

Hodnocení bakalářské práce Michaely Cajthamlové,
obor matematika se zaměřením na vzdělávání, na téma
Prvočísla: Klasické a nové poznatky.

Téma dělitelnosti přirozených čísel a studium prvočísel je klasickou součástí algebry, s níž se seznamují i studenti učitelství s matematikou. Mohlo by se ale zdát, že jde o problematiku neúčinnou. V posledních desetiletích však prvočísla našla výrazné uplatnění při šifrování zpráv (RSA šifrovací metoda). Ta je dnes hojně používána v souvislosti se zabezpečením kupř. internetové komunikace. Je proto pochopitelné, že o prvočíslech dnes máme nové a zajímavé poznatky. Cílem předkládané práce bylo alespoň některé z nich představit srozumitelnou formou.

Autorka práce se tedy musela seznámit nejen s klasickými poznatky (některé se vyučují již na základní škole), ale zvládnout i řadu poznatků z oblasti počítačové algebry a teorie šifrování. Bylo také potřebné se seznámit s moderními programy typu Mathematica či např. s aktivitami Argentince Dario Alperna (program Alperton).

Autorka se dosti důkladně seznámila i s texty z oboru, kupř. s pozoruhodnou knihou Hudba prvočísel od Marcuse du Satoye. V ní je uveden vzorec obsahující 23 proměnných, který umožňuje generovat prvočísla dosazováním přirozených čísel za všechny tyto proměnné. Vygeneruje-li se kladné číslo, je toto číslo zároveň prvočíslem. Přitom lze touto metodou získat všechna prvočísla. (Kupř. známý Eulerův polynom $x^2 + x + 1$ generuje řadu prvočísel, ale jen pro $x = 0, 1, \dots, 40$). Při generování prvočísel z výše uvedeného zdroje jsme nebyli úspěšní. Celkově je generování vzorců popsaného typu umožněno vyřešením 10. Hilbertova problému, čehož dosáhl J. Matijasevič v r. 1970, a dále ovšem další výzkumnou prací několika vědců v nedávné době.

Na jiném místě v práci ale autorka uvádí, jak dokázala generovat velká prvočísla pomocí jiných technik populárně popsaných v textu Paola Ribenboima. Poznamenejme, že to je podstatné pro moderní šifrování zpráv (RSA šifrovací metoda). To ovšem souvisí s dalším problémem, s testováním prvočíselnosti (primality testing). I v této disciplíně bylo dosaženo pozoruhodného pokroku, ale v bakalářské práci se autorka zaměřila kromě elementárních postupů na příklady užití této funkce v programech počítačové algebry, což je podle názoru vedoucího práce rozumné (nelze pokrývat příliš mnoho cílů).

M. Cajthamlová nad zadaným tématem pracovala samostatně a iniciativně a seznámila i s historií vědeckého pokroku v této oblasti algebry. Práce prošla kontrolou plagiátorství.

Doporučuji předloženou práci **uznat práci jako bakalářskou** a hodnotím ji stupněm **výborně**.

V Plzni dne 2. 6. 2024

doc. RNDr. Jaroslav Hora, CSc.
vedoucí práce