13.11.16

Aritmetică modulară

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

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

$\Leftrightarrow$ 1) $(\mathbb{Z}_n, +)$ grup comutativ

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

Ex: $\mathbb{Z}_7 = \{0, 1, \dots, 6\}$

$(\mathbb{Z}_7, +)$ $-2 = x \Leftrightarrow \underline{x + 2 = 0} \Rightarrow x = 5$

În particular, $-5 = 2$

$(\mathbb{Z}_7, +)$ grup com. $\Leftrightarrow \forall x \in \mathbb{Z}_7$, există $-x$.

$(\mathbb{Z}_7, \cdot)$ $3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = 5$

În particular, $5^{-1} = 3$

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

$(\mathbb{Z}_{10}, +, \cdot)$ $-6 = 4$ pt că $6 + 4 = 10 = 0$

6^{-1} nu există.

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

pt. $\mathbb{Z}_n$ se notează $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \exists x^{-1}\} = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$

↑ grupul unităților

$U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

Ec. de gradul I în $\mathbb{Z}_n$

$2x + 5 = 3$ în $\mathbb{Z}_7$

$2x = 3 - 5 = -2$

- $2x = -2 \Rightarrow x = -1 = 6$
- $2x = -2 = 5 \mid \cdot 2^{-1} = 4$

$4 \cdot 2 \cdot x = 4 \cdot 5$

$1 \cdot x = x = 20 = 6$

Ec. de gradul II în $\mathbb{Z}_n$

- $3x^2 - 5x + 1 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 25 - 4 \cdot 1 \cdot 3 = 25 - 12 = 13 = 2$

$\sqrt{2} = ?$ în $\mathbb{Z}_{11}$

$\sqrt{a} = b \Leftrightarrow b^2 = a$.

$\sqrt{2} \in \mathbb{Z}_4$ $\quad \sqrt{2} = a \in \mathbb{Z}_4 \Leftrightarrow a^2 = 2$

$\sqrt{2}$ nu există $\Rightarrow$ Ec. nu are soluții.

- $x^2 + 3x - 4 = 0 \in \mathbb{Z}_7$

$\Delta = 9 + 16 = 25 = 4$

$\sqrt{4} \in \mathbb{Z}_7 = \{2, 5\} = \{2, -2\}$

$x_{1,2} = (-3 \pm \sqrt{\Delta}) \cdot 2^{-1}$

$2^{-1} = 4$

$x_1 = (-3+2) \cdot 4 = -1 \cdot 4 = -4 = 3$

$x_2 = (-3-2) \cdot 4 = -5 \cdot 4 = -20 = \underbrace{-14}_{0} - 6 = 1$

$x_3 = (-3+5) \cdot 4 = 2 \cdot 4 = 8 = 1$

$x_4 = (-3-5) \cdot 4 = -8 \cdot 4 = -32 = \underbrace{-28}_{0} - 4 = 3$

Logaritmul discret

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

$\log_2 5$ în $\mathbb{Z}_7$ nu există

$\exists x \in \mathbb{N}$ cu $2^x = 5$ în $\mathbb{Z}_7$

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

$2^0 = 1$

$(\mathbb{Z}_7^*, \cdot)$

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\log_3 5$ în $\mathbb{Z}_7$

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

$3^5 = 5$

$\Rightarrow \boxed{\log_3 5 = 5}$

---

g^{45} în $\mathbb{Z}_{11} = (g^5)^9 = (g^2 \cdot g^2 \cdot g)^9$

$= (81 \cdot 81 \cdot g)^9 = (4 \cdot 4 \cdot g)^9 = 1^9 = 1.$

$5 \quad 1$

Teorema lui Lagrange

G grup cu n elemente, $g \in G$

$\Rightarrow g^n = el.\ neutru.$

Z_{29}

A	B	C	D	...	Z	␣	.	?
0	1	2	3		25	26	27	28

$A \in M_n(\mathbb{R})$ $A^{-1} = \frac{1}{\det A} \cdot A^*$ ex. $\Leftrightarrow$

$\Leftrightarrow \det A \neq 0.$

Cifruri folosind Z_n

Z_{29}: $\underbrace{A \to Z}_{Z_{26}}, \underbrace{␣, ., ?}_{}$

Z_{29}

Cifruri

1) Flux (stream cipher) = aceeași cheie pt tot mesajul
2) Pe blocuri (block cipher) = 1 cheie/bloc
   a) cu padding = toate blocurile de aceeași lungime
   b) fără padding : ≤ 1 bloc mai scurt

Caesar

$c = m + k$

Flux: Ec. de criptare: Cod = Mesaj + cheie în $\mathbb{Z}_{29}$

Ec. de decriptare: Mesaj = Cod − cheie

$m = c - k$

Ex: Mesaj = MESAJ

cheie = 20

[MESAJ] → [M, E, S, A, J] → [12, 4, 18, 0, 9]

$\xrightarrow[+20]{+K}$ [32, 24, 38, 20, 29] $\xrightarrow{\%29}$ [3, 24, 9, 20, 0]

$\rightarrow [D, Y, J, U, A] \rightarrow DYJUA$

Decriptare: $[D, Y, J, U, A] \rightarrow [3, 24, 9, 20, 0] \xrightarrow[-20]{-K}$

$\rightarrow [-17, 4, -11, 0, -20] \xrightarrow{\%29} [12, 4, 18, 0, 9]$

$\rightarrow$ MESAJ.

Pe blocuri: Fără padding

Mesaj: MERE

Bloc: $b = 3 \Rightarrow$ MER, E

Cheie: $K1 = 15$; $K2 = 7$

$[M, E, R] \rightarrow [12, 4, 17] \xrightarrow[+K1]{+15} [27, 19, 32] \xrightarrow{\%29}$

$\rightarrow [27, 19, 3] \rightarrow .TD$

$E \rightarrow [4] \underset{+7}{\overset{+K2}{\rightarrow}} [11] \rightarrow L$

$MERE \rightarrow .TDL$

Decriptare:

$.TD \rightarrow [27, 19, 3] \xrightarrow{-15} [12, 4, 17] \rightarrow MER$

$L \rightarrow [11] \xrightarrow{-7} [4] \rightarrow E$

Cu padding

Mesaj: MERE

Bloc: b=3 → MER

EOB

K1=15 ; K2=17

MER → ... → .TD

EOB → [4, 14, 1] $\xrightarrow{+17}$ [21, 31, 18] $\xrightarrow{\%29}$

→ [21, 2, 18] → VCS

MEREOB → .TDVCS

Afin

$c = m \cdot k1 + k2$

Ec. de criptare: Cod = Mesaj · Cheie1 + Cheie2

Ec. de decriptare: Mesaj = (Cod − cheie2) · Cheie1^{-1}

$m = (c - k2) \cdot k1^{-1}$

Ex: Mesaj = AZi

Cheie1 = 2 ; Cheie2 = 11

[A, Z, i] → [0, 25, 8] $\xrightarrow[\cdot 2 + 11]{\cdot k1 + k2}$ [11, 61, 27]

$\xrightarrow{\%29}$ [11,3,27] → L.D.

AZi → L.D.

Deriptare: 2^{-1} în $\mathbb{Z}_{29} = 15$

[L.D.] → [11,3,27] $\xrightarrow{\cdot 11 \cdot 15}$ [0,25,8] →

→ AZi

Hill

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

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

Ex: Mesaj = AER $\longrightarrow \begin{pmatrix} 0 \\ 4 \\ 17 \end{pmatrix}$

$MC = \begin{pmatrix} -1 & 0 & 2 \\ 2 & -2 & 1 \\ 3 & 1 & 1 \end{pmatrix}$

$$\begin{pmatrix} -1 & 0 & 2 \\ 2 & -2 & 1 \\ 3 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 4 \\ 17 \end{pmatrix} = \begin{pmatrix} 34 \\ 9 \\ 21 \end{pmatrix} \mid 29 = \begin{pmatrix} 5 \\ 9 \\ 21 \end{pmatrix} = \begin{matrix} F \\ J \\ V \end{matrix}$$

AER → FJV.

Deciptare : $\det(MC) = 2 + 4 + 12 + 1$

$= 19 \in \mathbb{Z}_{29}$

$19^{-1} \in \mathbb{Z}_{29} = 26$

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

$$MC^* = \begin{pmatrix} -3 & +2 & 4 \\ +1 & -7 & +5 \\ 8 & +1 & 2 \end{pmatrix}$$

$$MC^{-1} = 26 \cdot \begin{pmatrix} -3 & 2 & 4 \\ 1 & -7 & 5 \\ 8 & 1 & 2 \end{pmatrix}$$

$$26 \cdot \begin{pmatrix} -3 & 2 & 4 \\ 1 & -7 & 5 \\ 8 & 1 & 2 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \\ 21 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 17 \end{pmatrix} = \begin{matrix} A \\ E \\ R \end{matrix}$$

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: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC_1^{-1} \cdot \left[\begin{pmatrix} C \\ O \\ D \end{pmatrix} - MC_2 \right]$

Ex: Mesaj = CAL $\longrightarrow \begin{pmatrix} 2 \\ 0 \\ 11 \end{pmatrix}$

$MC_1 = \begin{pmatrix} -1 & 2 & 5 \\ 0 & 2 & -1 \\ -2 & 1 & 3 \end{pmatrix}$

$MC_2 = \begin{pmatrix} 5 \\ 7 \\ -3 \end{pmatrix}$

$\begin{pmatrix} -1 & 2 & 5 \\ 0 & 2 & -1 \\ -2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \\ 11 \end{pmatrix} + \begin{pmatrix} 5 \\ 7 \\ -3 \end{pmatrix} = \dots$

Teste de primalitate

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

OUTPUT: A/F dacă n e prim

Dacă n e compus => se afișează un divizor sau un martor.

1) Deterministe: sigure, dar ineficiente
2) Probabiliste: probabile, dar eficiente

1. Verificarea directă

Algoritm: Citesc $n \in \mathbb{N}$ impar

Pentru $x \in \{2, \dots, n-1\}$:

dacă $x \mid n \rightarrow n$ compus

STOP

n prim

2. Ciurul (Sita) lui Eratostene

INPUT: n

OUTPUT: lista de nr. prime $\leq n$
sau dacă n e prim

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

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

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

$n = 25$ INPUT

$\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$ OUTPUT

Testul Fermat

Mica Teoremă a lui Fermat

p prim $\Rightarrow a^{p-1} = 1$ în $\mathbb{Z}_p$, $\forall a \in \mathbb{Z}_p^*$

Varianta deterministă: Verific toți $a \in \mathbb{Z}_p^*$

Ex: $p=7$ prim $\Rightarrow a^6 = 1$ în $\mathbb{Z}_7$,

$\forall a \in \{1,2,3,4,5,6\}$

$1^6 = 1$ OK

$2^6 = 64 = 63+1$ OK

$3^6 = (3^2)^3 = 2^3 = 8 = 1$ OK

$4^6 = 2^{12} = (2^3)^4 = 1^4 = 1$ OK

$5^6 = (-2)^6 = 2^6 = 1$ OK

$6^6 = 2^6 \cdot 3^6 = 1$ OK

$\Rightarrow$ $p=7$ este prim.

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

$a^8 = 1$ în $\mathbb{Z}_9$, $\forall a \in \mathbb{Z}_9^*$

$1^8 = 1$ ok

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

$\Rightarrow$ 2 este martor, $p = 9$ nu e prim.

Varianta probabilistă: Aleg t mostre (nr. din $\mathbb{Z}_p^*$).

Simbolul Jacobi

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

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

Ex: $\left(\frac{7}{11}\right) = ?$ $\quad 11 \times 7$

7 este pătrat în $\mathbb{Z}_{11}$?

Pătratele din $\mathbb{Z}_{11}^* = \{1, 4, 9, 5, 3\} \neq 7$

$\Rightarrow \left(\frac{7}{11}\right) = -1$

Ex: $\left(\frac{20}{7}\right) = ?$ $7 \nmid 20$

$20 \notin \mathbb{Z}_7 \Rightarrow 20 = 6$

$\Rightarrow \left(\frac{20}{7}\right) = \left(\frac{6}{7}\right)$

Patrate din $\mathbb{Z}_7^* = \{1, 4, 2\} \not\ni 6 \Rightarrow \left(\frac{20}{7}\right) = -1$

Teorema Solovay-Strassen

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

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

$\Leftrightarrow b^3 = \left(\frac{b}{7}\right), \forall b \in \{1, \dots, 6\}$

Patratele din $\mathbb{Z}_7$: $\{1, 2, 4\}$

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

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

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

$4^3=1$; $\left(\frac{4}{7}\right)=1$ pt că 4 este pătrat OK

$5^3=25\cdot 5=4\cdot 5=6$; $\left(\frac{5}{7}\right)=-1=6$ OK

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

2) $n=7$ este prim.