16.03.2016.

ALGEBRĂ
CURS 4.

Polinoame

Teorema împărțirii cu rest

K - corp comutativ

$f, g \in K[x]$ $g \neq 0$ Atunci $\exists$ $q, r \in K[x]$ a.î.

$f = g \cdot q + r$ și gradul $r <$ grad $\cancel{g}$

$K[x]$ $\qquad$ $\mathbb{Z}$

f polinom ired în $K[x]$ $\xleftrightarrow{\text{analogie.}}$ p prim în $\mathbb{N}$

$\begin{cases} f \neq g \cdot h \ ; \ \text{grad } g < \text{grad } f \\ \qquad\qquad\quad \text{grad } h < \text{grad } f \end{cases}$

T. împ. cu rest (în $\mathbb{Z}$)

$a, b \in \mathbb{Z}$, $b \neq 0 \Rightarrow \exists$ $q, r \in \mathbb{Z}$ a.î. $a = bq + r$.
$0 \leq r < |b|$

Dem:

- inducție după grad f

verificare: grad $f <$ grad g, Alegem pe post de $q = 0$, $r = f$.

Presupun enunțul adevărat pentru $\forall f \in K[x]$, grad $f \leq n-1$.

Vrem să dem pt $\text{grad } f = n \geq \text{grad } g$

$f: f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$.

$a_j \in K$
$a_n \neq 0$

$g(x) = b_m x^m + \dots + b_1 x + b_0$ $\qquad b_j \in K$
$\forall j = \overline{0, m}$

$\boxed{n \geq m}$ $\qquad b_m \neq 0$.

$\text{grad}\Big(\underbrace{f(x) - g(x) \cdot \frac{a_n}{b_m} x^{n-m}}_{= f_1}\Big) \leq n-1$

<u>Obs</u>: K - corp $\quad x \in K \setminus \{0\}$

$\frac{1}{x}$ = inversul față de „$\cdot$" al lui x.

Aplicăm ipoteza de ind pt f_1 și g.

$f_1 = q_1 g + r \qquad \text{grad } r < \text{grad } g$.

$f(x) - g(x) \cdot \frac{a_n}{b_m} \cdot x^{n-m} = q_1 g + r$.

$$\boxed{f(x) = g(x)\left[q_1(x) + \frac{a_n}{b_m} x^{n-m}\right] + r(x)}$$

$\text{grad } r < \text{grad } g$

$\boxed{\begin{array}{l} g \neq 0. \\ \text{grad } g = 0. \end{array}}$ $\qquad g(x) = a \in K^* \setminus \{0\}$ - pol. constant.

$f = g \cdot q \qquad\qquad \text{grad } 0 \overset{\text{conv.}}{=} -\infty$

$q = \frac{f}{g}$

Consecințe

$$\begin{cases} g(x) = x - \alpha & \alpha \in K. \\ f \in K[x] \end{cases} \xrightarrow{Th. \hat{I}m R} \exists\, q \in K[x] \text{ a.î.}$$

grad $r < 1$

$$f(x) = (x-\alpha)\cdot q(x) + r \quad \boxed{r \in K}$$

$\boxed{\text{Obs}: \ \alpha \text{ răd pt } f \iff r = 0}$

$f \in K[x]$, grad $f = n$ $n \in \mathbb{N}^*$

$\Rightarrow$ nr răd. ale lui f este $\leq n$.

Presup. f are n rădăcini distincte în $K \Rightarrow$

$$\boxed{f(x) = a(x-a_1)(x-a_2)\ldots(x-a_n)}$$

Inducție după n $\quad n=1$.

$\Rightarrow f(x) = ax + b = a(x-a_1)$

$f(a_1) = 0.$

$a\, a_1 + b = 0.$

$b = -a a_1.$

$ax + b = ax - a\cancel{a_1} = a(x-a_1)$

Pp. adv. pt. polinoamele de grad $\leq n-1$ și dem pt grad $f = n$.

$\boxed{\text{grad } q_1 = n-1}$

$$f(a_1) = 0 \xrightarrow[\text{obs}]{\text{consec}} f(x) = (x-a_1)q(x)$$

$$0 = f(a_2) = (a_2 - a_1)\, q(a_2)$$

$\Rightarrow \cancel{a_2 - a_1 = 0}$ sau $\boxed{q(a_2) = 0}$ $\quad q(a_3) = \ldots = q(a_n) = 0.$

$a_2, a_3 \ldots a_n$ răd. dist. ale lui g.

ip. ind $f(x) = a(x-x_1) \ldots (x-x_n)$

$a_1, a_2 \ldots a_n$ răd dist ale lui f.

Form lui Viete

$$\begin{cases} f(x) = b_n x^n + b_{n-1} x^{n-1} \ldots + b_1 x + b_0 \in K[x] \quad b_n \neq 0. \\ a_1, a_2 \ldots a_n \text{ rădăcini dist. ale lui } f. \end{cases}$$

$$\Rightarrow \begin{cases} a_1 + a_2 + \ldots + a_n = -\dfrac{b_{n-1}}{b_n} \\ a_1 a_2 + a_1 a_3 + \ldots + a_{n-1} a_n = \dfrac{b_{n-2}}{b_n} \\ a_1 a_2 a_3 + \ldots \\ \vdots \\ a_1 a_2 \ldots a_n = (-1)^n \cdot \dfrac{b_0}{b} \end{cases}$$

$f(x) = b_n (x-a_1)(x-a_2) \ldots (x-a_n)$

coef. lui x^{n-1} este

$b_{n-1} = b_n(-a_n - a_{n-1} - \ldots - a_1)$

$b_0 = a_1 a_2 \ldots a_n \cdot (-1)^n \cdot b_n$

Consecință p. prim.

pol. $x^{p-1} - \bar{1} \in \mathbb{Z}_p[x]$

Rădăcinile lui f sunt $\bar{1}, \bar{2} \ldots \overline{p-1}$ (din Mica Th. a lui Fermat.)

sunt răd. dist.

p prim, $x \in \mathbb{Z}$, $p \nmid x$. $\Rightarrow x^{p-1} \equiv 1 (p)$

$\xRightarrow{\text{rez anterior}}$ $x^{p-1} - 1 = (x-\bar{1})(x-\bar{2}) \ldots (x-(\overline{p-1}))$

$-\bar{1} = (-1)^{p-2}\,\overline{(p-1)!}$

dacă $p=2$. $(\overline{-1})^2 = \bar{1}$

$(p-1)! \equiv -1 (p)$

$\boxed{\text{Dacă } p \text{ prim} \Rightarrow p \mid (p-1)! + 1 \quad \text{Th. Wilson}}$

$x^2 + \bar{1} \in \mathbb{Z}_p[x]$

p prim

1) $p = 4n+3 \Rightarrow f$ ireduct.

2) $p = 4n+1 \Rightarrow f$ are 2 răd în $\mathbb{Z}_p$.

<u>Dem pt 2</u>

$p = 4n+3$

înmulțesc congruențele

$$\begin{cases} 1 \equiv 1. \ (p) \\ 2 \equiv 2. \ (p) \\ \vdots \\ \frac{p-1}{2} \equiv \frac{p-1}{2} (p) \end{cases}$$

$\frac{p+1}{2} \equiv -\frac{p-1}{2} (p)$

$$\frac{p+3}{2} \equiv -\frac{p-3}{2} \ (p)$$

$$\frac{p+3}{2} \equiv -\frac{p-3}{2} \ (p)$$

$$\vdots$$

$$p-2 \equiv -2 \ (p)$$

$$p-1 \equiv -1 \ (p)$$

$$(p-1)! \overset{p}{\equiv} \left[\left(\frac{p-1}{2}\right)!\right]^2 \cdot \underbrace{(-1)^{p-1}}_{\text{face } 1} \qquad \frac{p-1}{2} = 2n.$$

Aplicam Wilson.

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \ (p)$$

$x^2+\hat{1}$ are că răd. pe $\pm\overline{\left(\frac{p-1}{2}\right)!}$

Dem (teoremă)

$$\left\{ x+y\cdot m \;\middle|\; \begin{matrix} x, y \in \mathbb{N} \\ 0 \le x, y < \sqrt{p} \end{matrix} \right\} \qquad m = \left(\frac{p-1}{2}\right)! \quad n^2 \equiv -1 (p)$$

avem $([\sqrt{p}]+1)^2$ alegeri de numere

$$y-1 < [y] \le y \qquad y = \sqrt{p}$$

$$[\sqrt{p}]+1 > \sqrt{p} \qquad \Rightarrow (\sqrt{p}+1)^2 > (\sqrt{p})^2 = p.$$

$\Rightarrow$ avem cel puțin $p+1$ numere

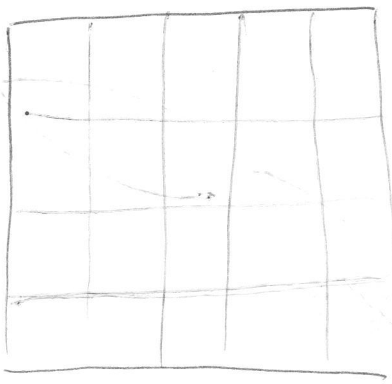
principiul cutiei $\Rightarrow \boxed{\exists (x,y) \neq (x_1,y_1)}$ $0 \le x, y, x_1, y_1 < \sqrt{p}$.

a.î. $x+yn \overset{p}{\equiv} x_1+y_1 n.$

Principiul cutiei

$n+1$ obiecte aparţinând la n clase $\Rightarrow \exists$ cel puţin 2 obiecte în aceeaşi clasă.

Pigeonhole principle



$a + mb \equiv 0(p)$ $\qquad (y - x_1) + m(y - y_1) \equiv 0(p)$

$(a+mb)(a-mb) \equiv 0(p)$ $\qquad \boxed{\begin{array}{l} b = y - y_1 \\ a = x - x_1 \end{array}}$

$a^2 - m^2 b^2 \equiv 0(p)$

$\boxed{a^2 + b^2 \equiv 0(p)}$ $\qquad 0 \leq a^2 + b^2 < p + p = 2p$

Dacă $a^2 + b^2 = 0 \Rightarrow a = b = 0.$

$\Rightarrow x = x_1$ şi $y = y_1$ $\qquad$ Abs $\Rightarrow (x, y) \neq (x_1, y_1)$

$$\left.\begin{array}{l} 0 < a^2 + b^2 < 2p \\ p \mid a^2 + b^2 \end{array}\right| \Rightarrow p = a^2 + b^2.$$

$x^3 - x^2 = x^2(x-1)$

Def: $f \in K[x]$ $\quad f \neq 0.$

$\alpha \in K \quad k \in \mathbb{N}^*$

Spunem că α răd. de ordin k pt f dacă $f(x)=(x-\alpha)^k \cdot g(x)$
$g(\alpha)\neq 0$.

α_n răd lui f (dacă α este răd. de ord. k a lui f)
ținând cont de ord fiecărei răd.

$$\begin{cases} \underbrace{\alpha, \alpha, \ldots \alpha}_{\text{de } k \text{ ori}} \\ \text{grad } f = n \\ f(x)=a(x-\alpha_1)\ldots(x-\alpha_n) \end{cases}$$

α s.n. răd $\begin{cases} \text{simplă pt } f \text{ dacă } k=1. \\ \text{multiplă pt } f \text{ dacă } k\geq 2 \end{cases}$

Prop. α răd. multiplă pt $f \Leftrightarrow \begin{cases} f(\alpha)=0. \\ f'(\alpha)=0 \end{cases}$

$f(x)=a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ K - corp.

Deriv. $f'(x) \overset{def.}{=} a_n \cdot n \cdot x^{n-1} + a_{n-1}\cdot(n-1)\cdot x^{n-2} \ldots + 2a_2 x + a_1$.

$(f\cdot g)' = f'\cdot g + f\cdot g'$