08.03.2018

CURS 3

TEOREMĂ: $f \in K[X]$, grad $f \geq 1$, K corp com.

Atunci: $\boxed{\text{nr. rădăcini } f \leq \text{grad } f}$

CONSECINȚĂ: $\left[\begin{array}{l} p \text{ prim} \\ (\mathbb{Z}_p^*, \cdot) \text{ ciclic} \end{array}\right.$ $\left((\exists)\, a \in \{1, 2, \dots, p-1\} \text{ a.î. } \operatorname{ord} \bar{a} = p-1 \text{ în } (\mathbb{Z}_p^*, \cdot) \right)$

$$\left.\begin{array}{l} (G, \cdot) \leq (K^*, \cdot) \\ K \text{ corp comutativ} \\ G \text{ finit} \end{array}\right\} \Rightarrow G \text{ ciclic } \left((\exists)\, g \in G \text{ a.î. } G = \{ g^k \mid k \in \mathbb{N} \} \right)$$

Dacă aleg $K = \mathbb{Z}_p$ (p prim) $\Rightarrow (\mathbb{Z}_p^*, \cdot)$ ciclic

---

$p = 13$ $\quad (\mathbb{Z}_{13}^*, \cdot)$

$\mathbb{Z}_{13}^* = \{ \bar{2}^k \mid k \in \mathbb{N} \}$

$\bar{2}^1 = \bar{2}$ $\quad \bar{2}^5 = \bar{6}$

$\bar{2}^2 = \bar{4}$ $\quad \bar{2}^6 = \overline{12}$

$\bar{2}^3 = \bar{8}$ $\quad \bar{2}^7 = \overline{11}$

$\bar{2}^4 = \bar{3}$ $\quad \bar{2}^8 =$

$\bar{2}^9 = \bar{5}$

$\bar{2}^{10} = \overline{10}$

$\bar{2}^{11} =$

$\bar{2}^{12} =$

CRIPTARE CU CHEIE PUBLICĂ:

p prim mare public $\quad r \equiv a^x \pmod{p}$, $\; r \in \{1, \dots, p-1\}$

a public

$a \in \{1, 2, \dots, p-1\}$

$\operatorname{ord} \bar{a} = p-1$

în $(\mathbb{Z}_p^*, \cdot)$

$$\begin{tikzcd} \text{secret } x \; A \arrow[r, bend left, "r"] & B \; y \text{ secret} \arrow[l, bend left, "s"] \end{tikzcd}$$

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

$s \in \{1, \dots, p-1\}$

A: $s^x \underset{p}{\equiv} (a^y)^x = a^{x \cdot y}$

B: $r^y \underset{p}{\equiv} (a^x)^y = a^{xy}$

ÎDEE DE DEMONSTRAȚIE:

$m = \max\{\text{ord } g \mid g \in G\}$

Vă arăta că $\boxed{\text{ord } g \mid m,\ (\forall)\, g \in G}$

presupun adev.

$$\left.\begin{array}{l} |G| = n \\ m = \text{ord } h \\ h \in G \end{array}\right\} \Rightarrow m \mid n \Rightarrow m \leq n$$

$(G, \cdot) \leq (K^*, \cdot)$ $f(x) = x^m - 1 \in K[x]$

1 el. neutru al acestui grup.

$g \in G \Rightarrow \text{ord } g \mid m$

$g^m = (g^{\text{ord } g})^{\frac{m}{\text{ord } g}} = 1^{\frac{m}{\text{ord } g}} = 1 \Rightarrow f(g) = 0 \Rightarrow$

$\Rightarrow g$ răd. pt. f

$\boxed{\underset{m}{\underset{\parallel}{\text{grad } f}} \geq \text{nr. răd. } f \geq |G| = n} \Rightarrow$

T. curs. precedent

$\Rightarrow m = n$

$\text{ord } h = n$

$\{1, h, h^2, h^3, \ldots\} \subseteq G$ (subgrupul [illegible] a lui G)

$|\{1, h, h^2, \dots\}| = n = |G|$

<u>PROP</u>: $(G, \cdot)$ grup. comutativ finit

$m = \max\{\text{ord } g \mid g \in G\}$

Voi arăta că $\text{ord } g \mid m$ $(\forall)\, g \in G$

<u>Remember</u>: 1) $\text{ord } g^k = \dfrac{\text{ord } g}{(\text{ord } g, k)}$

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

$\Rightarrow \text{ord } g_1 \cdot g_2 = \text{ord } g_1 \cdot \text{ord } g_2$

$m = \text{ord } h = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$

$n = \text{ord } g = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_r^{b_r}$

p_i prim, $(\forall)\, i = \overline{1, r}$

$p_i \neq p_j$ pt. $i \neq j$

$a_i\, b_j \in \mathbb{N}$

Trb. să arat că $a_i \geq b_i$, $(\forall)\, i = \overline{1, r}$

\# Arăt că $a_1 \geq b_1$

$14 = 2^1 \cdot 5^0 \cdot 7^1$

$20 = 2^2 \cdot 5^1 \cdot 7^0$

Pp. că $a_1 < b_1$

$\text{ord } g^{p_2^{b_2} \dots p_r^{b_r}} = \dfrac{\text{ord } g}{(\text{ord } g, p_2^{b_2} p_3^{b_3} \dots p_r^{b_r})} = p_1^{b_1}$

$\text{ord } g = p_1^{b_1} p_2^{b_2} \cdot \dots \cdot p_r^{b_r}$

$$\operatorname{ord} h^{p_1^{a_1}} = \frac{\operatorname{ord} h}{(\operatorname{ord} h, p_1^{a_1})} = \frac{\operatorname{ord} h}{p_1^{a_1}} = p_2^{a_2} \cdots p_r^{a_r}$$

$$\left(\operatorname{ord}\left(g^{p_2^{b_2} \cdots p_r^{b_r}}\right), \operatorname{ord} h^{p_1^{a_1}}\right) = 1$$

$$\overset{2)}{\Longrightarrow} \operatorname{ord}\left(g^{p_2^{b_2} \cdots p_r^{b_r}} \cdot h^{p_1^{a_1}}\right) = p_1^{b_1} \cdot p_2^{a_2} \cdots p_r^{a_r} > \underbrace{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}}_{m}$$

Asta contrazice maximalitatea lui m.

Q.E.D.

$p = 23$

$\mathbb{Z}_{/23}^{*} = \{\bar{1}, \bar{g}, \bar{g}^2, \dots\}$

$g \in \{1, 2, \dots, 22\}$ $\quad \operatorname{ord} \bar{g} = 22$

$2^{11} = 2048 = 1 \ (\mathbb{Z}_{/23})$ $\quad \operatorname{ord} \bar{2} = 11$

$\operatorname{ord} \overline{22} = 2$

$(\operatorname{ord} \bar{2}, \operatorname{ord} \overline{22}) = (11, 2) = 1$

$\Rightarrow \operatorname{ord} \bar{2} \cdot \overline{22} = 2 \cdot 11 = 22$

$(k, 22) = 1$

$k \in \{0, 1, \dots, 21\}$

$k \in \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$

probabilitate $= \frac{10}{22} = \frac{5}{11}$