Posudek vedoucího bakalářské práce
Malé kořeny celočíselných polynomů více proměnných
Dory Todorovové

V devadesátých letech představil D. Coppersmith metodu pro hledání řešení kongruencí $f(r) \equiv 0 \bmod N$, kde $f \in \mathbb{Z}[x]$, $N \in \mathbb{N}$ je (velké) číslo s neznámou faktorizací a $r \in \mathbb{Z}$ splňuje $|r| < \delta$, kde δ je nějaká vzhledem k N poměrně malá mez. Kryptografickou motivací tohoto problému byl útok na RSA s malým veřejným exponentem e, kdy f je tvaru $x^e - c$, kde c je zašifrovaná zpráva a N je RSA modulus. Coppersmithova metoda byla dále rozvíjena, například D. Boneh a G. Durfee představili její variantu pro polynomy dvou proměnných, konkrétně studovali metodu pro hledání řešení kongruence $x(A + y) - 1 \equiv 0 \bmod N$, kde $|x| < N^{0.297}$ a $|y| < N^{0.5}$ (tento problém je opět motivovaný útokem na RSA).

V rámci bakalářské práce se měla studentka seznámit s touto vícerozměrnou variantou Coppersmithovy metody. V první kapitole je shrnuta základní teorie mřížek v rozsahu nezbytném pro pochopení dalších kapitol. Ve druhé kapitole je představen hrubý postup z výše zmíněné práce Boneha a Durfeeho doplněný o některé drobné detaily, v sekci 2.2 je pak představeno obecné schéma pro hledání malých kořenů polynomiálních kongruencí ve více neurčitých podle článku E. Jochemsze a A. Maye z roku 2006. Je nutno dodat, že se jedná skutečně jenom o schéma, pomocí kterého je možné sestavit konkrétní algoritmus až po poměrně složité analýze, kterou je potřeba provést pro každý konkrétní typ polynomu. Práci uzavírá třetí sekce, kde jsou konkrétněji propočítány dva typy polynomů - lineární polynom ve třech neurčitých a polynom tvaru $axy + bx + c$ podle základního postupu v článku Jochemsze a Maye.

První kapitola je zpracována solidně, druhou kapitolu jsem si představoval napsanou trochu srozumitelněji. Je pravda, že zdrojové články, obzvláště článek Jochemsze a Maye, jsou poměrně obtížně čitelné a stručné a autorka měla tendenci se od nich příliš neodchylovat. Dovysvětlující poznámky, které jsem navrhoval, zapracovávala zpravidla dost minimalisticky. Určité potíže by též mohl způsobit fakt, že stanovení oblasti, ve které budeme hledat řešení kongruence (tedy hodnota δ na straně 11 a vzorec (2.1) na straně 14), není provedeno pomocí přesného výpočtu, jsou ignorovány členy, jejichž vliv na stanovenou mez by při realistických volbách parametrů nebyl zásadní.

Z časových důvodů se bohužel nepodařilo zařadit ani malý příklad s konkrétním vstupem do sekce 2.1, ani detailněji provedený příklad 3.1 (bez zanedbávání 'nepodstatných členů'). Obojí by přispělo k pochopení způsobu, jak z uvedených úvah sestavit konkrétní algoritmus.

Předložená práce z větší části splnila zadání, i přes uvedené výhrady ji proto navrhuji uznat jako práci bakalářskou.

V Praze, 2. 9. 2020

Pavel Příhoda