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

Altă dem:

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

Săpt. ~~p~~ prec: $f \in K[X]$

K corp comutativ

$\operatorname{grad} f \geq 1$

$x_0 \in K$

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

$$\left.\begin{array}{l} p \text{ prim} \\ a \in \mathbb{Z} \\ p \nmid a \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

(MICA TEOREMĂ A LUI FERMAT)

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

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

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

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

$g = \overline{21}$

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

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

$\boxed{\begin{array}{c} \text{Dacă } p = 2, \mathbb{Z}_2 \\ \overline{(-1)}^{2-1} = \overline{-1} = \hat{1} \end{array}}$

Created with ScanWritr. To remove this watermark please use the upgrade options.

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

<u>Prop:</u> p prim, $p \geq 5$

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

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 f

[Contabilizez multiplicitățile]

$$X \cdot f(X) = (X - x_1)^a \cdot g(X)$$

$$g(x_1) \neq 0$$

Pe x_1 îl scriu de a ori

$x_1 + x_2 + \dots + x_n =$

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

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

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

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

Created with ScanWritr. To remove this watermark please use the upgrade options.

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

$2X + 1 = 0$ $\quad \left.\begin{matrix} \mathbb{Z}_1 \\ \mathbb{Q} \end{matrix}\right]$

$\mathbb{Z}_1 \subsetneq \mathbb{Q}$

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

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

$a_n X^n + \dots + a_1 X + a_0 = 0$ $\quad a_j \in \mathbb{C}$
$(\forall)\, j = \overline{0,n}$

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

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

dacă: 1) $(I, +)$ grup
2) $(\forall)\, r \in R$, $(\forall)\, i \in I$
$\Rightarrow r \cdot i \in I$

Created with ScanWritr. To remove this watermark please use the upgrade options.

Prop: $I \trianglelefteq K[X]$

$\Rightarrow (\exists)\ f \in K[X]$ a.î. $f \cdot K[X] = \{f \cdot g \mid g \in K[X]\}$

Dem: Dacă $I = \{0\}$ aleg $f = 0$

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

a.î. grad f = ~~min~~ $= \min\{\text{grad}\, g \mid g \in I \setminus \{0\}\}$

$f K[X] = I$

„$\subseteq$" banal

„$\supseteq$" Aleg $h \in I \xRightarrow[\text{cu rest}]{\text{T. împ.}} h = f \cdot g + r$

$g, r \in K[X]$

grad $r <$ grad f

$r = h - fg \in I$

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

$\Rightarrow r = 0$ conform alegerii lui f

Created with ScanWritr. To remove this watermark please use the upgrade options.