Posudek oponenta k bakalářské práci
Fermatova prvočísla v geometrii
Adama Zemánka

Fermatova čísla jsou čísla tvaru $F_m = 2^{2^m} + 1$, kde $m \in \mathbb{N}_0$, pro $m = 0, 1, 2, 3, 4$ je $F_m \in \mathbb{P}$. Euler zjistil, že 641 dělí F_5 a žádné prvočíslo tvaru $F_m, m \geq 5$ není zámo. Nicméně hledání úplné faktorizace Fermatových čísel patří mezi oblíbené úlohy při konstrukci faktorizačních algoritmů (viz např. faktorizace F_7 metodou CFRAC v roce 1970).

Předložená práce se zabývá souvislostí Fermatových čísel a geometrie. Ve třetí kapitole je zaveden pojem konstruovatelného komplexního čísla a Věta 3.7 spolu s Lemmatem 3.8 charakterizují konstruovatelná komplexní čísla. Ve čtvrté kapitole je předveden důkaz Gaussovy-Wantzelovy věty charakterizující pravidelné n-úhelníky konstruovatelné pravítkem a kružítkem (Věta 4.4). Poslední kapitola ukazuje poměrně nedávný výsledek Floriana Lucy (2003), který popisuje trojúhelníky s celočíselnými délkami stran a celočíselným obsahem (Věta 5.9).

Práci považuji za zdařilou, po obsahové stránce je zajímavá a dobře se čte. Od tématu se příliš nedalo čekat, že by vlastní přínos autora mohl přesáhnout podrobnější rozepsání důkazů z literatury nebo případně drobná zjednodušení těchto důkazů. Nicméně si myslím, že autor dostatečně demonstroval schopnost napsat samostantě korektní matematický text.

Množství překlepů v práci by mohlo být menší, ale v principu je v mezi, kterou lze považovat vzhledem k délce textu za přiměřenou.

Věcné připomínky k práci jsou v seznamu níže.

Celkově si myslím, že práce splnila zadání a doporučuji ji uznat jako práci bakalářskou.

V Praze, 2. září 2024,

Pavel Příhoda

Konkrétní připomínky k práci

- Tvrzení 1.2: Vzhledem k tomu, že potřebujeme vyloučit případ, že F_m a F_n mají společného prvočíselného dělitele, stačí pouze první část důkazu.
- Lemma 2.5: u, v nemůžou být libovolné prvky U
- Definice na str. 10: Galoisovo rozšíření se zpravidla definuje obecněji
- Tvrzení 3.1: Konstrukce využívá kružnice s poloměrem daným vzdáleností konstruovatelných bodů. Proti tomu definice (str. 12 nahoře) připouští pouze vzdálenost konstruovatelného bodu od nuly.

- Tvrzení 3.5: $\sqrt{z_1}$ není jednoznačně definovaná, asi by bylo lepší napsat 'každá druhá odmocnina ze z_1'.
- str. 18, řádek -4: v rovnici má být $+\sin(\frac{\varphi}{2})$ místo $+\sin(\varphi)$
- Věta 3.6: Ze vzorců není vidět, že uvedené polynomy mají skutečně koeficienty v L (bylo by to tak, pokud bychom předpokládali implikaci $u \in L \Rightarrow \overline{u} \in L$).
- Důkaz Lemmatu 4.3: Definice φ_a není příliš jasná ('pro každé dva kořeny existuje právě jeden prvek φ_a').
- Věta 5.9, důkaz: Myslím, že nejsou diskutovány případy $p_1 = p_2 = p_3 = 2$ a $i > j = k$ (v tomto příadě je $(2^{i-k} + 2^{j-k})^2 + 1$ sudé) a případ $p_1 = p_2 \neq 2$ a $i \neq j$. Kromě toho na str. 30, řádek -14 má být 'rozdíl' místo 'součet'.