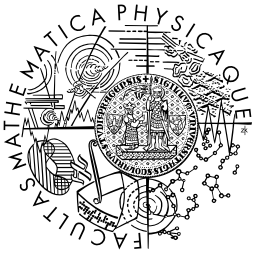

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Martin Kuděj

Řetězové zlomky s předepsanou periodou

Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2020

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Rád bych poděkoval vedoucímu práce Mgr. Vítězslavu Kalovi, Ph.D. za veškerou jeho ochotu a čas věnovaný individuálním konzultacím, dále za cenné připomínky a rady k psaní této práce.

Název práce: Řetězové zlomky s předepsanou periodou

Autor: Martin Kuděj

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Tato práce se zabývá řetězovými zlomky algebraických čísel stupně 2. Jsou ukázány jejich základní vlastnosti, včetně sepsání potřebné teorie. Tato teorie je poté použita k nalezení tvaru řetězového zlomku druhých odmocnin z přirozených čísel, které nejsou čtverce, a jejich symetrické posloupnosti $(a_1, \ldots, a_k)$. Dále, pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, jsou charakterizována všechna N přirozená, jejichž druhé odmocniny mají řetězový zlomek právě s touto symetrickou posloupností $(a_1, \ldots, a_k)$. Tato přirozená N jsou popsána jako funkční hodnoty nějakého kvadratického polynomu, jehož vlastnosti budou v této práci rovněž zkoumány.

Klíčová slova: Řetězový zlomek, periodicita, algebraické číslo stupně 2, kvadratický polynom, symetrická posloupnost

Title: Continued fractions with prescribed period

Author: Martin Kuděj

Department: Department of algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of algebra

Abstract: This thesis concerns continued fractions of quadratic irrationals. Their basic properties are shown, including mentioning necessary theory to do this. Then, this theory is used to find the form of continued fractions of square roots of positive nonsquare integers and their symmetric part $(a_1, \ldots, a_k)$. Next, for a given symmetric sequence of positive integers $(a_1, \ldots, a_k)$, we find all natural numbers N, whose square root has a continued fraction with symmetric part $(a_1, \ldots, a_k)$. These positive N will be described as values of a certain quadratic polynomial, whose properties are studied as well in the thesis.

Keywords: Continued fraction, periodicity, quadratic irrational, quadratic polynomial, symmetric sequence

Obsah

Úvod **2**

1 Řetězové zlomky algebraických čísel stupně 2 **4**
1.1 Zavedení řetězových zlomků 4
1.2 Některá známá tvrzení a značení 6
1.2.1 Základní vlastnosti řetězových zlomků 6
1.2.2 Lineární diofantické rovnice 7
1.2.3 $p-$prvková konečná tělesa 8
1.3 Algebraická čísla stupně 2 9
1.3.1 Základní definice 9
1.3.2 Čistě periodické řetězové zlomky 10
1.4 Redukované kvadratické iracionality 13
1.4.1 Základní vlastnosti redukovaných kvadratických iracionalit 13
1.4.2 Opačná implikace k větě 23 14

2 Řetězové zlomky druhých odmocnin z přirozených čísel **17**
2.1 Případ $k = 0$ 18
2.2 Obecný případ $k \in \mathbb{N}$ 19
2.2.1 Ekvivalentní podmínka k $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$ . . . 19
2.2.2 Charakterizace případů, kdy vhodná čísla N existují . . . 20
2.2.3 Samotné určení kvadratického polynomu 23

3 Zkoumání hodnot čísel N modulo prvočísla **26**
3.1 Hodnoty čísel N modulo 2 26
3.1.1 Případ 1 27
3.1.2 Případ 2 27
3.1.3 Případ 3 27
3.2 Hodnoty čísel N modulo lichá prvočísla 28

Závěr **30**

Seznam použité literatury **31**

Úvod

Řetězové zlomky patří mezi základní objekty teorie čísel. Obecně slouží řetězové zlomky k aproximaci iracionálních čísel racionálními, jde o tzv. dobré aproximace. Co se konkrétně týká řetězových zlomků druhých odmocnin z přirozených čísel, kterým se v této práci budeme primárně věnovat, tak z řetězového zlomku $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_k, 2a_0}]$, kde $a_0 = \lfloor \sqrt{N} \rfloor$ a $(a_1, \ldots, a_k)$ je symetrická posloupnost přirozených čísel, lze vyčíst spoustu informací. Například nám umožní nalézt všechna řešení Pellovy rovnice, což je diofantická rovnice $x^2 - Ny^2 = 1$, která popisuje všechny invertibilní prvky v okruhu $\mathbb{Z}[\sqrt{N}]$. Jak konkrétně tato řešení vypadají, lze nalézt ve skriptech [3], věta 1.15.

V této práci zkoumáme právě tyto řetězové zlomky druhých odmocnin z přirozených čísel. Odvodíme, že každý takový řetězový zlomek je tvaru $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_k, 2a_0}]$, kde $a_0 = \lfloor \sqrt{N} \rfloor$ a $(a_1, \ldots, a_k)$ je symetrická posloupnost přirozených čísel. C. Friesen ve svém článku [2] zkoumal, pro jaké symetrické posloupnosti přirozených čísel $(a_1, \ldots, a_k)$ může tato situace nastat a pokud nastane, tak explicitně popsal všechna přirozená N, jejichž druhá odmocnina má takový řetězový zlomek. C. Friesen dále ukázal, že existuje nekonečně mnoho bezčtvercových N, jejichž druhá odmocnina má řetězový zlomek se symetrickou částí periody o délce k, pro každé $k \in \mathbb{N}$.

V první kapitole této práce zavedeme pojem řetězového zlomku (libovolného reálného čísla) a připomeneme jeho základní vlastnosti, které se dokazují na přednášce Teorie čísel a RSA (viz skripta [3]), a některé z těchto vlastností trochu zobecníme. Dále v sekci 1.2 zmíníme potřebnou teorii týkající se lineárních diofantických rovnic a $p-$prvkových konečných těles, kde p je prvočíslo. Ty samy o sobě s řetězovými zlomky moc nesouvisí, ale v následujících kapitolách se nám budou velice hodit. Dále charakterizujeme ve větách 23, 28 a 29 periodické a čistě periodické řetězové zlomky pomocí čísel, které těmto řetězovým zlomkům přísluší, kvůli čemuž připomeneme pojem algebraického čísla stupně 2 (nad tělesem $\mathbb{Q}$) a zavedeme pojem tzv. redukované kvadratické iracionality, přičemž tato teorie byla čerpána z učebnice C. D. Oldse [5].

Ve druhé kapitole této práce se již zaměříme jenom na řetězové zlomky druhých odmocnin z přirozených čísel a ve větě 30 odvodíme jejich tvar s využitím prostředků odvozených v první kapitole práce. Poté reprodukujeme důkaz C. Friesena z článku [2] o popisu všech přirozených čísel N takových, že $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_k, 2a_0}]$ pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, včetně nutných a postačujících podmínek na tuto posloupnost, aby tato N vskutku existovala, které shrneme ve větě 35. Podotkněme, že samotný důkaz v článku [2] je relativně stručný, v této práci pak dojde k jeho důkladnému rozpracování, a také k částečnému zjednodušení. Nebudeme se však věnovat otázce, zda-li tato nalezená N jsou bezčtvercová či nikoliv.

Třetí kapitola je čistě vlastní přínos autora práce, kde se věnuje chování kvadratických polynomů zkonstruovaných ve druhé kapitole práce, jejichž funkční hodnoty dávají požadovaná přirozená N, v konečných tělesech $\mathbb{Z}_p$ pro p prvočíslo. Ve větách 36 a 37 popíšeme podmínky na symetrickou posloupnost $(a_1, \ldots, a_k)$, aby příslušný kvadratický polynom tvořil bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$ pro dané p prvočíslo. Tyto podmínky jsou ekvivalentní tomu, že pro dané p prvočíslo existuje neko-

nečně mnoho N přirozených s předepsanou symetrickou částí periody takových, že $N \equiv l \bmod p$ pro každé $l \in \mathbb{Z}_p$.

Zkoumání této problematiky je motivováno nedávnými články V. Blomera a V. Kaly [1], [4], ve kterých autoři využili věty 35 ke zkoumání univerzálních kvadratických forem nad tělesy $\mathbb{Q}(\sqrt{N})$. Pro další využití se však může hodit i kontrola nad hodnotou N modulo dané prvočíslo p, k čemuž výsledky této práce představují první krok.

1. Řetězové zlomky algebraických čísel stupně 2

1.1 Zavedení řetězových zlomků

V této sekci si zavedeme pojem řetězového zlomku a základních pojmů s ním souvisejících. Důkazy tvrzení z této sekce lze nalézt v 1. kapitole ve skriptech V. Kaly k předmětu Teorie čísel a RSA [3].

Symbolem $\mathbb{N}_0$ budeme dále značit množinu přirozených čísel s nulou.

Definice 1. *Buď $k \in \mathbb{N}_0$. Konečným řetězovým zlomkem délky k rozumíme formální výraz tvaru*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}$$

kde $\{a_i\}_{i=0}^{k}$ je posloupnost reálných čísel, přičemž pokud $k \neq 0$, tak $a_k \neq 0$. Pro konečný řetězový zlomek budeme používat značení $[a_0, a_1, \ldots, a_k]$.

Definice 2. *Definujme posloupnost zobrazení $\{k_i\}_{i=-1}^{\infty}$ takto:*

$$\begin{aligned} k_{-1} &= 0, \\ k_0 &= 1, \\ \text{pro } i \geq 1, k_i(x_1, \ldots, x_i) &= x_i k_{i-1}(x_1, \ldots, x_{i-1}) + k_{i-2}(x_1, \ldots, x_{i-2}). \end{aligned}$$

Je zřejmé, že se jedná o posloupnost jistých polynomů. Pro $i < 1$ jde o konstantní polynomy, jinak jde o polynomy v i proměnných $x_1, \ldots, x_i$. Polynom k_i nazveme i-tým řetězovým polynomem.

Lemma 3. *Pro každé $n \in \mathbb{N}$ a pro každé $a_1, a_2, \ldots, a_n \in \mathbb{R}$ platí*

$$k_n(a_1, a_2, \ldots, a_n) = k_n(a_n, a_{n-1}, \ldots, a_1). \tag{1.1}$$

Důkaz. Toto lemma je částí tvrzení 1.6 ve skriptech [3]. □

Definice 4. *Ať $\{a_i\}_{i=0}^{\infty}$ je posloupnost přirozených čísel. Definujme posloupnosti*

$$\begin{aligned} p_{-1} &= 1 & q_{-1} &= 0, \\ p_0 &= a_0 & q_0 &= 1, \\ p_n &= a_n p_{n-1} + p_{n-2} & q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

Posloupnosti z předchozí definice $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$ jsou rostoucí. Též platí, že $\forall n \in \mathbb{N}_0$, $p_n = k_{n+1}(a_0, a_1, \ldots, a_n)$, $q_n = k_n(a_1, a_2, \ldots, a_n)$.

Věta 5. *Buď α reálné číslo. Definujme následující posloupnosti čísel:*
$\alpha_0 := \alpha$, $a_0 := \lfloor \alpha_0 \rfloor$ *a pro $i \in \mathbb{N}$, pokud $a_{i-1} \neq \alpha_{i-1}$, tak rekurentně definujeme*

$$\alpha_i := \frac{1}{\alpha_{i-1} - a_{i-1}}, a_i := \lfloor \alpha_i \rfloor.$$

- *α je racionální, právě když existuje $k \in \mathbb{N}_0$ takové, že $\alpha_k = a_k$. Navíc, $\alpha = [a_0, a_1, \ldots, a_k]$.*
- *α je iracionální, právě když $\forall k \in \mathbb{N}_0$, $a_k \neq \alpha_k$. Dále existuje limita posloupnosti $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n]$ a tato limita je rovna právě číslu α. Budeme též psát $\alpha = [a_0, a_1, a_2, \ldots]$.*

Důkaz. Právě racionální čísla mají konečný řetězový zlomek vzhledem k tvrzení 1.4 ve skriptech [3]. Zbytek věty je dokázán ve větě 1.9 ve skriptech [3]. □

Všimněme si, že v případě minulé věty platí, že $a_1, a_2, \cdots \in \mathbb{N}$.
Jelikož platí $a_0 = \lfloor \alpha \rfloor$, tak dostáváme jednoduchý odhad

$$a_0 \leq \alpha \leq a_0 + 1. \tag{1.2}$$

Definice 6. *Nechť α je reálné číslo, které si vyjádříme jako řetězový zlomek stejně jako ve větě 5. Tento řetězový zlomek nazveme* řetězovým zlomkem čísla α, *nebo* rozvojem čísla α do řetězového zlomku.

Rozvoj každého iracionálního čísla α do řetězového zlomku je určen jednoznačně.

Dosud jsme předpokládali, že α, pro které chceme nalézt jeho rozvoj do řetězového zlomku (přesný návod, jak to udělat, je popsán ve větě 5), je libovolné reálné číslo. Nadále budeme zkoumat především rozvoje *iracionálních čísel* do řetězových zlomků a zejména budeme potřebovat pro příslušnou posloupnost celých čísel $\{a_i\}_{i=0}^{\infty}$ pracovat s odpovídajícími posloupnostmi $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$, které byly zadefinované v definici 4. Abychom toto mohli provést, tak potřebujeme, aby všechny členy $a_i \in \mathbb{N}$. Díky větě 5 k tomu stačí předpokládat, že α je iracionální číslo, větší než 1.

Definice 7. *Nechť α je iracionální číslo a $[a_0, a_1, a_2, \ldots]$ je nekonečný řetězový zlomek čísla α. Říkáme, že řetězový zlomek $[a_0, a_1, a_2, \ldots]$ je* periodický *s* periodou *$(a_k, \ldots, a_l)$, pokud existují $k, l \in \mathbb{N}_0, k \leq l$ taková, že*

$$\forall i \in \{0, 1, \ldots, l-k\}, \forall j \in \mathbb{N}, a_{k+i} = a_{k+i+j(l-k+1)}.$$

Pro takový řetězový zlomek používáme značení $[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_l}]$. Takový řetězový zlomek $[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_l}]$ je čistě periodický, *pokud $k = 0$, neboli $\alpha = [\overline{a_0, a_1, \ldots, a_l}]$.*

Tato definice se možná jeví na první pohled trochu komplikovaně, nicméně jde o něco velice intuitivního, k čemuž máme analogii v reálných číslech, neboť obdobným způsobem značíme periodický desetinný rozvoj nějakého racionálního čísla, např. $0,\overline{12} = 0{,}1212121212\ldots$. Tedy pokud máme $\alpha = [\overline{a_0, a_1}]$, tak platí, že $a_0 = a_2 = a_4 \ldots$, a podobně $a_1 = a_3 = a_5 \ldots$.

Index k z předchozí definice 7 odpovídající „začátku periody“, stejně jako index l, představující „konec periody“, není jednoznačně určen. Stejně jako v reálných číslech platí, že $0,\overline{12} = 0,\overline{1212} = 0,12\overline{12}$ apod. Standardně ovšem uvažujeme indexy k, l co nejmenší možné, což budeme nadále u periodického řetězového zlomku $[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_l}]$ předpokládat.

Příklad. Buď $\alpha = \sqrt{2}$. Potom $a_0 = 1$ a pro každé $i \in \mathbb{N}$, $\alpha_i = 1 + \sqrt{2}$, $a_i = 2$. Proto $\alpha = [1, \overline{2}]$.

Ne všechna iracionální čísla mají rozvoj do periodického řetězového zlomku, například $\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2 \dots]$.

Číslo α má periodický řetězový zlomek, právě když je α algebraické číslo stupně 2, a navíc platí, že α má rozvoj do čistě periodického zlomku (s kladným a_0), právě když je α je tzv. *redukovaná kvadratická iracionalita*. Druhou zmíněnou ekvivalenci si dokážeme v této kapitole, ve větách 23 a 28, přičemž první ekvivalence je poté jejím nepříliš složitým důsledkem 29. Pojmy algebraického čísla stupně 2 a redukované kvadratické iracionality si formálně zavedeme v sekci 1.3.

1.2 Některá známá tvrzení a značení

V této sekci si připomeneme známá tvrzení a pojmy z teorie čísel a algebry, které budeme potřebovat v celé této práci, a podle potřeby je i zobecníme, či dokážeme opačné implikace a podobně. Nejprve se ještě podíváme na vlastnosti řetězových zlomků. Poté si ukážeme, jak vypadá množina všech řešení lineární diofantické rovnice, a nakonec si připomeneme p-prvková konečná tělesa, kde p je prvočíslo, a kvadratické funkce nad těmito tělesy.

1.2.1 Základní vlastnosti řetězových zlomků

Posloupnosti $\{a_i\}_{i=0}^{\infty}$, $\{p_i\}_{i=0}^{\infty}$ a $\{q_i\}_{i=0}^{\infty}$, zadefinované v sekci 1.1, mají následující vlastnosti. Důkazy většiny tvrzení v této sekci lze opět nalézt ve skriptech [3] v 1. kapitole.

Lemma 8. *$\forall k \in \mathbb{N}_0$ platí, že* $[a_0, a_1, \dots, a_k] = \dfrac{p_k}{q_k}$.

Důkaz. Toto lemma je dokázáno jako tvrzení 1.5 ve skriptech [3]. □

Definice 9. *Zlomek $\dfrac{p_k}{q_k}$ z předchozího lemmatu 8 nazveme k-tým sblíženým zlomkem čísla $[a_0, a_1, \dots]$.*

Tvrzení 10. *Pro $k \in \mathbb{N}_0$ platí, že $p_{k-1}q_k - p_k q_{k-1} = (-1)^k$.*

Důkaz. Tato identita je dokázána ve tvrzení 1.7 ve skriptech [3]. □

Důsledek 11. *Za stejných předpokladů jsou vždy dvojice čísel (p_k, q_k), (p_k, p_{k-1}), (q_k, q_{k-1}) nesoudělné.*

Důkaz. Pokud jakákoliv z těchto dvojic čísel má nějakého společného dělitele d, potom díky tvrzení 10 d dělí i číslo 1, či -1. To ovšem nutně znamená, že d je rovno nějakému z těchto invertibilních prvků okruhu $\mathbb{Z}$. □

Tvrzení 12. *Nechť $\alpha = [a_0, a_1, \dots, a_k, \beta]$, kde α je iracionální a $\beta > 1$. Pak*

$$\alpha = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}. \tag{1.3}$$

Důkaz. Toto tvrzení odpovídá tvrzení 1.8 ve skriptech [3]. □

K tomuto tvrzení platí též opačná implikace, která však ve skriptech [3] není ani vyslovena, proto ji zde uvedeme i s důkazem v následujícím lemmatu:

Lemma 13. *Mějme $\alpha \in \mathbb{R}, \beta > 1$ iracionální číslo, $a_0 \in \mathbb{Z}$. Potom $\forall m \in \mathbb{N}_0$ a libovolná přirozená čísla $a_1, a_2, \ldots, a_m$, rovnost $\alpha = \dfrac{\beta p_m + p_{m-1}}{\beta q_m + q_{m-1}}$, implikuje $\alpha = [a_0, a_1, \ldots, a_m, \beta]$.*

Důkaz. Důkaz provedeme matematickou indukcí podle m.

Pro $m = 0$ máme $\alpha = \dfrac{\beta p_0 + p_{-1}}{\beta q_0 + q_{-1}} = \dfrac{\beta a_0 + 1}{\beta} = a_0 + \dfrac{1}{\beta} = [a_0, \beta]$.

Pro indukční krok uvažme platnost tvrzení pro nějaké $m - 1 \in \mathbb{N}_0$ a ukažme platnost tvrzení pro m:

$$\alpha = \frac{\beta p_m + p_{m-1}}{\beta q_m + q_{m-1}} = \frac{p_m + \dfrac{p_{m-1}}{\beta}}{q_m + \dfrac{q_{m-1}}{\beta}} = \frac{p_{m-1}\left(a_m + \dfrac{1}{\beta}\right) + p_{m-2}}{q_{m-1}\left(a_m + \dfrac{1}{\beta}\right) + q_{m-2}}$$ a použitím indukčního předpokladu (pro $m - 1$) dostáváme $\alpha = \left[a_0, a_1, \ldots, a_{m-1}, a_m + \dfrac{1}{\beta}\right] = [a_0, a_1, \ldots, a_m, \beta]$, což jsme chtěli ukázat. □

1.2.2 Lineární diofantické rovnice

V této práci využijeme rovněž znalosti popisu množiny všech řešení lineární diofantické rovnice. Konkrétně tato rovnice vypadá tak, že pro dané celočíselné parametry a, b, c hledáme všechna celočíselná řešení (x, y), vyhovující podmínce $ax - by = c$. Budeme se věnovat pouze speciálnímu případu, kdy a, b jsou nesoudělná. Budeme také potřebovat známou Bézoutovu rovnost, podle které pro a, b nesoudělná čísla existuje právě jedna dvojice celých čísel r, s tak, že $ra + sb = 1$.

Bézoutova rovnost rovněž zajišťuje existenci řešení lineární diofantické rovnice. Jak vypadají všechna řešení této rovnice, si dokážeme v tomto lemmatu:

Lemma 14. *Buďte a, b nesoudělná celá čísla, $c \in \mathbb{Z}$. Zvolme nějaké řešení (x_1, y_1) rovnice*

$$ax - by = c. \tag{1.4}$$

Potom (x_2, y_2) je řešením rovnice (1.4), právě když existuje $k \in \mathbb{Z}$ tak, že

$$x_2 = x_1 + kb,\ y_2 = y_1 + ka. \tag{1.5}$$

Důkaz. Je zřejmé, že (x_2, y_2) vyhovující podmínce v (1.5) též splňují rovnost (1.4).

Opačně, mějme (x_2, y_2) nějaké řešení rovnice (1.4), tedy nechť $ax_2 - by_2 = c$. Jelikož (x_1, y_1) též řeší tuto rovnici, tak odečtením vzniklých rovnic dostáváme vztah

$$a(x_2 - x_1) = b(y_2 - y_1). \tag{1.6}$$

Dále si napišme Bézoutovu rovnost pro nesoudělná a, b, tedy nechť $ra + sb = 1$ pro nějaká r,$s \in \mathbb{Z}$. Tuto rovnost přenásobíme rozdílem $x_2 - x_1$ a dosazením vztahu (1.6) dostáváme, že $rb(y_2 - y_1) + sb(x_2 - x_1) = x_2 - x_1$.

To ovšem znamená, že b dělí $x_2 - x_1$, neboli existuje $k \in \mathbb{Z}$ tak, že $x_2 - x_1 = kb$, což přesně znamená $x_2 = x_1 + kb$.

Nakonec dosadíme vztah $x_2 - x_1 = kb$ do (1.6) a dostaneme $y_2 - y_1 = ka$, což odpovídá vztahu $y_2 = y_1 + ka$ a lemma je dokázané. □

Zobecnění tohoto důkazu a další informace k (nejen lineárním) diofantickým rovnicím lze nalézt v [7].

1.2.3 $p-$prvková konečná tělesa

Ke konci této práce též využijeme $p-$prvková konečná tělesa (pro která budeme používat standardní značení $\mathbb{Z}_p$, kde p je prvočíslo).

Definice 15. *Buďte a, b, m celá čísla, $m > 0$. Řekneme, že a je* kongruentní *b modulo m, píšeme $a \equiv b \bmod m$, pokud m dělí $a - b$, tedy existuje $k \in \mathbb{Z}$ tak, že $a - b = mk$.*

Snadno nahlédneme, že $a \equiv b \bmod m$ je ekvivalentní s tím, že a a b mají stejný zbytek po dělení číslem m. Speciálně dostáváme, že pro p prvočíslo je $a \equiv b \bmod p$, právě když $a = b$ v tělese $\mathbb{Z}_p$.

Konkrétně nás bude zajímat dosti specifická situace, a sice jak je to s prostotou kvadratické funkce $ax^2 + bx + c$ jakožto zobrazení $\mathbb{Z}_p \to \mathbb{Z}_p$, pro p fixní prvočíslo, výhradně v závislosti na koeficientech $a, b, c \in \mathbb{Z}_p$. Jelikož jde o zobrazení mezi konečnými množinami stejné velikosti, tak prostota této funkce implikuje, že tato funkce je bijekce, neboli pro libovolné d celé existuje (dokonce právě jedno) $x \in \mathbb{Z}_p$ tak, že $d \equiv ax^2 + bx + c \bmod p$, kde $a, b, c \in \mathbb{Z}_p$ jsou zvoleny tak, že daná kvadratická funkce je prostá. Jak tyto koeficienty volit, si ukážeme v tomto tvrzení:

Tvrzení 16. *Buď p prvočíslo, $a, b, c \in \mathbb{Z}_p$ a mějme funkci $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = ax^2 + bx + c$. Potom platí:*

- *Pokud je p liché ($p \neq 2$), tak funkce f je prostá, právě když $a = 0$ a současně $b \neq 0$.*
- *Pro $p = 2$ je funkce f prostá, právě když $a \neq b$, tedy a,b jakožto prvky $\mathbb{Z}$ mají různou paritu.*

Důkaz. V první řadě je třeba si uvědomit, že na absolutním členu c nezáleží, neboť c pouze „posouvá“ hodnoty funkce f o nějakou konstantu, nezávislou na x. Tak tedy bez újmy na obecnosti předpokládejme, že $c = 0$.

Případem $p = 2$ se také nebudeme zabývat, neboť to je pouze rozbor 4 případů podle koeficientů $a, b \in \mathbb{Z}_2$.

Případ, kdy p je liché prvočíslo, rozebereme podrobněji:

$\Leftarrow$: Buď $b \neq 0$ a chceme ukázat prostotu funkce $f(x) = bx$. To znamená, že chceme ukázat, že $\forall k, l \in \mathbb{Z}_p$, $bk = bl \implies k = l$. $\mathbb{Z}_p$ je ale těleso, tedy můžeme nenulovým prvkem b krátit, a proto je vskutku tato funkce f prostá.

$\Rightarrow$: Tuto implikaci dokážeme nepřímo: Nechť $a \neq 0$, nebo $b = 0$ (v $\mathbb{Z}_p$). Chceme ukázat, že za těchto předpokladů existují různá $k, l \in \mathbb{Z}_p$ taková, že $f(k) = f(l)$. Rozlišíme 2 případy:

1. Nechť $b = 0$. Potom $f(x) = ax^2$, $a \neq 0$. Nahlédneme, že $f(1) = f(-1)$, a zároveň $1 \neq -1$, neboť p je liché (nepracujeme v tělese charakteristiky 2). Tedy v tomto případě funkce f není prostá.
2. Nechť $b \neq 0$. Všimneme si, že $f(x) = ax^2 + bx = x(ax + b)$. Potom $f(0) = f\left(\frac{-b}{a}\right)$. Zároveň platí, že $0 \neq \frac{-b}{a}$, protože $b \neq 0$ (a zároveň zlomek $\frac{-b}{a}$ je dobře definovaný, protože $a \neq 0$). Tedy ani v tomto případě f není prostá, čímž je důkaz dokončen, protože žádný jiný případ nastat nemůže.

□

1.3 Algebraická čísla stupně 2

V této sekci si zadefinujeme některé vlastnosti iracionálních čísel α, jejichž řetězové zlomky budeme v této kapitole zkoumat. Půjde o algebraická čísla stupně 2, speciálně tzv. redukované kvadratické iracionality (viz definice 21).

1.3.1 Základní definice

Definice 17. *Buď N přirozené číslo. Řekneme, že N je* čtverec*, pokud je N druhou mocninou nějakého přirozeného čísla, tedy pokud $\exists k \in \mathbb{N}$, $k^2 = N$. V opačném případě říkáme, že N* není čtverec*.*

Dále řekneme, že N je bezčtvercové*, pokud není dělitelné žádným čtvercem různým od 1, neboli $\forall k, l \in \mathbb{N}$, $k > 1$, $N \neq k^2 l$.*

Dále platí, že pro každé přirozené číslo N: N není čtverec $\iff$ $\sqrt{N}$ je iracionální.

Nyní si zavedeme pojmy algebraického čísla stupně 2 a ireducibilního polynomu, který využijeme čistě z technických důvodů. Mělo by jít o známé pojmy z kurzu Algebra 2, podrobnosti viz učebnice D. Stanovského [6].

Definice 18. *Buď $f \in \mathbb{Q}[x]$ polynom stupně alespoň 1. Řekneme, že f je* ireducibilní *polynom, pokud pro každé dva polynomy $g, h \in \mathbb{Q}[x]$, $f = gh$ platí, že g nebo h je konstantní polynom.*

Definice 19. *Buď α reálné číslo. Řekneme, že α je* algebraické stupně 2*, existuje-li ireducibilní polynom f stupně 2 s celočíselnými koeficienty, tedy existují-li čísla $a, b, c \in \mathbb{Z}$, $a \neq 0$, $f(x) = ax^2 + bx + c$ taková, že $f(\alpha) = 0$.*

Nejprve poukážeme na to, že libovolné α algebraické číslo stupně 2 je nutně iracionální. Pokud by totiž α bylo racionální, pak by jistě bylo kořenem nějakého polynomu stupně 1 s celočíselnými koeficienty, a tak by příslušný polynom f dle definice 19 nebyl ireducibilní. Dále si všimneme, že polynom f je jednoznačně určen až na násobek. Je více způsobů, jak si lze toto uvědomit, např. pomocí tzv. *minimálního polynomu* a jeho jednoznačnosti, z čehož nám plyne jednoznačnost polynomu f, ale s racionálními koeficienty. Poté by ještě bylo potřeba přenásobit koeficienty tohoto polynomu nějakým společným násobkem jmenovatelů koeficientů tohoto polynomu. Podrobnosti k minimálnímu polynomu lze nalézt v učebnici D. Stanovského [6] na straně 135.

Je-li α algebraické číslo stupně 2, kořenem polynomu s celočíselnými koeficienty $ax^2 + bx + c$, $a \neq 0$, bez újmy na obecnosti $a > 0$ (jinak bychom přenásobili celý polynom -1), poté aplikací vzorce pro kvadratickou rovnici snadno dostaneme, že

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Dále vidíme, že $b^2 - 4ac \in \mathbb{N}$ a není to čtverec, neboť α je iracionální. Nadále budeme psát, že

$$\alpha = \frac{u \pm \sqrt{N}}{v} = e + f\sqrt{N}, \tag{1.7}$$

kde $u = -b \in \mathbb{Z}$, $v = 2a \in \mathbb{N}$, $N = b^2 - 4ac \in \mathbb{N}$ takové, že N není čtverec (viz definice 17), dále $e, f \in \mathbb{Q}$, $f \neq 0$.

Pokud navíc přidáme předpoklad, že N je bezčtvercové (viz definice 17), tak racionální čísla e, f, i přirozené N, jsou určena jednoznačně. To nám zajistí korektnost definice následujícího pojmu konjugátu:

Definice 20. *Je-li $\alpha = e + f\sqrt{N}$, kde $e, f \in \mathbb{Q}$, $N \in \mathbb{N}$, N není čtverec, pak definujeme* konjugát *čísla α jako $\alpha' := e - f\sqrt{N}$.*

Je-li takovéto α kořenem polynomu $ax^2 + bx + c$, pak α' je kořenem téhož polynomu. Přesně pro $f = 0$ platí, že α není algebraické číslo stupně 2, a právě pro tyto α platí, že $\alpha = \alpha'$.

Snadno se dají dokázat vztahy $(a+b)' = a'+b'$, $(a-b)' = a'-b'$, $(ab)' = a'b'$, $\left(\frac{a}{c}\right)' = \frac{a'}{c'}$ pro libovolná a, b, c vyhovující podmínce v definici 20, $c \neq 0$.

Nyní konečně můžeme zavést slíbený pojem redukované kvadratické iracionality:

Definice 21. *Buď α algebraické číslo stupně 2. Řekneme, že α je* redukovaná kvadratická iracionalita*, pokud $\alpha > 1$, a zároveň $\alpha' \in (-1, 0)$.*

Příklad. Nechť N je přirozené číslo, N není čtverec a uvažujme $\alpha = \sqrt{N} = [a_0, a_1, \dots]$. Potom $a_0 + \sqrt{N}$ je redukovaná kvadratická iracionalita.

Pro redukované kvadratické iracionality bude stěžejní jejich zápis ve tvaru $\alpha = \frac{u \pm \sqrt{N}}{v}$, viz rovnost (1.7), čemuž se podrobněji budeme věnovat v sekci 1.4.

1.3.2 Čistě periodické řetězové zlomky

Chceme charakterizovat redukované kvadratické iracionality pomocí jejich řetězových zlomků, a sice tak, že právě redukované kvadratické iracionality mají čistě periodický řetězový zlomek s kladným prvním členem. Začneme implikací, dle které každé číslo, které má čistě periodický řetězový zlomek s kladným prvním členem, je nutně redukovaná kvadratická iracionalita (a že vůbec jde o algebraické číslo stupně 2). K důkazu této implikace, který provedeme ve větě 23, budeme potřebovat posloupnosti $\{p_i\}_{i=0}^{\infty}$ a $\{q_i\}_{i=0}^{\infty}$, zadefinované v definici 4 a jejich vlastnosti, popsané ve sekci 1.2. Opačnou implikaci dokážeme ve větě 28. Ještě předtím si odvodíme jednu jednoduchou vlastnost těchto posloupností:

Lemma 22. *Mějme $[a_0, a_1, \dots, a_k] = \frac{p_k}{q_k}$, podobně jako v lemmatu 8. Poté platí:*

1.
$$[a_k, a_{k-1}, \dots, a_0] = \frac{p_k}{p_{k-1}} \tag{1.8}$$

2.
$$\text{pokud } k \in \mathbb{N}, \text{ tak } [a_k, a_{k-1}, \dots, a_1] = \frac{q_k}{q_{k-1}}. \tag{1.9}$$

Důkaz. Dokážeme pouze první rovnost (1.8), důkaz rovnosti (1.9) je obdobný. Důkaz obou rovností je jednoduchý, opírá se pouze o rekurentní definici $p_k, p_{k-1} \dots$, respektive $q_k, q_{k-1} \dots$:

$\frac{p_k}{p_{k-1}} = \frac{a_k p_{k-1} + p_{k-2}}{p_{k-1}} = a_k + \frac{p_{k-2}}{p_{k-1}} = a_k + \frac{1}{\frac{p_{k-1}}{p_{k-2}}}$ a iterujeme tentýž postup pro $\frac{p_{k-1}}{p_{k-2}}$. Je jasné, že tímto postupem tvoříme nějaký řetězový zlomek. Tento postup opakujeme tak dlouho, dokud nedojdeme k rovnosti

$$\frac{p_k}{p_{k-1}} = \left[a_n, a_{n-1}, \ldots, a_1, \frac{p_0}{p_{-1}}\right].$$

Jelikož $p_0 = a_0$, $p_{-1} = 1$, opravdu jsme odvodili rovnost (1.8). □

Nyní již dokážeme první implikaci slíbené charakterizace redukovaných kvadratických iracionalit pomocí jejich řetězových zlomků.

Věta 23. *Buď $k \in \mathbb{N}_0$ a mějme přirozená čísla $a_0, a_1, \ldots, a_k$. Označme $\alpha := [\overline{a_0, a_1, \ldots, a_k}]$. Potom α je redukovaná kvadratická iracionalita, a navíc platí rovnost*

$$\frac{-1}{\beta} = \alpha', \text{ kde } \beta := [\overline{a_k, a_{k-1}, \ldots, a_0}]. \tag{1.10}$$

Důkaz. Jelikož $a_0 \in \mathbb{N}$, tak z nerovností (1.2) a iracionality α plyne, že $\alpha > 1$; analogicky platí i $\beta > 1$. Odlišme 2 případy:

1): $k = 0$:

V tomto případě platí, že $\alpha = [\overline{a_0}]$. Z věty o aritmetice limit a periodicitě tohoto řetězového zlomku snadno nahlédneme, že $\alpha = [a_0, \alpha] = a_0 + \frac{1}{\alpha}$. Tuto rovnost upravíme, vynásobením α:

$$\alpha^2 - a_0\alpha - 1 = 0. \tag{1.11}$$

Právě jsme ukázali, že α je algebraické číslo stupně 2. Nyní se podívejme na β. V našem případě platí, že $\alpha = \beta = [\overline{a_0}]$, a proto bude platit rovnost $\beta^2 - a_0\beta - 1 = 0$. Vynásobíme tuto rovnost zlomkem $\frac{-1}{\beta^2}$ a dostaneme:

$$-1 - a_0\left(\frac{-1}{\beta}\right) + \frac{1}{\beta^2} = \left(\frac{-1}{\beta}\right)^2 - a_0\left(\frac{-1}{\beta}\right) - 1 = 0. \tag{1.12}$$

Z rovností (1.11) a (1.12) plyne, že jak α, tak $\frac{-1}{\beta}$ jsou kořeny kvadratické rovnice $x^2 - a_0x - 1 = 0$. α je ale kladné, $\frac{-1}{\beta}$ je záporné, jedná se tedy o dva různé kořeny této rovnice, proto platí rovnost (1.10). Konečně, $\beta > 1$, proto $\alpha' = \frac{-1}{\beta} \in (-1, 0)$ a z definice jsme tedy ověřili, že α je redukovaná kvadratická iracionalita.

2): $k > 0$:

V tomto případě budeme postupovat obdobně, jenom si pro nalezení příslušné kvadratické rovnice budeme muset pomoci lemmatem 22.

Nechť $\alpha = [\overline{a_0, a_1, \ldots, a_k}]$. Potom $\alpha = [a_0, a_1 \ldots, a_k, \alpha]$ a použitím tvrzení 12 dostáváme, že $\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$. Přenásobíme jmenovatelem a upravíme:

$$q_k\alpha^2 - (p_k - q_{k-1})\alpha - p_{k-1} = 0. \tag{1.13}$$

Tedy α je opět algebraické číslo stupně 2. Nyní tedy zkoumejme číslo β:

$\beta = [\overline{a_k, a_{k-1}, \ldots, a_0}]$. Označme $\frac{r_n}{s_n}$ n-tý sblížený zlomek čísla β. Speciálně se podíváme na k-tý a $k-1$-ní sblížený zlomek, pro který dle lemmatu 8 platí:

$$[a_k, a_{k-1}, \ldots, a_1] = \frac{r_{k-1}}{s_{k-1}},\ [a_k, a_{k-1}, \ldots, a_0] = \frac{r_k}{s_k}. \tag{1.14}$$

Již zmíněné lemma 22 dává:

$$[a_k, a_{k-1}, \ldots, a_0] = \frac{p_k}{p_{k-1}} \text{ a dále } [a_k, a_{k-1}, \ldots, a_1] = \frac{q_k}{q_{k-1}}. \tag{1.15}$$

Porovnáním rovností (1.14) a (1.15) dostáváme, že $\frac{p_k}{p_{k-1}} = \frac{r_k}{s_k}$ a $\frac{q_k}{q_{k-1}} = \frac{r_{k-1}}{s_{k-1}}$. Všechny tyto zlomky jsou nějaké sblížené zlomky, proto jsou dle důsledku 11 v základním tvaru, takže musí nastat rovnost příslušných čitatelů a jmenovatelů, neboli dostáváme:

$$p_k = r_k,\ p_{k-1} = s_k,\ q_k = r_{k-1},\ q_{k-1} = s_{k-1}. \tag{1.16}$$

Nyní s výrazem β uděláme podobné úpravy jako s výrazem α výše:

$\beta = [\overline{a_k, a_{k-1}, \ldots, a_0}] = [\overline{a_k, a_{k-1}, \ldots, a_0}, \beta]$, tedy opět použijeme tvrzení 12 a dostáváme, spolu s použitím vztahu (1.16), rovnost:

$$\beta = \frac{\beta r_k + r_{k-1}}{\beta s_k + s_{k-1}} \overset{(1.16)}{=} \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}. \tag{1.17}$$

Opět se zbavíme jmenovatele, upravíme: $\beta^2 p_{k-1} + \beta(q_{k-1} - p_k) - q_k = 0$. Stejně jako v minulém případě, i zde nás zajímá výraz $\frac{-1}{\beta}$, tedy vydělme celou rovnost $-\beta^2$. Po úpravě:

$$q_k \left(\frac{-1}{\beta}\right)^2 - (p_k - q_{k-1})\left(\frac{-1}{\beta}\right) - p_{k-1} = 0. \tag{1.18}$$

Odvodili jsme rovnosti (1.13) a (1.18), ze kterých plyne, že α a $\frac{-1}{\beta}$ jsou dva různé kořeny rovnice $q_k x^2 - (p_k - q_{k-1})x - p_{k-1} = 0$, tedy vztah (1.10) platí.

Zbytek důkazu je pak analogický prvnímu případu $k = 0$, tedy $\alpha > 1$, a zároveň $\alpha' = \frac{-1}{\beta} \in (-1, 0)$, takže i v tomto případě je α redukovaná kvadratická iracionalita. Žádný jiný případ nastat nemůže, tím byl tedy proveden důkaz. □

Všimněme si, že pro druhý případ $k > 0$, vzniklý polynom s kořenem α dává po dosazení $k = 0$ přesně polynom, který jsme odvodili v prvním případě důkazu. Jediným důvodem, proč jsme se s případem $k = 0$ museli vypořádat zvlášť, byly předpoklady lemmatu 22, které pro $k = 0$ nedává smysl, neboť $q_{-1} = 0$ a nulou dělit nemůžeme.

Platí též opačná implikace k větě 23, kterou si dokážeme na konci sekce 1.4 ve větě 28.

1.4 Redukované kvadratické iracionality

1.4.1 Základní vlastnosti redukovaných kvadratických iracionalit

Zde se budeme podrobněji věnovat redukovaným kvadratickým iracionalitám, zadefinovaným v definici 21. Redukovaná kvadratická iracionalita α je nutně algebraické číslo stupně 2, tedy jde o iracionální číslo, které je kořenem nějakého kvadratického polynomu s celočíselnými koeficienty. Tedy lze použít vzorec pro výpočet kvadratické rovnice, což jsme si odvodili a zapsali v rovnosti (1.7). Především se budeme věnovat zápisu $\alpha = \frac{u \pm \sqrt{N}}{v}$, kde $u \in \mathbb{Z}, v, N \in \mathbb{N}$, N není čtverec (tedy opět bez újmy na obecnosti $v > 0$, jinak bychom příslušný minimální polynom čísla α přenásobili -1). Tento zápis je v prvé řadě pouhou aplikací vzorce pro výpočet kvadratické rovnice, ale též nám umožní charakterizovat redukované kvadratické iracionality pouze pomocí koeficientů u, v, čehož využijeme v důkazu věty 28. Abychom toto mohli provést, potřebujeme mít ještě jednoznačnost těchto koeficientů u, v v rovnosti (1.7), pokud máme N fixní:

Lemma 24. *Nechť α je algebraické číslo stupně 2, $\alpha = \frac{u_1 \pm \sqrt{N}}{v_1} = \frac{u_2 \pm \sqrt{N}}{v_2}$, kde $u_1, u_2 \in \mathbb{Z}, v_1, v_2, N \in \mathbb{N}$, N není čtverec. Potom $u_1 = u_2$, $v_1 = v_2$.*

Důkaz. Pokud $v_1 \neq v_2$, pak snadnou úpravou zjistíme, že $\sqrt{N}$ je racionální, což je ve sporu s tím, že N není čtverec. Proto nutně $v_1 = v_2$, z čehož snadno plyne $u_1 = u_2$. □

Uvědomíme si ještě jednu věc: Pokud $\alpha = \frac{u - \sqrt{N}}{v}$ jako výše, tak α nemůže být redukovanou kvadratickou iracionalitou. Pokud by tomu tak bylo, potom $\frac{u - \sqrt{N}}{v} > 1$, $\frac{u + \sqrt{N}}{v} \in (-1, 0)$. První nerovnost nutně implikuje $u > 0$, pak ale i $\frac{u + \sqrt{N}}{v} > 0$ a máme spor. Proto všechny redukované kvadratické iracionality budou tvaru

$$\frac{u + \sqrt{N}}{v}, \text{ kde } u \in \mathbb{Z},\ v, N \in \mathbb{N}, N \text{ není čtverec.} \tag{1.19}$$

Duálně lze ověřit, že pokud by koeficient v byl záporný, tak aby ten samý výraz tvořil redukovanou kvadratickou iracionalitu, tak bychom museli $\sqrt{N}$ v čitateli odečítat. Přesně tento případ nastane v tvrzení 27.

Jak konkrétně je třeba volit koeficienty u, v, aby se vskutku jednalo o redukovanou kvadratickou iracionalitu, si ukážeme v tomto tvrzení:

Tvrzení 25. *Nechť α je algebraické číslo stupně 2, tvaru jako ve* (1.19)*. Pak α je redukovaná kvadratická iracionalita, právě když platí následující nerovnosti:*

$$0 < u < \sqrt{N} \tag{1.20}$$

$$\sqrt{N} - u < v < u + \sqrt{N} \tag{1.21}$$

Důkaz. $\Rightarrow$: Buď α redukovaná kvadratická iracionalita, tedy $\alpha = \dfrac{u+\sqrt{N}}{v} > 1$, $\alpha' = \dfrac{u-\sqrt{N}}{v} \in (-1,0)$. Potom platí: $\alpha + \alpha' > 0$, čili $\dfrac{2u}{v} > 0$, ale $v > 0$, proto i $u > 0$. Dále, $\alpha' = \dfrac{u-\sqrt{N}}{v} < 0$, opět $v > 0$, takže $u - \sqrt{N} < 0$, celkově jsme dostali nerovnost (1.20).

Nyní, $\alpha > 1$, proto $u+\sqrt{N} > v$. Nakonec, $\alpha' > -1$, a dostaneme $u-\sqrt{N} > -v$, což po drobné úpravě dává nerovnosti (1.21) a tato implikace je hotová.

$\Leftarrow$: Nechť platí nerovnosti(1.20) a (1.21). Poté platí:

$\alpha = \dfrac{u+\sqrt{N}}{v} \overset{(1.21)}{>} \dfrac{u+\sqrt{N}}{u+\sqrt{N}} = 1.$

$0 \overset{(1.20)}{>} \alpha' = \dfrac{u-\sqrt{N}}{v} \overset{(1.21)}{>} \dfrac{u-\sqrt{N}}{\sqrt{N}-u} = -1$, čili α je skutečně redukovaná kvadratická iracionalita, což jsme chtěli ukázat. □

Právě dokázané tvrzení má následující důležitý důsledek:

Důsledek 26. *Pro každé $N \in \mathbb{N}$, N není čtverec, existují nějaké redukované kvadratické iracionality tvaru* (1.19)*, ale je jich konečně mnoho.*

Důkaz. Plyne okamžitě z nerovností (1.20) a (1.21) a předchozího tvrzení 25. □

Pro důsledek 26 stačilo dokázat pouze implikaci ($\Rightarrow$) v tvrzení 25, nicméně opačná implikace nám zaručuje, že vůbec pro libovolné N přirozené, co není čtverec, existují příslušné redukované kvadratické iracionality.

1.4.2 Opačná implikace k větě 23

Nyní se již podíváme na rozvoj redukované kvadratické iracionality do řetězového zlomku. Nejprve se podíváme na začátek tohoto rozvoje, na α_1 v následujícím tvrzení, tento postup poté budeme iterovat na začátku důkazu klíčové věty 28, opačné implikace k větě 23 o charakterizaci redukovaných kvadratických iracionalit pomocí jejich řetězových zlomků.

Tvrzení 27. *Buď α redukovaná kvadratická iracionalita, $\alpha = \dfrac{u+\sqrt{N}}{v}$ jako ve vztahu* (1.19)*. Napišme si $\alpha = a_0 + \dfrac{1}{\alpha_1}$, kde $a_0 = \lfloor \alpha \rfloor$ a $\alpha_1 \in \mathbb{R}$. Potom α_1 je též redukovaná kvadratická iracionalita, tvaru $\alpha_1 = \dfrac{u_1+\sqrt{N}}{v_1}$ pro vhodná u_1,$v_1 \in \mathbb{Z}$.*

Důkaz. Nechť α je redukovaná kvadratická iracionalita,tvaru (1.19), kořen polynomu ax^2+bx+c, kde $u = -b$, $v = 2a$, $N = b^2 - 4ac$. Potom $a\alpha^2 + b\alpha + c = 0$. Dosadíme $\alpha = a_0 + \dfrac{1}{\alpha_1}$ a po úpravě dostaneme:

$$\alpha_1^2(aa_0^2 + ba_0 + c) + \alpha_1(2aa_0 + b) + a = 0.$$

Tedy α_1 je algebraické číslo stupně 2. Nyní spočítáme diskriminant příslušné kvadratické rovnice: $(2aa_0+b)^2-4a(aa_0^2+ba_0+c)=b^2-4ac=N$, tedy diskriminant je stejný jako u rovnice, která vyhovuje α, což jsme chtěli ukázat. Proto

$$\alpha_1=\frac{-(2aa_0+b)\pm\sqrt{N}}{2(aa_0^2+ba_0+c)}. \tag{1.22}$$

Jelikož $2(aa_0^2+ba_0+c)<0$, tak správná volba znaménka v čitateli bude $-$, proto je potřeba volit $u_1=2aa_0+b$, $v_1=-2(aa_0^2+ba_0+c)$. Nyní stačí ukázat nerovnosti $\alpha_1>1$, $\alpha_1'\in(-1{,}0)$. To však plyne ze vztahu $\alpha=a_0+\dfrac{1}{\alpha_1}$:

Jelikož $\dfrac{1}{\alpha_1}=\alpha-a_0\in(0,1)$, tak jistě $\alpha_1>1$. Nyní stačí ukázat, že $\alpha_1'\in(-1,0)$, ekvivalentně $\dfrac{-1}{\alpha_1'}>1$:

$\dfrac{-1}{\alpha_1'}=a_0-\alpha'>1$, protože $a_0\in\mathbb{N}$ a $\alpha'<0$. Tedy jsme ukázali, že α_1 je redukovaná kvadratická iracionalita a důkaz je hotov. □

Tvrzení 27 nám naznačuje, jakým způsobem se rozvíjí redukovaná kvadratická iracionalita do řetězového zlomku. Jak tento rozvoj opravdu vypadá, si dokážeme v následující větě 28, což bude rovněž opačná implikace k větě 23.

Věta 28. *Nechť α je redukovaná kvadratická iracionalita. Potom řetězový zlomek čísla α je čistě periodický.*

Důkaz. Nejprve se podíváme na posloupnost reálných čísel $\{\alpha_i\}_{i=0}^{\infty}$ z definice 6. Opakovaným použitím tvrzení 27 zjistíme, že každé z těchto α_i jsou redukované kvadratické iracionality, tvaru $\dfrac{u_i+\sqrt{N}}{v_i}$ pro vhodná $u_i,v_i\in\mathbb{N}$. Podle důsledku 26 ovšem platí, že takových α_i je konečně mnoho.

Existuje tedy právě jedna volba indexů k,l, $0\le k<l$ taková, že

$\alpha_0,\alpha_1,\ldots,\alpha_k,\ldots,\alpha_{l-1}$ jsou po dvou různá, a navíc $\alpha_l=\alpha_k$ (značení odpovídá definici periodického řetězového zlomku 7). Matematickou indukcí se poté snadno ukáže, že $\forall i\in\mathbb{N}$, $\alpha_{k+i}=\alpha_{l+i}$. Dále platí pochopitelně vztah $\alpha_i=\alpha_j\implies a_i=a_j$ pro libovolná i,j, čímž jsme ukázali, že $[a_0{,}a_1,\ldots,a_{k-1},\overline{a_k,a_{k+1},\ldots,a_{l-1}}]$, tedy řetězový zlomek čísla α je od nějakého místa periodický. Nyní zbývá ukázat, že $k=0$, tedy že jde o čistě periodický řetězový zlomek. To ukážeme sporem:

Ukážeme, že $\alpha_k=\alpha_l$ implikuje $\alpha_{k-1}=\alpha_{l-1}$, čímž bychom pro $k>0$ dostali spor s tím, že $\alpha_0,\alpha_1,\ldots,\alpha_k,\ldots,\alpha_{l-1}$ jsou po dvou různá. Pro větší přehlednost si označíme $\beta_i=\dfrac{-1}{\alpha_i'}$, podobné značení jako ve větě 23. Upravujme:

$$\begin{aligned}
\alpha_{k-1}&=a_{k-1}+\frac{1}{\alpha_k} & \qquad \alpha_{l-1}&=a_{l-1}+\frac{1}{\alpha_l}\\
\alpha_{k-1}'&=a_{k-1}-\beta_k & \qquad \alpha_{l-1}'&=a_{l-1}-\beta_l\\
\beta_k&=a_{k-1}+\frac{1}{\beta_{k-1}} & \qquad \beta_l&=a_{l-1}+\frac{1}{\beta_{l-1}}
\end{aligned}$$

Z rovnosti $\alpha_k = \alpha_l$ okamžitě plyne $\beta_k = \beta_l$. Z toho, že α_{k-1} je redukovaná kvadratická iracionalita plyne, že $\dfrac{1}{\beta_{k-1}} \in (0,1)$, a tak $\lfloor \beta_k \rfloor = a_{k-1}$, analogicky $\lfloor \beta_l \rfloor = a_{l-1}$. Z toho dostáváme, že $a_{k-1} = a_{l-1}$, z čehož dále snadno plyne požadovaná rovnost $\alpha_{k-1} = \alpha_{l-1}$, a proto nutně $k = 0$ a řetězový zlomek čísla α je čistě periodický, což jsme chtěli ukázat. □

Právě jsme ukázali, že právě redukované kvadratické iracionality mají čistě periodický řetězový zlomek s kladným prvním koeficientem. Prvním důsledkem této ekvivalence je charakterizace všech periodických řetězových zlomků, kterou v této práci dokazovat nebudeme.

Věta 29. *Reálné číslo α je algebraické číslo stupně 2, právě když řetězový zlomek čísla α je periodický.*

Důkaz. Jedna implikace je dokázána v učebnici C. D. Oldse [5] v sekci 4.6, druhá ve skriptech [3] ve větě 1.13. □

Dalším důsledkem charakterizace redukovaných kvadratických iracionalit jsou vlastnosti řetězového zlomku pro $\sqrt{N}$, kde N je přirozené číslo, N není čtverec. Tento důsledek je naprosto klíčový pro další vývoj této práce, vlastnosti právě těchto řetězových zlomků budou zkoumány v následujících kapitolách.

2. Řetězové zlomky druhých odmocnin z přirozených čísel

V této kapitole se začneme podrobněji věnovat řetězovým zlomkům z přirozených čísel, které nejsou čtverce.

Po celou práci dále budeme předpokládat, že N je přirozené číslo, které není čtverec (u důležitých vět bude tento předpoklad připomenut). Hlavním předmětem našeho zkoumání bude řetězový zlomek čísla $\sqrt{N}$. Jak vlastně takový řetězový zlomek vypadá, si ukážeme v následující větě:

Věta 30. *Nechť N je přirozené číslo, které není čtverec, ať $\sqrt{N} = [a_0, a_1, a_2, \dots]$. Poté existuje $k \in \mathbb{N}_0$ tak, že $\sqrt{N} = [a_0, \overline{a_1, a_2, \dots, a_k, 2a_0}]$, kde navíc $a_i = a_{k+1-i}$ pro každé $i \in \{1, 2, \dots, k\}$, tedy posloupnost přirozených čísel $(a_1, a_2, \dots, a_k)$ je symetrická.*

Důkaz. Nechť $\sqrt{N} = [a_0, a_1, a_2, \dots]$. Potom jistě $\sqrt{N} + a_0 = [2a_0, a_1, a_2, \dots]$.

$\sqrt{N} + a_0$ je zřejmě redukovaná kvadratická iracionalita, a tak podle věty 28 je řetězový zlomek $[2a_0, a_1, a_2, \dots]$ čistě periodický.

Pokud $\sqrt{N}+a_0 = [\overline{2a_0}]$, poté jednoduchou úpravou dostaneme $\sqrt{N} = [a_0, \overline{2a_0}]$ (toto odpovídá případu $k = 0$) a jsme v tomto případě hotovi.

Pokud existuje $k \in \mathbb{N}$ tak, že $\sqrt{N} + a_0 = [\overline{2a_0, a_1, a_2, \dots, a_k}]$, pak jistě $\sqrt{N} = [a_0, \overline{a_1, a_2, \dots, a_k, 2a_0}]$, zbývá ukázat symetrii posloupnosti $(a_1, a_2, \dots, a_k)$.

Označme $\alpha := a_0 + \sqrt{N}$ a $\beta = \dfrac{1}{-\alpha'}$, poté podle věty 23 platí, že

$$\beta = [\overline{a_k, a_{k-1}, \dots, a_1, 2a_0}]. \tag{2.1}$$

Vztah $\beta = \dfrac{1}{-\alpha'}$ nám však umožní určit řetězový zlomek čísla β i jinak:

$-\alpha' = \sqrt{N} - a_0 = [0, \overline{a_1, a_2, \dots, a_k, 2a_0}] = \dfrac{1}{[\overline{a_1, a_2, \dots, a_k, 2a_0}]}$, z čehož snadno dostáváme

$$\beta = [\overline{a_1, a_2, \dots, a_k, 2a_0}]. \tag{2.2}$$

Rozvoj čísla β do řetězového zlomku je však jednoznačný, a proto porovnáním koeficientů řetězových zlomků u rovností (2.1) a (2.2) dostaneme požadované vztahy $a_i = a_{k+1-i}$ pro každé $i \in \{1, 2, \dots, k\}$, tedy posloupnost $(a_1, a_2, \dots, a_k)$ je symetrická, což jsme chtěli ukázat. □

Nyní si uveďme nějaké příklady, jak hledat symetrické posloupnosti:

Příklad. Pro $k = 0$ je posloupnost $(a_1, a_2, \dots, a_k)$ prázdná a tímto degenerovaným případem se budeme zabývat pouze v sekci 2.1.

Pro $k = 1$ platí, že libovolná jednoprvková posloupnost (a_1), kde $a_1 \in \mathbb{N}$, je symetrická.

Pro $k = 2$ platí, že posloupnost přirozených čísel (a_1, a_2) je symetrická, právě když $a_1 = a_2$.

Pro $k = 3$ dostaneme, že posloupnost přirozených čísel (a_1, a_2, a_3) je symetrická, právě když $a_1 = a_3$.

Pokud je posloupnost přirozených čísel $(a_1, \ldots, a_k)$ symetrická, pro nějaké $k \in \mathbb{N}$, poté využijeme platnost následující identity:

Lemma 31. *Buď $a_0 \in \mathbb{N}$ a symetrická posloupnost přirozených čísel $(a_1, \ldots, a_k)$ pro nějaké $k \in \mathbb{N}$. Potom $p_k = a_0 q_k + q_{k-1}$.*

Důkaz. V tomto důkazu využijeme řetězové polynomy z definice 2 a jejich vlastnosti z lemmatu 3. Pro $k = 1$ je tvrzení zřejmé. Pro $k > 1$ upravujme:

$p_k = k_{k+1}(a_0, \ldots, a_k) = k_{k+1}(a_k, \ldots, a_0) = a_0 k_k(a_k, \ldots, a_1) + k_{k-1}(a_k, \ldots, a_2)$
$= a_0 k_k(a_1, \ldots, a_k) + k_{k-1}(a_1, \ldots, a_{k-1})$,

kde v poslední rovnosti jsme u prvního sčítance použili lemma 3 a u druhého sčítance jsme použili symetrii posloupnosti $(a_1, \ldots, a_k)$.

Platnost vztahu $q_i = k_i(a_1, \ldots, a_i)$, který platí pro každé $i \in \mathbb{N}$, nám pak dokazuje tvrzení. □

Bez předpokladu symetrie posloupnosti $(a_1, \ldots, a_k)$ lemma 31 neplatí. Protipříkladem budiž nesymetrická posloupnost přirozených čísel $(1, 2)$.

Ve větě 30 jsme si odvodili, že pro každé přirozené číslo N, které není čtverec, platí vztah

$$\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}] \tag{2.3}$$

pro nějaké $k \in \mathbb{N}_0$, kde posloupnost $(a_1, a_2, \ldots, a_k)$ je symetrická nebo prázdná $(k = 0)$. Jelikož $a_0 = \lfloor \sqrt{N} \rfloor$, pak má smysl zabývat se otázkou, zda-li pro danou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$ (či prázdnou posloupnost pro případ $k = 0$) existují přirozená N, jejichž $\sqrt{N}$ má právě řetězový zlomek tvaru (2.3).

Skutečnost je taková, že pro danou symetrickou posloupnost tato N buď vůbec neexistují, nebo jich existuje nekonečně mnoho, dokonce bezčtvercových čísel N, což dokázal C. Friesen v článku [2]. Charakterizaci kongruenčních podmínek, závisejících pouze na symetrické posloupnosti $(a_1, a_2, \ldots, a_k)$ a její délce k, si odvodíme v této kapitole. Za jistých předpokladů si pro tuto symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$ vyjádříme všechna N přirozená, pro která platí rovnost (2.3), jako vhodné funkční hodnoty jakéhosi kvadratického polynomu s celočíselnými koeficienty, které závisejí pouze na hodnotách q_k a q_{k-1}, které jsou definované rekurentním vzorcem z definice 4. V závěru práce budeme zkoumat další vlastnosti takto získaných čísel N.

Degenerovanému případu $k = 0$, kdy tato symetrická posloupnost je prázdná, neboli $\sqrt{N} = [a_0, \overline{2a_0}]$ se budeme věnovat zvlášť, a to hned v následující sekci.

2.1 Případ $k = 0$

V této krátké sekci si charakterizujeme všechna N přirozená, pro která platí rovnost

$$\sqrt{N} = [a_0, \overline{2a_0}], \tag{2.4}$$

kde a_0 je dolní celá část čísla $\sqrt{N}$.

Tak tedy mějme takové N přirozené číslo. Poté lze snadno nahlédnout rovnost

$$\sqrt{N} = a_0 + \frac{1}{\sqrt{N} + a_0},$$

což je ekvivalentní vztahu

$$N = a_0^2 + 1. \tag{2.5}$$

Opačně lze též ověřit, že taková čísla tvaru a_0^2+1 mají přesně požadovaný řetězový zlomek, což lze ukázat přímo z definice posloupnosti $\{a_i\}$.

Shrňme si právě získané poznatky do této věty:

Věta 32. *Existuje nekonečně mnoho přirozených čísel N, které nejsou čtverce, takových že platí rovnost* (2.4)*. Taková čísla N jsou navíc právě funkční hodnoty kvadratického polynomu $x^2 + 1$, pro $x = 1, 2, 3, \ldots$.*

Fakt, že takto získaná čísla N jsou vhodné funkční hodnoty jakéhosi kvadratického polynomu, platí obecně pro libovolnou délku periody $k \in \mathbb{N}_0$ a symetrickou posloupnost $(a_1, \ldots, a_k)$, jak se přesvědčíme v sekci 2.2. Také se ovšem může stát, že důkaz popisující konstrukci tohoto polynomu selže, což bude odpovídat tomu, že neexistuje žádné N přirozené, aby platila rovnost (2.3). Konstrukci tohoto polynomu a charakterizaci případů, kdy ten polynom existuje, popíšeme v následující sekci:

2.2 Obecný případ $k \in \mathbb{N}$

V této sekci zobecníme výsledek z minulé sekce 2.1 na libovolné $k \in \mathbb{N}_0$, tedy pro libovolnou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$ přirozených čísel charakterizujeme všechna přirozená čísla N taková, že $\sqrt{N} = [a_0,\overline{a_1, a_2, \ldots, a_k, 2a_0}]$ přesně s touto symetrickou posloupností $(a_1, \ldots, a_k)$, a zda taková čísla N vůbec existují.

2.2.1 Ekvivalentní podmínka k $\sqrt{N} = [a_0,\overline{a_1, a_2, \ldots, a_k, 2a_0}]$

Buďte N, k přirozená čísla a uvažujme symetrickou posloupnost přirozených čísel $(a_1, a_2, \ldots, a_k)$ takové, že platí rovnost $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$

Potom platí též rovnost $\sqrt{N} = [a_0, a_1, \ldots, a_k, \sqrt{N}+a_0]$. Nyní použijeme vztah (1.3) z tvrzení 12 a dostaneme

$$\sqrt{N} = \frac{(\sqrt{N} + a_0)p_k + p_{k-1}}{(\sqrt{N} + a_0)q_k + q_{k-1}}. \tag{2.6}$$

Tuto rovnost lze ekvivalentně přepsat jako

$$Nq_k + \sqrt{N}(a_0q_k + q_{k-1}) = \sqrt{N}p_k + a_0p_k + p_{k-1}. \tag{2.7}$$

Podobným způsobem jakým se dokazovalo lemma 24 si lze rozmyslet, že předchozí rovnost je ekvivalentní tomu, že se rovnají celočíselné části a koeficienty u $\sqrt{N}$ těchto dvou čísel. Tedy dostáváme 2 rovnosti:

$$, p_k = a_0q_k + q_{k-1} \tag{2.8}$$

$$. Nq_k = a_0p_k + p_{k-1} \tag{2.9}$$

I toto tedy byla ekvivalentní úprava. Teď si vezmeme ještě jednu rovnost, která jistě platí, a to díky tvrzení 10 a jednoduché úpravě vzniklého výrazu:

$$p_{k-1} = \frac{p_k q_{k-1} + (-1)^k}{q_k}. \tag{2.10}$$

Rovnost (2.8) jsme již získali v lemmatu 31. Toto nám umožní odvodit klíčovou rovnost, která vznikne tak, že vezmeme rovnost (2.9) a dosadíme za p_k, p_{k-1} vztahy (2.8) a (2.10), vzniklý výraz upravíme a dostaneme:

$$(N - a_0^2)q_k - 2a_0 q_{k-1} = \frac{q_{k-1}^2 + (-1)^k}{q_k}. \tag{2.11}$$

Nyní ale není vůbec jasné, že šlo o ekvivalentní úpravu v tom smyslu, že pro každé $a_0 \in \mathbb{N}$ a symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$ z rovnosti (2.11) plyne, že $\sqrt{N}$ má přesně požadovaný tvar řetězového zlomku dle (2.3). K tomu ovšem stačí ukázat, že platí všechny rovnosti od (2.6) až po (2.10). Upozorněme, že v tomto konkrétním případě nedefinujeme posloupnosti $\{p_i\}, \{q_i\}$ jakožto čitatele a jmenovatele nějakých sblížených zlomků, neboť nemáme žádný řetězový zlomek (naopak jej chceme určit). Proto definujeme posloupnosti $\{p_i\}$,$\{q_i\}$ v této úvaze rekurencí, danou v definici 4. S rovností (2.10) není problém, ta plyne z tvrzení 12, stejně jako s rovností (2.8), která přesně plyne z lemmatu 31.

Z rovností (2.8) a (2.10) již lze úpravou rovnosti (2.11) snadno odvodit i rovnost (2.9), což nás přesně zajímalo.

Nicméně platnost rovností (2.8) a (2.9) je ekvivalentní s tím, že platí rovnice (2.7) a ta je ekvivalentní se vztahem (2.6).

Nyní zbývá dojít od vztahu (2.6) zpět k rovnosti (2.3). To znamená, proč z $\sqrt{N} = \dfrac{(\sqrt{N} + a_0)p_k + p_{k-1}}{(\sqrt{N} + a_0)q_k + q_{k-1}}$ plyne $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_k, 2a_0}]$. To však plyne z lemmatu 13 volbou $\alpha = \sqrt{N}$, $\beta = \sqrt{N} + a_0$ a $m = k$. Tedy jsme vskutku odvodili rovnost (2.3), jak jsme si přáli.

Shrňme si aktuálně získané výsledky do této věty:

Věta 33. *Buďte N, k, a_0 přirozená čísla, N není čtverec a uvažme symetrickou posloupnost přirozených čísel $(a_1, a_2, \ldots, a_k)$. Potom $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, právě když platí rovnost* (2.11)*, tedy $(N - a_0^2)q_k - 2a_0 q_{k-1} = \dfrac{q_{k-1}^2 + (-1)^k}{q_k}$.*

Připomeňme, že naším cílem je určit všechna přirozená N taková, že pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, $k \in \mathbb{N}$ platí vztah (2.3). Díky větě 33 stačí ukázat, pro která přirozená N platí rovnost (2.11).

Prvním, naivním přístupem je vyjádřit si číslo N přímo z rovnosti (2.11), což ovšem nevede k ničemu zajímavému, protože dané vyjádření N by záviselo na q_k, q_{k-1}, k, což je v pořádku, ale také by záviselo na a_0, nicméně z věty 33 plyne, že $a_0 = \lfloor \sqrt{N} \rfloor$, což činí toto vyjádření irelevantním.

To znamená, že chceme vyjádřit a_0 jako něco, co závisí pouze na q_k, q_{k-1} a k.

2.2.2 Charakterizace případů, kdy vhodná čísla N existují

Podle důsledku 11 jsou čísla q_k, q_{k-1} nesoudělná. Pak ovšem z rovnosti (2.11)

plyne, že dvojice přirozených čísel $(N - a_0^2, 2a_0)$ je řešením diofantické rovnice

$$xq_k - yq_{k-1} = \frac{q_{k-1}^2 + (-1)^k}{q_k}. \tag{2.12}$$

To je ovšem lineární diofantická rovnice, čili můžeme využít teorii z části 1.2.2. Nějakým řešením diofantické rovnice (2.12) je:

$$x = \frac{(-1)^k z(q_{k-1}^2 + (-1)^k)}{q_k},\ y = (-1)^k z q_{k-1}, \tag{2.13}$$

kde $z := \dfrac{q_{k-1}^2 + (-1)^k}{q_k}$ je pravá strana rovnice (2.12). Všechna řešení této rovnice jsme popsali v rovnosti (1.5) v lemmatu 14, jehož aplikací (a dosazením za z) dostáváme: Pro libovolné $m \in \mathbb{Z}$,

$$N - a_0^2 = \frac{(-1)^k (q_{k-1}^2 + (-1)^k)^2}{q_k^2} + m q_{k-1}, \tag{2.14}$$

$$2a_0 = (-1)^k q_{k-1} \frac{q_{k-1}^2 + (-1)^k}{q_k} + m q_k. \tag{2.15}$$

Tady však ztrácíme kontrolu nad znaménkem a celočíselností a_0. V předpokladech věty 33 máme $a_0 \in \mathbb{N}$, což však z rovnosti (2.15) není zaručené. V prvé řadě požadujeme $a_0 > 0$, což lze zajistit tím, že si množinu vhodných celočíselných m zdola omezíme, neboť pro některá m záporná se jistě stane $a_0 < 0$. Pojďme si vhodná m specifikovat dle rovnice (2.15):

$$2a_0 = (-1)^k q_{k-1} \frac{q_{k-1}^2 + (-1)^k}{q_k} + m q_k = \frac{1}{q_k}\left((-1)^k q_{k-1}(q_{k-1}^2 + (-1)^k) + m q_k^2 \right).$$

Protože $q_k > 0$, tak jistě stačí volit právě taková $m \in \mathbb{Z}$, pro která platí nerovnost

$$m q_k^2 > (-1)^{k-1} q_{k-1}(q_{k-1}^2 + (-1)^k). \tag{2.16}$$

Pokud označíme m_0 nejmenší $m \in \mathbb{Z}$, které vyhovuje nerovnosti (2.16), potom všechna taková vhodná m lze zřejmě charakterizovat vztahem $m \geq m_0$.

Právě zde došlo k částečnému zjednodušení důkazu C. Friesena z článku [2]. C. Friesen totiž tvrdí, že z odhadu (2.16) plynou nerovnosti $2a_0 \geq N - a_0^2 > 0$, což je sice pravda, nicméně ověření těchto dvou nerovností je relativně pracné. Z těchto dvou nerovností snadno plyne, že pokud $a_0 \in \mathbb{Z}$ (což ověříme později), tak nutně $a_0 = \lfloor \sqrt{N} \rfloor$. Nicméně v naší práci z věty 33 plyne, že stačí zajistit $a_0 \in \mathbb{N}$, z toho již plyne $a_0 = \lfloor \sqrt{N} \rfloor$. Proto není potřeba ověřovat nerovnosti $2a_0 \geq N - a_0^2 > 0$, ale stačí vztah $a_0 > 0$, který je o dost jednodušší a výše jsme jej ověřili.

Nyní je tedy zajištěné $a_0 > 0$. Ovšem dále ještě potřebujeme zkontrolovat, aby a_0 bylo vůbec celočíselné. To zajistíme tak, že ověříme, pro která $m \in \mathbb{Z}$, která vyhovují vztahu (2.16), současně potvrdí, aby pravá strana rovnosti (2.15) byla sudá, tedy

$$(-1)^k q_{k-1} \frac{q_{k-1}^2 + (-1)^k}{q_k} + m q_k \text{ je sudé.} \tag{2.17}$$

V tuto chvíli je třeba odlišit několik případů podle parity čísel q_{k-1}, q_k a

$\frac{q_{k-1}^2+(-1)^k}{q_k}$: Tyto případy budeme odlišovat až do konce této práce a budeme se držet jejich značení „Případ i“ pro $i = 1,2,3,4$.

1. q_{k-1} je sudé. Potom z nesoudělnosti čísel q_{k-1} a q_k plyne, že q_k je nutně liché, což znamená, že (2.17) platí, právě když je m sudé a vyhovuje (2.16).

2. q_{k-1} je liché, q_k je liché. Poté snadno nahlédneme, že zlomek $\frac{q_{k-1}^2+(-1)^k}{q_k}$ je nutně sudý, a tak (2.17) platí, právě když je m sudé a vyhovuje (2.16).

3. q_{k-1} je liché, q_k je sudé a $\frac{q_{k-1}^2+(-1)^k}{q_k}$ je sudé.V tomto případě dokonce platí, že libovolné m vyhovující (2.16) zajišťuje platnost (2.17).

4. q_{k-1} je liché, q_k je sudé a $\frac{q_{k-1}^2+(-1)^k}{q_k}$ je liché. V tomto případě bude pravá strana rovnosti (2.15) pro libovolné $m \in \mathbb{Z}$ lichá, a tak (2.17) nebude platit nikdy.

   Jiný případ zjevně nastat nemůže.

Pojďme si shrnout tuto diskuzi o paritách čísel q_{k-1}, q_k a $\frac{q_{k-1}^2+(-1)^k}{q_k}$ do tabulky, přičemž se nadále budeme držet značení $z := \frac{q_{k-1}^2+(-1)^k}{q_k}$:

číslo případu	q_{k-1}	q_k	z	vhodná m vyhovující (2.16)
1	sudé	liché	liché	sudá
2	liché	liché	sudé	sudá
3	liché	sudé	sudé	libovolná
4	liché	sudé	liché	žádná

Volba vhodných m nám tedy zajistí, aby z rovnosti (2.15) vyplynulo, že $a_0 \in \mathbb{N}$, či pro případ, kdy z i q_{k-1} jsou lichá, jsme se přesvědčili o tom, že z rovnosti (2.15) plyne, že a_0 nikdy přirozené nebude. Spolu s použitím věty 33 jsme tak odvodili tuto další ekvivalentní podmínku k původní rovnosti (2.3), která se zároveň ukáže být charakterizací případů, pro jakou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$ existuje N přirozené, vyhovující rovnosti (2.3), tedy $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$.

Popišme si právě odvozené výsledky v následující větě:

Věta 34. *Buďte N, k, a_0 přirozená čísla, N není čtverec a uvažujme symetrickou posloupnost přirozených čísel $(a_1, a_2, \ldots, a_k)$. Potom rovnost* (2.3)*, čili $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$ je ekvivalentní s rovnostmi* (2.14) *a* (2.15)*, tedy po označení $z := \frac{q_{k-1}^2+(-1)^k}{q_k}$ se vztahy:*

$$N - a_0^2 = (-1)^k z^2 + m q_{k-1}, m \in \mathbb{Z} \tag{2.18}$$

$$2a_0 = (-1)^k q_{k-1} z + m q_k, m \in \mathbb{Z}. \tag{2.19}$$

Navíc, výroky na obou stranách ekvivalence platí, právě když nastane jeden z případů $1, 2, 3$ *dle diskuze shrnuté v tabulce výše, tedy zda-li buď* q_{k-1}*, nebo* z *jsou sudá,* m *vyhovuje odhadu* (2.16) *a pro případy 1, 2 je navíc* m *sudé.*

Pro případ 4*, ani jeden z výroků na obou stranách ekvivalence neplatí.*

Připomeňme, že pokud chceme-li se ujistit, který z případů 1, 2, 3, 4 nastane, tak se postačí podívat na příslušnou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$, z té odvodíme hodnotu q_{k-1} i z, speciálně zjistíme jejich paritu.

Současně jsme zjistili, že pokud q_{k-1} i z jsou lichá, tak neexistuje žádné N přirozené, které splňuje rovnost (2.3). V ostatních případech jsme již jen krůček od vyjádření čísla N jakožto něčeho, co závisí pouze na q_{k-1}, q_k a k, neboť si budeme moci takto vyjádřit a_0 z rovnosti (2.19) a poté bude stačit dosadit do vztahu (2.18). Tyto výsledky si odvodíme v následující části:.

2.2.3 Samotné určení kvadratického polynomu

V této části dokončíme náš úkol, tedy pro danou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$ popsat všechna čísla N přirozená s řetězovým zlomkem $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, jakožto vhodné funkční hodnoty kvadratického polynomu s celočíselnými koeficienty, které závisejí pouze na posloupnosti $(a_1, a_2, \ldots, a_k)$, tedy zobecnit případ $k = 0$ ze sekce 2.1 i pro libovolné $k \in \mathbb{N}$, to vše za předpokladu, že q_{k-1} či z je sudé (což odpovídá případům 1, 2, 3 z diskuze v minulé části). Nejprve se budeme věnovat zvlášť případu 3 (q_{k-1} liché, q_k a z sudé) a poté najednou vyšetříme případy 1 (q_{k-1} sudé, q_k i z lichá) a 2 (q_{k-1} i q_k liché, z sudé), neboť se v nich bude postupovat zcela analogicky. Jak jsme již avizovali, budeme vycházet z rovností (2.19) a (2.18), což motivuje k tomu, proč zkoumat případ 3 zvlášť. V případě 3 je m libovolné, zatímco v případech 1, 2 musí být m sudé. Současně v každém z případů 1, 2, 3 musí být m dostatečně velké, tato podmínka je popsána nerovností (2.16).

Případ 3: Nechť $(a_1, a_2, \ldots, a_k)$ je symetrická posloupnost přirozených čísel taková, že q_{k-1} je liché, z i q_k jsou sudá. Přeznačíme $x := m$, obdobně přeznačíme $x_0 := m_0$, kde m_0 bylo to nejmenší m, vyhovující odhadu (2.16). V tomto případě je tedy $x \in \mathbb{Z}$ takové, že $x \geq x_0$. Vydělením obou stran rovnice (2.19) dvěma dostaneme:

$$a_0 = (-1)^k q_{k-1}\frac{z}{2} + x\frac{q_k}{2},$$

a tedy

$$a_0^2 = q_{k-1}^2\frac{z^2}{4} + (-1)^k q_{k-1} z\frac{q_k}{2}x + \frac{q_k^2}{4}x^2. \tag{2.20}$$

Dosazením rovnosti (2.20) do rovnice (2.18) a drobné úpravě dostáváme:

$$N = \frac{q_k^2}{4}x^2 + q_{k-1}\frac{3 + (-1)^k q_{k-1}^2}{2}x + \frac{z^2}{4}(4(-1)^k + q_{k-1}^2), \tag{2.21}$$

kde $x \in \mathbb{Z}$, $x \geq x_0$. To je kvadratický polynom $e_1x^2 + f_1x + g_1$, kde

$$e_1 = \frac{q_k^2}{4},\ f_1 = q_{k-1}\frac{3 + (-1)^k q_{k-1}^2}{2},\ g_1 = \frac{z^2}{4}(4(-1)^k + q_{k-1}^2), \tag{2.22}$$

což jsme chtěli odvodit.

Dá se ukázat, že tento případ 3 může nastat jedině tehdy, pokud je k liché. K tomu je potřeba spočítat diskriminant polynomu (2.21), který vyjde $(-1)^{k-1}$, čili $b_1^2 - 4a_1c_1 = (-1)^{k-1}$. Z toho plyne $b_1^2 \equiv (-1)^{k-1} \bmod 4$. Nicméně, žádný čtverec nemůže být kongruentní -1 modulo 4, proto k nemůže být sudé.

Případy 1, 2: Nyní předpokládejme, že máme takovou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$, že buď je q_{k-1} sudé, nebo je q_{k-1} liché, ale zároveň je i q_k liché. V těchto případech musí být vhodná m nejen dostatečně velká, ale i sudá, a tak označme $x := \frac{m}{2}$, $x_0 := \frac{m_0}{2}$, kde opět m_0 je to nejmenší m vyhovující odhadu (2.16). Postupujme obdobně jako u případu 3 výše, vydělme obě strany rovnice (2.19) dvěma:

$$a_0 = (-1)^k q_{k-1}\frac{z}{2} + xq_k,$$

a tedy

$$a_0^2 = q_{k-1}^2\frac{z^2}{4} + (-1)^k q_{k-1} z q_k x + q_k^2 x^2. \tag{2.23}$$

Opět dosadíme (2.23) do rovnice (2.18) a po drobné úpravě dostáváme:

$$N = q_k^2 x^2 + q_{k-1}(3 + (-1)^k q_{k-1}^2)x + \frac{z^2}{4}(4(-1)^k + q_{k-1}^2), \tag{2.24}$$

kde $x \in \mathbb{Z}$, $x \geq x_0$. To je kvadratický polynom $e_2x^2 + f_2x + g_2$, kde

$$e_2 = q_k^2,\ f_2 = q_{k-1}(3 + (-1)^k q_{k-1}^2),\ g_2 = \frac{z^2}{4}(4(-1)^k + q_{k-1}^2), \tag{2.25}$$

což nás přesně zajímalo. Dále si všimneme, že platí

$$4e_1 = e_2,\ 2f_1 = f_2,\ g_1 = g_2. \tag{2.26}$$

Dále, v rámci lineárního členu těchto polynomů je vhodné občas využít tento vztah, který plyne snadno z definice z:

$$3 + (-1)^k q_{k-1}^2 = 2 + (-1)^k z q_k. \tag{2.27}$$

Přesně tímto způsobem jsme zobecnili výsledek ze sekce 2.1 pro libovolné $k \in \mathbb{N}$, popsali jsme všechna čísla N přirozená s řetězovým zlomkem

$$\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}],$$

kde $a_0 = \lfloor\sqrt{N}\rfloor$ a $(a_1, a_2, \ldots, a_k)$ je symetrická posloupnost přirozených čísel, jako vhodné funkční hodnoty kvadratického polynomu s celočíselnými koeficienty, závisejícími pouze na q_{k-1},q_k a k, tedy závisejícími pouze na symetrické posloupnosti $(a_1, a_2, \ldots, a_k)$ v dostatečně velkých celých číslech.

Shrňme si výsledky celé této kapitoly, co jsme vlastně odvodili, do následující shrnující věty, kde budeme nadále používat značení $z := \frac{q_{k-1}^2 + (-1)^k}{q_k}$. Po tomto označení si povšimneme, že odhad (2.16), popisující dolní mez pro vhodná m, lze ekvivalentně přepsat takto:

$$mq_k > (-1)^{k-1} z q_{k-1} \tag{2.28}$$

Současně připomeňme, že z posloupnosti $\{a_i\}_{i=1}^k$ definujeme posloupnost $\{q_i\}_{i=1}^k$ rekurentně tak, jak je popsáno v definici 4.

Věta 35. *Mějme čísla N, a_0, k přirozená, N není čtverec a uvažujme symetrickou posloupnost přirozených čísel $(a_1, a_2, \ldots, a_k)$. Potom platí:*

1. *Pokud je q_{k-1} sudé (případ 1) nebo je q_{k-1} i q_k liché a zároveň z sudé (případ 2), tak $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, právě když platí* (2.24) *pro $x \geq x_0 = \dfrac{m_0}{2}$, kde m_0 je to nejmenší m vyhovující odhadu* (2.28).

2. *Pokud je q_{k-1} liché a současně jsou obě čísla q_k i z sudá (případ 3), tak $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, právě když platí* (2.21) *pro $x \geq x_0 = m_0$, kde m_0 je to nejmenší m vyhovující odhadu* (2.28).

3. *V případě 4, tedy q_{k-1} i z jsou lichá, neexistuje žádné číslo N přirozené, které vyhovuje vztahu $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$.*

Na závěr kapitoly aplikujme tuto větu na dva jednoduché příklady:

Příklad. Nejprve uvažujme jednoprvkovou symetrickou posloupnost $a_1 = 1$. Potom $k = q_{k-1} = q_k = 1$, $z = 0$. Vidíme, že zde se jedná o případ 2, tedy podle věty 35 po dosazení do (2.24) a (2.28) pro každé $N \in \mathbb{N}$ je $\sqrt{N} = [a_0, \overline{1, 2a_0}]$, kde $a_0 = \lfloor \sqrt{N} \rfloor$, právě když platí $N = x^2 + 2x$ pro $x \geq x_0 = \dfrac{m_0}{2}$, kde m_0 je to nejmenší sudé m vyhovující vztahu (2.28). Vidíme, že v tomto příkladu je $m_0 = 2$, tedy volíme právě $x \in \mathbb{N}$. Vskutku lze i přímým výpočtem ověřit rovnost, že pro každé $x \in \mathbb{N}$ je $[x, \overline{1, 2x}] = \sqrt{x(x+2)}$.

Obecně lze říct, že volba $k = 1$, tedy posloupnost $(a_1, \ldots, a_k)$ je jednoprvková, nám zajistí, že nastane právě jeden z případů 2, 3, protože potom je $q_{k-1} = 1$ liché a zároveň $z = 0$ je sudé. Zda-li nastane případ 2, nebo 3, záleží na paritě $q_k = a_1$. Lichá q_k dají případ 2, sudá q_k dají případ 3.

Příklad. Nyní uvažujme opět symetrickou posloupnost samých jedniček, ale dvouprvkovou, tedy nechť $a_1 = a_2 = 1$. Potom $k = q_k = 2$, $z = q_{k-1} = 1$. Vidíme, že jsme narazili na případ 4, proto dle věty 35 platí, že neexistuje žádné číslo N přirozené, vyhovující vztahu $\sqrt{N} = [a_0, \overline{1, 1, 2a_0}]$, kde $a_0 = \lfloor \sqrt{N} \rfloor$. Dokonce lze přímým výpočtem relativně snadno ukázat, že pro libovolné $x \in \mathbb{N}$ platí $[x, \overline{1, 1, 2x}] = \dfrac{\sqrt{4x^2 + 4x + 2}}{2}$, což je typické cvičení pro předmět Teorie čísel a RSA.

C. Friesen dále ve svém článku [2] ukázal, že pro danou symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$, pro kterou je q_{k-1} nebo z sudé (tedy nastane jeden z případů 1, 2 nebo 3), existuje nekonečně mnoho dokonce bezčtvercových přirozených čísel N, pro která platí rovnost (2.3). V této kapitole jsme dokázali o něco slabší tvrzení. Netvrdíme totiž nic o tom, zda nalezená čísla N z věty 35 jsou bezčtvercová. Připomeňme, že bezčtvercové číslo jsme si zadefinovali v definici 17.

3. Zkoumání hodnot čísel N modulo prvočísla

V poslední kapitole této práce se pokusíme odvodit nějaké důsledky výsledků z druhé kapitoly této práce. Budeme vycházet z věty 35, pomocí které jsme si pro danou symetrickou posloupnost přirozených čísel $(a_1, a_2, \ldots, a_k)$ charakterizovali všechna čísla N přirozená, pro která platí $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, případně jsme ukázali neexistenci takových čísel N. Zároveň jsme tato čísla N, pokud existují, popsali jako vhodné funkční hodnoty jakéhosi kvadratického polynomu s celočíselnými koeficienty, které závisí pouze na volbě symetrické posloupnosti $(a_1, a_2, \ldots, a_k)$, přičemž pouze na základě této posloupnosti jsme též schopni rozhodnout o (ne)existenci takových přirozených N.

Konkrétně se budeme zabývat otázkou, jaké další podmínky musíme klást na symetrickou posloupnost $(a_1, a_2, \ldots, a_k)$, aby pro dané p prvočíslo a libovolné $l \in \mathbb{Z}_p$ měla kongruence $N \equiv l \bmod p$ nekonečně mnoho řešení N získaných z věty 35. To je ekvivalentní zkoumání, kdy kvadratické polynomy (2.21) a (2.24) tvoří bijekci nad konečným tělesem $\mathbb{Z}_p$, k čemuž stačí ověřit, že jde o prosté zobrazení (jedná se totiž o zobrazení mezi konečnými množinami stejné velikosti). V části 1.2.3 jsme si charakterizovali, kdy je kvadratická funkce nad tělesem $\mathbb{Z}_p$ prostá, čehož v této kapitole budeme využívat (konkrétně se jedná o tvrzení 16).

Již v části 1.2.3 jsme si všimli, že je potřeba řešit případ $p = 2$ zvlášť, a stejně tak budeme postupovat i nadále.

Ještě předtím si připomeneme, jak tyto polynomy, jejichž prostotu nad p-prvkovými tělesy budeme zkoumat, vypadají. Jejich odvození je závěrem druhé kapitoly této práce.

V případě 1 (q_{k-1} sudé, q_k i z liché) a v případě 2 (q_{k-1} i q_k liché, z sudé), vypadá příslušný polynom takto:

$$N = q_k^2 x^2 + q_{k-1}(3 + (-1)^k q_{k-1}^2)x + \frac{z^2}{4}\left(4(-1)^k + q_{k-1}^2\right).$$

V případě 3 (q_{k-1} liché, q_k i z sudé) vypadá příslušný polynom takto:

$$N = \frac{q_k^2}{4} x^2 + q_{k-1}\frac{3 + (-1)^k q_{k-1}^2}{2} x + \frac{z^2}{4}\left(4(-1)^k + q_{k-1}^2\right).$$

3.1 Hodnoty čísel N modulo 2

Začneme degenerovaným případem, který je třeba prozkoumat zvlášť, a sice zkoumat koeficienty výše zmíněných polynomů v tělese $\mathbb{Z}_2$, tedy zkoumat jejich paritu v $\mathbb{Z}$. Z tvrzení 16 plyne, že daný polynom je prostá funkce (tedy bijekce), právě když mají koeficienty u kvadratického a lineárního členu různou paritu, neboli jsou různé v $\mathbb{Z}_2$. Je patrné, že parita těchto koeficientů bude záviset právě na paritě q_k, q_{k-1} a dokonce i z, z čehož plyne, že bude třeba prozkoumat každý z případů 1, 2, 3 zvlášť, neboť tyto případy se liší právě v paritách těchto hodnot.

3.1.1 Případ 1

Uvažme, že nastane případ 1, tedy mějme takovou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, že q_{k-1} je sudé a hodnoty q_k a z jsou liché. V tomto případě vidíme, že příslušný kvadratický polynom, jehož vhodné funkční hodnoty dají požadovaná čísla N, je následující:

$$N = q_k^2 x^2 + q_{k-1}(3 + (-1)^k q_{k-1}^2)x + z^2\left((-1)^k + \frac{q_{k-1}^2}{4}\right).$$

Vidíme, že kvadratický člen tohoto polynomu q_k^2 je lichý, protože q_k je liché. Lineární člen je $q_{k-1}(3 + (-1)^k q_{k-1}^2)$ a vidíme, že zde se jedná o součin sudého (q_{k-1}) a lichého $(3 + (-1)^k q_{k-1}^2)$ čísla, tedy lineární člen je sudý. Proto mají kvadratický a lineární člen v tomto případě různou paritu, a proto podle tvrzení 16 určuje tento polynom bijekci $\mathbb{Z}_2 \to \mathbb{Z}_2$, kdykoliv nastane případ 1.

3.1.2 Případ 2

Nyní předpokládejme, že nastane případ 2, tedy pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$ platí, že hodnoty q_{k-1} i q_k jsou liché, zatímco z je sudé. Příslušný kvadratický polynom, vyjadřující vhodná čísla N, je tento:

$$N = q_k^2 x^2 + q_{k-1}(3 + (-1)^k q_{k-1}^2)x + \frac{z^2}{4}(4(-1)^k + q_{k-1}^2).$$

Nyní bude následovat obdobná diskuze jako u případu 1. Kvadratický člen q_k^2 je opět lichý, neboť q_k je liché, a lineární člen je opět sudý, protože jde o součin sudého $(3 + (-1)^k q_{k-1}^2)$ a lichého (q_{k-1}) čísla. Tvrzení 16 nám tedy i v tomto případě 2 říká, že tento kvadratický polynom určuje bijekci $\mathbb{Z}_2 \to \mathbb{Z}_2$.

3.1.3 Případ 3

Pokud nastane případ 3, tedy pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$ platí, že q_{k-1} je liché, a hodnoty q_k a z jsou sudé, tak bude diskuze o koeficientech odpovídajícího polynomu složitější. Kvadratický polynom vypadá takto (využijeme vztahu (2.27) pro lineární člen):

$$N = \frac{q_k^2}{4}x^2 + q_{k-1}\frac{2 + (-1)^k z q_k}{2}x + \frac{z^2}{4}(4(-1)^k + q_{k-1}^2).$$

Začneme diskuzí o lineárním členu. Jde o součin lichého čísla q_{k-1} a jistého zlomku. Čitatel tohoto zlomku $2 + (-1)^k z q_k$, bude jistě kongruentní 2 modulo 4, protože z i q_k jsou sudá. Pokud takové číslo vydělíme dvěma, dostaneme liché číslo. Proto je lineární člen součin dvou lichých čísel, tedy je lineární člen lichý.

Co se týká parity kvadratického členu $\frac{q_k^2}{4}$, zde nezbývá nic jiného než odlišit dva případy, a sice zda je sudé q_k kongruentní 0, či 2 modulo 4. Snadno nahlédneme, že je-li $q_k \equiv 0 \bmod 4$, tak je kvadratický člen sudý, a pokud $q_k \equiv 2 \bmod 4$, tak je kvadratický člen lichý. To ovšem znamená, podle tvrzení 16, že v případě $q_k \equiv 0 \bmod 4$ tvoří tento polynom bijekci $\mathbb{Z}_2 \to \mathbb{Z}_2$, ale v případě $q_k \equiv 2 \bmod 4$ nikoliv.

Shrňme si výsledky odvozené v této kapitole do následující věty:

Věta 36. *Uvažujme všechna čísla N přirozená, která mají tvar podle věty 35. Potom pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, pro kterou nenastane případ 4, existuje nekonečně mnoho lichých, a zároveň nekonečně mnoho sudých čísel N, právě když nastane případ 1,2, nebo $q_k \equiv 0 \bmod 4$.*

Odpověď na otázku, zda při případu 3, a zároveň $q_k \equiv 2 \bmod 4$ budou nalezená N pouze sudá, či lichá, bude záviset na paritě absolutního členu. Relativně snadno lze nahlédnout, že v tomto případě parita všech takto získaných čísel N bude rovna paritě výrazu $\frac{z^2}{4}$, tedy $N = \frac{z^2}{4}$ v tělese $\mathbb{Z}_2$ pro všechna takto získaná N.

Již v příkladech na konci druhé kapitoly jsme ukázali, jakým způsobem lze jednoduše konstruovat příklady symetrických posloupností, pro které nastane případ 3. Stačí volit jednoprvkovou posloupnost (tedy $k = 1$) a její jediný člen ať je sudý, tedy nechť $a_1 = q_k$ je sudé. Pak jistě nastane případ 3, což demonstrujeme na těchto dvou příkladech:

Příklad. Uvažme symetrickou posloupnost (2). Podle věty 35 potom pro všechna čísla N přirozená, pro která platí $\sqrt{N} = [a_0, \overline{2, 2a_0}]$, platí $N = x^2 + x$ pro nějaké $x \in \mathbb{N}$. V tomto případě, $q_k \equiv 2 \bmod 4$, a tak podle věty 36 $x^2 + x$ není bijekce $\mathbb{Z}_2 \to \mathbb{Z}_2$, což lze velice snadno ověřit.

Příklad. Nyní uvažme symetrickou posloupnost (4). Opět nastane případ 3, a jelikož $q_k \equiv 0 \bmod 4$, tak podle věty 36 bude příslušný polynom z věty 35 bijekce $\mathbb{Z}_2 \to \mathbb{Z}_2$. Tento polynom je $4x^2 + x$, což vskutku bijekce $\mathbb{Z}_2 \to \mathbb{Z}_2$ je.

3.2 Hodnoty čísel N modulo lichá prvočísla

Nyní se budeme věnovat na první pohled obecnějšímu, ale přitom méně pracnému případu vyšetřování prostoty polynomů z (2.21) a (2.24), a sice nad tělesem $\mathbb{Z}_p$, kde p je liché prvočíslo. Tato situace bude pro nás příjemnější z toho důvodu, že nebudeme muset odlišovat případy 1, 2, 3 jako v sekci 3.1, kde jsme totéž dělali modulo 2.

V první řadě nahlédneme, že samotná parita čísel q_{k-1}, q_k a z neukazuje na nic z toho, čemu budou tyto hodnoty rovno modulo nějaké liché prvočíslo p. Komplikací by mohlo být, že polynom v případě 3 se lehce liší od polynomů v případech 1, 2. V rovnosti (2.26) jsme si všimli, že se tyto polynomy pouze liší v kvadratickém členu o $4-$násobek a v lineárním členu o $2-$násobek. Podle tvrzení 16 však platí, že takový polynom tvoří bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$, právě když je kvadratický člen tohoto polynomu nulou v $\mathbb{Z}_p$, a zároveň lineární člen je nenulový v $\mathbb{Z}_p$. Nicméně, p je liché prvočíslo, proto je jak 2, tak 4 nenulový (a tedy invertibilní) prvek v $\mathbb{Z}_p$ a násobení, či dělení takovým číslem nám (ne)nulovost daného koeficientu neovlivní. Z těchto důvodů se stačí zabývat polynomem z (2.24) z případu 1.

Stále platí, že na absolutním členu tohoto polynomu nezáleží. Zkoumáme polynom

$$N = q_k^2 x^2 + q_{k-1}(3 + (-1)^k q_{k-1}^2)x + z^2\left((-1)^k + \frac{q_{k-1}^2}{4}\right),$$

kdy se bude jednat o bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$ pro dané p liché prvočíslo. Chceme určit ekvivalentní kongruenční podmínky na to, aby kvadratický člen toho polynomu byl dělitelný p a lineární člen naopak nebyl dělitelný p.

Kvadratický člen q_k^2 je dělitelný p, právě když je $q_k \equiv 0 \bmod p$, což plyne jednoduše z toho, že p je prvočíslo (a tedy prvočinitel). Pokud jde o lineární člen $q_{k-1}(3+(-1)^k q_{k-1}^2)$, tak potřebujeme zajistit aby čísla q_{k-1} a $(3+(-1)^k q_{k-1}^2$ nebyla dělitelná p. To, že q_{k-1} není dělitelné p, však plyne z toho, že q_k je dělitelné p a důsledku 11, podle kterého jsou čísla q_k a q_{k-1} nesoudělná. Druhá podmínka, tedy $(-1)^k q_{k-1}^2 \not\equiv -3 \bmod p$, není potřeba dále rozvádět.

Použitím tvrzení 16 jsme tedy charakterizovali podmínky pro to, aby polynomy z (2.21) a (2.24) tvořily bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$, a tyto poznatky si shrneme do následující věty.

Věta 37. *Nechť p je liché prvočíslo. Uvažujme všechna čísla N přirozená, která vznikla jako ve větě 35. Potom pro danou symetrickou posloupnost přirozených čísel $(a_1, \ldots, a_k)$, pro kterou nenastane případ 4, takto vznikne nekonečně mnoho čísel N vyhovujících podmínce $N \equiv l \bmod p$ pro každé $l \in \mathbb{Z}_p$, právě když $q_k \equiv 0 \bmod p$, a zároveň $(-1)^k q_{k-1}^2 \not\equiv -3 \bmod p$.*

Na závěr uvedeme ještě 2 jednoduché příklady, na kterých zjistíme, kdy kongruenční podmínky z věty 37 platí, a kdy nikoliv.

Nechť p je liché prvočíslo. Zůstaneme u jednoprvkových posloupností (a_1). Zde tedy platí, že $k = 1$, $q_{k-1} = 1$, $z = 0$ a $q_k = a_1$. Poté zřejmě platí, že $(-1)^k q_{k-1}^2 \not\equiv -3 \bmod p$. Tedy záleží na volbě $q_k = a_1$.

Příklad. Nejprve předpokládejme, že $q_k = p$. Potom $q_k \equiv 0 \bmod p$, a tak podle věty 37 tvoří příslušný polynom bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$. Jelikož $q_k = p$ je liché, tak jde o případ 2, z čehož na základě věty 35 odvodíme, že tento polynom je roven $p^2x^2 + 2x$. Jelikož platí $p^2x^2 + 2x \equiv 2x \bmod p$ pro každé $x \in \mathbb{N}$, tak jsme dostali, že $x \to 2x$ je bijekce $\mathbb{Z}_p \to \mathbb{Z}_p$, což jsme si ostatně ukázali již v tvrzení 16.

Příklad. Nyní naopak předpokládejme, že $q_k = p + 2$. Pak opět nastane případ 2, ale zároveň platí, že $q_k \not\equiv 0 \bmod p$. Proto nám věta 37 říká, že příslušný polynom, kterým je dle věty 35 $(p+2)^2x^2 + 2x$, netvoří bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$. To je pravda, jelikož tento polynom zobrazí různé prvky 0 a -2^{-1} na ten samý prvek v tělese $\mathbb{Z}_p$. Návod, jak tyto prvky nalézt, nám přesně dává důkaz složitější implikace ve tvrzení 16.

Závěr

V této práci byla sepsána potřebná teorie k tomu, abychom byli schopni dokázat symetrii periody u řetězového zlomku druhých odmocnin z přirozených čísel. Dále jsme charakterizovali, pro jaké symetrické posloupnosti přirozených čísel $(a_1, \ldots, a_k)$ existují přirozená čísla N taková, že $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$ a pokud existují, přesně jsme je charakterizovali jako dostatečně velké funkční hodnoty jakéhosi kvadratického polynomu s celočíselnými koeficienty, které závisejí pouze na symetrické posloupnosti $(a_1, \ldots, a_k)$. Navíc jsme popsali další podmínky na posloupnost $(a_1, \ldots, a_k)$, aby tento příslušný polynom tvořil bijekci $\mathbb{Z}_p \to \mathbb{Z}_p$ pro p dané prvočíslo, přičemž tyto podmínky se liší pro $p = 2$ a p liché, ale jinak jsou víceméně stejné. To je ekvivalentní s tím, že jsme popsali takové podmínky na $(a_1, \ldots, a_k)$, aby pro každé p prvočíslo a pro každé $l \in \mathbb{Z}_p$ existovalo nekonečně mnoho čísel N přirozených, pro která platí $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, a zároveň $N \equiv l \bmod p$.

Nabízí se několik otázek, na které tato práce neodpovídá a dalo by se jim věnovat při dalším zkoumání.

Jako nejužitečnější by se patrně ukázalo, kdybychom pro dané p liché prvočíslo a dané $l \in \mathbb{Z}_p$ byli schopni popsat úplně všechny nutné a postačující podmínky na posloupnost $(a_1, \ldots, a_k)$, aby pro nekonečně mnoho čísel N, splňujících $N \equiv l \bmod p$, platilo $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_k, 2a_0}]$, včetně rozebrání případů, kdy příslušný kvadratický polynom, jehož funkční hodnoty generují N, není bijekcí $\mathbb{Z}_p \to \mathbb{Z}_p$. I případ $p = 5$ by mohl být velice zajímavý.

Dále se nabízí nějakým způsobem zjednodušit podmínku $(-1)^k q_{k-1}^2 \not\equiv -3 \bmod p$ z věty 37 pro p liché prvočíslo užitím např. kvadratických zbytků.

Seznam použité literatury

[1] V. Blomer, V. Kala. *Number fields without n-ary universal quadratic forms*. Math. Proc. Cambridge Philos. Soc., 159(2):239-252, 2015.

[2] C. Friesen. *On continued fractions of given period*. Proceedings of the American Mathematical Society, **103** (1988), 9–14.

[3] V. Kala. *Teorie čísel* [online]. Datum poslední revize 23. 06. 2020, [citováno 20. 07. 2020] `http://karlin.mff.cuni.cz/~kala/1920tc/TCskripta.pdf`

[4] V. Kala. *Universal quadratic forms and elements of small norm in real quadratic fields*. Bull. Aust. Math. Soc., 94(1):7-14, 2016.

[5] C. D. Olds. *Continued fractions*. Random House, 1963.

[6] D. Stanovský. *Základy algebry*. První vydání. Praha: Matfyzpress, 2010. ISBN 978-80-7378-105-7.

[7] Wikipedia contributors. *Diophantine equation* [online]. Wikipedia: The Free Encyclopedia, c2019, Datum poslední revize 11. 07. 2020, 14:10 UTC, [citováno 20. 07. 2020] `https://en.wikipedia.org/w/index.php?title=Diophantine_equation&oldid=967160687`