

Aritmetică în \mathbb{Z}_n

Ecuații de gradul I \rightarrow CAESAR
AFIN

Ex: $5x + 1 = 3 \text{ în } \mathbb{Z}_7$

$$5x = 3 - 1 = 2 \quad | \cdot 5^{-1} = 3$$

$$\underbrace{5 \cdot 3 \cdot x}_{1} = 2 \cdot 3 \Rightarrow \underline{1x = 6}$$

Ex: $6x + 2 = 1 \text{ în } \mathbb{Z}_{10}$

$$6x = 1 - 2 = -1 = 9 \quad | \cdot 6^{-1} \text{ NU există în } \mathbb{Z}_{10}$$

Teoremă: x^{-1} există în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(x, n) = 1$

$6x = 9$ 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

\Rightarrow ec m
are sol.

Sisteme liniare

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

Matricea sistemului: $A = \begin{pmatrix} 2 & 3 \\ 5 & -1 \end{pmatrix} \in M_2(\mathbb{Z}_7)$

$$\det A = -2 - 15 = -17 = -14 - 3 = -3 = 4 \in U(\mathbb{Z}_7)$$

\Rightarrow sistem hamer \Rightarrow sol. unică.

$$\begin{cases} 2x + 3y = 1 \\ 5x - y = 2 \end{cases} \cdot 3 \Rightarrow \begin{cases} 2x + 3y = 1 \\ 15x - 3y = 6 \end{cases} \Rightarrow \begin{aligned} 17x &= 7 \\ 3x &= 0 \\ \Rightarrow x &= 0 \end{aligned}$$

(+)

$$5 \cdot 0 - y = 2 \Rightarrow \underline{y = -2 = 5}$$

Ex: $\begin{cases} 2x + y = 3 \\ 4x + 2y = 1 \end{cases} \in \mathbb{Z}_{11}$

$$A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_{11}) \Rightarrow \det A = 0 \Rightarrow \text{sist. nu este hamer.}$$

$$\begin{cases} 2x + y = 3 \cdot 2 \\ 4x + 2y = 1 \end{cases} \Rightarrow \begin{cases} 4x + 2y = 6 \\ 4x + 2y = 1 \end{cases}$$

$$\Rightarrow 0 = 5 \Rightarrow \text{incompat.}$$

Def: $a \mid b \in X \Leftrightarrow \exists c \in X \text{ a.i. } a \cdot c = b$

Ecuații de gradul II

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

$$a=3; b=-1; c=2$$

$$\Delta = b^2 - 4ac = 1 - 4 \cdot 2 \cdot 3 = 1 - 24 = -23 \stackrel{0}{=} -21 - 2 \\ = -2 = 5$$

$$\exists \sqrt{5} \text{ în } \mathbb{Z}_7? \quad \sqrt{5} = y \Leftrightarrow y^2 = 5$$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} \quad \underset{\substack{\uparrow \\ \text{potențiale}}}{P(\mathbb{Z}_7)} = \{0, 1, 4, 2\} \neq 5$$

$\Rightarrow \nexists \sqrt{5} \text{ în } \mathbb{Z}_7 \Rightarrow$ nu are soluție.

$$\text{Ex: } x^2 - 5x + 7 = 1 \stackrel{\text{în } \mathbb{Z}_{11}}{=} \Leftrightarrow x^2 - 5x + 6 = 0 \text{ în } \mathbb{Z}_{11}$$

$$a=1; b=-5; c=6$$

$$\Delta = b^2 - 4ac = 25 - 24 = 1$$

$$2^{-1} \text{ în } \mathbb{Z}_{11} = 6$$

$$\sqrt{1} \in \{1, 10\}$$

$$x_1 = (5 + 1) \cdot 2^{-1} = 6 \cdot 6 = 36 \stackrel{0}{=} 33 + 3 = 3$$

$$x_2 = (5 - 1) \cdot 2^{-1} = 4 \cdot 6 = 24 = 22 + 2 = 2$$

$$x_3 = (5 + 10) \cdot 2^{-1} = 15 \cdot 6 = 90 = 88 + 2 = 2$$

$$x_4 = (5 - 10) \cdot 2^{-1} = -5 \cdot 6 = -30 = -22 - 8 = -8 = 3$$

NU
enumere

Inverse matriciale \rightarrow HILL

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \in M_3(\mathbb{Z}_5)$ $A^{-1} = ?$ dacă există

$$\det A = \underbrace{1+4}_0 - 1 + 2 = 1 \in U(\mathbb{Z}_5)$$

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

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 1 \cdot \begin{pmatrix} -3 & 3 & 3 \\ 2 & 0 & 2 \\ -1 & 3 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 3 \\ 2 & 0 & 2 \\ 4 & 3 & 4 \end{pmatrix}$$

$$A^{-1} \cdot A = A \cdot A^{-1} = I_3$$

Ex: $A = \begin{pmatrix} 2 & -1 & 3 \\ 5 & 2 & 1 \\ 7 & 1 & 4 \end{pmatrix} \in M_3(\mathbb{Z}_{11})$ $A^{-1} = ?$ dacă există

$$\det A = 16 - 7 + 15 - 42 - 2 + 20$$

$$= 5 + 4 + 4 + 2 - 2 - 2 = 11 = 0 \Rightarrow \nexists A^{-1}$$

Logarithm discret \rightarrow DIFFIE-HELLMAN

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

Ex. $\log_2 5 \in \mathbb{Z}_7$

$$\log_2 5 = x \Leftrightarrow 2^x = 5 \in \mathbb{Z}_7$$

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

$\nearrow \text{ord } 2 = 3$ $\neq 5$

$\Rightarrow \log_2 5$ nu exista in \mathbb{Z}_7 .

Teorema lui Lagrange pt grupuri

G grup finit, cu n elemente.

$\forall g \in G, \text{ord } g \mid n$

In particular, $g^n = e$, elem. neutru.

Multiplicativ, lucram in $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$

$$\# \mathbb{Z}_n^* = n-1 \Rightarrow \forall x \in \mathbb{Z}_n^*, x^{n-1} = 1$$

Ex: $\log_3 2$ în \mathbb{Z}_{11}

$\log_3 2 = x \Leftrightarrow 3^x = 2$ în \mathbb{Z}_{11}

Sol 1: Calculăm puterile

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

$\rightarrow \text{ord } 3 = 5$ în \mathbb{Z}_{11}

$3^4 = 3^3 \cdot 3 = 5 \cdot 3 = 15 = 4$

$3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 1$

$\Rightarrow \log_3 2$ nu există în \mathbb{Z}_{11}

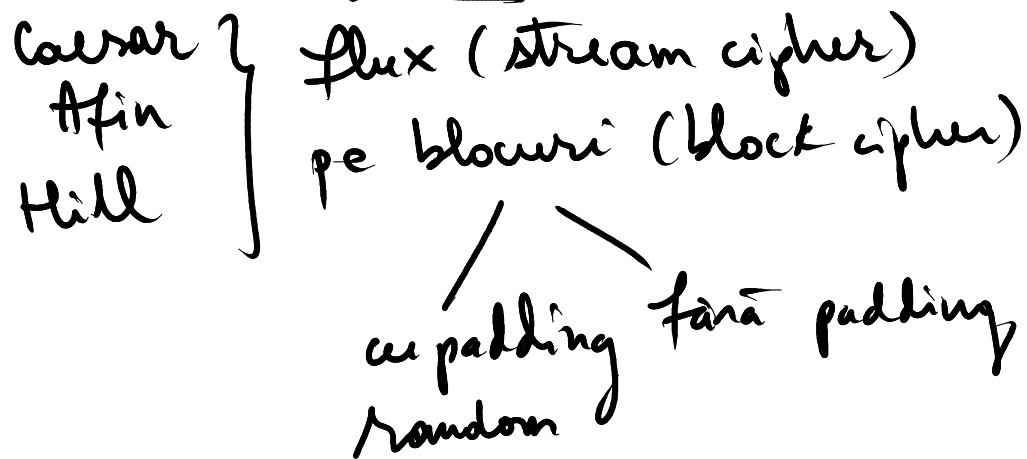
Sol 2: $3^x = 2$ în $\mathbb{Z}_{11} \Leftrightarrow 3^x = 11K + 2$

Enumerăm elem. $11K + 2$ și vom avea o putere a lui 3

$11K + 2 = \{2, 13, 24, 35, 46, \dots, 3^{10} \sim 50,000\}$

↑
Cont puterile de puteri ale lui 3

Algoritmi criptografici



A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
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				

Adaug ? \Rightarrow lucrăm în \mathbb{Z}_{29}
26 27 28

Caesar - flux: o cheie pt tot mesajul

Ecuația de criptare: $m + K = C$, $\forall m \in \text{Mesaj}$
K cheie
 $C \in \text{Cod}(C_{\text{fun}})$

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

$\text{Enc}(m) = m + K$; $\text{Dec}(C) = C - K$

Ex: Mesaj: LABORATOR
cheie: $K=15$

$$[L, A, B, O, R, A, T, O, R] \rightarrow [11, 0, 1, 14, 17, 0, 19, 14, 17]$$
$$\xrightarrow[+15]{+K} [26, 15, 16, \underline{29}, \underline{32}, 15, \underline{34}, \underline{29}, \underline{32}] \xrightarrow{\text{mod } 29}$$

$$[26, 15, 16, 0, 3, 15, 5, 0, 3] \rightarrow _P Q A D P E A D$$

Conduziu: LABORATOR $\xrightarrow[\text{Caesar}]{+15}$ $_P Q A D P E A D$.

Decriptare: $[_P, Q, A, D, P, E, A, D] \rightarrow [26, 15, 16, 0, 3, 15, 5, 0, 3]$

$$\xrightarrow[-15]{-K} [11, 0, 1, -15, -12, 0, -10, -15, -12] \xrightarrow{\text{mod } 29}$$

$$[11, 0, 1, 14, 17, 0, 19, 14, 17] \rightarrow \text{LABORATOR}$$

Caesar pe blocuri, fără padding

o cheie/bloc cel mult un bloc mai scurt

Ex: Mesaj: LABORATOR \Rightarrow LABOR, $K_1=15$
 bloc: 5 ATOR, $K_2=11$

$$[L, A, B, O, R] \rightarrow \text{LPQAD}$$
$$[A, T, 0, R] \rightarrow [0, 19, 14, 7] \xrightarrow[\substack{+K^2 \\ +11}]{\substack{+K^2 \\ +11}} [11, 30, 25, 18] \xrightarrow{\text{mod } 29}$$
$$[11, 1, 25, 18] \rightarrow \text{LBZS}$$

LABORATOR $\xrightarrow[\text{pe blonni}]{\text{Caesar}}$ PQADLBZS

Caesar pe Yawon, ce padding random

Ex. Mesg: MARTI → MAR
 Bloc: 3 TIE → padding random

$$K_1 = 5; \quad K_2 = 10$$
$$[M, A, R] \rightarrow [12, 0, 17] \xrightarrow[+5]{+K!} [17, 5, 22] \rightarrow \text{RFW}$$
$$[\tau, i, E] \rightarrow [19, 84] \xrightarrow[\substack{+K^2 \\ +10}]{\quad} [29, 18, 14] \xrightarrow{\text{mod } 29} [0, 18, 14]$$

→ ASo

MARTIE \rightarrow RFWASO

padding Levine Zgomot

Cifrul afin - varianta flux

Ec. de criptare: $m \cdot K_1 + K_2 = C, \forall m \in \text{Mesaj}$
 $K_1, K_2 \text{ chei}$
 $C \in \text{Cod}$

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

Ex: Mesaj: CRIPTO ; $K_1 = 7$; $K_2 = 13$

$$[C, R, I, P, T, O] \rightarrow [2, 17, 8, 15, 19, 14] \xrightarrow{\cdot K_1 + K_2} \xrightarrow{\cdot 7 + 13}$$

$$[27, 132, 69, 118, 146, 111] \xrightarrow{\text{mod } 29}$$

$$[27, 16, 11, 2, 1, 24] \rightarrow [., Q, L, C, B, Y]$$

$$132 = 116 + 16 = 16$$

$$\rightarrow .QLCBY$$

$$4 \cdot 29 = 116$$

$$\text{Decriptare: } [., Q, L, C, B, Y] \rightarrow [27, 16, 11, 2, 1, 24]$$

$$\xrightarrow{-13 \cdot 7^{-1}} \xrightarrow{-13 \cdot 25} [350, 75, -50, -275, -300, 275] \xrightarrow{\text{mod } 29}$$

$$[2, 17, 8, 15, 19, 14] \rightarrow \text{CRIPTO.}$$

Hill - Flux

Ec. de criptare:
$$\begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix} \cdot \begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} C \\ 0 \\ D \end{pmatrix}$$

Ec. de decriptare:
$$\begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix}^{-1} \cdot \begin{pmatrix} C \\ 0 \\ D \end{pmatrix}$$

Matricea de criptare $\in M_3(\mathbb{Z}_{29})$, inversabilă

Mesaj, Cod $\in M_{3,1}(\mathbb{Z}_{29})$

Ex: Mesaj: YES ; Mat. cr. $= \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} = A$

$$\det(A) = -1 - 8 + 2 = -7 = 22$$

$$\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}; \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} -24 + 8 + 18 \\ 4 + 36 \\ -48 + 18 \end{pmatrix}$$

$$= \begin{pmatrix} 2 \\ 40 \\ -30 \end{pmatrix} \bmod 29 = \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = CL?$$

Scriptare $A^{-1} = ?$

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

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 22^{-1} \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix}$$

$$\text{Mesaj} = \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = \begin{pmatrix} Y \\ E \\ S \end{pmatrix}$$

Ex de examen: Criptat în Caesar - flux numele de familie, cu cheia = prenume (sau invers).

Mesaj: MANEA

M A N E A \leftarrow m

+ + + + +
A D R I A \leftarrow k

Chia: ADRIAN

$$\begin{array}{r} 12 \quad 0 \quad 13 \quad 4 \quad 0 \\ + \quad 0 \quad 3 \quad 17 \quad 8 \quad 0 \\ \hline 12 \quad 3 \quad 30 \quad 12 \quad 0 \end{array}$$

$\rightarrow 12, 3, 1, 12, 0 = \dots$

Temă: 1) Criptare cu Caesar - flux

Mesaj: Numele de familie

+ decriptare

Cheie: Luna nașterii

2) Criptare cu Caesar pe blocuri fără padding

Mesaj: Prenume; $b=3$; Cheie: ultimele cifrele
din nr. de telefon.

+ decriptare

3) Criptare cu afin - flux, Mesaj = Orasul de naștere,

K_1 = luna de naștere, K_2 = ziua de naștere

+ decriptare

4) Hill: Mesaj: Joi; $MC = \begin{pmatrix} -2 & 1 & 0 \\ 2 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$.

+ decriptare

Teste de primalitate

INPUT: $n \in \mathbb{N}$, impar

OUTPUT: n prim/compus

- 1) Cercul / Sita lui Eratostene
- 2) Testul Fermat
- 3) Testul Solovay - Strassen

→ Teste deterministe (sigure)

+ sigure

- ineficiente

→ Teste probabiliste

+ eficiente

- probabiliste

+/- sigur nu, probabil da

Cercul lui Eratostene - sigur

INPUT: $n \in \mathbb{N}$

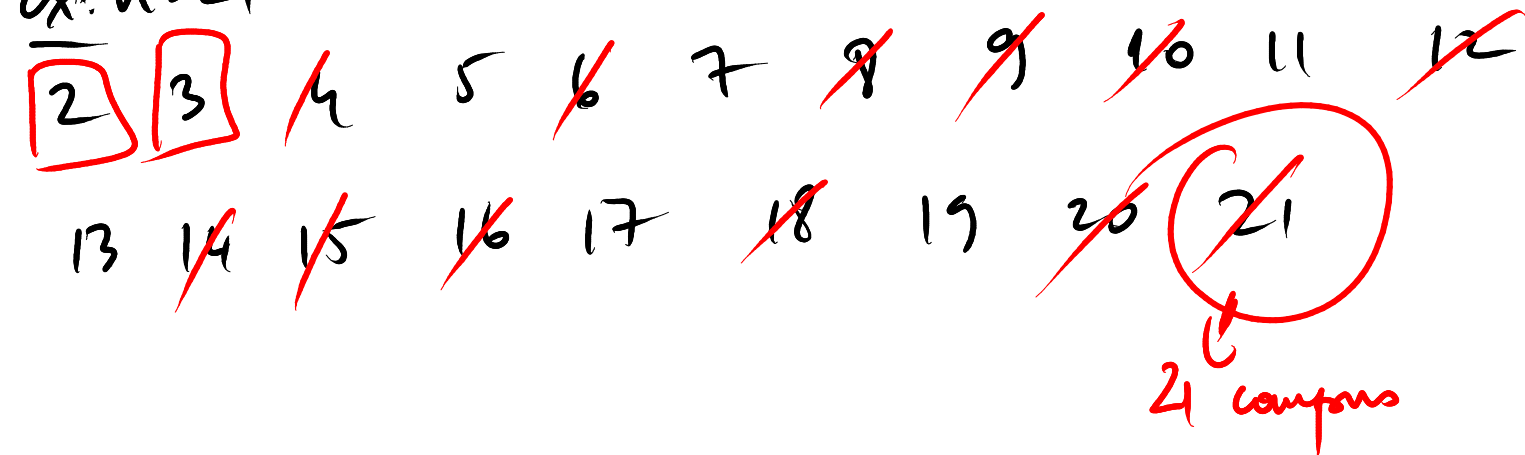
OUTPUT: lista de nr prime $\leq n$

Ex: $n = 20$

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	

OUTPUT: 2, 3, 5, 7, 11, 13, 17, 19 prime ≤ 20

Ex: $n=21$



Testul Fermat - Varianta sigură

Mica Teoremă a lui Fermat

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

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

Exemplu: $n=7 \stackrel{?}{\Rightarrow} a^{7-1} = 1 \in \mathbb{Z}_7^*$

$$a=1 \Rightarrow 1^6 = 1 \text{ OK}$$

$$a=2 \Rightarrow 2^6 = 64 = 63 + 1 = 1 \text{ OK}$$

$$a=3 \Rightarrow 3^6 = (3^2)^3 = 2^3 = 1 \text{ OK}$$

$$a=4 \Rightarrow 4^6 = (2^2)^6 = (2^6)^2 = 1^2 = 1 \text{ OK}$$

$$a=5 \Rightarrow 5^6 = (-2)^6 = 2^6 = 1 \text{ OK}$$

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

$\Rightarrow n=7$ prim (cf. Fermat)

Varianta probabilită

Aleg t mostre pentru $a \in \mathbb{Z}_n^*$ și verificăm dacă $a^t = 1$ în \mathbb{Z}_n .

Ex: $n=11$, $t=3$, $a \in \{3, 5, 8\}$

$a^{10} = 1 \stackrel{?}{\in} \mathbb{Z}_{11}^*$?

$$3^{10} = (3^2)^5 = 9^5 = (-2)^5 = -32 = -33 + 1 = 1 \quad \text{ok}$$

$$5^{10} = (5^2)^5 = 3^5 = 3^2 \cdot 3^2 \cdot 3 = (-2) \cdot (-2) \cdot 3 = 12 = 1 \quad \text{ok}$$

$$8^{10} = (-3)^{10} = 3^{10} = 1 \quad \text{ok}$$

$\Rightarrow n=11$ probabil prin $p = \frac{3}{10} = 30\%$.

Ex: $n=9$, $t=3$ mostre, $a \in \{2, 3, 4\}$

$a=2 \Rightarrow 2^8 = 1 \stackrel{?}{\in} \mathbb{Z}_9^*$?

$$2^8 = (2^3)^2 \cdot 2^2 = (-1)^2 \cdot 4 = 4 \neq 1$$

$\Rightarrow n=9$ compus (sigur!)

$a=2$ witness (martor)

Simbolul Jacobi

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

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

Ex: $\left(\frac{3}{7}\right) = ?$ $7 \nmid 3$

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

\mathbb{Z}_7

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

Ex: $\left(\frac{4}{11}\right) = ?$ $11 \nmid 4$
 $4 = 2^2 \Rightarrow \left(\frac{4}{11}\right) = 1$

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

Deci $\left(\frac{18}{3}\right) = \left(\frac{0}{3}\right) = 0$ $\text{pt că } 3 | 0$.

Testul Solovay-Strassen

Teoremă: n prim $\Rightarrow b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \approx \pm 1$
 $\forall b \in \mathbb{Z}_n^*$

Ex: $n=7 \Rightarrow b^{\frac{7-1}{2}} = b^3 = \left(\frac{b}{7}\right), \forall b \in \mathbb{Z}_7^*$?

$b=1 \Rightarrow 1^3 = 1; \left(\frac{1}{7}\right) = 1$ pt că $1=1^2$ OK

$b=2 \Rightarrow 2^3 = 8 = 1; \left(\frac{2}{7}\right) = 1$ pt că $2=3^2=4^2$ OK

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

$b=3 \Rightarrow 3^3 = 27 = 6 = -1; \left(\frac{3}{7}\right) = -1$ OK

$b=4 \Rightarrow 4^3 = (2^2)^3 = (2^3)^2 = 1; \left(\frac{4}{7}\right) = 1$ pt că $4=2^2$ OK

$b=5 \Rightarrow 5^3 = 5^2 \cdot 5 = 4 \cdot 5 = 6 = -1; \left(\frac{5}{7}\right) = -1$ OK

$b=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot (-1) = -1; \left(\frac{6}{7}\right) = -1$ OK

$\Rightarrow n=7$ prim.

Ex: $n=15 \Rightarrow \forall a \in \mathbb{Z}_{15}^*, a^{\frac{15-1}{2}} = a^7 = \left(\frac{a}{15}\right) ?$

$a=1$ OK

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

$\Rightarrow n=15$ Compus, $a=2$ mantor.

Solovay-Strassen probabilist

Alg + master $b \in \mathbb{Z}_n^*$ of test $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right)$.

Ex: $n=17$, $t=3$, $a \in \{5, 9, 13\}$

$$a=5 \Rightarrow 5^{\frac{17-1}{2}} = 5^8 = \left(\frac{5}{17}\right) \in \mathbb{Z}_{17}^*$$

$$5^8 = 5^3 \cdot 5^3 \cdot 5^2 = 125 \cdot 125 \cdot 5^2 = 6 \cdot 6 \cdot 5^2$$

$$119 = 17 \cdot 7$$

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

$$= 2^2 \cdot 15^2 \quad \text{OK}$$

$$= 2^2 \cdot (-2)^2$$

$$= 4 \cdot 4 = 16 = 1$$

$$= 4^4 = 16 \cdot 16 = 1 \cdot 1 = 1 \quad \text{OK}$$

$$g = 3^{16} = (3^4)^4 = 81^4 = (-4)^4 = 4^4 = 16 \cdot 16 = 1 \cdot 1 = 1$$

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

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

x	11	12	13	14	15	16
x ²	2	8	16	9	4	1

$$\left(\frac{9}{17}\right) = 1 \text{ pt c\u0103 } 9 = 3^2$$

$$13^8 = (-4)^8 = 4^8 = (4^2)^4 = (-1)^4 = 1$$

$$\left(\frac{13}{17}\right) = 1 \text{ pt c\u0103 } 13 = 8^2 = 9^2 \text{ OK}$$

Concluzie: $n=17$ probabilitate prim, $p = \frac{3}{16}$.