

1342b

Aritmetică în Z_n : $(Z_n, +, \cdot)$ este comutativ
 $\{Z_n, +\}$ grup comutativ
 $\{Z_n - \{0\}, \cdot\}$ monoid
 L'nu orice element este inversabil

Ex: $(Z_7, +, \cdot)$

$$\begin{aligned} 2+3 &= 5 \quad (\Rightarrow 16+17=12 \Rightarrow 23+3=5 \text{ etc. (in } Z_7)) \\ 2 &= \{7k+2 \mid k \in \mathbb{Z}\} = \{2, 9, 16, 23, \dots\} \quad \text{modulo 7} \\ 3 &= \{7k+3 \mid k \in \mathbb{Z}\} = \{3, 10, 17, 24, \dots\} \\ 5 &= \{7k+5 \mid k \in \mathbb{Z}\} = \{5, 12, 19, 26, \dots\} \end{aligned}$$

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\} \rightarrow \text{reprezentanți}$$

0 = element neutru la + $\Rightarrow x+0=x, \forall x \in Z_7$

Notez: $-x$ simetricul (inverseul) lui x față de $+$
 $-x$ se mai numește opusul lui x .

Def: $-x = y \Leftrightarrow y+x=0$

$$-2=y \Leftrightarrow y+2=0=\{7k \mid k \in \mathbb{Z}\} \Rightarrow y=5$$

$$\text{Obs: } -2=0-2=7-2=14-2=\dots \quad \text{pt că}\\ 0 = \text{multiplu de 7}$$

$$\text{Înmulțirea: } 2 \cdot 3 = 6 \Rightarrow 9 \cdot 24 = 13 \Rightarrow 16 \cdot 10 = 34 \text{ etc}$$

Def: x^{-1} = simetricul lui x față de \cdot = invers

Obs: $(Z_n, +, \cdot)$ este $\Rightarrow x^{-1}$ nu există pentru orice x .

Def: $U(Z_n) = \{x \in Z_n \mid \text{există } x^{-1}\} = \text{unități}$

Teorema: x este unitate în $Z_n \Leftrightarrow \text{cumod}(x, n) = 1$

$$\Rightarrow U(Z_n) = \{x \in Z_n \mid \text{cumod}(x, n) = 1\}$$

Obs: Dacă n este număr prim $\Rightarrow U(Z_n) = Z_n - \{0\} = Z_n^*$

Cum căutați x^{-1} ?

Ex: În Z_7 , $U(Z_7) = Z_7^*$ pt că 7 este prim.

$$2^{-1}=y \Leftrightarrow 2 \cdot y = 1 \Leftarrow \text{el. neutru la } \cdot \\ y=4 \quad \text{pt că } 2 \cdot 4 = 8 = 1.$$

Ecuatii de gradul I

$$1) 5x+2=1 \text{ in } Z_7 = \{0, 1, \dots, 6\}$$

$$5x+2-2=-1=6 \quad | \cdot 5^{-1}=3$$

$$3 \cdot 5 \cdot x = 6 \cdot 3 \quad | \cdot x=4 \quad \text{pt că } 3 \cdot 4 = 12 = 1.$$

$$2) 3x+1=7 \text{ in } Z_9 = \{0, 1, 2, \dots, 8\}$$

$$3x+1-1=6 \quad | \cdot 3^{-1} \text{ NU EXISTĂ IN } Z_9 \quad \text{pt că cumod}(3, 9)=3+1 \\ \Rightarrow 3 \notin U(Z_9)$$

Razoluție numărătore:

$$\begin{aligned} x=0 &\text{ NU; } x=1 \text{ NU; } x=2 \text{ OK; } x=3 \text{ NU; } x=4 \text{ NU; } x=5 \text{ OK; } \\ x=6 \text{ NU; } x=7 \text{ NU; } x=8 \text{ OK} \end{aligned}$$

Ecuatii de gradul II

$$\text{Ex: } 2x^2-5x+1=0 \text{ in } Z_7 = \{0, 1, \dots, 6\}$$

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

Există $\sqrt{3}$?

$$\text{dacă } \sqrt{3}=y \Leftrightarrow \Delta=y^2$$

Există $\sqrt{3}$ in $Z_7 \Leftrightarrow$ există $a \in Z_7$ ai cărui $a^2=3$.

$$\begin{array}{c|cccccc} a & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline a^2 & 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{array} \text{ in } \mathbb{Z}_7$$

\Rightarrow nu există $\sqrt{3}$ în $\mathbb{Z}_7 \Rightarrow$ e.c. nu are soluții în \mathbb{Z}_7 !

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

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

Există $\sqrt{1}$ în \mathbb{Z}_{11} ?

$$\begin{array}{c|ccccccccc} a & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline a^2 & 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{array}$$

$\Rightarrow \sqrt{1} \in \{1, 10\}$ dar $10 = -1$

Aleg $\sqrt{1} = 1$: $x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 6 = 36 = 3$

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

Datăi lăsături în $\sqrt{1} = 10$: $x_1 = (5+10) \cdot 2^{-1} = 15 \cdot 6 = 90 = 2$

$$x_2 = (5-10) \cdot 2^{-1} = (-5) \cdot 6 = 6 \cdot 6 = 36 = 3$$

Ex: $3x^2 + x + 4 = 2$ în \mathbb{Z}_8

$$3x^2 + x + 2 = 0$$

$$\Delta = 1 - 4 \cdot 3 \cdot 2 = 1 - 24 = -23 = -16 - 7 = -7 = 1$$

$\sqrt{1}$ în \mathbb{Z}_8 și 1 sau 7

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

\hookrightarrow Nu există în \mathbb{Z}_8 (cum $\det(6, 8) = 2$)

\Rightarrow nu are soluții.

Sisteme liniare (2×2)

Dacă \det matricei sistemului nu este element inversabil

\Rightarrow rezolvă prin incercări.

Afăl, aplic reducere sau substituție.

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

$$A = \begin{pmatrix} 2 & 3 \\ 1 & -5 \end{pmatrix} \quad \det A = -10 - 3 = -13 = 1 \neq 0$$

Reducere: $\begin{cases} 2x + 3y = 1 \\ x - 5y = 2 \end{cases} \Rightarrow \begin{cases} 2x + 3y = 1 \\ 2x - 10y = 4 \end{cases}$

$$13y = -3 \Rightarrow 6y = 4 \cdot 6^{-1}$$

$$y = 24 = 3$$

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

$$4 + 10y + 3y = 1$$

$$13y = -3 = 4 \Rightarrow y = 3$$

Inversă matricială

$\exists M, M$ este inversabilă $\Leftrightarrow \det M \neq 0$

$\exists \mathbb{Z}_n, M$ este inversabilă $\Leftrightarrow \det M \in U(\mathbb{Z}_n)$

Ex: $A = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \in M_2(\mathbb{Z}_7) \quad A^{-1} \Rightarrow$ dacă există

$$\det A = 10 = 3 \in U(\mathbb{Z}_7) \Rightarrow$$
 există A^{-1} (line + col)

$$A \rightarrow A^* = \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 5 & -3 \\ 0 & 2 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 3^{-1} \cdot \begin{pmatrix} 5 & -3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 25 & -15 \\ 0 & 10 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 4 & 6 \\ 0 & 3 \end{pmatrix}$$

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

Cifruri elementare

Setup:

A	B	C	D	E	F	G	H	I	J	K
O	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				

Alfabetul englezesc conduce la $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$

DAR 26 nu este nr prim \Rightarrow

$U(\mathbb{Z}_{26}) \subsetneq \mathbb{Z}_{26}^*$ (există elemente/litere neinversabile/indecifrabile)

Completem alfabetul la \mathbb{Z}_{29} , 29 prim $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$.

Cifrul Caesar (flux = stream cipher)

Ecuatii de criptare: text + cheie = cod
 clar $\xrightarrow{\text{mesaj}} \xrightarrow{\text{key}} \xrightarrow{\text{cod}}$ ($m + k = c$)

Ecuatia de decriptare: Cod - cheie = text ($c - k = m$)

Exemplu: mesaj: "Salut"; cheie: 17

Criptarea: $[S, A, L, U, T] \rightarrow [18, 0, 11, 20, 19] \xrightarrow{+17} [35, 17, 28, 37, 36]$

$\rightarrow [35, 17, 28, 37, 36] \xrightarrow{\text{mod } 29} [6, 17, 28, 8, 7]$

$\rightarrow G R ? i H$

SALUT $\xrightarrow{+17} G R ? i H$ (Caesar)

Decriptarea : $GR?IH \rightarrow [6, 17, 28, 8, 7] \xrightarrow[-K]{-17}$

$\rightarrow [-11, 0, 11, -9, -10] \xrightarrow[\text{mod } 29]{} [18, 0, 11, 20, 19]$

$\rightarrow SALUT$

Variatie : Caesar pe blocuri

- a) fără padding
- b) cu padding random

a) Împart mesajul în blocuri de lungime b (data) și folosesc
cîte o cheie pt fiecare bloc.

Ex: mesaj: TOAMNA , bloc: 4

$\Rightarrow b_1: TOAM , b_2: NA$

chei: $K_1 = 15 ; K_2 = 6$

Criptarea : Blocul 1 : $[T, O, A, M] \rightarrow [19, 14, 0, 12] \xrightarrow[+15]{+K_1}$

$\rightarrow [34, 29, 15, 27] \xrightarrow[\text{mod } 29]{} [5, 0, 15, 27] \rightarrow [F, A, P, .]$

Blocul 2 : $[N, A] \rightarrow [13, 0] \xrightarrow[+6]{+K_2} [19, 6] \rightarrow [T, G]$

$TOAMNA \rightarrow FAP.TG$ (Caesar, 2 blocuri)

b) Cu padding random : toate blocurile vor avea aceeași lungime

Ex: mesaj: CAIET , blocuri de lungime 4

b. : CAIE $\Rightarrow K_1 = 7$

$$b_1 : \text{CAIE} \Rightarrow K_1 = 7$$

$$b_2 : \text{TMZ?} \Rightarrow K_2 = 10 \quad \text{etc.}$$

Obs 1: Dacă 2 car. identice se găsesc în blocuri diferite
 \Rightarrow ele se vor codifica diferit \Rightarrow securitate ++

Obs 2: Nu putem elimina padding-ul fără a fi mesajul inițial.

Cifrul afin

Varianta flux:

$$\text{Ec. de criptare: } \text{text} \cdot \text{cheie1} + \text{cheie2} = \text{cod}$$

$$m \cdot K_1 + K_2 = c$$

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

$$\text{Ex: } m = \text{AZI} ; K_1 = 5 ; K_2 = 6$$

$$[A, Z, I] \rightarrow [0, 25, 8] \xrightarrow[\substack{\cdot K_1 + K_2 \\ \cdot 5 + 6}]{} [6, 131, 46] \rightarrow$$

$$\xrightarrow{\substack{\text{mod } 29}} [6, 15, 17] \rightarrow [G, P, R]$$

$$\text{AZI} \rightarrow \text{GPR} \text{ (afin, flux)}$$

$$\text{Decriptarea: } [G, P, R] \rightarrow [6, 15, 17] \xrightarrow[\substack{-K_2 \cdot K_1^{-1} \\ -6 \cdot 5 - 1}]{} [0, 54, 66] \xrightarrow{\substack{\text{mod } 29 \\ -6, 6}}$$

$$5^{-1} \text{ în } \mathbb{Z}_{29} = 6$$

$$\rightarrow [0, 25, 8] \rightarrow \text{AZI}$$

2) Varianta pe blocuri cu/fără padding
! cite 2 chei / bloc.

: cîte 2 chei / bloc.

Ex: mesaj: CARTE , blocuri de lungime 3

$$\begin{array}{l} b_1 : \text{CAR} \quad K1=3 \quad K2=5 \\ b_2 : \text{TE } \hookleftarrow \quad K3=6 \quad K4=8 \end{array}$$

$$\text{Blocul 1: } [C, A, R] \rightarrow [2, 0, 17] \xrightarrow[\cdot 3+5]{\cdot K1+K2} [11, 5, 56] \xrightarrow{\text{mod } 29} [11, 5, 27]$$

→ LF.

$$\text{Blocul 2: } [T, E, \omega] \rightarrow [19, 4, 26] \xrightarrow[\cdot 6+8]{\cdot K3+K4} [122, 32, 164]$$

$$\xrightarrow{\text{mod } 29} [6, 3, 19] \rightarrow \text{GDT}$$

$$\text{CARTE } \hookleftarrow \rightarrow \text{LF. GDT}$$

Cifrul Hill

Flux: Ecuatia de criptare: cheie · mesaj = cod, unde

cheie este matrice

mesaj, cod = vectori

Ecuatie de decriptare: mesaj = cheie⁻¹ · cod

$$\text{Ex: Mesaj: Joi} \rightarrow \begin{pmatrix} 7 \\ 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = M$$

$$\text{Cheie (matrice de criptare): } K = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & -2 & 0 \end{pmatrix}$$

Criptarea: $KM = C$

$$\begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 24 \\ 30 \\ -37 \end{pmatrix} \text{ mod } 29 = \begin{pmatrix} 24 \\ 1 \\ 21 \end{pmatrix} \begin{matrix} Y \\ B \\ V \end{matrix}$$

$$\begin{pmatrix} 5 & 1 & 2 \\ 0 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 30 \\ -37 \end{pmatrix} \bmod 29 = \begin{pmatrix} 1 \\ 21 \end{pmatrix} \checkmark$$

$$-37 = -29 - 8 = -8$$

Jo î → YBV (Hill)

Decriptarea $\det K = -2 - 1 + 8 = 5 \in U(\mathbb{Z}_{29})$

$$(\det K)^{-1} = 5^{-1} = 6.$$

$$K \rightarrow K^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & -2 \\ -1 & 2 & 0 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} 1 & +2 & 3 \\ -2 & -1 & -4 \\ 1 & +3 & 2 \end{pmatrix}$$

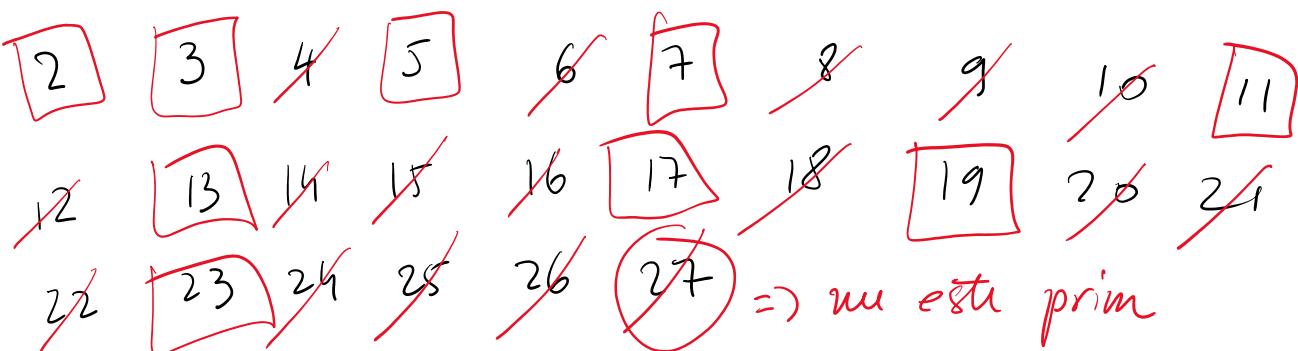
$$K^{-1} = (\det K)^{-1} \cdot K^* = 6 \cdot \begin{pmatrix} 1 & 2 & 3 \\ -2 & -1 & -4 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 24 & 12 & 18 \\ -12 & -6 & -24 \\ 6 & 18 & 12 \end{pmatrix}$$

Mesaj: $K^{-1} \cdot C = \begin{pmatrix} 24 & 12 & 18 \\ -12 & -6 & -24 \\ 6 & 18 & 12 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 1 \\ 21 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

Teste de primalitate

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

$$n = 27$$



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

2) Testul Fermat (sec. XVII)

Teorema (Mica teorema Fermat)

Dacă p prim $\Rightarrow a^{p-1} \equiv 1 \pmod p$ și $a < p$.

E) Dacă p prim $\Rightarrow a^{p-1} \equiv 1$ în \mathbb{Z}_p^* , $a \in \mathbb{Z}_p^*$

Ex: $p = 9 \stackrel{?}{\Rightarrow} \forall a \in \mathbb{Z}_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\}$,
 $a^8 = 1$ în \mathbb{Z}_9^* ?

$$1^8 = 1 \text{ ok}$$

$$2^8 = 2^3 \cdot 2^3 \cdot 2^2 = (-1) \cdot (-1) \cdot 4 = 4 \neq 1 \Rightarrow 9 \text{ nu este prim}$$

2 s.n. martor (witness) — Contraexemplu al testului

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

$$1^{10} = 1 \text{ ok}$$

$$2^{10} = (2^5)^2 = (32)^2 = (-1)^2 = 1 \text{ ok}$$

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

$$4^{10} = (2^{10})^2 = 1^2 = 1 \text{ ok}$$

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

$$\therefore 10 \quad -10, 10 - 1 \cdot 1 = 1 \text{ ok}$$

$$\begin{aligned}
 5^{10} &= (5^2)^5 = 25 - 1 = 24 = 1 \text{ OK} \\
 6^{10} &= 2^{10} \cdot 3^{10} = 1 \cdot 1 = 1 \text{ OK} \\
 7^{10} &= (-4)^{10} = 4^{10} = 1 \text{ OK} \\
 8^{10} &= 2^{10} \cdot 4^{10} = 1 \cdot 1 = 1 \text{ OK} \\
 9^{10} &= (3^{10})^2 = 1^2 = 1 \text{ OK} \\
 10^{10} &= 2^{10} \cdot 5^{10} = 1 \cdot 1 = 1 \text{ OK} \\
 \Rightarrow 11 \text{ nr. prim (cf. Fermat)}
 \end{aligned}$$

Varianta probabilistica

Testez doar t elemente din \mathbb{Z}_p^* și rezultatul va avea probabilitate de adevăr $\frac{t}{p-1}$.

Obs: Dacă printre nr. alese găsește un marțor
 \Rightarrow SIGUR nr. nu este prim.

$$\begin{aligned}
 \text{Ex: } n &= 23 \quad t = 3, \text{ aleg } a \in \{5, 6, 15\} \\
 \text{Testez } a^{n-1} &= 1 \pmod{n} \text{ doar pt } a \in \{5, 6, 15\} \\
 5^{22} &= (5^2)^{11} = 25^{11} = (2^5)^2 \cdot 2 = 9^2 \cdot 2 = 3^4 \cdot 2 \\
 &= 3^3 \cdot 3 \cdot 2 = 27 \cdot 3 \cdot 2 = 4 \cdot 3 \cdot 2 = 24 = 1. \text{ OK} \\
 6^{22} &= 2^{22} \cdot 3^{22} = \underbrace{(2^{11})^2}_{1} \cdot \underbrace{(3^3)^7}_{1} \cdot 3 = 9^7 \cdot 3 = \\
 &= 9^{14} \cdot 3 - 9^{11} \cdot 9^3 \cdot 3 = 8 \cdot 3 = 24 = 1. \text{ OK}
 \end{aligned}$$

$$= 2^{14} \cdot 3 = 2^{\frac{11}{1}} \cdot 2^3 \cdot 3 = 8 \cdot 3 = 24 = 1 \text{. ok}$$

$$15^{22} = 3^{22} \cdot 5^{22} = 1 \cdot 1 = 1 \text{ ok}$$

\mathbb{Z}_{23}^* = {1, 2, ..., 22} $\Rightarrow 23$ este probabil prim (Fermat)
cu prob = $\frac{3}{22}$.

Testul Solovay-Strassen

Simbolul Jacobi

Def b, n nr. naturale, n impar

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

(Ex: $\exists \sqrt{b}$ în \mathbb{Z}_n^*)

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

X	1	2	3	4	5	6
X ²	1	4	2	2	4	1

în \mathbb{Z}_7^*

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

$$\left(\frac{4}{19} \right) = 1 \text{ pt că } 4 = 2^2 \text{ în } \mathbb{Z}_{19}^*$$

$$\left(\frac{15}{5} \right) = 0 \text{ pt că } 5 \mid 15.$$

$$\left(\frac{15}{5}\right) \neq 0 \text{ pt că } 5|15.$$

Testul Solovay-Strassen

Dacă p prim $\Rightarrow \forall a \in \mathbb{Z}_p^*, a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ în \mathbb{Z}_p^* .

Ex: $p=7 \Rightarrow \forall a \in \mathbb{Z}_7^*, a^3 = \left(\frac{a}{7}\right)$ în \mathbb{Z}_7^* . ?

$$a=1 \Rightarrow 1^3 = 1. \\ \left(\frac{1}{7}\right) = 1 \text{ pt că } 1=1^2 \quad \left\{ \text{OK} \right.$$

$$a=2 \Rightarrow 2^3 = 1; \left(\frac{2}{7}\right) = 1 \text{ pt că } 2=3^2 \text{ în } \mathbb{Z}_7 \quad \underline{\text{OK}}$$

$$a=3 \Rightarrow 3^3 = 27 = -1; \left(\frac{3}{7}\right) = -1 \quad \underline{\text{OK}}$$

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

$$a=5 \Rightarrow 5^3 = (-2)^3 = -8 = -1; \left(\frac{5}{7}\right) = -1 \quad \underline{\text{OK}}$$

$$a=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot (-1) = -1; \left(\frac{6}{7}\right) = -1 \quad \underline{\text{OK.}}$$

$\Rightarrow p=7$ prim (testul Solovay-Strassen)

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

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

$a=1$ OK.

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

$\Rightarrow p=15$ compus ($a=2$ nu este pt 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 $\underline{\mathbb{Z}_n}$)

Obs: Este posibil ca $\log_a b$ să nu existe în \mathbb{Z}_n , chiar dacă avem îndeplinite C.E.

Ex: $\log_3 5$ în \mathbb{Z}_7 dacă există

$$\log_3 5 = x \Leftrightarrow 3^x = 5 \text{ în } \mathbb{Z}_7 \Rightarrow \log_3 5 = 5 \text{ în } \mathbb{Z}_7.$$

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

$\log_2 7$ în \mathbb{Z}_{11} dacă există

$$\log_2 7 = x \Leftrightarrow 2^x = 7 \text{ în } \mathbb{Z}_{11} \Rightarrow \log_2 7 = 7 \text{ în } \mathbb{Z}_{11}$$

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

... Iată că invers $2^x = 7$ în \mathbb{Z}_{11} .

Obs: Putem lucra și invers: $2^x = 7$ în \mathbb{Z}_{11}

$$7 \text{ în } \mathbb{Z}_{11} = \{7, 18, 29, 40, 51, \dots\}$$

↑
Cant putere a lui 2

Obs: Este suficient în \mathbb{Z}_n să cătăram cel mult pînă la puterea $n-1$.

(Dacă n este prim $\Rightarrow a^{n-1} = 1$ în \mathbb{Z}_n , din Fermat)

Ordinul unui element într-un grup (\mathbb{Z}_n^*)

Def: $\text{ord}(x) = t$ în \mathbb{Z}_n^* dacă $x^t = 1$ și t este cea mai mare putere cu această proprietate.

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

Ex: \mathbb{Z}_{13} $\text{ord}(2) = ?$ $\text{ord}(7) = ?$ $\text{ord}(11) = ?$

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

\nearrow
Fermat

$\Rightarrow \text{ord } 2 = 12$ în \mathbb{Z}_{13}

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

$\Rightarrow \text{ord } 7 = 12 \text{ in } \mathbb{Z}_{13}$.

$$\begin{aligned} 11^x &= (-2)^x = 2^x \text{ dacă } x \text{ par} \\ &= -2^x \text{ dacă } x \text{ impar} \end{aligned}$$

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

$$11^3 = (-2)^3 = -2^3 = -8 = 5$$

$$11^5 = -2^5 = -6 = 7$$

$\Rightarrow \text{ord } 11 = 12 \text{ in } \mathbb{Z}_{13}$.

Def: Dacă $\text{ord } x = n-1$ în \mathbb{Z}_n^* , x s.u. generator $\rightarrow \mathbb{Z}_n^*$, care s.u. grup ciclic. Not. $\mathbb{Z}_n^* = \langle x \rangle$.

Ex: \mathbb{Z}_{13}^* ciclic, cu $\mathbb{Z}_{13}^* = \langle 2 \rangle = \langle 7 \rangle = \langle 11 \rangle$.

$\text{ord } 4 \text{ în } \mathbb{Z}_8$

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

$\Rightarrow \text{ord } 4 = \infty \text{ în } \mathbb{Z}_8$.

Teorema (Lagrange) Not. $|\mathbb{Z}_n^*|$ nr. de elemente din \mathbb{Z}_n^* , care c.u. ordinul grupului \mathbb{Z}_n^* ($|\mathbb{Z}_n^*| = n-1$).

S.n. ordinal grupului \mathbb{Z}_n^* ($|\mathbb{Z}_n^*| = n-1$).

$\forall x \in \mathbb{Z}_n^*, \text{ord } x = \omega$ sau $\text{ord } x$ este divizor al lui $n-1$.

Indicatorul lui Euler (Euler's TOTIENT function)

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

Ex: $\varphi(10) = ?$

$$\text{cmmdc}(x, 10) = 1 \Rightarrow x \in \{1, 3, 7, 9\}$$

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

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

Proprietăți: 1) Dacă p nr prim $\Rightarrow \varphi(p) = p-1$.

2) $\forall x, y \mid \varphi(xy) = \varphi(x) \cdot \varphi(y)$.

În particular, dacă $x = p \cdot q$, p, q prime

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

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

Ex: $n = 36$

$$\varphi(36) = 36 \cdot \prod_{p|36} \left(1 - \frac{1}{p}\right) = 36 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right)$$

$$\therefore 1 \not\equiv -26 \pmod{36}$$

$$P1 \sim \\ = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{36}{3} = 12.$$