Posudek oponentky diplomové práce			
Název práce:	**PARALELNÍ A ONLINE ARITMETIKA V IMAGINÁRNÍCH KVADRATICKÝCH TĚLESECH**		
Autorka:	**Bc. Pavla VESELÁ**	Akademický rok: 2020-2021	
Školitelka:	prof. Ing. Zuzana MASÁKOVÁ, Ph.D.	Konzultant:	Dr. techn. Ing. Jan LEGERSKÝ

Diplomová práce se zabývá numeračními systémy se základními aritmetickými operacemi (sčítání, násobení, dělení) fungujícími tak, aby jejich výpočetní náročnost byla nižší než při použití standardních metod. **Sčítání** je prováděno **algoritmem tzv. paralelním**, a **násobení / dělení algoritmem tzv. on-line**. On-line algoritmus zpracovává vstupy a produkuje výstupy směrem zleva doprava – tj. nejvýznamnější cifry nejdřív; paralelní algoritmus zpracovává dokonce všechny cifry zároveň (tj. v konstantním čase). Před aplikací on-line algoritmu pro dělení je vždy nutné provést ještě **před-zpracování dělitele** – tak, aby jeho velikost byla větší než pevné kladné číslo (parametr D_{min} pevný pro daný numerační systém). I to se provádí směrem zleva doprava, aplikací vhodných přepisovacích pravidel z předem určené sady ($\mathcal{A}$).

Fungování on-line algoritmů (pro násobení a dělení) je ještě výrazně efektivnější, pokud abeceda (množina cifer daného numeračního systému) je uzavřená na násobení. A právě na takové numerační systémy, s abecedami uzavřenými na násobení, se tato práce zaměřuje. Uvažují se **numerační systémy** (β, A) takzvaně **polygonální** – tedy s abecedou ve tvaru $A = A_n = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ pro $\xi = e^{2\pi i/n} = \sqrt[n]{1}$ *s* $n \in \mathbb{N}$, a také **kompletní** – kde každé komplexní číslo má alespoň jednu reprezentaci. Navíc se požaduje, aby báze β i abeceda A ležely v (jednom společném) okruhu O_K algebraických celých čísel imaginárního kvadratického tělesa $K = \mathbb{Q}(\sqrt{d})$, $d < 0$.

Hlavními novými výsledky této diplomové práce jsou jednak **klasifikace všech kompletních polygonálních numeračních systémů v imaginárních kvadratických tělesech**, a také **nalezení množin $I \subset \mathbb{C}$, které zajišťují tzv. OL-vlastnost** (nutnou pro algoritmy on-line násobení a dělení) pro několik vybraných numeračních systémů (β, A):

- báze $\beta = \pm i\sqrt{2}$ s abecedou $A = A_2 = \{0, \pm 1\}$,
- báze $\beta = 2\rho^k$ s abecedou $A = A_6 = \{0, 1, \rho, \ldots, \rho^5\}$, $\rho = \frac{1}{2}(1 + i\sqrt{3}) = \sqrt[6]{1}$,
- báze $\beta = \pm\frac{1}{2}(1 \pm i\sqrt{7})$ s abecedou $A = A_2 = \{0, \pm 1\}$,
- báze $\beta = \pm 1 \pm i\sqrt{2}$ s abecedou $A = A_4 = \{0, \pm 1, \pm i\}$.

Dále pak jsou tyto výsledky vhodně zkombinovány s dříve známými fakty, postupy a programy. Výsledkem je přehled **pěti tříd kompletních polygonálních numeračních systémů v imaginárních kvadratických tělesech, které umožňují paralelně sčítat i on-line násobit a dělit**. Přitom jsou vyčísleny základní parametry příslušných algoritmů.
Jako **nejvýhodnější z uvažovaných numeračních systémů** se jeví ty s bázemi $\beta = \pm i\sqrt{2}$ a s abecedou $A = A_2 = \{0, \pm 1\}$. Mají totiž malý rozsah vyhledávacích tabulek (**# LuT**), resp. sad přepisovacích pravidel ($\mathcal{A}$) používaných v algoritmech paralelního sčítání, resp. před-zpracování dělitele v on-line algoritmech. Přitom parametr D_{min} pro odhad minimální velikosti dělitele (po před-zpracování) mají větší než ostatní (β, A), což je optimální pro on-line dělení.

K prezentovaným výsledkům bych ráda položila následující doplňující otázky – k diskusi / komentáři při obhajobě:

- Pro několik numeračních systémů se nově povedlo nalézt **množinu $I \subset \mathbb{C}$, která zajišťuje OL-vlastnost systému**. Není zřejmé, **jakým způsobem byly tyto množiny $I \subset \mathbb{C}$ vlastně nalezeny** – byla použita nějaká jednotná metoda, nebo spíš ad-hoc přístup, pro každý numerační systém jinak?

- V kapitole 5 (na str. 67 / poslední odstavec) se uvádí, že **algoritmy paralelního sčítání a před-zpracování dělitele pro on-line dělení** jsou shodné pro dva numerační systémy, které mají **shodné abecedy A a navzájem komplexně sdružené báze β**, díky tomu, že tyto báze mají shodný minimální polynom. To je sice pravda, pokud uvažujeme systémy celočíselné – s využitím reprezentace nuly v podobě minimálního polynomu $f(x) \in \mathbb{Z}[x]$ – tedy polynom 2. stupně (pro kvadratické báze) s celo-číselnými koeficienty. Ovšem algoritmy EWM ("Extending Window Method" pro nalezení algoritmu paralelního sčítání) i před-zpracování (dělitele pro on-line dělení) zde ve skutečnosti pracují **s reprezentací nuly v podobě polynomu nižšího, 1. stupně** – totiž $f(x) = x - \beta$, a ten už pro dvě komplexně sdružené báze shodný není. Měl by být tedy zdůrazněn navíc ještě fakt, že uvažované **abecedy A** jsou **uzavřené na operaci komplexního sdružení**. S tímto upřesněním, je možné nalézt přímé předpisy pro převod algoritmů paralelního sčítání a před-zpracování dělitele z numeračního systému (A, β) na numerační systém (A, γ), kde β a γ jsou navzájem **komplexně sdružené**?

- Pro skupinu numeračních systémů (β, A) s abecedou $A = A_6 = \{0, 1, \rho, \ldots, \rho^5\}$ a s bázemi ve tvaru $\beta = 2\rho^k$, kde $k \in \{0, \ldots, 5\}$, se pomocí EWM-algoritmu nepodařilo nalézt algoritmus paralelního sčítání, ale přitom je známo, že

takový algoritmus existuje. Jaká množina $\boldsymbol{Q}$ váhových koeficientů $\boldsymbol{q_j \in Q}$ byla v EWM-algoritmu použita? A pokud byla v onom neúspěšném chodu EWM-algoritmu použita množina $\boldsymbol{Q = A_6}$, jaký výsledek má EWM-algoritmus v případě použití váhových koeficientů z větší množiny $\boldsymbol{Q' = A_6 + A_6}$?

- Při interpretaci výsledků v Table 5.10 (na str. 81) stojí za zmínku ten fakt, že velikost Look-up Table (**# LuT**) je zde uváděna jako počet skutečně všech předpisů pro určení váhových koeficientů $\boldsymbol{q_j := q_j\ (w_j, w_{j-1}, \ldots, w_{j-(r-1)})}$, bez zohlednění $\boldsymbol{n}$-četné symetrie abecedy $\boldsymbol{A = A_n}$. Pokud bychom vzali v úvahu $\boldsymbol{n}$-četnou symetrii abeced $\boldsymbol{A = A_n}$ a $\boldsymbol{B = A_n + A_n}$ i množiny $\boldsymbol{Q}$ všech váhových koeficientů $\boldsymbol{q_j}$, stačilo by pracovat s $\boldsymbol{n}$-krát menší Look-up Table (při současném využití pomocného násobení jednotkami $\boldsymbol{\xi^k, k \in \{0, \ldots, n-1\}}$).

Pokud jde o celkovou strukturu práce, je logicky a přehledně členěna; souvislosti mezi jednotlivými kapitolami jsou dobře srozumitelné. Na obecné základy a fakta o numeračních systémech navazují specifické vlastnosti / klasifikace vybrané třídy numeračních systémů, a následně relevantní metody pro práci s algoritmy paralelního sčítání a před-zpracování dělitele pro on-line dělení. Čerpá se z bohatého rozsahu související literatury, což je pro celkový kontext velmi přínosné.

V podrobnějším pohledu bych ovšem ocenila větší pozornost při interpretaci přejímaných / citovaných výsledků, například zde:

- str. 25 / Proposition 2.4.: Znění věty se týká **všech celých čísel** $\boldsymbol{d \in \mathbb{Z}}$, která neobsahují čtverec; následně ale důkaz věty se věnuje **pouze záporným hodnotám** $\boldsymbol{d < 0}$. Je zde zamýšlen širší rozsah tvrzení, a tedy důkaz by měl být rozšířen tak, aby pokryl i kladné hodnoty $\boldsymbol{d > 0}$; anebo naopak rozsah tvrzení má být zúžen pouze na záporné hodnoty $\boldsymbol{d < 0}$?

- str. 47 / Proposition 3.12.: Polynom Q(x) nemůže být zapsán jako $\boldsymbol{Q(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0}$, ale musí být $\boldsymbol{Q(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m}$, jinak nefunguje důkaz, resp. ani samotné tvrzení. Totiž **dominantní koeficient** má ležet na pozici $\boldsymbol{i_0 \in \{1, \ldots, m\}}$, což při značení $\boldsymbol{Q(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0}$ by nemohlo být v absolutním členu ($i_0 = 0$); ovšem právě tam často dominantní koeficient leže má.

- str. 51 / Example 3.13.: Reprezentace nuly ve tvaru $\boldsymbol{W(x) = x^4 - 3x^2 + 9}$, která pro **Eisensteinovu bázi** β (kořen minimálního polynomu $f(x) = x^2 + 3x + 3$) je nalezena pomocí Proposition 3.12. a má dominantní koeficient / parametr $\boldsymbol{P = 9}$, není reprezentace nuly s nejmenším možným dominantním koeficientem (jak se v textu tvrdí). Viz např. reprezentace nuly pro stejnou bázi β ve tvaru $\boldsymbol{W'(x) = -x^3 - x^2 + 3x + 6}$, která má menší dominantní koeficient / parametr $\boldsymbol{P' = 6}$, a také může být použita v „neighbour-free" WRZ-algoritmu paralelního sčítání v numeračním systému s bází β.

- str. 51 / Example 3.14.: V algoritmu paralelního sčítání je chyba v určení „váhových koeficientů" $\boldsymbol{q_j \in \{-1, 0, +1\}}$:
  - pro $\boldsymbol{w_j := +3}$ nemá být $\boldsymbol{q_j := 0}$, ale $\boldsymbol{q_j := +1}$, a
  - pro $\boldsymbol{w_j := -3}$ nemá být $\boldsymbol{q_j := 0}$, ale $\boldsymbol{q_j := -1}$;

  jinak totiž v některých případech výsledná cifra $z_j = w_j - 4q_j + q_{j-1}$ neleží v cílové / původní abecedě $A = \{-3, \ldots, +3\}$.
- str. 61 / Lemma 4.15.: Druhá část tvrzení – v bodě ***(ii)*** - má znít opačně – tj.
  - místo nesprávného „**or** $\boldsymbol{0.d_1d_2d_3\ldots d_m \neq 0.0\ d'_2\,d'_3\ldots d'_m}$ **for some string** $\boldsymbol{d'_2\,d'_3\ldots d'_m \in A^*}$"
  - ve skutečnosti platí „**or** $\boldsymbol{0.d_1d_2d_3\ldots d_m = 0.0\ d'_2\,d'_3\ldots d'_m}$ **for some string** $\boldsymbol{d'_2\,d'_3\ldots d'_m \in A^*}$".

Drobnější překlepy či nejasnosti jsou uvedeny ve druhé části posudku (Dodatek). Pokud by se text této práce používal pro další účely / publikace, bylo by vhodné tyto body opravit.

Celkově navrhuji hodnotit tuto diplomovou práci známkou **B – velmi dobře**.

V Praze, dne 18. května 2021 Ing. Milena SVOBODOVÁ, Ph.D. (oponentka)

Dodatek: drobnější překlepy a nejasnosti:

- str. 18 / Definition 1.6: pro úplnost se má explicitně požadovat rovnost hodnot $z = \sum_j z_j \beta^j$;
- str. 18 / Definition 1.7.: v případě komplexní báze $\beta \in \mathbb{C}$ se má požadovat $|\beta| > 1$, namísto $\beta > 1$;
- str. 19 / Definition 1.11.: omezujeme se zde na abecedu $A_n = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ jen pro $n \geq 4$, ale přitom dál v textu se pracuje i s variantami $n = 2$ a $n = 3$;
- str. 24 / Lemma 2.3.: správně patří inkluze $y_{k+1} \in \mathbb{Z}[\alpha]$ namísto $y_{k+1} \in \mathbb{Z}$ do 9. řádku zdola, a jmenovatel ve zlomku $y_k = 1 / \beta^k (\ldots)$ namísto $y_k = 1 / \beta^{k-1} (\ldots)$ do 6. řádku zdola;
- str. 25 / Proposition 2.4.: zřejmě patří $d \equiv 1$ namísto $m \equiv 1$ do druhé části tvrzení věty;
- str. 31+36 / Figures 2.3 / 2.10: znázorněné množiny $I \subset \mathbb{C}$ by spíš měly být značeny $V \subset \mathbb{C}$, aby odpovídaly konvenci v odkazovaném Theoremu 1.9;
- str. 30-37 / Figures 2.2 – 2.11: splnění požadované podmínky $\mathbb{Z}[\alpha] \subset A + \beta\, \mathbb{Z}[\alpha]$ je zde předvedeno pomocí obrázků – což je jistě ilustrativní, nicméně hodilo by se vypsat příslušné důkazy také analyticky;
- str. 33 / Case $n = 2$: pro tento případ je relevantní spíš argument $A_1 \subset A_2$, namísto $A_2 \subset A_4$;
- str. 45 / 11. řádek shora: používáme **násobky**, nikoliv **mocniny** reprezentace nuly;
- str. 58 / 2.-3. řádek: místo $(I + \varepsilon)$ asi patří $(1 + \varepsilon) I$;
- str. 61 / Lemma 4.14.: na konec důkazu místo $x = x_{k-1} \beta^{k-1} + x_{k-2} \beta^{k-2} + \ldots + x_1 \beta + x_0$ patří $x = x_{m-1} \beta^{m-1} + x_{m-2} \beta^{m-2} + \ldots + x_1 \beta + x_0$ s ciframi $x_j \in A$, kde buď $|x| \geq K$, anebo se x dá vyjádřit ve tvaru $x = y_{k-1} \beta^{k-1} + y_{k-2} \beta^{k-2} + \ldots + y_1 \beta + y_0$ s ciframi $y_j \in A$ a přitom $k-1 \leq m-2$;
- str. 68 / kapitola 5.1.2: báze $\beta = -1+i$ má minimální polynom $f(x) = x^2 + 2x + 2$, nikoliv $f(x) = x^2 - 2x + 2$;
- str. 73 / kapitola 5.3.2: báze $\beta = \frac{1}{2}(+3 \pm i\sqrt{3})$ má minimální polynom $f(x) = x^2 - 3x + 3$, nikoliv $f(x) = x^2 + 3x + 3$;
- str. 73 / kapitola 5.3: pro abecedu $A_3 = \{0, 1, \rho^2, \rho^4\}$ se mají uvažovat nejen báze $\beta = \pm i\sqrt{3}$, ale i $\beta = \frac{1}{2}(\pm 3 \pm i\sqrt{3})$ (podle výsledků v Table 5.1);
- str. 73 / kapitola 5.3.1: přepisovací pravidlo $1\rho^3 \rightarrow 0\rho^2$ není korektní (nezachovává hodnotu reprezentace), správně má zřejmě být předpis $1\rho^4 \rightarrow 0\rho^2$;
- str. 81 / Table 5.10: parametry p, r algoritmu paralelního sčítání jsou tu zaměněny, resp. uvedeny o 1 menší:
  - pro báze $\beta = \pm i\sqrt{2}$ s abecedou $\mathbf{A} = \mathbf{A_2}$ je správně $p = 5 = 1 + 4 = 1 + r$ namísto $\mathbf{p} = \mathbf{4}$,
  - pro báze $\beta = i\sqrt{3}\, \rho^k$, $k \in \{0, \ldots, 5\}$, s abecedou $\mathbf{A} = \mathbf{A_6}$ je správně $p = 4 = 1 + 3 = 1 + r$ namísto $\mathbf{p} = \mathbf{3}$, apod.;
- str. 68-80 / sady předpisů pro před-zpracování vs. přehledové tabulky s výsledky: hodil by se jednotný popis v tom smyslu, že kompletní množina $\mathcal{L}$ všech přepisovacích pravidel pro před-zpracování dělitele v (A, β) je rovna $\mathcal{L} = \mathcal{L}' \times \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$, kde $\mathcal{L}'$ je dílčí sada přepisovacích pravidel ve tvaru $1\ldots \rightarrow 0\ldots$ a n je četnost symetrie abecedy $A = A_n = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$.