

Abstrakt: Práce se zabývá různými způsoby volby báze v Rabinově-Millerově testu. V teoretické části je učiněn krátký přehled prvočíselných testů podobných Rabinovu-Millerovu testu a je dokázáno několik tvrzení o struktuře množiny silných lhářů v multiplikatívni grupě. Vybrané netradiční volby báze jsou otestovány na množině lichých složených čísel od 100 do 200 000 000 a výsledky jsou porovnány s výsledky při obvyklé volbě báze. Je vyslovena domněnka o vylepšení testu prostřednictvím používání bází určitého tvaru vzhledem k testovanému číslu. Součástí práce je také program, který implementuje posuzované způsoby volby báze. Tento program umožňuje uživateli pohodlné srovnávání výsledků testů s různými způsoby volby báze. V druhé části práce je dokumentace programu.

Seznam tabulek

2.1	Výsledky testů s různými volbami báze na testovací množině. . . .	19
2.2	Výsledky testů s různými volbami báze na $\text{spsp}(2,3,5) < 10^{12}$ z článku [7].	20
3.1	Typy zpráv.	28
4.1	Třídy hledačů bází.	32
4.2	Názvy a funkce reportérů.	33

Seznam obrázků

2.1	Hustota lhářů v závislosti na poměru lháře ku testovanému číslu.	18
3.1	Založka „one test“	22
3.2	Založka „file tester“	23
3.3	Založka „pseudoprime generator“	24