Seminar 8 - 143

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

$\hat{a}^{\varphi(m)} = \hat{1}$ in $\mathbb{Z}_m$.

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

$(a,p)=1$

Ex. 1: 2020^{2020} in $\mathbb{Z}_{31}$

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

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

$= \hat{25}^5 = \hat{25}^3 \cdot \hat{25}^2 = \hat{1} \cdot \hat{5} = \hat{5}$

$\hat{625} = \hat{620} + \hat{5} = \hat{5}$

$\hat{25}^3 = \hat{125}^2$

2020^{2020} in $\mathbb{Z}_{32}$

$(2020, 32) = 4$

$\hat{2020}^{2020} = (\hat{4} \cdot 505)^{2020} = \hat{4}^{2020} \cdot \underline{505^{2020}}$

Euler

$\varphi(32) = 32 \cdot \left(1 - \frac{1}{2}\right) = 16$

$n = p_1^{a_1} \cdots p_k^{a_k} \Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

Euler: $\hat{505}^{16} = \hat{1}$

$\hat{2020}^{2020} = \hat{4}^{2020} \cdot \hat{505}^{2020} = \hat{4}^{2020} \cdot \hat{505}^{16\cdot 126 + 4} =$

$= \hat{4}^{2020} \cdot (\hat{505}^{16})^{126} \cdot \hat{505}^4 = \hat{4}^{2020} \cdot \hat{505}^4 =$

$= \hat{4}^{2020} \cdot \hat{25}^4 = (\hat{2}^2)^{2020} \cdot \hat{25}^4 = (\hat{2}^5)^{\cdots} \cdot \hat{25}^4 = \hat{0}.$

$\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$; $\varphi(p) = p\left(1 - \frac{1}{p}\right) = p - 1$.

Ex 2: Fie G monoidul cu tabla de înmulțire:

·	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	b	c	1	e	f	g	d
b	b	c	1	a	f	g	d	e
c	c	1	a	b	g	d	e	f
d	d	g	f	e	1	c	b	a
e	e	d	g	f	a	1	c	b
f	f	e	d	g	b	a	1	c
g	g	f	e	d	c	b	a	1

a. Arătați că G este grup necomutativ, generat de $\{a, d\}$.

b. Det. ordinul elem. din G.

c. Det. subgrupurile lui G. Specificați care sunt normale.

d. Arătați că $G/\langle b \rangle$ este izomorf cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Rez:

- Elem. neutru: 1
- Elem. sim: $1 = ac = b^2 = ca = d^2 = e^2 = f^2 = g^2$

$G = \langle a, d \rangle$

$a, d \in G \Rightarrow \langle a, d \rangle$ subgrup în G.

$G \subseteq \langle a, d \rangle$

Putem să scriem fiecare $x \in G$ ca combinație de a și d

$\langle a, d \rangle = \{1, a, d, a^2 = b, a^3 = c, ad = e, a^2d = f, a^3d = g\}$

$G = \{1, a, a^2, a^3, d, ad, a^2d, a^3d\} \cong D_4$

Obs: Grupul DIEDRAL D_m (D_{2m}). Vom nota D_m (m = ordinul elementului rotație).

$D_m = \langle h, r \rangle$ $\Rightarrow$ h = simetrie, $h^2 = 1$

r = rotație de $\frac{2\pi}{m}$, $r^m = 1$.

b. $ord(b) = ord(d) = ord(e) = ord(f) = ord(g) = 2$

$ord(a) = ord(c) = 4$.

c. Subgrupurile lui $G: \{1\}, G$.

* $\langle a \rangle = \{1, a, b, c\} = \langle c \rangle$
* $\langle b \rangle = \{1, b\}$

$\langle d \rangle = \{1, d\}$

$\langle e \rangle = \{1, e\}$

$\langle f \rangle = \{1, f\}$.

$\langle g \rangle = \{1, g\}$.

* $\langle b, d \rangle = \{1, b, d, bd = f\}$

$\parallel$

$\langle b, f \rangle$

* $\langle b, e \rangle = \{1, b, e, g\} = \langle b, g \rangle$.

Obs: Se poate obs. că $xb = bx$, $\forall x \in G$.

Dacă H este subgrup în G cu proprietatea că $xh = hx$ $\forall h \in H$, $x \in G$, atunci H este normal.

$H = \langle a \rangle = \{1, a, b, c\}$.

$aH = H = Ha$

$bH = Hb = H$ deoarece $xb = bx$, $\forall x \in G$.

$cH = H = Hc$

$dH = \{d, da, db, dc\} = \{d, g, f, e\}$

$Hd = \{d, ad, bd, cd\} = \{d, e, f, g\}$.

$eH = \{e, d, g, f\} = \{e, f, g, d\} = He$

Se arată că $fH = Hf$ și $gH = Hg$.

Obs: Dacă G este grup finit și H subgrup în G cu $|G:H| = 2$, atunci H este normal.

$|G:H| = \frac{|G|}{|H|}$ (Lagrange)

d. $G/\langle b \rangle$, $\langle b \rangle = H$. - normal

Lagrange: $|G| = |H| \cdot |G:H|$

$8 = 2 \cdot |G:H| \Rightarrow |G:H| = 4 \Rightarrow |G/H| = 4$.

$H = \{1, b\}$

G/H : $\hat{1} = \hat{b}$

$G/H = \{\hat{x} \mid x \in G\}$, $\hat{x} = xH = Hx$.

$\hat{1} = \{1, b\} = H = \hat{b}$

$\hat{a} = aH = \{a, ab\} = \{a, c\} = \hat{c}$

$\hat{d} = dH = \{d, f\} = \hat{f}$

$\hat{e} = eH = \{e, g\} = \hat{g}$

$G/H = \{\hat{1}, \hat{a}, \hat{d}, \hat{e}\}$.

Altfel : $G = \{1, a, a^2, a^3, d, ad, a^2d, a^3d\}$, $b = a^2$.

$H = \{1, a^2\}$. $\hat{1} = \hat{a^2}$ $\hat{a} \cdot \hat{d} = \hat{1} \cdot \hat{a} = \hat{a}$ $\hat{d}$ $\hat{ad}$

$G/H = \{\hat{1}, \hat{a}, \hat{d}, \hat{ad}\} = \{\hat{1}, \hat{a}, \hat{d}, \hat{e}\}$.

$G/H \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

Obs: Un grup cu 4 elem. este izomorf cu $(\mathbb{Z}_4, +)$ sau cu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

$ord(\hat{a}) = ord(\hat{d}) = ord(\hat{e}) = 2$. $\Rightarrow G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$\hat{a}^2 = \hat{b} = \hat{1}$.

$(G/H)_D = \{xH \mid x \in G\}$

$\| \quad \hat{x}$

$x \sim y \iff xy^{-1} \in H \iff x \in Hy$. $(G/H)_d$.

$(\mathbb{Z}_4, +)$ → grup ciclic + are elem. de ordin 4.

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ → orice elem. ≠ elem. neutru are ordin 2

Ex. (temă): Fie G_1, G_2 două grupuri, 1_{G_1} = elem. neutru în G_1, 1_{G_2} = elem. neutru în G_2. Numai $G_1 \times G_2$ este grup cu elem. neutru $(1_{G_1}, 1_{G_2})$. Mai mult, dacă $a \in G_1$, $\text{ord}(a) = m < \infty$, $b \in G_2$, $\text{ord}(b) = n < \infty$, atunci $\text{ord}((a,b)) = [m,n]$.

$p = [m,n]$
$d = (m,n)$
$\Rightarrow p \cdot d = m \cdot n$
$m = d \cdot m'$
$n = d \cdot n'$
$(m',n') = 1$
$\Rightarrow p = d \cdot m' \cdot n'$.

$(a,b)^p = (a^p, b^p) = (a^{d \cdot m' \cdot n'}, b^{d \cdot m' \cdot n'}) = ((a^m)^{n'}, (b^n)^{m'})$
$= (1_{G_1}, 1_{G_2})$.

+ verif. că p este cel mai mic nr. nat. cu această proprie.

Ex. 3: Det. ordinul lui $(\hat{3}, \hat{2})$ în $(\mathbb{Z}_5 \times \mathbb{Z}_4, +)$, $(\mathbb{Z}_9 \times \mathbb{Z}_{12}, +)$ și $(\mathbb{Z}_{15} \times \mathbb{Z}_{20}, +)$.

Rez:

G grup, $\text{ord}(x) = m \Rightarrow \text{ord}(x^k) = \frac{m}{(m,k)}$ ← comandă

$\text{ord}(\hat{1}) = m$ în $(\mathbb{Z}_m, +)$
$\text{ord}(\hat{k}) = \frac{m}{(m,k)}$ în $(\mathbb{Z}_m, +)$

$\mathbb{Z}_5 \times \mathbb{Z}_4$
$\text{ord}(\hat{3}) = 5$
$\text{ord}(\hat{2}) = 4$
$\Rightarrow \text{ord}(\hat{3}, \hat{2}) = 35$

$\mathbb{Z}_9 \times \mathbb{Z}_{12}$:
$\text{ord}(\hat{3}) = 3 \left(= \frac{9}{3}\right)$
$\text{ord}(\hat{2}) = \frac{12}{2} = 6$
$\Rightarrow \text{ord}(\hat{3}, \hat{2}) = 6$.

$\mathbb{Z}_{15} \times \mathbb{Z}_{20}$:

$\left.\begin{array}{l} ord(\hat{3}) = \frac{15}{3} = 5 \\ ord(\hat{2}) = 10 \end{array}\right\} \Rightarrow ord(\hat{3}, \hat{2}) = 10.$

Ex. 4 : Det. câte elemente de ordin 10 din $\mathbb{Z}_{15} \times \mathbb{Z}_{20}$.

Rez :

$(a,b) \in \mathbb{Z}_{15} \times \mathbb{Z}_{20}$

$[ord(a), ord(b)] = 10$

$ord(a) \mid 15 \Rightarrow ord(a) \in \{1,3,5,15\}.$

$ord(b) \mid 20 \Rightarrow ord(b) \in \{1,2,4,5,10,20\}.$

$(ord(a), ord(b)) \in \{(1,10), (5,10), (5,2)\}$

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

$ord(b) = 10 \Rightarrow b \in \{\hat{2}, \hat{6}, \hat{14}, \hat{18}\}$

$ord(b) = \frac{20}{(b,20)} = 10 \Rightarrow (b,20) = 2 \Rightarrow b = 2 \cdot c$

$(c, 10) = 1$

$(\hat{0}, \hat{2}), (\hat{0}, \hat{6}), (\hat{0}, \hat{14}), (\hat{0}, \hat{18})$

II. $ord(a) = 5 = \frac{15}{(a,15)} \Rightarrow (a,15) = 3 \Rightarrow a \in \{\hat{3}, \hat{6}, \hat{9}, \hat{12}\}.$

$a = 3k$

$(k, 5) = 1$

$ord(b) = 10 \Rightarrow b \in \{\hat{2}, \hat{6}, \hat{14}, \hat{18}\}$

III. $ord(a) = 5 \Rightarrow a \in \{\hat{3}, \hat{6}, \hat{9}, \hat{12}\}.$

$ord(b) = 2 = \frac{20}{(b,20)} \Rightarrow (b,20) = 10 \Rightarrow b = \hat{10}.$

Obs : $\hat{Im}(\mathbb{Z}_p^*, \cdot)$, avem $\hat{a}^{p-1} = \hat{1}$, $\forall a \in \mathbb{Z}_p^*$.

$\Rightarrow ord(a) \mid p-1$, $\forall a \in \mathbb{Z}_p^*$.