

Teorie čísel: Cvičení 8

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Definice. Buď $n \neq 0$, $a \in \mathbb{Z}$. Pak a je *kvadratický zbytek* modulo n , pokud existuje nějaké $b \in \mathbb{Z}$ splňující $a \equiv b^2 \pmod{n}$; jinak je to *kvadratický nezbytek* modulo n .

Definice. Pro liché prvočíslo p definujeme také *Legendreův symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{pokud } p \nmid a \text{ a } a \text{ je kvadratický zbytek modulo } p, \\ -1, & \text{pokud } p \nmid a \text{ a } a \text{ je kvadratický nezbytek modulo } p, \\ 0, & \text{pokud } p \mid a. \end{cases}$$

Věta. Buď p liché prvočíslo, $a \in \mathbb{Z}$. Pak $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Důsledek. Máme $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ pro $a, b \in \mathbb{Z}$ a libovolné prvočíslo p .

Věta (Zákon kvadratické reciprocity). Pro různá lichá prvočísla p, q platí $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Věta (Dodatky ke kvadratické reciprocitě). Pro liché prvočíslo p platí $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

-2. Najděte všechny kvadratické zbytky modulo 4 a modulo 7.

-1. Určete hodnotu výrazů

(a) $\left(\frac{-1}{7}\right)$,

(b) $\left(\frac{3}{7}\right)$,

(c) $\left(\frac{17}{61}\right)$.

0. V závislosti na prvočísle p určete hodnotu výrazu $\left(\frac{3}{p}\right)$.

! 1. Najděte všechny kvadratické zbytky modulo 8, modulo 9 a modulo 17.

2. Bez použití kvadratické reciprocity spočítejte $\left(\frac{17}{5}\right)$ a $\left(\frac{5}{17}\right)$.

! 3. Určete hodnotu výrazů:

(a) $\left(\frac{11}{31}\right)$,

(b) $\left(\frac{17}{37}\right)$,

(c) $\left(\frac{523}{269}\right)$,

(d) $\left(\frac{61}{31}\right)$.

4. Ukažte, že pokud $3 \mid a^2 + b^2$, pak $3 \mid a$ a $3 \mid b$.

! 5. V závislosti na prvočísle p určete hodnotu výrazu $\left(\frac{7}{p}\right)$ a $\left(\frac{13}{p}\right)$.

Další příklady:

6. Ukažte, že rovnice $x^2 + y^2 = 8z + 6$ nemá žádné celočíselné řešení. Najděte nějakou další rovnici o třech neznámých, která nemá žádné celočíselné řešení.

7. Najděte všechna prvočísla p , pro která platí: Je-li x kvadratický zbytek modulo p , pak je i $-x$ kvadratický zbytek modulo p .

8. Najděte všechna prvočísla p , pro něž existuje $a \in \mathbb{Z}$ splňující $p \mid a^2 + 7$.

* 9. Ukažte, že pokud $p \neq 2, 3$ je prvočíslo, pak p dělí součet všech kvadratických zbytků modulo p .

* 10. Buď p prvočíslo, $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}$. Ukažte, že $\sum_{k=0}^{p-1} \left(\frac{ka+b}{p}\right) = 0$.

* 11. Pro liché prvočíslo p označme $a_1, \dots, a_{(p-1)/2}$ všechny nenulové kvadratické zbytky modulo p . Kolik kvadratických zbytků modulo p je mezi čísly $a_1 + 1, \dots, a_{(p-1)/2} + 1$?

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.

Úlohy s ! je doporučeno řešit přednostně, úlohy s * jsou náročnější.