11. cvičení (3. května 2007)

Co jsme dělali?

Definovali jsme kvadratické zbytky a nezbytky a Legendrův symbol $\left(\frac{a}{p}\right)$. Uvedli jsme si jeho základní vlastnosti a zákon kvadratické reciprocity, který umožňuje Legendrův symbol jednoduše počítat.

Příklady

0. Kolik má kongruence $x^2 \equiv 23 \pmod{113}$ řešení?

1. Spočti $\left(\frac{31}{71}\right)$.

2. V závislosti na prvočíslu p urči hodnotu $\left(\frac{3}{p}\right)$.

3. Kolik má kongruence $x^2 \equiv 37 \pmod{91}$ řešení (pozor, 91 není prvočíslo)?

4. Buď p prvočíslo. Dokaž, že $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

5. Buď p prvočíslo. Dokaž, že $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

6. Najdi všechny kvadratické zbytky modulo 15.

7. Buď p prvočíslo. Označme $M = \{r | 1 \leq r \leq p-1, r$ je kvadratický zbytek modulo $p\}$ a X součin všech prvků množiny M. Dokaž, že pokud $p \equiv 1 \pmod{4}$, pak $X \equiv -1 \pmod{p}$, a že pokud $p \equiv -1 \pmod{4}$, pak $X \equiv 1 \pmod{p}$.

8. Buď p liché prvočíslo a a číslo nesoudělné s p. Dokaž, že a je kvadratický zbytek modulo p^l právě tehdy, když $\left(\frac{a}{p}\right) = 1$.

9. Kolik je kvadratických zbytků modulo přirozené číslo m?