Cvičení 19. 4. 2012

Jak testovat, zda dané (dlouhé) číslo je prvočíslo? Existuje na to polynomiální algoritmus, ale ten je pořád pro praktické použití pomalý.

Naivní metoda z Malé Fermatovy věty: Víme, že pokud je n prvočíslo, a číslo nesoudělné s n, tak $a^{n-1} \equiv 1 \pmod{n}$. Můžeme tedy 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. Toto je Fermatův test.

Problém: Existují složená čísla (říká se jim Carmichaelova) n taková, že kdykoli jsou a, n nesoudělná, tak $a^{n-1} \equiv 1 \pmod{n}$.

Příklad 1. Aplikujte Fermatův test (dva pokusy stačí) na čísla:

1. 313
2. 5467

Příklad 2. Dokažte, že $3 \cdot 11 \cdot 17 = 561$ je Carmichaelovo číslo.

Příklad 3. Nechť p, q jsou prvočísla, $p \neq q$. Dokažte, že $n = pq$ není Carmichaelovo číslo.

Příklad 4. Může být p^n Carmichaelovo číslo pro p prvočíslo?

Příklad 5. Nechť $p = 6m+1, q = 12m+1, r = 18m+1$ jsou prvočísla. Dokažte, že pqr je Carmichaelovo číslo.