Posudek oponenta k bakalářské práci
Krátké invertibilní prvky v cyklotomických okruzích
Jaroslava Kroutila

Předložená práce představuje nedávno publikovaný důkaz věty Lyubashevského a Seilera o invertibilitě krátkých prvků cyklotomického okruhu (Věta 35). Konkrétněji, pokud $z, m \in \mathbb{N}$, z je dělitel m dělitelný každým prvočíselným dělitelem m a $p \in \mathbb{P}$ splňuje $p \equiv 1 \pmod{z}$ a $\mathrm{ord}_{\mathbb{Z}_m^*}(p \bmod m) = m/z$, pak je stanoveno kriterium invertibility prvků okruhu $R_{m,p} = \mathbb{Z}_p[x]/(Q_m^p)$, kde Q_m^p je m-tý cyklotomický polynom nad $\mathbb{Z}_p$. Kriterium je dáno velikostí vektoru koeficientů polynomiálního reprezentanta prvku $R_{m,p}$. Invertibilita prvků v cyklotomických okruzích je téma s možnými aplikacemi v různých kryptografických konstrukcích (NTRU, multilineární zobrazení apod.).

Práce je rozdělena do 4 kapitol, první kapitola obsahuje základní definice a věty. Ve druhé kapitole je v Tvrzení 16 ukázána za určitých omezení existence nekonečně mnoha prvočísel, pro která lze aplikovat Větu 35. Třetí kapitola se zabývá cyklotomickými polynomy, hlavním cílem je nalezení ireducibilního rozkladu polynomu Q_m^p (Tvrzení 28). Ve čtvrté kapitole je pak proveden vlastní důkaz hlavní věty.

Hlavním přínosem práce je podrobné a až na důkaz Lemmatu 32 kompletní představení důkazu Věty 35. Až na pár nepřesností (uvádím níže) je text srozumitelný a korektní. Autor dále doplnil 3 příklady demonstrující algoritmické uchopení předvedených důkazů.

Celkově si myslím, že zadání práce bylo splněno a uvedenou práci proto doporučuji uznat jako práci bakalářskou.

V Praze, 2. 9. 2019

Pavel Příhoda

Připomínky k práci (seřazeno dle závažnosti)

- Lemma 32 pravděpodobně není převzato správně. Pokud existuje nekonečně mnoho prvočísel p pro pevně daná m a z, pak pravá strana nerovnosti může být libovolně velká. Navíc ve verzi článku Lyubashevskeho a Seilera na eprint.iacr.org je Lemma 2.7 zformulováno pouze pro ideálové mřížky.
- V důkazu Tvrzení 34 se hledá ireducibilní rozklad Q_z^p dosazením $x^{z/m}$ do Q_m^p. Aby byl argument korektní, bylo by třeba specifikovat okruh, ve kterém výpočet probíhá. Tím, že z/m není celé číslo, si nevystačíme s okruhem polynomů.
- Podobný problém je v důkazu Tvrzení 25 - není specifikována grupa $\mathbf{G}$. Navíc by mělo být definováno $h(n)$ i pokud $p \mid n$.

- K Tvrzení 16 by se možná hodil komentář, že m/z je nejvyšší řád, který může p mod m mít. Asi by byl vhodný i komentář, zda je předpoklad $8 \mid m \Rightarrow 4 \mid z$ nutný.
- V posledním odstavci důkazu Tvrzení 28 nejspíš potřebujeme $k = m$ a $b \not\equiv 1 \pmod{m}$.
- V definici generátoru na str. 3 by mělo být $n \in \mathbb{Z}$.
- V definici okruhu na str. 3 by mělo být komutativní místo aditivní.
- Hodnost volného modulu (str. 4) lze takto definovat pouze pro komutativní okruhy.
- Na některých místech je argumentace trochu těžkopádná. Např. v důkazu Tvrzení 33 by bylo možno počítat $|R_{m,p}/L_p|$ jako $|\mathbb{Z}_p[x]/(x^{m/z} - r_j)|$.
- Tvrzení 11 a Tvrzení 12 by bylo lepší formulovat pro komutativní grupy, nebo pro obory hlavních ideálů. Formulace 'Mějme $\mathbb{Z}$ obor hlavních ideálů' mi nepřijde vhodná.
- Určitě by bylo možné práci vylepšit z typografického hlediska, např. v Lemmatu 7 psát NSD(k, l) místo NSD(k,l). V Lemmatu 31 $R_{m,p}$ místo $\mathbb{R}_{m,p}$.
- Dále pár překlepů, vzhledem k rozsahu práce v přijatelné míře.