2. cvičení (6. března 2008)

Co jsme dělali?

Zabývali jsme se grupami a řešením kongruencí: $\mathbb{Z}_p^*$ je cyklická pro prvočíslo p; je-li $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ rozklad n na součin různých prvočísel, pak $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$ a také $\mathbb{Z}_n^* \simeq \mathbb{Z}^*_{p_1^{\alpha_1}} \times Z^*_{p_2^{\alpha_2}} \times \cdots \times Z^*_{p_k^{\alpha_k}}$. Uvedli jsme si ještě druhou formulaci čínské zbytkové věty, která se týká řešení soustavy kongruencí tvaru $x \equiv b_i \pmod{m_i}$.

Pak jsme se zabývali polynomy a řešením kongruencí vyšších stupňů. Polynom stupně n nad tělesem (například $\mathbb{Z}_p$) má nejvýš n kořenů. Pro $P \in \mathbb{Z}[x]$ platí $a \equiv b \pmod m \Rightarrow P(a) \equiv P(b) \pmod m$, čehož využíváme při zkoušení všech možných zbytků.

Další vhodnou metodou řešení nelineárních kongruencí je najít nějaký primitivní prvek a využít izomorfismu $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$.

Příklady

-1. Vyřeš soustavu $3x \equiv 5 \pmod{17}$, $4x \equiv 20 \pmod{28}$.

0. Vyřeš kongruenci $x^2 \equiv 3 \pmod{13}$ (můžeš předpokládat, že víš, že 2 je primitivní prvek).

1. Vyřeš soustavu $5x \equiv 3 \pmod 7$, $3x \equiv 5 \pmod{11}$, $2x \equiv 1 \pmod 3$.

2. Vyřeš kongruenci $x^4 \equiv 8 \pmod{19}$.

3. Buď p liché prvočíslo. Dokaž, že $|x^2 \pmod p, 1 \leq x \leq p-1| = (p-1)/2$.

4. Vyřeš soustavu $4x \equiv 1 \pmod{27}$, $5x \equiv 27 \pmod{51}$.

5. Vyřeš $x^3 - 3x + 5 \equiv 0 \pmod{105}$.

6. V závislosti na $k \in \mathbb{N}$ a prvočíslu p spočti $1^k + 2^k + \cdots + (p-1)^k \pmod p$.

7. Vyřeš $x^8 \equiv 2 \pmod 7$.

8. Nechť $k, n \in \mathbb{N}$. Dokaž, že existuje k po sobě jdoucích přirozených čísla, z nichž každé je tvaru ab^n pro vhodná $a, b \in \mathbb{N}, b \neq 1$.

Těžší příklad

1. Myslím si přirozené číslo $n, 1 \leq n < 100$. Pomocí 7 otázek na hodnotu $(n+c, d)$ pro tebou zvolená $c, d, 1 \leq c, d < 100$, zjisti, o jaké číslo jde!