Tema 6

Exerciţiul 1. *Determinaţi inversele următoarelor elemente:*

(i) $\hat{3}$ *în* $(\mathbb{Z}_{100}, \cdot)$*;* *(ii)* $\hat{99}$ *în* $(\mathbb{Z}_{1000}, \cdot)$*.*

Exerciţiul 2. *(i) Fie* p, q *două numere prime distincte. Câte elemente inversabile conţine monoidul* $(\mathbb{Z}_{pq}, \cdot)$*?*

(ii) Dacă $n \in \mathbb{Z}$ *şi* $(n, pq) = 1$*, atunci*

$$n^{(p-1)(q-1)} \equiv 1 (\mathsf{mod} pq)$$

Exerciţiul 3. *Un* criptosistem cu cheie publică *constă din alegerea unui număr cu câteva sute de cifre* N*, care este produsul a două numere prime* p *şi* q *de aproximativ aceeaşi mărime, precum şi a unui întreg pozitiv* r *(*cheia publică de încifrare*), care este prim cu* $(p-1)(q-1)$*.*

(i) Arătaţi că există atunci un întreg pozitiv s *(*cheia secretă de descifrare*) astfel încât*

$$rs \equiv 1 (\mathsf{mod} (p-1)(q-1))$$

(ii) Deduceţi că dacă un mesaj $u \in \{1, \ldots, N-1\}$ *este trimis "încifrat" sub forma* $v \equiv u^r (\mathsf{mod} N)$*, iar* u *este prim cu* N*, atunci "descifrarea" (regăsirea lui* u*) se poate face ridicând pe* v *la puterea* s *şi luând restul la împărţirea cu* N*.*

Exerciţiul 4. *Fie* d *o dreaptă din plan şi* O *un punct de pe* d*. Fie* R *rotaţia în sens trigonometric cu unghiul* $\frac{2\pi}{3}$ *în jurul lui* O*,* S_0 *simetria faţă de dreapta* d *şi* S_k *simetria faţă de dreapta obţinută prin rotaţia (în sens trigonometric) lui* d *în jurul punctului* O*, cu unghiul* $\frac{k\pi}{3}$*,* $k \in \{1, 2\}$*.*

(i) Arătaţi că R *şi* S_0 *(privite ca elemente ale grupului funcţiilor bijective ale planului în el însuşi, cu operaţia de compunere) verifică* $R^3 = I$*,* $S_0^2 = I$ *şi* $R^k S_0 = S_k$*,* $k \in \{1, 2\}$*, unde am notat cu* I *transformarea identică a planului.*

(ii) Arătaţi că $\{I, R, R^2, S_0, S_1, S_2\}$ *formează un grup în raport cu compunerea (scrieţi şi tabla operaţiei).*

(iii) Este acest grup izomorf cu $(\mathbb{Z}_8, +)$*?*

Exerciţiul 5. *Determinaţi, dacă este posibil, un polinom ireductibil de grad* n *peste corpul* $\mathbb{k}$*, unde*

(i) $n = 3$, $\Bbbk = \mathbb{Q}$. *(iii)* $n = 4$, $\Bbbk = \mathbb{R}$.

(ii) $n = 2$, $\Bbbk = \mathbb{Z}_{11}$. *(iv)* $n = 2$, $\Bbbk = \mathbb{C}$.

Exerciţiul 6. *(i) Determinaţi polinoamele ireductibile de grad cel mult* 2 *din* $\mathbb{Z}_2[X]$ *şi din* $\mathbb{Z}_3[X]$.

(ii) Utilizând rezultatele obţinute anterior, scrieţi tablele operaţiei de înmulţire pentru corpul cu 4 *elemente, respectiv corpul cu* 9 *elemente.*

Exerciţiul 7. *(i) Pe mulţimea* $\mathbb{Z} \times \mathbb{Z}$ *consideră relaţia de ordine* produs

$$(x, y) \leq (x', y') \Longleftrightarrow x \leq x' \text{ şi } y \leq y', \forall x, x', y, y' \in \mathbb{Z}$$

Devine astfel $\mathbb{Z} \times \mathbb{Z}$ *o latice?*

(ii) Dar dacă pe $\mathbb{Z} \times \mathbb{Z}$ *luăm relaţia de ordine* lexicografică*, dată de*

$$(x, y) \leq (x', y') \Longleftrightarrow \begin{cases} x \leq x' \text{ sau} \\ x = x' \text{ şi } y \leq y' \end{cases} \quad \forall x, x', y, y' \in \mathbb{Z}$$

Este atunci $\mathbb{Z} \times \mathbb{Z}$ *o latice?*

Exerciţiul 8. *Fie* A *şi* B *două mulţimi nevide şi* $f : A \longrightarrow B$ *o funcţie. Arătaţi că mulţimea* $\{f(X) \subseteq B \mid X \subseteq A\}$ *formează o latice în raport cu relaţia de incluziune (am notat* $f(X) = \{f(x) \mid x \in X\}, \forall X \subseteq A$*).*