Hodnocení bakalářské práce Gabriely Stuchlíkové,
Přírodovědná studia, obor matematická studia, na téma
„Testování prvočíselnosti“.

Moderní šifrovací metody (RSA šifrování) podstatným způsobem využívají velká prvočísla p, q, jejichž součin pq je „těžké“ rozložit a tím je v současnosti garantována neprolomitelnost šifry. Tím ovšem narostla potřeba ověřovat, že jistá „velká“ přirozená čísla jsou skutečně prvočísly. Snadno se nahlédne, že ověřování tohoto faktu metodou opakovaného dělení je velice pomalé.

Předložená práce tedy alespoň informuje, jak by se při testování prvočíselnost dala užít malá Fermatova věta. Bohužel se při jejím použití objevují tzv. pseudoprvočísla při každém základu a. Dokonce existují složená čísla (tzv. Carmichaelova čísla), pro která platí, že a^{n-1} je kongruentní s 1 modulo n pro každé a, které je nesoudělné s n. Malá Fermatova věta tedy neposkytuje plně korektní prvočíselný test. Bylo by možná vhodné popsat, jak se postupuje dále: kupř. Miller – Rabinův prvočíselný test, silná pseudoprvočísla atd.

Vlastní zpracování textu je bohužel slabé. Je velmi patrné, že práce byla zpracovávána pod časovým tlakem, kdy šlo o to, stihnout termín odevzdání. To ovšem vedlo k povrchnostem, kupř. v posledním odstavci na straně 29 nacházíme skutečně „skvělá“ sdělení. Práce je na dolní hranici rozsahu bakalářské práce, přihlédneme –li k tomu, že v matematických vzorcích vytvořených asi v programu MathType jsou zřejmě dosti dlouhé sentence uloženy jako jediný znak (= obrázek).

Práce prošla kontrolou plagiátorství.

Doporučuji **uznat práci jako práci bakalářskou** a navrhuji hodnocení stupněm **dobře.**

V Plzni dne 29. 5. 2018

doc. RNDr. Jaroslav Hora, CSc.
vedoucí práce