Kvadratické zbytky

Víťa Kala

Představ si, že potřebuješ vyřešit kongruenci $x^2 \equiv a \pmod{p}$ pro nějaké celé číslo a a prvočíslo p. Když si s ní chvilku zkusíš hrát, nejspíš zjistíš, že se toho s ní moc dělat nedá. Přesto se ale o jejích řešeních leccos dá zjistit, a právě to bude cílem této přednášky.

Definice. *Buď p libovolné prvočíslo a a celé číslo. Legendrův symbol*[1] $\left(\frac{a}{p}\right)$ *definujeme takto:*

(i) $\left(\frac{a}{p}\right) = 1$, *pokud* $x^2 \equiv a \pmod{p}$ *má řešení,*
(ii) $\left(\frac{a}{p}\right) = -1$, *pokud* $x^2 \equiv a \pmod{p}$ *nemá řešení,*
(iii) $\left(\frac{a}{p}\right) = 0$, *pokud p dělí a.*

Věta. (Některé základní vlastnosti Legendrova symbolu)

(a) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

S trochou snahy se taky dá spočítat, že $\left(\frac{2}{p}\right) = 1$ pro $p \equiv \pm 1 \pmod{8}$ a $\left(\frac{2}{p}\right) = -1$ pro $p \equiv \pm 3 \pmod{8}$.

Věta. (Zákon kvadratické reciprocity)
Pro libovolná lichá prvočísla p a q platí:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

[1] Jméno toho pána se ve slušné společnosti vyslovuje lažándr.