Seminar 11 - 22.12.2021

Aplicație la T. Euler și Fermat:

Ex. 1: Să se calculeze ordinele elem.:

a. $\hat{6}$, $\hat{8}$, $\hat{11}$ în $(\mathbb{Z}_{31}, \cdot)$

b. $\hat{35}$, $\hat{5}$, $\hat{11}$ în $(\mathbb{Z}_{48}, \cdot)$

1a. 31 prim $\Rightarrow a^{30} \equiv 1 \bmod 31$, $\forall a \in \mathbb{Z}$, $31 \nmid a$

$\hat{a}^{30} = \hat{1}$ în $\mathbb{Z}_{31}$, $\forall \hat{a} \neq \hat{0}$

$\Rightarrow ord(\hat{a}) \mid 30 \Rightarrow ord(\hat{a}) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

$\hat{6}^2 = \hat{36} = \hat{5}$

$\hat{6}^3 = \hat{30} = -\hat{1} \Rightarrow \hat{6}^6 = \hat{1} \Rightarrow ord(\hat{6}) = 6$

$\hat{6}^5 = -\hat{5} = \hat{26}$

$\hat{6}^6 = \hat{1}$

b. 48 nu este prim, dacă $(a, 48) = 1 \Rightarrow a^{\varphi(48)} \equiv 1 \bmod 48$.

$\varphi(48) = 48\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 48 \cdot \frac{1}{2} \cdot \frac{2}{3} = 16$

$\hat{a}^{16} = \hat{1}$ în $\mathbb{Z}_{48}$ dacă $(a, 48) = 1$.

$ord(\hat{a}) \mid 16 \Rightarrow ord(\hat{a}) \in \{1, 2, 4, 8, 16\}$

$\hat{5}^2 = \widehat{25}$

$\hat{5}^4 = \widehat{625} = \hat{1} \Rightarrow ord(\hat{5}) = 4.$

Permutările

Ex. 2: Se consideră $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 1 & 4 & 2 & 9 & 8 & 6 \end{pmatrix} \in S_9$

a. Desc. σ în prod. de cicli disjuncți și în prod. de transp.

b. Aflați $sgn(\sigma)$, $ord(\sigma)$ și calculați σ^{2022}

a. $\sigma = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)\ (8)$

$\sigma = (1\ 3)(3\ 7)(7\ 9)(9\ 6)(6\ 2)(2\ 5)(5\ 4).$

$\tau = (1\ 2\ 5\ 7)\ (4\ 10\ 6)$

$\tau = (1\ 2)(2\ 5)(5\ 7)\ (4\ 10)(10\ 6)$

b. I. $sgn(\sigma) = (-1)^{m(\sigma)}$

$m(\sigma)$ = nr. inversiunilor

II. $sgn(\sigma) = (-1)^{\text{nr. transp. din desc. lui } \sigma}$ $= (-1)^7 = -1$

$sgn(\tau_1 \tau_2) = sgn(\tau_1)\, sgn(\tau_2)$

III. $\sigma = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)$

$\rho = c_1 \circ c_2 \cdot \ldots \cdot c_k$, c_i cicli disjuncți

$sgn(\rho) = sgn(c_1) \cdot sgn(c_2) \cdot \ldots \cdot sgn(c_k)$

!! Un ciclu de lungime n se descompune în $n-1$ transp.

c ciclu de lungime
- pară $\Rightarrow sgn(c) = -1$
- impară $\Rightarrow sgn(c) = 1$.

σ 8-ciclu $\Rightarrow sgn(\sigma) = -1$

$\tau = (1\ 2\ 5\ 7)(4\ 10\ 6)$

$sgn(\tau) = (-1) \cdot 1 = -1$.

$\mathrm{ord}(\sigma) = 8$

$g = c_1 \cdot \ldots c_k$, $l_i = \mathrm{ord}(c_i)$ (lungimea ciclului c_i)

$\mathrm{ord}(g) = [l_1, l_2, \ldots, l_k]$.

$\mathrm{ord}(\tau) = [4, 3] = 12$.

$\sigma^{2022} = ?$ $\quad \mathrm{ord}(\sigma) = 8 \Rightarrow \sigma^8 = e$

$\sigma^{2022} = \sigma^{8c+k} = \sigma^6$

$\sigma = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)$

$\sigma^2 = (1\ 7\ 6\ 5)(3\ 9\ 2\ 4) = (1\ 7\ 6\ 5)(2\ 4\ 3\ 9)$

$\sigma^6 = (\sigma^2)^{-1} = (1\ 5\ 6\ 7)(2\ 9\ 3\ 4)$

$c = (a_1\ a_2 \ldots a_m)$, $c^{-1} = (a_1\ a_m\ a_{m-1}, \ldots a_2)$

$\tau^{2022} = ?$, $\tau = (1\ 2\ 5\ 7)(4\ 10\ 6)$

$\mathrm{ord}(\tau) = 12$

$\tau^{2022} = \tau^{12c+r} = \tau^{6}$

$\tau^{6} = \left((1\ 2\ 5\ 7)(4\ 10\ 6)\right)^{6} \overset{!}{=} (1\ 2\ 5\ 7)^{6}(4\ 10\ 6)^{6}$

2022 2022

$= (1\ 2\ 5\ 7)^{2} \circ e$

$= (1\ 5)(2\ 7)$

Ex. 3: Fie $\sigma = (a_1\ a_2 \dots a_m)$ un m-ciclu. Ar. că $\forall i = \overline{1,m}$, $\sigma^{i}(a_k) = a_{k+i}$, unde $k+i$ este înlocuit de restul mod m dacă $k+i > m$.

Dem: Se face prin ind. după i

$\sigma^{i+1}(a_k) = \sigma(\sigma^{i}(a_k)) = \sigma(a_{k+i}) = a_{k+i+1}$.

Exemplu: $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$.

$\sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$

$\sigma^8 = (1\ 9\ 5)(2\ 10\ 6)(3\ 11\ 7)(4\ 12\ 8)$

σ^8 = produs de 4 3-cicli

Ex. 4: Fie σ un ciclu de lungime n. Arătați că:

a. σ^i este n-ciclu $\Leftrightarrow (i, n) = 1$.

b. Dacă $d \mid n$, atunci σ^d = produs de d cicli de lung. $\frac{n}{d}$.

Rez: $\operatorname{ord}(\sigma) = n$

$\operatorname{ord}(\sigma^i) = \frac{n}{(n, i)}$

"$\Leftarrow$" $\operatorname{ord}(\sigma^i) = n \Rightarrow \sigma^i$ n-ciclu

"$\Rightarrow$" σ^i n-ciclu $\Rightarrow \operatorname{ord}(\sigma^i) = n \Rightarrow (n, i) = 1$.

$\sigma = (a_1 \; a_2 \; \dots \; a_n) \;, \quad n = d \cdot m$

$\sigma^d = (a_1 \; a_{1+d} \; a_{1+2d} \; \dots \; a_{1+(m-1)d})(a_2 \; a_{2+d} \; \dots \; a_{2+(m-1)d})$

$\vdots$

$a_{1+md} \;, \; 1+md = 1+n \equiv 1 \bmod n)$

$(a_d \; a_{2d} \; \dots \; a_{md})$

Obs.: Ce se întâmplă când $(i, n) = d \neq 1 \;, \; i \nmid n$?

$i = d \cdot j \;, \; n = d \cdot m \;, \; (j, m) = 1.$

$\sigma^i = (\sigma^d)^j = (c_1 \; c_2 \; \dots \; c_d)^j = c_1^j c_2^j \dots c_d^j$

c_k cicli de lungime $\frac{n}{d} = m$, disjuncți

c_k^j ciclu de lungime m $((m, j) = 1)$

$\sigma = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)$

$\tau = (1\ 2\ 5\ 7)(4\ 10\ 6)$

Rez. ecuația $\rho^2 = \sigma$ / $\rho^2 = \tau$.

$sgn(\sigma) = -1 = sgn(\tau)$

$sgn(\rho^2) = (sgn(\rho))^2 = 1$.

$\rho^3 = \sigma$ = ciclu de lungime 8

$\rho = c_1 \dots c_k$ desc. în cicli disj., $ord(c_i) = l_i$

$\rho^3 = c_1^3 \dots c_k^3 = \sigma$

$3 | l_i \to c_i^3$ produs de 3 cicli de lung. $\frac{l_i}{3}$

$\boxed{3 \nmid l_i \to c_i^3 \text{ ciclu de lung. } l_i}$

$\rho = c$, c 8-ciclu, $\rho^3 = \sigma$

$\sigma^3 = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)$

σ 8 ciclu $\Rightarrow$ ord$(\sigma) = 8$ $\quad (\sigma^8 = e)$

$(\sigma^3)^3 = \sigma^9 = \sigma = (1\ 9\ 5\ 3\ 6\ 4\ 7\ 2)$

$(i, m) = 1 \Rightarrow \hat{i} \in U(\mathbb{Z}/m)$

$(\sigma^i)^j = \sigma$, $\hat{i} \cdot \hat{j} = \hat{1}$ in $\mathbb{Z}_m$

$\sigma^3 = (1\ 3\ 7\ 9\ 6\ 2\ 5\ 4)$

$\sigma = (\underline{1}\ \underline{9}\ \underline{5}\ \underline{3}\ \underline{6}\ \underline{4}\ \underline{7}\ \underline{2})$

$\sigma^3 = \tau = (1\ 2\ 5\ 7)(4\ 10\ 6)$ $\quad \sigma = c_1 \cdot c_2$

ciclu de l. 4

$(1\ 2\ 5\ 7) = c^3$, c 4-ciclu

c_2^3 ciclu de l. 3 - nu se poate

$c_2^3 = (4 \quad 6 \quad 10) \cdot \sigma_1.$

$\Rightarrow 3 \mid l_2 \qquad l_2 = ord(c_2)$

c_2^3 = prod. de 3 cicli de lungime $\frac{l_2}{3}$

Obs: Singurul mod în care putem obține un 3-ciclu dintr-un c^3 este dacă c este 9-ciclu.

Rez. în S_6 ecuația $\tau^2 = (1\ 3\ 6)(2\ 4\ 5) = \sigma$

$sgn(\sigma) = 1$

$\tau = c_1 \dots c_k$

$\tau^2 = c_1^2 \dots c_k^2$

$2 \mid l_i \Rightarrow c_i^2$ produs de 2 cicli de lung. $\frac{l_i}{2}$

$2 \nmid l_i \Rightarrow c_i^2$ ciclu de lung l_i

I. $\tau = c_1 \cdot c_2$, c_1, c_2 sunt cicli de l. 3.

$c_1^2 = (1\ 3\ 6) \Rightarrow c_1 = (1\ 6\ 3)$ sol. unică

$c_2^2 = (2\ 4\ 5) \Rightarrow c_2 = (2\ 5\ 4)$

II. τ - 6-ciclu

$\tau^2 = (1\ 3\ 6)(2\ 4\ 5) \Rightarrow \tau = (1\ 2\ 3\ 4\ 6\ 5)$

$(4\ 5\ 2) \Rightarrow \tau = (1\ 4\ 3\ 5\ 6\ 2)$

$(5\ 2\ 4) \Rightarrow \tau = (1\ 5\ 3\ 2\ 6\ 4)$