Nestandardní zápisy čísel

Edita Pelantová, Štěpán Starosta, Praha

Abstrakt

V článku představujeme poziční numerační systémy s neceločíselnou bází, porovnáváme jejich vlastnosti s klasickými soustavami a na příkladu ukazujeme jejich využití k dláždění prostoru.

Problém, jak zapisovat čísla, řeší lidstvo od nepaměti. Poziční zápis, kdy stejný symbol, např. 2, použitý na různých místech vyjadřuje jednou počet dva, jindy počet dvě stě, byl umožněn vynálezem symbolu 0 pro „nic“. I malému školákovi je jasné, že úloha vynásobit čísla 79 a 37 zapsaná v desítkové soustavě je jednodušší, než násobit tato čísla zapsaná římským způsobem LXXIX a XXXVII. Přesto se poziční zápis prosadil v Evropě až ve 13. století. V tomto příspěvku se nechceme věnovat dávné minulosti, to přísluší historikům matematiky. Chceme však ukázat, jaké poziční zápisy čísel se studují dnes.

V běžném životě zapisujeme čísla v desítkové soustavě. Každé přirozené číslo x zapíšeme jako $x_k(10)^k + x_{k-1}(10)^{k-1} + x_{k-2}(10)^{k-2} + \ldots + x_1(10) + x_0$, kde cifry x_j jsou z množiny $\{0, 1, 2, \ldots, 9\}$. Chceme-li zapsat záporné celé číslo, tak zapíšeme jeho absolutní hodnotu a před tento zápis dáme znaménko minus. Sčítat a násobit čísla v desítkové soustavě nás naučili už ve škole. Algoritmy pro tyto operace vyžadují, abychom si zapamatovali tabulky výsledků součtu dvou cifer a výsledků součinu dvou cifer.

I každé reálné číslo $x \in \mathbb{R}$ lze vyjádřit ve tvaru sumy $x = \pm \sum_{k=-\infty}^{n} x_k(10)^k$, kde $x_k \in \{0, 1, 2, \ldots, 9\}$, a zapsat v desítkové soustavě $(x)_{10} = \pm x_n \ldots x_1 x_0, x_{-1} x_{-2} \ldots$. Pochopení tohoto zápisu už vyžaduje povědomí o konvergenci v $\mathbb{R}$. Algoritmy na sčítání a násobení, jak nás je ve škole naučili, umějí ostatně pracovat jenom s čísly, která mají ve svém zápisu pouze konečně mnoho nenulových cifer, tj. jenom s čísly ve tvaru $(x)_{10} = \pm x_n \ldots x_1 x_0, x_{-1} x_{-2} \ldots x_{-m}$.

Bázi $\beta = 10$ v předchozím povídání můžeme zaměnit za libovolné celé přirozené číslo větší než jedna. Tím ovlivníme množinu potřebných cifer. V soustavě s bází $\beta = 2$ si vystačíme jen se dvěma ciframi, 0 a 1. Tabulka výsledků operací + a × dvou cifer je snadná k zapamatování. V této soustavě pracují skoro všechny počítače, protože realizovat technicky pouze dva symboly 0 a 1 je nejjednodušší.

Prof. Ing. Edita Pelantová, CSc., Katedra matematiky FJFI, ČVUT v Praze, Trojanova 13, 120 00 Praha 2, e-mail: edita.pelantova@fjfi.cvut.cz,
Ing. Štěpán Starosta, Katedra teoretické informatiky FIT, ČVUT v Praze, Thákurova 9, 160 00 Praha 6, e-mail: stepan.starosta@fit.cvut.cz

1. Poziční zápis komplexních čísel

Komplexní čísla jsou obvykle vyjádřena ve tvaru $x+\mathrm{i}y$. Reálnou složku x a imaginární složku y zapisujeme jako reálná čísla, tedy obvykle v desítkové soustavě. Násobení dvou komplexních čísel probíhá podle vzorečku pro výpočet reálné a imaginární složky součinu. Oddělování reálné a imaginární části při počítání není však šikovné. V roce 1965 Walter Penney, zaměstnanec ministerstva obrany USA, publikoval jedenapůlstránkový článek [16] a v něm následující větu.

Věta 1. *Nechť $\beta = \mathrm{i}-1$. Každé komplexní číslo $z \in \mathbb{Z}[\mathrm{i}] := \{a+\mathrm{i}b \mid a,b \in \mathbb{Z}\}$ lze jednoznačně zapsat ve tvaru*

$$z = \sum_{k=0}^{n} z_k \beta^k, \quad \textit{kde} \;\; z_k \in \{0,1\}\,.$$

Prvky $\mathbb{Z}[\mathrm{i}]$ se obvykle nazývají *gaussovská celá čísla*. Místo sumy budeme používat zápis

$$(z)_\beta = z_n z_{n-1} \ldots z_1 z_0 \bullet\ .$$

V něm se vyskytují pouze dvě cifry 0 a 1. Nepotřebujeme používat žádné znaménko $\pm$. Tabulka pro násobení cifer 0 a 1 je jednoduchá. Do tabulky pro součet dvou cifer potřebujeme doplnit $1+1$. Protože $\beta = \mathrm{i}-1$, $\beta^2 = -2\mathrm{i}$, $\beta^3 = 2+2\mathrm{i}$, $\beta^4 = -4, \ldots$, platí $2 = \beta^3 + \beta^2$, tj. $(2)_\beta = 1100\bullet$. Tedy sečíst $1+1$ na k-té pozici součtu dvou řetězců znamená napsat na k-tou pozici nulu a na pozice $k+2$ a $k+3$ přičíst cifru 1. Předveďme si to na příkladě $3+1=4$, zapsáno v bázi β.

					1	1	0	1	$\bullet$	=	$(3)_\beta$
								1	$\bullet$	=	$(1)_\beta$
					1	1	0	2	$\bullet$		
					1	1	0	0	$\bullet$		
					1	1	0	0	$\bullet$		
					2	2	0	0	$\bullet$		
			1	1	0	0	0	0	$\bullet$		
		1	1	0	0	0	0	0	$\bullet$		
		1	2	1	0	0	0	0	$\bullet$		
		1	0	1	0	0	0	0	$\bullet$		
1	1	0	0	0	0	0	0	0	$\bullet$		
1	1	1	0	1	0	0	0	0	$\bullet$	=	$(4)_\beta$

Důkaz Penneyovy věty je jednoduchý.

Označme $S := \left\{\sum_{k=0}^{n} z_k \beta^k \mid z_k \in \{0,1\}\right\}$. Zřejmě $S \subset \mathbb{Z}[\mathrm{i}]$. Chceme však ukázat, že $S = \mathbb{Z}[\mathrm{i}]$. K tomu stačí ověřit, že

a) $1, -1, \mathrm{i}, -\mathrm{i} \in S$ a

b) S je uzavřená vůči operaci sčítání.

a) Jelikož $\beta^4 = -4$ a $(4)_\beta = 111010000\bullet$, je $(\frac{4}{\beta^4})_\beta = 11101\bullet = (-1)_\beta$. Jednoduše nahlédneme, že $(\mathrm{i})_\beta = 11\bullet$ a $(-\mathrm{i})_\beta = 111\bullet$.

b) Uzavřenost vzhledem ke sčítání lze odvodit z faktu, že použití pravidla $2\bullet \mapsto 1100\bullet$ nemění součet cifer v zápisech $(x)_\beta$ a $(y)_\beta$, které chceme sečíst. Navíc jak jsme viděli na příkladě součtu 3+1, nevyhovující hodnoty cifer (tedy ty, co nejsou 0 a 1) se přesouvají v zápisu více doleva. To může pokračovat do nekonečna leda tak, že přesouvaná část cifer reprezentuje číslo 0, a lze ji proto vymazat.

Důkaz jednoznačnosti vyjádření čísla $z \in \mathbb{Z}[\mathrm{i}]$ v bázi $\beta = \mathrm{i} - 1$ využívá toho, že polynom minimálního stupně s celočíselnými koeficienty, který má kořen β, je polynom $x^2 + 2x + 2$. Kdyby některé $z \in \mathbb{Z}[\mathrm{i}]$ mělo dva různé zápisy v bázi β, pak by β bylo kořenem nenulového polynomu s koeficienty v $\{-1, 0, 1\}$, a tento polynom by měl být roven součinu $g(x)(x^2 + 2x + 2)$, kde $g(x)$ je polynom s celočíselnými koeficienty. To není možné. □

Množina $\frac{1}{\beta^n}\mathbb{Z}[\mathrm{i}] = \frac{1}{\beta^n}S$ představuje komplexní čísla, která lze zapsat v bázi β s nanejvýš n místy za zlomkovou tečkou $\bullet$. Množinu $\mathrm{Fin}(\beta) = \bigcup_{n\in\mathbb{N}} \frac{1}{\beta^n}\mathbb{Z}[\mathrm{i}]$ pak tvoří čísla, která lze zapsat v bázi β pomocí konečně mnoha cifer.[1] $\mathrm{Fin}(\beta)$ je hustá v $\mathbb{C}$, a tedy každé komplexní číslo je limitou nějaké posloupnosti s členy ve $\mathrm{Fin}(\beta)$. Další úsilí vyžaduje důkaz, že každé komplexní číslo z lze reprezentovat jako nekonečnou řadu

$$z = \sum_{j=-\infty}^{k} z_j \beta^j \quad \text{s koeficienty } z_j \in \{0, 1\}\,.$$

Vraťme se však ke gaussovským celým číslům. Jejich rozvoj v bázi β nehledáme tak naivně, jak jsme to dělali v případě čísla 4. Stačí se inspirovat algoritmem pro hledání zápisu přirozeného čísla v soustavě s bází $\beta \in \mathbb{N}$. Tak například při hledání koeficientů $a_j \in \{0, 1, , \ldots, 6\}$ pro zápis čísla $278 = a_k 7^k + \ldots + a_1 7^1 + a_0$ v bázi $\beta = 7$, vidíme, že číslo 278 a a_0 musejí mít stejný zbytek po dělení číslem 7. Tedy $a_0 = 5$. Protože $278 - a_0 = 273 = 7 \times 39 = 7 \times (a_k 7^{k-1} + \ldots + a_1)$, stačí teď vyjádřit v sedmičkové soustavě číslo 39. Jeho poslední cifru a_1 získáme stejně, tedy $a_1 = 4$, což je zbytek po dělení čísla 39 sedmičkou. A tak pokračujeme dál.

Vystačili jsme si s ciframi $0, 1, , \ldots, 6$, protože pokryjí všechny zbytky po dělení číslem 7. I na množině $\mathbb{Z}[\mathrm{i}]$ lze definovat dělení se zbytkem. Při popisu zbytků hraje důležitou roli norma komplexního čísla $N(z) = z\overline{z}$, kde $\overline{z}$ značí číslo komplexně sdružené k číslu z.

Věta 2. *Nechť $\beta = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$, kde a a b jsou nesoudělná. Ke každému $z \in \mathbb{Z}[\mathrm{i}]$ existuje $y \in \mathbb{Z}[\mathrm{i}]$ a zbytek $r \in \mathcal{R}$ tak, že $z = \beta y + r$, kde*

$$\mathcal{R} = \{0, 1, \ldots, N(\beta) - 1\}\,.$$

Tato věta pochází od Gausse [10] a její obdobu lze vyslovit i pro případ, kdy a a b jsou soudělná. Základ $\beta = \mathrm{i} - 1$ z věty 1 má normu 2. Množinou zbytků, a tedy množinou cifer, je $\mathcal{R} = \{0, 1\}$. Stejnou metodou, jakou jsme hledali rozvoj čísla 278 v bázi 7, můžeme hledat rozvoj gaussovských celých čísel v bázi $\mathrm{i} - 1$.

Až dosud vypadá situace v $\mathbb{Z}[\mathrm{i}]$ velice podobně jako v $\mathbb{Z}$. V $\mathbb{Z}$ lze za základ zvolit libovolné $\beta \in \mathbb{Z}, \beta > 1$ (a dokonce i $\beta < -1$). Čtenáře jistě napadlo, proč jsme si

[1] V českém textu se běžně používá v dekadické soustavě desetinná čárka k oddělení koeficientů u záporných mocnin základu, v obecných soustavách používáme značení mezinárodní, a to psaní tlusté tečky $\bullet$, kterou nazveme *zlomková tečka*.

vybrali v $\mathbb{Z}[\mathrm{i}]$ právě bázi $\beta = \mathrm{i} - 1$ a ne třeba $\beta = \mathrm{i} + 1$. I toto gaussovské číslo má přeci normu 2 a po dělení dva možné zbytky 0 a 1. Důvod je jednoduchý; pro $\beta = \mathrm{i} + 1$ by věta 1 neplatila. To zjistíme tak, že -1 ani $-\mathrm{i}$ se nám nepodaří v této bázi vyjádřit. Kdybychom totiž chtěli na výpočet posledního koeficientu v rozvoji čísla $-\mathrm{i}$ v bázi $\beta = \mathrm{i} + 1$ použít větu 2, dostaneme $-\mathrm{i} = \beta(-\mathrm{i}) + 1$, a tedy v dalším kroku máme hledat opět rozvoj stejného čísla $-\mathrm{i}$, a tak dokola.

Na otázku, s kterými bázemi β je vhodné pracovat v gaussovských celých číslech, odpovídá následující věta z [13]. Opět ji vyslovíme v jednodušší formě.

Věta 3. *Nechť $\beta = a + ib \in \mathbb{Z}[\mathrm{i}]$, a, b nesoudělná. Pak každé $z \in \mathbb{Z}[\mathrm{i}]$ lze zapsat ve tvaru*

$$z = \sum_{k=0}^{n} z_k \beta^k, \quad \text{kde} \;\; z_k \in \{0, 1, \ldots, N(\beta) - 1\},$$

tehdy a jen tehdy, když $\beta = -n \pm \mathrm{i}$ pro nějaké $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$.

Algoritmus pro hledání rozvoje čísla 278 v soustavě se sedmičkovým základem používal zbytky po dělení základem 7. Takový algoritmus je vhodný, když chceme hledat rozvoj celého čísla. Nehodí se však k tomu, abychom našli rozvoj čísla π v sedmičkové soustavě. Na hledání rozvojů libovolných reálných kladných čísel slouží

hladový algoritmus pro hledání rozvoje v bázi $\beta > 1$:

Pro zadané $x \in \mathbb{R}, x > 0$, nalezneme maximální $k \in \mathbb{Z}$ takové, aby $\beta^k \leqslant x$, a položíme $x_k = \lfloor \frac{x}{\beta^k} \rfloor$. Z volby k plyne, že $1 \leqslant x_k < \beta$ a číslo x lze napsat jako $x = x_k \beta^k + y$, kde $0 \leqslant y < \beta^k$. Je-li $y = 0$, končíme, jinak stejný postup použijeme pro číslo y. Tuto proceduru opakujeme, ale nemusíme se zastavit po konečném počtu kroků. Získáme tak konečný nebo nekonečný řetězec cifer z množiny $\{m \in \mathbb{Z} \mid 0 \leqslant m < \beta\}$ a číslo x zapsané jako

$$x = x_k \beta^k + x_{k-1} \beta^{k-1} + x_{k-2} \beta^{k-2} + \ldots$$

Např. číslo π v sedmičkové soustavě $(\pi)_7 = 3 \bullet 06634 \ldots$.

Co brání použití hladového algoritmu pro hledání rozvoje komplexních čísel? Na $\mathbb{C}$ nám schází rozumné uspořádání pro porovnání $\beta^k \leqslant x$. V roce 1989 našel Thurston [20] jednoduchou obdobu hladového algoritmu pro komplexní čísla.

Věta 4. *Nechť $\beta \in \mathbb{C}, |\beta| > 1$ je báze, $\mathcal{A} \subset \mathbb{C}$ je konečná množina cifer a $V \subset \mathbb{C}$ je omezená množina obsahující ve svém vnitřku 0. Pokud*

$$\beta V \subset V + \mathcal{A} := \{v + a \mid v \in V, a \in \mathcal{A}\},$$

pak každé $z \in \mathbb{C}$ lze zapsat ve tvaru

$$z = z_k \beta^k + z_{k-1} \beta^{k-1} + z_{k-2} \beta^{k-2} + \ldots \text{ , kde } z_j \in \mathcal{A} \text{ pro každé } j \leqslant k\,.$$

Důkaz. Protože V obsahuje ve svém vnitřku 0, každé $z \in \mathbb{C}$ můžeme vydělením vhodnou mocninou β^k dostat do V. Proto stačí větu dokázat pro $z \in V$. Z podmínky $\beta V \subset V + \mathcal{A}$ najdeme k číslu βz číslo $z_1 \in V$ a cifru a_1 tak, že $\beta z = z_1 + a_1$, tj. $z = \frac{a_1}{\beta} + \frac{z_1}{\beta}$. Analogicky najdeme z_2 a cifru a_2 tak, že $\beta z_1 = z_2 + a_2$, tj. $z_1 = \frac{a_2}{\beta} + \frac{z_2}{\beta}$.

Po dosazení pak $z = \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \frac{z_2}{\beta^2}$. Zkonstruujeme tak posloupnost cifer a_n a čísel $z_n \in V$ takovou, že pro každé n platí

$$z = \frac{a_1}{\beta} + \frac{a_2}{\beta^2} + \ldots + \frac{a_n}{\beta^n} + \frac{z_n}{\beta^n}\,.$$

Jelikož je V omezená a $|\beta| > 1$, je $\lim \frac{z_n}{\beta^n} = 0$. □

Okamžitě nás napadne, zda by nebylo možné využít předchozí větu k důkazu reprezentovatelnosti komplexních čísel $z \in \mathbb{C}$ v bázi $\beta = \mathrm{i} - 1$ a abecedě $\mathcal{A} = \{0, 1\}$. Stačilo by najít nějaké okolí nuly V tak, aby $(\mathrm{i}-1)V \subset V \cup (V+1)$. Kdybychom se omezili na nějakou „slušnou" množinu V s plochou $\mu(V)$, tak množina $(\mathrm{i}-1)V$ má plochu $2\mu(V)$, a tu máme pokrýt dvěma kopiemi V a $V+1$ původní množiny. Až na nějaké hraniční body by musela platit rovnost $(\mathrm{i}-1)V = V \cup (V+1)$.

Hned je jasné, že jako V nemůže sloužit kruh, protože kruh dvojnásobné plochy nepokryjeme dvěma původními kruhy. A stejně nevhodné jsou i další množiny, jejichž obrázek si v ruce načrtneme. Z toho však nelze usoudit, že vhodné V neexistuje.

V roce 1981 Hutchinson [12] dokázal následující větu.

Věta 5. *Pro libovolná kontrahující zobrazení* [2] $f_1, \ldots, f_r : \mathbb{R}^n \mapsto \mathbb{R}^n$ *existuje jediná neprázdná kompaktní množina* $C \subset \mathbb{R}^n$ *taková, že*

$$C = f_1(C) \cup \ldots \cup f_r(C)\,.$$

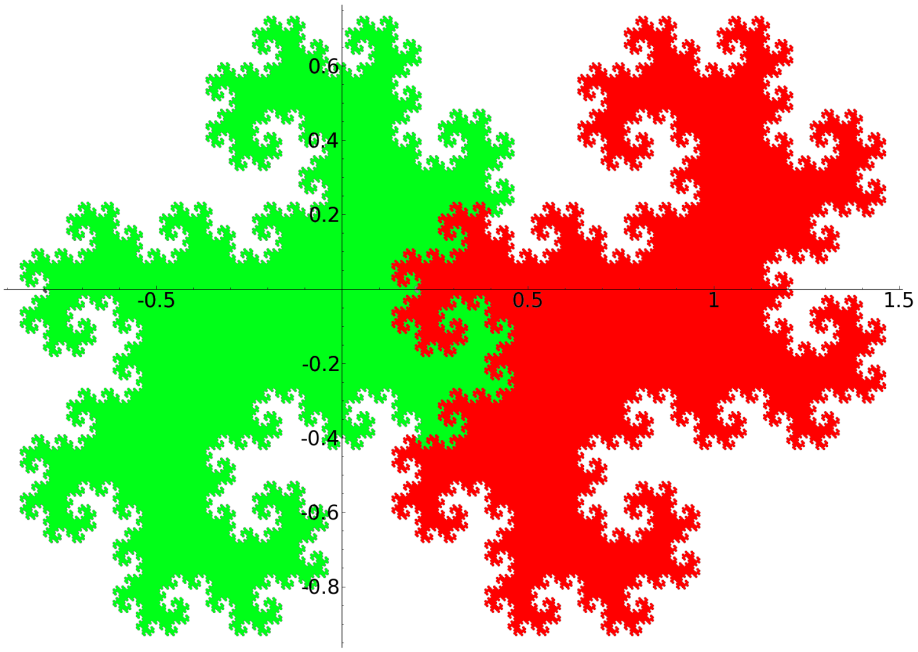
Pro $\beta = \mathrm{i} - 1$ nám tato věta aplikovaná na dvě kontrahující zobrazení komplexní roviny $f_1(z) = \frac{z}{\beta}$ a $f_2(z) = \frac{z+1}{\beta}$ zaručí existenci V s vlastností $V = \frac{1}{\beta}V \cup \frac{1}{\beta}(V+1)$.

Jak V vypadá? Na to odpoví pohled do důkazu Hutchinsonovy věty. Nejdříve se ukáže, že na prostoru všech kompaktních podmnožin $\mathbb{R}^n$, který je vybaven Hausdorffovou metrikou, je zobrazení $F : X \mapsto f_1(X) \cup \ldots \cup f_r(X)$ také kontrahující. Pak už stačí použít Banachovu větu o pevném bodě kontrahujícího zobrazení. Pevný bod lze zkonstruovat jako limitu iterací kontrahujícího zobrazení libovolné počáteční kompaktní množiny. Takže stačí vzít např. V_0 kruh. Pak iterace $F^k(V_0)$ s dostatečně velkým k bude velice blízká hledané množině V, viz obr. 1. Tato množina má fraktální hranici. Na druhé straně když už víme, že každé komplexní číslo lze v bázi $\beta = \mathrm{i} - 1$ a abecedě $\{0, 1\}$ reprezentovat, stačí položit $V = \{z \in \mathbb{C} \mid (z)_\beta = 0 \bullet a_1 a_2 a_3 \ldots\}$. Pro komplexní rovinu zřejmě platí $\mathbb{C} = \mathbb{Z}[\mathrm{i}] + V$, a rovinu lze tedy periodicky vydláždit stejnými kopiemi fraktální dlaždice V.

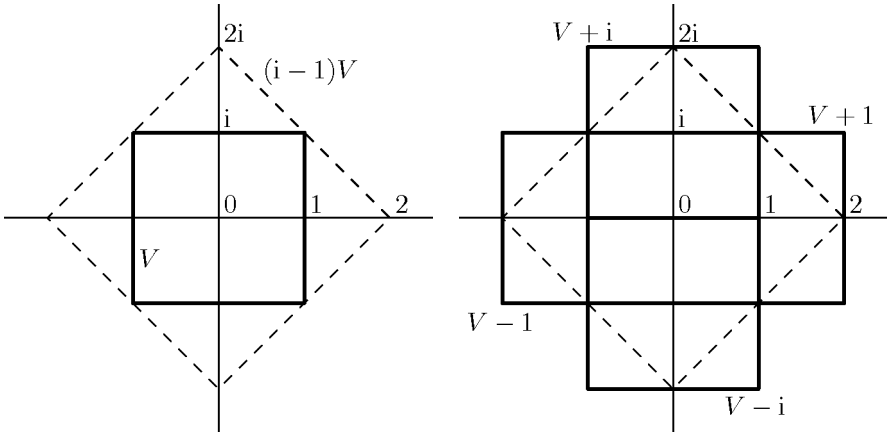
Problém s hledáním vhodné množiny V je způsoben tím, že na pokrytí βV jsme povolili jenom dvě kopie V. Kdybychom zvětšili dostatečně abecedu, pokryjeme βV snadno. Na obr. 2. je zobrazena jiná volba množiny V: β násobek množiny V je pokryt 5 kopiemi V posunutými o prvky abecedy $\{0, 1, -1, \mathrm{i}, -\mathrm{i}\}$.

Soustavy, ve kterých je použito více cifer, než je nutné, se nazývají redundantní. Čísla v nich nemají jednoznačný zápis. Velkým kladem redundantních soustav je, že umožňují při sčítání dvou řetězců zpracovávat všechny pozice paralelně. Máme-li dostatek procesorů, rychlost, kterou získáme součet dvou čísel, nezávisí na délce řetězců. První algoritmus pro paralelní sčítání navrhl Avizienis v roce 1961, kdy představy

[2] Konečná množina kontrahujících zobrazení na úplném metrickém prostoru se obecně nazývá *systém iterovaných funkcí* (angl. iterated function system), tento koncept byl zaveden v [12] a často slouží ke konstrukci fraktálních množin.



Obr. 1. Množiny V a $V+1$ splňující vlastnost $(\mathrm{i}-1)V = V \cup (V+1)$.



(a) (b)

Obr. 2. (a) Jiná volba množiny V, vyobrazena je také množina $(\mathrm{i}-1)V$. (b) Množina $(\mathrm{i}-1)V$ pokryta 5 kopiemi V.

o použití libovolného počtu procesorů byly hodně vzdálené realitě. Algoritmus pracoval s desítkovou soustavou a třinácti ciframi $\{-6,-5,\ldots,-1,0,1,\ldots,5,6\}$, viz [2]. Také v soustavě se základem $\beta = \mathrm{i}-1$ lze paralelně sčítat, musíme však pracovat alespoň s pětiprvkovou množinou cifer, viz [8].

2. Soustavy s iracionální bází

Pro zjednodušení situace se omezíme na reprezentace reálných čísel. Jako bázi β si zvolíme libovolné reálné číslo $\beta > 1$. Pozorný čtenář si všiml, že popsaný hladový algoritmus nevyžaduje, aby báze byla přirozeným číslem. Soustavy s neceločíselným základem začal jako první studovat Alfréd Rényi v [17]. Předpokládejme v této kapitole, že $\beta \notin \mathbb{N}$. Cifry, které hladový algoritmus pro zápis kladného čísla používá, jsou $0, 1, \ldots, \lfloor \beta \rfloor$.

Příklad 6. Uvažujme základ $\beta = \frac{1+\sqrt{5}}{2}$, tj. *zlatý řez*, větší z kořenů kvadratické rovnice $x^2 = x+1$. Obvykle se značí ϕ a my toto značení nadále použijeme. Rozvoje čísel s tímto základem budou využívat cifry 0 a 1. Protože $\phi^k = \phi^{k-1} + \phi^{k-2}$ pro každý index $k \in \mathbb{Z}$, hladový algoritmus nepřipustí, aby dva sousední koeficienty x_{k-1} a x_{k-2} byly oba jedničky, viz [21]. To je rozdíl oproti dvojkové soustavě, kde žádná kombinace cifer není v zápisu čísel zakázaná. Hledejme rozvoj čísla $x = 2$. Protože $\phi \leqslant 2 < \phi^2$, hladový algoritmus dává $x_1 = 1$ a $2 = x_1\phi + y$, kde pro zbytek y platí $y = 2 - \phi = \phi^{-2}$. Poslední rovnost plyne ze vztahu $\phi^2 = \phi + 1$. V dalším kroku hladového algoritmu dostaneme už nulový zbytek a algoritmus se zastaví. Získali jsme tak vyjádření $2 = \phi + \phi^{-2}$, což obvykle zapisujeme $(2)_\phi = 10\bullet01$. V rozvoji celého čísla 2 se uplatní i záporné mocniny báze. Tento jev se u soustav s celočíselnou bází β nevyskytoval. To vedlo k zavedení nových „celých“ čísel v článku [4].

Pro obecný základ $\beta > 1$ se definují množiny *β-celých čísel* a čísel s konečným β-rozvojem předpisem

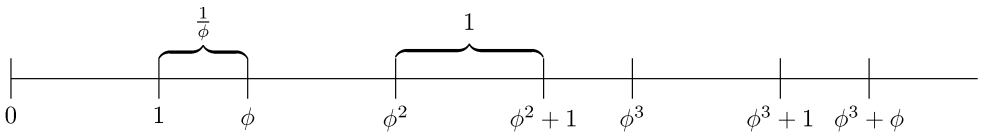
$$\mathbb{Z}_\beta = \{\pm x \mid x \in \mathbb{R}, x \geqslant 0 \text{ a } (x)_\beta = x_k x_{k-1} \ldots x_0 \bullet\} \quad \text{a} \quad \mathrm{Fin}(\beta) = \bigcup_{n \in \mathbb{N}} \frac{1}{\beta^n} \mathbb{Z}_\beta.$$

Je-li základ $\beta \in \mathbb{N}, \beta \geqslant 2$, množina $\mathbb{Z}_\beta = \mathbb{Z}$. Jinak je $\mathbb{Z}_\beta \neq \mathbb{Z}$. Pro všechny základy je však množina $\mathbb{Z}_\beta$ diskrétní a relativně hustá, tj. nemá vlastní hromadné body a vzdálenosti mezi nejbližšími sousedy jsou omezené. Např. pro zlatý řez má množina $\mathbb{Z}_\phi$ mezi sousedy dva různé typy mezer, a to mezeru délky 1 a mezeru délky $\frac{1}{\phi}$, viz obr. 3. Je-li báze $\beta = \frac{3}{2}$, vzdálenosti mezi sousedy nabývají nekonečně mnoha hodnot.

Mezi fyziky vzrostl zájem o množinu $\mathbb{Z}_\phi$ po objevu kvazikrystalů, tj. pevných látek, jejichž difrakční obrázky lokálně vykazují pětičetnou rotační symetrii. Tato symetrie se u běžných krystalů nemůže vyskytovat. Objev prvního kvazikrystalu se datuje rokem 1982, kdy Shechtman[3] se spolupracovníky prudce zchladili slitinu hliníku a manganu, viz [18]. Od té doby byly objeveny i další pevné látky s krystalograficky zakázanými symetriemi, a to s lokální osmičetnou a dvanáctičetnou symetrií. Dnes používané matematické modely kvazikrystalů popisují koordináty atomů pomocí množiny $\mathbb{Z}_\phi$ (v případě pětičetné symetrie) namísto množiny $\mathbb{Z}$ v klasických krystalech, viz [4].

Viděli jsme, že množina $\mathbb{Z}_\phi$ není uzavřená vůči sčítání. Vskutku, číslo $1 + 1 = 2$ má v bázi ϕ rozvoj s nenulovými ciframi i za zlomkovou tečkou. Pro základ $\beta \notin \mathbb{N}$ platí obecně, že $\mathbb{Z}_\beta + \mathbb{Z}_\beta \not\subset \mathbb{Z}_\beta$. Z aritmetického hlediska je však uspokojující, když součet dvou čísel s konečným rozvojem má také konečný rozvoj. To už implikuje, že

[3] Dan Shechtman dostal za tento objev v letošním roce Nobelovu cenu za chemii.



Obr. 3. Několik nejmenších nezáporných ϕ-celých čísel.

součin dvou čísel s konečným rozvojem má také konečný rozvoj. Ani taková vlastnost však není samozřejmá, jak dokazuje následující věta, která pochází od Frougny a Solomyaka [9].

Věta 7. *Nechť pro bázi $\beta > 1$ platí* $\mathrm{Fin}(\beta) + \mathrm{Fin}(\beta) \subset \mathrm{Fin}(\beta)$. *Pak β je algebraické celé číslo a všechny jeho sdružené kořeny jsou v absolutní hodnotě menší než jedna.*

Připomeňme, že číslo β nazýváme *algebraickým*, je-li kořenem nějakého polynomu $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$, kde $a_k \in \mathbb{Q}$. Takovýchto polynomů je víc, ale jenom jeden mezi nimi má minimální stupeň, tomu říkáme *minimální polynom* čísla β. Ostatním kořenům minimálního polynomu se říká *sdružené* k číslu β. Stupněm algebraického čísla β se rozumí stupeň jeho minimálního polynomu. Jsou-li koeficienty minimálního polynomu celočíselné, nazýváme β algebraické celé číslo. Např. zlatý řez $\phi = \frac{1+\sqrt{5}}{2}$ je algebraické celé číslo s minimálním polynomem $x^2 - x - 1$ a k němu sdružený kořen je $\phi' = \frac{1-\sqrt{5}}{2}$.

Snadno se ukáže, že algebraické celé číslo $\beta > 1$, jehož sdružené kořeny jsou v absolutní hodnotě menší než jedna, má následující vlastnost: existuje $\lambda \neq 0$ takové, že

$$\lim_{n\to\infty} \|\lambda\beta^n\| = 0, \tag{1}$$

kde $\|x\|$ značí vzdálenost x od nejbližšího celého čísla. Algebraická čísla $\beta > 1$ s vlastností definovanou (1) se nazývají *Pisotova čísla*. Na druhé straně lze ukázat, že každé algebraické Pisotovo číslo je algebraické celé a jeho sdružené kořeny jsou v absolutní hodnotě menší než jedna. Větu 7 bychom tedy mohli vyslovit i ve tvaru, že uzavřenost $\mathrm{Fin}(\beta)$ vůči sčítání vynucuje, aby základem β bylo Pisotovo číslo. Množina Pisotových čísel, obvykle se značí S, má zajímavé vlastnosti: je uzavřená, její minimální prvek je reálný kořen polynomu x^3-x-1 (jeho hodnota je $\beta = 1,32471\ldots$), množina S má nekonečně mnoho hromadných bodů, nejmenší hromadný bod je zlatý řez ϕ atp. Pro další podrobnosti odkazujeme čtenáře na [5]. Dlouholetou nevyřešenou otázkou (Pisotův-Vijayaraghavanův problém) je existence čísla s vlastností (1), které by nebylo algebraické.

Pisotova čísla hrají v numeračních systémech důležitou roli: je-li základ β Pisotovo číslo, pak množina β-celých čísel má pouze konečně mnoho různých mezer mezi sousedními prvky [19]. Navíc posloupnost těchto mezer lze generovat přepisovacími pravidly [7].

Demonstrujme to na příkladě zlatého řezu. Zde, jak jsme již zmínili, mezi sousedy v množině $\mathbb{Z}_\phi$ jsou mezery dvojího typu: mezera délky 1, tu označme písmenem A, a mezera délky $\frac{1}{\phi}$, tu označme písmenem B. Opakovaně budeme přepisovat slova v binární abecedě $\{A, B\}$ pomocí přepisovacích pravidel „A zaměň za AB“ a „B zaměň za A“, přičemž začneme s jednopísmenným slovem A. Postupně dostáváme:

$$A \mapsto AB \mapsto ABA \mapsto ABAAB \mapsto ABAABABA \mapsto ABAABABAABAAB \mapsto \dots$$

Každé další slovo má jako svoji předponu předchozí slovo, takže nekonečným přepisováním získáme nekonečně dlouhé slovo, které kóduje posloupnost mezer v množině $\mathbb{Z}_\phi$, srovnej s obr. 3. Délkami generovaných slov jsou postupně $1, 2, 3, 5, 8, 13, \dots$, tedy Fibonacciho čísla. Numerační soustava se základem zlatý řez úzce souvisí se soustavou, ve které se přirozená čísla vyjadřují pomocí Fibonacciho čísel, pro tento účel definovaných jako $F_0 = 1, F_1 = 2$ a $F_n = F_{n-1} + F_{n-2}$ pro každé $n = 2, 3, 4, \dots$. Libovolné $m \in \mathbb{N}$ lze vyjádřit ve tvaru $m = F_{k_n} + F_{k_{n-1}} + \dots + F_{k_0}$, přičemž $k_i - 1 > k_{i-1}$ pro každé $i = 1, 2, \dots, n$. Tedy zápis nedovoluje použít dvě sousedící Fibonacciho čísla. Tomuto zápisu, zavedenému v [21], se říká Zeckendorfova reprezentace čísla. Pro další souvislosti, např. mezi prováděním aritmetických operací s čísly zapsanými v bázi ϕ a v Zeckendorfově reprezentaci, odkazujeme čtenáře na [11] nebo česky psanou knihu [14].

3. Pisotova čísla a aperiodická dláždění prostoru

Další hezkou vlastností pisotovského základu β je souvislost takového numeračního systému s dlážděním prostoru.

Dláždění prostoru $\mathbb{R}^n$ je dáno konečnou množinou $\mathcal{D}$ dlaždic, jejichž kopiemi lze vyplnit celý prostor bez mezer a toho, aby se dlaždice překrývaly. Upřesněme, že *dlaždicí* $D \in \mathcal{D}$ se rozumí kompaktní množina s neprázdným vnitřkem v $\mathbb{R}^n$ taková, že D se shoduje s uzávěrem svého vnitřku; kopie dlaždice D je množina $x + D$ pro nějaké $x \in \mathbb{R}^n$; dvě kopie dlaždic se nepřekrývají, pokud žádný vnitřní bod jedné dlaždice nepatří jiné dlaždici. Rozhodnout o dané konečné množině $\mathcal{D}$, zda její pomocí lze vydláždit prostor, je obecně velice obtížná úloha.

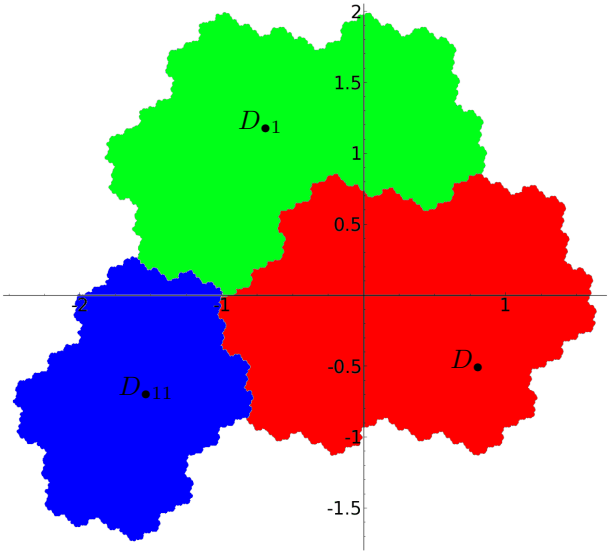
Pro názornost ukážeme, jak využít kubické iracionality k vydláždění roviny. Uvažujme kubický polynom $x^3 - x^2 - x - 1$. Jeden jeho reálný kořen je $\beta = 1,83929\dots$, další dva kořeny tvoří komplexně sdružená čísla γ a $\overline{\gamma}$, v absolutní hodnotě menší než 1. Číslo β je tedy Pisotovo. Numerační systém používá cifry 0 a 1, a protože pro β platí $\beta^3 = \beta^2 + \beta + 1$, hladový algoritmus nepřipustí, aby β-rozvoj nějakého čísla obsahoval tři po sobě jdoucí jedničky, tj. řetězec 111. Platí tedy

$$\mathrm{Fin}(\beta) = \Big\{ \pm \sum_{k=m}^{n} x_k \beta^k \;\Big|\; m, n \in \mathbb{Z},\ x_i \in \{0,1\} \text{ a } x_{i+2}x_{i+1}x_i \neq 111 \Big\}.$$

Ke konstrukci dláždění roviny budeme využívat pouze nezáporné prvky $\mathrm{Fin}(\beta)$. Ty lze rozdělit disjunktně do spočetně mnoha množin podle toho, jaká posloupnost 0 a 1 se vyskytuje v jejich zápise za zlomkovou tečkou. Nechť tedy w je řetězec v abecedě $\{0, 1\}$, který neobsahuje tři po sobě jdoucí jedničky. Množinu takových řetězců označme R a položme

$$T_{\bullet w} = \{x \geqslant 0 \mid (x)_\beta = x_k x_{k-1} \dots x_1 x_0 \bullet w\} \qquad \text{pro každé } w \in R\,.$$

Speciálně, je-li w prázdný řetězec, tj. za zlomkovou tečkou nejsou žádné nenulové cifry, je $T_\bullet = \mathbb{Z}_\beta \cap [0, +\infty)$.



Obr. 4. Dlaždice $D_\bullet$, $D_{\bullet 1}$ a $D_{\bullet 11}$.

Definujme zobrazení množiny $\mathrm{Fin}(\beta) \cap [0, +\infty)$ do $\mathbb{C}$ předpisem

$$x = \sum_{k=m}^{n} x_k \beta^k \;\mapsto\; x' = \sum_{k=m}^{n} x_k \gamma^k.$$

Pro čtenáře sběhlého v algebře dodejme, že přiřazení $x \mapsto x'$ je definováno izomorfizmem σ mezi algebraickými tělesy $\mathbb{Q}(\beta)$ a $\mathbb{Q}(\gamma)$.

Protože sdružený kořen γ je v absolutní hodnotě menší než jedna, je obraz všech nezáporných β-celých čísel, tj. $(T_\bullet)' = \{x' = \sigma(x) \mid x \geqslant 0,\ x \in \mathbb{Z}_\beta\}$, množina omezená v $\mathbb{C}$. Uzávěr této množiny se nazývá *centrální dlaždice* příslušející k Pisotovu číslu β, značí se $D_\bullet$ a je znázorněn na obr. 4. O této dlaždici bylo ukázáno [1], že je uzávěrem svého vnitřku a že hranice $D_\bullet$ má Lebesgueovu míru 0. Nyní už můžeme popsat dláždění celé gaussovské roviny. Definujme dlaždice

$$D_{\bullet w} := \overline{\{x' \mid x \in T_{\bullet w}\}} \quad \text{pro každé } w \in R,$$

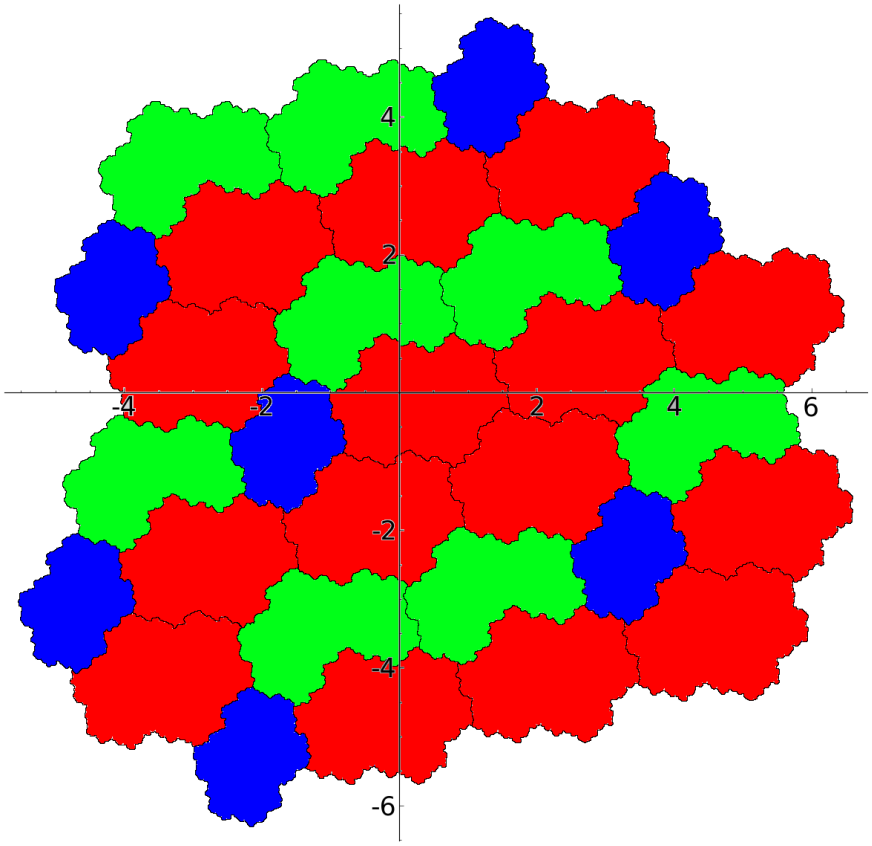
kde pruh nad množinou značí její uzávěr v klasické eukleidovské metrice na $\mathbb{C}$. Část dláždění je na obr. 5. Toto dláždění má následující vlastnosti:

a) Každá dlaždice $D_{\bullet w}$ je posunutou kopií jedné ze tří různých dlaždic $D_\bullet$, $D_{\bullet 1}$ nebo $D_{\bullet 11}$.

b) Každá dlaždice po zvětšení faktorem $\frac{1}{\gamma}$ se dá poskládat z kopií $D_\bullet$, $D_{\bullet 1}$ a $D_{\bullet 11}$.

Odůvodněme tyto vlastnosti. Množinu řetězců R neobsahující tři po sobě jdoucí jedničky lze totiž napsat jako disjunktní sjednocení

$$R = \{0w \mid w \in R\} \cup \{10w \mid w \in R\} \cup \{110w \mid w \in R\}\,.$$



Obr. 5. Část dláždění gaussovské roviny dlaždicemi $D_\bullet$, $D_{\bullet 1}$ a $D_{\bullet 11}$.

Z definice množiny $T_{\bullet w}$ přímo plyne

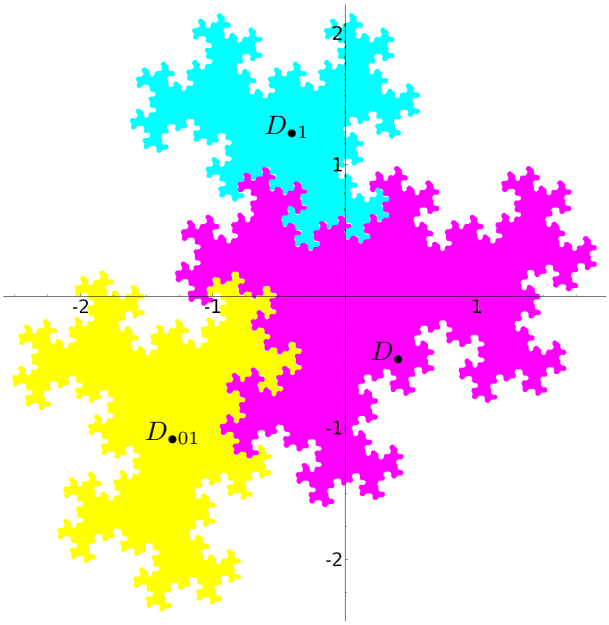
$$T_{\bullet 0w} = T_\bullet + \bullet 0w\,, \qquad T_{\bullet 10w} = T_{\bullet 1} + \bullet 00w\,, \quad T_{\bullet 110w} = T_{\bullet 11} + \bullet 000w\,,$$

kde $\bullet w$ ztotožňujeme s číslem x, pro které $(x)_\beta = \bullet w$. Dlaždice $D_{\bullet 0w}$ je tedy posunutou kopií dlaždice $D_\bullet$, dlaždice $D_{\bullet 10w}$ je kopií $D_{\bullet 1}$ a dlaždice $D_{\bullet 110w}$ je kopií $D_{\bullet 11}$. Pro odůvodnění vlastnosti **b)** si stačí uvědomit, že $\frac{1}{\beta}T_\bullet$ je množinou čísel, která mají za zlomkovou tečkou nanejvýš jednu cifru. Proto zřejmě $\frac{1}{\beta}T_\bullet = T_\bullet \cup T_{\bullet 1}$, což, vyjádřeno v dlaždicích, znamená

$$\frac{1}{\gamma}\, D_\bullet = D_\bullet \cup D_{\bullet 1}.$$

Obdobně ze vztahů $\frac{1}{\beta}T_{\bullet 1} = T_{\bullet 11} \cup T_{\bullet 01} = T_{\bullet 11} \cup \big(T_\bullet + \bullet 01\big)$ a $\frac{1}{\beta}T_{\bullet 11} = T_{\bullet 011} = T_\bullet + \bullet 011$ dostaneme další škálovací identity. Vlastnost **b)** se nazývá soběpodobnost dláždění a dává návod, jak z centrální dlaždice $D_\bullet$ nagenerovat dláždění celé roviny postupným škálováním faktorem $\frac{1}{\gamma}$.

Konstrukci množin $D_{\bullet w}$, kterou jsme právě popsali, lze provést pro každé Pisotovo číslo β stupně d. Tyto množiny budou tvořit pokrytí prostoru $\mathbb{R}^{d-1}$, nemusejí však



Obr. 6. Základní trojice dlaždic odpovídající kořenu rovnice $x^3 = x^2 + 1$.

tvořit dláždění prostoru, a to kvůli překryvům. Na otázku, kdy tvoří dláždění, odpovídá částečně následující věta z [1], která spojuje geometrické a aritmetické vlastnosti numeračního systému.

Věta 8. *Nechť $\beta > 1$ je Pisotova jednotka*[4] *stupně $d \geqslant 2$ a R množina všech konečných řetězců vyskytujících se v β-rozvojích reálných čísel. Pak množiny $D_{\bullet w}$, kde w probíhá R, tvoří dláždění prostoru $\mathbb{R}^{d-1}$ právě tehdy, když* $\mathrm{Fin}(\beta) + \mathrm{Fin}(\beta) \subset \mathrm{Fin}(\beta)$.

V případě, že množiny $D_{\bullet w}$ tvoří dláždění, je počet různých dlaždic roven alespoň stupni β a závisí na množině řetězců, které se vyskytují v rozvojích čísel v bázi β. Např. nejmenší Pisotovo číslo β, které je kubické, generuje dláždění s pěti různými dlaždicemi. Různost dlaždic nevylučuje, že jedna dlaždice je násobkem jiné. Např. na obr. 4. vidíme, že $D_{\bullet 11}$ je posunutou $\gamma D_{\bullet}$. Zajímavé je dláždění pomocí kubické iracionality, která je kořenem rovnice $x^3 = x^2 + 1$, viz obr. 6. Všechny dlaždice jsou pouze kopiemi centrální dlaždice v různých velikostech.

Zásadní rozdíl mezi dlážděním roviny pomocí dlaždice V, které jsme získali při zápisu komplexních čísel v bázi $\beta = \mathrm{i} - 1$, a dlážděním konstruovaným pro Pisotovo číslo je, že Pisotova čísla dávají *aperiodická* dláždění, tedy dláždění nelze posunout o nějaký vektor tak, aby se krylo s původním dlážděním.

[4] Minimální polynom čísla β má absolutní člen ± 1.

4. Závěr

Náš příspěvek se věnoval pouze pozičním zápisům čísel. Tím nechceme říct, že jiné než poziční systémy nejsou důležité. Např. zápis reálného čísla pomocí řetězového zlomku, tj. ve tvaru

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{a_3} \cdots}}, \quad \text{kde } a_0 \in \mathbb{Z} \text{ a } a_i \in \mathbb{N} \text{ pro } i \geqslant 1, \tag{2}$$

je nenahraditelný při racionálních aproximacích iracionálních čísel. V matematické literatuře lze nalézt různá zobecnění řetězových zlomků. Jedno z nich, zavedeno Bernatem [3], připouští v zápisu (2) jako koeficienty ϕ-celá čísla, tj. $a_i \in \mathbb{Z}_\phi$. Zajímavé výsledky o řetězových zlomcích by však samy stačily na dlouhý článek.

Poziční soustavy s celočíselným základem a rozšířenou množinou cifer, tedy soustavy umožňující paralelní zpracování cifer daného čísla, se dnes běžně využívají ve víceprocesorových aritmetických jednotkách. Ty se uplatňují hlavně při algoritmech pro šifrování, které pracují s velkými čísly, např. metoda RSA. O těchto soustavách jsme se zmínili jenom krátce. Do povědomí širší odborné veřejnosti totiž vstoupily samy kvůli „slavné“ chybě procesoru Pentium odhalené v roce 1997. Pentium (tenkrát i dnes) používá pro dělení algoritmus SRT a redundantní soustavu se základem $\beta = 4$ a pěti ciframi $\{-2, -1, 0, 1, 2\}$, viz [15].

Praktických využití pozičních soustav s neceločíselným základem zatím není mnoho. Kromě již zmíněných modelů kvazikrystalů je pozoruhodná další aplikace numerační soustavy se základem ϕ (zlatý řez). Ta posloužila Daubechiesové a spol. k robustnímu kódování analogového signálu, viz [6].

Shrňme nicméně, že studium pozičních systémů přináší řadu hezkých matematických problémů, které zasahují do teorie čísel, teorie fraktálů, teorie komplexní proměnné či topologie.

Poděkování: Autoři děkují své kolegyni Ing. Ľ. Balkové, Ph.D. a RNDr. Pavle Pavlíkové, Ph.D. za pečlivé přečtení rukopisu. Tato práce byla podpořena grantem Studentské grantové soutěže ČVUT č. SGS11/162/OHK4/3T/14.

Literatura

[1] Akiyama, S.: *On the boundary of self affine tilings generated by Pisot numbers.* J. Math. Soc. Jap. *54* (2002), 283–308.

[2] Avizienis, A.: *Signed-digit number representations for fast parallel arithmetic.* IRE Trans. Electron. Comput. *10* (1961), 389–400.

[3] Bernat, J.: *Continued fractions and numeration in the Fibonacci base.* Discrete Math. *306* (2006), 2828–2850.

[4] Burdík, Č., Frougny, Ch., Gazeau, J. P., Krejcar, R.: *Beta-integers as natural counting systems for quasicrystals.* J. Phys. A-Math. Gen. *31* (1998), 6449–6472.

[5] Boyd, D. W.: *Pisot and Salem numbers in intervals on the real line.* Math. Comput. *32* (1978), 1244–1260.

[6] Daubechies, I., Güntürk, C.S., Wang, Y., Yilmaz, Ö.: *The golden ratio encoder.* IEEE Trans. Inform. Theory *56* (2010), 5097–5110.

[7] Fabre, S.: *Substitutions et β-systèmes de numération.* Theor. Comput. Sci. *137* (1995), 219–236.

[8] Frougny, Ch., Pelantová, E., Svobodová, M.: *Parallel addition in non-standard numeration systems.* Theor. Comput. Sci. *412* (2011), 5714–5727.

[9] Frougny, Ch., Solomyak, B.: *Finite beta-expansions.* Ergod. Theor. Dyn. Syst. *12* (1992), 713–723.

[10] Gauss, C. F.: *Werke.* Teubner 1900.

[11] Graham, R. L., Knuth, D. E., Patashnik, O.: *Concrete mathematics: a foundation for computer science.* 2nd ed., 1994, Addison-Wesley.

[12] Hutchinson, J.: *Fractals and self-similarity.* Indiana Univ. Math. J. *30* (1981), 713–747.

[13] Katai, I., Szabó, J.: *Canonical number systems*, Acta Sci. Math. *37* (1975), 255–280.

[14] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel*, Academia, Praha 2011.

[15] Muller, J.-M.: *Elementary functions, algorithms and implementation.* 2nd ed., Birkhäuser, Boston 2006.

[16] Penney, W.: *A "binary" system for complex numbers.* J. ACM *12* (1965), 247–248.

[17] Rényi, A.: *Representations for real numbers and their ergodic properties.* Acta Math. Acad. Sci. Hung. *8* (1957), 477–493.

[18] Shechtman, D., Blech, I., Gartias, D., Cahn, J. W.: *Metallic phase with Long-range orientational order and no translation symmtery.* Phys. Rev. Lett. *53* (1984), 1951–1953.

[19] Schmidt, K.: *On periodic expansions of Pisot numbers and Salem numbers.* Bull. London Math. Soc. *12* (1980), 269–278.

[20] Thurston, W. P.: *Groups, tilings, and finite state automata.* AMS Colloquium Lecture Notes, American Mathematical Society, Boulder 1989.

[21] Zeckendorf, E.: *Représentation des nombres naturels par une somme des nombres de Fibonacci ou de nombres de Lucas.* Bull. Soc. Roy. Sci. Liège *41* (1972), 179–182.