3. domácí úloha z MIN401, jaro 2024

Příklad 1. Vyřešte polynomiální kongruenci $7x^6 + 4x + 12 \equiv 0 \pmod{135}$, celkem byste měli najít 2 řešení modulo 135.

Řešení. Protože $135 = 3^3 \cdot 5$, budeme prvně řešit kongruenci zvlášť modulo 5, pak modulo $3, 3^2, 3^3$.

Modulo 5 ji lze s přihlédnutím k $x \not\equiv 0 \pmod 5$ podle Eulerovy věty $x^4 \equiv 1 \pmod 5$ upravit na

$$7x^6 + 4x + 12 \equiv 2x^2 + 4x + 2 \equiv 2(x+1)^2 \equiv 0 \pmod 5.$$

Jediným řešením je tak $x \equiv 4 \pmod 5$.

Modulo 3 máme buď $x \equiv 0 \pmod 3$ nebo opět podle Eulerovy věty $x^2 \equiv 1 \pmod 3$ můžeme kongruenci upravit na

$$7x^6 + 4x + 12 \equiv 1 + x \equiv 0 \pmod 3$$

a dalším řešením je tak $x \equiv 2 \pmod 3$.

Nyní přejděme k modulu 9: Pro $x \equiv 0 \pmod 3$, tj. $x = 3t$ dostáváme

$$7(3t)^6 + 4(3t) + 12 \equiv 3t + 3 \equiv 0 \pmod 9 \quad \Leftrightarrow \quad t + 1 \equiv 0 \pmod 3$$

a tedy $t \equiv 2 \pmod 3$ neboli $x = 9s + 6$; dále

$$7(9s+6)^6 + 4(9s+6) + 12 \equiv 9s + 9 \equiv 0 \pmod{27} \quad \Leftrightarrow \quad s + 1 \equiv 0 \pmod 3$$

a tedy $s \equiv 2 \pmod 3$ neboli $x = 27r + 24$. Podobně pro $x \equiv 2 \pmod 3$, tj. $x = 3t + 2$ dostáváme

$$7(3t+2)^6 + 4(3t+2) + 12 \equiv 7 \cdot 2^6 + 3t + 2 \equiv 0 \pmod 9 \quad \Leftrightarrow \quad t \equiv 0 \pmod 3$$

a tedy $t \equiv 0 \pmod 3$ neboli $x = 9s + 2$; dále

$$7(9s+2)^6 + 4(9s+2) + 12 \equiv 7 \cdot 2^6 + 9s + 20 \equiv 0 \pmod{27} \quad \Leftrightarrow \quad s + 1 \equiv 0 \pmod 3$$

a tedy $s \equiv 2 \pmod 3$ neboli $x = 27r + 20$. Dostali jsme tak dvě řešení $x \equiv 20, 24 \pmod{27}$.

Nyní je potřeba dát tyto výsledky dohromady. Standardním způsobem dostaneme vyřešením soustav

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 20 \pmod{27} \end{aligned} \qquad\qquad \begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 24 \pmod{27} \end{aligned}$$

finální řešení $x \equiv 74 \pmod{135}$ a $x \equiv 24 \pmod{135}$. □

Příklad 2. Rozložte polynom

$$f(x) = x^6 - 2x^5 + 2x + 1$$

na součin ireducibilních polynomů nad $\mathbb{C}$, když víte, že $f(x)$ obsahuje násobné kořeny. Jak bude rozklad vypadat nad $\mathbb{R}$?

Řešení. Spočítáme největší společný dělitel $(f(x), f'(x))$:

$$\begin{aligned}(x^6 - 2x^5 + 2x + 1, 6x^5 - 10x^4 + 2) &= (6x^5 - 10x^4 + 2, x^4 - 3x - 2)\\ &= (x^4 - 3x - 2, x^2 - x - 1)\\ &= (x^2 - x - 1, 0) = x^2 - x - 1.\end{aligned}$$

Násobné kořeny $f(x)$ jsou proto kořeny $x^2 - x - 1$, tedy

$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Vydělením $(x - \frac{1+\sqrt{5}}{2})^2(x - \frac{1-\sqrt{5}}{2})^2 = (x^2 - x - 1)^2$ dostáváme

$$f(x)/(x^2 - x - 1)^2 = x^2 + 1 = (x - i)(x + i)$$

a příslušné rozklady nad $\mathbb{C}$ a nad $\mathbb{R}$ jsou

$$\begin{aligned}f(x) &= (x - \tfrac{1+\sqrt{5}}{2})^2(x - \tfrac{1-\sqrt{5}}{2})^2(x - i)(x + i)\\ &= (x - \tfrac{1+\sqrt{5}}{2})^2(x - \tfrac{1-\sqrt{5}}{2})^2(x^2 + 1).\end{aligned}$$

$\square$