

Oponentský posudek bakalářské práce

Název: **Úlohy z oblasti teorie čísel ve školských souvislostech**

Autorka: **Tereza Soukupová**

Studijní obor: **Matematická studia**

Katedra: **Katedra matematiky, fyziky a technické výchovy Fakulty pedagogické ZČU**

Vedoucí práce: **doc. RNDr. Jaroslav Hora, CSc.**

Rok odevzdání: **2020**

Oponent: **PhDr. Lukáš Honzík, Ph.D.**

Předložená bakalářská práce věnovaná teorii čísel ve školských souvislostech sestává z 9 kapitol. V nich je čtenáři postupně představen krátký historický úvod do problematiky, zaveden pojem prvočíslo a prvočíselný rozklad, definovány NSD a NSN s využitím ve slovních úlohách, poté jsou zavedeny kongruence, představena kritéria dělitelnosti pro čísla 2 až 10 včetně důkazů. Následně autorka pojednala o Mersennových a Fermatových prvočíslech, krátce představila vybrané testy prvočíselnosti, zmínila trojici šifrovacích metod a na závěr uvedla prvočíselnou větu.

Práce jen zlehka přesahuje minimální přípustný rozsah 54 tisíc znaků. Po formální stránce pak nesplňuje některé požadavky stanovené vyhláškou děkana č. 1VD/2018, kde jsou stanoveny například velikosti okrajů stran (kromě velkých okrajů je v práci nastaveno odsazení textu zprava i zleva, takže výsledné okraje jsou 5 cm u hřbetu a 4,5 cm vpravo, text tak tvoří úzký sloupec vprostřed stránky) nebo obvyklé řazení listů v práci. Samotnou kapitolou je autorčina práce s textovým editorem, kdy dolní a horní indexy zapisuje nikoliv příslušným formátováním textu, ale zmenšením velikosti písma a jeho vertikálním odsazením, nebo užitím anglosaské desetinné tečky místo české desetinné čárky (na některých místech se navíc za desetinnou tečkou/čárkou před desetinnými číslicemi vyskytuje mezera) či oddělováním tisíců v zápisu čísla normální (nikoliv pevnou) mezerou, což pak vede k zalamování textu a dělení zápisu na více řádek.

V textu práce je určité množství pravopisných chyb, které ve velké míře vznikly jako překlepy a vyskytují se téměř v každé kvalifikační práci. Horší je situace v případě některých vyjádření, která jsou pro čtenáře těžko uchopitelná až nesrozumitelná, např. na str. 28: „Kongruence je pojem, který označuje v algebře ekvivalenci. Tato ekvivalence je sluchitelná se všemi operacemi. Tedy pokud jsou prvky ekvivalentní a jejich operativní výsledek je též ekvivalentní, poté bude existovat kongruence pro tyto zvolené prvky.“

Po obsahové stránce oponent našel poměrně velké množství nesrovnalostí odborného rázu. Například hned v úvodu se čtenář dozví o největším společném násobku a nejmenším společném děliteli. Na str. 10 je jako příklad egyptského zápisu čísla uvedeno, že symboly zahnuté kosti a dvou čárek představuje číslo 7, ve skutečnosti však jde o číslo 12. V příkladu 2) na str. 14 je třeba určit, zda je číslo 2771 prvočíslem. Tato skutečnost je odhalena poměrně záhy, přesto jsou zbytečně dopočítávány i zbývající možnosti. V příkladu věnovaném nalezení NSD (60, 90) na str. 20 jsou do množiny společných dělitelů zahrnuta pouze čísla 1, 2, 3 a 30. Zbývající společní dělitelé 5, 6 a 15 jsou opomenuti. Poměrně velký zmatek lze nalézt v kapitole 5 věnované kongruencím. Autorka zde míchá dohromady relace (které ani nezavádí) s ekvivalencemi, operacemi a kongruencemi. Nic na tom nemění ani fakt, že zavedení relace ekvivalence je pro další tematické celky počínaje kongruencemi naprosto zbytečné. Dále pak v důkazech kritérií dělitelnosti je uveden rozvinutý zápis čísla v desítkové soustavě, který je nakonec vhodně využit. Jsou však nesprávně stanoveny meze pro jednotlivé číslice daného čísla, a to řetězcem nerovností $0 \leq a_0, a_{n-1} \leq 10$. Ze zmíněného lze usoudit dvě věci. Jednak není stanoven rozsah pro číslice a_1, a_2, \dots, a_{n-2} a vedoucí číslici a_n , za druhé

čísllice a_0 a a_{n-1} mohou nabývat hodnoty 10. V několika případech jsou uvedeny faktické nesmysly. Kupříkladu autorka píše o Fermantových prvočíslech (ve skutečnosti Fermatova), či Martinu Mersennovi (ve skutečnosti šlo o Marina Mersenna). Největší Mersennovo prvočíslo bylo dle autorčiných informací nalezeno roku 207 (správně 2016) a má hodnotu $2^{32582657} - 1$, avšak podle internetových zdrojů bylo doposud největší Mersennovo prvočíslo nalezeno v prosinci 2018 a jeho hodnota je $2^{82589933} - 1$. V závěru kapitoly 8.3 utorka zavádí pojem pseudočísla. Na str. 47 je pojednáno o tom, že algoritmus šifrování ElGamal byl navržen v roce 1895, a to přesto, že Taher ElGamal, autor algoritmu, se narodil v roce 1955.

Otázky k diskuzi:

1. Na str. 9 je popsán způsob zapisování čísel na tzv. vrubovce. Užití jaké číselné soustavy v podstatě tento způsob zápisu odpovídá?
2. V kapitole 4 jsou NSD a NSN počítány vesměs pomocí rozkladu v součin prvočísel. Tento postup může být zvlášť u větších čísel zdlouhavý, protože existují i jiné způsoby zjištění NSD a NSN, konkrétně například Euklidův algoritmus. Uveďte, jakým způsobem Euklidův algoritmus funguje a demonstруйте jej na konkrétní úloze.
3. V úloze c) na str. 25 je více možných řešení, například 24 kytic, v každé je 6 bílých a 8 červených růží. Upravte zadání úlohy tak, aby měla pouze jedno (v textu práce zmíněné) řešení.
4. Úloha f) na str. 27 má více než jen jedno uváděné řešení. Zdůvodněte, proč tomu tak je a uveďte alespoň jedno další řešení.
5. Na str. 28 a 29 jsou uvedeny vlastnosti relací. Určete, jaké vlastnosti má relace „znát někoho“ definovaná na množině všech lidí na Zemi.
6. Na str. 30 je zaveden pojem modulo m . Není zde však uvedeno, jaké podmínky jsou číslo m kladeny. Uveďte je.
7. Jak vypadá rozklad na třídy navzájem ekvivalentních prvků u relace kongruence modulo m .
8. V příkladu na str. 41 stojí: „...je zřejmé, že (...) číslo 211 budeme dělit prvočísly 2, (...) a 13.“ Jak je to zřejmé a jakou souvislost to má s odmocňováním čísla 211?
9. V závěru příkladu na str. 42 je uvedeno: „Jen jediné prvočíslo a to číslo 5 dělí (...) číslo 505.“ To není pravda, existuje ještě jedno prvočíslo, které číslo 505 dělí. Uveďte jej.

Na základě výše uvedeného nedoporučuji práci k obhajobě a navrhuji klasifikaci **nevyhověla**.

V Plzni dne 26. července 2020

PhDr. Lukáš Honzík, Ph.D.