8. Aplicatii (15 aprilie 2019)

8.1. **Elemente de Aritmetică.**

Lema 8.1. *Fie $(A,+)$ un grup abelian şi $H,K \leq A$. Atunci $H \cap K$ şi $H+K = \{h+k \mid h \in H \text{ şi } k \in K\}$ sunt sungrupuri ale lui A.*

Propoziţia 8.2. *Considerăm grupul $(\mathbb{Z},+)$. Sunt adevărate afirmaţiile:*

(a) *O submulţime $H \subseteq \mathbb{Z}$ este subgrup în $\mathbb{Z}$ dacă şi numai dacă există $a \in \mathbb{N}$ astfel încât $H = a\mathbb{Z}$.*
(b) *Fie $a,b \in \mathbb{Z}$. Atunci*

$$a\mathbb{Z} \subseteq b\mathbb{Z} \Leftrightarrow b \mid a.$$

(c) *Dacă $a,b \in \mathbb{Z}^*$, atunci*
   (i) *$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, unde $m = [a,b]$;*
   (ii) *$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, unde $d = (a,b)$.*

Demonstraţie.

□

Corolarul 8.3. ***(Bézout)***
Fie $a,b \in \mathbb{Z}^*$ şi $d = (a,b)$. Atunci există $u,v \in \mathbb{Z}$ astfel încât

$$d = au + bv.$$

Reciproc, dacă există $u,v \in \mathbb{Z}$ astfel încât $1 = au+bv$, atunci $(a,b) = 1$.

Definiţia 8.4. Fie $n \in \mathbb{N}^*$. Numărul

$$\varphi(n) = |\{k \mid 0 < k \leq n \text{ şi } (k,n) = 1\}|$$

se numeşte *indicatorul lui Euler*.

Exemplul 8.5.

Corolarul 8.6. *Fie $n \in N$, $n \geq 2$ şi $a \in \mathbb{Z}$. Atunci*

$$(a, n) = 1 \Leftrightarrow \widehat{a} \text{ este inversabil în monoidul } (\mathbb{Z}_n, \cdot).$$

Prin urmare, $\varphi(n) = |U(\mathbb{Z}_n, \cdot)|$.

Definiţia 8.7. Fie $n \in \mathbb{N}$, $n \geq 2$. Relaţia definită pe $\mathbb{Z}$ de

$$a \equiv b (\mathrm{mod}\, n) \Leftrightarrow n \mid b - a$$

se numeşte *relaţia de congruenţă modulo n.*

Observaţia 8.8. Relaţia de congruenţă modulo n coincide cu relaţia de echivalenţă la stânga indusă de subgrupul $nZ \leq \mathbb{Z}$.

Teorema 8.9. ***(Teorema Euler-Fermat)***
Dacă $n \in \mathbb{N}$, $n \geq 2$ şi $a \in \mathbb{Z}$ este un număr astfel încât $(a, n) = 1$, atunci

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n).$$

Demonstraţie.

□

Corolarul 8.10. ***(Mica teoremă a lui Fermat)***
Dacă p este un număr prim şi $a \in \mathbb{Z}$ este un număr astfel încât p nu divide pe n, atunci

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Dacă p este un număr prim şi $a \in \mathbb{Z}$, atunci

$$a^p \equiv a (\mathrm{mod}\, p).$$

Teorema 8.11. *Dacă $m, n \in \mathbb{N}^*$ şi $(m, n) = 1$, atunci $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demonstraţie.

□

Corolarul 8.12. *Fie $n \in \mathbb{N}$, $n \geq 2$. Dacă $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ este descompunerea lui n ˆ i n produs de puteri nenule de numere prime diferite două câte două, atunci*

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{k}{p_k}).$$

Exemplul 8.13. 1) $n = p$ este număr prim

2) $n = pq$ cu $p \neq q$ numere prime.

8.2. **Criptografie cu cheie publică.**

Definiţia 8.14. **Criptografia** studiază metode de securizare a informaiei precum i de autentificare şi restricionare a accesului ntr-un sistem informatic.

Metodă de bază: transformarea (criptarea) informaţiilor/mesajelor astfel încât acestea să poată fi descifrate doar de către persoane/entităţi autorizate.

$$\boxed{\text{plaintext}} \Longrightarrow \text{criptare} \Longrightarrow \boxed{\text{cyphertext}} \Longrightarrow \text{decriptare} \Longrightarrow \boxed{\text{plaintext}}$$

Definiţia 8.15. Totalitatea cuvintelor necriptate (plaintext), a cuvintelor criptate (cypertext) şi a metodelor de criptare sau decriptare (chei) se numeşte *criptosistem*.

Observaţia 8.16. Un criptosistem constă în următoarele date:

- o mulţime $\mathcal{P}$ a cuvintelor necriptate;
- o mulţime $\mathcal{C}$ a cuvintelor criptate;
- o mulţime de funcţii $f : \mathcal{P} \to \mathcal{C}$, numite chei de criptare;
- o mulţime de funcţii $f : \mathcal{C} \to \mathcal{P}$, numite chei de criptare.

Observaţia 8.17. Un criptosistem trebuie să îndeplinească următoarele condiţii:

- să fie uşor de criptat (din punct de vedere al complexităţii algoritmilor folosiţi);
- dacă se cunoşte cheia de decriptare, să fie uşor de decriptat;
- dacă nu se cunoşte cheia de decriptare, să fie greu de decriptat.

Un sistem de criptare are cheia simetrică dacă avem nevoie de aceleşi informaţii pentru realizarea proceselor de criptare şi decriptare. In aceste situaţii atat metodele de criptare cât si cele de decriptare trebuie să fie secrete.

Exemplul 8.18. (Criptarea Caesar)

Exemplul 8.19. (Criptarea Vigenère)

Sisteme de criptare cu cheie asimetrică: sisteme în care din cheia de criptare/decriptare nu se poate deduce cheia de decriptare/criptare.

Sistemul cu cheie publică RSA (Rivest-Shamir-Adleman)

Algoritmii cu cheie publică au următoarele caracteristici:

- cheia de criptare este cunoscută de toţi cei care doresc să trimită un mesaj către destinatar;
- cheia de decriptare este privată, ea fiind cunoscută doar de către destinatarii autorizaţi;
- probabilitatea ca folosind un algoritm bazat pe cheia publică să se poată decripta un mesaj în timp util este foarte mică.

Protocolul de realizare a unui criptosistem RSA:

(I) **Construcţia cheii publice**
  (a) se aleg două numere prime p şi q suficient de mari;
  (b) calculăm $m = pq$ şi $\varphi(m) = (p-1)(q-1)$;
  (c) alegem (aleator) un număr $e > 1$ astfel încât $(e, \varphi(m)) = 1$;
  (d) cheia publică de criptare este (m, e).

(II) **Construcţia cheii private**

(i) se rezovă ecuaţia $ex \equiv 1(\mathrm{mod}\,\varphi(m))$ şi se alege o soluţie $d \in \{1, \ldots, \varphi(m)\}$;
(ii) cheia privată de decriptare este (m, d).

Criptarea se realizează astfel:

- Se imparte mesajul numeric (binar) în blocuri de lungime mai mică decât lungimea lui m.
- Dacă b este numărul dat de un astfel de bloc, atunci se consideră corespondenţele:

$$b \mapsto \widehat{b} \in \mathbb{Z}_m \mapsto \widehat{b}^e \in \mathbb{Z}_m \mapsto c,$$

unde $0 \leq c \leq m-1$ are proprietatea că $\widehat{c} = \widehat{b}^e$.

Decriptarea: dacă se recepţionează c, calculăm $\widehat{c}^d$ în $\mathbb{Z}_m$ şi alegem $b \in \{0, \ldots, m-1\}$ astfel încât $\widehat{b} = \widehat{c}^d$.

Propoziţia 8.20. *Fie p şi q două numere prime. Dacă $\overline{e} \cdot \overline{d} = 1$ în $\mathbb{Z}_{\varphi(pq)}$, atunci:*

$$\forall \widehat{b} \in \mathbb{Z}_{pq},\ \widehat{b}^{\,ed} = \widehat{b} \text{ în } \mathbb{Z}_{pq}.$$

Demonstraţie.

□

Exemplul 8.21. I. Criptarea:

- cheia publică $(m, e) = (2823907, 3)$;
- plaintext: $b = 71520$;
- criptarea: $\widehat{b}^3 = \widehat{83246}$ în $\mathbb{Z}_m$;
- cypertext: $c = 83246$;

II. Decriptarea:

- factorizăm $m = 1223 \cdot 2309$ (găsirea factorilor unui număr se bazează momentan pe algoritmi care au timp de rulare exponenţial);
- calculăm $\varphi(m) = 1222 \cdot 2308 = 2320376$;

- rezolvăm în $\mathbb{Z}_{2320376}$ ecuaţia $\overline{3} \cdot \overline{d} = \overline{1}$ şi găsim soluţia $\overline{d} = \overline{1880251}$;
- cheia privată este: $(2823907, 1880251)$;
- decriptarea: $\widehat{c}^d = \widehat{\overline{83246}}^{1880251} = \widehat{\overline{71520}}$ în $\mathbb{Z}_m$.

Observaţia 8.22. Dacă vrem să aflăm numărul d, ştiind m şi e, atunci trebuie să-l aflăm pe $\varphi(m)$. Se poate domnstra că aflarea lui $\varphi(m)$ este la fel de dificilă ca descompunerea lui m în factori primi.

Observaţia 8.23. Schimbarea unei singure cifre a lui b poate modifica foarte mult forma cuvântului criptat.

In exemplul anterior, daca criptăm $b = 71510$ obţinem $c = 2389184$.