1343b - Aritmetică modulară (în $\mathbb{Z}_n$)

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

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

$\rightarrow (\mathbb{Z}_n, \cdot)$ monoid comutativ

Ex: $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

- a = opusul elem. a
  = simetricul în raport cu „$+$"

$-3 = x$ pt care $3 + x = 0 \Rightarrow -3 = 4$

a^{-1} = inversul elem. a
= simetricul față de „$\cdot$"

$3^{-1} = x$ pt care $3x = 1 \Rightarrow 3^{-1} = 5 \Rightarrow 5^{-1} = 3$

$2^{-1} = 4 \Rightarrow 4^{-1} = 2$; $6^{-1} = 6$

$\mathbb{Z}_{10} = \{0,1,\dots,9\}$

$3^{-1} = 7$; 5^{-1} nu există

= grupul unităților

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

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

$U(Z_{10}) = \{1, 3, 7, 9\}$ $\quad 3^{-1} = 7 \Rightarrow 7^{-1} = 3$

$1^{-1} = 1$; $9^{-1} = 9$

$(U(Z_{10}), \cdot)$ grup comutativ.

Ec. de gradul I

- $3x + 2 = 1$ în Z_7

$3x = 1 - 2 = -1 = 6 \Rightarrow x = 2$

Sau: $3x = -1 \mid \cdot 3^{-1}$

$3^{-1} \cdot 3 \cdot x = (-1) \cdot 3^{-1}$

$x = (-1) \cdot 5 = -5 = 2$

- $\boxed{4}x - 1 = 5$ în Z_{10} nu are sol. pt că

$4 \notin U(Z_{10})$.

- $4x + 1 = 5$ în Z_{10}

$4x = 4 \boxed{= 1} \; x = 1$ (NU)

Ec. de gradul II

- $2x^2 - 5x + 1 = 3$ în Z_{11}

$2x^2 - 5x - 2 = 0$

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

$\sqrt{8} = a \Leftrightarrow a^2 = 8$

$0^2=0;\ 1^2=1;\ 2^2=4;\ 3^2=9;\ 4^2=5;\ 5^2=3;\ 6^2=3;$

$7^2=5;\ 8^2=9;\ 9^2=4;\ 10^2=1$

$\Rightarrow \sqrt{8}$ nu există în Z_{11} $\Rightarrow$ ec. nu are sol.

- $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{13}$

$\Delta = 25 - 24 = 1 \Rightarrow \sqrt{\Delta} = \{1, 12\} = \{1, -1\}$

$x_{1,2} = (5 \pm \sqrt{1}) \cdot 2^{-1}$

$x_1 = 6 \cdot 7 = 42 = 3$

$x_2 = 4 \cdot 7 = 28 = 2$

$\Rightarrow x \in \{2, 3\}$.

Logaritmul discret

$\log_a b = c \Leftrightarrow a^c = b$

$\log_2 3$ în $Z_5 \Rightarrow 2^x = 3$ în Z_5

$2^0=1;\ 2^1=2;\ 2^2=4;\ 2^3=3$

$\Rightarrow \log_2 3 = 3$ în Z_5

$\log_2 3 \in \mathbb{Z}_7 \Rightarrow 2^x = 3 \in \mathbb{Z}_7$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 1;\ 2^4 = 2;\ 2^5 = 4$

$\Rightarrow$ nu există.

$\log_a b \in \mathbb{Z}_n \Leftrightarrow a^x = b \in \mathbb{Z}_n,\ x \in \{0, 1, \dots, n-1\}$

Teorema lui Lagrange pt grupuri

$(G, \cdot)$ grup, $g \in G \Rightarrow g^n = e$.

Dacă $\#G = n$

Obs: $(\mathbb{Z}_p^*, \cdot)$ grup $\#\mathbb{Z}_p^* = p-1$.

p nr. prim

$(\mathbb{Z}_{23}^*, \cdot)$ $\log_5 11 \in \mathbb{Z}_{23}$

$5^x = 11 \in \mathbb{Z}_{23},\ x \in \{0, \dots, 22\}$

$4^{100} \in \mathbb{Z}_{11} = ?$

$4^{100} = (4^2)^{50} = (16)^{50} = 5^{50} = (5^2)^{25} = 1^{25} = 1$

$= 3^{25} = (3^5)^5$

$3^5 = 3^2 \cdot 3^2 \cdot 3 = 1$

$3^5 = 3^2 \cdot 3^2 \cdot 3$ — $3^2 \cdot 3^2$ = 5, 5 · 3 = 1

$A \in \mathcal{M}_n(\mathbb{Z}_t)$

$A^{-1} = (\det A)^{-1} \cdot A^*$ există $\Leftrightarrow$ $\det A$ este element inversabil în $\mathbb{Z}_t \Leftrightarrow \det A \in U(\mathbb{Z}_t) \Leftrightarrow$

$\text{cmmdc}(\det A, t) = 1$

Alg. criptografice bazate pe $\mathbb{Z}_n$

1) Flux (stream cipher): aceeași cheie pt tot mesajul

2) Pe blocuri (block cipher): 1 cheie / bloc
   a) fără padding: ≤ 1 bloc mai scurt
   b) cu padding: toate blocurile au aceeași lungime

Z_{29} Z_{26} Z_{29}

A	B	C	...	Z	␣	.	?
0	1	2	...	25	26	27	28

Caesar $c = m + k$

Ec. de criptare: Cod = Mesaj + Cheie

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

Ex: Flux: Mesaj: ANDREEA

cheia: 21

$[A, N, D, R, E, E, A] \rightarrow [0, 13, 3, 17, 4, 4, 0]$

$\xrightarrow{+21} [21, 34, 24, 38, 25, 25, 21]$

$\xrightarrow{\%29} [21, 5, 24, 9, 25, 25, 21]$

$\rightarrow$ VFYJZZV

Decriptare:

VFY] ZZV → [21,5,24,9,25,25,21]

$\xrightarrow{-24}$ [0,-16,3,-12,4,4,0] $\xrightarrow{\%29}$

→ [0,13,3,17,4,4,0] → ANDREEA.

Pe blocuri, fără padding

Mesaj: ANDREEA

Bloc: b=5 ⇒ ANDRE K1:5

EA K2:12

[A,N,D,R,E] → [0,13,3,17,4] $\xrightarrow[+5]{+K1}$

→ [5,18,8,22,9] → FSiW]

[E,A] → [4,0] $\xrightarrow[+12]{+K2}$ [16,12] → QM

ANDREEA → FSiW]QM

Pe blocuri, cu padding

Mesaj: ANDREEA ANDRE K1 = 11

Bloc: b = 5 => EAMDS, K2 = 7

[A, N, D, R, E] → [0, 13, 3, 17, 4] $\xrightarrow{+K1}$

→ [11, 24, 14, 28, 15] → LYO?P

[E, A, M, D, S] → [4, 0, 12, 3, 18] $\xrightarrow[+7]{+K2}$

[11, 7, 19, 10, 25] → LHTKZ

ANDREEAMDS → LYO?PLHTKZ

Cifrul afin

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

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

Ex: Mesaj: CAIET plus

Cheia 1: K1 = 5

Cheia 2: K2 = 15

$[C,A,I,E,T] \to [2,0,8,4,19] \xrightarrow[\cdot 5+15]{\cdot K1+K2}$

$\to [25,15,55,35,110] \xrightarrow{\%.29}$

$\to [25,15,26,6,23] \to ZP\_GX$

$55 = 58-3 = -3 = 26$

$110 = 116-6 = -6 = 23$

$CAIET \to ZP\_GX$

Decriptare: $c = m \cdot 5 + 15 \Rightarrow m = (C-15) \cdot 5^{-1}$

5^{-1} în $Z_{29} = 6$

$ZP\_GX \to [25,15,26,6,23] \xrightarrow{-15;6} [60,0,66,-54,48]$

$\xrightarrow{\%.29} [2,0,8,4,19] \to CAIET.$

Ex. afin pe blocuri fără padding

Mesaj: CAIET

Blocuri: $b=3$

CAI $\to K1=2; K2=5$

ET $\to K3=10; K4=2$

$[C,A,I] \to [2,0,8] \xrightarrow{\cdot 2+5} [9,5,21]$

JFV

$[6,7] \to [4,19] \xrightarrow{\cdot 10+7} [42,192] \xrightarrow{:29}$

$\to [13,18] \to NS$

$29 \mid 203$

$192 = 203 - 11 = -11 = 18$

$\downarrow$

6

CAIET $\to$ JFVNS.

Hill

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix}$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC^{-1} \cdot \begin{pmatrix} C \\ O \\ D \end{pmatrix}$

Ex: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} J \\ O \\ I \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

$MC = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ -2 & -1 & 1 \end{pmatrix}$

$\begin{pmatrix} C \\ O \\ D \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ -2 & -1 & 1 \end{pmatrix} \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ -24 \end{pmatrix} \overset{:29}{\equiv} \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix} \begin{matrix} H \\ D \\ F \end{matrix}$

$$\det MC = \begin{vmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ -2 & -1 & 1 \end{vmatrix} = 1 - 2 - 4 - 1$$

$$= -6 = 23$$

$$(\det MC)^{-1} = 23^{-1} = 24 \qquad 23^{-1} = x \Leftrightarrow 23x = 1 \text{ în } \mathbb{Z}_{29}$$

$$MC^{-1} = 24 \cdot MC^*$$

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

$$\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \underbrace{24 \cdot \begin{pmatrix} 0 & -2 & 2 \\ -3 & 3 & 3 \\ -3 & -1 & 1 \end{pmatrix}}_{MC^{-1}} \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} C \\ O \\ D \end{pmatrix}$$

Hill afin

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC_1 \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix} + MC_2$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC_1^{-1} \left(\begin{pmatrix} C \\ O \\ D \end{pmatrix} - MC_2 \right)$

Teste de primalitate

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

OUTPUT: A/F dacă n este prim

1) Sigure = Deterministe: răsp. cu certitudine, calcul ineficient

2) Probabiliste: răspuns probabil, calcul ef.

---

1. Verificarea directă

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

- Pentru $d \in \{2, \dots, n-1\}$, verific dacă $d \mid n$.
  - $\rightarrow$ NU, $\forall d$ = „PRIM
  - $\rightarrow \exists d$ a.î. $d \mid n \Rightarrow n$ COMPUS

Varianta sigură = deterministă

Varianta prob: Alg t moshe pt. d

Ex: $n = 23$

- Varianta simplă: Testez $d \in \{2, \dots, 22\}$

$2 \nmid 23$; $3 \nmid 23$, $4 \nmid 23$, ---

- Varianta prob: Alg $\nmid = 3$ mostre

$d \in \{5, 7, 17\}$

$5 \nmid 23$, $7 \nmid 23$, $17 \nmid 23$ =)

=> 23 PROBABIL prim,

prob. $= \frac{3}{20}$

---

2. Ciurul (Sita) lui Eratostene

Ex: $n = 25$

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~

~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17

~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

3. Testul Fermat

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

Ex: $n = 7 \Rightarrow \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} \Rightarrow a^6 = 1$ în $\mathbb{Z}_7^*$, $\forall a \in \mathbb{Z}_7^*$?

$1^6 = 1$; $2^6 = 64 = 1$; $3^6 = (3^2)^3 = 2^3 = 1$;

$4^6 = (2^2)^6 = (2^6)^2 = 1$;

$5^6 = (-2)^6 = 2^6 = 1$; $6^6 = 2^6 \cdot 3^6 = 1$

$\Rightarrow n = 7$ prim.

Ex: $n = 9 \Rightarrow \mathbb{Z}_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\} \Rightarrow a$

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

$= 4 \neq 1$

$\Rightarrow n = 9$ compus, $a = 2$ martor

↑ var-deterministă (sigură)

Varianta probabilistă:

$n = 27409 \Rightarrow$

$\forall a \in \mathbb{Z}_{27409}^*, a^{27408} = 1 \in \mathbb{Z}_{27409}^*$

Alg t = 20 moștre aleatorii

Alg $a = 9731 \Rightarrow 9731^{27408} \overset{?}{=} 1 \in \mathbb{Z}_{27409}^*$

$x = 9731$

$x^2 \,\%\, 27409 = 9731^2 \,\%\, 27409 = \underline{21675}$

$x^3 \,\%\, 27409 = (21675 \cdot 9731) \,\%\, 27409$

$= 7170$

$x^4 \,\%\, 27409 = (7170 \cdot 9731) \,\%\, 27409$ etc

.....

$\Rightarrow$ 20 moștre dau rez-pozitiv $\Rightarrow$

$\Rightarrow 27409$ PROBABIL prim, $prob = \frac{20}{27407}$

4. Simbolul Jacobi

$a, b \in \mathbb{N}$, n impar

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

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

Pătratele din $\mathbb{Z}_7^* = P(\mathbb{Z}_7^*) = \{1, 4, 2\} \not\ni 3$

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

Ex: $\left(\frac{15}{9}\right) = ?$ $\quad 9 \nmid 15$

$P(\mathbb{Z}_9^*) = \{1, 4, 0, 7\}$

$\left(\frac{15}{9}\right) = \left(\frac{6}{9}\right) = -1$

Teoremă (Solovay-Strassen)

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

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

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

$P(\mathbb{Z}_7^*) = \{1, 2, 4\}$

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

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

$b=4 \Rightarrow 4^{\frac{7-1}{2}} = 4^3 = 2^6 = (2^3)^2 = 1$

$\left(\frac{4}{7}\right) = 1$ pt că 4 este pătrat

$b=5 \Rightarrow 5^{\frac{7-1}{2}} = 5^3 = 5^2 \cdot 5 = 4 \cdot 5 = 6$

$\left(\frac{5}{7}\right) = -1 = 6$

$b=6 \Rightarrow 6^{\frac{7-1}{2}} = 6^3 = 2^3 \cdot 3^3 = 1 \cdot 6 = 6$

$\left(\frac{6}{7}\right) = -1 = 6$

$\Rightarrow n = 7$ este prim.

Ex: $n = 9$

$P(\mathbb{Z}_9^*) = \{0, 1, 4, 7\}$

$b=1 \Rightarrow 1^{\frac{9-1}{2}} = 1^4 = 1$; $\left(\frac{1}{9}\right) = 1$ ✓

$b=2 \Rightarrow 2^{\frac{9-1}{2}} = 2^4 = 7$; $\left(\frac{2}{9}\right) = -1 = 8$ ✗

$\Rightarrow n = 9$ compus, 2 este martor

$b=3 \Rightarrow 3^{\frac{9-1}{2}} = 3^4 = 0$; $\left(\frac{3}{9}\right) = -1 = 8$ ✗

$b=4 \Rightarrow 4^{\frac{9-1}{2}} = 4^4 = (2^4)^2 = 49 = 4$; $\left(\frac{4}{9}\right) = 1$ ✗