Posudek oponenta bakalářské práce

Název: Algoritmy dokazující prvočíselnost
Autor: Jiří Pavlů

Shrnutí obsahu práce

Předložená práce představuje Goldwasserův-Killianův test prvočíselnosti spolu s přehledem potřebných teoretických nástrojů z algebraické geometrie. Text kromě úvodu a závěru sestává ze čtyř částí. Zatímco je poněkud solitérní první kapitola věnována stručnému nástin několik testů prvočíselnosti (Lucas-Lehmer-Rieslerův, Prothův, Pocklingtonův a Agraval-Kayal-Saxenův test), další dvě části obsahují úvod do teorie projektivních algebraických křivek a její použití pro práci s grupovou operací danou na bodech afinní eliptické křivky. Těžiště práce spočívá ve čtvrtá kapitole, v níž je popsán a analyzován samotný Goldwasserův-Killianův test.

Celkové hodnocení práce

Téma práce. Přestože bylo téma poměrně obtížné, bylo přiměřené nároku na bakalářskou práci. Zadání bylo studentem podle mého mínění úspěšně naplněno.

Vlastní příspěvek. Student zasadil popis Goldwasserova-Killianova algoritmu do kontextu teorie, která není v plném rozsahu obsahem bakalářského studia. Vedle porozumění popisovaného textu bylo potřeba části obsáhlé teorie nastudovat a ve stručné podobě prezentovat.

Matematická úroveň. Matematická úroveň práce je uspokojivá a formulace jsou až na několik výjimek vesměs korektní. Nejlépe je zpracována klíčová čtvrtá kapitola. V druhé a třetí kapitole nejsou některé partie dostatečně matematicky věrohodné a srozumitelné (viz připomínky níže). První část je do textu pravděpodobně zařazena jen s ohledem na plurál použitý v názvu a podle mého mínění by bylo vhodnější na její úkor rozšířit některé příliš stručné části druhé a třetí kapitoly.

Práce se zdroji. Text práce je výběrovou kompilací různých zdrojů, na nichž zjevně není příliš formulačně závislý.

Formální úprava. Formální náležitosti práce nezasluhují žádné podstatnější výtky. Ač jsou některé formulace poněkud neobratné, je množství jazykových a stylistických nepřesností úměrné rozsahu práce.

Připomínky a otázky

1. s.4, ř.3 sekce 1.3 - není vysvětleno, co je p.
2. s.4, ř.11-13 sekce 1.3 - sluší se poznamenat vzhledem k čemu uvažujeme polynomiální časovou složitost či jak měříme počty čísel a.
3. s.5, Poslední věta v důkazu Lemmatu 2 patří k důkazu přímé implikace (tedy na 2. řádek důkazu).
4. s.6, používaný pojem projektivní přímky stálo za to korektně definovat.
5. s.10, Definice 10 bod 1, je někde vysvětleno, co s míní ,,protínáním" křivek?

6. s.10, po Definici 10 by stálo za to aspoň poznamenat, že zavedené I je podmínkami jednoznačně určeno (mimochodem, pojem je ve Fulltonově textu, na nějž je definice odkázána, zaveden v afinním, nikoli projektivním prostoru).

7. s.10 5.-2, (nejen) pro účely Definice 13 by $\mathcal{O}_P(\mathbb{P}_2)$ mělo být zavedeno jako okruh (nikoli jen množina).

8. s.11, v Definici 12 by stálo za to zavést i sčítání průnikových cyklů.

9. s.14, co znamená symbol $*$ ve výrazech $y = s * x + b$ a $(L + L) * q/2$?

10. s.15, co rozumíme racionální funkcí nad obecným $\mathbb{Z}_n$?

Závěr

Přes uvedené drobné výhrady doporučuji práci uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
15.9.2016