Seminar 11

ex 1

1583^{1723} restul împărțirii la 29

Sol:

$$1583 : 29 = 54 \text{ r } 17$$

```
1583
145
=133
 116
 =17
```

$$1583^{1723} \equiv 17^{1723} \pmod{29}$$

$$29 \text{ e prim } \overset{\text{Fermat}}{\underset{(17,29)=1}{\Longrightarrow}} 17^{28} \equiv 1 \pmod{29}$$

```
1723 | 28
168  | 61
  43
  28
  15
```

$n = p$ prim

$\varphi(p) = p-1$

Euler $n \in \mathbb{N}^*$

$a \in \mathbb{Z}$ $(a, n) = 1$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Fermat p prim $a \in \mathbb{Z}$

$$a^p \equiv a \pmod{p}$$

Dacă $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$$17^{1723} = 17^{28\cdot 61+15} = (17^{28})^{61}\cdot 17^{15} \pmod{29} \overset{(1)}{\equiv} 1\cdot 17^{15} \pmod{29}$$

$$\equiv (17^2)^7 \cdot 17 \pmod{29}$$

$$\equiv 289^7 \cdot 17 \pmod{29}$$

$$\equiv (-1)^7 \cdot 17 \pmod{29}$$

$$\equiv -17 \pmod{29}$$

$$\equiv 12 \pmod{29}$$

$\Rightarrow$ Restul împ. lui 1583^{1723} la 29 este 12

ex 2

$$1333^{4132^{6243}} \pmod{31} \equiv 0 \pmod{31}$$

Sol:

$$1333 : 31 = 43$$

$$\begin{array}{l} \underline{124} \\ ==93 \end{array}$$

ex 3

$$3145^{4132^{6243}} \pmod{31} \equiv 14^{4132^{6243}} \pmod{31}$$

Sol:

$$3145 \equiv 14 \pmod{31}$$

$(14, 31) = 1$; 31 e prim $\overset{\text{Euler}}{\Rightarrow}$ $14^{\varphi(31)} \equiv 1$

$\varphi(31) = 30$

Vrem să aflăm restul împ. lui $x = 4132^{6243}$ la 30

$$4132^{6243} = (-8)^{6243} \pmod{30}$$

$4132 : 30 = 137$
30
113
90
232
210
$= 22 = -8$

$$\equiv -2^{3\cdot 6243} \pmod{30}$$

$$\overset{32}{2^5} \equiv 2 \pmod{30}$$

$$(2^5)^5 \equiv 2^5 \pmod{30} \equiv 2 \pmod{30}$$

$$\equiv -2^{18729} \text{ (mod}$$

$18729 : 25 = 749$
175
$= 122$
100
$= 229$
225
$= 4$

$$\equiv -2^{25\cdot 749+4} \pmod{30}$$

$$\equiv -(2^{25})^{749} \cdot 2^4 \pmod{30}$$

$$\equiv -2^{749} \cdot 2^4 \pmod{30}$$

$$\equiv -(2^{25})^{30} \cdot 2^3 \pmod{30}$$

$753 = 25 \cdot 30 + 3$

$$= -2^{33} \cdot 2 \pmod{30}$$

$$= (-2^{25}) \cdot 2^8 \pmod{30}$$

$$= -2 \cdot 64 \pmod{30}$$

$$= -128 \pmod{30}$$

$$= -8 \pmod{30}$$

$$= 22 \pmod{30}$$

$$14^x \equiv 14^{30 \cdot k + 22} \pmod{31}$$

$$\equiv (14^{30})^k \cdot 14^{22} \pmod{31}$$

$$\equiv 14^{22} \pmod{31}$$

$$\equiv 196^{11} \pmod{31}$$

$$\equiv 10^{11} \pmod{31}$$

$$\equiv (10^3)^3 \cdot 100 \pmod{31}$$

$$\equiv 8^3 \cdot 100 \pmod{31}$$

$1000 \equiv 8 \pmod{31}$

$100 \equiv 7 \pmod{31}$

$$\equiv 8^3 \cdot 7 \pmod{31}$$

$$\equiv 16 \cdot 7 \pmod{31}$$

$$\equiv 112 \pmod{31}$$

$$\equiv 19 \pmod{31}$$

$512 : 31 = 16$
31
$\overline{202}$
186
$\overline{16}$

Avem că $3145^{4132^{6247}} \equiv 19 \pmod{31}$

$\square$

$U(\mathbb{Z}_n, \cdot) = \{ \hat{k} \mid 1 \le k \le n-1, \ (k, n) = 1 \}$ ↳ grup abelian

$n \in \mathbb{N}, n \ge 2$

Exemple

$U(\mathbb{Z}_8, \cdot) = \{ \hat{1}, \hat{3}, \hat{5}, \hat{7} \}$ → grup cu 4 elemente

$U(\mathbb{Z}_{12}, \cdot) = \{ \hat{1}, \hat{5}, \hat{7}, \hat{11} \}$ → grup cu 4 el

$U(\mathbb{Z}_{20}, \cdot) = \{ \hat{1}, \hat{3}, \hat{7}, \hat{9}, \hat{11}, \hat{13}, \hat{17}, \hat{19} \}$

2 grupuri

$f : (G_1, \cdot) \to (G_2, *)$ morfism de grupuri

$$\boxed{f(x \cdot y) = f(x) * f(y)} \quad \forall\, x, y \in G_1$$

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) * f(e_1) \quad \Big| \cdot f(e_1)^{-1}$$

$$f(e_1) * f(e_1)^{-1} = f(e_1) * \left(f(e_1) * f(e_1)^{-1} \right)$$

$$e_2 = f(e_1) * e_2$$

$$e_2 = f(e_1)$$

---

izomorfism de grupuri = morfism bij

Ordinul unui element g în grupul $(G, \cdot)$

$$\text{ord}(g) = \begin{cases} \infty, & \text{dacă } g^n \neq e \ (\forall)\, n \in \mathbb{N}^* \\ \text{cel mai mic } n \in \mathbb{N}^* \text{ a.î. } g^n = e & \text{altfel} \end{cases}$$

$\text{ord}(g) = 1 \iff g = e \to$ el. neutru

Exemple

$$U(\mathbb{Z}_{23}, \cdot) = \mathbb{Z}_{23} \setminus \{\hat{0}\} = \{\hat{1}, \dots, \widehat{22}\}$$

$(G, \cdot)$ grup finit

$g \in G$ $\quad \langle g \rangle$ = subgrup gen. de g în G

$$\text{ord}(g) = |\langle g \rangle| \;\big|\; |G|$$

$\Rightarrow g^{|G|} = e \quad \forall\, g \in G \to$ grup finit

$\mathrm{ord}(\hat{2}) =$ $\qquad \hat{2}^2 = \hat{4}$

$\hat{2}^{11} = \widehat{32} \cdot \widehat{32} \cdot \hat{2} = \widehat{200} = \hat{2}$

$(\Leftrightarrow 2^{11} = 32 \cdot 32 \cdot 2 \pmod{23}$

$\equiv 9 \cdot 9 \cdot 2 \pmod{23}$

$\equiv 162 \pmod{23}$

$\equiv 1 \pmod{23})$

$\Rightarrow \mathrm{ord}(\hat{2}) \mid 11)$

$\hat{2}^3, \dots, \hat{2}^{10} \neq 1$

(Ex!)

$\Rightarrow \mathrm{ord}(\hat{2}) = \widehat{11}$

Dacă $g \in (G, \cdot)$

$g^n = e \Rightarrow \underline{\mathrm{ord}(g) \mid n}$

<u>Teoremă</u>

Orice grup abelian finit e izomorf cu

$\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r}$

$1 < d_1 \mid \dots \mid d_r$

$d_1 \cdot \ldots \cdot d_r = n$

Obs Dacă $f:(G_1,\cdot)\to(G_2,+)$ este izomorfism de grupuri $\Rightarrow (\forall)\ g\in G_1$ avem $ord(g) = ord(f(g))$

Exerciții

$U(\mathbb{Z}_8,\cdot) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\}$

$ord(\hat{1}) = 1$

$ord(\hat{3}) = 2$

$ord(\hat{5}) = 2$

$ord(\hat{7}) = 2$

$U(\mathbb{Z}_{12},\cdot) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}\}$

$ord(\hat{1}) = 1$

$ord(\hat{5}) = 2$

$ord(\hat{7}) = 2$

$ord(\hat{11}) = 2$

$U(\mathbb{Z}_{20},\cdot) = \{\hat{1}, \hat{3}, \hat{7}, \hat{9}, \hat{11}, \hat{13}, \hat{17}, \hat{19}\}$

$ord\ \hat{1} = 1$ $\qquad$ $ord\ \hat{13} = \hat{4}$

$ord\ \hat{3} = 4$

$ord\ \hat{7} = 4$

$ord\ \hat{9} = 2$

$ord\ \hat{11} = 2$

$U(\mathbb{Z}_8, \cdot)$

	$\hat{1}$	$\hat{3}$	$\hat{5}$	$\hat{7}$
$\hat{1}$	$\hat{1}$	$\hat{3}$	$\hat{5}$	$\hat{7}$
$\hat{3}$	$\hat{3}$	$\hat{1}$	$\hat{7}$	$\hat{5}$
$\hat{5}$	$\hat{5}$	$\hat{7}$	$\hat{1}$	$\hat{3}$
$\hat{7}$	$\hat{7}$	$\hat{5}$	$\hat{3}$	$\hat{1}$

$U(\mathbb{Z}_{12}, \ )$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\hat{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\hat{1}$

$f : U(\mathbb{Z}_8, \cdot) \to U(\mathbb{Z}_{12}, \cdot)$

$f(\hat{1}) = \hat{1}$

$f(\hat{3}) = \hat{5}$ izom de grupuri

$f(\hat{5}) = \hat{7}$

$f(\hat{7}) = \hat{11}$

Temă

__Exe.__ aflați celelalte 5 izomorfisme

$\square$

$U_n = \{ z \in \mathbb{C}^* \mid z^n = 1 \}$

$(U_n, \cdot) \to$ grup abelian cu n elemente

$U_4 = \{ \pm 1, \pm i \}$

$\circ$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	
$-i$	$-i$	1	i	-1

$\operatorname{ord} 1 = 1$

$\operatorname{ord} i = 4$

$\operatorname{ord} -1 = 2$

$\operatorname{ord} -i = 4$

Din cele 2 tabele (în U_4 avem el. de ordin 4 și în $U(\mathbb{Z}_8, \cdot)$ nu avem elem. de ordin 4)

Remarcă $\Longrightarrow$ Grupurile $U(\mathbb{Z}_8, \cdot)$ nu e izomorf cu $(U_4, \cdot)$

! Citiți:

- grup factor
- Th. fund. de izomorfism
- ordinul unui element