Cvičení 29. 3. 2012

Číslo a je kvadratický zbytek modulo n, pokud existuje m, že $m^2 \equiv a \pmod{n}$. Ne každé číslo je kvadratický zbytek.

Značení: Pro p *prvočíslo* (to je důležité!) zachycuje vlastnost „a je kvadratický zbytek modulo p“ takzvaný Legendreův symbol $\left(\frac{a}{p}\right)$ s hodnotou 0 pokud $p|a$, 1 pokud a je kvadratický zbytek a -1 pokud a je kvadratický nezbytek (tj. není kvadratický zbytek).

S Legendreovými symboly jde rozumně počítat:

1. Pokud $a \equiv b \pmod{p}$, tak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
2. pro p liché platí $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,
3. platí $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,
4. $\left(\frac{2}{p}\right) = 1$ pro $p \equiv 1, 7 \pmod{8}$ a -1 pro $p \equiv 3, 5 \pmod{8}$.
5. Pokud p, q jsou prvočísla různá od 2, tak platí kvadratická reciprocita

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

(Tj. napravo vychází -1, právě když $p, q \equiv 3 \pmod{4}$, jinak vyjde 1.)

Příklad 1. Spočtěte:

1. $\left(\frac{24}{37}\right)$
2. $\left(\frac{31}{71}\right)$
3. $\left(\frac{512}{29}\right)$
4. $\left(\frac{12345}{331}\right)$

Příklad 2. Kolik řešení má rovnice $x^2 \equiv 23 \pmod{113}$? A co rovnice $x^2 \equiv 37 \pmod{91}$ (pozor, není prvočíslo)?

Příklad 3. Mějme rovnici $ax^2 + bx + c \equiv 0 \pmod{p}$, kde p nedělí a. Označme $D = b^2 - 4ac$. Dokažte, že tato rovnice má řešení, právě když $\left(\frac{D}{p}\right) \geq 0$. Jak je to s počtem řešení?

Příklad 4. Spočtěte $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)$ pro p prvočíslo.

Příklad 5. Dokažte, že pro p liché platí $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Příklad 6. Buď p prvočíslo, $n \in \mathbb{N}$. Dokažte, že a nesoudělné s p je kvadratický zbytek modulo p^n, právě když $\left(\frac{a}{p}\right) = 1$.

Příklad 7. Pomocí zákona kvadratické reciprocity vyjádřete v závislosti na p hodnoty $\left(\frac{3}{p}\right)$ a $\left(\frac{5}{p}\right)$.