

Wilsonova a Lagrangeova veta

18. novembra 2025

Lagrangeova veta

Veta (Lagrangeova veta)

Ak $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ je polynóm s celočíselnými koeficientami, p je prvočíslo a $p \nmid a_n$, tak kongruencia $f(x) \equiv 0 \pmod{p}$ má najviac n (navzájom nekongruentných) riešení. Ekvivalentne, ak táto kongruencia má viac ako n (navzájom nekongruentných) riešení, tak p delí všetky koeficienty polynómu $f(x)$.

Lagrangeova veta

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

- ▶ Počet riešení kongruencie $f(x) \equiv 0 \pmod{p}$.
- ▶ Počet koreňov polynómu $f(x)$ v poli $\mathbb{Z}_p$

Pre ľubovoľné pole platí: Nenulový polynóm $f(x) \in F[x]$ stupňa n má v poli F najviac n koreňov.

Lagrangeova veta

Pre ľubovoľné pole platí: Nenulový polynóm $f(x) \in F[x]$ stupňa n má v poli F najviac n koreňov.

- ▶ Nenulový polynóm $f(x) \in \mathbb{Z}_p[x]$ stupňa n .
- ▶ $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ taký, že $p \nmid a_n$.

Vandermondov determinant

Tvrdenie (Vandermondov determinant)

Nech $x_1, \dots, x_n$ sú prvky poľa F . Potom

$$\begin{vmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_n & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Špeciálne dostávame, že ak $x_i \neq x_j$ pre všetky $i \neq j$, tak Vandermondov determinant je nenulový.

Wilsonova veta

Veta (Wilsonova veta)

Číslo p je prvočíslo práve vtedy, keď platí kongruencia

$$(p-1)! \equiv -1 \pmod{p}. \quad (1)$$

$$f(x) = x^{p-1} - 1 - \prod_{m=1}^{p-1} (x - m)$$

Kombinatorický dôkaz

$$B(n, r) = r(B(n-1, r) + B(n-1, r-1)) \quad (2)$$

$$B(n, r) = \sum_{k=1}^{n-r+1} \binom{n}{k} B(n-k, r-1) \quad (3)$$

Lema

Nech p je prvočíslo. Potom

- (i) $p \mid B(p, r)$ pre všetky $r \geq 2$,*
- (ii) $p \mid B(p-1, r) + (-1)^r$ pre všetky r také, že $1 \leq r \leq p-1$.*

Kvadratické zvyšky

Definícia

Číslo q sa nazýva kvadratický zvyšok modulo n , ak existuje také $x \in \mathbb{Z}$, že

$$x^2 \equiv q \pmod{n}.$$

Veta

Ak p je prvočíslo tvaru $p = 4k + 1$, tak -1 je kvadratický zvyšok modulo p .