Cvičení 25. 4. 2012

Na vstupu máme liché číslo n a chceme vědět, zda je n prvočíslo.

Fermatův test: Pro dané n zkusit několik náhodně vybraných $0 < a < n$ umocnit na $n-1$. Pokud nám pokaždé vyjde 1, naznačuje to, že by n mohlo být prvočíslo.

Číslo n je Carmichaelovo, pokud skoro vždy generuje falešně pozitivní výsledek ve Fermatově testu: kdykoli je a nesoudělné s n, tak $a^{n-1} \equiv 1 \pmod{n}$.

Rabin-Millerův test: Mám zadané liché číslo n. To lze psát ve tvaru $n = 2^r s + 1$, kde s je liché. Zvolím si $a \in \{1, \ldots, n-1\}$. Pokud n je prvočíslo, tak buď $a^s \equiv 1 \pmod{n}$, nebo existuje $0 \leq j < r$ takové, že $a^{2^j s} \equiv -1 \pmod{n}$. Pokud ani jedna z těchto podmínek není splněna, je a (silný) svědek pro to, že n není prvočíslo.

Pokud Rabin-Millerův test dává pro dané a, n falešně pozitivní výsledek, nazveme a silným lhářem pro n a n pseudoprvočíslem v bázi a. Silných lhářů je málo (v množině $\{1, \ldots, n-1\}$ je jich méně než $n/4$), opakováním testu tedy můžeme libovolně zmenšit pravděpodobnost chyby.

Příklad 1. Dokažte, že $3 \cdot 11 \cdot 17 = 561$ je Carmichaelovo číslo.

Příklad 2. Nechť $p = 6m+1, q = 12m+1, r = 18m+1$ jsou prvočísla. Dokažte, že pqr je Carmichaelovo číslo.

Příklad 3. Aplikujte Rabin-Millerův test s hodnotami

1. $n = 7$, $a = 2$,
2. $n = 11$, $a = 2$,
3. $n = 25$, $a = 10$,
4. $n = 25$, $a = 7$,
5. $n = 25$, $a = 4$.

Příklad 4. Popište všechny svědky a silné lháře pro 49, 21, 25 a 45.

Příklad 5. Dokažte, že páté Fermatovo číslo $2^{2^5} + 1$ není prvočíslo.

Příklad 6. Dokažte, že pokud $(\varphi(n), n-1) = 2$, tak jediní silní lháři pro n jsou ± 1.