23.03.2016.

ALGEBRĂ

CURS 5

K corp comutativ. , $(G, \cdot)$ subgrup finit. Al lui $(K^*, \cdot)$. Atunci G este ciclic

$$G = \langle \alpha \rangle = \{ \alpha^n \mid n \in \mathbb{N} \}$$

Consecință : p prim $\Rightarrow (\mathbb{Z}_p^*, \cdot)$ ciclic

Definiție $(G, \cdot)$ grup finit , e - element neutru al lui G , $g \in G$

$$\text{ord } g = \min \{ k \in \mathbb{N}^* \mid g^k = e \}$$

$(\mathbb{Z}_{100}, +)$

ord $\hat{15} = 20$.

$k \cdot \hat{15} = \hat{0}$ cel. mai mic $k \in \mathbb{N}^*$

ord $\hat{3}$ în $U(\mathbb{Z}_{100}, \cdot)$

$3^4 = 81 = 1 + 80.$

$3^{20} = (1+80)^5 \overset{100}{\equiv} 1$

Proprietăți :

1) $g^{\text{ord } g} = e$.
2) $n \in \mathbb{Z}$, $g^n = e \Rightarrow \text{ord } g \mid n$
3) $\text{ord } g \mid |G|$
4) $\text{ord } g^k = \dfrac{\text{ord } g}{(\text{ord } g, k)}$
5) G comutativ.

$$\left.\begin{array}{l} \text{ord } g_1 = m \\ \text{ord } g_2 = n \\ (m, n) = 1 \end{array}\right\} \Rightarrow \text{ord } g_1 g_2 = m \cdot n$$

Lemă

$(G,\cdot)$ grup comutativ finit $\quad m = \max\{ \operatorname{ord} g \mid g \in G \}$

Atunci $\operatorname{ord} g \mid m \ \forall g \in G$ Consecință: $g^m = e \ \forall g \in G$

Dem: $\exists g_0 \in G$ a.î. $\operatorname{ord} g_0 = m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$p_1 < p_2 < \ldots < p_r < p_{r+1} < \ldots < p_s$.

p_j prim, $\alpha_j \in \mathbb{N}^*$ $\forall j = \overline{1,r}$

$g \in G$, $\operatorname{ord} g = p_1^{\beta_1} \cdots p_r^{\beta_r} \cdot p_{r+1}^{\beta_{r+1}} \cdots p_s^{\beta_s}$.

Presup că $\exists p$ prim, $p \mid \operatorname{ord} g$ $p \neq p_j$ $\forall j = \overline{1,r}$ $\quad p = p_{r+1}$

$g_1 = g^{p_1^{\beta_1} \cdots p_r^{\beta_r} \cdot p_{r+2}^{\beta_{r+2}} \cdots p_s^{\beta_s}}$

$\operatorname{ord} g_1 \overset{4)}{=} \dfrac{\operatorname{ord} g}{(\operatorname{ord} g, p_1^{\beta_1} \cdots p_r^{\beta_r} p_{r+2}^{\beta_{r+2}} \cdots p_s^{\beta_s})} = \dfrac{p_1^{\beta_1} \cdots p_s^{\beta_s} \cdot p_{r+1}^{\beta_{r+1}}}{\cdots \; p_{r+1}^{\beta_{r+1}}}$

~~$\operatorname{ord} g_1 = p_{r+1}$~~

Prop:

$(\operatorname{ord} g_1, \operatorname{ord} g_0) = 1$.

$\operatorname{ord} g_1 = p_{r+1}^{\beta_{r+1}}$

$\operatorname{ord} g_0 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

5) $\operatorname{ord} g_0 g_1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot p_{r+1}^{\beta_{r+1}} > p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \operatorname{ord} g_0$

$\text{ord } g = p_1^{\beta_1} \cdots p_r^{\beta_r}$ Trb. să arăt că $\beta_j \leq \alpha_j$ $\forall j = \overline{1,r}$

Presupunem $\beta_1 > \alpha_1$

$g_1 = g_0^{p_1^{\alpha_1}}$ $\quad \text{ord } g_1 \overset{1)}{=} \dfrac{\text{ord } g_0}{(\text{ord } g_0, p_1^{\alpha_1})} = \dfrac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}}{p_1^{\alpha_1}}$

$= p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \text{ord } g_1$

$\text{ord } g_2 \overset{4)}{=} p_1^{\beta_1}$

$(\text{ord } g_1, \text{ord } g_2) = 1$

$\overset{3)}{\Rightarrow} \text{ord } g_1 g_2 = \text{ord } g_1 \cdot \text{ord } g_2 = p_1^{\beta_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} > p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \text{ord } g_0$

↳ presup.

contradicție cu maximalitatea lui g_0

Dem: $m = \max \{ \text{ord } g \mid g \in G \}$ $\quad m = \text{ord } g_0 \mid |G|$

$\Rightarrow g^m = 1 \ \forall g \in G$ $\quad m \leq |G|$

$f(x) = X^m - 1 \in \mathbb{K}[X]$

$f(g) = 0 \ \forall g \in G$ $\quad \text{grad } f = m \geq$ nr. rădăcini $f \geq |G|$

$(\mathbb{Z}_{89}^*, \cdot)$ ciclic ord e = 1.

Gasiti $\hat{x}$ a.i. $\langle \hat{x} \rangle = \mathbb{Z}_{89}^*$

$d = \text{ord } \hat{2} \mid |\mathbb{Z}_{89}^*| = 88$

$d \in \{1, 2, 4, 8, 11, 22, 44, 88\}$

$\hat{2}^{44}$

$\hat{2}^{10} = \hat{45}$

$\hat{2}^{20} = \hat{2025} = -\hat{22}$

$\hat{2}^{40} = \hat{484}$

$\hat{2}^{41} = \hat{-78} = -\hat{11}$

$\hat{2}^{44} = -\hat{88} = \hat{1}$

$\text{ord } \hat{2} \leq 44$

$\hat{3}^{5} = 243 \overset{89}{\equiv} -24$

$\hat{3}^{10} = 576 = 42.$

$3^{20} = -\hat{16}$

$3^{44} \equiv 88 \equiv -1 (89)$

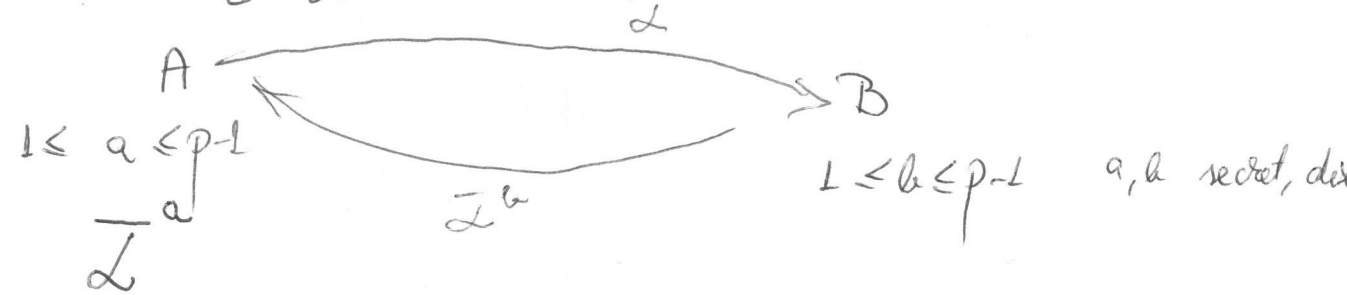
$3^{8} \equiv 64 = 11 \, 89$

$\langle \hat{3} \rangle$ - generator.

1975 Diffie-Hellman

Schimbul public de chei.

Public: $\begin{cases} p \text{ prim mare} & \langle \hat{\alpha} \rangle = \mathbb{Z}_p^* \\ \alpha \end{cases}$



a, b secret, discret

α este

$\alpha^{(x)} \equiv u \pmod p$

Prb. log discret

$x = \log_\alpha u$ cheia : $\overline{\alpha^{ab}}$

B:

test

săpt viitoare 2-4 (poate 1:40)

- avem voie cu notițe / fără telefoane / cale.
- 4-5 probleme

Public 2027. , $\overline{2}$ $\langle \overline{2} \rangle = \mathbb{Z}_{2027}^*$

am interceptat 95

$2^x \equiv 95 (2027)$

$x = ?$ $1 \leq x < 2026.$