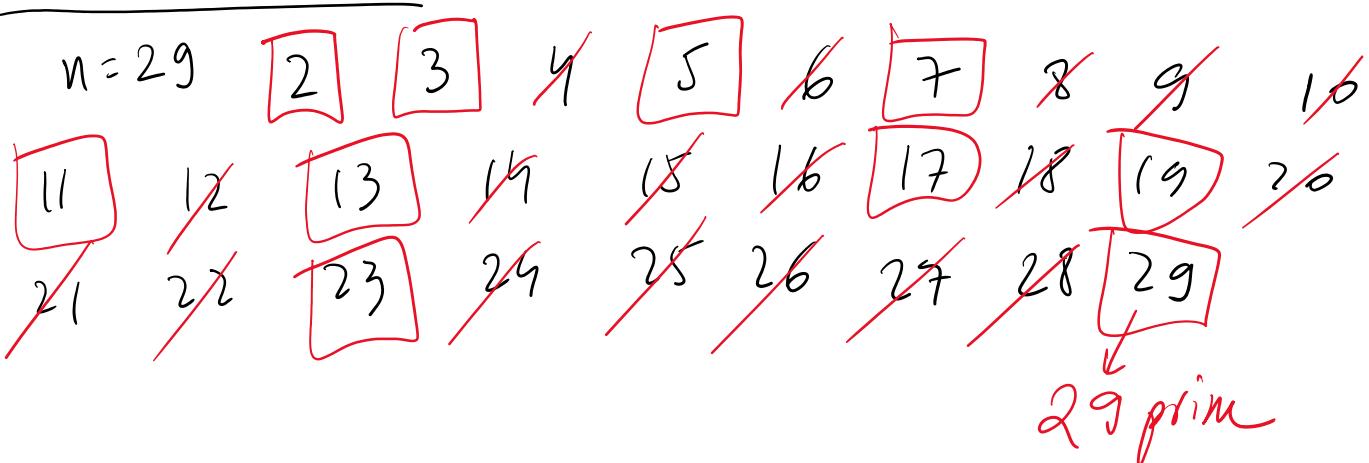
Teste de primalitate

1) Ciurul (sita) lui Eratostene (≈ Greaca antică)

Ex: $n = 27$



⇒ lista de nr prime $\leq n$



Testul Fermat

Testul Fermat

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

Dacă n este prim $\Rightarrow \forall 0 < a < n, a^{n-1} \equiv 1 \pmod{n}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$a=2 \Rightarrow 2^{14} = (2^4)^3 \cdot 2^2 = 16^3 \cdot 2^2 = 1 \cdot 2^2 = 4 \neq 1 \text{ STOP.}$$

$\therefore 15$ nu este prim / $a=2$ martor [witness] = contrarezemplu

u

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

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

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

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

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

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

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

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

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

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

$$(fără deja)$$

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

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

Testul Solovay - Strassen (sec XX)

Simbolul Jacobi

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

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

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

exista $\sqrt{b \bmod n} \in \mathbb{Z}_n$

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

$$\left(\frac{6}{3}\right) = ? \quad \text{pt ca } 3|6$$

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

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

Teorema (Solovay-Strassen)

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

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

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

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

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

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

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

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

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

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

$$\left(\frac{3}{8}\right) = -1$$

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

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

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

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

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

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

$$a=9 : 9^8 = (3^4)^2 = 1 \quad ; \quad \left(\frac{9}{17}\right) = 1 \text{ pt ca } 9 = 3^2 \checkmark$$

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

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

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

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

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

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

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

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

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

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

Logaritmul discret

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	$\left(\begin{matrix} 5 \\ 1 \end{matrix}\right)$	6	7	8	9	10
3^x	3	9	5	4	(1)	3	9	5	4	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	$\left\{ \begin{matrix} 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \\ 12 \end{matrix} \right.$			
5^x	5	12	8	1				1

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

$\log_5 8 = 3$ în \mathbb{Z}_{13} .

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

Def 1) Ordinal unui grup = nr. de elemente al 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 $\text{ord } x = \infty$.

Dacă nu există $(x \neq 1, \forall t)$, pentru care $x^t = 1$.

Ex: $\text{ord} 3 = 5$ în \mathbb{Z}_7 , și $\text{ord} 5 = 4$ în \mathbb{Z}_{13} (rezultatul este corect).

Teorema (Lagrange)

În \mathbb{Z}_p^* , ordinul 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^* sună grup ciclic, iar elementul = generator.

Ex: Este \mathbb{Z}_7^* ciclic?

x	1	2	3	4	5	6
$2x$	2	4	1			
$3x$	3	2	6	4	5	1
$4x$	4	1				
$5x$	5	4	6	2	3	1

$\Rightarrow \text{ord}(2) = 3$

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

$\Rightarrow \mathbb{Z}_7^*$ ciclic, 3 generatori

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

Obs: Dacă există generatori
nu este unic.

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

Indicatorul lui Euler (Euler's TOTIENT function)

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

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

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

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

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

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

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 $n = pq$

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

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

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

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

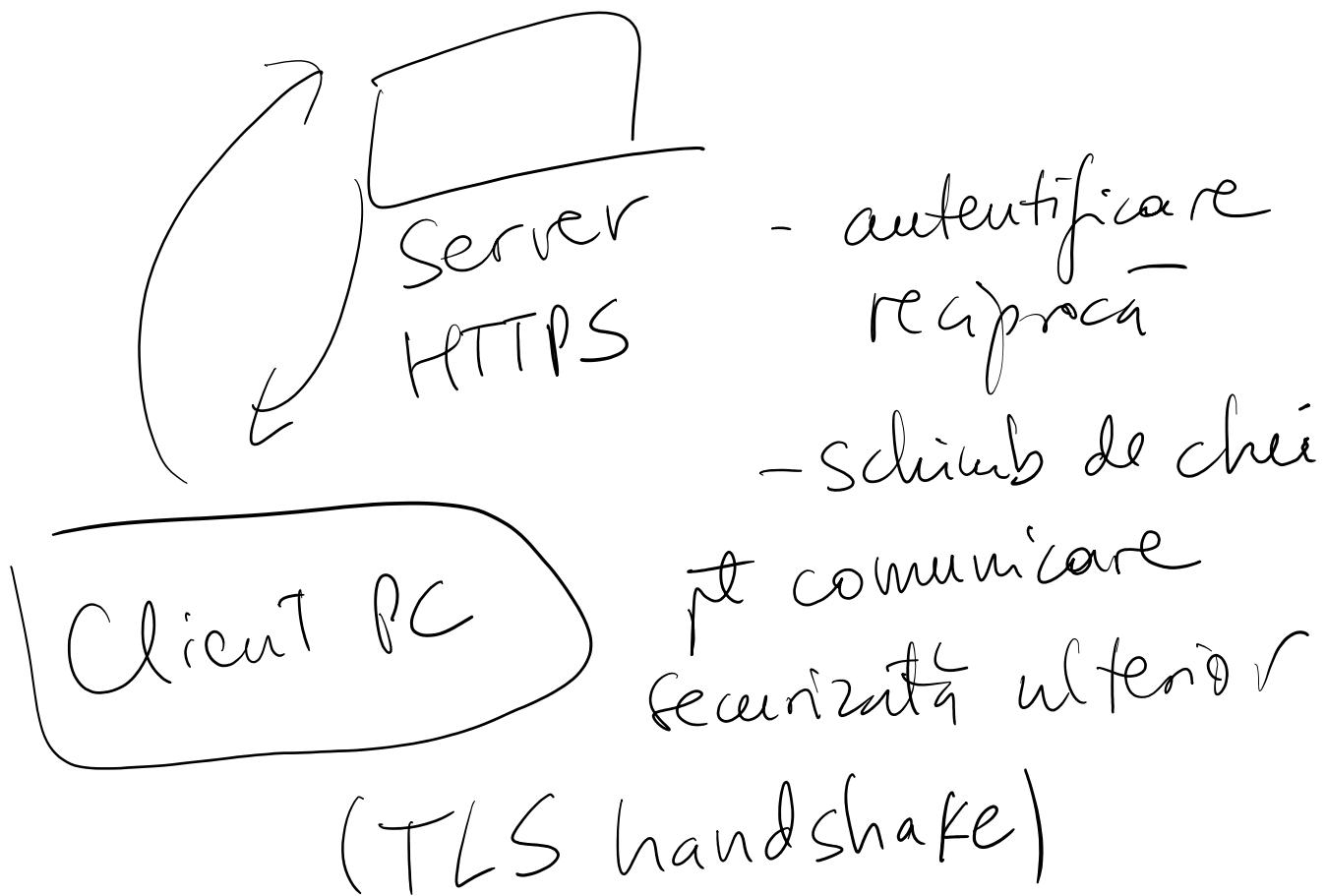
$$342 = 2 \cdot 3^2 \cdot 19$$

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

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

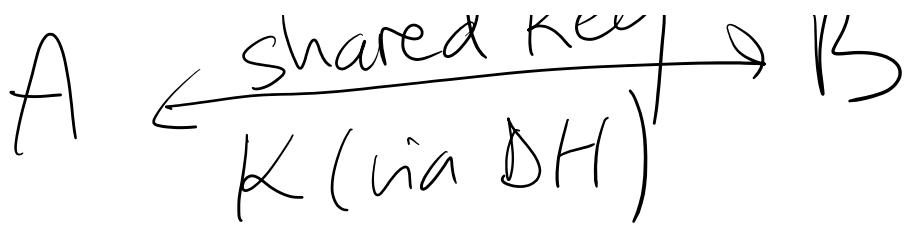
Diffie - Hellman

- se bazează pe log discret ($\log \in \mathbb{Z}_n$)
- ne cripteză mesajele și stabilește un canal securizat de comunicare



Diffie - Hellman produce o cheie comună pt partile comunicante.

A $\xleftarrow{\text{shared Key}}$ B



Ex:

- 1) Alice: cheic ~~pirata~~ $a = 7$
- 2) Bob: cheic ~~pirata~~ $b = 4$
- 3) p prim , $p = 11$ } public
 $\alpha \in \mathbb{N}$, $\alpha = 10$ }
- 4) Cheia publică a lui Alice:
 $A = \alpha^a \bmod p = 10^7 \bmod 11$
 $a = \log_{\alpha} A = (-1)^7 \bmod 11 = -1 = 10$
- 5) Cheia publică a lui Bob:
 $b = \log_{\alpha} B$, $b = 4$ and $n = 10^4 \bmod 11 = 1$

$$b = \log_2^P \leftarrow B = x^b \text{ mod } p = 10^4 \text{ mod } 11 = 1$$

6) Cheie comună (Shared Key), publică

$$K = B^a \text{ mod } p = A^b \text{ mod } p$$

$$\begin{matrix} 1 & \text{mod } 11 = 1 \\ 10^4 & \text{mod } 11 = 1 \end{matrix} \quad \left. \begin{array}{c} \uparrow \\ \downarrow \end{array} \right\} K$$

$K = 1$

El Gamal

Se bazează pe generatori și gr. ciclice

I. Generarea cheii de criptare

G grup ciclic , $G = \mathbb{Z}_7^*$

U gruppen
g generator $g = 3$

Vorfrage:

x	1	2	3	4	5	6	
$3x$	3	2	6	4	5	1	OK

ordinul lui \mathbb{Z}_7^* este $7-1=6$

$$\Rightarrow q=7 \quad ; \quad e=1$$

Aleg $x \in \{1, 2, 3, 4, 5, 6\}$

$$\underline{x=3}$$

$$\text{Calculez } h = g^x \bmod q = 3^3 \bmod 7 \\ = 6$$

$$\text{Cheia pública} = (G, g, h)$$

~~G~~

$$= (\mathbb{Z}_7^*, 7, 3, 6)$$

$$\text{Cheia privada: } X = 3.$$

~~X~~

II Criptarea

$$M = 51 \xrightarrow{\text{mod}} m \in \mathbb{Z}_7^*$$

$$m = M \bmod 7 = 51 \bmod 7 = 2$$

Aleg $y \in \{1, 2, 3, 4, 5, 6\}$

$$S = h^y \bmod q = 6^5 \bmod 7 = -1 = 6$$

$$y = 5$$

$$1^5 - 3^5 \bmod 7 = 5$$

$$c_1 = g^y \mod q = 3^3 \mod 7 = 5$$

$$c_2 = m \cdot s = 2 \cdot 6 = 12 \mod 7 = 5$$

Cifru: $M = 51 \rightarrow (5, 5)$. public.

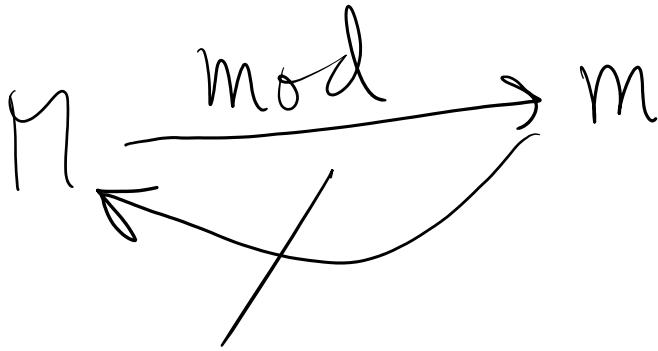
III Decriptarea

$$\begin{aligned} s &= c_1 \mod q = 5^3 \mod 7 \\ &= (2)^3 = -8 = -1 = 6 \end{aligned}$$

$$s^{-1} \text{ in } \mathbb{Z}_7^* = 6^{-1} \text{ in } \mathbb{Z}_7^* = 6$$

$$m = c_2 \cdot s^{-1} = 5 \cdot 6 = 30 = 2$$

Obs: Operația modulo NU este inversabilă.



RSA

- se bazează pe factorizare pt
numere (mari) de forma

$$n = p \cdot q \quad p, q \text{ prime}$$

- în 2024, se folosesc $p, q \approx 10^{600}$

Generarea cheilor:

$$p = 5$$

$$q = 7$$

prime ~~private~~

$$n = 5 \cdot 7 = 35 \quad \text{modul de criptare public}$$

$$n = 5 \cdot 7 = 35$$

~~public~~

$$\varphi(n) = \varphi(5 \cdot 7) = \varphi(5)\varphi(7) = 4 \cdot 6 = 24$$

Exponent de criptare

$$e \in \{3, 4, 5, \dots, 23\} \text{ a.i.}$$

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

$$(e \in U(\mathbb{Z}_{\varphi(n)}^*))$$

$$e = 5$$

Exponent de decriptare

$$d \text{ a.i. } d \cdot e \equiv 1 \pmod{\varphi(n)}$$

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

$\Rightarrow d = e^{-1} \text{ mod } \varphi(n)$

$$5^{-1} \text{ in } \mathbb{Z}_{24}^* = 5$$

Cheie publică: $(e, n) = (5, 35)$

Cheie pirată: $d = 5$

Criptarea

Mesaj: $m = 3$

Cifrul (codul)

$$c = m^e \text{ mod } n = 3^5 \text{ mod } 35$$

$$= 3^4 \cdot 3 = 81 \cdot 3 = 33$$

10. - 25 RSA $\rightarrow c = 33$

$$m = 33 \xrightarrow{\text{RSA}} c = 33$$

Decryption

$$m' = c^d \bmod n = ?$$

$$= 33^5 \bmod 35$$

$$= (-2)^5 = -32 = 3 = m$$