Posudek vedoucího na bakalářskou práci

Jiří Pavlů: Algoritmy dokazující prvočíselnost

Práce se zabývá algoritmy, pomoci nichž je možné s jistotou ověřit, že nějaké číslo je prvočíslo. Důraz je kladen na popis a analýzu složitosti Goldwasserova-Killianova algoritmu, který umožňuje pro dané číslo vygenerovat rychle ověřitelný „certifikát prvočíselnosti“. Jelikož algoritmus využívá eliptické křivky, které nejsou v náplni bakalářských přednášek, jsou v práci též zavedeny.

Cíl práce považuji za splněný. Téma jsem vypsal na přání autora a i práci (včetně celkového pojetí) zpracoval velice samostatně. Finalizace práce byla bohužel poněkud uspěchaná, což se na několika místech projevuje nekonzistencí značení (např. v definici 9 na str. 8 jsou křivky definovány coby množiny bodů, zatímco v definici 10 je bez vysvětlení použita obecnější konvence z Fultonovy knihy, kde jsou za křivky považovány nenulové polynomy až na nenulový skalární násobek). Celkově je však práce dobře napsaná a srozumitelná.

Práci **doporučuji k obhajobě** a návrh hodnocení přikládám zvlášť.

V Praze dne 20. 6. 2016 doc. RNDr. Jan Šťovíček, Ph.D.