Igor Eržiak: Counting points on elliptic curves over finite fields

Posudek oponenta

V práci je popsán Schoofův algoritmus, který pro danou eliptickou křivku nad konečným tělesem spočte počet jejích bodů. V prvních dvou kapitolách je shrnuta teorie nutná k popisu algoritmu, ve třetí je uveden samotný algoritmus, sepsaný v jazyku systému Sage. Díky implementaci je zřejmé, že student musel algoritmus pochopit.

Po obsahové stránce je práce na solidní úrovni. Teorie je stručná, ale jasně směřuje k vytčenému cíli, popisu algoritmu. Ten je uveden ve formě programu v Sage, ale je napsán dostatečně srozumitelně, aby se v něm čtenář vyznal. Občas mi chybí širší kontext. Např. v kapitole 2.2 bylo možné uvést, že grupovou operaci lze definovat s libovolnou nulou, přičemž výběr bodu v nekonečnu je motivován hezkými rovnicemi pro grupovou operaci. Definice polynomů psi_n není dobře motivovaná, jejich význam je uveden až později. Definice 2.1 do jisté míry opakuje definici 1.1. Ale nejde o nic, co by znemožnilo text číst.

Chybí mi časový odhad složitosti vzhledem k velikosti tělesa. Uvádí jej literatura? Liší se odhad od skutečnosti? Analýza výsledků by bývala práci obohatila.

Po stránce formální a jazykové je práce výborná.

Poslední připomínka: Z textu bohužel není dobře poznat, co je přesně autorovým přínosem, co práce obsahuje navíc proti předloze (kromě implementace). Prosil bych okomentovat při obhajobě.

Text splňuje nároky kladené na bakalářskou práci a prokazuje schopnost samostatné práce v matematice. *Práci navrhuji uznat jako bakalářskou.*

Ve Špindlerově Mlýně 3.9.2018
David Stanovský