Oponentní posudek diplomové práce Bc. Stanislava **Heflera** studijní program B1001 Přírodovědná studia, na téma

„Prvočísla a faktorizace celých čísel“.

Práce se zabývá částí teorie čísel, především prvočíselností a faktorizací celých čísel. Práce je velmi rozsáhlá, zahrnuje cca 70 stránek textu. Je vhodně doplněna kvalitními volnými obrázky. její grafická úroveň je velmi vysoká.

Obsahuje větší množství definic a především vět, z nichž je část přímo dokázána. Velmi pěkně jsou zakomponovány historické souvislosti.

V první části práce se autor věnuje prvočíslům. Uvádí různé metody prvočíselného rozkladu, ale i prvočíselných testů. Zároveň je ukázáno i na problematiku chybných závěrů z těchto testů.

Druhá část práce je věnována pseudoprvočíslům. Autor uvádí známou definici i výčet Fermatových pseudoprvočísel do 1000 pro základy do čísla 22. Nezabývá se jen Fermatovými čísly, ale definuje a určuje Carmichaelova pseudoprvočísla, Eulerova a silná pseudoprvočísla.. Na základě takovýchto definic pseudoprvočísel jsou uvedeny definice a užití silnějších prvočíselných testů. V kapitole 2.3 jsou uvedeny moderní prvočíselné testy, které jsou zavedeny například do software Mathematica. Tyto testy jsou založeny na některých speciálních rovnostech, které platí jen pro prvočísla. Tyto testy jsou velmi rychlé. V části 2.4 autor porovnává funkce a procedury několika matematických počítačových programů.

Třetí část se zabývá problematikou faktorizace čísel. Jsou ukázány některé dnes již historické metody jako například metoda opakovaného dělení, Fermatova faktorizační metoda, Eulerova faktorizační metoda a klasický Euklidův algoritmus.

Na tyto základní metody navazuje čtvrtá část s moderními metodami faktorizace: Pollardova p-1 metoda, Pollardova ρ metoda a další moderní metody. Nejenže je u jednotlivých metod popsán algoritmus, ale autor metody vždy aplikuje na konkrétní úlohy.

Poslední pátá část je zaměřena výhradně na použití prvočísel v praxi. Je zde jednoduše popsán šifrovací algoritmus RSA s ukázkami generování klíče, zašifrování zprávy a dešifrování zprávy. Podobně je popsán tzv. elektronický podpis.

Práce je velmi pěkně zpracována, jak po odborné stránce, tak i po grafické. Práci doporučuji k obhajobě a navrhuji známku **výborně.**

RNDr. Václav Kohout.

V Plzni dne 23.4 2015