23.03.2016.

ALGEBRĂ
SEMINAR 3

Criterii ireductibilitate

$f \in \mathbb{K}[X]$ grad $f = n$

f s.n. ireductibil dacă $\nexists\ g, h \in \mathbb{K}[X]$ a.î.

$f = g \cdot h$ și $\begin{cases} \text{grad } g < n \\ \text{grad } h < n \end{cases}$

1) $f \in \mathbb{Z}[X]$; $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$.

p prim, $p \nmid a_n$, $\overline{f}$ - notație

$\overline{f} = \overline{a_n} x^n + \overline{a_{n-1}} \cdot x^{n-1} + \dots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_p[X]$.

Presupunem $\overline{f}$ ireductibil în $\mathbb{Z}_p[X] \Rightarrow f$ ired în $\mathbb{Q}[X]$

$\{ g \in \mathbb{Z}_p[X], \text{grad } g \leq n \}$ finită $\Rightarrow \exists\ p^{n+1}$ obiecte.

ex: $X^4 + 2014X^3 + 7X^2 + 40X + 1$

$p = 2$ $\quad X^4 + X^2 + \hat{1} \in \mathbb{Z}_2[X]$, nu este ireductibil.

$= (X^2 + X + \hat{1})^2$

$p = 3$ $\quad \overline{f}(X) = X^4 + X^3 + X^2 + X + \hat{1}$ în $\mathbb{Z}_3[X]$

$\overline{f}(\hat{2}) = 2^4 + 2^3 + 2^2 + 2 + 1 = 31 = \hat{1}$

$\overline{f}(\hat{1}) = \hat{5} = \hat{2}$.

$\overline{f}(\hat{0}) = \hat{1}$

nu are zero, dacă ar fi pol. de grad 3 - nu de grad 1.

$x^4+x^3+x^2+x+\bar{1} = (x^2+ax+b)(x^2+cx+d)$

$\mathbb{Z}_3 = \{0,1,2\}$.

$\bar{1} = a+c$

în $\mathbb{Z}_3[x]$ $\quad \bar{1} = d+b+ac$

$\bar{1} = ad+bc$

$\boxed{\bar{1} = bd}$

Caz I: $b = \bar{1} \Rightarrow d = \bar{1}$

$a+c = \bar{1}$ $\qquad a\cdot c = \bar{1}\cdot\bar{2} = 2.$

$\bar{1} = \bar{1}+\bar{1}+ac \Rightarrow ac = -\bar{1} = 2.$

$a+c = \bar{0}$

$\bar{1}+\bar{2} = \bar{3} = \bar{0}$ dar $a+c = \bar{1}$ fals.

Caz II

$b = \bar{2} \qquad d = \bar{2}$

$\bar{2}a + \bar{2}c = \bar{1}\cdot\bar{2} \Rightarrow a+c = \bar{2}$ fals.

$\Rightarrow$ scrierea ca $(x^2+ax+b)(x^2+cx+d)$ nu are sol.

$\Rightarrow x^4+x^3+x^2+x+1$ ireductibil

$\underline{1}\,x^4 + \underline{2014}\,x^3 + \underline{7}x^2 + \underline{40}x + \underline{1}$ ired în $\mathbb{Q}[x]$

$a_4 \equiv a_3 \equiv a_2 \equiv a_1 \equiv a_0 \equiv 1 \,(3)$

Reciproca

! f ired în $\mathbb{Q}[x] \Rightarrow \exists\, p$ prim a.î. f ired (NU e adev)

contrad.: x^4+1 ired în $\mathbb{Q}[x]$.

$x^4+\bar{1}$ nu e ired în $\mathbb{Z}_p[x]$ $\forall\, p$ prim

$p=2 \Rightarrow x^4+\bar{1}=(x+\bar{1})^4$

p prim $\quad p=4k+1$

$\boxed{\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1\,(p)}$ $\quad a\in\mathbb{Z}\quad a^2\equiv -1\,(p)$

$1\equiv -a^2\,(p)$

$\mathbb{Z}_p[x] \ni x^4+\bar{1}=x^4-\bar{a}^2$

$=(x^2-\bar{a})(x^2+\bar{a})$

La curs: p prim $\Rightarrow (\mathbb{Z}_p^*,\cdot)$ ciclic ($\exists\,\hat{a}\in\mathbb{Z}_p$ a.î. $\{\bar{1},\hat{a},\hat{a}^2,\dots\}=\mathbb{Z}_p^*$

$\boxed{\mathbb{Z}_p^*=<\hat{a}>}$ - notație

$p=4k+3$

$\mathbb{R}[x]$; $x^4+1=(x^2+1)^2-2x=(x^2+1)^2-(\sqrt{2}x)^2$

$=(x^2+1+\sqrt{2}x)(x^2+1-\sqrt{2}x)$

1) Raționamentul de sus funcționează dacă $\boxed{\bar{2}=\bar{a}^2}$ în $\mathbb{Z}_p$

$\Rightarrow x^4+\bar{1}=(x^2+\bar{1})^2-2x^2=(x^2+\bar{1})^2-\bar{a}^2x^2=(x^2+\bar{1}+\bar{a}x)(x^2+\bar{1}-\bar{a}x)$

$\mathbb{Z}_7 \quad \bar{3}^2=\bar{2}$

$\mathbb{Z}_{23} \quad \bar{5}^2=\bar{2}$

2) $\boxed{\bar{2}=-\bar{a}^2}$ în $\mathbb{Z}_p \quad x^4+\bar{1}=(x^2-\bar{1})^2+\bar{2}x^2=(x^2-\bar{1})^2-\bar{a}^2x^2=$

$=(x^2-\bar{1}-\bar{a}x)(x^2-\bar{1}+\bar{a}x)$ ✓

$\mathbb{Z}_3 : \bar{2}=-\bar{1}^2$

$\mathbb{Z}_{11} : \bar{2}=-\bar{3}^2$

Caz n prost

$\bar{2} \neq \bar{a}^2 \quad \forall \bar{a} \in \mathbb{Z}_p$.

$-\bar{2} \neq \bar{b}^2 \quad \forall \bar{b} \in \mathbb{Z}_p$

Demonstrație: $p \neq 2$. $\bar{2} \in \mathbb{Z}_p^*$, $-\bar{2} \in \mathbb{Z}_p^*$

$\bar{2} = \bar{\alpha}^j \Rightarrow j$ impar

$-\bar{2} = \bar{\alpha}^k \Rightarrow k$ impar

$-\bar{2}^2 = \bar{\alpha}^{j+k} = \bar{\alpha}^{2u}$

$\bar{\alpha}^{p-1} = \bar{1}$ (M. th. Ferm)

$\bar{2}^{p-1} = \bar{1}$

$-\bar{2}^{*2} = \bar{\alpha}^{2u} \Rightarrow (-\bar{2})^{\frac{p-1}{2}} = (\bar{\alpha}^{2u})^{\frac{p-1}{2}} = 1.$

$(-1)^{\frac{p-1}{2}} \cdot 2^{p-1} = (-1)^{\frac{p-1}{2}} = -\bar{1}$ $\quad \bar{1} = -\bar{1}$ fals. $\Rightarrow p/2 \Rightarrow p = 2$

p era de forma $4k+3 \Rightarrow \frac{p-1}{2} = 2k+1.$

$X^4 + \bar{1} \in \mathbb{Z}_p[X]$ nu e ired $\forall$ p prim

---

Criterii ireductibile (Eisenstein)

2) $f(X) = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$

p prim, $p \nmid a_n$, $p \mid a_j \quad \forall j = \overline{0, n-1}$, $p^2 \nmid a_0$

Atunci f este ireductibil în $\mathbb{Q}[X]$

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

$X^n + 3$ ired

ex: $X^n + 3$ ired. (Eisenstein $p = 3$)

$p = 3$

$1, 0, 0, \dots, 0, (3)$

ex: p prim.

$\Rightarrow f(x) = X^{p-1} + X^{p-2} + \dots + X + 1$ ired in $\mathbb{Q}[X]$.

$X^{p-1} + X^{p-2} + \dots + X + 1 = \dfrac{X^p - 1}{X - 1} \quad X \neq 1.$

$g(X) = f(X+1)$ $\qquad \dfrac{(X+1)^p - 1}{(X+1) - 1}$

$= \dfrac{X^p + C_p^1 X^{p-1} + C_p^2 X^{p-2} + \dots + C_p^{p-1} X}{X}$

$\rightarrow = X^{p-1} + C_p^1 X^{p-2} + \dots + C_p^2 X^{p-3} + \dots + C_p^{p-2} X + C_p^{p-1}$

$\Rightarrow p \mid C_p^j \quad \forall\, j = \overline{1, p-1}$

$C_p^j = \dfrac{p!}{(p-j)! \cdot j!} = \dfrac{(p-j+1)(p-j+2)\cdots p}{j!} \in \mathbb{N}$

$\rightarrow$ multiplu de p.

$p^2 \nmid C_p^{p-1} = p \Rightarrow g$ ired $\Rightarrow f$ ired.

Găsiți $\hat{\alpha}$ a.î.

$\langle \hat{\alpha} \rangle = (\mathbb{Z}_{97}^*, \cdot)$

$(G, \cdot)$ grup finit

e - elem neutru

$g \in G$

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

1) $g^{\text{ord } g} = e$.

2) $m \in \mathbb{Z}$, $g^m = e \Rightarrow \text{ord } g \mid m$

3) $\text{ord } g \mid |G|$
↳ card m. G.

---

ord $\bar{2} = 96$ ($\mathbb{Z}_{97}^*$ are 96 elem față de $\bar{0}$)

$d = \text{ord } \bar{2} \mid |\mathbb{Z}_{97}^*| = 96$ $\quad d = \{1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 96\}$

$\bar{2}^{48} = \bar{1}$

$\bar{2}^{10} = 1024 \mid 97$
97
$= 54$ $\quad 1$.

$\bar{2}^{10} = \overline{54}$

$\bar{2}^{20} = \overline{54}^2 = \bar{6}$

$\bar{2}^{40} = \bar{36}$

$\bar{2}^{38} = \bar{9}$

$\bar{2}^{48} = \bar{2}^{10} \cdot \bar{2}^{38} = \overline{54} \cdot \bar{9} = \overline{486} = \bar{1}$

$54 \cdot$
54
216
270
$2916 \mid 97$
291
$= = = 6$

$\bar{3}^{48} = \bar{1}$.

~~$1 \equiv (3^4)^{12}$~~

2 nu e lui
3 nu e lui.
4 nu e lui.

5^{48}

$5^3 = 125 \overset{97}{\equiv} 28$.

$5^6 \equiv 784$

$\bar{5}^{48} \overset{97}{\equiv} (2^3)^8 = 2^{24}$.

$\bar{5}^{48} = -\bar{1}$

$d \in \{1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 96\}$

$\langle \bar{5} \rangle = (\mathbb{Z}_{97}^*, \cdot)$ $\quad 96 = \text{ord } \bar{5}$

Câți $\bar{\alpha} \in \mathbb{Z}_{97}^*$ cu proprietatea că $\langle \bar{\alpha} \rangle = (\mathbb{Z}_{97}^*, \cdot)$

generatori $\begin{cases} \bar{5}^j \\ (j, 96) = 1 \\ 1 \le j \le 96 \end{cases}$

$$\text{ord } g^k = \frac{\text{ord } g}{(k, \text{ord } g)}$$

$$\text{ord } \bar{5}^j = \frac{\text{ord } \bar{5}}{(\text{ord } \bar{5}, j)} = \frac{96}{(96, j)} = 96.$$

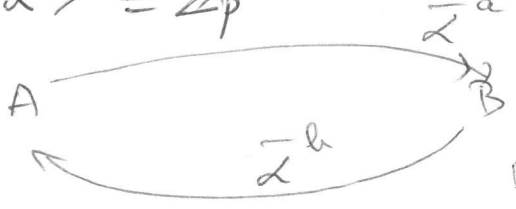
probabil $\frac{\varphi(96)}{96} = \frac{96\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)}{96} = \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$.

---

p prim mare.

p, α publice

$\langle \bar{\alpha} \rangle = \mathbb{Z}_p^*$



a secret $\quad$ b secret.

α^a

Logaritm discret.

$\overline{m} = \overline{\alpha}^{\overline{a}}$

$a = \log_\alpha m$

$(\overline{\alpha}^{b})^{a}$ cheie comună $(\overline{\alpha}^{a})^{b}$.

$(\overline{\alpha}^{a})^{b} = \overline{\alpha}^{ab}$

ex: $\begin{cases} \overline{5}^{a} = \overline{11} \\ \mathbb{Z}_{97} \end{cases}$ Baby Step / Gigant Step.