Algebră ID

Fie G o mulţime şi $*$ o operaţie pe G (adică $*$ este o funcţie definită pe $G \times G$ cu valori în mulţimea G; în loc de $*((x,y))$ se notează tradiţional $x * y$).

Definiţie: Mulţimea G împreună cu operaţia $*$ formează un grup (notat cu $(G,*)$) dacă au loc următoarele proprietăţi:

1) $x*(y*z) = (x*y)*z$, pentru orice $x,y,z \in G$. Această proprietate a operaţiei $*$ se numeşte asociativitate.

2) Există un element $e \in G$ astfel încât $e*x = x*e = x$ pentru orice $x \in G$. [e se numeşte elementul neutru al grupului G; el este unic]

3) Pentru orice $x \in G$, există $y \in G$ astfel încât $x*y = y*x = e$. [y se numeşte inversul lui x; el este unic]

Dacă în plus $x*y = y*x$, pentru orice $x,y \in G$, grupul se numeşte comutativ.

Observaţie: Dacă avem $g*x = g*y$, într-un grup $(G,*)$, atunci $x = y$.

Exemple de grupuri:

1) $(\mathbb{R},+)$, $(\mathbb{Q}^*,\cdot)$, unde $+$ şi $\cdot$ sunt adunarea şi înmulţirea obişnuită de numere reale (respectiv raţionale). Inversul lui 3 în primul grup este -3 iar inversul lui 3 în al doilea grup este $\frac{1}{3}$.

2) Fie $n \geq 2$ un număr natural. Vom descrie în continuare grupul $(\mathbb{Z}_n,+)$ (grupul claselor de resturi modulo n cu adunarea). Fie $a,b \in \mathbb{Z}$. Scriem $a \equiv b \pmod{n}$ (şi spunem că "a este congruent cu b modulo n") dacă n divide $a-b$. Acelaşi lucru îl notăm şi cu $\overline{a} = \overline{b}$ (spunem că "clasa lui a modulo n este egală cu clasa lui b modulo n"). Vom nota cu $\mathbb{Z}_n = \{\overline{a} | a \in \mathbb{Z}\}$. Aceasta este o mulţime cu n elemente. Pe ea se defineşte următoarea operaţie:

$$\overline{a} + \overline{b} = \overline{a+b}, \forall a,b \in \mathbb{Z}.$$

Este uşor de văzut că $(\mathbb{Z}_n,+)$ este un grup comutativ cu n elemente. Elementul neutru este $\overline{0}$.

Exerciţiu: Inversul lui $\overline{3}$ în grupul $(\mathbb{Z}_{10},+)$ este $\overline{7}$.

3) Cu notaţiile de mai sus, vom considera mulţimea

$$U(\mathbb{Z}_n) = \{\overline{m} | m \in \mathbb{Z}, (m,n) = 1\}.$$

Se defineşte următoarea operaţie pe $U(\mathbb{Z}_n)$:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}, \forall \overline{a}, \overline{b} \in U(\mathbb{Z}_n).$$

$U(\mathbb{Z}_n), \cdot)$ este un grup comutativ cu $\phi(n)$ elemente; elementul neutru este $\overline{1}$. Funcţia ϕ se numeşte funcţia lui Euler. Avem următoarea formulă:

$$\phi(n) = n \cdot \prod_{p \ prim, \ p|n} (1 - \frac{1}{p}), \forall n \in \mathbb{N}^*.$$

Exemplu: $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$.

Exemplu: Să se calculeze inversul lui $\overline{37}$ în $U(\mathbb{Z}_{100}, \cdot)$. Inversul căutat este $\overline{73}$ deoarece

$$\overline{37} \cdot \overline{73} = \overline{2701} = \overline{1}.$$

Procedură de calcul pentru inversul lui $\overline{a}$ în grupul $(U(\mathbb{Z}_n), \cdot)$ (une $a < n$ este un număr natural, prim cu n):

Se scrie algoritmul lui Euclid pentru a şi n. Ultimul rest nenul va fi 1. Avem egalităţile:

$$n = a \cdot q_1 + r_1,$$
$$a = r_1 \cdot q_2 + r_2,$$
$$\vdots$$
$$r_{m-2} = r_{m-1} \cdot q_m + r_m,$$
$$r_{m-1} = r_n \cdot q_{m+1},$$

unde câturile şi resturile sunt numere naturale cu

$$a > r_1 > r_2 > ... > r_{m-1} > r_m = 1.$$

Se calculează fracţia ireductibilă

$$\frac{A}{B} = q_1 + \frac{1}{q_2 + \frac{1}{\vdots + q_{m-1} + \frac{1}{q_m}}}.$$

Avem următorul rezultat:

$$\frac{n}{a} - \frac{A}{B} = \frac{(-1)^{m+1}}{a \cdot B}.$$

De aici deducem uşor că

$$\overline{a} \cdot \overline{(-1)^m \cdot A} = \overline{1}.$$

Ne întoarcem la exemplul anterior: calculul inversului lui $\overline{37}$ în $U(\mathbb{Z}_{100}, \cdot)$. Urmăm procedura descrisă anterior:

$$100 = 37 \cdot 2 + 26,$$
$$37 = 26 \cdot 1 + 11,$$
$$26 = 11 \cdot 2 + 4,$$
$$11 = 4 \cdot 2 + 3,$$
$$4 = 3 \cdot 1 + 1.$$
$$3 = 1 \cdot 3.$$

Calculăm fracţia

$$\frac{A}{B} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} = 2 + \frac{1}{1 + \frac{3}{7}} = 2 + \frac{7}{10} = \frac{27}{10}.$$

Avem

$$\frac{100}{37} - \frac{27}{10} = \frac{(-1)^6}{37 \cdot 27},$$
$$100 \cdot 10 - 37 \cdot 27 = 1,$$
$$\overline{37} \cdot \overline{(-27)} = \overline{1}.$$

Deoarece $\overline{-27} = \overline{73}$ în $\mathbb{Z}_{100}$, regăsim rezultatul anterior: inversul lui $\overline{37}$ este $\overline{73}$ în grupul $U(\mathbb{Z}_{100}, \cdot)$.

4) Fie $n \in \mathbb{N}^*$. Se notează cu S_n mulţimea permutărilor cu n elemente (adică funcţiile bijective

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

Se defineşte operaţia $\circ$ pe S_n în felul următor:

$$\sigma \circ \tau(j) = \sigma(\tau(j)), \forall \sigma, \tau \in S_n, j = \overline{1, n}.$$

$(S_n, \circ)$ este un grup cu $n!$ elemente. Dacă $n \geq 3$, acest grup nu este comutativ. O permutare σ din S_n se notează în mod tradiţional ca o matrice cu două linii şi n coloane. Pe prima linie se pun în ordine numerele $1, 2, \ldots, n$. Pe linia a doua se pune sub j numărul $\sigma(j)$. Cum se calculează inversa unei permutări în grupul $(S_n, \circ)$? Se inversează cele două linii şi apoi se ordonează numerele de pe prima linie.

Exemplu: să se calculeze inversa matricii $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Inversarea celor două linii produce permutarea $\tau = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$. Ordonând numerele din prima linie (şi valorile care le corespund în a doua), găsim următoarea descriere pentru τ, inversa lui σ:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4.$$

Pentru permutări se defineşte conceptul de signatură al permutării $\sigma \in S_n$. Pentru aceasta, definim întâi ce înseamnă o inversiune a permutării σ; o pereche (i, j), cu

i, j numere naturale din mulţimea $\{1, 2, \ldots, n\}$ astfel încât $i < j$ şi $\sigma(i) > \sigma(j)$. Notăm cu m numărul de inversiuni ale permutării σ. Signatura permutării σ se notează cu $\epsilon(\sigma)$ şi este numărul

$$\epsilon(\sigma) = (-1)^m.$$

Signatura unei permutări are următoarea proprietate:

$$\epsilon(\sigma \circ \tau) = \epsilon(\sigma) \cdot \epsilon(\tau), \forall \sigma, \tau \in S_n.$$

Exemplu: calculaţi signatura permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Inversiunile permutării σ sunt perechile: $(1,4), (2,4), (3,4)$. Deci $m = 3$ şi $\epsilon(\sigma) = (-1)^3 = -1$.

Teoreme:

1) (Lagrange) Într-un grup finit $(G, *)$, avem că $g^{|G|} = e$, pentru orice $g \in G$. Prin g^n înţelegem $g^n = g * g * ... * g$, unde semnul $*$ apare de $n-1$ ori. Prin convenţie, $g^0 = e$. Am notat cu e elementul neutru al grupului G şi prin $|G|$ cardinalul mulţimii G.

2) Dacă n este un număr natural nenul şi a este un număr întreg prim cu n, atunci n divide $a^{\phi(n)} - 1$ (Teoremă lui Euler). Acest rezultat este o consecinţă a teoremei lui Lagrange.

3) Dacă p este un număr prim şi a este un număr întreg care nu se divide cu p, atunci p divide $a^{p-1} - 1$ (Mica Teoremă a lui Fermat). Acest rezultat este un caz particular al teoremei lui Euler.

4) Dacă p este un număr prim, atunci p divide $(p-1)! + 1$ (teorema lui Wilson).

Exerciţii:

1) Care sunt ultimele două cifre ale numărului 37^{79}? Din teorema lui Euler ştim că

$$\overline{37}^{\phi(100)} = \overline{1}$$

în $U(\mathbb{Z}_{100})$. Dar $\phi(100) = 40$ (vezi un calcul anterior). Deducem că $\overline{37}^{79}$ este inversul lui $\overline{37}$ în grupul $(U(\mathbb{Z}_{100}), \cdot)$. Acest invers era $\overline{73}$ (vezi exerciţiu anterior). Deducem că ultimele două cifre ale numărului 37^{79} sunt 73.

2) Care este restul împărţirii lui $n = 2^{39} + 3^{39}$ la 41?

Din Mica teoremă a lui Fermat ştim că $2^{40} \equiv 3^{40} \equiv 1 \pmod{41}$. Atunci

$$6n \equiv 3 + 2 \equiv 5 \equiv -36 \pmod{41}.$$

Deducem că

$$n \equiv -6 \equiv 35 \pmod{41}.$$

Restul căutat este 35.

3) Care este restul împărţirii lui $n = 38! + 1$ la 41? Din teorema lui Wilson ştim că

$$40! \equiv -1 \pmod{41}.$$

Avem că $39 \cdot 40 \cdot n \equiv -1 + 39 \cdot 40 \pmod{41}$. Dar

$$39 \cdot 40 \equiv (-2) \cdot (-1) \equiv 2 \pmod{41}$$

şi deci

$$2n \equiv 1 \equiv 42 \pmod{41}.$$

De aici rezultă imediat că $n \equiv 21 \pmod{41}$.

Definiţie; Fie $(G, *)$ un grup finit (cu elementul neutru e) şi $g \in G$. Se notează cu $ord(g)$ cel mai mic număr natural nenul k cu proprietatea că $g^k = e$ (se numeşte ordinul lui g în grupul $(G.*)$). Proprietăţile ordinului:

1) $g^{ord\, g} = e$.

2) Dacă $g^k = e$ (unde k este un număr natural), atunci $ord(g)$ divide k.

3) Ordinul lui g divide întotdeauna cardinalul lui G.

4) $ord(g^k) = \frac{ord(g)}{(ord(g),k)}$, pentru orice $k \in \mathbb{N}$.

5) Dacă $g * h = h * g$, $ord(g) = n, ord(h) = m$ şi $(m, n) = 1$ atunci

$$ord(g * h) = ord(g) \cdot ord(h).$$

Exerciţii:

1) Să se calculeze ordinul lui $\overline{52}$ în grupul $(\mathbb{Z}_{100}, +)$. Notăm $k = ord(\overline{52})$. k este cel mai mic număr natural nenul pentru care $\overline{52k} = \overline{0}$. Deci $k = 25 = ord(\overline{52})$.

2) Să se calculeze $ord(\overline{52})$ în grupul $(U(\mathbb{Z}_{59}, \cdot)$. Să notăm cu k acest ordin. Din proprietatea 3) ştim că k divide $|U(\mathbb{Z}_{59}| = \phi(59) = 58$. Deci

$$k \in \{1, 2, 29, 58\}.$$

Singurul element de ordin 1 este elementul neutru, deci $k \neq 1$. Avem $\overline{52}^2 = (\overline{-7})^2 = \overline{49} = \overline{-10}$; deci $k \neq 2$. Trebuie să calculăm $\overline{52}^{29}$. Avem

$$\overline{52}^4 = \overline{100} = \overline{-18}, \overline{52}^8 = \overline{324} = \overline{29},$$

$$\overline{52}^{14} = \overline{52}^8 \cdot \overline{52}^4 \cdot \overline{52}^2 = \overline{29} \cdot (\overline{-18}) \cdot (\overline{-10}) = \overline{29} \cdot \overline{3} = \overline{28},$$

$$\overline{52}^{29} = (\overline{52}^{14})^2 \cdot \overline{52} = \overline{28}^2 \cdot (\overline{-7}) = \overline{-7 \cdot 17} = \overline{-1}.$$

Din calculele anterioare deducem că $k \neq 29$; deci $ord(\overline{52}) = k = 58$.

3) Cum se calculează ordinul unei permutări?

a) se descompune în cicli disjuncţi b) se calculează cel mai mic multiplu comun al lungimilor ciclilor; acesta este ordinul permutării

a) Scriem $\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_m$, unde $\sigma_j = (a_1, a_2, ..., a_k)$ este următoarea permutare ($a_1, a_2, ..., a_m$ sunt numere naturale distincte din intervalul $\{1, 2, .., n\}$):

$$\sigma_j(a_i) = a_{i+1}, \forall i = \overline{1, k-1}, \sigma_j(a_k) = a_1; \sigma_j(x) = x, \forall x \neq a_i.$$

Descompunerea în cicli disjuncţi presupune că un număr a_t din ciclul σ_j este diferit de orice număr b_s dintr-un ciclu σ_u, cu $u \neq j$. Ciclul $\sigma_j = (a_1, a_2, ..., a_k)$ are lungimea k.

b) $ord(\sigma)$ este cel mai mic multiplu comun al lungimilor ciclilor disjuncţi din descompunerea lui σ.

Exemplu: să se calculeze ordinul permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix} \in S_7$. Găsim descompunerea în cicli disjuncţi $\sigma = (1, 2, 3, 4) \circ (5, 6, 7)$.

$$ord(\sigma) = [4, 3] = 12.$$

4) Cum să găseşti factori primi ai unui număr mare?

Exemplu: arătaţi că $65537 = 2^{16} + 1$ este număr prim. Deoarece $[\sqrt{2^{16} + 1}] = 2^8 = 256$, trebuie să arătăm că numărul 65537 nu are factori primi mai mici decât 256. Fie p un număr prim care-l divide pe 65537. Atunci

$$2^{16} \equiv -1 \pmod{p} \tag{1}$$

şi

$$2^{32} \equiv 1 \pmod{p}. \tag{2}$$

Notăm cu k ordinul lui $\overline{2}$ în grupul $(U(\mathbb{Z}_p), \cdot)$. Din formula (2) şi din proprietatea 2) a ordinului ştim că k este un divizor al lui 32. Dacă cumva k divide 16, atunci

$$2^{16} \equiv (2^k)^{\frac{16}{k}} \equiv 1 \pmod{p};$$

am folosit proprietatea 1) a ordinului. Combinând această informaţie cu formula (1) ajungem la o contradicţie:

$$-1 \equiv 2^{16} \equiv 1 \pmod{p}, p = 2.$$

Deci k nu divide 16 şi divide 32. Neapărat $k = 32$. Din proprietatea 3) a ordinului ştim că $32 = k = ord(\overline{2})$ este un divizor al cardinalului grupului $(U(\mathbb{Z}_p), \cdot)$. Acest număr este $\phi(p) = p - 1$. Am descoperit deci că $p = 1 + 32 \cdot t$, pentru un număr natural t. Inspectând numerele prime $p = 1 + 32 \cdot t < 256$, găsim doar două: $p = 97$ şi $p = 193$. Verificăm dacă 65537 se divide cu 97 sau 193:

$$65537 = 97 \cdot 675 + 62, 65537 = 193 \cdot 339 + 110.$$

Din toate argumentele precedente deducem că $65537 = 2^{16} + 1$ este număr prim.

Lucrarea nr. I

1) Găsiţi numărul $x \in \{0, 1, 2, ..., 2020\}$ astfel încât $97 \cdot x \equiv 1 \pmod{2021}$.

2) Găsiţi acel număr $x \in \{0, 1, 2, ..., 428\}$ astfel încât să fie îndeplinite simultan condiţiile $x \equiv 2 \pmod 3, x \equiv 2 \pmod{11}, x \equiv 8 \pmod{13}$.

3) Câte submulţimi $A \subseteq \{1, 2, 3, 4, 5, 6\}$ au proprietatea că nu conţin "vecini" (adică nu există j natural cu $\{j, j+1\} \subseteq A$)?

4) Decriptaţi DNSDDS, criptat cu metoda Vigenère (cu alfabetul standard latin de 26 de litere, ordonate în mod obişnuit); cuvântul cheie are 2 litere.

Lucrarea nr. II

1) Cât este restul împărţirii lui 2^{149} la 323 (formulare echivalentă: criptaţi litera C folosind RSA cu $n = 323, e = 149$ şi alfabetul latin standard de 26 de litere)?

2) Calculaţi restul împărţirii lui $6^{99} + 3^{99} + 2^{99}$ la 101.

3) Fie $(G, *)$ un grup cu 211 eleemnte. Câte elemente $g \in G$ au proprietatea că $g^3 = e$?

4) Fie $\sigma \in S_{36}$ definită prin faptul că $\sigma(x)$ este unicul număr din $\{1, 2, 3..., 36\}$ astfel încât $\sigma(x) \equiv 3x \pmod{37}$. Să se calculeze ordinul permutării σ.

Lucrarea nr. III

1) Să se calculeze $ord(\overline{2})$ în grupul $(U(\mathbb{Z}_{47}), \cdot)$.

2) Găsiţi $a \in \{1, 2, 3...22\}$ cu proprietatea că $ord(\overline{a}) = 22$ în grupul $(U(\mathbb{Z}_{23}), \cdot)$.

3) Care este cel mai mic factor prim al numărului $2^{24} + 1$?

4) Găsiţi cel mai mare ordin al unei permutări din S_{12}.

Lucrarea nr. IV

1) Rezolvaţi ecuaţia $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix}$, în S_9.

2) Găsiţi $x \in \{1, 2, 3, ..., 58\}$ astfel încât $2^x \equiv 29 \pmod{59}$.

3) Să se calculeze cardinalul mulţimii $A = \{x \in \mathbb{N} | x \leq 200, (x, 30) = 1\}$.

4) Câte submulţimi $A \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ au proprietatea că nu conţin "vecini" (adică nu există j natural cu $\{j, j+1\} \subseteq A$)?