Posudek vedoucího na diplomovou práci Adély Haníkové nazvanou
Eliptické křivky a testování prvočíselnosti

Jde o práci, která má rozměr teoretický i aplikační. Je patrné, že autorce nečiní problémy orientace v abstraktních pojmech, což přispívá k příznivému dojmu z práce. Matematické vyjadřování je kvalitní, až na několik formálních drobností: odkazy na rovnice by měly být závorkované, tedy (3.3) a ne pouze 3.3. Stejně je třeba hovořit o části nebo podkapitole 3.4, a ne pouze odkázat na 3.4 bez upřesnění. Tak, jak je to napsaáno, je občas třeba přemýšlet, která z obou možných interpretací platí. Dále na vícero místech chybí odkaz do literatury (například poslední odstavec strana 10 nebo Věty 3.3 a 3.4).

Práci lze rozložit na dvě zhruběstejné a relativně nezávislé části. Prvni část by bylo možno nazvat *Okolo Edwardsových křivek*. V ní autorka využívá své znalosti algebraických funkčních těles k tomu, aby osvětlila některé jejich vlasnosti. Je tam několik výsledků, které sice nejdou za rámec variací na základní vlastností eliptických funkčních těles, ale přesto je lze považovat za netriviální a originální, tedy nepřevzaté z literatury. Sem patří odvození rodu přímočaře z vlastností příslušného funkčního tělesa, tedy bez využití obecnějších vět, zkoumání prvků řádu čtyři, určení nevlastních míst využtím divisorů a přímočaré odovození sčítání na Edwardsově křivce. Výsledky zde uvedené považuji za zdařilý počin, který má svůj smysl v rámci celé práce, protože dává pevnější základ následným aplikacím. Některé věci však mohly být dotaženy o něco dále a také celkové uspořádání mohlo být lépe organizované. Tvrzení 3.6 mohlo být využito k úplnému výkladu struktury prvků řádu 4. V samém závěru podkapitoly 3.3 není komentována možnost $\mathbb{Z}_2 \times \mathbb{Z}_4$. Geometrickému pohledu by prospěl výklad, že použité hyperboly vlastně vytvářejí model projektivní roviny, a úvaha, zda tento model nevzniká nějakou konkrétní racionální transformací. Drobnost: Lemma 3.1 platí i pro $d = 0$.

Druhá část práce se věnuje nejprve popisu Lenstrova faktorizačního algoritmu a jeho adaptace z Weierstraßových křivek na Edwardsovy. Tento popis vychází z volby parametru d. V podkapitole 4.4 je vysvětleno, jak se výpočty dají realizovat bez jeho přímé účasti. Trochu mne mate, proč je vůbec v Algoritmu 4.4 parametr d uveden jako jedna ze vstupních hodnot. Prosím o vysvětlení během prezentace. Závěrečná kapitola je věnována implementaci, s komentáři týkajícími se grafických karet, aritmetiky velkých čísel a měření. To, že algoritmus byl úspěšně naprogramován, považuji za velmi důležitou součást práce. Trochu mi je ale líto, že z tohoto procesu nevzešla žádná otázka, která by se bývala stala podnětem pro nějaký vlastní výzkum.

V druhé části lze tu a tam nalézt překlep, například v důkazu tvrzení 4.4 by nemělo figurovat jenom p, ale také q. Nadpis podkapitoly 4.3.3 zní *Volba paramterů*.

Nedostatky výše zmíněné by neměly zastínit fakt, že celkově jde o diplomovou práci, která je šíří záběru, porozuměním tématu i zvládnutím používané matematiky na vysoké úrovni.

Navrhuji, aby práce byla přijata jako práce diplomová a hodnocena stupněm *výborně*.

Aleš Drápal
V Dolním Údolí 24. srpna 2015