Florea Mădălin-Alexandru 06.06.2022
Grupa 143

Examen scris
- Structuri algebrice în informatică -

(1) $a = 6$
$b = 9$
$m = \min(6,9) = 6$
$M = \max(6,9) = 9$

(4) $M^{a^{b^m}} \pmod{31} = 9^{6^{9^6}} \pmod{31}$

31 este număr prim $\overset{T.Fermat}{\Rightarrow}$ $9^{30} \equiv 1 \pmod{31}$

Deci, pentru a calcula $9^{6^{9^6}} \pmod{31}$ este suficient să calculăm $6^{9^6} \pmod{30}$

$(6, 30) = 6 \neq 1$

$6^1 \pmod{30} = 6 \pmod{30}$
$6^2 \pmod{30} = 6 \pmod{30}$
$6^3 \pmod{30} = 6 \pmod{30}$

Deci $6^u \pmod{30} = 6 \pmod{30}$ $(\forall)\, u \in \mathbb{N}$

$\Rightarrow 6^{9^6} \pmod{30} = 6 \pmod{30}$

$\Rightarrow 9^{6^{9^6}} \pmod{31} = 9^6 \pmod{31} = 9^{3\cdot 2} \pmod{31} =$

$= (9^3)^2 \pmod{31} = 729^2 \pmod{31} =$

Florea Mădălin-Alexandru
Grupa 143

$= 16^2 \pmod{31} = 256 \pmod{31} = 8 \pmod{31}$

$$\begin{array}{l} 729 : 31 = 23 \\ \underline{62} \\ 109 \\ \underline{\ 93} \\ \ 16 \end{array}$$

⑥ Numărul elementelor de ordin 12 din
$(\mathbb{Z}_{2^6}, +) \times (\mathbb{Z}_{6^9}, +)$

$\{(\hat{k}, \bar{l}) \in \mathbb{Z}_{2^6} \times \mathbb{Z}_{6^9} \mid ord(\hat{k}, \bar{l}) = 12\}$

$ord((\hat{k}, \bar{l})) = [ord(\hat{k}), ord(\bar{l})] = 12$

$(ord(\hat{k}), ord(\bar{l})) = \{(1,12), (2,6), (3,4), (4,3), (6,2), (12,1)\}$

Din Lagrange $ord(\hat{k}) \mid 2^6$
$ord(\bar{l}) \mid 6^9$

$\Rightarrow (ord(\hat{k}), ord(\bar{l})) = \{(1,12), (2,6), (4,3)\}$

Fldea Mădălin-Alexandru
Grupa 143

Caz 1

$$ord(\hat{k}) = 1 \Rightarrow k = 0 \text{ în } \mathbb{Z}_{2^6}$$

$$ord(\bar{l}) = 12 \Rightarrow \frac{6^9}{(6^9, l)} = 12 \Rightarrow (6^9, l) = \frac{6^9}{12}$$

$$\Rightarrow (6^9, l) = 6^7 \cdot 3$$

$$l = \{6^7 \cdot 3\}$$

1 element de ordin 12

Caz 2

$$ord(\hat{k}) = 2 \Rightarrow \frac{2^6}{(2^6, k)} = 2 \Rightarrow (2^6, k) = 2^5 \Rightarrow$$

$$\Rightarrow k = \{2^5\}$$

$$ord(\bar{l}) = 6 \Rightarrow \frac{6^9}{(6^9, l)} = 6 \Rightarrow (6^9, l) = 6^8$$

$$\Rightarrow l = \{6^8, 6^8 \cdot 5\}$$

2 elemente de ordin 12

Caz 3

$$ord(\hat{k}) = 4 \Rightarrow \frac{2^5}{(2^6, k)} = 4 \Rightarrow (2^6, k) = 2^4 \Rightarrow k = \{2^4\}$$

Floroa Mădălin-Alexandru
Grupa 143

$ord(\bar{l}) = 3 \Rightarrow \frac{6^9}{(6^9, l)} = 3 \Rightarrow (6^9, l) = 6^8 \cdot 2$

$\Rightarrow l = \{6^8 \cdot 2\}$

1 element de ordin 12

Avem 4 elemente de ordin 12 în grupul produs direct $(\mathbb{Z}_{2^6}, +) \times (\mathbb{Z}_{6^9}, +)$.

⑧ $f: \mathbb{R} \to \mathbb{R}$.

$$f(x) = \begin{cases} 6x + 9(1-9) & \text{dacă } x < 6 \\ 4 \cdot 6x^2 - 4 \cdot 6(6+9)x + 6^2(6+2\cdot 9) + 9(6\cdot 9+1) & \text{dacă } x \in [6,9] \\ 9x - 6\cdot 9 + 6 & \text{dacă } x > 9 \end{cases}$$

$$f(x) = \begin{cases} 6x - 72 & \text{dacă } x < 6 \\ 24x^2 - 360x + 1359 & \text{dacă } x \in [6,9] \\ 9x - 48, & \text{dacă } x > 9 \end{cases}$$

$6x - 72$ dacă $x < 6$

$f(6) = 36 - 72 = -36$

Este funcție de gradul 1, deci imaginea este

$\operatorname{im} f = (-\infty, -36)$

Florea Mădălin-Alexandru
Grupa 143

$9x-48$ dacă $x>9$

$f(9)=9\cdot 9-48=33$

Este funcție de gradul I deci imaginea este

$Im f=(33,+\infty)$

$24x^2-360x+1359$, $x\in[6,9]$

$V_f(x_v,y_v)=V_f\left(\frac{15}{2},9\right)$

$x_v=\frac{-b}{2a}=-\frac{-360}{2\cdot 24}=\frac{15}{2}$

$y_v=f(x_v)=f\left(\frac{15}{2}\right)=24\cdot\left(\frac{15}{2}\right)^2-\overset{180}{\cancel{360}}\cdot\frac{15}{\cancel{2}}+1359=$

$=6\cdot 15^2-180\cdot 15+1359=$

$=6\cdot 225-2700+1359=1350-2700+1359=9$

$Im f=[y_v,+\infty)\Rightarrow Im f=[9,+\infty)$ (funcție de gradul 2 cu $a=24>0$)

$f(6)=24\cdot 6^2-360\cdot 6+1359=$

$=24\cdot 36-2160+1359$

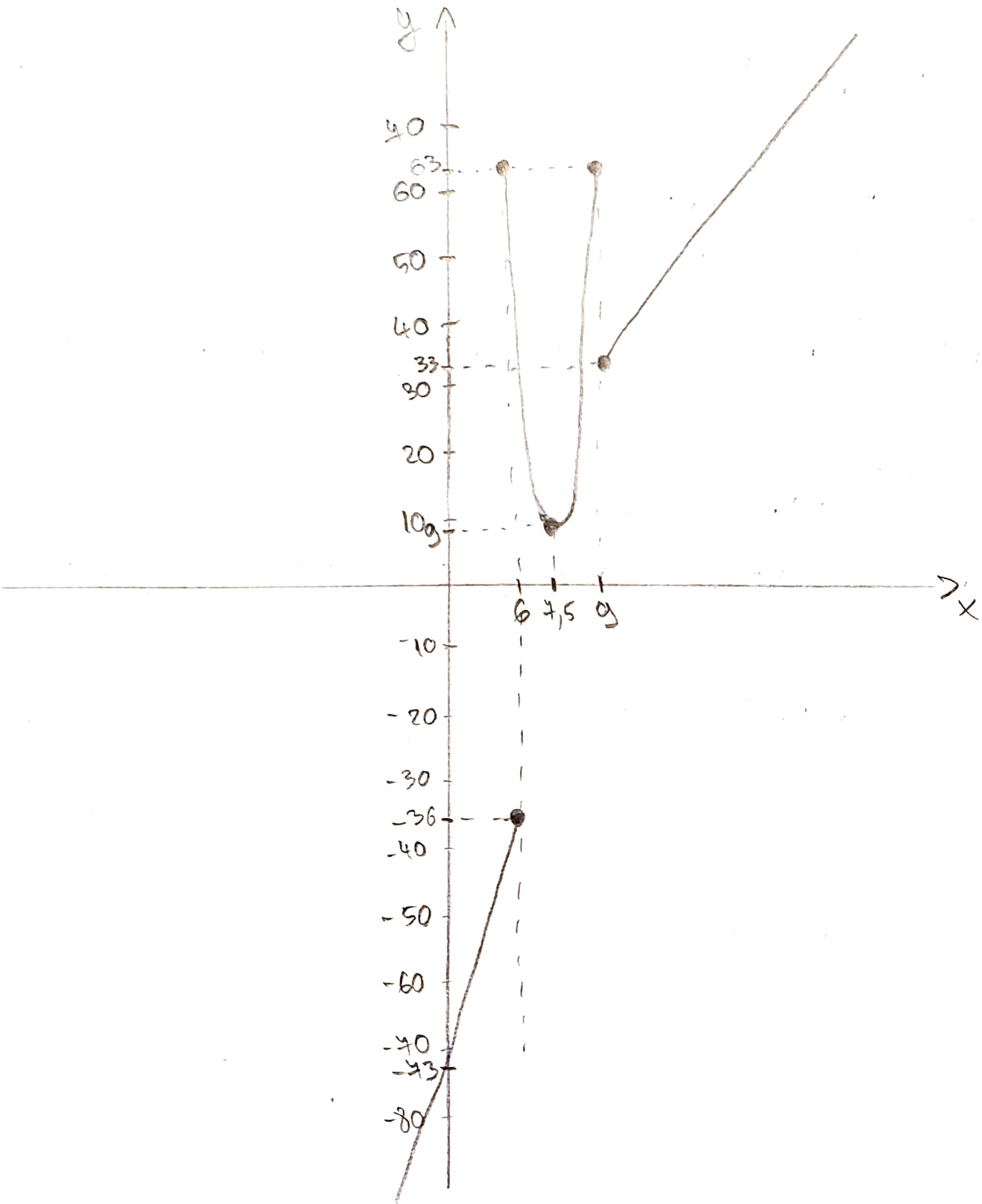
$=864-2160+1359$

$=63$

Floarea Mădălin-Alexandru
Grupa 143

$$f(9) = 24 \cdot 9^2 - 360 \cdot 9 + 1359 =$$
$$= 24 \cdot 81 - 3240 + 1359 =$$
$$= 1944 - 3240 + 1359 =$$
$$= 63$$

$$\Rightarrow \operatorname{Im} f = [9, 63]$$



Florea Mădălin-Alexandru
Grupa 143

Funcția f nu este injectivă deoarece dacă ducem o paralelă la ax pt $y>9$, aceasta intersectează graficul în 2 puncte. (Pentru a fi injectivă, trebuia să intersecteze graficul funcției în cel mult un punct).

Funcția f nu este surjectivă deoarece dacă ducem o paralelă la ax pt $y>-36$ și $y<9$ aceasta nu intersectează graficul funcției în niciun punct. (Pentru a fi surjectivă, trebuia să intersecteze graficul în cel puțin un punct).

f nu e injectivă, f nu e surjectivă

$\Rightarrow$ f nu este bijectivă

$$f^{-1}([6-1,6+6]) = f^{-1}([5,12]) = f^{-1}([5,9)) \cup f^{-1}([9,12])$$

$$\operatorname{Im} f = (-\infty,-36) \cup (9,+\infty) \Rightarrow f^{-1}(5,9) = \emptyset$$

$$f^{-1}([9,12])$$

$f(x)=9 \Rightarrow x=\frac{15}{2}$ (calculat anterior când am aflat coordonatele vârfului)

$f(x)=12$

$$24x^2-360x+1359=12$$

$$24x^2-360x+1347=0 \quad |:3$$

$$8x^2-120x+449=0$$

Florea Mădălin-Alexandru
Grupa 143

$$x_{1,2} = \frac{-(-120) \pm \sqrt{(-120)^2 - 4 \cdot 8 \cdot 449}}{2 \cdot 8} =$$

$$= \frac{120 \pm \sqrt{14400 - 14368}}{16} =$$

$$= \frac{120 \pm \sqrt{32}}{16} = \frac{120 \pm 4\sqrt{2}}{16} = \frac{30 \pm \sqrt{2}}{4}$$

$$x_1 = \frac{30 + \sqrt{2}}{4} \simeq 7,85$$

$$x_2 = \frac{30 - \sqrt{2}}{4} \simeq 7,14$$

$$f^{-1}([9,12]) = \left[\frac{30-\sqrt{2}}{4}, \frac{30+\sqrt{2}}{4}\right]$$

Deci $f^{-1}([5,12] = \left[\frac{30-\sqrt{2}}{4}, \frac{30+\sqrt{2}}{4}\right)$

5

$$n \equiv 6 \pmod{13}$$
$$n \equiv 6 \pmod{14}$$
$$n \equiv 6 \pmod{15}$$

Notăm $a_1 = 6, a_2 = 6, a_3 = 9$

$$m_1 = 13, m_2 = 14, m_3 = 15$$

Observăm că $(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$

Flodea Mădălin-Alexandru
Grupa 143

$$N = 13 \cdot 14 \cdot 15 = 2730$$

$$N_1 = \frac{N}{n_1} = \frac{\cancel{13} \cdot 14 \cdot 15}{\cancel{13}} = 14 \cdot 15 = 210$$

$$N_2 = \frac{N}{n_2} = \frac{13 \cdot \cancel{14} \cdot 15}{\cancel{14}} = 13 \cdot 15 = 195$$

$$N_3 = \frac{N}{n_3} = \frac{13 \cdot 14 \cdot \cancel{15}}{\cancel{15}} = 13 \cdot 14 = 182$$

$N_1 x_1 = 1 \pmod{n_1} \rightarrow 210 x_1 \equiv 1 \pmod{13} \rightarrow$

$N_2 x_2 \equiv 1 \pmod{n_2} \rightarrow 195 x_2 \equiv 1 \pmod{14} \rightarrow$

$N_3 x_3 \equiv 1 \pmod{n_3} \rightarrow 182 x_3 \equiv 1 \pmod{15} \rightarrow$

$\rightarrow 2x_1 \equiv 1 \pmod{13} \rightarrow x_1 \equiv 7 \pmod{13}$

$\rightarrow 13 x_2 \equiv 1 \pmod{14} \rightarrow x_2 \equiv 13 \pmod{14}$

$\rightarrow 2x_3 \equiv 1 \pmod{15} \rightarrow x_3 \equiv 8 \pmod{15}$

Soluția unică modulo $N = 2730$ este $x \pmod N$

unde $x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$= 6 \cdot 210 \cdot 7 + 6 \cdot 195 \cdot 13 + 9 \cdot 182 \cdot 8 =$

$= 8820 + 15210 + 13104 = 37134$

$37134 \pmod{2730} = 1644 \pmod{2730}$

$37134 = 2730 \cdot 13 + 1644$

Florea Mădălin-Alexandru
Grupa 143

=> Unica soluție a sistemului mod 2730 este 1644.

(2) Permutări de ordin 6 în S_9?

$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k$ produs de k cicli disjuncți, lungimea lui σ_i este l_i

$ord(\sigma) = [l_1, \ldots, l_k]$

Avem 3 cazuri:

caz 1: un ciclu de lungime 6 și unul de lungime 3

caz 2: trei cicli de lungime 3

caz 3: patru cicli de lungime 2 și unul de lungime 1

$$\frac{9!}{1! 6^1 \cdot 1! \cdot 3^1} + \frac{9!}{3! \, 3^3} + \frac{9!}{4! \, 2^4 \cdot 1! \cdot 1} =$$

$$= \frac{9!}{6 \cdot 3} + \frac{9!}{3! \cdot 27} + \frac{9!}{4! \cdot 16} =$$

$$\overset{9)}{=} \frac{9!}{18} + \frac{9!}{162} + \frac{\cancel{4!} \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9}{\cancel{4!} \cdot 2^4} =$$

$$= \frac{9 \cdot 9! + 9!}{162} + \frac{9 \cdot \cancel{2}^{3} \cdot 7 \cdot 6 \cdot 5}{2\cancel{4}}$$

Florea Mădălin-Alexandru
Glupa 143

$$= \frac{5 \cdot 362880}{81} + \frac{5 \cdot \overset{3}{\cancel{6}} \cdot 7 \cdot 9}{\cancel{2}} =$$

$$= 5 \cdot 4480 + 5 \cdot 3 \cdot 7 \cdot 9 = 22400 + 945 = 23345$$

Sunt 23345 permutări de ordin 6 în S_9

(3) $\sigma = (1, \dots, 6)(7, \dots, 18)(19, \dots, 27)$ produs de 3 cicli disjuncți în S_{27}

$\tau^2 = \sigma$

Presupunem că $(\exists)\ \tau \in S_{27}$ a.î. $\tau^2 = \sigma$

Fie $\tau = c_{i_1} \cdot c_{i_2} \cdot \ldots \cdot c_{i_k}$ descompunerea lui τ în produs de cicli disjuncți

$$i_1 + i_2 + \ldots + i_k = 27$$

$$1 \leq k < 27 \quad (k = 27 \Rightarrow \tau = e \ \text{\#})$$

$$\tau^2 = c_{i_1}^2 \cdot c_{i_2}^2 \cdot \ldots \cdot c_{i_k}^2$$

$\text{ord}(x) = n$

$\text{ord}(\sigma) = [6, 12, 9] = 2^2 \cdot 3^2 = 36$

$\text{ord}(\tau^2) = \frac{n}{(n, 2)} = 36 \Rightarrow 36 \mid n$

Florea Mădălin-Alexandru
Grupa 143

$2 \mid 6 \Rightarrow c_{ij}^2$ = produs de 2 cicli de lungime 3

$2 \mid 12 \Rightarrow c_{ij}^2$ = produs de 2 cicli de lungime 6

$2 \nmid 9 \Rightarrow c_{ij}^2$ = produs de 1 ciclu de lungime 9