Seminar 10

Ex. 1: Fie $(G, \cdot)$ un grup, $a, b \in G$ de ordin finit a.î. $ab = ba$, $\text{ord}(a) = m$, $\text{ord}(b) = n$. Arătați că dacă $(m, n) = 1$, atunci $\text{ord}(ab) = mn$.

Rez: $\text{ord}(ab) = mn \Leftarrow (ab)^{mn} = e$ ✓

mn este minim cu această proprietate.

Pp. că $\text{ord}(ab) = k \Rightarrow (ab)^k = e$

$(ab)^{mn} = e \Rightarrow k \mid mn$.

$(ab)^k = e \Rightarrow a^k \cdot b^k = e \Rightarrow a^k = b^{-k} \Big|^n$

$$\left.\begin{array}{l} a^{nk} = b^{-nk} \\ \text{ord}(a) = n \end{array}\right\} \Rightarrow b^{-nk} = e \Rightarrow \left.\begin{array}{l} n \mid nk \\ (n, n) = 1 \end{array}\right\} \Rightarrow n \mid k.$$

Analog se arată că $\left.\begin{array}{l} n \mid k \\ n \mid k \end{array}\right\} \Rightarrow \left.\begin{array}{l} [n, n] \mid k \\ (n, n) = 1 \end{array}\right\} \Rightarrow mn \mid k$

$k \mid mn$ și $mn \mid k \Rightarrow k = mn$.

Ex. 2: Fie G, H două grupuri, $G \times H$ grup. Fie $a \in G$, $b \in H$ cu $\text{ord}(a) = m$ în G, $\text{ord}(b) = m$ în H. Atunci $\text{ord}((a,b)) = [m, m]$.

Rez: Asemănător cu Ex. 1.

Ex. 3: Calculați ordinul lui $(\hat{5}, \overline{3})$ în $(\mathbb{Z}_6 \times \mathbb{Z}_8, +)$, $(\mathbb{Z}_{11} \times \mathbb{Z}_9, +)$.

Rez: $(\mathbb{Z}_6 \times \mathbb{Z}_8, +)$

$\text{ord}(\hat{k}) = \frac{m}{(m,k)}$ în $\mathbb{Z}_m$

$\text{ord}((\hat{5}, \overline{3})) = [\text{ord}(\hat{5}), \text{ord}(\overline{3})]$

$\text{ord}(\hat{5}) = \frac{6}{(6,5)} = 6$

$\text{ord}(\overline{3}) = \frac{8}{(8,3)} = 8$

$\text{ord}((\hat{5}, \overline{3})) = [6, 8] = 24$.

$(\mathbb{Z}_{11} \times \mathbb{Z}_9, +)$

$ord((\hat{5}, \bar{3})) = [ord(\hat{5}), ord(\bar{3})] = [11, 3] = 33$

$ord(\hat{5}) = \frac{11}{(11,5)} = 11$, $ord(\bar{3}) = \frac{9}{(3,9)} = \frac{9}{3} = 3$

Ex. 4 : a. Determinați elementele de ordin 4 din $(\mathbb{Z}_{12} \times \mathbb{Z}_{14}, +)$.

b. Determinați elementele de ordin 12 din $(\mathbb{Z}_9 \times \mathbb{Z}_{24}, +)$.

Rez :

a. $(a, b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{14}$

$[ord(a), ord(b)] = 4$

$[m, m] = 4$, $(m, m) \in \{(1,4), (2,4), (4,4), (4,2), (4,1)\}$

$a \in \mathbb{Z}_{12} \Rightarrow m \mid 12$

$b \in \mathbb{Z}_{14} \Rightarrow m \mid 14$

Obs: G grup finit. Atunci orice $x \in G$ are ordin finit. În mai mult, $ord(x) \mid |G|$.

$(m,m) \in \{(1,4),(2,4),(4,4),(4,2),(4,1)\}$.

$m \mid 12$, $m \mid 14$.

$\Rightarrow (m,m) \in \{(4,2),(4,1)\}$.

$(m,m) = (4,2)$

$ord(a) = 4$

$ord(a) = \frac{12}{(a,12)} = 4 \Rightarrow (a,12) = 3 \Rightarrow a \in \{\hat{3}, \hat{9}\}$.

$ord(b) = 2 = \frac{14}{(b,14)} \Rightarrow (b,14) = 7 \Rightarrow b \in \{\hat{7}\}$

$(\hat{3},\hat{7})$, $(\hat{9},\hat{7})$

$(m,m) = (4,1)$

$ord(a) = 4 \Rightarrow a \in \{\hat{3}, \hat{9}\}$
$ord(b) = 1 \Rightarrow b = \hat{0}$
$\Rightarrow (\hat{3},\hat{0}), (\hat{9},\hat{0})$.

In total sunt 4 elem. de ordin 4 în $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$.

$ord(x) = k \in \mathbb{N}^* \iff kx = 0$ și k este minim cu această proprietate.

$ord(x) = 1 \iff 1 \cdot x = 0.$

b. $ord\ 12$ dim $(\mathbb{Z}_9 \times \mathbb{Z}_{24}, +)$

$ord(a,b) = [ord(a), ord(b)] = [m,n] = 12$

$(m,n) \in \{(1,12), (2,12), (3,12), (4,12), (6,12),$
$(12,12), (12,1), (12,2), (12,3), (12,4), (12,6), (4,3),$
$(4,6), (3,4), (6,4)\}$

$a \in \mathbb{Z}_9 \Rightarrow m \mid 9 \Rightarrow m \in \{1,3,9\}$

$b \in \mathbb{Z}_{24} \Rightarrow m \mid 24$

$\Rightarrow (m,n) \in \{(1,12), (3,12), (3,4)\}$

$(m,m) = (1,12)$

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

$ord(b) = 12 = \frac{24}{(24,b)} \Rightarrow (24,b) = 2 \Rightarrow b \in \{\hat{2}, \hat{10}, \hat{14}, \hat{22}\}$ — 4 per.

$b = 2k, \ (k,12) = 1 \Rightarrow k \in \{1,5,7,11\}$

$(m,m) = (3,12)$

$ord(a) = 3 = \frac{9}{(a,9)} \Rightarrow (a,9) = 3 \Rightarrow a \in \{\hat{3}, \hat{6}\}$.

$ord(b) = 12 \Rightarrow b \in \{\hat{2}, \hat{10}, \hat{14}, \hat{22}\}$. → 8 perechi

$(m,m) = (3,4)$

$ord(a) = 3 \Rightarrow a \in \{\hat{3}, \hat{6}\}$

$ord(b) = 4 = \frac{24}{(b,24)} \rightarrow (b,24) = 6 \Rightarrow b \in \{\hat{6}, \hat{18}\}$ — 4 perechi

$b = 6k, \ (k,4) = 1$

În total sunt 16 perechi

$[m, n] = 12$

$m \mid 9 \Rightarrow m \in \{1, 3, 9\}$

$m \mid 24 \Rightarrow m \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

Euler: $a, m \in \mathbb{N}^*$, $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$

Fermat: p prim, $a \in \mathbb{N}$, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \mod p$.

Ex. 5: Calculați:

a. 2020^{2020} în $\mathbb{Z}_{31}$

b. 2020^{2020} în $\mathbb{Z}_{30}$

c. 2020^{2020} în $\mathbb{Z}_{21}$

Rez: a. 31 nr. prim, $31 \nmid 2020$

$\hat{2020} = \hat{5}$ $\qquad$ $\hat{5}^{2020} = \hat{2020}^{2020}$

$2020 = 31 \cdot 65 + 5$

Fermat: $\hat{5}^{30} = \hat{1}$

$\hat{5}^{2020} = \hat{5}^{30 \cdot 67 + 10} = \left(\hat{5}^{30}\right)^{67} \cdot \hat{5}^{10} = \hat{5}^{10} = \hat{5}^{1}$

$\hat{1}^{67} = \hat{1}$

Var. 1: $\hat{5}^2 = \hat{25} = \hat{-6}$ $\quad \hat{25} = \hat{25} - \hat{31} = \hat{-6}$

$\hat{5}^4 = \hat{625} = \hat{36} = \hat{5}$

$\hat{5}^8 = \hat{5}^2$, $\hat{5}^{10} = \hat{5}^2 \cdot \hat{5}^8 = \hat{5}^2 \cdot \hat{5}^2 = \hat{5}^4 = \hat{5}$

Var 2: $\operatorname{ord}(\hat{5}) = 3$ $\quad$ in $\mathbb{Z}_{31}$

b. 2020^{2020} in $\mathbb{Z}_{30}$

$\hat{2020}^{2020} = \hat{10}^{2020} = \hat{10}$

$(10, 30) = 10 \neq 1$

$\hat{10}^2 = \hat{100} = \hat{10}$

$\hat{5}^{2020} = \hat{25}$

$\hat{5}^2 = \hat{25} \quad (= -\hat{5})$

$\hat{5}^3 = \hat{125} = \hat{5}$

$\hat{5}^{2k+1} = \hat{5}$

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

c. 2020^{2020} în $\mathbb{Z}_{21}$

$\hat{2020}^{2020} = \hat{4}^{2020}$

$(4, 21) = 1 \rightarrow$ Putem aplica Euler

$\varphi(21) = 21\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12.$

$m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ desc. în factori primi, $a_i \geq 1$, p_i prime

$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

$\hat{4}^{12} = \hat{1}$

$\hat{4}^{2020} = \hat{4}^{12 \cdot 168 + 4} = \hat{4}^{4} = \hat{16} \cdot \hat{16} = (\hat{-5}) \cdot (\hat{-5}) = \hat{25} = \hat{4}$

Obs: $\hat{12}^{2020}$ în $\mathbb{Z}_{30}$

$(12, 30) = 6$

$\hat{12} = \hat{6} \cdot \hat{2}$

$\hat{14}^{2020} = \hat{2}^{2020} \cdot \hat{7}^{2020}$ → Euler

$a^{b^b} \bmod n$

$(a, n) = 1 \rightsquigarrow$ Euler

$a^{b^b} \bmod \varphi(m)$