Hodnocení oponenta bakalářské práce

Autor práce: **Petra POJAROVÁ**

Název práce: **Klasické i moderní faktorizační algoritmy**

Splnění bodů zadání

úplně

Formální úroveň

Průměrné

Práce s literaturou

Průměrné

Slovní hodnocení

ad Splnění bodů zadání
Nad rámec úkolů popsaných v zásadách pro vypracování autorka zařadila opakování základních pojmů, užití faktorizace v RSA-metodě, Euklidův algoritmus, testování prvočíselnosti, polynomickou faktorizaci, životopisy P. Fermata, L. Eulera a Shanksovu čtvercovou faktorizační metodu. Tento text tvoří zhruba polovinu bakalářské práce.
ad Formální úroveň
Práce je dobře logicky členěna do kapitol a podkapitol. Je napsána srozumitelně a z hlediska grafického přehledně. Na některých místech se objevují pravopisné chyby ("s čísli" na str. 9, 12; "projít všechny prvočísla" na str. 21, "Práci mu komplikovali úřední povinnosti…" na str. 27), někde chybí čárky (str. 13_1, str. 15_4, str. 20_{11}, …). Počet překlepů je přiměřený rozsahu práce. Jsou-li v matematickém zápisu, mohu komplikovat porozumění textu (např. str. 7_1, str. 8^5, str. 10^7, str. $12_{13,14}$, str. 15_2). V práci se nevhodně píše o rovnicích (např. str. 11, str. 21). Na str. 4 je nepatřičně psáno "dělitelné jedničkou, ... a dvojkou", v tabulkách na str. 7 a 13 jsou nešikovně zvolena písmena pro proměnné v zápisu n_n. Celá část čísla je v práci značena dvěma různými způsoby (např. str. 23). Na přiloženém CD/DVD není zdrojový dokument bakalářské práce (viz Vyhláška děkana č. 1VD/2018, Proces zadávání, odevzdávání a vypracování kvalifikační práce, bod 14).
ad Práce s literaturou
V seznamu použitých zdrojů mají značnou převahu internetové zdroje. Tištěné zdroje mohly být vyčleněny a uspořádány abecedně podle autora. Zdroje jsou v práci citovány uvedením čísla ze seznamu literatury. Nelze tedy snadno zjistit, jakým způsobem byl zdroj použit (doslovné převzetí textu, převzetí s úpravou, ...).
Vlastní přínos autorky lze spatřovat ve způsobu prezentace algoritmů a v příkladech, na kterých se je snažila objasnit. Faktorizační postup podle D. Shankse by zasluhoval aspoň krátké nebo částečné vysvětlení, proč se má postupovat tak, jak je uvedeno. Jinak představuje jen „kuchařku“, které má čtenář plně důvěřovat. Příklad 16 považuji za nadbytečný, volí se v něm stejná mez B a stejné celé číslo a jako v příkladě 15. Na str. 47 – 49 je uveden souhrn faktorizačních postupů, nelze ho však považovat za srovnání těchto metod. Porovnání je zcela ponecháno na čtenáři.

Dotazy k práci

(1) Vysvětlete, co znamená hodnota celého čísla, viz str. 2.
(2) Najděte faktor čísla 121 podle pravidla na str. 19, které omezuje výběr prvočísel k pokusnému dělení.
(3) Objasněte, jak je to s předpokladem nesoudělnosti a a p v Malé Fermatově větě na str. 36.
(4) Srovnejte Fermatovu faktorizační metodu a metodu kvadratického síta.

Doporučení k obhajobě

velmi dobře

V -------------------- dne --------------------

Mgr. Martina Kašparová, Ph.D.