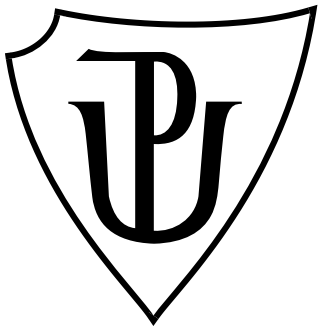
Univerzita Palackého v Olomouci
Přírodovědecká fakulta
Katedra algebry a geometrie



Bakalářská práce

Řetězové zlomky

Vypracoval: Lukáš Klouda
Studijní program: B1701 Fyzika
Studijní obor: Fyzika-Matematika
Forma studia: Prezenční
Vedoucí práce: Doc. RNDr. Alena Vanžurová, CSc.
Rok obhajoby: 2013

Prohlášení

Prohlašuji, že jsem předloženou bakalářskou práci vypracoval samostatně pod vedením doc. RNDr. Aleny Vanžurové, CSc. a použil výhradně zdroje uvedené v oddílu ‘Reference’.

V Olomouci, 27.6.2013, Lukáš Klouda.

Poděkování

Děkuji vedoucí práce, doc. RNDr. Alena Vanžurové, CSc., za rady a připomínky. Děkuji rodině za podporu ve studiu.

Bibliografická identifikace

Jméno a příjmení autora	Lukáš Klouda
Název práce	Řetězové zlomky
Typ práce	bakalářská
Pracoviště	Katedra algebry a geometrie
Vedoucí práce	Doc. RNDr. Alena Vanžurová, CSc.
Rok obhajoby práce	2013
Abstrakt	Základní vlastnosti konečných a nekonečných řetězových zlomků. Aplikace: řešení kongruenčních rovnic, aproximace čísel, Pellovy rovnice.
Klíčová slova	řetězový zlomek, kongruenční rovnice, diofantická rovnice, nejlepší racionální přiblížení, Pellova rovnice
Počet stran	31
Počet příloh	0
Jazyk	český

Bibliographical identification

Author's first name and surname	Lukáš Klouda
Thesis title	Continued Fractions
Type of thesis	Bachelor
Department	Department of Algebra and Geometry
Supervisor	Doc. RNDr. Alena Vanžurová, CSc.
Year of presentation	2013
Abstract	Fundamentals of finite and infinite continued fractions. Applications: congruence equations, number approximation, Pell's equation.
Key words	continued fraction, congruence equation, Diophantine equation, best rational approximation, Pell's equation
Number of pages	31
Number of appendices	0
Language	Czech

Obsah

Úvod **1**

1 Konečné řetězové zlomky **2**

2 Nekonečné řetězové zlomky **7**

3 Řešení kongruenčních rovnic **11**

4 Lineární diofantické rovnice o dvou neznámých **12**
4.1 Převedení na kongruenční rovnici 1. stupně 12
4.2 Metoda výpočtu partikulárního řešení 12
4.3 Příklady 14

5 Aproximace **15**
5.1 Teorie 15
5.2 Nejlepší přiblížení druhého druhu 19
5.3 Příklady 23

6 Pellova rovnice **24**
6.1 Kvadratické iracionality 24
6.2 Pellova rovnice 26
6.3 Příklady 29

Vysvětlivky **30**

Reference **31**

Úvod

Jako téma své bakalářské práce jsem si vybral řetězové zlomky. Zaujalo mě to, že existuje mnoho jejich aplikací (zejména v oblasti teorie čísel). V literatuře lze nalézt další souvislosti, například s teorií uzlů, algebrou oborů integrity, teorií ortogonálních polynomů, atd. V bakalářském studijním programu není toto téma zařazeno.

Cílem práce je vystavění teorie k některým aplikacím řetězových zlomků. Základní vlastnosti řetězových zlomků jsou uvededny v oddílech 1, 2. Příklady jsou voleny tak, aby byly jednoduché a ilustrativní. Dalším cílem práce je uvedení některých aplikací – řešení kongruenčních rovnic (oddíl 3), řešení diofantických rovnic (oddíl 4), racionální aproximace (oddíl 5), řešení Pellových rovnic (oddíl 6). Přitom se snažím vystavět teorii tak, aby ke všem tvrzením byly připojeny důkazy. Na konci oddílů uvádím jednoduše formulované příklady, jež mají demonstrovat použití vybudované teorie.

V oddílu 'Vysvětlivky' na straně 30 je uveden matematický formalizmus, jenž se běžně nepoužívá a který není definován přímo v textu. *Prosím čtenáře, aby se s ním seznámil před tím, než začne číst hlavní text.* Tento formalizmus považuji za výhodný z důvodu větší stručnosti nebo lepšího dorozumění. V rámci práce jsem zavedl též vlastní značení, abych lépe odlišil vnímání řetězového zlomku jako symbolu a jako čísla. Myslím si, že takto dosáhnu větší srozumitelnosti pro čtenáře, kteří se s problematikou řetězových zlomků ještě nesetkali.

V oddílu 'Reference' na straně 31 jsou uvedeny použité zdroje. V oddílech 1, 2 jsem čerpal zejména z [1], [2], v oddílu 3 věnovaném řešení kongruenčních rovnic z [1], v oddílu 4 o diofantických rovnicích z [1], [3], v oddílu 5 o aproximacích z [2], [1] a v oddílu 6 o Pellových rovnicích z [2], [3], [1]. V samotném textu na reference neodkazuji – k tvrzením jsou připojeny důkazy.

Věty, lemmata a důsledky jsou číslovány společně, rovněž i drobnější tvrzení (pozorování a poznámky) jsou číslována společně. Samostatně čísluji definice, algoritmy, úmluvy a příklady.

Jazyk volím jednoduchý, jazyková forma definic a tvrzení se často opakuje, což považuji za dobré, neboť čtenáři tak umožním soustředit se spíše na význam textu, než na různorodost formy.

1 Konečné řetězové zlomky

$(\mathbb{Z}, +, -, 0, \cdot, 1)$ je eukleidovský obor integrity, s eukleidovskou funkcí (normou) ν, '$k \mapsto |k|$', tj. absolutní hodnotou. Je tedy i oborem integrity hlavních ideálů, přičemž každý jeho vlastní ideál lze psát jako $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$, kde $n \in \mathbb{N}$, $n > 1$. Kongruenci na $\mathbb{Z}$ indukovanou ideálem $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$ budeme značit symbolem $\equiv_n$. Třídu kongruence $\equiv_n$ danou reprezentantem $a \in \mathbb{Z}$ budeme značit $[a]_{\equiv_n}$ nebo $\overline{a}$ (bude-li zřejmé o kterou kongruenci se jedná).

Vlastnost

$$\forall (a, b \in \mathbb{Z},\ b \neq 0)\ \exists q, r \in \mathbb{Z} :\ a = bq + r\ , \tag{1}$$

kde $(r = 0 \vee |r| < |b|)$, umožňuje definovat celočíselné dělení. Číslo r s touto vlastností nazveme *eukleidovským zbytkem* při dělení a číslem b.
Nabízí se otázka, jak je to s jednoznačností eukleidovských zbytků. Mohou nastat právě dvě situace:

1. $b \mid a$. Pak čísla q, r z (1) jsou dána jednoznačně ve tvaru $a = b \cdot (a/b) + 0$. Pak zřejmě $\mathrm{NSD}(a, b) = b = \mathrm{NSD}(b, 0) = \mathrm{NSD}(b, r)$.

2. $b \nmid a$. Pak čísla q, r z (1) nejsou dána jednoznačně a zbytky r jsou určeny třídou $[a]_{\equiv b} = \{a + bk;\ k \in \mathbb{Z}\}$ a požadavkem $|r| < |b|$. Protože je (největší) společný násobek x, b pro $x \in [a]_{\equiv_b}$ vlastností celé třídy $[a]_{\equiv_b}$, platí pro eukleidovské zbytky $\mathrm{NSD}(r, b) = \mathrm{NSD}(a, b)$.

Mějme $a, b \in \mathbb{Z}$, $b \neq 0$. Nechť $b \nmid a$. Hledáme eukleidovský zbytek r při dělení b. Je prvkem třídy $[a]_{\equiv_b} = \{a + bk;\ k \in \mathbb{Z}\}$, přičemž $|r| < |b|$. Protože $\varnothing \subsetneq \nu_*[a]_{\equiv_b} \subset \mathbb{N}$ $(r \neq 0)$ je podmnožinou dobře uspořádané množiny, má minimum. To je menší než $|b|$. Prvek, v němž se toto minimum nabývá, označme $r = a + bk$. Je-li $r > 0$, pak $r' = r - |b| < 0$ a jeho norma splňuje $|r'| = |r - |b|| = |b| - r < |b|$, je proto rovněž eukleidovský zbytek. Analogicky, kdyby $r < 0$, pak $r' = |b| + r > 0$ je rovněž eukleidovský zbytek.

Víme, že existují aspoň dva. Kdyby existovaly tři, pak je můžeme seřadit, nejmenší označit r_0, největší r_1 a musí být $r_1 - r_0 \geq 2|b|$, tedy $|b| < 2|b| \leq |r_1 - r_0| \leq ||r_1| - |r_0|| < |r_1|$, což je spor.

Definice 1. $a, b \in \mathbb{Z}$, $b > 0$.
Dolní celou částí čísla $\frac{a}{b} \in \mathbb{Q}$ nazveme číslo q z rovnosti $a = bq + r$, kde $r \geq 0$ je eukleidovským zbytkem při dělení a číslem b. Značíme $\lfloor a/b \rfloor$.
Horní celou částí čísla $\frac{a}{b} \in \mathbb{Q}$ nazveme číslo q z rovnosti $a = bq + r$, kde $r \leq 0$ je eukleidovským zbytkem při dělení a číslem b. Značíme $\lceil a/b \rceil$.

Již víme, že pro danou dvojici celých čísel a, b, $b \neq 0$ existuje právě jeden nezáporný eukleidovský zbytek. Ukažme, že definice je korektní, tedy nezávisí na reprezentaci racionálního čísla.

Lemma 1. *Dolní, resp. horní celá část čísla $\frac{a}{b}$ je největší, resp. nejmenší celé číslo menší nebo rovno, resp. větší nebo rovno $\frac{a}{b}$. Neboli*

$$\lfloor a/b \rfloor = \max\{k \in \mathbb{Z};\ k \leq a/b\}\ , \tag{2}$$

analogicky pro horní celou část.

Důkaz. Díky archimedovskosti $\mathbb{Q}$ číslo vpravo existuje. Označme jej m. Je $mb \leq a$ a $r = a - mb$ je minimální z třídy $[a]_{\equiv_b}$, jež jsou nezáporné, neboť jinak by existovalo $m' > m$ takové, že $0 \leq r' = a - m'b$, tedy $m' \leq a/b$, což by byl spor. Analogicky pro horní celou část. □

Definice 2. $a, b \in \mathbb{Z}$, $b \neq 0$.
Označme $\left\{\frac{a}{b}\right\} \coloneqq \frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor \in \mathbb{Q}$ a nazvěme *zlomkovou částí* čísla $\frac{a}{b}$.

Díky předchozí definici je pro $a, b \in \mathbb{Z}$, $b > 0$

$$\begin{aligned} \frac{a}{b} &= \left\lfloor \frac{a}{b} \right\rfloor + \left\{\frac{a}{b}\right\} , \\ \left\lfloor \frac{a}{b} \right\rfloor &= q , \qquad \left\{\frac{a}{b}\right\} = \frac{r}{b} , \end{aligned} \tag{3}$$

kde q, r splňují (1) a $r \geq 0$ je eukleidovský zbytek (při dělení a číslem b).

Napišme nyní tvrzení s Eukleidovým algoritmem.

Věta 2 (Eukleidův algoritmus)**.**
Pokud $a, b \in \mathbb{Z}$, $b \neq 0$, *pak* $\exists n \in \mathbb{N}$, $\exists q_1, \ldots, q_n, r_1, \ldots, r_{n-1}$ *takové, že*

$$r_{i-1} = r_i q_{i+1} + r_{i+1} , \quad i = 0, \ldots, n-2 , \tag{4a}$$

$$r_{n-2} = r_{n-1} q_n , \tag{4b}$$

kde $|r_i| < |r_{i-1}|$ *pro* $i = 1, \ldots, n-1$ *a* $r_{n-1} = \mathrm{NSD}(a, b)$, *přičemž jsme položili* $r_{-1} \coloneqq a, r_0 \coloneqq b$.

Speciálně pro $b > 0$ lze vždy volit $r_i \geq 0$ pro $i = 0, \ldots, n-1$. To nám ovšem umožňuje algoritmus přepsat následujícím způsobem.

Algoritmus 1. Nechť $a, b \in \mathbb{Z}$, $b > 0$.

$$\begin{aligned} \frac{a}{b} &= \left\lfloor \frac{a}{b} \right\rfloor + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} , \\ \frac{b}{r_1} &= \left\lfloor \frac{b}{r_1} \right\rfloor + \frac{r_2}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}} , \\ &\vdots \\ \frac{r_{n-1}}{r_n} &= \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor = q_n . \end{aligned}$$

Zpětným dosazováním obdržíme

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\frac{r_1}{r_2}}} = \ldots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} ,$$

kde poslední způsob zápisu graficky zjednodušíme na $(q_1, \ldots, q_n)$.

Z algoritmu je patrné, že $q_i \in \mathbb{Z}$ pro $i \in \boldsymbol{n}$, $q_i > 0$ pro $i \in \{2, \ldots, n\}$. Pokud $n > 1$, pak $q_n > 1$.

Definice 3. Nechť $n \in \mathbb{N}$, $c_i \in \mathbb{Z}$ pro $i \in \boldsymbol{n}$, $c_i > 0$ pro $i \in \{2, \dots, n\}$.
Zápis

$$c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \ddots + \cfrac{1}{c_{n-1} + \cfrac{1}{c_n}}}} \tag{5}$$

nazýváme *konečným jednoduchým řetězovým zlomkem* (dále jen řetězovým zlomkem), zkráceně pišme $(c_1, \dots, c_n)$. Číslo c_i nazveme *i-tým členem* řetězového zlomku $(c_1, \dots, c_n)$, index n nazveme jeho *délkou*.

Volbu zkrácení značení z definice výše můžeme považovat za injekci množiny všech řetězových zlomků do množiny všech konečných celočíselných posloupností, čímž jsme v podstatě řekli, že dva řetězové zlomky považujeme za sobě rovné, právě když se rovnají příslušné posloupnosti jejich členů. Množinu všech řetězových zlomků budeme značit $\mathscr{F}$, její prvky budeme značit malými písmeny řecké abecedy.

Máme-li $\gamma \in \mathscr{F}$, můžeme provést tzv. vyčíslení, tedy přiřadit řetězovému zlomku číslo tak, že již nepovažujeme γ jen jako schéma, nýbrž jako složený zlomek. Po provedení všech racionálních úkonů zřejmě dostaneme (jednoznačně) racionální číslo.

Úmluva 1. Zobrazení $\mathscr{F} \to \mathbb{Q}$ popsané v odstavci výše označme '$\downarrow$'.

Definice 4. Zobrazení $\downarrow\colon \mathscr{F} \to \mathbb{Q}$ z úmluvy 1 nazveme *vyčíslením*.
Nechť $x \in \mathbb{Q}$, $\gamma \in \mathscr{F}$. Řekneme, že γ je *rozvojem* x, právě když $\downarrow\gamma = x$.

Víme, již díky algoritmu 1, že zobrazení $\downarrow$ je surjektivní. Je i injektivní?

Lemma 3. *Každé racionální číslo má právě dva rozvoje.*

Důkaz. Pro každý $(c_1, \dots, c_n) \in \mathscr{F}$ zřejmě platí

$$\downarrow(c_1, \dots, c_n) = c_1 + \frac{1}{\downarrow(c_2, \dots, c_n)}\,. \tag{6}$$

Volme $x = a/b \in \mathbb{Q}$, kde $a, b \in \mathbb{Z}$, $b > 0$. Nechť $(c_1, \dots, c_n) \in \mathscr{F} : \downarrow(c_1, \dots c_n) = x$.

1. Je-li $n = 1$, pak $\downarrow(c_1) = c_1 = x \in \mathbb{Z}$. Každý řetězový zlomek (c_1', c_2'), jenž je rozvojem x musí mít $c_2' = 1$, aby $\downarrow(c_1', c_2') \in \mathbb{Z}$. Pak je ale díky (6) $c_1' = c_1 - 1$. Nechť $(c_1'', \dots, c_m'') \in \mathscr{F}$, kde $m > 2$. Pak $\downarrow(c_1'', \dots, c_m'') = c_1'' + \frac{1}{\downarrow(c_2'', \dots, c_m'')}$, kde $\downarrow(c_2'', \dots, c_m'') > 1$, tedy $\downarrow(c_1'', \dots, c_m'') \notin \mathbb{Z}$ a nerovná se x.

2. Je-li naopak $n > 1$, rozlišme dvě možnosti:

   (a) $c_n > 1$. Pak $\frac{a}{b} = c_1 + \frac{1}{\downarrow(c_2, \dots, c_n)}$. Je $\downarrow(c_2, \dots, c_n) > 1$, neboť buďto $n = 2$ a $c_2 > 1$, nebo opět využijeme (6) a rozepíšeme

   $$\downarrow(c_2, \dots, c_n) = c_2 + \frac{1}{\underbrace{\downarrow(c_3, \dots, c_n)}_{>0}}\,,$$

odkud $c_1 = \lfloor a/b \rfloor$ a $\downarrow(c_2, \ldots, c_n) = \{\frac{a}{b}\}^{-1}$. Nyní je ale $(c_2, \ldots, c_n)$ délky $n-1$ s posledním členem větším než 1 a celou proceduru můžeme zopakovat, tedy dostaneme $c_2 = \left\lfloor \{\frac{a}{b}\}^{-1} \right\rfloor$. Odtud je zřejmé, že se postupuje přesně podle algoritmu 1 pro nalezení rozvoje čísla a/b. Všechny členy jsou dány jednoznačně. Takovýto zlomek tedy existuje právě jeden.

(b) $c_n = 1$. Pak

$$x = \downarrow(c_1, \ldots, c_n) = \downarrow(c_1, \ldots, c_{n-2}, c_{n-1} + c_n)\,,$$

odkud z předchozího víme, že členy $c_1, \ldots, c_{n-2}$ jsou určeny jednoznačně. □

Jako důsledek dostáváme z důkazu, že každé racionální číslo má právě jeden rozvoj liché, resp. sudé délky.

K hledání rozvoje daného čísla je výhodné sestavit si tabulku podle algoritmu 1, jak je demonstrováno v příkladu.

Příklad 1. Najdi všechny rozvoje $\frac{11}{30}$. Totéž pro číslo 1.
Řešení: Sestavme tabulku podle algoritmu 1, kde položíme $r_{-1} = a$, $r_0 = b$.
Odtud, $\frac{11}{30} = \downarrow(0, 2, 1, 2, 1, 2)$. Z důkazu lemmatu 3 plyne, že existuje už jen jeden další rozvoj

i	1	2	3	4	5	6
r_{i-2}	11	30	11	8	3	2
r_{i-1}	30	11	8	3	2	1
q_i	0	2	1	2	1	2

Tabulka 1: Rozvoj 11/30 do řetězového zlomku

11/30, totiž $(0, 2, 1, 2, 1, 1, 1)$.
Pro číslo 1 dostáváme rozvoje $(1), (0, 1)$.

Poznámka 1.

1. Je-li $x \in \mathbb{Q}$, $x > 1$ a $\gamma = (c_1, \ldots, c_n)$ rozvojem x, pak $c_1 \geq 1$.
2. Jsou-li x a $(c_1, \ldots, c_n)$ jako výše, pak $\downarrow(0, c_1, \ldots, c_n) = x^{-1}$.

Kdybychom v definici řetězového zlomku požadovali místo kladných členů od druhého počínaje záporné, dostali bychom takový jednoduchý vztah právě pro inverze záporných čísel.

Důkaz.

1. Z předpokladu dostaneme algoritmem 1 rozvoj $(d_1, \ldots, d_m)$, přičemž platí $d_1 \geq 2 \vee m \geq 2$, tedy též první člen druhého rozvoje x je kladný.
2. Plyne z předchozího a (6). □

K opačné proceduře – nalezení $\downarrow(c_1, \ldots, c_n)$ pro daný $(c_1, \ldots, c_n) \in \mathscr{F}$ – a ke zkoumání vlastností řetězových zlomků pomohou definice dalších pojmů.

Definice 5. Nechť $n \in \mathbb{N}$, $\gamma = (c_1, \ldots, c_n) \in \mathscr{F}$.
Pro $i \in \boldsymbol{n}$ definujme *i-tý parciální zlomek* (řetězového zlomku $(c_1, \ldots, c_n)$) jako

$$\gamma_i = (c_1, \ldots, c_{i-1}, c_i) \in \mathscr{F} \ . \tag{7}$$

Definujme *posloupnost čitatelů* $(P_i)_{i=1}^n$ a *posloupnost jmenovatelů* $(Q_i)_{i=1}^n$ zlomku $\gamma \in \mathscr{F}$

$$P_{-1} \coloneqq 0 \ , \qquad P_0 \coloneqq 1 \ , \tag{8a}$$
$$P_i \quad = a_i P_{i-1} + P_{i-2} \ ,$$
$$Q_{-1} \coloneqq 1 \ , \qquad Q_0 \coloneqq 0 \ , \tag{8b}$$
$$Q_i \quad = a_i Q_{i-1} + Q_{i-2} \ .$$

Číslo P_i, resp. Q_i nazveme *čitatel*, resp. *jmenovatel* i-tého parciálního zlomku řetězového zlomku γ. Zkracujme na i-tý čitatel/jmenovatel.

Protože $Q_0 = 0$ je zřejmé, že posloupnost jmenovatelů je kladná.

Věta 4. *Nechť $\gamma = (c_1, \ldots, c_n) \in \mathscr{F}$.*

$$\forall i \in \boldsymbol{n} : \ \lfloor\!\!\lfloor \gamma_i = \frac{P_i}{Q_i} \ , \tag{9}$$

kde P_i, resp. Q_i je i-tý čitatel, resp. jmenovatel γ.

Před důkazem této věty zobecníme některé pojmy, abychom se vyhnuli problémům se zápisem. Připustíme-li v řetězovém zlomku $(c_1, \ldots, c_n)$ členy $c_1 \in \mathbb{R}$, $c_i \in \mathbb{R}^+$ pro $i > 1$ (mluvme o *zobecněném řetězovém zlomku*), pak jej lze rovněž považovat za zápis nějakého reálného čísla x (analogie vyčíslení) – pišme $x = \lfloor\!\!\lfloor (c_1, \ldots, c_n)$, čímž jsme zavedli zobrazení množiny všech zobecněných řetězových zlomků $\mathscr{F}_z$ do $\mathbb{R}$. Pak $\lfloor\!\!\lfloor$ je restrikcí $\lfloor\!\!\lfloor$. Pro zobecněné řetězové zlomky lze přímočaře použít definici parciálních zlomků a jejich čitatelů/jmenovatelů. Výše uvedená věta platí i pro zobecněné řetězové zlomky, což dokážeme.

Důkaz věty 4. Dokažme indukcí. Nechť $\beta = (b_1, \ldots, b_n) \in \mathscr{F}_z$. Vychází $P_1 = b_1$, $Q_1 = 1$, odkud $\frac{P_1}{Q_1} = b_1 = \lfloor\!\!\lfloor \beta_1$, tedy tvrzení platí pro $i = 1$. Předpokládejme, že tvrzení platí pro všechny indexy do k-tého včetně, kde $k \in \mathbb{N}$ pevné. Mějme $\beta = (b_1, \ldots, b_n) \in \mathscr{F}_z$ z předpokladu věty takový, že $k + 1 \leq n$. Položme $\beta' = (b_1, \ldots, b_{k-1}, \lfloor\!\!\lfloor (b_k, b_{k+1})) = (b'_1, \ldots, b'_k)$, tedy $b'_j = b_j$ pro $j \in \boldsymbol{k-1}$ a $b'_k = b_k + \frac{1}{b_{k+1}}$. Pak

$$\lfloor\!\!\lfloor \beta_{k+1} = \lfloor\!\!\lfloor \beta'_k = \frac{P'_k}{Q'_k} = \frac{b'_k P'_{k-1} + P'_{k-2}}{b'_k Q'_{k-1} + Q'_{k-2}} = \frac{(b_k + \frac{1}{b_{k+1}})P_{k-1} + P_{k-2}}{(b_k + \frac{1}{b_{k+1}})Q_{k-1} + Q_{k-2}} = \frac{(b_k P_{k-1} + P_{k-2}) + P_{k-1}/b_{k+1}}{(b_k Q_{k-1} + Q_{k-2}) + Q_{k-1}/b_{k+1}}$$
$$= \frac{P_k + P_{k-1}/b_{k+1}}{Q_k + Q_{k-1}/b_{k+1}} \frac{b_{k+1}}{b_{k+1}} = \frac{b_{k+1}P_k + P_{k-1}}{b_{k+1}Q_k + Q_{k-1}} \ ,$$

tedy tvrzení platí pro $i = k + 1$. □

Věta 5. *Nechť $\gamma = (c_1, \ldots, c_n) \in \mathscr{F}$.*

$$\forall i \in \{2, \ldots, n\} : \ \lfloor\!\!\lfloor \gamma_i - \lfloor\!\!\lfloor \gamma_{i-1} = (-1)^i \frac{1}{Q_i Q_{i-1}} \ , \tag{10}$$

kde Q_j, $j \in \boldsymbol{n}$ jsou jmenovatelé γ.

Důkaz.

$$\lfloor\gamma_i - \lfloor\gamma_{i-1} = \frac{P_iQ_{i-1} - P_{i-1}Q_i}{Q_iQ_{i-1}} \,.$$

Upravujme čitatel:

$$\begin{aligned} P_iQ_{i-1} - P_{i-1}Q_i &= (c_iP_{i-1} + P_{i-2})Q_{i-1} - P_{i-1}(c_iQ_{i-1} + Q_{i-2}) = (-1)^1(P_{i-1}Q_{i-2} - P_{i-2}Q_{i-1}) \\ &= \ldots = (-1)^i(P_0Q_{-1} - P_{-1}Q_0) = (-1)^i \,, \end{aligned}$$

odkud plyne dokazované. □

Důsledek 6. *Nechť $\gamma = (c_1, \ldots, c_n) \in \mathscr{F}_z$, P_i, resp. Q_i je i-tý čitatel, resp. jmenovatel γ.*

$$\forall i \in \boldsymbol{n} : \ \mathrm{NSD}(P_i, Q_i) = 1 \,. \tag{11}$$

Důkaz. Pro $i = 1$ platí tvrzení triviálně, neboť $Q_1 = 1$. Je-li $i > 1$, vynásobíme rovnici (10) číslem Q_iQ_{i-1}. Dostaneme

$$P_iQ_{i-1} - P_{i-1}Q_i = (-1)^i \,. \tag{12}$$

Protože $Q_{i-1}, P_{i-1} \in \mathbb{Z}$, každý společný dělitel čísel P_i, Q_i dělí i $(-1)^i$, což je jednotka v oboru integrity $\mathbb{Z}$. □

Příklad 2. Spočti $\lfloor\gamma = \lfloor(0, 2, 1, 2, 1, 2)$.
Řešení: Sestrojme tabulku pomocí definice 5 a věty 4.

i	-1	0	1	2	3	4	5	6
c_i	-	-	0	2	1	2	1	2
P_i	0	1	0	1	1	3	4	11
Q_i	1	0	1	2	3	8	11	30
$\lfloor\gamma_i$	-	-	0	1/2	1/3	3/8	4/11	11/30

Tabulka 2: Výpočet $\lfloor(0, 2, 1, 2, 1, 2)$

2 Nekonečné řetězové zlomky

Rozšíříme-li přirozeně definici dolní celé části na obor reálných čísel, budeme moci napsat algoritmus podobný algoritmu 1 i pro iracionální čísla.

Definice 6. Nechť $x \in \mathbb{R}$.
Dolní celou částí čísla x rozumějme číslo

$$\lfloor x \rfloor := \max\{k \in \mathbb{Z};\ k \leq x\} \,. \tag{13}$$

Platí zřejmě $\lfloor x \rfloor \leq x$ pro každé $x \in \mathbb{R}$. Je-li navíc $x \in \mathbb{R} \setminus \mathbb{Q}$, pak $0 < x - \lfloor x \rfloor < 1$, je $x - \lfloor x \rfloor \in \mathbb{R} \setminus \mathbb{Q}$, a tedy jeho inverze ($\mathbb{Q}$ je těleso) je iracionální a větší než jedna.

Algoritmus 2. Nechť $x \in \mathbb{I}$.

$$x = \lfloor x \rfloor + \frac{1}{x_1}\,, \tag{14}$$

$$x_i = \lfloor x_i \rfloor + \frac{1}{x_{i+1}}\,, \quad i \in \mathbb{N}\,. \tag{15}$$

i-tý krok algoritmu definuje iracionální číslo x_i.

Všimněme si, že algoritmus 2 je formálně shodný s algoritmem 1. Pokud jej aplikujeme na racionální číslo, dostaneme po konečně mnoha krocích jeho řetězový rozvoj a další kroky nemají smysl. Aby byl korektní i v tomto případě, museli bychom přidat mezikrok s kontrolou nenulovosti zbytkového čísla a případného ukončení algoritmu. Z indukce je ale zřejmé, že pro $x \in \mathbb{I}$ jsou čísla x_i iracionální kladná čísla a algoritmus má smysl v každém kroku.

Položme nyní $x_0 := x$ a $q_i := \lfloor x_{i-1} \rfloor$. Formálně můžeme psát

$$x_0 = q_1 + \frac{1}{x_1} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{x_2}} \overset{*}{=} \ldots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n + \ddots}}}}\,, \tag{16}$$

výraz vpravo zapisujme jako $(q_1, q_2, \ldots)$. Poslední rovnost je symbolicky označena hvězdičkou, neboť představuje zatím jen to, že můžeme zápis rozšiřovat do nekonečna.

Definice 7. Nechť $c_i \in \mathbb{Z}$, pro $i \in \mathbb{N}$, $c_j > 0$ pro $j > 1$.
Výraz $(c_1, c_2, \ldots)$ (rozepsán v (16) – jen záměna 'q_i' za 'c_i') nazveme *nekonečným jednoduchým řetězovým zlomkem* (dále jen nekonečným řetězovým zlomkem či řetězovým zlomkem). Řekneme, že dva nekonečné řetězové zlomky $(d_1, d_2, \ldots)$, $(e_1, e_2, \ldots)$ jsou si rovny, právě když $\forall i \in \mathbb{N} : \; d_i = e_i$. Řetězový zlomek $(c_1, c_2, \ldots)$ nazveme *rozvojem čísla* $x \in \mathbb{R}$, právě když $\gamma = (c_1, c_2, \ldots) = (q_1, q_2, \ldots)$, kde zlomek vpravo byl získán pomocí algoritmu 2 aplikovaného na x. Též říkáme, že γ je řetězový zlomek příslušný číslu x. Čísla x_i z algoritmu 2 nazýváme *zbytkovými čísly i-tého řádu* čísla x.

Množinu všech nekonečných řetězových zlomků zapisujme jako $\mathscr{I}$. Protože platí[1]

$$\forall i \in \mathbb{N}_0 : \; x = \downarrow\!\!\circ(q_1, q_2, \ldots, q_i, x_i)\,, \tag{17}$$

kde $(q_1, q_2, \ldots, q_i, x_i) \in \mathscr{F}_z$, můžeme ke zkoumání vlastností nekonečných řetězových zlomků použít některé partie teorie konečných řetězových zlomků, konkrétně větu 4. Zobecnění pojmu 'i-tý parciální zlomek γ_i' zlomku $\gamma \in \mathscr{I}$ pro $i \in \mathbb{N}$ je přímočaré, stejně jako definice posloupnosti čitatelů, resp. jmenovatelů.

Věta 7. *Nechť $x \in \mathbb{I}$, $\gamma = (c_1, c_2, \ldots) \in \mathscr{I}$.*

1. *Podposloupnost $(\downarrow\!\!\circ \gamma_{2i-1})_{i=1}^{\infty}$ je rostoucí.*

[1] pro symbol '$\downarrow\!\!\circ$' viz text před důkazem věty 4

2. *Podposloupnost* $(\lfloor\gamma_{2i}\rfloor)_{i=1}^{\infty}$ *je klesající.*

3. $\forall i \in \mathbb{N}: \lfloor\gamma_{2i-1} < \lfloor\gamma_{2i}$.

4. *Je-li navíc* γ *rozvojem* x*, pak*

$$\forall i \in \mathbb{N}: \begin{cases} \lfloor\gamma_i < x & \text{, pokud je } i \text{ liché,} \\ x < \lfloor\gamma_i & \text{jinak.} \end{cases} \tag{18}$$

Důkaz. Pro $n \in \mathbb{N}$, $n > 2$ platí

$$\lfloor\gamma_n - \lfloor\gamma_{n-2} = (-1)^{n-1} \frac{c_n}{Q_n Q_{n-2}}\,, \tag{19}$$

neboť

$$\begin{aligned} \lfloor\gamma_n - \lfloor\gamma_{n-2}\,(\mp\lfloor\gamma_{n-1}) &\overset{V5}{=} \frac{(-1)^n}{Q_n Q_{n-1}} - \frac{(-1)^{n-1}}{Q_{n-1}Q_{n-2}} = (-1)^{n-1}\frac{Q_n - Q_{n-2}}{Q_{n-2}Q_{n-1}Q_n} \overset{D5}{=} \\ &= (-1)^{n-1}\frac{c_{n-1}Q_{n-1} + Q_{n-2} - Q_{n-2}}{Q_{n-2}Q_{n-1}Q_n} = (-1)^{n-1}\frac{c_n}{Q_n Q_{n-2}}\,. \end{aligned}$$

Volme $i \in \mathbb{N}$. Pak

1. podle (19) je $\lfloor\gamma_{2i+1} - \lfloor\gamma_{2i-1} = (-1)^{2i}\frac{c_{2i+1}}{Q_{2i+1}Q_{2i-1}} > 0$, neboť jmenovatelé jsou kladní a c_{2i+1} také, protože $2i+1 > 1$.

2. podle (19) je $\lfloor\gamma_{2i+2} - \lfloor\gamma_{2i} = (-1)^{2i+1}\frac{c_{2i+2}}{Q_{2i+2}Q_{2i}} > 0$, neboť $c_{2i+1} > 0$, protože $2i+2 > 1$.

3. díky větě 5, $\lfloor\gamma_{2i} - \lfloor\gamma_{2i-1} = (-1)^{2i}\frac{1}{Q_{2i}Q_{2i-1}} > 0$.

4. díky (17) je $x = \lfloor(c_1, c_2, \ldots, c_i, x_i)$. Označíme-li $\beta = (c_1, c_2, \ldots, c_i, x_i)$, a jeho čitatele a jmenovatele parciálních zlomků pro odlišnost očárkujeme, je na jednu stranu $\lfloor\beta_{i+1} - \lfloor\beta_i = \frac{(-1)^{i+1}}{Q'_{i+1}Q'_i}$, ale $\lfloor\beta_{i+1} = x$, $\beta_i = \gamma_i$. Odtud a díky kladnosti jmenovatelů dostaneme dokazované. □

Víme tedy, že platí nerovnosti

$$\lfloor\gamma_1 < \lfloor\gamma_3 < \cdots < (x) < \cdots < \lfloor\gamma_4 < \lfloor\gamma_2\,. \tag{20}$$

Obě posloupnosti jsou omezené a ryze monotónní, jsou tudíž konvergentní. Označme $L^o_\gamma = \lim_{i\to\infty}\lfloor\gamma_{2i-1}$, $L^e_\gamma = \lim_{i\to\infty}\lfloor\gamma_{2i}$. Je zřejmě $L^o_\gamma \le L^e_\gamma$. Ukažme, že jsou si rovny.

$$|L^e_\gamma - L^o_\gamma| \le |L^e_\gamma - \lfloor\gamma_{2i}| + |\lfloor\gamma_{2i} - \lfloor\gamma_{2i-1}| + |\lfloor\gamma_{2i-1} - L^o_\gamma|\,, \tag{21}$$

kde krajní dva členy konvergují k nule pro $i \to \infty$ a

$$|\lfloor\gamma_{2i} - \lfloor\gamma_{2i-1}| = \frac{1}{Q_{2i}Q_{2i-1}} \overset{*}{\le} \frac{1}{(2i-2)^2} \overset{i\to\infty}{\to} 0\,. \tag{22}$$

Odhad z hvězdičkou plyne z definice posloupnosti Q_i. Limita pravé strany (21) je nula, tudíž

$$L^o_\gamma = L^e_\gamma\,.$$

Důsledek 8. *Nechť $\gamma \in \mathscr{I}$, $x \in \mathbb{I}$.*
Posloupnost $(\downarrow_\circ \gamma_i)$ je konvergentní. Je-li γ rozvojem x, pak $\downarrow_\circ \gamma_i \to x$.

To nám dává možnost rozšířit obor zobrazení $\downarrow_\circ$ o množinu $\mathscr{I}$ přiřazením $\downarrow_\circ \gamma := \lim_{i\to\infty} \downarrow_\circ \gamma_i$ (značme rozšíření zobrazení stejně – v případě potřeby obor napíšeme explicitně).

Věta 9. *Restrikce $\downarrow_\circ$ na $\mathscr{I} \to \mathbb{I}$ je bijekce.*

Před důkazem věty formulujme lemma.

Lemma 10. *Nechť $\gamma = (c_1, \dots) \in \mathscr{I}$.*

$$\forall i \in \mathbb{N} : \downarrow_\circ \gamma = \downarrow_\circ (c_1, \dots, c_i, \downarrow_\circ (c_{i+1}, \dots)) .$$

Důkaz. Označíme-li $\beta = (c_{i+1}, c_{i+2}, \dots)$, pak $\forall j \in \mathbb{N} : \downarrow_\circ \gamma_{i+j} = \downarrow_\circ (c_1, \dots, c_i, c_{i+1}, \dots, c_{i+j}) = \downarrow_\circ (c_1, \dots, c_i, \downarrow_\circ \beta_j)$. Z věty o limitě složené funkce (nebo o aritmetice limit) už plyne tvrzení $(1 < \downarrow_\circ \beta)$. □

Důkaz věty 9. Nechť $\gamma \in \mathscr{I}$. Označme $\downarrow_\circ \gamma = x$. Ukažme, že $\forall i \in \mathbb{N} : c_i = q_i$, kde q_i je i-tý člen rozvoje x spočtený podle algoritmu 2.

Pro $i = 1$ je podle lemmatu 10 $\downarrow_\circ \gamma = \downarrow_\circ (c_1, \downarrow_\circ (c_2, \dots))$, kde díky (20) je $1 \le c_2 < \downarrow_\circ (c_2, \dots)$, tedy $c_1 = q_1$ a $x_1 = \downarrow_\circ (c_2, \dots)$. Můžeme tedy totéž použít pro x_1. Zbytek indukce je zřejmý.

Víme, že algoritmus 2 je jednoznačný a jeho aplikace na racionální číslo by vedla po konečně mnoha krocích k nedefinovaným operacím (dělení nulou). Restrikce $\downarrow_\circ : \mathscr{I} \to \mathbb{I}$ tedy existuje a je bijektivní. □

S ohledem na další aplikace uveďme lemma a poznámku.

Lemma 11. *Nechť $\gamma = (c_1, c_2, \dots) \in \mathscr{I}$, $x = \downarrow_\circ \gamma$.*

$$\forall (i \in \mathbb{N},\ i > 2) : |\downarrow_\circ \gamma_i - x| < |\downarrow_\circ \gamma_{i-1} - x| . \tag{23}$$

Důkaz. Volme $i \in \mathbb{N}$. Je (díky větě 9) $\downarrow_\circ (c_1, c_2, \dots) = \downarrow_\circ (c_1, \dots, c_i, x_i)$, kde x_i je i-té zbytkové číslo x. Označme $\beta = (c_1, \dots, c_i, x_i)$ a parciální čitatele a jmenovatele tohoto zlomku očárkujme.

$$x = \frac{P'_{i+1}}{Q'_{i+1}} = \frac{x_i P_i + P_{i-1}}{x_i Q_i + Q_{i-1}} .$$

Rovnost upravíme:

$$x_i (x Q_i - P_i) = -(x Q_{i-1} - P_{i-1}) = -Q_{i-1} \left(x - \frac{P_{i-1}}{Q_{i-1}} \right) ,$$

odkud

$$x - \frac{P_i}{Q_i} = \frac{-Q_{i-1}}{Q_i x_i} \left(x - \frac{P_{i-1}}{Q_{i-1}} \right) .$$

Posloupnost Q_i je neklesající, rostoucí (aspoň druhým indexem počínaje), tedy pro $i > 1$ je $|Q_{i-1}/Q_i| \le 1$ a $\frac{1}{x_i} \le 1$, tedy $|\downarrow_\circ \gamma_i - x| \le |\downarrow_\circ \gamma_{i-1} - x|$, přičemž ostrou nerovnost jsme dokázali pro $i > 2$. □

Poznámka 2. Větu 7 a lemma 11 lze upravit k aplikaci na konečné řetězové zlomky.

3 Řešení kongruenčních rovnic prvního stupně

Mějme kongruenční rovnici prvního stupně

$$ax \equiv_n b\,, \tag{24}$$

kde $a, b \in \mathbb{Z}$, $a \not\equiv_n 0$. Je-li $x' \in \mathbb{Z}$ řešením této rovnice, pak všechny prvky třídy $[x']_{\equiv_n}$ jsou také řešením. Existuje tedy vzájemně jednoznačná korespondence rovnice výše s rovnicí v $\mathbb{Z}_n$

$$\overline{a}\,\overline{x} = \overline{b}\,. \tag{25}$$

Řešení existuje, právě když $b \mid \mathrm{NSD}(a, n)$, neboť společný dělitel s modulem n je rovněž vlastností celé třídy (každého jejího reprezentanta).

Nechť jsou a, n nesoudělné. Pak je a invertibilní a lze jeho inverzí násobit celou rovnici a dostat tak řešení, jež je tedy jediné. Je-li $\mathrm{NSD}(a, n) = d > 1$ a $d \mid b$, pak bychom mohli celou rovnici tímto číslem dělit:

$$(a/d)x \equiv_{n/d} b/d \tag{26}$$

a převedli bychom ji na případ nesoudělného lineárního koeficientu a modulu. Jediné řešení v modulu n/d odpovídá právě d řešením v modulu n.

Popíšeme metodu hledání řešení kongruenční rovnice (24) pomocí řetězových zlomků. Nechť již jsou a, n nesoudělné. Existuje právě jedno $a' \in \overline{a} : \ 0 < a' < n$. Bez újmy na obecnosti ať právě a toto splňuje. Rozvineme n/a v řetězový zlomek $(c_1, \ldots, c_m)$. Podle (12) platí

$$(-1)^m = P_m Q_{m-1} - P_{m-1} Q_m\,, \tag{27a}$$

$$P_m = n\,, \qquad Q_m = a\,, \tag{27b}$$

přičemž druhý řádek plyne z nesoudělnosti a, n. Dosazením získáme

$$(-1)^m = nQ_{m-1} - aP_{m-1} \equiv_n -aP_{m-1}$$

a vynásobením $(-1)^m b$ dostaneme $a\,((-1)^{m-1} P_{m-1} b) \equiv_n b$, tedy řešením je $\overline{(-1)^{m-1} P_{m-1} b}$.

Zjevně lze dojít k cíli i tak, že vybereme jiného reprezentanta $a' \in \overline{a}$ nebo najdeme řetězový zlomek čísla a'/n místo n/a'. Porovnejme původně zvolený postup s některými ze zmiňovaných možností.

Je-li $a' = a + kn$ pro jisté $k \in \mathbb{Z}$, pak $\frac{a+kn}{n} = k + \frac{a}{n}$, první člen zlomku je k a pak pokračuje algoritmus dělením n/a, což byl výchozí bod původního postupu. Díky poznámce 1 lze případ a/n, resp. n/a' pro $a' > 0$ snadno převést na již probrané. Otázkou zůstává, zda lze porovnat optimálnost řešení s volbou n/a' pro $a' < 0$. V praxi chceme obvykle pracovat s co nejmenšími čísly (v absolutní hodnotě), čemuž volba $a - n$ může vyhovovat.

Poznámka 3. Pokud bychom volili $a' < 0$, je nutné přenásobit pravé strany v (27b) číslem $\operatorname{sign} a$.

Věta 12. *Nechť $a, b, n \in \mathbb{Z}$, $n > 1$.*
Jsou-li a, n nesoudělné, pak kongruenční rovnice (25) v $\mathbb{Z}_n$ má jediné řešení,

$$\overline{x} = \overline{(-1)^{m-1} (\operatorname{sign} a) P_{m-1} b}\,, \tag{28}$$

kde P_{m-1} je $(m-1)$-ní čitatel řetězového zlomku $(c_1, \ldots, c_m)$ – rozvoje n/a.

4 Lineární diofantické rovnice o dvou neznámých

4.1 Převedení na kongruenční rovnici 1. stupně

Rovnici pro neznámé $x, y \in \mathbb{Z}$

$$ax + by = c\,, \tag{29}$$

kde $a, b \in \mathbb{Z}$, $a, b \neq 0$ nazveme *lineární diofantickou rovnicí o dvou neznámých*. Bez újmy na obecnosti nechť je $b > 0$. Je-li (x', y') řešením (29), pak $c - ax' = by'$, tedy $b \mid c - ax'$, neboli $ax' \equiv_b c$, je tedy x' řešením kongruenční rovnice

$$ax \equiv_b c\,. \tag{30}$$

Pokud naopak $x' \in \mathbb{Z}$ řeší (30), platí $b \mid c - ax'$, tedy $\exists!\, y' \in \mathbb{Z} :\ c - ax' = y'b$, odkud

$$(x', y') = (x', (c - ax')/b) \tag{31}$$

řeší (29).

Korespondence řešení rovnic (29) a (30) je vzájemně jednoznačná. Řešení rovnice (30) existuje, právě když $d := \mathrm{NSD}(a, b) \mid c$. Pokud $1 < d$, pak můžeme rovnici (30) dělit d a dostaneme

$$(a/d)x \equiv_{b/d} c/d\,, \tag{32}$$

jež odpovídá rovnici (29) vydělené d. Proto předpokládejme rovnou, že $d = 1$. Pak řešení v $\mathbb{Z}_b$ existuje právě jedno – vyjádřeno nějakým reprezentantem jako $[x']_{\equiv_b}$. Odtud (a díky (31)) lze řešení (29) napsat jako $\{(x' + kb, \frac{c-a(x'+kb)}{b});\ k \in \mathbb{Z}\}$, kde $\frac{c-a(x'+kb)}{b} = \frac{c-ax'}{b} + ak = y' - ak$.

Poznámka 4. Protože $b \parallel -b$, stačí nahradit v (30) '$\equiv_b$' symbolem '$\equiv_{|b|}$' a (31) je řešením (29).

Formulujme předchozí poznatky do tvrzení:

Věta 13. *Mějme diofantickou rovnici* (29)*, kde a, b jsou nesoudělná.*

1. *Pokud x' řeší rovnici* (30)[2]*, pak (x', y') z* (31) *řeší rovnici* (29)*.*
2. *Pokud (x', y') řeší rovnici* (29)*, pak množina všech řešení* (29) *je $\{(x_k, y_k);\ k \in \mathbb{Z}\}$, kde*

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} + k \begin{pmatrix} b \\ -a \end{pmatrix} \tag{33}$$

4.2 Metoda výpočtu partikulárního řešení

Další přístup je časově náročnější, neboť je nutné spočítat čitatel i jmenovatel parciálního řetězového zlomku, ale nepředpokládá znalost kongruencí. Fundamentální je opět využití vlastnosti řetězových zlomků z důsledku 6. Některé poznatky zde zopakujeme.

Především lze snadno ukázat, že pokud $\mathrm{NSD}(a, b) \nmid c$, pak řešení (29) neexistuje. V opačném případě můžeme celou rovnici vydělit $\mathrm{NSD}(a, b)$. Dále bez újmy na obecnosti ať $\mathrm{NSD}(a, b) = 1$.

Lemma 14. *Množina všech řešení diofantické rovnice*

$$ax + by = 0 \tag{34}$$

je množina $\{t(-b, a);\ t \in \mathbb{Z}\}$.

[2] V případě $b < 0$ nahraďme '$\equiv_b$' symbolem '$\equiv_{|b|}$'.

Důkaz. Je $x = \frac{-b}{a}y$. Tedy $x \in \mathbb{Z} \iff \frac{-b}{a}y \in \mathbb{Z} \overset{y\in\mathbb{Z}}{\iff} a \mid y$. Odtud plyne dokazované. □

Definice 8. *Homogenní rovnicí* diofantické rovnice (29) nazveme rovnici (34).
Partikulárním řešením diofantické rovnice nazveme její libovolné řešení.

Pro $d, e \in \mathbb{Z}$ zaveďme označení $\left\langle \begin{matrix} d \\ e \end{matrix} \right\rangle := \{t(d,e);\ t \in \mathbb{Z}\}$.

Zápisem $\begin{pmatrix} f \\ g \end{pmatrix} + \left\langle \begin{matrix} d \\ e \end{matrix} \right\rangle$ rozumějme množinu $\{(f,g) + t(d,e);\ t \in \mathbb{Z}\}$

Věta 15. *Mějme diofantickou rovnici (29) a nechť existuje její řešení.*
Množina všech jejích řešení je

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \left\langle \begin{matrix} -b \\ a \end{matrix} \right\rangle , \tag{35}$$

kde (x_0, y_0) je jejím partikulárním řešením.

Důkaz. Je-li (x_1, y_1) řešením původní rovnice, pak $(x_1, y_1) - (x_0, y_0)$ řeší příslušnou homogenní rovnici – stačí odečíst následující rovnosti

$$ax_1 + by_1 = c\,,$$
$$ax_0 + by_0 = c\,.$$

Protože $(x_1, y_1) = (x_0, y_0) + ((x_1, y_1) - (x_0, y_0))$, je díky lemmatu 14 $(x_1, y_1) \in \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \left\langle \begin{matrix} -b \\ a \end{matrix} \right\rangle$.

Dokažme opačnou inkluzi. Volme $(x_0, y_0) + t(-b, a) \in \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \left\langle \begin{matrix} -b \\ a \end{matrix} \right\rangle$. Pak

$$a(x_0 - tb) + b(y_0 + ta) = ax_0 + by_0 + (-tab + tab) = c\,,$$

tedy $(x_0, y_0) + t(-b, a)$ řeší původní rovnici. □

Zbývá zjistit, ve kterých případech řešení existuje, a nalézt způsob, jak najít partikulární řešení.

Pozorování 5. Nechť $k \in \mathbb{Z}$.
(x_0, y_0) řeší diofantickou rovnici (29), pak $k(x_0, y_0)$ řeší diofantickou rovnici

$$ax + by = kc\,. \tag{36}$$

Důkaz. $a(kx_0) + b(ky_0) = k(ax_0 + by_0) = kc$. □

Ať $\frac{a}{b} = \lfloor (z_1, \ldots, z_n)$. Pak $\frac{P_n}{Q_n} = \frac{a \operatorname{sign}(ab)}{b}$ a čitatelé, resp. jmenovatelé se navzájem rovnají. Dosazením do (12) dostaneme

$$a\,(\operatorname{sign} ab) Q_{n-1} - bP_{n-1} = (-1)^n\,, \tag{37}$$

tedy $((\operatorname{sign} ab)Q_{n-1}, -P_{n-1})$ řeší rovnici

$$ax + by = (-1)^n\,. \tag{38}$$

Díky pozorování 5 je $(-1)^n\, c \cdot ((\operatorname{sign} ab)Q_{n-1}, -P_{n-1})$ řešením rovnice (29).

Věta 16. *Nechť jsou a, b nesoudělná.*
Je-li $a/b = \lfloor\!\lfloor(z_1, \ldots, z_n)$ a P_{n-1}, resp. Q_{n-1} je příslušný čitatel, resp. jmenovatel, pak partikulární řešení diofantické rovnice (29) je

$$(-1)^n\, c \begin{pmatrix} \operatorname{sign}(ab)\, Q_{n-1} \\ -P_{n-1} \end{pmatrix} . \tag{39}$$

4.3 Příklady

Příklad 3. Vyřeš diofantickou rovnici

$$1721x - 5279y = 2000 . \tag{40}$$

Řešení: V souladu se značením v tvrzeních, položme $a = 1721$, $b = -5279$, $c = 2000$. Zjistíme, že a, b jsou prvočísla, tedy jsou nesoudělná. Rovnice má řešení.

1. Rovnici převedeme na kongruenční:

$$1721x \equiv_{5279} 2000 . \tag{41}$$

Najdeme její řešení pomocí věty 12. Spočtěme rozvoj čísla 5279/1721 do řetězového zlomku:

i	1	2	3	4	5	6
r_{i-2}	5279	1721	116	97	19	2
r_{i-1}	1721	116	97	19	2	1
z_i	3	14	1	5	9	2

Hledaný rozvoj je $(3, 14, 1, 5, 9, 2)$. Potřebujeme spočítat P_5.

i	-1	0	1	2	3	4	5
z_i	-	-	3	14	1	5	9
P_i	0	1	3	43	46	273	2503
Q_i	1	0	1	14	15	89	816

Je $P_5 = 2503$. Třída příslušná $(-1)^5\, 2503 \cdot 2000$ řeší (41). Volme menšího reprezentanta, $(-1)^5\, 2503 \cdot 2000 \equiv_{5279} -5006 \cdot 10^3 + 5276 \cdot 10^3 \equiv_{5279} 273 \cdot 10^3 - 40 \cdot 5279 \equiv_{5279} 61840 - 11 \cdot 5279 \equiv_{5279} 3771$. Položme $x' = 3771$. Podle věty 13 je $y' = \frac{1721 \cdot 3771 - 2000}{5279} = 1229$. Množina všech řešení je $\{(x_k, y_k);\ k \in \mathbb{Z}\}$, kde

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} 3771 \\ 1229 \end{pmatrix} + k \begin{pmatrix} 5279 \\ 1721 \end{pmatrix} . \tag{42}$$

2. Najdeme partikulární řešení pomocí věty 16. V předchozím jsme spočítali, že $(-b)/a = \lfloor\!\lfloor(3, 14, 1, 5, 9, 2)$. Je $P_5 = 2503$, $Q_5 = 816$. Odtud, $(-1)^6 2000(816, -2503)$ je partikulárním řešením rovnice

$$(-b)x + ay = 2000 ,$$

tedy $2000\,(-2503, -816)$ je partikulárním řešením původní rovnice.
Porovnejme, zda je to v souladu s předchozím výsledkem. Je $2000\,(-2503, -816) - (3771, 1229) = -949(5279, 1721)$, takže oba výsledky jsou v souladu.

5 Aproximace

5.1 Teorie

V poznámce 2 jsme předeslali, že lze přeformulovat větu 7 a lemma 11 i pro racionální čísla. Protože chceme tvrzení formulovat jak pro racionální, tak pro iracionální čísla, avšak v prvním případě je rozvoj do řetězového zlomku konečný, platí pochopitelně příslušná tvrzení pro ty indexy, jež jsou menší nebo rovny délce rozvoje. V platnosti zůstávají body 1,2,3 věty 7, jak je zřejmé z důkazů. Ve čtvrtém tvrzení stačí místo ostré nerovnosti pro poslední parciální zlomek psát rovnost. Důkaz lemmatu 11 je nepoužitelný pro porovnání posledních dvou parciálních zlomků. Poslední parciální zlomek přísluší rozkládanému racionálnímu číslu a předposlední jinému racionálnímu číslu, takže tvrzení pro tuto dvojici platí také.

Úkolem je nyní aproximovat co nejlépe zvolené číslo zlomkem v základním tvaru tak, aby zároveň jeho jmenovatel byl co nejmenší.

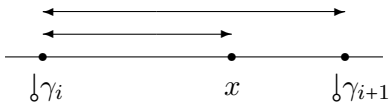
Představu o aproximaci čísla pomocí jeho rozvoje dává následující lemma:

Lemma 17. *Nechť $x \in \mathbb{R}$.*
Pokud $x = \lfloor\!\lfloor \gamma$, pak

$$\left| x - \frac{P_i}{Q_i} \right| \leq \frac{1}{Q_{i+1} Q_i} \,, \tag{43}$$

přičemž rovnost nastane, právě když $i+1$ je délka rozvoje γ.

Důkaz. Nerovnost $\left| x - \frac{P_i}{Q_i} \right| \leq |\lfloor\!\lfloor \gamma_{i+1} - \lfloor\!\lfloor \gamma_i|$ plyne z řetězce nerovností (20). Rovnost může nastat jen tehdy, pokud je již $\lfloor\!\lfloor \gamma_{i+1} = x$.



Pravou stranu upravíme pomocí věty 5. □

Věnujme se ještě další úpravě nerovnosti (43). V případě, kdy je nerovnost ostrá, lze díky monotonii posloupnosti jmenovatelů psát: $\left| x - \frac{P_i}{Q_i} \right| < \frac{1}{Q_i^2}$. Zbývá vyšetřit případ, kdy

1. $i+1$ je délka rozvoje x. Tehdy je $Q_i \leq Q_{i+1}$, kde rovnost může nastat jen pro $i = 1$, je-li navíc $c_2 = 1$ (druhý člen γ). Pak $x \in \mathbb{Z}$ a navíc při rozkladu nepostupujeme podle algoritmu 1. *V této sekci vyloučíme tento případ.*

2. i je délka rozvoje – triviálně je $\left| x - \frac{P_i}{Q_i} \right| = 0 < \frac{1}{Q_i^2}$.

Lemma 18. *Nechť $x \in \mathbb{R}$.*
Je-li $x = \lfloor\!\lfloor \gamma$, pak

$$\left| x - \frac{P_i}{Q_i} \right| < \frac{1}{Q_i^2} \,. \tag{44}$$

Máme možnost zvolené číslo aproximovat zlomkem v základním tvaru, s chybou menší než je převrácený kvadrát jmenovatele. Chceme nyní vědět, jak dobře lze zlomkem aproximovat dané číslo, pokud shora omezíme jeho jmenovatele daným číslem.

Věta 19 (Dirichlet)**.** *Nechť $x, \tau \in \mathbb{R}$, $\tau \geq 1$.*

$$\exists a, b \in \mathbb{Z},\ 0 < b \leq \tau,\ \mathrm{NSD}(a,b) = 1 \ :\ \left| x - \frac{a}{b} \right| < \frac{1}{b\tau}\ .$$

Důkaz. Chceme využít postupu z předchozího důkazu. Vidíme z (43), že pokud bychom položili zrovna $a/b = P_i/Q_i$ tak, že

$$Q_i \leq \tau < Q_{i+1}\ , \tag{45}$$

dostaneme požadované. Pro iracionální x je to možné vždy, neboť posloupnost jmenovatelů je (aspoň od druhého členu) rostoucí a není shora omezená (můžeme připustit i $\tau \leq Q_{i+1}$). Buď pro $x \in \mathbb{Q}$ existuje i vyhovující (45), nebo ne – pak samotné x má v základním tvaru jmenovatele, jenž je menší nebo roven τ. □

Všimněme si blíže rychlosti divergence posloupnosti jmenovatelů.

Lemma 20. *Nechť $\alpha \in \mathscr{F} \cup \mathscr{I}$, $i \in \mathbb{N}$.*

$$Q_i \geq 2^{\frac{i-2}{2}}\ .$$

Důkaz. Je $Q_2 \geq 1$. Dále, pro $n \in \mathbb{N}$ je $Q_{2+n} \geq Q_{2+n-1} + Q_{2+n-2} \geq 2Q_{2+n-2}$. Odtud $Q_{2+2n} \geq 2^n Q_2 \geq 2^n = 2^{\frac{(2+2n)-2}{2}}$ a $Q_{2+2n+1} \geq 2^n Q_3 \geq 2^{n+1} \geq 2^{\frac{(2+2n+1)-2}{2}}$. □

Jmenovatelé tedy rostou geometricky.

Definice 9. Nechť $\alpha \in \mathscr{F} \cup \mathscr{I}$, $i \in \mathbb{N}$, $i \geq 3$.
Je-li a_i i-tý člen řetězového zlomku α, definujeme pro $k \in \{0, 1, \ldots, a_i\}$ *i-tý vsunutý parciální zlomek* (řetězového zlomku α) jako $P_{i,k}/Q_{i,k}$, kde

$$P_{i,k} = kP_{i-1} + P_{i-2}\ , \tag{46a}$$
$$Q_{i,k} = kQ_{i-1} + Q_{i-2}\ . \tag{46b}$$

Dle definice je tedy $P_{i,0}/Q_{i,0} = P_{i-2}/Q_{i-2}$ a $P_{i,a_i}/Q_{i,a_i} = P_i/Q_i$. Spočtěme, jaká je vzájemná poloha vsunutých zlomků. Pro $k \geq 0$ je

$$\begin{aligned} \frac{(k+1)P_{i-1} + P_{i-2}}{(k+1)Q_{i-1} + Q_{i-2}} - \frac{kP_{i-1} + P_{i-2}}{kQ_{i-1} + Q_{i-2}} &= \frac{P_{i-1}Q_{i-2} - P_{i-2}Q_{i-1}}{[(k+1)Q_{i-1} + Q_{i-2}][kQ_{i-1} + Q_{i-2}]} = \\ &\overset{V5}{=} \frac{(-1)^{i-1}}{[(k+1)Q_{i-1} + Q_{i-2}][kQ_{i-1} + Q_{i-2}]}\ . \end{aligned} \tag{47}$$

Je-li i liché, resp. sudé, je tento rozdíl kladný, resp. záporný. Pro názornost pišme

$$\lfloor \alpha_{2i-1} = \frac{P_{2i-1}}{Q_{2i-1}} = \frac{P_{2i+1,0}}{Q_{2i+1,0}} < \frac{P_{2i+1,1}}{Q_{2i+1,1}} < \ldots < \frac{P_{2i+1,a_{2i+1}}}{Q_{2i+1,a_{2i+1}}} = \frac{P_{2i+1}}{Q_{2i+1}} = \lfloor \alpha_{2i+1}\ , \tag{48a}$$
$$\lfloor \alpha_{2i} = \frac{P_{2i}}{Q_{2i}} = \frac{P_{2i,a_{2i}}}{Q_{2i,a_{2i}}} < \frac{P_{2i,a_{2i-1}}}{Q_{2i,a_{2i-1}}} < \ldots < \frac{P_{2i,0}}{Q_{2i,0}} = \frac{P_{2i-2}}{Q_{2i-2}} = \lfloor \alpha_{2i-2}\ , \tag{48b}$$

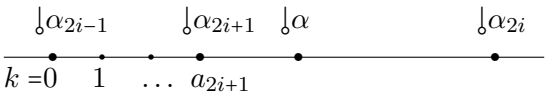
což je v souladu s větou 13. Takže i-tý vsunutý parciální zlomek leží (je vsunutý) mezi i-tým a $(i-2)$-hým parciálním zlomkem.

Definice 10. Nechť $a, b, c, d \in \mathbb{Z}$, $b, d > 0$.
Zlomek $\frac{a+c}{b+d}$ nazveme *mediantou* zlomků $\frac{a}{b}$, $\frac{c}{d}$.

Lemma 21. *Medianta dvou (rozdílných) zlomků leží striktně mezi nimi.*

Důkaz. Mějme a, b, c, d jako v definici 10. Nechť $\frac{a}{b} < \frac{c}{d}$. Kdyby $\frac{c}{d} \le \frac{a+c}{b+d}$, pak $c(b+d) \le (a+c)d$, tedy $bc \le ad$, tedy $\frac{c}{d} \le \frac{a}{b}$, což je spor. Analogicky pro druhou nerovnost. □

Je tedy $\frac{P_{i,k+1}}{Q_{i,k+1}}$ mediantou $\frac{P_{i,k}}{Q_{i,k}}$ a $\frac{P_{i-1}}{Q_{i-1}}$. Začneme-li od P_{i-2}/Q_{i-2} tímto způsobem tvořit medianty, postupně se dostaneme až k P_i/Q_i. S využitím věty 13 načrtněme schéma pro vzájemné polohy jistých zvolených zlomků: ve schématu níže jsou načrtnuty $(2i+1)$-ní vsunuté zlomky, tj. postupně zleva tvoříme $\frac{P_{2i+1,k}}{Q_{2i+1,k}}$ – medianty z $\lfloor\alpha_{2i-1}$ s opakovaně použitým $\lfloor\alpha_{2i}$.



Lemma 22. *Nechť $\alpha \in \mathscr{F} \cup \mathscr{I}$, $i \in \mathbb{N}$.*
Pokud $\alpha \in \mathscr{I}$ nebo délka α je aspoň $i+2$, pak medianta $\lfloor\alpha_i$ a $\lfloor\alpha_{i+1}$ leží od $\lfloor\alpha$ na stejné straně jako $\lfloor\alpha_i$.

Důkaz. Medianta $\lfloor\alpha_i$ a $\lfloor\alpha_{i+1}$ je $\frac{P_{i+1}+P_i}{Q_{i+1}+Q_i}$ a je tedy již $(i+2)$-hým vsunutým zlomkem. Speciálně, jedná-li se o rozvoj délky $i+2$ a $a_{i+2} = 1$, je tato medianta rovna $\lfloor\alpha$. □

Úmluva 2. Uvažujme nyní pod symbolem $\mathscr{F}$ jen konečné řetězové zlomky končící členem větším než 1. Ostatní z úvah vylučujeme.

Tedy rozvoje $\mathbb{R}\setminus\{1\}$ do řetězových zlomků jsou v tomto smyslu jendoznačné. Konečné řetězové zlomky a jejich parciální zlomky můžeme v tomto smyslu ztotožnit s číslem, jež reprezentují. Díky definici vsunutých zlomků nepřijdeme o předposlední parciální zlomky řetězových zlomků (délky aspoň 4), jež jsme právě vyloučili.

Jako důsledek předchozích úvah dosáváme následující větu.

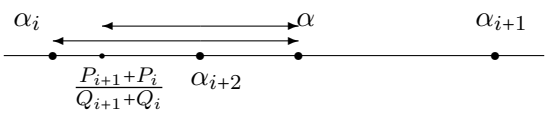
Věta 23. *Pokud $\alpha \in \mathbb{R}$, $i \in \mathbb{N}$, pak*

$$|\alpha - \alpha_i| > \frac{1}{Q_i(Q_{i+1} + Q_i)} \,. \tag{49}$$

Důkaz. Je-li délka rozvoje α právě $i+1$, pak $\frac{P_{i+1}+P_i}{Q_{i+1}+Q_i}$ je mediantou α_i a α, tedy její vzdálenost od α je menší než vzdálenost α_i od α. Díky (47) máme (za 'i' dosaďme '$i+2$', za 'k' dosaďme '0') dokazované.

Je-li délka rozvoje větší než $i+1$, víme, že $\frac{P_{i+1}+P_i}{Q_{i+1}+Q_i}$ je $(i+2)$-hým vsunutým zlomkem a že od α leží na stejné straně jako α_{i+2}, tedy i α_i a zároveň je mezi nimi (schéma níže). Odtud

$$|\alpha - \alpha_i| > \left|\frac{P_{i+1} + P_i}{Q_{i+1} + Q_i} - \frac{P_i}{Q_i}\right| \overset{(47)}{=} \frac{1}{Q_i(Q_{i+1} + Q_i)} \,.$$



□

Definice 11. Nechť $\alpha \in \mathbb{R}$, $a, b \in \mathbb{Z}$, $b > 0$.
Řekneme, že a/b je *nejlepším racionálním přiblížením* α, právě když obecně platí implikace

$$\left(a', b' \in \mathbb{Z}, 0 < b' \leq b, \frac{a'}{b'} \neq \frac{a}{b}\right) \Rightarrow \left|\alpha - \frac{a'}{b'}\right| > \left|\alpha - \frac{a}{b}\right| . \tag{50}$$

Příklad 4. Například $0/1$, $1/3$, $1/4$ jsou všechna nejlepší přiblížení $1/4$. Je $1/4 = (0, 4)$ a $0/1$, $1/4$ jsou parciální zlomky. Podle definice 9 neexistují vsunuté zlomky. Kdybychom však formálně přidali $P_0/Q_0 = 1/0$ a považovali $\frac{kP_1+P_0}{kQ_1+Q_0}$ za vsunuté zlomky (příslušné indexu 2), dostaneme vsunuté zlomky $1/0$, $(1+0)/(0+1)$, $(1+0)/(0+2)$, $(1+0)/(0+3)$, $(1+0)/(0+4)$, mezi nimiž je i $1/3$.

Věta 24. *Nechť $\gamma \in \mathbb{R}$, ($a, b \in \mathbb{Z}$, $b > 0$, $\mathrm{NSD}(a, b) = 1$)*[3].
Je-li $\frac{a}{b}$ nejlepším přiblížením γ, pak $\frac{a}{b}$ je parciálním nebo vsunutým zlomkem γ (včetně druhých vsunutých zlomků).

Důkaz. Nechť je a/b nejlepším přiblížením γ. Značme členy rozkladu γ písmenem c. Pak

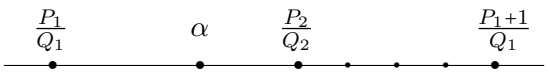
$$c_1 = \frac{P_1}{Q_1} \leq \frac{a}{b} \leq \frac{P_1 + 1}{Q_1} = c_1 + 1 .$$

Kdyby totiž $\frac{a}{b} < \frac{P_1}{Q_1}$, pak je $\frac{a}{b}$ dále od x než $\frac{P_1}{Q_1}$ (neboť $\gamma_1 \leq \gamma$), přitom $b \geq 1 = Q_1$. Podobně, kdyby $c_1 + 1 = \frac{P_1+1}{Q_1} < \frac{a}{b}$, pak z definice c_1 jakožto dolního celého čísla x, leží a/b od x dále než $\frac{P_1+1}{Q_1}$.

Nastane-li někde rovnost, jsme hotovi, neboť $\frac{P_1}{Q_1}$ je parciálním zlomkem a $\frac{P_1+1}{Q_1} = \frac{P_1+P_0}{Q_1+Q_0}$ je vsunutým zlomkem (díky dohodě ve větě). Jsou-li obě nerovnosti ostré a sporem předpokládáme, že a/b není parciálním, ani vsunutým zlomkem, pak leží a/b mezi jistými dvěma po sobě jdoucími vsunutými zlomky

$$\frac{kP_i + P_{i-1}}{kQ_i + Q_{i-1}} , \qquad \frac{(k+1)P_i + P_{i-1}}{(k+1)Q_i + Q_{i-1}} ,$$

kde $(i = 1 \wedge 1 \leq k < c_1) \vee (i > 1 \wedge 0 \leq k < c_i)$ (viz schéma níže).



Pak je

$$\left|\frac{a}{b} - \frac{kP_i + P_{i-1}}{kQ_i + Q_{i-1}}\right| < \left|\frac{kP_i + P_{i-1}}{kQ_i + Q_{i-1}} - \frac{(k+1)P_i + P_{i-1}}{(k+1)Q_i + Q_{i-1}}\right| \overset{(47)}{=} \frac{1}{[(k+1)Q_i + Q_{i-1}][kQ_i + Q_{i-1}]} .$$

Ale existuje $n \in \mathbb{N}$ takové, že

$$\left|\frac{a}{b} - \frac{kP_i + P_{i-1}}{kQ_i + Q_{i-1}}\right| = \frac{n}{b(kQ_i + Q_{i-1})} .$$

Dosazením do předchozí nerovnosti dostaneme

$$\frac{n}{b(kQ_i + Q_{i-1})} < \frac{1}{[(k+1)Q_i + Q_{i-1}][kQ_i + Q_{i-1}]} ,$$

odkud $b > n[(k+1)Q_i + Q_{i-1}] \geq (k+1)Q_i + Q_{i-1}$, přitom ale víme, že $\frac{kP_i+P_{i-1}}{kQ_i+Q_{i-1}}$ aproximuje α lépe než $\frac{a}{b}$ (viz (48a),(48b)). To je spor s tím, že je $\frac{a}{b}$ nejlepším přiblížením α. □

[3] Přidáno, aby nemohlo dojít k nedorozumění.

5.2 Nejlepší přiblížení druhého druhu

Cílem této části je zejména věta 26. Použijeme ji k důkazu věty, kterou potřebujeme k aplikaci teorie řetězových zlomků na řešení Pellových rovnic.

Definice 12. Nechť $\alpha \in \mathbb{R}$, $a, b \in \mathbb{Z}$, $b > 0$.
Řekneme, že $\frac{a}{b}$ je *nejlepším* (racionálním) *přiblížením α druhého druhu*, právě když obecně platí implikace

$$\left(a', b' \in \mathbb{Z}, 0 < b' \leq b, \frac{a'}{b'} \neq \frac{a}{b}\right) \Rightarrow \left|\alpha b' - a'\right| > |\alpha b - a| \ . \tag{51}$$

Nejlepší racionální přiblížení z definice 11 budeme též označovat jako nejlepší přiblížení *prvního druhu*.

Poznámka 6. Nechť $\gamma \in \mathbb{R}$.
Je-li $\frac{a}{b}$ nejlepším přiblížením γ druhého druhu, pak $\frac{a}{b}$ je nejlepším přiblížením γ prvního druhu. Obrácená implikace obecně neplatí.

Důkaz. Mějme $\gamma \in \mathbb{R}$, $a, b \in \mathbb{Z}$, $b > 0$.

Není-li $\frac{a}{b}$ nejlepším přiblížením γ prvního druhu, pak existuje $a', b' \in \mathbb{Z}$, $0 < b' \leq b$ takové, že $|\gamma - a'/b'| \leq |\gamma - a/b|$. Protože také $0 < b \leq b'$, vynásobením obou nerovností dostaneme $|\gamma b' - a'| \leq |\gamma b - a|$, tedy $\frac{a}{b}$ není nejlepším přiblížením druhého druhu. Dokázali jsme obměnu implikace.

Hledejme nyní protipříklad. Nejlepší přiblížení 1/3 jsou 0/1, 1/2, 1/3. Ukažme, že 1/2 není nejlepším přiblížením druhého druhu: $|(1/3) \cdot 2 - 1| = 1/3 \not< |(1/3) \cdot 1 - 0| = 1/3$. Vezmeme-li si jako protipříklad 1/5, pak 0/1 a 1/3 jsou nejlepší přiblížení 1/5, ale dokonce $|(1/5) \cdot 3 - 1| = \frac{2}{5} > |(1/5) \cdot 1 - 0| = 1/5$. □

Věta 25. *Nechť $\gamma \in \mathbb{R}$, $a, b \in \mathbb{Z}$, ($b > 0$, $\mathrm{NSD}(a, b) = 1$).*
Je-li $\frac{a}{b}$ nejlepším přiblížením γ druhého druhu, pak je parciálním zlomkem rozvoje γ.

Důkaz. Mějme $\gamma \in \mathbb{R}$. Ať $\frac{a}{b}$ je nejlepším přiblížením γ druhého druhu. Pak je[4]

$$c_1 = \frac{P_1}{Q_1} \leq \frac{a}{b} \leq \frac{P_2}{Q_2} \ . \tag{52}$$

Kdyby neplatila nerovnost vlevo, nebyl by $\frac{a}{b}$ nejlepším přiblížením prvního druhu (viz důkaz věty 23). Kdyby neplatila druhá nerovnost, je

$$\left|\gamma - \frac{a}{b}\right| > \left|\frac{a}{b} - \frac{P_2}{Q_2}\right| \geq \frac{1}{bQ_2} \ ,$$

odkud vynásobením b dostaneme

$$|\gamma b - a| > \frac{1}{Q_2} = \frac{1}{c_2} \ .$$

Srovnejme toto s racionálním přiblížením daným $\frac{P_1}{Q_1} = \frac{c_1}{1}$. Podle algoritmu rozvoje $x := \gamma$ do řetězového zlomku je $\gamma \cdot 1 - c_1 = \frac{1}{x_1}$, kde $x_1 \geq c_2 = Q_2$ (značení jako v algortimu 2). Odtud

$$|\gamma \cdot 1 - c_1| \leq \frac{1}{c_2} \ .$$

[4] Je-li délka rozvoje jedna, nutně je $a = \gamma$, $b = 1$.

To je spor s tím, že $\frac{a}{b}$ je nejlepším přiblížením druhého druhu.

Víme nyní, že je splněno (52). Kdyby $\frac{a}{b}$ nebyl parciálním zlomkem, pak musí ležet mezi dvěma parciálními zlomky stejné parity, nebo v případě konečného rozvoje – délky n – mezi n-tým a $(n-1)$-ním.

V prvním případě si označme $\frac{P_{i-1}}{Q_{i-1}}$, $\frac{P_{i+1}}{Q_{i+1}}$ zmíněné parciální zlomky. Platí

$$\left|\frac{a}{b}-\frac{P_{i-1}}{Q_{i-1}}\right| \geq \frac{1}{bQ_{i-1}}\,,$$
$$\left|\frac{a}{b}-\frac{P_{i-1}}{Q_{i-1}}\right| < \left|\frac{P_i}{Q_i}-\frac{P_{i-1}}{Q_{i-1}}\right| = \frac{1}{Q_iQ_{i-1}}\,.$$

Odtud je

$$\frac{1}{bQ_{i-1}} < \frac{1}{Q_iQ_{i-1}}\,,$$

tedy $b > Q_i$. Srovnejme nyní přiblížení dané $\frac{a}{b}$ s přiblížením daným $\frac{P_i}{Q_i}$.

$$\left|\gamma-\frac{a}{b}\right| > \left|\frac{P_{i+1}}{Q_{i+1}}-\frac{a}{b}\right| \geq \frac{1}{bQ_{i+1}}\,,$$

tedy $|\gamma b - a| \geq \frac{1}{Q_{i+1}}$. Porovnáním s

$$\left|\gamma-\frac{P_i}{Q_i}\right| \leq \frac{1}{Q_iQ_{i+1}}\,,$$

takže $|\gamma Q_i - P_i| \leq \frac{1}{Q_{i+1}}$. Dostali jsme spor s tím, že $\frac{a}{b}$ je nejlepším přiblížením druhého druhu.

V druhém případě $\frac{a}{b}$ leží mezi $\frac{P_{n-1}}{Q_{n-1}}$ a $\frac{P_n}{Q_n} = \gamma$. Pak

$$\left|\gamma-\frac{a}{b}\right| = \left|\frac{P_n}{Q_n}-\frac{a}{b}\right| \geq \frac{1}{bQ_n}\,,$$
$$\left|\gamma-\frac{a}{b}\right| < \left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right| = \frac{1}{Q_nQ_{n-1}}\,,$$

odkud $b > Q_{n-1}$. Protože je nejlepším přiblížením druhého druhu, je

$$\left|\frac{P_n}{Q_n}b-a\right| < \left|\frac{P_n}{Q_nQ_{n-1}-P_{n-1}}\right|\,.$$

Vynásobením Q_n dostaneme

$$|P_nb-aQ_n| < |P_nQ_{n-1}-P_{n-1}Q_n| = 1\,,$$

tedy $\gamma = \frac{a}{b}$, což je spor. □

Poznámka 7. Je-li $2\gamma \in [1]_{\equiv_2}$, pak γ_1 není nejlepším přiblížením γ druhého druhu.

Důkaz. $\gamma = k+1/2$, kde $k \in \mathbb{Z}$, tedy $\gamma_1 = k/1$. Pak ale též $(k+1)/1$ dává 'stejně dobré' přiblížení:

$$|(k+1/2)\cdot 1 - k| = 1/2 = |(k+1/2)\cdot 1 - (k+1)|\,.$$ □

Věta 26. *Nechť $\alpha \in \mathbb{R}$, $i \in \mathbb{N}$.*

$$\left(i > 1 \vee \left(i = 1 \wedge \alpha \neq \alpha_1 + \frac{1}{2}\right)\right) \Rightarrow \alpha_i \textit{ je nejlepší přiblížení } \alpha \textit{ druhého druhu.}$$

Důkaz. Díky větě 25 stačí ukázat, že pro $i \in \mathbb{N}$ existuje nejlepší přiblížení druhého druhu v množině $\{\frac{x}{y};\ x \in \mathbb{Z},\ y \in \boldsymbol{Q_i}\}$ a je dáno právě zlomkem s jmenovatelem Q_i.

Existence: Označme $M_i := \{(x,y) \in \mathbb{Z};\ y \in \boldsymbol{Q_i}\}$ a definujme zobrazení

$$f_i : M_i \to \mathbb{R}_0^+,\ (x,y) \mapsto |\alpha \cdot y - x| \,.$$

Zřejmě $\forall y \in \boldsymbol{Q_i}\ \exists \min(f_i)_*(\mathbb{Z} \times \{y\})$. Protože je $\boldsymbol{Q_i}$ konečná, existuje $m := \min(f_i)_* M_i$. Označme $y_0 = \min\{y \in \boldsymbol{Q_i};\ \exists x \in \mathbb{Z} :\ f_i(x,y) = m\}$.
Ukažme, že existuje jediné $x \in \mathbb{Z} :\ f_i(x,y_0) = m$. Kdyby tomu tak nebylo, existují $x_0 \neq x_0'$ taková, že $f_i(x_0,y_0) = f_i(x_0',y_0) = m$, tedy

$$\left|\alpha - \frac{x_0}{y_0}\right| = \left|\alpha - \frac{x_0'}{y_0}\right| \,,$$

odkud

$$\alpha = \frac{x_0 + x_0'}{2y_0} \,.$$

Tedy $\alpha \in \mathbb{Q}$. Dokažme, že zlomek výše musí být v základním tvaru. Sporem, ať $1 < d$ je největším společným dělitelem $x_0 + x_0'$, $2y_0$. Kdyby $d = 2$, pak $\alpha = \frac{(x_0+x_0')/2}{y_0}$ je základní tvar α. Pak ale $f_i((x_0 + x_0')/2, y_0) = 0 < m$ (nemohou existovat tři různé vzory jednoho prvku kooboru zobrazení $f_i(-,y_0)$). To je spor s definicí x_0, neboť se v něm má nabývat minimum. Ať je nyní naopak $d > 2$. Pak $f_i((x_0 + x_0')/d, 2y_0/d) = 0$, kde ale $2y_0/d < y_0$, což je spor s tím, jak jsme y_0 definovali.

Nechť je n délka rozvoje α. Pak $\alpha = \frac{P_n}{Q_n} = \frac{x_0+x_0'}{2y_0}$ a $Q_n = a_n Q_{n-1} + Q_{n-2}$, kde $a_n > 1$ díky úmluvě 2. Případ $n = 1$ je triviální, případ $n = 2$, $a_2 = 2$ jsme v předpokladu věty vyloučili. Zbývá $(a_n > 2)$ nebo $(a_n = 2 \wedge n > 2)$. Pak $Q_{n-1} < y_0$, tudíž

$$|\alpha Q_{n-1} - P_{n-1}| = \frac{1}{Q_n} = \frac{1}{2y_0} \leq \frac{1}{2} \,.$$

To je ale aspoň stejně dobré přiblížení jako pro $\frac{x_0}{y_0}$, neboť

$$|\alpha \cdot y_0 - x_0| = \left|\frac{x_0 + x_0'}{2y_0} \cdot y_0 - x_0\right| = \left|\frac{x_0' - x_0}{2}\right| \geq \left|\frac{1}{2}\right| \,.$$

Dostali jsme spor.

Rovnost '$y_0 = Q_i$': Díky větě 25 a z definice y_0 je nejlepším přiblížením α druhého řádu α_j, kde $j \leq i$ a $Q_j = y_0$. Kdyby $j < i$, pak podle věty 23 je

$$|\alpha \cdot Q_j - P_j| > \frac{1}{Q_{j+1} + Q_j} \geq \frac{1}{Q_i + Q_{i-1}} \,,$$

dále (pokud by byla délka rozkladu i, nebylo by co řešit) díky lemmatu 17

$$|\alpha \cdot Q_i - P_i| \leq \frac{1}{Q_{i+1}} \,.$$

Protože je však $\frac{x_0}{y_0} = \alpha_j$ nejlepším přiblížením druhého druhu, musí být

$$\frac{1}{Q_i + Q_{i-1}} < \frac{1}{Q_{i+1}} ,$$

tedy $Q_{i+1} < Q_i + Q_{i-1}$, což není pravda.
Dokázali jsme, že $i = j$. □

Připravme si několik tvrzení, které použijeme v dalším tématu.

Lemma 27. *Nechť $\alpha \in \mathbb{R}$, $i \in \mathbb{N}$, $i > 2$.*
Je-li $\alpha \in \mathbb{I}$ nebo délka rozvoje α je aspoň i, pak

$$|\alpha - \alpha_i| < \frac{1}{2Q_i^2} \ \vee \ |\alpha - \alpha_{i-1}| < \frac{1}{2Q_{i-1}^2} .$$

Důkaz. Případ $\alpha_i = \alpha$ je triviální. Jinak každý z těchto dvou parciálních zlomků leží na jiné straně od α, tedy

$$|\alpha - \alpha_i| + |\alpha - \alpha_{i-1}| = |\alpha_i - \alpha_{i-1}| = \frac{1}{Q_i Q_{i-1}} < \frac{1}{2Q_i^2} + \frac{1}{2Q_{i-1}^2} ,$$

kde nerovnost je důsledkem aritmeticko-geometrické nerovnosti pro $\frac{1}{Q_i^2} \neq \frac{1}{Q_{i-1}^2}$. □

Věta 28. *Nechť $\alpha \in \mathbb{R}$, $a, b \in \mathbb{Z}$, $b > 0$,* $\mathrm{NSD}(a, b) = 1$.

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2} \Rightarrow \exists i \in \mathbb{N} : \ \frac{a}{b} = \alpha_i .$$

Důkaz. Pokud platí nerovnost z předpokladu, pak $\frac{a}{b}$ je nejlepším přiblížením druhého druhu. Nechť $a', b' \in \mathbb{Z}$, $b' > 0$. Je-li

$$\left|\alpha \cdot b' - a'\right| \leq |\alpha \cdot b - a| < \frac{1}{2b} ,$$

pak $|\alpha - (a'/b')| < 1/(2bb')$ a

$$\left|\frac{a}{b} - \frac{a'}{b'}\right| \leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{a'}{b'}\right| < \frac{1}{2b^2} + \frac{1}{2bb'} = \frac{b + b'}{2b^2 b'} .$$

Na druhou stranu, kdyby $a/b \neq a'/b'$, pak

$$\left|\frac{a}{b} - \frac{a'}{b'}\right| \geq \frac{1}{bb'} ,$$

dohromady tedy dostaneme

$$\frac{1}{bb'} < \frac{b + b'}{2b^2 b'} ,$$

tedy $b < 2b < b'$. □

5.3 Příklady

Příklad 5. Užijte řetězových zlomků k aproximaci čísla $x = 5279/1721$ racionálním číslem s co nejmenším jmenovatelem tak, aby chyba byla menší než 10^{-3}.
Řešení: Využijme lemmatu 18. V příkladu 3 jsme spočítali rozvoj x do řetězového zlomku. Hledáme i nejmenší takové, aby $\frac{1}{Q_i^2} \leq \frac{1}{10^3}$. To jistě splňuje $i = 4$, neboť $1000 < 6000 < 80^2 < 89^2 = Q_4^2$. Odtud, $P_4/Q_4 = 273/89$ splňuje zadání.
Kdybychom využili lemmatu 17, zjistíme, že již $Q_3Q_4 = 15 \cdot 89 > 15 \cdot 80 = 1200 > 1000$, tedy platí

$$\left|\frac{5279}{1721} - \frac{46}{15}\right| < 0.001 \,.$$

Navíc můžeme zjistit díky větě 23 i dolní odhad chyby:

$$\left|\frac{5279}{1721} - \frac{46}{15}\right| > \frac{1}{Q_3(Q_3+Q_4)} = \frac{1}{15 \cdot 104} = \frac{1}{1560} \approx 6 \cdot 10^{-4} \,.$$

Protože se jedná o lichý parciální zlomek, musí být menší než aproximované číslo. Díky větě 26 je to rovněž nejlepší racionální přiblížení, tj. každé racionální číslo, které je ještě blíže x, už má nutně většího jmenovatele.

6 Pellova rovnice

6.1 Kvadratické iracionality

Definice 13. Nechť $\alpha \in \mathbb{I}$.
Řekneme, že $\alpha = (a_1, \ldots)$ je *periodický* řetězový zlomek, právě když

$$(\exists n, t \in \mathbb{N})(\forall i \geq n) : \; a_{i+t} = a_i \; ,$$

píšeme $\alpha = (a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+(t-1)}})$.
Řekneme, že je periodický *od n_0-tého členu*, právě když je periodický, a

$$n_0 = \min\{n \in \mathbb{N};\; (\exists t \in \mathbb{N})\; (\forall i \geq n_0) : \; a_{i+t} = a_i\} \; .$$

Řekneme, že α má *periodu t_0*, právě když je periodický a

$$t_0 = \min\{t \in \mathbb{N};\; (\exists n \in \mathbb{N})\; (\forall i \geq n) : \; a_{i+t_0} = a_i\} \; .$$

Řetězový zlomek nazveme *ryze periodický*, resp. *smíšený periodický*, právě když je periodický od prvního členu, resp. od n_0-tého členu, kde $n_0 > 1$.

Definice 14. Nechť $\alpha \in \mathbb{R}$.
Řekneme, že α je *kvadratická iracionalita*, právě když $\alpha \in \mathbb{I}$ a existuje taková kvadratická rovnice s celočíselnými koeficienty, že α je jejím kořenem.

Lemma 29. *Nechť $\alpha \in \mathbb{I}$.*
α je kvadratickou iracionalitou, právě když

$$\alpha = \frac{b + \sqrt{c}}{d} \; ,$$

kde $b, c, d \in \mathbb{Z}$, $c > 0$ a $\sqrt{c} \notin \mathbb{N}$.

Důkaz. '$\Rightarrow$': plyne ze vzorce pro výpočet kořenu kvadratické rovnice.
'$\Leftarrow$': Stačí upravit rovnici

$$\left(x - \frac{b + \sqrt{c}}{d}\right)\left(x - \frac{b - \sqrt{c}}{d}\right) = 0 \; . \qquad \square$$

Poznámka 8. Kvadratické iracionality $\frac{b+\sqrt{c}}{d}$ a $\frac{b-\sqrt{c}}{d}$ nazýváme navzájem konjugované. Každá kvadratická iracionalita je kořenem jediné kvadratické rovnice s navzájem nesoudělnými celočíselnými koeficienty. Její konjugovaná kvadratická iracionalita řeší tutéž rovnici.

Uvidíme, že kvadratické iracionality a periodické řetězové zlomky spolu úzce souvisí.

Věta 30. *Nechť $\alpha \in \mathbb{R}$.*

$$\alpha \textit{ je kvadratickou iracionalitou} \iff \alpha \textit{ je periodický.}$$

Důkaz. '$\Leftarrow$': Je-li α periodický od n-tého členu s periodou t, pak $\alpha \in \mathbb{I}$. Označme $x := \alpha$, a $x_i \in \mathbb{I}$ zbytková čísla x (viz definice 7). Díky větě 9, lemmatu 10 je

$$x_{n-1} = (a_n, \ldots, a_{n+(t-1)}, x_{n-1}) \; ,$$

Označme čitatele, resp. jmenovatele x_{n-1} jako P'_i, resp. Q'_i. Je

$$x_{n-1} = \frac{x_{n-1}P'_{t-1} + P'_{t-2}}{x_{n-1}Q'_{t-1} + Q'_{t-2}}\,,$$

což lze upravit na kvadratickou rovnici s celočíselnými koeficienty[5], tedy je x_{n-1} kvadratickou iracionalitou. Je ale též

$$\alpha = (a_1, \ldots, a_{n-1}, x_{n-1})\,.$$

Označíme-li čitatele a jmenovatele α nečárkovaně, je

$$\alpha = \frac{x_{n-1}P_{n-1} + P_{n-2}}{x_{n-1}Q_{n-1} + Q_{n-2}}\,.$$

S využitím lemmatu 29 na x_{n-1} dostaneme, že α je kvadratickou iracionalitou.

‘⇒’: Označme $x := \alpha$ a x_i zbytková čísla. Uvědomme si, že pokud je $Z = \{x_i;\ i \in \mathbb{N}\}$ konečná, pak je řetězový zlomek α periodický. Algoritmus 2 totiž indukuje na Z transformaci danou předpisem $x_i \mapsto x_{i+1}$. Cílem tedy bude ukázat konečnost množiny všech zbytkových čísel.

Nechť pro α platí

$$a\alpha^2 + b\alpha + c = 0\,, \tag{53}$$

kde $a, b, c \in \mathbb{Z}$, $a \neq 0$. Pro $i \in \mathbb{N}$ je $\alpha = (a_1, \ldots, a_i, x_i)$, tedy

$$\alpha = \frac{x_iP_i + P_{i-1}}{x_iQ_i + Q_{i-1}}\,, \tag{54}$$

odkud dosazením do (53) dostaneme, že platí

$$A_ix_i^2 + B_ix_i + C_i = 0\,,\ \text{kde} \tag{55a}$$
$$A_i = aP_i^2 + bP_iQ_i + cQ_i^2\,, \tag{55b}$$
$$B_i = 2aP_iP_{i-1} + b(P_iQ_{i-1} + P_{i-1}Q_i) + 2cQ_iQ_{i-1}\,, \tag{55c}$$
$$C_i = aP_{i-1}^2 + bP_{i-1}Q_{i-1} + cQ_{i-1}^2\,. \tag{55d}$$

Všimněme si, že diskriminant rovnice, jež splňuje α (vztah (53)), je stejný jako diskriminant rovnice, jež splňuje x_i (rovnost (55a)):

$$B_i^2 - 4A_iC_i = (B_i^2 - 4A_iC_i)(P_iQ_{i-1} - P_{i-1}Q_i)^2 = b^2 - 4ac\,. \tag{56}$$

Koeficienty A_i, B_i, C_i jsou celočíselné. Podaří-li se nám ukázat, že množina $\{A_i; i \in \mathbb{N}\}$ je omezená, pak je konečná a též $\{C_i;\ i \in \mathbb{N}\}$ je konečná ($A_i = C_{i+1}$), jakož i $\{B_i;\ i \in \mathbb{N}\}$ (platí (56)). Díky (55a) je konečná i množina všech zbytků, tedy α je periodický.

Dokažme omezenost $\{A_i; i \in \mathbb{N}\}$. Dle lemmatu 18 je

$$\left|\alpha - \frac{P_i}{Q_i}\right| < \frac{1}{Q_i^2}\,,$$

odkud $|\alpha Q_i - P_i| < 1/Q_i$, proto

$$\exists\delta_i,\ |\delta_i| < 1:\ P_i = \alpha Q_i + \frac{\delta_i}{Q_i}\,.$$

[5] V případě, kdy je perioda t rovna jedné, vezmeme místo ní například $t' = 2t$.

Dosaďme tento výsledek do (55b). Je

$$A_i = a\left(\alpha Q_i + \frac{\delta_i}{Q_i}\right)^2 + b\left(\alpha Q_i + \frac{\delta_i}{Q_i}\right)Q_i + cQ_i^2 = Q_i^2(\overbrace{a\alpha^2 + b\alpha + c}^{=0}) + 2a\alpha\delta_i + a\frac{\delta_i^2}{Q_i^2} + b\delta_i\,,$$

tedy

$$|A_i| < |2a\alpha| + |a| + |b|\,. \qquad \square$$

6.2 Pellova rovnice

Definice 15. Rovnici pro neznámé $x, y \in \mathbb{Z}$ tvaru

$$x^2 - Ny^2 = 1\,, \tag{57}$$

kde $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{N}$ nazýváme *Pellovou rovnicí*.
Řešení $(1,0)$ nazveme *triviálním* řešením. Řešení (x_0, y_0) nazveme *kladným řešením*, právě když $x_0, y_0 \in \mathbb{N}$.

Poznámka 9. Zřejmě (x', y') řeší (57), právě když $(|x'|, |y'|)$ řeší (57). Jediná řešení s nulovou druhou proměnnou jsou triviální řešení a $(-1, 0)$. Můžeme se proto omezit na hledání právě všech kladných řešení.

Věnujme se nyní vlastnostem oboru integrity $\mathbb{Z}[\sqrt{N}] = \{a + b\sqrt{N};\ a, b \in \mathbb{Z}\}$, kde N je jako v definici 15, tedy podle lemmatu 29 je $\sqrt{N}$ kvadratická iracionalita. Značme též $a + b\sqrt{N}$ jako (a, b). Víme, že množina všech jednotek, tj. invertibilních prvků (vzhledem k násobení) tvoří komutativní grupu – značme ji $\mathcal{J}$. Hledejme všechny jednotky. Pro tento účel zaveďme automorfismus φ oboru integrity $\mathbb{Z}[\sqrt{N}]$ tak, že

$$a + b\sqrt{N} \overset{\varphi}{\longmapsto} a - b\sqrt{N}\,. \tag{58}$$

Snadno se ukáže, že zobrazení

$$\psi:\ \mathbb{Z}[\sqrt{N}] \to \mathbb{Z}\,, \quad x \overset{\psi}{\longmapsto} x\varphi(x) \tag{59}$$

je homomorfismus $(\mathbb{Z}[\sqrt{N}], \cdot) \to (\mathbb{Z}, \cdot)$. Odtud plyne následující lemma.

Lemma 31. *Nechť $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{N}$.*
Množina všech řešení rovnice

$$x^2 - Ny^2 = \pm 1 \tag{60}$$

je nosičem grupy jednotek oboru integrity $\mathbb{Z}[\sqrt{N}]$.

Důkaz. Je $\psi(x, y) = x^2 - Ny^2$. Je-li $(x, y) \in J$, pak $(x, y) \mid (1, 0)$, tedy $\psi(x, y) \mid \psi(1, 0)$. Na druhou stranu, pokud $\psi(x, y) \mid 1$, pak $|\psi(x, y)| = 1$, tedy $|(x, y)\varphi(x, y)| = \pm(1, 0)$, tedy $(x, y) \mid (1, 0)$. $\square$

Poznámka 10. Našli jsme tak korespondenci (bijekci) všech kladných řešení rovnice (57) a jednotek $(x, y) \in \mathcal{J}$, jež splňují rovnici (60) s kladnou pravou stranou. Díky ní budeme mezi oběma pojetími volně přecházet.

Lemma 32. *Nechť $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{N}$.*
Jsou-li (x', y') a $(\tilde{x}, \tilde{y})$ kladná řešení (57), pak $(\hat{x}, \hat{y})$ definované vztahem

$$\hat{x} + \sqrt{N}\hat{y} = (x' + \sqrt{N}y')(\tilde{x} + \sqrt{N}\tilde{y}) \tag{61}$$

je kladným řešením.

Důkaz. Zřejmě je $\hat{x}, \hat{y} > 0$. Protože (x', y') a $(\tilde{x}, \tilde{y})$ odpovídají jednotkám oboru integrity $\mathbb{Z}[\sqrt{N}]$, jež zobrazí ψ (viz (59)) na 1. Je rovněž obraz součinu roven jedné. □

Je-li (x, y) kladné řešení (57), pak inverze jednotky $(x, y) \in \mathcal{J}$ je $(x, -y) = \varphi(x, y)$. Je tedy řád každého takového prvku nekonečný.

Důsledek 33. *Existuje-li kladné řešení rovnice (57), pak jich existuje nekonečně mnoho.*

Definice 16. Řekneme, že (x_0, y_0) je *fundamentálním řešením* rovnice (57), právě když je jejím kladným řešením a $x_0 = \min\{x \in \mathbb{N};\ (x, y) \text{ kladné řešení (57)}\}$.

Fundamentální řešení zřejmě existuje vždy, když existuje nějaké kladné řešení. Podle definice je minimální v první složce, zřejmě je tedy minimální i v druhé složce.

Věta 34. *Existuje fundamentální řešení rovnice (57).*

Důkaz. Stačí dokázat, že existuje kladné řešení. Hledáme $x, y \in \mathbb{N}$ takové, že $x^2 - Ny^2 = 1$. Pišme

$$\begin{aligned} \frac{x^2}{y^2} - N &= \frac{1}{y^2}\,, \\ \frac{x}{y} - \sqrt{N} &= \frac{1}{y^2(\frac{x}{y} + \sqrt{N})}\,. \end{aligned} \tag{62}$$

Protože je pravá strana poslední rovnosti kladná, je $\frac{x}{y} > \sqrt{N}$, tedy $\frac{x}{y} + \sqrt{N} > 2\sqrt{N} > 2$, což použijeme k úpravě (62) a dostaneme

$$0 < \frac{x}{y} - \sqrt{N} < \frac{1}{2y^2}\,. \tag{63}$$

Díky větě 28 je $\frac{x}{y}$, pokud existuje, nutně parciálním zlomkem $\sqrt{N}$ sudého řádu (viz (20)).

Nechť je $k \in \mathbb{N}$ sudé. Označme P_i, Q_i čitatele, resp. jmenovatele $\sqrt{N}$ a δ_i jeho i-tá zbytková čísla. Je

$$\sqrt{N} = \frac{\delta_k P_k + P_{k-1}}{\delta_k Q_k + Q_{k-1}}$$

Upravujme tuto rovnost.

$$\begin{aligned} \sqrt{N}(\delta_k Q_k + Q_{k-1}) &= \delta_k P_k + P_{k-1} \\ \sqrt{N}Q_{k-1} - P_{k-1} &= \delta_k(P_k - \sqrt{N}Q_k)\,. \end{aligned}$$

Vynásobením poslední rovnosti $(P_k + \sqrt{N}Q_k)$ dostaneme vpravo $\delta_k(P_k^2 - NQ_k^2)$. Vlevo dostaneme

$$(\sqrt{N}Q_{k-1} - P_{k-1})(P_k + \sqrt{N}Q_k) = \sqrt{N}(\underbrace{P_kQ_{k-1} - P_{k-1}Q_k}_{=(-1)^k}) + NQ_kQ_{k-1} - P_kP_{k-1}\,,$$

tedy dohromady

$$\delta_k(P_k^2 - NQ_k^2) = \sqrt{N} + NQ_kQ_{k-1} - P_kP_{k-1}\,. \tag{64}$$

k-tý parciální zlomek $\sqrt{N}$ tedy řeší (57), právě když

$$\delta_k = \sqrt{N} + NQ_kQ_{k-1} - P_kP_{k-1}\,.$$

Označme $m \coloneqq NQ_kQ_{k-1} - P_kP_{k-1}$. Označme dále $\sqrt{N} = (N_1, \ldots)$. Pak

$$N_{k+1} = \lfloor \delta_k \rfloor = \lfloor \sqrt{N} \rfloor + m = N_1 + m\,.$$

Pokračujeme v rozvoji:

$$\delta_{k+1} = \frac{1}{\sqrt{N} + m - N_{k+1}} = \frac{1}{\sqrt{N} - \lfloor \sqrt{N} \rfloor} = \delta_1\,.$$

To znamená, že $\sqrt{N} = (N_1, \ldots, N_k, N_1 + m, \overline{N_2, \ldots, N_1 + m})$, tedy (rozvoj) $\sqrt{N}$ je periodický od členu $j \leq 2$ s periodou t, $lt = k$, kde $l \in \mathbb{N}$. □

Důkaz věty 34 zůstává nekompletní – poznamenejme, že každá kvadratická iracionalita tvaru $\sqrt{N}$, kde $N \in \mathbb{N}$ je periodická od druhého členu, přičemž označíme-li její periodu t, pak (viz [3])

$$\sqrt{N} = (N_1, \overline{N_2, \ldots, N_t, 2N_1})\,.$$

Pokud bychom ukázali, že navíc $m = N_1$, důkaz by byl dokončen.

Důsledek 35. *Nechť $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{N}$.*
Pokud perioda $\sqrt{N}$ je t, pak fundamentální řešení rovnice (57) je (P_k, Q_k), kde

$$k = \begin{cases} 2t & \text{, pokud je } t \text{ liché,} \\ t & \text{jinak.} \end{cases}$$

P_i, resp. Q_i značí čitatele, resp. jmenovatele rozvoje $\sqrt{N}$.
Každé další kladné řešení rovnice (57), (x', y'), splňuje

$$x' + \sqrt{N}y' = (P_k, Q_k)^j$$

pro jisté $j \in \mathbb{N}$.

Důkaz. Důsledek důkazu věty 34. □

Vidíme, že věta 34 nezávisle potvrzuje některé získané výsledky. Vzhledem k neúplnosti důkazu je však ponechávám.

6.3 Příklady

Příklad 6. Najděte fundamentální řešení rovnice

$$x^2 - 29y^2 = 1\,. \tag{65}$$

Řešení: 29 není mocninou přirozeného čísla. Rozvineme $\sqrt{29}$ podle algoritmu 2.

$$\begin{aligned}
\sqrt{29} &= 5 + (\sqrt{29} - 5)\,,\\
\frac{\sqrt{29}+5}{4} &= 2 + \frac{\sqrt{29}-3}{4}\,,\\
\frac{4(\sqrt{29}+3)}{20} &= 1 + \frac{\sqrt{29}-2}{5}\,,\\
\frac{5(\sqrt{29}+2)}{25} &= 1 + \frac{\sqrt{29}-3}{5}\,,\\
\frac{5(\sqrt{29}+3)}{20} &= 2 + \frac{\sqrt{29}-5}{4}\,,\\
\frac{4(\sqrt{29}+5)}{4} &= 10 + (\sqrt{29} - 5)\,,
\end{aligned}$$

odkud $\sqrt{29} = (5, \overline{2, 1, 1, 2, 10})$. Perioda řetězového zlomku je $t = 5$, je tedy fundamentálním řešením (důsledek 35) $(P_{2t}, Q_{2t}) = (P_{10}, Q_{10})$.

i	-1	0	1	2	3	4	5	6	7	8	9	10
N_i	-	-	5	2	1	1	2	10	2	1	1	2
P_i	0	1	5	11	16	27	70	727	1524	2251	3775	9801
Q_i	1	0	1	2	3	5	13	135	283	418	701	1820

Fundamentální řešení $(9801, 1820)$ je zároveň nejmenším kladným řešením rovnice (65).

Vysvětlivky, použité značení

$\mathbb{N} = \{1, 2, 3, \ldots\}$	množina všech přirozených čísel
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$
$\boldsymbol{n}$	značí množinu $\{1, 2, \ldots, n\}$ v případě, že $n \in \mathbb{N}$.
$A \subset B$	A je podmnožinou B, tj. $a \in A \Rightarrow a \in B$. Ostrou inkluzi značím '$A \subsetneq B$'.
$f : A \to B$	zobrazení/funkce s oborem A a kooborem B. Tedy $\forall a \in A\, \exists b \in B : f(a) = b$. Někdy píši místo '$f(a)$' pouze '$fa$'.
f_*	je-li $f : A \to B$, pak $f_* : P(A) \to P(B)$, $M \mapsto \{fm;\, m \in M\}$, kde $P(X)$ značí potenční množinu množiny X
NSD	největší společný dělitel

Reference

[1] Halaš, R.: *Teorie čísel*, Vydavatelství Univerzity Palackého, Olomouc 1997

[2] Chinčin, A. J.: *Řetězové zlomky*, Přírodovědecké vydavatelství, Praha 1952

[3] Olds, C. D.: *Continued Fractions*, Random House, 1963