Oponentský posudek bakalářské práce

Název: **Testování prvočíselnosti**
Autorka: **Gabriela Stulíková**
Studijní obor: **Matematická studia**
Katedra: **Katedra matematiky, fyziky a technické výchovy Fakulty pedagogické ZČU**
Vedoucí práce: **doc. RNDr. Jaroslav Hora, CSc.**
Rok odevzdání: **2018**
Oponent: **PhDr. Lukáš Honzík, Ph.D.**

Předložená bakalářská práce s názvem *Testování prvočíselnosti* je rozdělena do tří kapitol, které jsou postupně věnovány Malé Fermatově větě, testování prvočíslenosti a pseudoprvočíslům při základu *a* a Carmichaelovým číslům.

Práce je bohužel poměrně tenká, nejde příliš do hloubky problematiky a zřejmě vznikala ve spěchu před blížícím se termínem odevzdání. Kromě postřehů a připomínek zmíněných níže v příloze by oponent autorce vytkl především fakt, že poměrně velká část textu je bez valného uplatnění věnována zavedení Euklidova algoritmu a jeho využití pro výpočet největšího společného dělitele a nejmenšího společného násobku (opravdu zde nevidím souvislost; pokud nějaká taková existuje, měla by být v práci uvedena), zatímco poslední kapitola pojednávající o Carmichaelových číslech má rozsah pouhé dvě strany, přičemž polovina z toho je pojednání o životě Václava Šimerky (o Robertu Carmichaelovi a jeho životě se autorka vůbec nezmiňuje), další podstatnou část kapitoly pak zabírá obrázek. O samotné předpokládané náplni této kapitoly, tedy Carmichaelových číslech, se čtenář mnoho nedozví. V textu se v některých částech bohužel objevují ve vcelku velké míře překlepy (například v kapitole třetí: „jedná se **i Ch**armichaelova čísla“, „nelze **požít**“, „v **t**oce 1851“). Autorka v několika případech pod hlavičku definice či matematické věty schovává normální popisné tvrzení, které definicí ani větou není. Použitá literatura není citována podle aktuální normy a obsahuje drobné pravopisné chyby (někde chybějící, jinde naopak přebývající mezery).

Kontrolou plagiátorství v systému Thesis nebyly zjištěny shody s dalšími dokumenty a práce je tedy původní.

Práce bez výhrad splňuje požadavky kladené na úroveň bakalářské práce, a proto ji doporučuji k obhajobě. V hodnocení navrhuji klasifikování stupněm **dobře**.

V Plzni dne 14. V. 2018 PhDr. Lukáš Honzík, Ph.D.

Příloha oponentského posudku bakalářské práce

Název: **Testování prvočíselnosti**
Autorka: **Gabriela Stulíková**

6 - první odstavec: v první (hlavní) větě chybí sloveso, zní tedy divně;
7 - předposlední odstavec: „Karla Matěje Čapka nazvaná“ – má být „nazvané“;
- předposlední odstavec: „známka věnované“ – má být „věnovaná“;
8 - první odstavec: druhá věta je bez slovesa a zní divně;
11 - důkaz matematickou indukcí: v části 2. by místo symbolu = mělo být použito snad $\Rightarrow$;
12 - důkaz pomocí faktoriálu: v zápise $p|(nk - mk) \vee p|(n - m)k$ je zřejmě nesprávně použita operace disjunkce, měla zde být spíše ekvivalence;
14 - řešení příkladu 1.4: ve druhé větě je dvakrát sloveso „je“;
- na této a dalších dvou stranách je poměrně dlouhý a nic neříkající zápis čísla 7^{3822};
17 - příklad 1.6 a příklad 1.7: co je zadáním?
19 - první a čtvrtý odstavec: v prvním odstavci je použito slovní spojení „pařížská akademie“, ve čtvrtém je naopak „Pařížská akademie“ – toto by bylo vhodné sjednotit, nejlépe podle příslušných pravidel;
- třetí odstavec: v poslední větě uvedený rok 1838, kdy Euler oslepl, má být 1738;
20 - definice 2.1: použité označení „jednička“ není vhodné (jednička je tramvaj, nikoliv číslo);
- definice 2.1: poslední věta „Jsou to všechna čísla $p \geq 2$.“ není právě nejšťastněji formulována, v návaznosti na předchozí text totiž působí dojmem, že všechna čísla číslem 2 počínaje jsou čísla složená;
21 - poslední odstavec: program Mathematica není oproti autorčinu tvrzení volně dostupný;
22 - věta 2.4: nejedná se o matematickou větu, přestože je odstavec tak uveden, v první větě odstavce navíc chybí podmět;
23 - příklad 2.5: zadání příkladu je bez jakékoliv úpravy převzato z textů k předmětu Elementární algebra zpracovaných doc. Drábkem (bez uvedení ve zdrojích);
- řešení příkladu 2.5: „rozložíme ho na součin prvočísla + zbytek“ – v Euklidově algoritmu nejde o rozkládání v součiny prvočísel (natož součin prvočísla), konec konců ono to 729 ani prvočíslem není, neboť $729 = 27^2$;
25 - druhý odstavec definice 2.7: místo „rozdíl $(a - b)$ dělí m“ má být „m dělí rozdíl $(a - b)$“;
- třetí odstavec definice 2.7: co je „základ množiny“?
- tvrzení o relaci ekvivalence a jejích vlastnostech: skutečnost, že se jedná o relaci ekvivalence, bývá obvykle vyvozována právě podle platnosti zmíněných vlastností, nežli naopak;
26 - příklad 2.9: zadání příkladu je bez jakékoliv úpravy převzato z textů k předmětu Elementární algebra zpracovaných doc. Drábkem (bez uvedení ve zdrojích);
- příklad 2.10: zadání příkladu je bez jakékoliv úpravy převzato z textů k předmětu Elementární algebra zpracovaných doc. Drábkem (bez uvedení ve zdrojích);
27 - definice 2.11: věta pod nadpisem definice není definicí;
29 - předposlední věta: „Pokud tyto tvrzení spojením získáme…“ je divná věta a nedává smysl;
30 - definice 2.14: není zavedena zkratka MFV, není ji tedy vhodné v textu používat (byť jen jednou);
31 - řešení příkladu 2.18: věta „Svědkem je zde použito číslo 2.“ je divná;
32 - odstavec k Solovayovu-Strassenovu testu: „věta…je prvočíslo p číslo složené“ je nesmyslná;
- řešení příkladu 2.21: věta „Následně podmínky z uvedené definice.“ postrádá sloveso a zní divně;

33 - konec kapitoly druhé: nebyly by ilustrační příklady Pépinova testu, Wolsonova testu, Lucasova-Lehmerova testu?

34 - definice 3.1: první věta je divná, její hlavní věta neobsahuje sloveso;
- druhý odstavec: věta „S tímto pojmem souvisí V. Šimerka…“ je poněkud nešikovně formulována;
- předposlední odstavec: „Na přelomu let 1839/40 a 1840/41…“ by snad bylo lépe formulováno jako „V letech 1839 až 1841…“;

Otázky k obhajobě:

1. Užití příkazu QuotientRemainder [7^3822, 15] na straně 14 je dosti nepěkné, a to kvůli výpisu celého zadaného čísla, jehož hodnota nás v zadaném úkolu vlastně vůbec nezajímá. Šlo by v programu Mathematica využít ke zjištění hodnoty 7^{3822} v Z_{15} nějaký lepší příkaz? Pokud ano, o který příkaz se jedná?
2. Naznačte důkaz věty 2.4 na straně 22.
3. Na straně 27 autorka píše, že všechny testy prvočíselnosti řeší otázku, zda zadané přirozené číslo je prvočíslo, obvykle bez použití prvočíselného rozkladu. Uveďte, kde je v testech prvočíselnosti využíváno prvočíselného rozkladu?