UNIVERZITA KARLOVA – PEDAGOGICKÁ FAKULTA

KATEDRA MATEMATIKY A DIDAKTIKY MATEMATIKY

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Autor práce	*Matěj KOVÁŘÍK*
Název práce	*Polynomiální a exponenciální kongruence*
Autor posudku	*JUDr. Mgr. Filip Beran*

Cíle (stanovení, splnění, reflexe splnění)

Cílem práce bylo podat přehledný a dostatkem příkladů ilustrovaný výklad řešení polynomiálních a exponenciálních kongruencí, který bude možné používat jako skripta k příslušné části předmětu Teorie čísel – vše pokud možno co nejvíce intuitivním přístupem, srozumitelným pro studenty učitelství, příp. zájemce z řad sš. studentů či učitelů.

To se autorovi v zásadě podařilo splnit.

Obsahové části (úplnost, relevance, řazení)

Práce sestává ze tří kapitol, postupně věnovaných polynomiálním kongruencím, exponenciálním kongruencím a nakonec souhrnnému strukturálnímu náhledu. Toto řazení dává dobrý smysl: přirozeně navazuje na řešení lineárních kongruencí a od úvodních analogií postupů řešení kvadratických rovnic přechází ke hlubším tvrzením (Zákon kvadratické reciprocity; Malá Fermatova, Eulerova a Carmichaelova věta) a účinnějším nástrojům (počítání s kvadratickými zbytky; grupový náhled na počítání modulo n), který předchozí postupy a výsledky projasňuje a vysvětluje.

Práce tak propojuje několik témat, která často bývají vykládána odděleně bez patřičných souvislostí, neúplně či bez sjednocujícího náhledu. Nejobsáhleji je zpracovaná část věnovaná kvadratickým kongruencím; z důvodu rozsahu i obtížnosti se autor o polynomiálních kongruencí vyšších stupňů nakonec zmiňuje jen okrajově, což ale není na újmu celkovému cíli. U částí o exponenciálních kongruencích a strukturálním náhledu si lze také představit možná rozšíření, nicméně nic podstatného autor nevynechává a čtenáře vede k přirozenému završení předchozích poznatků ve Větě 5, která objasňuje strukturu grup $\mathbb{Z}_n^*$. Zde v závěru pouze postrádám více řešených příkladů a též zpětné ohlédnutí na předchozí postupy a výsledky, které lze dobře interpretovat právě ve světle tohoto strukturálního tvrzení.

Práce je poměrně rovnoměrně členěna do obsahově soudržných podkapitol. Orientaci v samotném textu dále napomáhá přehledné rozlišování definic, tvrzení, důkazů, příkladů a poznámek. Místy by jen prospělo vhodnější členění do odstavců, někdy není jasné, že skončil předchozí příklad a začínají nové úvahy apod.

Odborná část (matematika/didaktika: náročnost, správnost, výstavba, konzistence apod.)

Odbornou náročností téma přesahuje sš. matematiku a navazuje na základní kurz Teorie čísel. Především části věnované řešení kvadratických kongruencí modulo p^k si autor musel dostudovat z dostupných zdrojů (vč. Gaussových *Disquisitiones Arithmeticae*) a případné mezery sám překlenout. Ve výsledku prokázal schopnost jednotlivá témata samostatně pochopit, propojit a stručně, ale zároveň srozumitelně vysvětlit.

V práci zvláště oceňuji rozšíření rozpoznávání kvadratických zbytků z prvočísel na jejich mocniny a následně tedy i složená čísla, tj. po cestě inspirované Gaussem a nikoliv užitím Legendrova, resp. Jacobiho symbolu, které je v tomto pouze omezené, a dále i samotné postupy dohledání řešení kvadratických kongruencí, pokud pomocí zbytků zjistíme, že řešení existuje. Čtenáři tak je poskytnut úplný návod, jak vyřešit libovolnou kvadratickou kongruenci, což se přinejmenším v tuzemských zdrojích obvykle nevyskytuje.

Autorovi se ovšem nepodařilo zachytit některé obsahové chyby: Příklad 19 na s. 45 je evidentně vyřešen chybně a také závěrečný Příklad 48 na s. 112 obsahuje mylný výsledek: i $\mathbb{Z}_{16}^*$ je také izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_4$, nikoliv $\mathbb{Z}_8$, což přímo plyne z předchozí věty. Spíše než o neporozumění konceptu se však jedná o chyby z nepozornosti, které autor mohl důkladnější kontrolou snadno odhalit. I pro zamýšlené použití práce jako studijního materiálu tak doporučuji před publikováním text ještě jednou projít a opatřit erraty.

Přínos (originalita, použitelnost apod.)

Na základě výše uvedeného hodnotím autorský přínos jako nadprůměrný. Práce sice neobsahuje (až na drobná vylepšení některých důkazů) originální výsledky, ale je systematickou kompilací do hloubky pochopené teorie; zvláště kap. 1.2, 1.3 a 1.4 jsou vítaným doplněním dostupných textů.

Použitelnost práce je současně podpořena podrobně řešenými a vysvětlenými příklady, takže čtenář při řešení vlastních úloh snadno najde vzor, podle kterého může postupovat. I díky tomu práce splní svůj cíl posloužit jako studijní materiál k základnímu kurzu Teorie čísel.

Formální náležitosti (gramatika, styl, typografie, grafické části, odkazy a citace, úprava)

Styl je kultivovaný, odborně korektní a dobře vyvažuje stručnost a srozumitelnost; snad jen pro některé formulace např. v důkazech by se našly výstižnější obraty. V textu narazíme na minimum překlepů, místy však upoutají naši pozornost chyby pravopisné: např. na s. 79 neshoda podmětu s přísudkem nebo poměrně často chybné oddělování vložených vět čárkami, které by snadno odhalila důkladnější revize. Typografickou chybou je soustavné užívání spojovníku místo pomlčky při udávání rozsahu (životopisná data v úvodu, citace stran odkazovaných zdrojů napříč prací).

Celková úprava je ale jinak velmi dobrá; přehlednosti napomáhají vložené vlastní tabulky i kreslená schémata; jen některé mohly mít vhodnější velikost (např. v kap. 3.6). Odkazy a citace jsou v zásadě korektní. V seznamu zdrojů čtenáři usnadní jejich vyhledání uvedení internetových odkazů. V elektronické verzi použitelnosti napomáhá obsah vytvořený pomocí vnitřních odkazů, škoda, že nejsou užívány i v samotném textu; a naopak ji snižuje posunutí číslování stran pdf oproti stranám práce.

Zdroje (reprezentativnost, relevance, použití)

Zdroje pokládám pro autorův záměr za plně dostačující, studium a užití Gaussových přelomových *Disquisitiones* za chvályhodné, stejně jako dostatek autorem navržených řešených úloh.

Otázky k obhajobě

Jaké je správné řešení Příkladu 19? Opravte jej a upřesněte shrnutí v závěru příslušné podkapitoly.

Vyjádření ke shodám v systému Theses: Vše v pořádku, vše řádně citováno.

Hodnocení: Práce splňuje podmínky kladené na bakalářskou práci. Práci velmi rád doporučuji k obhajobě.

Datum a podpis autora posudku: V Praze dne 3. ledna 2024, Filip Beran