Curs 14. Numere prime. Polinoame ireductibile

15.01.2024

Def: Fie $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Dacă n nu are divizori diferiți de ± 1 și $\pm n$ spunem că n este <u>număr prim</u>.
Altfel, n este număr <u>compus</u>.

Dacă n prim și $n = a \cdot b$ cu $a, b \in \mathbb{Z} \Rightarrow a \in \{\pm 1\}$ sau $b \in \{\pm 1\}$
$(\Leftrightarrow |n| = |a|$ sau $|n| = |b|)$

Ex: 2, 3, 5, ... prime

Dacă $M_n = 2^n - 1$ este prim, s.n. nr. prim <u>Mersenne</u>

$M_2 = 3$, $M_3 = 7$, $\cancel{M_4 = 15}$, ... $M_{82589933}$ este cel mai mare nr prim Mersenne cunoscut (2023)
prim, prim, nu e prim

Testare primalitate:

- ciurul lui Eratostene
- metode de indexe
- Algoritmi probabiliști:
  - Fermat

    Pentru $n \in \mathbb{N} \setminus \{0, 1\}$ alegem $a \in \mathbb{N}$ și dacă $a^n \not\equiv a \pmod{n}$, atunci a nu e prim

<u>Mica teoremă a lui Fermat</u>

Dacă p prim și $a \in \mathbb{Z}$ $\quad a^p \equiv a \bmod p$

- $\exists$ numere Carmichael: n compus și $a^n \equiv a \bmod n$

Ex: $n = 561$ este cel mai mic nr Carmichael

Obs: Fie p un nr prim și $n \in \mathbb{Z}$.
Atunci $\gcd(p, n) = \begin{cases} 1, & \text{dacă } p \nmid n \\ p, & \text{dacă } p \mid n \end{cases}$

Teoremă: Fie $p \in \mathbb{Z} \setminus \{0, \pm 1\}$. Atunci
p prim $\Leftrightarrow \left(\forall a, b \in \mathbb{Z} \text{ cu } p \mid a \cdot b \Rightarrow p \mid a \text{ sau } p \mid b \right)$

Dem: „$\Rightarrow$" Sp că p e prim
Fie $a, b \in \mathbb{Z}$ aî $p \mid a \cdot b$
Dacă $p \mid a$ gata ✓
Dacă $p \nmid a \Rightarrow \gcd(p, a) = 1$ $\Bigg\} \Rightarrow p \mid b$

„$\Leftarrow$" Sp că p nu e prim, dacă $\exists a, b \in \mathbb{Z}$ cu $p = a \cdot b$ și $|a| > 1$ și $|b| > 1$.

$p \mid a \cdot b \Rightarrow p \mid a$ sau $p \mid b$

$\Downarrow \qquad\qquad \Downarrow$

$|p| \le |a| \qquad |p| \le |b|$

Deci $|p| = |a| \cdot |b| \Rightarrow |a| = 1$ sau $|b| = 1$

Teoremă: Fie $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Atunci putem scrie
$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ cu $p_i \in \mathbb{N}$ prime distincte și $a_i \in \mathbb{N}^*, \forall i = \overline{1,k}$

Mai mult, această descompunere e <u>unică</u> până la o rearanjare a factorilor.

<u>Dem</u>: • Existența: Inducție după $|n|$.
Dacă $|n| = 2 \Rightarrow n$ prim ✓
Dacă n prim ✓
Dacă n nu e prim $\Rightarrow n = a \cdot b$ cu $1 < |a|, |b| < |n|$
Pt a și b avem descompuneri în factori primi, și astfel găsim o descomp. și pt. n

• Unicitate: Sp $n = \pm p_1^{a_1} \cdots p_k^{a_k} = \pm q_1^{b_1} \cdots q_s^{b_s}$ $\quad b_i \ge 0$, $q_1, \ldots, q_s$ prime $\in \mathbb{N}$ distincte

$p_1 \mid n = \underbrace{q_1 \cdot q_1}_{b_1} \cdots \underbrace{q_s}_{b_s} \xRightarrow{p_1 \text{ prim}} \exists i$ cu $p_1 \mid q_i \Rightarrow p_1 = q_i$

$\Rightarrow \frac{n}{p_1} = \frac{n}{q_1} \Rightarrow$ pt n am o unică astfel (prime $\in \mathbb{N}$) al descomp.

Teorema (Euclid) Există o infinitate de numere prime.

Dem: Dacă RA $p_1, \dots, p_t \in \mathbb{N}$ sunt toate numerele prime (din $\mathbb{N}$)

$N = p_1 \cdots p_t + 1$ este coprim cu toți p_i

nu se divide cu $p_1, \dots, p_t$ $\Rightarrow N$ este prim Fals!

Teorema numerelor prime (Hadamard, de la Vallée-Poisson)

Notăm cu $\pi(n)$ = numărul numerelor (naturale) prime între $[0, n]$

$$\lim_{n \to \infty} \frac{\pi(n)}{n/\log n} = 1 \qquad \boxed{\pi(n) \sim \frac{n}{\log n}}$$

Teorema (Dirichlet)

Fie $a, d \in \mathbb{N}$, $\gcd(a,d) = 1$. Atunci $\exists$ o infinitate de nr prime de forma $\boxed{a + nd}$ cu $n \in \mathbb{N}$

Polinoame ireductibile

$K[X]$ unde K corp comutativ, $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p\}$ p prim

Def: Fie $f \in K[X]$ un polinom neconstant (grad $f \geq 1$)

Atunci f este ireductibil în $K[X]$ cu grad ≥ 1

Dacă f nu e ireductibil, spunem că f e reductibil în $K[X]$.

Ex: $X + 2 \in \mathbb{Q}[X]$ e ireductibil

$(X+2)^2 = (X+2) \cdot (X+2)$ e reductibil

$(X+2)^3 \cdot (X+5)^7$ e reductibil

Teoremă: Fie $f \in K[X]$ polinom neconstant

1) Dacă grad $f = 1 \Rightarrow f$ ireductibil

2) Dacă grad $f \geq 2$ și f ireductibil în $K[X] \Rightarrow f$ nu are rădăcini în K.

3) Dacă grad $f \in \{2, 3\}$, atunci f este ireductibil în $K[X]$

$\Leftrightarrow f$ nu are rădăcini în K

Dem: 2) Dacă $a \in K$ este răd. pt $f \Rightarrow f(x) = (x-a) \cdot g(x)$ cu $g \in K[X]$
$\Rightarrow f$ reductibil în $K[X]$.

3) „$\Rightarrow$" ✓ la 2)
„$\Leftarrow$" Sp că f nu are rădăcini în K
Dacă RA. f ar fi reductibil în $K[X]$
$f = g_1 \cdot g_2$ cu $g_1, g_2 \in K[X]$ neconstante

$\underbrace{\text{grad } f}_{= \text{grad } g_1 + \text{grad } g_2} \in \{2, 3\} \Rightarrow$ unul din factori are gradul 1

$\text{grad } g_1 \geq 1$, $\text{grad } g_2 \geq 1$

Sp că $g_1(x) = \alpha x + \beta$ cu $\alpha, \beta \in K$, $\alpha \neq 0$

Dar $\underbrace{-\frac{\beta}{\alpha}}_{\in K}$ răd. pt g_1, deci și pt f

Deci f ired. în $K[X]$

Ex: 1) $x^2 - 2 \in \mathbb{Q}[X]$ e ired în $\mathbb{Q}[X]$ pt că răd. sale $\pm\sqrt{2} \notin \mathbb{Q}$
Dar $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2}) \in \mathbb{R}[X]$ este red. în $\mathbb{R}$.
2) $(x^2+1)(x^2-2) \in \mathbb{Q}[X]$ este red în $\mathbb{Q}[X]$, dar nu are rădăcini în $\mathbb{Q}$.

Teoremă: Fie $f \in K[X]$ polinom neconstant
1) Dacă f ireductibil în $K[X] \Rightarrow \forall g \in K[X]$ avem

$$\gcd(f, g) = \begin{cases} 1, & \text{dacă } f \nmid g \\ f, & \text{dacă } f \mid g \end{cases}$$

2) f ireductibil în $K[X] \Leftrightarrow \forall a, b \in K[X]$ ($f \mid a \cdot b \Rightarrow f \mid a$ sau $f \mid b$)

Teorema de descompunere în factori ireductibili

Fie $f \in K[X]$ polinom neconstant. Atunci putem scrie
$f = c \cdot f_1^{a_1} \cdot f_2^{a_2} \cdot \ldots \cdot f_t^{a_t}$ cu $c \in K \setminus \{0\}$

$f_1, \ldots, f_t \in K[X]$ polinoame monice (ireductibile)

$a_1, \ldots, a_t \in \mathbb{N}^*$

Descomp. e unică până la o rearanjare a factorilor

Th: Există o infinitate de polinoame ireductibile (monice)

Teorema fundamentală a algebrei (D'Alambert)

Orice polinom neconstant $f \in \mathbb{C}[X]$ are măcar o răd. în $\mathbb{C}$

Corolar: Polinoamele ired. din $\mathbb{C}[X]$ sunt cele de grad 1.

Deci pt $f \in \mathbb{C}[X]$, $f = \underset{\mathbb{C}^*}{c} \cdot (X-\alpha_1)^{a_1}(X-\alpha_2)^{a_2} \cdot \ldots \cdot (X-\alpha_t)^{a_t}$ cu $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{C}$ distincte, $a_1, \ldots, a_t \geq 1$

este descompunerea în factori ireductibili în $\mathbb{C}[X]$.

a_i = multiplicitatea rădăcinii α_i

în $\mathbb{R}[X]$: • Dacă $\alpha \in \mathbb{C} \setminus \mathbb{R}$ este rădăcină pt $f \in \mathbb{R}[X]$, atunci $\overline{\alpha}$ este rădăcină pt f cu aceeași multiplicitate ca α.

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - \underbrace{(\alpha+\overline{\alpha})}_{2\cdot \mathrm{Re}(\alpha)} X + \underbrace{\alpha \cdot \overline{\alpha}}_{|\alpha|^2 \in \mathbb{R}} \in \mathbb{R}[X]$$

• Prop: Un polinom neconstant $f \in \mathbb{R}[X]$ este ired. în $\mathbb{R}[X]$ $\Leftrightarrow$ (grad $f = 1$) sau (grad $f = 2$, $f(X) = aX^2 + bX + c$ cu $\Delta = b^2 - 4ac < 0$.)

în $\mathbb{Q}[X]$: • $f \in \mathbb{Q}[X]$ are factori de grad 1 $\Leftrightarrow$ are rădăcini în $\mathbb{Q}$

f și $N \cdot f$ au aceleași rădăcini $\forall N \in \mathbb{Q}^*$.

pot reduce problema la aflarea răd. naturale pt $f \in \mathbb{Z}[X]$.

• Prop: $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$, $a_n \neq 0$ cu $\gcd(a_0, \ldots, a_n) = 1$

Atunci dacă $\frac{u}{v}$ cu $u, v \in \mathbb{Z}$, $(u,v) = 1$ este răd. pt f

$$\Rightarrow \boxed{\begin{array}{l} u \mid a_0 \\ v \mid a_n \end{array}} \text{ și}$$

Dem: $f\left(\frac{u}{v}\right) = 0 \Rightarrow a_n \left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \ldots + a_1 \cdot \frac{u}{v} + a_0 = 0 \quad | \cdot v^n$

$a_n \cdot u^n + a_{n-1} \cdot v \cdot u^{n-1} + \ldots + a_1 \cdot u \cdot v^{n-1} + a_0 \cdot v^n = 0$

$\Rightarrow u \mid a_0 \cdot v^n$, $(u,v)=1$ $\Big| \Rightarrow u \mid a_0$ și $v \mid a_n \cdot u^n \Rightarrow v \mid a_n$.