

Examen scris  
Structuri Algebrice în Informatică  
25/01/2021

Nume: .....

Punctaj parțial 1.....

Prenume: .....

Punctaj parțial 2.....

**IMPORTANT!!.** Punctul din oficiu este acordat pentru aflarea lui  $a$  și  $b$  pe care, ulterior, le veți înlocui în toate enunțurile problemelor. Pe foile voastre de examen veți scrie enunțurile problemelor cu  $a$  și  $b$  înlocuite cu valorile anterior determinate.

$a = \dots,$

$b = \dots,$

unde

- (1)  $a$  este egal cu maximum dintre numerele de litere ale cuvintelor care compun numele vostru de familie. (de exemplu, dacă numele de familie este Popescu-Simion atunci  $a = 7$ , maximum dintre 7 (nr. de litere al cuvântului Popescu) și 6 (nr. de litere al cuvântului Simion); dacă numele de familie este Moiescu atunci  $a = 8$ )
- (2)  $b$  este egal cu maximum dintre numerele de litere ale cuvintelor care compun prenumele vostru. (de exemplu, dacă prenumele este Andreea-Beatrice-Luminița atunci  $b = 8$ , maximum dintre 7 (nr. de litere al cuvântului Andreea) și 8 (nr. de litere atât al cuvântului Beatrice cât și al cuvântului Luminița).)

Problema	Punctaj	Total
1	1	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	
8	1	
9	1	
oficiu	1	
Total	10	

**Justificați toate răspunsurile!**

- Există permutări de ordin  $a \cdot b - 1$  în grupul de permutări  $S_{a+b}$ ?
- Se consideră permutarea  $\sigma = (1, \dots, a)(a+1, \dots, a+b)$ , un produs de 2 cicli disjuncți de lungime  $a$ , respectiv  $b$ , din  $S_{a+b}$ . Determinați toate permutările  $\tau \in S_{a+b}$  astfel încât  $\tau^3 = \sigma$ .
- Calculați  $a^{a^b} \pmod{31}$ .
- Considerăm polinomul cu coeficienți întregi  $P(X) = X^3 - aX + b$ . Determinați dacă polinomul  $P(X)$  este ireductibil în  $\mathbb{Q}[X]$ .
- Determinați numărul elementelor de ordin 8 din grupul produs direct  $(\mathbb{Z}_{2^a}, +) \times (\mathbb{Z}_{2^b}, +)$ .
- Fie  $p$  cel mai mic număr prim din descompunerea în factori primi a lui  $a$  și  $q$  cel mai mare număr prim mai mic sau egal cu  $a+b$ , diferit de  $p$ . Pentru un număr natural nenul  $n$  notăm cu  $\exp_p(n)$  exponentul la care apare  $p$  în descompunerea în factori primi a lui  $n$ . Considerăm pe  $\mathbb{N}$  relația binară  $\rho$  dată astfel:  $m\rho n$  dacă  $\exp_p(n) = \exp_p(m)$  și  $\exp_q(n) = \exp_q(m)$ . Să se arate că  $\rho$  este relație de echivalență, să se calculeze clasele de echivalență ale lui  $a$  și  $b$  și să se determine un sistem complet de reprezentanți pentru această relație de echivalență.
- Se consideră funcția  $f : \mathbb{R} \mapsto \mathbb{R}$  definită astfel:
$$f(x) = \begin{cases} ax + b(1+a), & \text{dacă } x < -b, \\ ax^2 + 2a(a-1)x + a^3 - 2a^2 + a + b, & \text{dacă } x \geq -b. \end{cases}$$
Decideți dacă funcția  $f$  este injectivă, surjectivă, respectiv bijectivă. Calculați  $f^{-1}([-b-1, b+1])$ .
- Demonstrați că inelul factor  $\mathbb{Q}[X]/(X^2 - a^2 - a)$  este izomorf cu inelul  $(\mathbb{Q}[\sqrt{a^2+a}], +, \cdot)$ , unde  $\mathbb{Q}[\sqrt{a^2+a}] = \{\alpha + \beta\sqrt{a^2+a} \mid \alpha, \beta \in \mathbb{Q}\}$ .
- Determinați constantele  $c, d \in \mathbb{Q}$  astfel încât polinoamele  $X^b - aX + 1$  și  $cX + d$  să fie în aceeași clasă de echivalență în inelul  $\mathbb{Q}[X]/(X^2 - a^2 - a)$ .

# Examen Structuri algebrice în informatică

$$a = 4$$

$$b = 9$$

$$1. a \cdot b - 1 = 4 \cdot 9 - 1 = 35$$

$$S_{13}$$

ordin 35 în  $S_{13}$

$$35 = 5 \cdot 7$$

O permutare posibilă din  $S_{13}$  de ordin 35 ( $= 5 \cdot 7$ ) este formată dintr-un ciclu de lungime 5 și un ciclu de lungime 7.

$$\text{Ex: } \tau = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12)$$

$$2. \tau = (1 \ 2 \ 3 \ 4)(5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13)$$

$$\tau \in S_{13}, \tau^3 = \tau$$

$$\text{sgn}(\tau) = (-1)^{4-1} \cdot (-1)^{9-1} = (-1)^3 \cdot (-1)^8 = -1 \Rightarrow \tau \text{ permutare impară}$$

$\Rightarrow \tau^3$  permutare impară

Fie  $\tau = C_{i_1} \cdot C_{i_2} \cdot \dots \cdot C_{i_k}$  descompunerea lui  $\tau$  în produs de cicli disjuncti, unde  $\text{ord}(C_{i_j}) = i_j$  ( $\forall j$ ) și  $i_1 + i_2 + \dots + i_k = 13$

$$\tau^3 = C_{i_1}^3 \cdot C_{i_2}^3 \cdot \dots \cdot C_{i_k}^3$$

$C_{i_j}^3 \rightarrow 3 | i_j \Rightarrow C_{i_j}^3$  este produs de 3 cicli disjuncti de lungime egale cu  $i_j/3$

$\rightarrow 3 \nmid i_j \Rightarrow C_{i_j}^3$  este tot un ciclu de lungime  $i_j$ .

$(1 \ 2 \ 3 \ 4) \rightarrow$  a provenit tot dintr-un ciclu de lungime 4 deoarece  $3 \nmid 4$

$(5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13) \rightarrow$  a provenit tot dintr-un ciclu de lungime 9, Fals deoarece  $3 | 9$ .

~~$\rightarrow$  a provenit~~

$\Rightarrow$  Nu există permutări  $\tau \in S_{13}$  a.2.  $\tau^3 = \tau$

5. el. de ordin 8 din  $(\mathbb{Z}_{16}, +) \times (\mathbb{Z}_{512}, +)$

Fie  $(\hat{k}, \bar{l}) \in \mathbb{Z}_{16} \times \mathbb{Z}_{512}$ .

$$\text{ord}(\hat{k}, \bar{l}) = [\text{ord}(\hat{k}), \text{ord}(\bar{l})] = 8 = 2^3 \Rightarrow \begin{matrix} \text{ord}(\hat{k}) \mid 8 \\ \text{ord}(\bar{l}) \mid 8 \end{matrix}$$

$$\text{Lagrange} \Rightarrow \begin{matrix} \text{ord}(\hat{k}) \mid 16 \\ \text{ord}(\bar{l}) \mid 512 \end{matrix} \quad \begin{matrix} \text{ord}(\hat{k}) \mid 2^4 \\ \text{ord}(\bar{l}) \mid 2^9 \end{matrix}$$

$$D_{16} = \{1, 2, 2^2, 2^3, 2^4\}$$

$$D_{512} = \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$$

$$(\text{ord}(\hat{k}), \text{ord}(\bar{l})) \in \{(1, 8), (2, 8), (4, 8), (8, 8), (8, 1), (8, 2), (8, 4)\}$$

$$\text{ord}(\hat{k}) \in \{1, 2, 4, 8\}$$

$$\text{ord}(\bar{l}) \in \{1, 2, 4, 8\}$$

$$\text{ordin 1 in } \mathbb{Z}_{16} \quad \text{ord}(\hat{x}) = \frac{16}{(16, x)} = 1 \Rightarrow (16, x) = 1 \Rightarrow x = \hat{0}$$

$$\text{ordin 2 in } \mathbb{Z}_{16} \quad \text{ord}(\hat{x}) = \frac{16}{(16, x)} = 2 \Rightarrow (16, x) = 8 \Rightarrow x = \hat{8}$$

$$\text{ordin 4 in } \mathbb{Z}_{16} \quad \text{ord}(\hat{x}) = \frac{16}{(16, x)} = 4 \Rightarrow (16, x) = 4 \Rightarrow x \in \{\hat{4}, \hat{12}\}$$

$$\text{ordin 8 in } \mathbb{Z}_{16} \quad \text{ord}(\hat{x}) = \frac{16}{(16, x)} = 8 \Rightarrow (16, x) = 2 \Rightarrow x \in \{\hat{2}, \hat{6}, \hat{10}, \hat{14}\}$$

$$\text{ordin 1 in } \mathbb{Z}_{512} \quad \text{ord}(\hat{x}) = \frac{512}{(512, x)} = 1 \Rightarrow (512, x) = 512 \Rightarrow x = \bar{0}$$

$$\text{ordin 2 in } \mathbb{Z}_{512} \quad \text{ord}(\hat{x}) = \frac{512}{(512, x)} = 2 \Rightarrow (512, x) = 256 \Rightarrow x = \bar{256}$$

$$\text{ordin 4 in } \mathbb{Z}_{512} \quad \text{ord}(\hat{x}) = \frac{512}{(512, x)} = 4 \Rightarrow (512, x) = 128 \Rightarrow$$

$$\text{ordin 8 in } \mathbb{Z}_{512} \quad \text{ord}(\hat{x}) = \frac{512}{(512, x)} = 8 \Rightarrow (512, x) = 64 \Rightarrow$$

$$\Rightarrow x = \{128, 384\}$$

$$\# = \# \text{ord}(\hat{k})=1 \times \# \text{ord}(\bar{l})=8 + \# \text{ord}(\hat{k})=2 \times \# \text{ord}(\bar{l})=8 + \dots$$

$$\# = 1 \cdot 4 + 1 \cdot 4 + 2 \cdot 4 + 4 \cdot 4 + 4 \cdot 1 + 8 \cdot 1 + 4 \cdot 2$$

$$= 4 + 4 + 8 + 16 + 4 + 8 + 8 =$$

$$= 52$$

52 de el au ordin 8 in  $(\mathbb{Z}_{16}, +) \times (\mathbb{Z}_{512}, +)$

G

$$6. \quad a = 2^2 \Rightarrow p = 2$$

$$b = 3^2 \Rightarrow \cancel{g=3} \quad a+b=13 \Rightarrow g=13$$

$$\exp_2(m)$$

$$m \text{ p m } \begin{cases} \exp_2(m) = \exp_{13}(m) \\ \exp_{13}(m) = \exp_2(m) \end{cases}$$

$p$  rel. de echivalență dacă este reflexivă  
simetrică  
transitivă

$p$  reflexivă dacă  $a p a \quad (\forall a \in \mathbb{N})$

$$a p a \Rightarrow \begin{cases} \exp_2(a) = \exp_{13}(a) \\ \exp_{13}(a) = \exp_2(a) \end{cases} \quad \text{Adv.}$$

$p$  ~~simetrică~~ <sup>transitivă</sup> dacă  $a p b, b p c \Rightarrow a p c$

$$a p b \Rightarrow \begin{cases} \exp_2(a) = \exp_{13}(b) \\ \exp_{13}(a) = \exp_2(b) \end{cases}$$

$$b p c \Rightarrow \begin{cases} \exp_2(b) = \exp_{13}(c) \\ \exp_{13}(b) = \exp_2(c) \end{cases} \Rightarrow \begin{cases} \exp_2(a) = \exp_2(c) \\ \exp_{13}(a) = \exp_{13}(c) \end{cases}$$

$p$  simetrică dacă  $a p b \Rightarrow b p a$

$$a p b \Rightarrow \begin{cases} \exp_2(a) = \exp_{13}(b) \\ \exp_{13}(a) = \exp_2(b) \end{cases} \Leftrightarrow \begin{cases} \exp_2(b) = \exp_{13}(a) \\ \exp_{13}(b) = \exp_2(a) \end{cases} \Leftrightarrow b p a$$

$\Rightarrow p$  rel de echivalență

$$[a] = \{ b \in \mathbb{N} \mid a p b \} \Rightarrow [2^2] = \{ 13^2 \cdot \alpha, \alpha \in \mathbb{N} \} = [a]$$

$$[3^2] = \{ 13^0 \cdot \alpha, \alpha \in \mathbb{N} \} = [b]$$

$$SER = \{ (2 \cdot 13)^0, (2 \cdot 13)^1, (2 \cdot 13)^2, \dots \} =$$

$$= \{ 1, 26, 26^2, 26^3, \dots \}$$

$$4. \quad f(x) = \begin{cases} 4x + 45 & x < -9 \\ 4x^2 + 2 \cdot 12x + 64 + 32 + 4 + 9 & , x \geq -9 \end{cases}$$

$$\Rightarrow f(x) = \begin{cases} 4x + 45 & , x < -9 \\ 4x^2 + 24x + 45 & , x \geq -9 \end{cases}$$

~~Verificare~~ dacă

$f$  injectivă dacă  $(\forall) x, y \in \mathbb{R}$  cu  $f(x) = f(y) \Rightarrow x = y$

$$f(x) = f(y)$$

$$4x + 45 = 4y + 45 \Rightarrow x = y$$

$$4x^2 + 24x + 45 = 4y^2 + 24y + 45 \Rightarrow x = y$$

$$x(4x + 24) = y(4y + 24)$$

$f$  surjectivă dacă  $(\forall) y \in B, \exists x \in A$  a.i.  $f(x) = y$

8.  ~~$\mathbb{Q}[x]/(x^2)$~~

9.  $x^3 - 4x + 1, cx + d$

$$x^2 - 20 = 0$$

$$x^2 = 20 \Rightarrow x = \pm\sqrt{20}$$

$$x^3 - 4x + 1 = q_1(x) \cdot (x^2 - 4^2 - 4) + r$$

$$cx + d = q_2(x) \cdot (x^2 - 4^2 - 4) + r$$

$$(\sqrt{20})^3 - 4\sqrt{20} + 1 = r$$

$$\text{si } (-\sqrt{20})^3 + 4\sqrt{20} + 1 = r$$

$$c\sqrt{20} + d = r$$

$$-c\sqrt{20} + d = r$$

$$(\sqrt{20})^3 - 4\sqrt{20} + 1 = r$$

$$(-\sqrt{20})^3 + 4\sqrt{20} + 1 = r$$

$$\frac{\quad}{\quad} \quad \quad \quad 2 = 2r \Rightarrow r = 1 \Rightarrow c\sqrt{20} + d = 1$$

$$-c\sqrt{20} + d = 1$$

$$\frac{\quad}{\quad} \quad \quad \quad 2d = 2 \Rightarrow d = 1 \Rightarrow c = 0$$

3.  $4^4 \cdot 9^9 \pmod{31} =$

$$= (256)^9 \pmod{31} = (8)^9 \pmod{31} = (134214728)^9 \pmod{31}$$

4.  $P(x) = x^3 - 4x + 9$

$P(x)$  ireductibil în  $\mathbb{Q}[x]$  dacă nu are rădăcini în  $\mathbb{Q}[x]$

Fie  $x = \frac{p}{q}$  ( $p, q$  prime între ele) rădăcina a lui  $P(x)$  ( $P(x) = 0$ )

$p \in \{-9, -3, -1, 0, 1, 3, 9\}$  - divizorii termenului liber

~~$q \in \{-4, -2, -1, 0, 1, 2, 4\}$~~

$q \in \{-1, 0, 1\}$  - divizorii coeficientului dominant



$$P(3) = 429 - 4 \cdot 9 + 9 \neq 0$$

$$P(-9) = -429 + 4 \cdot 9 + 9 \neq 0$$

$$P(0) = 9 \neq 0$$

$$P(3) = 27 - 12 + 9 \neq 0$$

$$P(-3) = -27 + 12 + 9 \neq 0$$

$$P(1) = 1 - 4 + 9 \neq 0$$

$$P(-1) = -1 + 4 + 9 \neq 0$$

$\Rightarrow P(x)$  ireductibil în  $\mathbb{Q}[x]$

1. Există permutări de ordin  $4 \cdot 9 - 1$  în grupul de permutări  $S_{4+9}$
2. Se cons. permutarea  $\tau = (1 \dots 4)(5 \dots 13)$  un prod de 2 cicli disjuncti de lung 4, respectiv 9, din  $S_{13}$ . Det toate permutările  $T \in S_{13}$  a.i.  $T^3 = \tau$
3. Calculați  $4^{4^{9^9}} \pmod{31}$
4. Considerăm pol cu coef întregi  $P(x) = x^3 - 4x + 9$ . Det dacă polinomul  $P(x)$  este ireductibil în  $\mathbb{Q}[x]$ .
5. Determinați numărul elementelor de ordin 8 din grupul produs direct  $(\mathbb{Z}_{24}, +) \times (\mathbb{Z}_9, +)$ .
8. Demonstrați că inelul factor  $\mathbb{Q}[x]/(x^2 - 16 - 4)$  este izomorf cu inelul  $(\mathbb{Q}[\sqrt{20}], +, \cdot)$ , unde  $\mathbb{Q}[\sqrt{20}] = \{\alpha + \beta\sqrt{20}, \alpha, \beta \in \mathbb{Q}\}$ .
9. Determinați constantele  $c, d \in \mathbb{Q}$  a.i. polinoamele  $x^3 - 4x + 1$  și  $cx + d$  să fie în aceeași clasă de echivalență în inelul  $\mathbb{Q}[x]/(x^2 - 20)$ .
- \* Se cons. funcția  $f: \mathbb{R} \rightarrow \mathbb{R}$ 

$$f(x) = \begin{cases} 4x + 45 \\ 4x^2 + 24x + 45 \end{cases}$$

Decideți dacă  $f$  e inj, surj, bij. Calculați  $f^{-1}([-10, 10])$