

Lukáš Perůtka: Hledání optimálních strategií číselného síta
POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Předloženou diplomovou práci považuji za vynikající. Zhruba na čtyřiceti stranách jsou shrnuty prakticky všechny poznatky z algebraické teorie čísel, které jsou potřebné pro pochopení a implementaci algoritmu číselného síta. Jistá část z nich má charakter standardní kursovní látky, kterou nebylo nezbytně nutné uvádět. Jejím uvedením však výklad získal charakter samostatného pojednání, které je natolik kvalitní, že ho lze nabídnout jako studijní materiál i těm, kteří daný kurs neabsolvovali.

Na dalších čtyřiceti stranách se podrobně rozebírají jednotlivé fáze algoritmu. Text je velmi zdařilý a vhodným způsobem spojuje popis vlastního algoritmu s výkladem matematického zdůvodnění jeho správnosti.

V samém závěru je pojednáno měření vycházející z implementace, na které se diplomant aktivně podílí. Výsledky měření vedly k určitým změnám v implementaci. Bohužel u vybraného stociferného prvočísla se přesto nepotvrdilo očekávání vycházející z publikací jiných autorů, podle kterého při délce sto cifer by mělo mřížové prosívání být efektivnější než klasické, a také by se měla projevit jako efektivnější metoda dvou kvadratických polynomů. Lze očekávat, že dalším zdokonalením implementace se podaří tento rozpor vyjasnit.

V textu lze občas najít chybějící čárky či mezery. Počet jazykových prohrěšků je však natolik malý, že nestojí za podrobný komentář.

Doporučuji, aby práce byla uznána jako diplomová a hodnocena známkou

Ujbně

V Praze 18. května 2009

Aleš Drápal *Ujbně*