Teorie čísel: Cvičení 11

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Definice. Mějme $a \in \mathbb{Z}$ a **liché** $n \in \mathbb{N}$. *Jacobiho symbol* $\left(\frac{a}{n}\right)$ definujeme jako $\left(\frac{a}{n}\right) = \left(\frac{a}{q_1}\right) \cdots \left(\frac{a}{q_k}\right)$, kde $q_1 \cdots q_k$ je rozklad n na součin (ne nutně různých) prvočísel a výrazy napravo jsou Legendreovy symboly.

Věta. *Mějme celá čísla a, b a lichá přirozená čísla m, n. Jacobiho symbol má následující vlastnosti:*

(i) Multiplikativita: $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right), \quad \left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(ii) Periodicita: $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ *pro* $a \equiv b \pmod{n}$.

(iii) Doplňky k reciprocitě: $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

(iv) Reciprocita: $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

-1. Určete hodnotu výrazu $\left(\frac{477}{247}\right)$.

0. Řešte kongruenci $x^2 \equiv 53 \pmod{77}$.

! 1. Určete hodnotu výrazů (a) $\left(\frac{98}{51}\right)$, (b) $\left(\frac{89}{63}\right)$, (c) $\left(\frac{347}{221}\right)$, (d) $\left(\frac{675}{223}\right)$.

! 2. Podívejte se na vztah Jacobiho symbolů a kongruencí. Konkrétně:
   (a) Rozhodněte, zda mají kongruence $x^2 \equiv 18$ a $x^2 \equiv 14 \pmod{127}$ řešení. (127 je prvočíslo.)
   (b) Řešte kongruenci $x^2 \equiv 58 \pmod{209}$. $(209 = 11 \cdot 19)$
   (c) Rozhodněte, jestli má kongruence $x^2 \equiv 58 \pmod{65}$ řešení.

! 3. Nechť n je liché přirozené číslo. Pomocí vztahu pro $\left(\frac{-1}{n}\right)$ a $\left(\frac{2}{n}\right)$ určete explicitně hodnoty $\left(\frac{-1}{n}\right)$, $\left(\frac{2}{n}\right)$ a $\left(\frac{-2}{n}\right)$ v závislosti na zbytku n modulo 4, resp. 8.

4. Vyšetřete vztah Jacobiho symbolů a kvadratických zbytků. Konkrétně:
   (a) Nechť $n = p_1 \cdots p_k$ je prvočíselný rozklad bezčtvercového čísla n. Ukažte, že $x^2 \equiv a \pmod{n}$ má řešení, právě když má řešení každá z kongruencí $x^2 \equiv a \pmod{p_1}, \ldots, x^2 \equiv a \pmod{p_k}$.
   (b) Odvoďte, že pokud $\left(\frac{a}{n}\right) = -1$, pak a není kvadratický zbytek modulo n.
   (c) Najděte příklad, kdy $\left(\frac{a}{n}\right) = 1$, ale a není kvadratický zbytek modulo n.

5. Na základě znalosti příslušných tvrzení pro Legendreovy symboly odvoďte výše uvedenou větu pro Jacobiho symboly. Zaměřte se zvláště na bod (iii).

! 6. Rozmyslete si některé speciální případy Dirichletovy věty:
   (a) Připomeňte si Eukleidův důkaz, že existuje nekonečně mnoho prvočísel.
   (b) Upravte ho a ukažte, že existuje nekonečně mnoho prvočísel tvaru i) $4k + 3$, ii) $6k + 5$.
   (c) Proč předchozí postup nefunguje pro prvočísla jiného tvaru, například $4k + 1$? Funguje obecně pro $ak - 1$ pro kterékoli dané $a \in \mathbb{N}$? Najdete další tvar, pro který důkaz funguje?
   (d) Ukažte, že každé liché prvočíslo p splňující $p \mid n^2 + 1$ pro nějaké $n \in \mathbb{N}$ musí být tvaru $4k + 1$.
   (e) Ukažte, že prvočísel tvaru $4k + 1$ je nekonečně mnoho. (Zkombinujte (d) a Eukleidův důkaz.)

7. Dokončete důkaz tvrzení 4.16. ve skriptech:
   (a) Ukažte chybějící implikaci: Pro liché prvočíslo tvaru $p = a^2 + 2b^2$ platí $p \equiv 1, 3 \pmod{8}$.
   (b) Pro prvočíslo p ukažte: p je tvaru $a^2 + 2b^2$, právě když p není prvočinitel v $\mathbb{Z}[\sqrt{-2}]$.

8. Uvažte obor $\mathbb{Z}[\frac{-1+\sqrt{3}\mathrm{i}}{2}]$ s normou danou $\mathrm{N}(x + y\sqrt{3}\mathrm{i}) = x^2 + 3y^2$.
   (a) Vyjádřete normu prvku $a + b\frac{-1+\sqrt{3}\mathrm{i}}{2}$ pro $a, b \in \mathbb{Z}$.
   (*b) Ukažte, že tento obor je eukleidovský.
   (c) Pro která prvočísla p existuje řešení kongruence $x^2 \equiv -3 \pmod{p}$?
   (*d) Charakterizujte prvočísla tvaru $a^2 - ab + b^2$. Postupujte jako v důkazu tvrzení 2.18.

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.
Úlohy s ! je doporučeno řešit přednostně.
Úlohy s $*$ jsou náročnější.