MATEMATICKO FYZIKÁLNÍ FAKULTA UNIVERZITY KARLOVY
Malostranské nám 25, 118 00 Praha 1–Malá Strana

Bakalářská práce

Bc. Martin Franců: Test Rabina-Millera a volba báze

Posudek školitele.

Rozhodnout, zda dané číslo je prvočíslem, je otázka, kterou se matematici zabývají od nepaměti. A nalézt postup rychlejší, než postupné dělení menšími čísly, je při řešení této otázky klíčovou složkou. Od roku 2002 víme, že existuje deterministický algoritmus na určení prvočíselnosti, který je polynomiální v počtu cifer testovaného čísla (Agrawal-Kayal-Saxena), avšak běžně se používají i starší algoritmy pro svou snadnější implementaci, menší nároky na paměť a rychlost v oblasti menších čísel. Jedním z nich je test Rabina-Millera, který zesiluje klasický test Fermatův a test Eulerův. Stručně: Chceme určit, zda číslo N je prvočíslem. Zvolme číslo $b < N$, tak zvanou bázi, a počítáme čísla $b^k \mathrm{mod} N$, pro $k = N-1, \frac{N-1}{2}, \frac{N-1}{4}...$ tak dlouho, dokud je exponent celé číslo, nebo do prvního výskytu $b^k \not\equiv 1 \mathrm{mod} N$. Číslo je složené, pokud získaná posloupnost nemá tvar $1, 1, ..., 1$ ani tvar $1, 1, ..., 1, -1$. Rabinův-Millerův test však není deterministický: Pokud po jednom průchodu oznámí, že dané číslo je složené, pak je skutečně složené, v opačném případě se však může mýlit s pravděpodobností menší, než $\frac{1}{4}$. Z toho plyne potřeba, aby test proběhl vícekrát. Typická, běžně používaná volba bází je posloupnost několika prvních prvočísel.

Bc. Martin Franců dostal za úkol testovat jiné možnosti voleb bází a tohoto zadání se s úspěchem zhostil. Napsal program, který bezchybně funguje, je uživatelsky přátelský a umožňuje různé možnosti voleb bází vyhodnocovat. Jako testovací množiny použil množinu všech lichých čísel menších, než 200 000 000 a množinu všech silných pseudoprvočísel menších než 10^{12}. V obou případech se ukázalo, že některé z jeho voleb jsou efektivnější, než postupná volba malých prvočísel.

Práce je rozvržena do čtyř kapitol. V první kapitole jsou uvedeny základní prvočíselné testy a některé věty z teorie čísel, které se týkají problematiky práce, posléze je vysvětlen algoritmus Rabinova-Millerova testu. V druhé kapitole je popis užitých voleb bází a shrnutí získaných výsledků. Třetí kapitola obsahuje uživatelskou dokumentaci k vyvinutému programu a čtvrtá programátorskou dokumentaci. Práce napsána velice pečlivě s minimem tiskových chyb a dobře osvětluje vyšetřovanou problematiku.

Podle mého soudu Bc. Martin Franců odevzdal nadprůměrně kvalitní bakalářskou práci a doporučuji, aby po jejím obhájení mu byl udělen titul Bakalář informatiky.

V Praze, 22. září 2011

prof. RNDr. Petr Simon, DrSc.
školitel.