

Oponentský posudek bakalářské práce

Autor práce: Ivan Štubňa

Název: Klasické metody faktorizace čísel

Vedoucí: David Stanovský

Hlavním cílem práce Ivana Štubni je popis a matematické zdůvodnění čtveřice klasických algoritmů prvočíselného rozkladu: pokusného dělení, Lehmanova algoritmu, Pollardovy p-1 metody a Pollardovy ρ -metody. Součástí práce jsou i implementace popsaných algoritmů na přiloženém CD a porovnání implementací. Text je rozčleněn do šesti částí. Po úvodu následují dvě kapitoly, v nichž je kromě popisu základních algoritmů zaveden matematický aparát potřebný v odhadech časové složitosti. Popisu a časové složitosti jmenovaných faktorizačních algoritmů včetně kompletních důkazů je věnována rozsáhlá čtvrtá kapitola. Testování jednotlivých implementací a porovnání výsledku testů se věnuje předposlední pátá část, po níž následuje závěr.

Třebaže zpracované algoritmy mají exponenciální časovou složitost, tedy jsou asymptoticky horší než moderní algoritmy na faktorizaci čísel, je téma bezpochyby zajímavé a aktuální, neboť jsou tyto algoritmy v některých případech stále využívány. Téma práce je zpracováno neobyčejně pečlivě a student prokázal schopnost práce s odbornou literaturou. Po matematické ani jazykové stránce se textu nedá téměř nic vytknout, oponent jiné nedostatky než několik málo překlepů nezaznamenal (například označení kroku 5. Algoritmu 4.3 bezprostředně za algoritmem číslem 6.). Škoda, že část porovnávající implementace algoritmů nezahrnuje srovnání s některou z moderních metod faktorizace, takové rozšíření textu, jehož těžiště spočívá v teoretickém popisu algoritmů, by však pravděpodobně příliš překračovalo obvyklý rozsah bakalářské práce.

Předkládaná práce zjevně bezezbytku splnila cíle kladené v jejím zadání, proto ji doporučuji uznat jako bakalářskou a navrhoji ji ohodnotit známkou výborně.

oponent: Jan Žemlička