POSUDEK DIPLOMONÉ PRÁCE "HLEDÁNÍ OPTIMÁLNÍCH STRATEGIÍ ČÍSELNÉHO SÍTA"

LUKÁŠ PERŮTKA

Práce sestává ze tří částí. V první je vybudován teoretický základ potřebný k pochopení použitých faktorizačních metod. Jde o vybrané základní i speciální partie z komutativní algebry. Druhá část sestává z popisu algoritmu číselného síta. Tento algoritmus se skládá z několika kroků, každému z nich je věnována samostatná kapitola. V poslední části je popsaný algoritmus použit k porovnání efektivnosti různých metod použitých ve vybraných (fáze prosívání) krocích algoritmu. Zhodnoťme nejprve jednotlivé části.

V první části, odpovídající Kapitole 2, jsou rozebrány základy algebraické teorie čísel doplněné o některé rozšiřující pasáže potřebné k teoretickému základu dále popisovaného algoritmu. Zde mám několik výhrad k popisu základů teorie, které by měly být zpracovány pečlivěji. Například v Lemmatu 2.3 není jasné odkud je prvek ρ, v důkazu Lemmatu 2.4 nestačí aby byl $\mathbb{Z}[\vartheta, \mu]$ konečně generován jako okruh, v důkazu Lemmatu 2.11 je zbytečné uvažovat množinu $I = \{1, \ldots, n\}$, v důkazu Lemmatu 2.27 neplyne z $(m) \subseteq I$, že $O_K/I \subseteq O_K/(m)$, argumentace v důkazu Věty 2.29 (iii) vedoucí k použití Lemmatu 2.3 je nepřesná.

Ve druhé části je nejprve popsán algoritmus číselného síta a po té jsou podrobněji rozebrány jeho jednotlivé části. Zde jde zřejmě o popis metod nikoli o přesný matematický text (s výjimkou např. sekce 3.5.1). Místy je to na úkor srozumitelnosti. Otázkou je jaký by měla práce rozsah v případě, že by vše bylo podrobně zdůvodněno.

Poslední kapitole se na příkladu konkrétního 100 ciferného čísla testují popsané prosívací metody.

Domnívám se, že v práci je popsána netriviální praktická aplikace vyžadující rozsáhlé teoretické znalosti. Vzhledem k náročnosti úkolu navrhuji hodnotit práci, i přes výše uvedené připomínky, výborně.

[redacted]