1. Elemente de aritmetică

$(\mathbb{Z}_n, +)$ - știm că este grup abelian ; $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\} \simeq \mathbb{Z}(n) = \{0, 1, \dots, n-1\}$

$(U(\mathbb{Z}_n), \cdot)$ - știm că este grup abelian ; $(\mathbb{Z}(n), \oplus, \odot)$ $\quad x \oplus y = z \Leftrightarrow \hat{x} + \hat{y} = \hat{z}$

$x \odot y = t \Leftrightarrow \hat{x} \cdot \hat{y} = \hat{t}$

z - restul împărțirii la n a lui $x+y$

t - restul împărțirii la n a lui $x \cdot y$

$U(\mathbb{Z}_n) = \{\hat{i} \mid (i, n) = 1\}$

$U(\mathbb{Z}(n)) = \{i \in \{0, \dots, n-1\} \mid (i, n) = 1\}$

Exemple

a) $n = 7 \qquad 3 \oplus 5 = 1$

$U(\mathbb{Z}(7)) = \{1, 2, \dots, 6\} \qquad 3 \odot 5 = 4$

b) $n = 21 \qquad 3 \oplus 5 = 8 \quad , \quad 13 \oplus 15 = 7$

$U(\mathbb{Z}(21)) = \{i \in \{0, \dots, 20\} \mid (i, 21) = 1\} = \{1, 2, 4, 5, 8, \dots\}$

Facem calcule modulo n

Propoziție (exercițiu la seminar)

Fie $a, b \in \mathbb{Z}^*$. Atunci:

$(a, b) \cdot \mathbb{Z} = a\mathbb{Z} + b \cdot \mathbb{Z}$

Corolar

Dacă $a, b \in \mathbb{N}^*$, atunci $\exists\, u, v \in \mathbb{Z}$ a.î. $(a, b) = au + bv$

Obs: Numerele u și v pot fi obținute folosind algoritmul lui Euclid pentru calculul a.m.m.d.c.

Def: Dacă $n \in \mathbb{N}$, $n \geq 2$, atunci numărul $|U(\mathbb{Z}_n)|$ s.n. INDICATORUL LUI EULER asociat lui n și se notează cu $\varphi(n)$

T. Lagrange

G - grup finit, $x \in G \Rightarrow x^{|G|} = 1$

Teoremă (Euler-Fermat)

Dacă $n \in \mathbb{N}$, $n \geq 2$ și $a = \overline{0, n-1}$ cu $(a, n) = 1$, atunci $a^{\varphi(n)} = 1$ în $\mathbb{Z}(n)$

$\left(\hat{a}^{\varphi(n)} = \hat{1} \text{ în } \mathbb{Z}_n \text{ sau } n \mid a^{\varphi(n)} - 1\right)$

Corolar 1 (mica teoremă a lui Fermat)

Dacă p - prim și $a = \overline{1, p-1} \Rightarrow a^{p-1} = 1$ în $\mathbb{Z}(p)$

Corolar 2

Dacă $n = pq$ cu p, q - prime, $p \neq q$ și $a = \overline{1, pq-1}$ cu $(a, pq) = 1$, atunci:

$a^{(p-1)(q-1)} = 1$ în $\mathbb{Z}(pq)$

$U(\mathbb{Z}(p)) = \{1, 2, \dots, p-1\} \Rightarrow \varphi(p) = p-1$

$U(\mathbb{Z}(pq)) = \{1, \dots, pq-1\} \setminus \left(\{p, 2p, \dots, (q-1)p\} \cup \{q, 2q, \dots, (p-1)q\}\right)$

$\Rightarrow \varphi(pq) = (p-1)(q-1)$

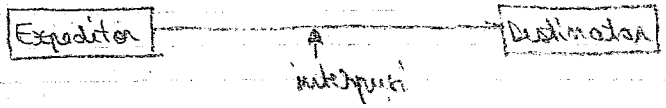
Obs: Se poate demonstra, folosind izomorfismul:

Dacă $(m, n) = 1 \Rightarrow \mathbb{Z}_{m \cdot n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

$\Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Elemente de criptografie

Scop: Transmiterea în siguranță a unor informații secrete.



Exemple
→ Transmiterea de mesaje scrise (mesaje)
- alfabet englez $\underbrace{A, B, C, \dots, X, Y, Z}_{\mathcal{A}}$ (26 simboluri)

$\mathcal{A}$ - mulțimea literelor

Criptare = stabilirea unei funcții bijective $\alpha: \mathcal{A} \to \mathcal{A}$ a.î. α este cunoscută de către expeditor.

Destinatarul trebuie să cunoască funcția $\alpha^{-1}: \mathcal{A} \to \mathcal{A}$

α - permutare a mulțimii $\mathcal{A}$ ⇒ α = produs de cicluri disjuncte

→ α^{-1} se obține inversând toate ciclurile

$c = (x, y, z, t) \Rightarrow c^{-1} = (t, z, y, x)$

Obs: $S_{26} = 26!$

pt. ASCII: $S_{27} = 27!$

Condiții
1) Criptarea și decriptarea trebuie să se realizeze ușor
2) Găsirea funcției α^{-1} (cât de dată și a lui α) trebuie să fie dificilă pt un interpus

→ Codul lui Caesar
- se deplasează fiecare literă la dreapta cu 3 poziții

Literele inițiale:	a	b	c	d	e	...	u	v	x	y	z
Literele codate:	D	E	F				Y	Z	A	B	C

cad ⟼ FDG

Fiecărei litere îi asociem un număr de la 0 la 26

a	b	c	...	z
↓	↓	↓		↓
0	1	2		25

$\in \mathbb{Z}(26)$

Procesul de criptare = stabilirea unei bijecții între $\mathbb{Z}(26) \longrightarrow \mathbb{Z}(26)$

→ Criptarea Caesar se va realiza cu ajutorul funcției

$f: \mathbb{Z}(26) \longrightarrow \mathbb{Z}(26)$; $f(x) = x \oplus 3$

$f^{-1}: \mathbb{Z}(26) \longrightarrow \mathbb{Z}(26)$: $f^{-1}(y) = y \ominus 3$

$(-y)$ → simetricul lui y)

Mașina Enigma $f \in S_{26}$: $f^2 = e$ ⇒ f - produs de transpoziții disjuncte

↓ înlocuirea înformații

Criptări cu cheie publică

- Algoritmul de criptare este public
- Algoritmul folosit pentru descriptare este privat
- Criptarea este asimetrică, în sensul că determinarea algoritmului folosit la descriptare este mult mai dificilă decât determinarea celui pentru criptare

Exemple
- Algoritmul RSA (1977) (Rivest-Shamir-Adlemen)
  C. Cocks (1973) - raport ştiinţific secret
- Informaţia e codată în secvenţe de numere suficient de mari

Teoremă
Dacă p, q - prime cu $p \neq q$ şi $e, d \in \mathbb{N}^*$ a.î. $\varphi(p \cdot q) \mid ed-1$, atunci:
$\forall x \in \{0, \dots, pq-1\}$, $x^{ed} = x$ în $\mathbb{Z}(pq)$

Dem - se bazează pe teorema Euler-Fermat.

Criptare
1) se aleg 2 nr. prime p şi q suficient de mari
2) se calculează $m = p \cdot q$ şi $\varphi(m) = (p-1)(q-1)$
3) alegem $e \in \mathbb{N}^*$ a.î. $(e, \varphi(m)) = 1$.
4) facem publică cheia de criptare (m, e) cu algoritmul de criptare $x \longmapsto x^e$ în $\mathbb{Z}(m)$

Descriptarea
1) identificăm $d \in \mathbb{N}^*$ a.î. $e \cdot d = 1$ în $\mathbb{Z}(\varphi(m))$
2) construim algoritmul de criptare $y \longmapsto y^d$ din $\mathbb{Z}(m)$

Obs 1) $x \xmapsto{\text{criptare}} x^e$ în $\mathbb{Z}(m) \xmapsto{\text{descript}} x^e \longmapsto (x^e)^d = x^{ed} = x$ în $\mathbb{Z}(m)$

2) Informaţiile se partiţionează în blocuri de lungime cel mult m

3) Ca să găsim pe d din cheia publică (m, e) trebuie să descompunem $m = p \cdot q$, iar astfel de descompuneri durează foarte mult

$\mathbb{Z}_p$ - corp finit

$\mathbb{F}_{p^n}$ - corpuri finite cu p^n elemente