Cvičení 29. 3. 2013

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 $a \in \{1, \dots, n-1\}$. 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 $\{1, \dots, n-1\}$ je jich méně než $n/4$ – viz přednáška), opakováním testu tedy můžeme libovolně zmenšit pravděpodobnost chyby.

Příklad 1 (Opakování: Eulerova věta není optimální)**.** Jaké nejmenší $e \in \mathbb{N}$ můžeme zvolit, aby platila věta: „Pro každé a nesoudělné s 91 platí $a^e \equiv 1 \pmod{91}$“?

Příklad 2. Aplikujte Rabin-Millerův test s hodnotami

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

Příklad 3. Popište všechny svědky a silné lháře pro 9, 21, 49 a 105.

Příklad 4. Nechť p, q jsou prvočísla, $p \neq q$. Dokažte, že $n = pq$ není Carmichaelovo číslo.

Kreativní úlohy

Příklad 5. Může být p^n Carmichaelovo číslo pro p prvočíslo?

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

Příklad 7. Dokažte Wilsonovu větu: Číslo $p > 0$ je prvočíslo, právě když

$$(p-1)! \equiv -1 \pmod{p}.$$