Oponentský posudek na diplomovou práci

Adéla Haníková: Eliptické křivky a testování prvočíselnosti

Předložená práce se zabývá využitím eliptických křivek pro rozklad přirozených čísel na prvočísla. Obsáhlý celek lze rozdělit na tři hlavní části:

1. diskuze teorie algebraických křivek s důrazem na eliptické křivky v Edwardsově tvaru,
2. vysvětlení a optimalizace faktorizačního algoritmu,
3. implementace algoritmu s využitím paralelizace výpočtu pomocí grafických karet.

Práci považuji za velice zdařilou, všechny body ze zadání byly bez pochyby splněny. Výsledný text je na dobré matematické úrovni, přestože totéž by jistě o všech použitých zdrojích říci nešlo. Uvádím seznam vesměs drobnějších připomínek a otázek:

1. V definici valuačního okruhu na str. 6 by R měl být obor integrity, abychom vůbec mohli mluvit o podílovém tělese. Stejně tak musí být R obor v charakterizaci DVO nahoře na straně 7 (okruh $\mathbb{Z}/(4)$ je noetherovský lokální okruh s hlavním max. ideálem, ale ne DVO).
2. U některých tvrzení v první kapitole bych považoval za vhodné uvést přesnější citaci, kde zhruba lze v knihách výsledek najít. Text by pak byl více přístupný. Konkrétně jde o lemmata 1.5, 1.6 a větu 1.8. Nechybí navíc u inverzní Hasseho věty u členů $\sqrt{q}$ násobení dvěma?
3. V lemmatu 2.1 na str. 13 mi není jasná ekvivalence mezi ireducibilitou a absolutní ireducibilitou polynomu $g = x_2^2 - f(x_1)$. Co když $K = \mathbb{R}$, $f = -x_1^4$ a $g = x_2^2 + x_1^4$? Pak g je ireducibilní v $\mathbb{R}[x_1, x_2]$ (netriviální faktor by byl lineární v x_1), ale $g = (x_2 - ix_1^2)(x_2 + ix_1^2)$ v $\mathbb{C}[x_1, x_2]$.
4. Jak přesně v prvních dvou řádcích na str. 15 z předchozího plyne, že $y \in K(x)$?
5. U odkazů na rovnice by bylo lepší používat příkaz TeXu `\eqref` než `\ref` (vyskytuje se např. na str. 23, 25 a dalších). Takto není někdy z kontextu úplně jasné, jestli jde o odkaz např. na rovnici 3.2 nebo tvrzení 3.2, což trochu ztěžuje orientaci v textu.
6. V prvním řádku kap. 3.3.2 (str. 24) by mělo být $(y^2 - d^{-1})(x^2 - d^{-1}) = d^{-1}(d^{-1} - 1)$.

7. Argument na začátku kap. 3.4, str. 26, že nenulovost $1 \pm dx_1x_2y_1y_2$ vyplývá v kap. 3.3.1, mi nepřipadá úplně zřejmý. Stále zbývá zdůvodnit, proč by podíly definující součet bodů v grupě křivky nemohly být tvaru $\frac{0}{0}$ a nebylo by tedy nutné hledat jiné vyjádření definujících racionálních funkcí.

8. Lemma 4.1 a jeho použití v důkazu tvrzení 4.2 je vysvětleno dosti nejasně. I tady by mohla pomoci přesnější citace, je-li k dispozici. Argument v tvrzení 4.2 by nejspíše měl být formulován tak, že pokud je kP definováno (tj. výpočet nenašel netriviálního dělitele N) a $kP_p = \mathcal{O}_p$, pak nutně $kP = \mathcal{O}$.

9. V prvním vzorci pro X_3 na str. 42 je překlep.

Předloženou práci **doporučuji uznat jako diplomovou** a hodnocení pro komisi přikládám na zvláštním listě.

V Barceloně dne 3. 9. 2015 doc. RNDr. Jan Šťovíček, Ph.D.