Teorie čísel: Cvičení 13

16. května 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@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 $n = q_1 \cdots q_k$ je součin (ne nutně různých) prvočísel a výrazy na pravé straně jsou Legendreovy symboly. Také definujeme $\left(\frac{a}{1}\right) = 1$.

Definice: Buď $N \in \mathbb{N}$ složené liché, $N - 1 = 2^e m, m$ liché. Pokud pro $0 < a < N$ platí, že

$$(\heartsuit) \quad \begin{cases} a^{m2^j} \equiv -1 & (\text{mod } N) \text{ pro nějaké } 0 \leq j < e, \text{ nebo} \\ a^m \equiv 1 & (\text{mod } N), \end{cases}$$

nazývá se N *silné pseudoprvočíslo v bázi* a, neboli a je *lhář* pro N. Naopak, pokud a nesplňuje podmínku $(\heartsuit)$, nazývá se a *svědek* složenosti N.

-2. Určete hodnotu výrazu $\left(\frac{477}{247}\right)$.

-1. Řešte kongruenci $x^2 \equiv 53 \pmod{77}$.

0. Najděte nějakého lháře různého od 1 a nesoudělného svědka pro
   (a) $N = 51$,
   (b) $N = 221$.

! 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. Vyšetřete vztah Jacobiho symbolů a kongruencí. Konkrétně:
   (a) Rozhodněte, jestli mají kongruence $x^2 \equiv 18 \pmod{127}$ 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. Najděte všechna $0 < a < 9$ taková, že a je lhář pro 9.

! 4. Najděte nějakého lháře různého od 1 a nesoudělného svědka pro
   (a) $N = 39$,
   (b) $N = 121$.

! 5. Najděte všechna $0 < a < 77$ taková, že a je lhář pro 77.

! 6. Pomocí Rabin-Millerova testu ukažte, že 7 je prvočíslo.

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

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