08.03.2018

CURS 3

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

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

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

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

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

---

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

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

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

$\hat{2}^2 = 4$ $\quad \hat{2}^6 = \hat{12}$

$\hat{2}^3 = \hat{8}$ $\quad \hat{2}^4 = \hat{11}$

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

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

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

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

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

CRIPTARE CU CHEIE PUBLICĂ:

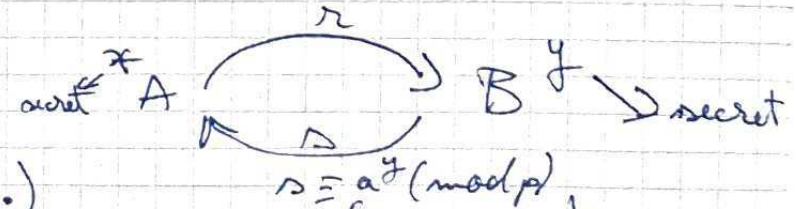
p prim mare public $r \equiv a^x \pmod p$, $r \in \{1,\dots,p-1\}$

a public

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

$\text{ord}\, \hat{a} = p-1$

$\hat{a} \in (\mathbb{Z}_p^*, \cdot)$



A: $a^{x} \underset{P}{=} (a^{y})^{x} = a^{x \cdot y}$

B: $a^{y} \underset{P}{=} (a^{x})^{y} = a^{x*y}$

IDEE DE DEMONSTRATIE:

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

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

presupun altfel.

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

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

↓ el. neutru al acestui grup.

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

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

$\Rightarrow g$ rădăc. pt. f

$\boxed{\operatorname{grad} f \geq \text{nr. rădăc. } f \geq |G| = n} \Rightarrow$

$\operatorname{grad} f = m$

↓ T. curs. precedent

$\Rightarrow m = n$

$\operatorname{ord} h = n$

$\{1, h, h^2, h^3, \ldots\} \subseteq G$ (subgrupul generat de h în G)

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

PROP: $(G, \cdot)$ grup. comutativ finit

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

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

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

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

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

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

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

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 arăt 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 $a_1 < b_1$

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

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

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

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

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

Asta contrazice maximalitatea lui m.

Q.E.D.

$p = 23$

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

$g \in \{1, 2, \ldots, 22\}$ $\quad \text{ord } \bar{g} = 22$

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

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

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

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

$(k, 22) = 1$

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

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

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

TEOREMA WILSON: p - prim $\Rightarrow p \mid (p-1)! + 1$

Altă dem:

(care folosește polinoame)

$f(X) = X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$

Sâpt. prec: $f \in K[X]$

K corp comutativ

$\text{grad } f \geq 1$

$x_0 \in K$

x_0 rădăcină pt. $f \Leftrightarrow f(X) = g(X) \cdot (X - x_0)$

p prim
$a \in \mathbb{Z}$
$p \nmid a$
$\Rightarrow a^{p-1} \equiv 1 \pmod p$

(MICA TEOREMĂ A LUI FERMAT)

$f(\hat{1}) = 0 \quad f(\hat{j}) = 0, \ (\forall) j \in \{1, 2, \dots, p-1\}$

$X^{p-1} - \hat{1} = f(X) = (X - \hat{1})(X - \hat{2}) \cdots (X - \widehat{p-1})$

$\hat{1}, \hat{2}, \dots, \widehat{p-1}$ rădăcinile lui f

$\text{grad } f = p - 1$

$g = \hat{2}\hat{1}$

coeficientul lui X^0 este $-\hat{1} = \widehat{(p-1)!} \cdot \widehat{(-1)^{p-1}}$

$p \mid (p-1)! + 1$

Dacă $p = 2$, $\mathbb{Z}_2$

$\widehat{(-1)}^{2-1} = -\hat{1} = \hat{1}$

$p \mid (p-1)! \cdot \left(\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1}\right)$

Prop: p prim, $p \geq 5$

$\Rightarrow p \mid (p-1)! \cdot \sum \overline{i \cdot j}$

$1 \leq i < j \leq p-1$

FORMULELE LUI VIÈTE

$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X]$

$x_1, x_2, \dots, x_n \in K$ sunt rădăcinile lui f

[Contabilizează multiplicitățile]

$X \cdot f(X) = (X - x_1)^{\alpha} \cdot g(X)$

$g(x_1) \neq 0$

Pe x_1 îl scrie de α ori

$x_1 + x_2 + \dots + x_n =$

coeficientul lui X^{n-1}: este $a_{n-1} = a_n(-x_1 - x_2 \dots - x_n)$

$x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n = \frac{a_{n-2}}{a_n}$

$x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_{n-2} x_{n-1} x_n = \frac{-a_{n-3}}{a_n}$

$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k} = \frac{(-1)^k a_{n-k}}{a_n}$

$\Rightarrow$ Există un corp comutativ L, $K \subseteq L$ a.î. f are exact n rădăcini în L

$2X + 1 = 0$ $\quad \mathbb{Z}_2$, $\mathbb{Q}$

$\mathbb{Z}_2 \subsetneq \mathbb{Q}$

$x^2 + 1 = 0$ $\quad \mathbb{R}$

$(x-i)(x+i) = 0$ $\quad \mathbb{C}$

$a_n X^n + \dots + a_1 X + a_0 = 0 \quad a_j \in \mathbb{C}$

$(\forall)\ j = \overline{0,n}$

$\Rightarrow (\exists)\ x_1, x_2, \dots x_n \in \mathbb{C} \quad a_n \neq 0$

rădăcini ale ec.

$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$

$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$

$i^2 = j^2 = k^2 = -1$

$i \cdot j = k$; $j \cdot k = i$; $k \cdot i = j$

$j \cdot i = -k$; $k \cdot j = -i$; $i \cdot k = -j$

R ~~$\neq$~~ INEL COMUTATIV

$I \trianglelefteq R$, I s.n. ideal

dacă: 1) $(I, +)$ grup

2) $(\forall)\ r \in R$, $(\forall)\ i \in I$

$\Rightarrow r \cdot i \in I$

Prop: $I \trianglelefteq K[X]$

$\Rightarrow \exists\, f \in K[X]$ a.î. $f \cdot K[X] = I$

$= \{f \cdot g \mid g \in K[X]\}$

Dem: Dacă $I = \{0\}$ alegem $f = 0$

Dacă $\{0\} \subsetneq I$ alegem $f \in I$, $f \neq 0$

a.î. $\operatorname{grad} f = \min$

$= \min \{\operatorname{grad} g \mid g \in I \setminus \{0\}\}$

$f \cdot K[X] = I$

$\subseteq$ " banal

$\supseteq$ " Alegem $h \in I \overset{\text{T. împ. cu rest}}{\Rightarrow}$ $h = f \cdot g + r$

$g, r \in K[X]$

$\operatorname{grad} r < \operatorname{grad} f$

$r = h - fg \in I$

$f \in I, g \in K[X] \Rightarrow fg \in I$

$\Rightarrow r = 0$ conform alegerii lui f