9. LAGRANGEOVA VETA

Symbolom $\mathbb{Z}[x]$ budeme označovať množinu všetkých polynómov s celočíselnými koeficientami. V našich ďalších úvahách bude mať veľký význam nasledujúce tvrdenie.

Veta 11. Nech $f(x) \in \mathbb{Z}[x]$ **a** $n = st\, f(x), n > 0$**. Ak kongruencia**

$$f(x) \equiv 0 \pmod{p}, \tag{14}$$

kde p **je prvočíslo, má viac ako** n **primitívnych riešení, potom každý koeficient polynómu** $f(x)$ **je deliteľný prvočíslom** p.

Dôkaz tejto vety nájdeme v nasledujúcich úlohách.

Úloha 203. Nech $a, b \in \mathbb{Z}$, p je prvočíslo a pre $x_1 \neq x_2 \in \mathbb{Z}_p$ platí

$$ax_1 + b \equiv 0 \pmod{p},$$
$$ax_2 + b \equiv 0 \pmod{p}.$$

Potom $p|a$ a $p|b$. Dokážte.

Dôkaz vety 11 urobíme matematickou indukciou vzhľadom na stupeň polynómu $f(x)$. Prípad, kedy $st\, f(x) = 1$, je dokázaný v úlohe 203.

Úloha 204. Nech $f(x) \in \mathbb{Z}[x]$ a $st\, f(x) > 1$. Ak $a \in \mathbb{Z}$, potom existuje polynom $g(x) \in \mathbb{Z}[x]$ taký, že $st\, g(x) = st\, f(x) - 1$ a

$$f(x) = g(x)(x - a) + f(a).$$

Dokážte.

(Návod: Uvedomte si, že $x^k - a^k = (x - a)(x^{k-1} + x^{k-2}a + \cdots + xa^{k-2} + a^{k-1})$.)

Úloha 205. Nech $st\, f(x) = n$ a $x_1, \ldots, x_{n+1}$ sú primitívne korene kongruencie (14). Nech

$$f(x) = g(x)(x - x_{n+1}) + f(x_{n+1}).$$

Dokážte, že $x_1, \ldots, x_n$ sú primitívne korene kongruencie

$$g(x) \equiv 0 \pmod{p},$$

kde p je prvočíslo.

Úloha 206. Matematickou indukciou dokážte vetu 11 pomocou úloh 203, 204 a 205.

Veta 11 sa nazýva *Lagrangeova veta*. Pod týmto názvom poznáme viacero tvrdení. Táto veta je analógiou tvrdenia o koreňoch polynomu stupňa n.

Joseph Luis Lagrange (1736-1813) patril medzi významných matematikov, akými boli aj Euler a Fermat. Na vrchole svojej slávy pôsobil J. Langrange ako profesor v Paríži na univerzite Sorbona, kde jedna z posluchární nesie jeho meno. Taktiež je po ňom pomenovaná aj jedna stanica metra.

Najskôr si použitie Lagrangeovej vety ukážeme na dôkaze Wilsonovej vety (veta 9), ktorý sa tým zjednoduší.

Úloha 207. Nech p je nepárne prvočíslo. Uvažujme polynom

$$f(x) = (x-1)...(x-(p-1)) - x^{p-1} + 1.$$

a) Dokážte, že $stf(x) = p-2$.
b) Dokážte, že každé z čísel $1, ..., p-1$ je primitívnym koreňom kongruencie

$$f(x) \equiv 0 \pmod{p}.$$

(Návod: V dôkaze časti b) použite malú Fermatovu vetu.)

Úloha 208. Dokážte vetu 9 pomocou úlohy 207 a vety 11.

– – – – – – – – – – – –

Nájsť všetky primitívne riešenia kongruencie $f(x) \equiv 0 \pmod{m}$, *keď* $m = p$ *je prvočíslo, môže byť dosť náročné na čas. Táto úloha sa ale dá zjednodušiť, ak* m *je zložené číslo. Uvažujme najprv prípad, keď* $m = p^\alpha$, *pričom* p *je prvočíslo. Každé riešenie kongruencie*

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}$$

je aj riešením kongruencie

$$f(x) \equiv 0 \pmod{p^\alpha}.$$

Teda niekedy sa dá riešenie kongruencie $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ *previesť na riešenie kongruencie* $f(x) \equiv 0 \pmod{p^\alpha}$ *a tak postupne až na riešenie kongruencie* $f(x) \equiv 0 \pmod{p}$.

Nech $x_0, t \in \mathbb{N}$. *Potom z binomickej vety dostávame*

$$(x_0 + tp^\alpha)^j = x_0^j + jx_0^{j-1}tp^\alpha + kp^{\alpha+1}$$

pre $j = 0, 1, 2, ...$ *Teda*

$$(x_0 + tp^\alpha)^j \equiv x_0^j + jx_0^{j-1}tp^\alpha \pmod{p^{\alpha+1}}.$$

Z toho pre každý polynom s celočíselnými koeficientami dostávame

$$f(x_0 + tp^\alpha) \equiv f(x_0) + f'(x_0)tp^\alpha \pmod{p^{\alpha+1}}.$$

Teda ak x_1 *je primitívne riešenie kongruencie* $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ *a* $x_0 \equiv x_1 \pmod{p^{\alpha+1}}$, *potom* x_0 *je primitívne riešenie kongruencie* $f(x) \equiv 0 \pmod{p^\alpha}$ *a platí* $x_1 = x_0 + tp^\alpha$, *kde* $t \in \{0, 1, ..., p-1\}$. *Podľa* $f(x_0 + tp^\alpha) \equiv f(x_0) + f'(x_0)tp^\alpha$

$(\mathrm{mod}\ p^{\alpha+1})$ *dostávame* $f(x_0)+f'(x_0)tp^\alpha \equiv 0\ (\mathrm{mod}\ p^{\alpha+1})$ *a po vydelení* p^α *dostávame* $\frac{f(x_0)}{p^\alpha} + tf'(x_0) \equiv 0\ (\mathrm{mod}\ p)$. *Z tejto kongruencie môžeme niekedy vypočítať* t. *Ak* $(f'(x_0), t) = 1$, *také* t *existuje jediné.*

Uvažujme kongruenciu

$$x^2 + x + 3 \equiv 0\ (\mathrm{mod}\ 25).$$

Najprv riešime kongruenciu

$$x^2 + x + 3 \equiv 0\ (\mathrm{mod}\ 5).$$

Táto kongruencia má dve primitívne riešenia 1 a 3. Primitívne riešenie prvej kongruencie budeme hľadať v tvare $1+5t_1, 3+5t_2$. *Vieme, že* t_1 *spĺňa kongruenciu*

$$1 + 3t_1 \equiv 0\ (\mathrm{mod}\ 5).$$

Teda $t_1 = 3$. *Podobne,* t_2 *spĺňa kongruenciu*

$$3 + 7t_2 \equiv 0\ (\mathrm{mod}\ 5).$$

Teda $t_2 = 1$. *Máme dve primitívne riešenia, 16 a 8.*

Nakoniec ak riešime kongruenciu

$$f(x) \equiv 0\ (\mathrm{mod}\ m),$$

kde $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ *je kanonický rozklad čísla* m, *tak riešime* n *kongruencií*

$$f(x) \equiv 0\ (\mathrm{mod}\ p_j^{\alpha_j}), j = 1, 2, ..., n$$

a ku každej n*-tici riešení* $x_1, x_2, ..., x_n$ *(*x_j *je riešenie kongruencie* $f(x) \equiv 0\ (\mathrm{mod}\ p_j^{\alpha_j})$*) nájdeme rovnakým postupom ako v dôkaze čínskej zvyškovej vety také* x, *aby* $x \equiv x_j\ (\mathrm{mod}\ p_j^{\alpha_j}), j = 1, 2, ..., n$ *a* $x \in \{0, 1, ..., m-1\}$.