4. cvičení (8. 3. 2007)

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 $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{\alpha_1}}^* \times Z_{p_2^{\alpha_2}}^* \times \cdots \times Z_{p_k^{\alpha_k}}^*$, odkud snadno vyplývá vzorec pro výpočet hodnoty $\varphi(n)$.

A řešili jsme kongruence o jedné neznámé $ax \equiv b \pmod{m}$. Nakonec jsme si uvedli ještě druhou formulaci čínské zbytkové věty, která se týká řešení soustavy kongruencí tvaru $x \equiv b_i \pmod{m}_i$.

Nakonec jsme si řekli, že pro $P \in \mathbb{Z}[x]$ platí $a \equiv b \pmod{m} \to P(a) \equiv P(b) \pmod{m}$ a jak toho využít při řešení nelineárních kongruencí (vhodné metody jsou zkoušení všech možných zbytků a použití Eulerovy věty).

Příklady

-2. Najdi všechna celá čísla x, pro která platí $29x \equiv 1 \pmod{17}$.

-1. Dva bratři (jednomu bylo 5 a druhému 7 let) měli spravedlivě rozděleno několik hraček. Co ale čert nechtěl, narodila se jim sestřička. Až trochu vyrostla (a byly jí 3 roky), chtěla taky nějaké hračky, se kterými by si mohla hrát. Bratříčci byli hodní, a tak se chtěli se sestřičkou rozdělit. Ať to ale zkoušeli, jak jen chtěli, spravedlivě rozdělit hračky se jim nedařilo - vždy 2 zbyly. Kolik mohli mít celkem hraček?

0. $x^2 \equiv 2 \pmod{3}$

1. Najdi všechna celá čísla x, pro která platí $21x + 5 \equiv 0 \pmod{29}$.

2. Spočti $\varphi(84)$.

3. Vyřeš soustavu $x \equiv -3 \pmod{49}$, $x \equiv 2 \pmod{11}$.

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

5. Vyřeš $x^3 \equiv 2 \pmod{5}$.

6. Vyřeš $x^8 \equiv 2 \pmod{7}$.

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

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 příklady

1. Vyřeš kongruenci $(a+b)x \equiv a^2 + b^2 \pmod{ab}$, kde $a, b \in \mathbb{N}, (a, b) = 1$.

2. 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!

3. Vyřeš $23941x \equiv 915 \pmod{3564}$.