Seminar 12 - 20.12.2021.

Ex. 1: Calculati ordinele elem:

a. $\hat{5}, \hat{13}, \hat{20}$ în $(\mathbb{Z}_{31}^*, \cdot)$

b. $\hat{7}, \hat{11}, \hat{15}$ în $(\mathbb{Z}_{32}^*, \cdot)$ $\quad (U(\mathbb{Z}_{32}), \cdot)$

Rez: a. 31 prim

Th. Fermat: $a^{p-1} \equiv 1 \bmod p, \ \forall a \in \mathbb{Z}, p \nmid a$.

$\hat{a}^{30} = \hat{1}, \ \forall \hat{a} \in \mathbb{Z}_{31}^*$.

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

$\hat{5}^2 = \hat{25}, \quad \hat{5}^3 = \hat{1} \Rightarrow ord(\hat{5}) = 3$.

$\hat{13}^2 = \hat{169} = \hat{14}, \quad \hat{13}^3 = \hat{13} \cdot \hat{14} = \hat{27} = -\hat{4}$

$\hat{13}^5 = \hat{14} \cdot (-\hat{4}) = -\hat{56} = \hat{6}, \quad \hat{13}^6 = \hat{16}$

$\left.\begin{array}{l} \hat{13}^{10} = \hat{36} = \hat{5} \\ ord(\hat{5}) = 3 \end{array}\right\} \Rightarrow ord(\hat{13}) = 30$.

$\hat{13}^{10} = \hat{5}$

$(\hat{13}^{10})^3 = \hat{5}^3 = \hat{1}$

$ord(x^k) = \frac{m}{(m, k)}$

$m = ord(x)$

$ord(\hat{13}^{10}) = 3$

$\Rightarrow \frac{m}{(m, 10)} = 3$

$\hat{20} = -\hat{11}$

$\hat{20}^2 = \hat{28} = -\hat{3}$

$\hat{20}^3 = -\hat{60} = \hat{2}$

$\hat{20}^5 = -\hat{6}$

$\hat{20}^6 = \hat{4}$

$\hat{20}^{10} = \hat{36} = \hat{5}$

$\hat{20}^{15} = -\hat{30}$

$\Rightarrow \text{ord}(\hat{20}) = 30$.

$\hat{31} = \hat{62} = \hat{0}$

$-\hat{60} = \hat{0} - \hat{60} = \hat{62} - \hat{60} = \hat{2}$.

b. $\hat{7}, \hat{11}, \hat{15}$ în $(\mathbb{Z}_{32}, \cdot)$

$(7, 32) = (11, 32) = (15, 32) = 1$

Obs: $\hat{a} \in \mathbb{Z}_m$, $(a, m) \neq 1 \Rightarrow \hat{a} \notin U(\mathbb{Z}_m)$

Dacă $\text{ord}(\hat{a}) = k \Rightarrow \hat{a}^k = \hat{1} \Rightarrow \hat{a} \cdot \hat{a}^{k-1} = \hat{1} \Rightarrow \hat{a} \in U(\mathbb{Z}_m)$.

TR. Euler: $a^{\varphi(m)} \equiv 1 \mod m$, $(a, m) = 1$, $32 = 2^5$

$\varphi(32) = 32 \cdot \left(1 - \frac{1}{2}\right) = 16$. $\Rightarrow \text{ord}(\hat{a}) \mid 16$.

$\hat{7}^2 = \hat{49} = \hat{17} = -\hat{15}$

$\hat{7}^4 = \hat{17} \cdot \hat{17} = \hat{15} \cdot \hat{15} = \hat{15} \cdot \hat{3} \cdot \hat{5} = \hat{45} \cdot \hat{5} = \hat{13} \cdot \hat{5} = \hat{65} = \hat{1}$

$\Rightarrow ord(\hat{7}) = 4.$

$\hat{11}^2 = \hat{121} = -\hat{1}$ $\qquad ord(\hat{15}) = 2.$

$\hat{11}^4 = \hat{49} = -\hat{15}$

$\hat{11}^8 = \hat{1} \Rightarrow ord(\hat{11}) = 8.$

p prim, $\varphi(p) = p\left(1 - \frac{1}{p}\right) = p \cdot \frac{p-1}{p} = p - 1$

Temă: Det. elem. de ordin k în grupul specificat:

a. $k = 2$, $(\mathbb{Q}^*, \cdot)$

b. $k = 2$, $(\mathbb{Z}_{14}, +)$ $\qquad x^k = 1.$

c. $k = 3$, $(\mathbb{Z}_{48}, +)$

d. $k = 4$, $(\mathbb{C}^*, \cdot)$

Permutări

Ex. 2: Fie $\sigma = (a_1\ a_2 \dots a_m)$ un ciclu de lungime m.
Arătați că pt. orice $i = \overline{1,m}$ avem că:

$\sigma^i(a_k) = a_{k+i}$ (unde $k+i$ este înlocuit de restul mod m dacă $k+i > m$).

Rez: Dem. prin inducție după i.

$$\sigma^1 = (a_1 \dots a_m)$$

$$\begin{cases} \sigma(a_i) = a_{i+1}, & 1 \le i \le m-1 \\ \sigma(a_m) = a_1 & (m+1 \equiv 1 \bmod m) \end{cases}$$

Pasul de inducție: $\sigma^i(a_k) = a_{k+i}$

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

Ex. 3: Pentru ce valori ale lui i, $1 \le i \le 6$, este permutarea σ^i un 6-ciclu, unde $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$?

Rez: $\sigma^1 = \sigma = (1\ 2\ 3\ 4\ 5\ 6)$ 6-ciclu

$\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$ produs de 2 3-cicli

$\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$ produs de 3 2-cicli (transp)

$\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$ produs de 2 3-cicli

$\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2) = \sigma^{-1}$, $\sigma^6 = e$.

σ^i 6-ciclu $\Leftrightarrow$ $(i, 6) = 1$.

Obs: σ ciclu de lungime n

σ^i:
- $i \mid n \rightarrow i$ cicli de lung. $\frac{n}{i}$
- $(i, n) = 1 \rightarrow n$-ciclu
- $(i, n) \neq 1$

$(i, n) = d \neq 1$

$i = d \cdot j \qquad (j, m) = 1$

$n = d \cdot m$

$\sigma^i = (\sigma^d)^j = (c_1 \cdot c_2 \cdots c_d)^j$

$= c_1^j \cdot c_2^j \cdot \ldots \cdot c_d^j$

c_k - cicli de lung $\frac{n}{d} = m$

c_k^j - m-ciclu

Rezolvarea ecuațiilor de tip $\tau^i = \sigma$.

$\tau = c_1 \cdot \ldots \cdot c_k$ produs de cicli disjuncți, $\mathrm{ord}(c_t) = l_t$.

$\tau^2 = c_1^2 \ldots c_k^2$,

$2 \mid l_t \Rightarrow c_t^2$ - produs de 2 cicli de lungime $l_t/2$

$2 \nmid l_t \Rightarrow c_t^2$ - l_t - ciclu

Ex. 4: Rezolvați ecuația $\tau^2 = \sigma$ în S_{10}, unde:

a. $\sigma = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$

b. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 4 & 10 & 6 & 1 & 2 & 9 & 7 \end{pmatrix} = (1\ 5\ 10\ 7)(2\ 8) \to \tau^2 = \sigma$ nu va avea sol.

c. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 1 & 5 & 10 & 8 & 6 & 9 & 7 \end{pmatrix} = (1\ 2\ 3\ 4)(6\ 10\ 7\ 8) \to \tau^2 = \sigma$ va avea 4 sol.

Rez: a. $\operatorname{sgn}(\sigma) = 1$.

$\tau^2 = \sigma$

$\tau = c_1 \dots c_k$ produs de cicli disj., $\operatorname{ord}(c_i) = l_i$

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

Dacă $\begin{cases} 2 \mid l_i \Rightarrow c_i^2 \text{ produs de 2 cicli de lung. } \frac{l_i}{2} \\ 2 \nmid l_i \Rightarrow c_i^2\ \ l_i\text{-ciclu} \end{cases}$

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

τ^2 = produs de 2 5-cicli

$\tau = c_1 \cdot c_2$, c_1, c_2 5-cicli

$c_1^2 c_2^2 = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$

$c_1^2 = (1\ 2\ 3\ 4\ 5) \Rightarrow c_1 = c_1^6 = (1\ 4\ 2\ 5\ 3)$

$c_2^2 = (6\ 7\ 8\ 9\ 10) \Rightarrow c_2 = (6\ 9\ 7\ 10\ 8)$

$c^2 = (1\ 2\ 3\ 4\ 5)$

$c = (1\ \underline{4}\ 2\ \underline{5}\ 3)$

sau $\tau = c$, c = 10-ciclu

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

$c = (1\ 6\ 2\ 7\ 3\ 8\ 4\ 9\ 5\ 10)$

$(6\ 7\ 8\ 9\ 10) = (7\ 8\ 9\ 10\ 6) = (8\ 9\ 10\ 6\ 7) = \ldots$

$c = (1\ 7\ 2\ 8\ 3\ 9\ 4\ 10\ 5\ 6)$

$c = (1\ 8\ 2\ 9\ 3\ 10\ 4\ 6\ 5\ 7)$

$c = (1\ 9\ 2\ 10\ 3\ 6\ 4\ 7\ 5\ 8)$, $c = (1\ 10\ 2\ 6\ 3\ 7\ 4\ 8\ 5\ 9)$