Examen scris
Structuri Algebrice în Informatică
25/01/2021

Nume: .... **Punctaj parţial 1................**

Prenume: .... **Punctaj parţial 2................**

<u>IMPORTANT!!</u>. Punctul din oficiu este acordat pentru aflarea lui a şi b pe care, ulterior, le veţi înlocui în toate enunţurile problemelor. Pe foile voastre de examen veţi scrie enunţurile problemelor cu a şi b înlocuite cu valorile anterior determinate.

$a = ...,$ $b = ...,$

unde

(1) a este egal cu maximul dintre numerele de litere ale cuvintelor care compun numele vostru de familie. (de exemplu, dacă numele de familie este Popescu-Simion atunci $a = 7$, maximul dintre 7 (nr. de litere al cuvântului Popescu) şi 6 (nr. de litere al cuvântului Simion); dacă numele de familie este Moisescu atunci $a = 8$)

(2) b este egal cu maximul dintre numerele de litere ale cuvintelor care compun prenumele vostru. (de exemplu, dacă prenumele este Andreea-Beatrice-Luminiţa atunci $b = 8$, maximul dintre 7 (nr. de litere al cuvântului Andreea) şi 8 (nr. de litere atât al cuvântului Beatrice cât şi al cuvântului Luminiţa).)

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	

Justificaţi toate răspunsurile!

1. Există permutări de ordin $a \cdot b - 1$ în grupul de permutări S_{a+b}?

2. Se consideră permutarea $\sigma = (1, \ldots, a)(a+1, \ldots, a+b)$, un produs de 2 cicli disjuncţi de lungime a, respectiv b, din S_{a+b}. Determinaţi toate permutările $\tau \in S_{a+b}$ astfel încât $\tau^3 = \sigma$.

3. Calculaţi $a^{a^{b^b}} \pmod{31}$.

4. Considerăm polinomul cu coeficienţi întregi $P(X) = X^3 - aX + b$. Determinaţi dacă polinomul $P(X)$ este ireductibil în $\mathbb{Q}[X]$.

5. Determinaţi numărul elementelor de ordin 8 din grupul produs direct $(\mathbb{Z}_{2^a}, +) \times (\mathbb{Z}_{2^b}, +)$.

6. Fie p cel mai mic număr prim din descompunerea în factori primi a lui a şi 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 $\mathbb{N}$ relaţia binară ρ dată astfel: $m \rho n$ dacă $\exp_p(n) = \exp_p(m)$ şi $\exp_q(n) = \exp_q(m)$. Să se arate că ρ este relaţie de echivalenţă, să se calculeze clasele de echivalenţă ale lui a şi b şi să se determine un sistem complet de reprezentanţi pentru această relaţie de echivalenţă.

7. Se consideră funcţia $f : \mathbb{R} \mapsto \mathbb{R}$ definită astfel:

$$f(x) = \begin{cases} ax + b(1+a), & \text{dacă} \quad x < -b, \\ ax^2 + 2a(a-1)x + a^3 - 2a^2 + a + b, & \text{dacă} \quad x \geq -b. \end{cases}$$

   Decideţi dacă funcţia f este injectivă, surjectivă, respectiv bijectivă. Calculaţi $f^{-1}([-b-1, b+1])$.

8. Demonstraţi că inelul factor $\mathbb{Q}[X]/(X^2 - a^2 - a)$ este izomorf cu inelul $(\mathbb{Q}[\sqrt{a^2+a}], +, \cdot)$, unde $\mathbb{Q}[\sqrt{a^2+a}] = \{\alpha + \beta\sqrt{a^2+a} | \alpha, \beta \in \mathbb{Q}\}$.

9. Determinaţi constantele $c, d \in \mathbb{Q}$ astfel încât polinoamele $X^b - aX + 1$ şi $cX + d$ să fie în aceeaşi clasă de echivalenţă în inelul $\mathbb{Q}[X]/(X^2 - a^2 - a)$.

Structuri Algebrice în Informatică

[redacted]

Grupa 143

$a = 11$

$b = 7$

1. $a \cdot b - 1$ în S_{a+b}

$a \cdot b = 11 \cdot 7 = 77$

$a+b = 18$

$a \cdot b - 1 = 77 - 1 = 76$

Dacă ar exista permutări de ordin 76 în S_{18} ar însemna ca $76 \mid 18!$ (fals!)

$\Rightarrow \nexists$ permutări de ordin 76 în S_{18}

2. $\sigma = (1 \ldots a)(a+1 \ldots a+b)$

$a = 11$

$a+b = 18$

$\sigma = (1 \ldots 11)(12 \ldots 18)$

$\tau^3 = \sigma$

$ord(\sigma) = [11, \cancel{7}] = 77$

$ord(\cancel{\tau}^3) = \dfrac{ord(\tau)}{(ord(\tau), 3)} = 77 \Rightarrow ord(\tau) \vdots 77$

$\Rightarrow ord(\tau) = 77$

$= 18 = 7 + 11$

$\sigma^3 = x^3 y^3$

x = 7-ciclu

y = 11-ciclu

$x^3 = (12\ 13\ 14\ 15\ 16\ 17\ 18)$

$\Rightarrow x = (12\ 15\ 18\ 14\ 17\ 13\ 16)$

$y^3 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$

$\Rightarrow y = (1\ 4\ 7\ 10\ 2\ 5\ 8\ 11\ 3\ 6\ 9)$

$\Rightarrow \sigma = (1\ 4\ 7\ 10\ 2\ 5\ 8\ 11\ 3\ 6\ 9)(12\ 15\ 18\ 14\ 17\ 13\ 16)$

3. $a^{a^{b^b}} \pmod{31}$

$\varphi(31) = 30$

$11^{11^{7^7}} = m$

$\hat{11}^{30} = \hat{1}$ (Fermat)

$7^7 = 823\ 543$

$11^{7^7} = 11^{823\ 543}$

$\hat{7}^7 = \hat{28}$

$\hat{11}^{7^7} = \hat{11}^{28} = \hat{10}$

$\hat{11}^{11^{7^7}} = \hat{17}$

$\hat{11}^{11^{7^7}} = (\hat{24})^{7^7} = \hat{3}^7 = \hat{17}$.

$\hat{11}^{11} = (\hat{11}^2)^5 \cdot 11 = \hat{22}^5 \cdot 11 = \hat{5} \cdot \hat{11} = 24$

$\hat{24}^7 = (\hat{24}^2)^3 \cdot \hat{24} = \hat{18}^3 \cdot \hat{24} = \hat{4} \cdot \hat{24} = \hat{3}$

$\hat{3}^7 = (\hat{3}^2)^3 \cdot \hat{3} = \hat{9}^3 \cdot \hat{3} = \hat{19} \cdot \hat{9} \cdot \hat{3} = \hat{16} \cdot \hat{3} = \hat{48} = 17$

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

$a = 11$

$b = 7$

$P(x) = x^3 - 11x + 7$

Presupunem că P e reductibil în $\mathbb{Q}[x]$.

Un polinom de gradul 3 este reductibil în $\mathbb{Q}$ dacă acesta se poate descompune ca produs de un polinom de gradul I și un polinom de gradul II (cu $\Delta < 0$) sau ca produs de 3 polinoame de gradul I.

Fie $\frac{p}{q}$ o rădăcină în $\mathbb{Q}$ a polinomului, $(p, q) = 1$

$\Rightarrow p \mid 7$ și $q \mid 1$

$\Rightarrow \frac{p}{q} \in \{7, -7\}$

$P(7) = 7^3 - 11 \cdot 7 + 7 = 343 - 77 + 7 = 343 - 70 = 273 \neq 0$

$P(-7) = (-7)^3 - 11 \cdot (-7) + 7 = -343 + 77 + 7 = -259 \neq 0$

$\Rightarrow P(7) \neq 0, P(-7) \neq 0 \Rightarrow$ Presupunerea făcută este falsă

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

5. $a = 11$

$b = 7$

$(\mathbb{Z}_{2^a}, +) \times (\mathbb{Z}_{2^b}, +)$

$2^a = 2^{11} = 2048$

$2^b = 2^7 = 128$

$\Rightarrow (\mathbb{Z}_{2048}, +) \times (\mathbb{Z}_{128}, +)$

Fie $(a,b) \in (\mathbb{Z}_{2048}, +) \times (\mathbb{Z}_{128}, +)$

$ord((a,b)) = 8$

$\Rightarrow [ord(a), ord(b)] = 8$

$\Rightarrow (ord(a), ord(b)) \in \{(1,8), (2,8), (4,8), (8,8), (8,4), (8,2), (8,1)\}$

$ord(a) = 1 \Rightarrow a = \hat{0}$

$ord(a) = 2 = \dfrac{2048}{(2048,a)} \Rightarrow (2048,a) = 1024 \Rightarrow a \in \{\widehat{1024}\}$

$ord(a) = 4 = \dfrac{2048}{(2048,a)} \Rightarrow (2048,a) = 512 \Rightarrow a \in \{\widehat{512}, \widehat{1536}\}$

$ord(a) = 8 = \dfrac{2048}{(2048,a)} \Rightarrow (2048,a) = 256 \Rightarrow a \in \{\widehat{256}, \widehat{768}, \widehat{1280}, \widehat{1792}\}$

$ord(b) = 1 \Rightarrow b = \hat{0}$

$ord(b) = 2 = \dfrac{128}{(128,b)} \Rightarrow (128,b) = 64 \Rightarrow b \in \{\widehat{64}\}$

$ord(b) = 4 = \dfrac{128}{(128,b)} \Rightarrow (128,b) = 32 \Rightarrow b \in \{\widehat{32}, \widehat{96}\}$

$ord(b) = 8 = \dfrac{128}{(128,b)} \Rightarrow (128,b) = 16 \Rightarrow b \in \{\widehat{16}, \widehat{48}, \widehat{80}, \widehat{112}\}$

$\Rightarrow$ nr de elemente de ordin 8 din $(\mathbb{Z}_{2048}, +) \times (\mathbb{Z}_{128}, +)$ este

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

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

$= 16 + 16 + 16$

$= 48$ elemente

6. $a = 11 \Rightarrow p = 11$

$b = 7$

$a + b = 18 \Rightarrow q = 17$

$m \, \rho \, n \Leftrightarrow exp_p(n) = exp_p(m)$

$exp_q(n) = exp_q(m)$

reflexivitate

$x \, \rho \, x \Leftrightarrow exp_{11}(x) = exp_{11}(x)$

$exp_{17}(x) = exp_{17}(x)$

simetrie

$x \, \rho \, y \Leftrightarrow exp_{11}(x) = exp_{11}(y) \Rightarrow exp_{11}(y) = exp_{11}(x)$

$exp_{17}(x) = exp_{17}(y) \Rightarrow exp_{17}(y) = exp_{17}(x)$

$\Rightarrow y \, \rho \, x$

tranzitivitate

$$\left.\begin{aligned} x \, \rho \, y &\Rightarrow exp_{11}(x) = exp_{11}(y) \\ &\quad\; exp_{17}(x) = exp_{17}(y) \\ y \, \rho \, z &\Rightarrow exp_{11}(y) = exp_{11}(z) \\ &\quad\; exp_{17}(y) = exp_{17}(z) \end{aligned}\right\} \Rightarrow \left.\begin{aligned} exp_{11}(x) &= exp_{11}(z) \\ exp_{17}(x) &= exp_{17}(z) \end{aligned}\right\} \Rightarrow$$

$\Rightarrow x \, \rho \, z$

$\Rightarrow \rho$ e rel de echiv.

$[11] = \{$ numerele care sunt de forma $11k$, $k \notin M_{11}$, $k \notin M_{17}$ $\}$

$[7] = \{$ numerele care nu sunt divizibile nici cu 17, nici cu 11 $\}$

~~$[11] = \{11k$~~

$[11] = \{a \in \mathbb{N} \mid (17, a) = 1, a = 11k, (11, k) = 1\}$

$[7] = \{b \in \mathbb{N} \mid (17, b) = 1, (11, b) = 1\}$

$SCR = \mathbb{N}$

7

$$f(x) = \begin{cases} ax + b(1+a) & , x \le -b \\ ax^2 + 2a(a-1)x + a^3 - 2a^2 + a + b & , x \geq -b \end{cases}$$

$a = 11$
$b = 7$

$$f(x) = \begin{cases} 11x + 84, & x \le -7 \\ 11x^2 + 220x + 1331 - 242 + 11 + 7, & x \geq -7 \end{cases}$$

$$f(x) = \begin{cases} 11x + 84, & x \le -7 \\ 11x^2 + 220x + 1107, & x \geq -7 \end{cases}$$

- $x < -7$

Fie $g: (-\infty, -7] \to \mathbb{R}$

$g(x) = 11x + 84$

$\lim_{x \to -\infty} g(x) = -\infty$

$g(-7) = -77 + 84 = 7$

g este o funcție de gradul I și $11 > 0 \Rightarrow g$ e strict crescătoare, deci injectivă

$\Rightarrow \operatorname{Im} g = (-\infty, 7]$

- $x \geq -7$

Fie $h: [-7, \infty) \to \mathbb{R}$

$h(x) = 11x^2 + 220x + 1107$

$h(-7) = 106$

$\lim_{x \to \infty} h(x) = +\infty$

Obs: că h este continuă și derivabilă pe $[-7,\infty)$

$h'(x) = 22x + 220$

$h'(x) = 0$

$22x = -220 \Rightarrow x = -10 \notin [-7,\infty)$

$h'(0) = 220 > 0$

x	-7				∞
$h'(x)$	+ + +	+	+	+ + +	
$h(x)$	106	$\nearrow$	$\nearrow$	$\nearrow$	∞

$\Rightarrow \operatorname{Im} h = [106,\infty)$

h e injectivă pe $[-7,\infty)$

$f(-8) =$

$\Rightarrow \operatorname{Im} f = (-\infty, 7] \cup [106,\infty) \neq \mathbb{R} \Rightarrow$ f nu e surjectivă

$\Rightarrow$ f nu e bijectivă

f e inj. pe $(-\infty,-7]$ și pe $[-7,\infty) \Rightarrow$ f e injectivă

$\cancel{11x+84 = 11x^2+220x+1107}$

$\cancel{0 = 11x^2+209x+1023}$

$\cancel{\Delta = -1331 < 0}$

$f^{-1}([-8,8]) = f^{-1}([-8,-7) \cup [7,8])$

$= [-4,7] \cup [106, 3571]$

8.

$$\mathbb{Q}[x]/(x^2-a^2-a) = \mathbb{Q}[x]/(x^2-121-11) = \mathbb{Q}[x]/(x^2-132)$$

$$\mathbb{Q}[\sqrt{a^2+a}] = \mathbb{Q}[\sqrt{132}]$$

$$\mathbb{Q}[\sqrt{132}] = \{ \alpha + \beta\sqrt{132} \mid \alpha, \beta \in \mathbb{Q} \}$$

Fie $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{132}]$

$$\varphi(P(x)) = P(\sqrt{132})$$

1) φ morfism

Fie $(\forall) f, g \in \mathbb{Q}[x]$

$$\left.\begin{array}{l} \varphi(f(x)) \cdot \varphi(g(x)) = f(\sqrt{132}) \cdot g(\sqrt{132}) \\ \varphi((f\cdot g)(x)) = \varphi(f(x)\cdot g(x)) = (f\cdot g)(\sqrt{132}) = f(\sqrt{132})\cdot g(\sqrt{132}) \end{array}\right\}$$

$\Rightarrow$ φ e morfism de inele

2) Surjectivitate

$$\varphi(a+bx) = a + b\sqrt{132} \quad (\forall) a, b \in \mathbb{Q}$$

$\Rightarrow \operatorname{Im}\varphi = \mathbb{Q}[\sqrt{132}]$

3) Demonstrăm că $\ker\varphi = (x^2-132)$ cu dublă incluziune

„$\supseteq$" Fie $f(x) \in (x^2-132) \overset{def}{\Rightarrow} f(x) = (x^2-132)\, g(x)$ cu $g(x) \in \mathbb{Q}[x]$

$$\varphi(f(x)) = \varphi((x^2-132)g(x)) = ((\sqrt{132})^2-132)\, g(\sqrt{132})$$

$$= 0 \cdot g(\sqrt{132})$$

$$= 0$$

$\Rightarrow f(x) \in \ker\varphi \Rightarrow (x^2-132) \subseteq \ker\varphi$

„$\subseteq$" Fie $P(x) \in \ker f \Rightarrow f(P(x)) = 0 \Rightarrow P(\sqrt{132}) = 0$

Aplic teorema împărțirii cu rest:

$$P(x) = (x^2 - 132)\, g(x) + r(x) \quad , g, r \in \mathbb{Q}[x]$$
$$r(x) = ax + b, \quad a, b \in \mathbb{Q}$$

$$P(x) = (x^2 - 132)\, g(x) + ax + b$$

$$P(\sqrt{132}) = 0 + a\sqrt{132} + b = 0$$

Dacă $a \neq 0 \Rightarrow a\sqrt{132} + b = 0 \Rightarrow a\sqrt{132} = -b$

$$\left.\begin{array}{l} \Rightarrow \sqrt{132} = -\frac{b}{a} \\ \text{dar } -\frac{b}{a} \in \mathbb{Q} \text{ și } \sqrt{132} \in \mathbb{R}\setminus\mathbb{Q} \end{array}\right\} \text{ abs}$$

$\Rightarrow a = 0 \Rightarrow b = 0 \Rightarrow r(x) = 0, \forall x$

$\Rightarrow P(x) = (x^2 - 132)\, g(x) \Rightarrow P(x) \in (x^2 - 132)\mathbb{Q}[x] = (x^2 - 132)$

$\Rightarrow \ker f \subseteq (x^2 - 132)$

$\Rightarrow \ker f = (x^2 - 132)$

Aplic TFI:

$$\mathbb{Q}[x]/_{\ker f} \simeq \operatorname{Im} f \overset{(1),(2),(3)}{\Rightarrow} \mathbb{Q}[x]/_{(x^2 - 132)} \simeq \mathbb{Q}[\sqrt{132}]$$

9. $x^b - aX + 1 = x^7 - 11x + 1$

$cx + d$, $c, d = ?$

$$\mathbb{Q}[x]/(x^2 - a^2 - a) = \mathbb{Q}[x]/(x^2 - 132) = \{ \widehat{ax+b} \mid a, b \in \mathbb{Q} \}$$

$x^7 - 11x + 1$ și $cx + d$ se află în aceeași clasă de echivalență dacă au același rest la împărțirea cu $x^2 - 132$.

grad $(cx + d) \leq 1 \Rightarrow$ $cx+d$ este chiar restul la împărțirea cu $x^2 - 132$

Aflăm restul lui $x^7 - 11x + 1$ la $x^2 - 132$.

$$\begin{array}{l|l} x^7 - 11x + 1 & x^2 - 132 \\ \hline -x^7 + 132x^5 & x^5 + 132x^3 + 132^2 x \\ \hline / \quad 132x^5 - 11x + 1 & \\ -132x^5 + 132^2 \cdot x^3 & \\ \hline 132^2 x^3 - 11x + 1 & \\ -132^2 x^3 + 132^3 x & \\ \hline / \quad 132^3 x - 11x + 1 & \end{array}$$

$\Rightarrow x^7 - 11x + 1 = (x^5 + 132x^3 + 132^2 x)(x^2 - 132) + (132^3 x - 11x + 1)$

$132^3 x - 11x + 1 = x(132^3 - 11) + 1$

$\Rightarrow \quad c = 132^3 - 11 = 2299957$

$d = 1$