Univerzita Karlova

Pedagogická fakulta

Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Pellova rovnice, řetězové zlomky a diofantické aproximace iracionálních čísel

Pell's equation, continued fractions and Diophantine approximations of irrational numbers

Jakub Kodýtek

Vedoucí práce: JUDr. Mgr. Filip Beran

Studijní program: Specializace v pedagogice

Studijní obor: Anglický jazyk a Matematika se zaměřením na vzdělávání

2023

Odevzdáním této bakalářské práce na téma Pellova rovnice, řetězové zlomky a aproximace iracionálních čísel potvrzuji, že jsem ji vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Praha, 10.7.2023

Tímto bych chtěl poděkovat vedoucímu této práce JUDr. Mgr. Filipu Beranovi za jeho čas, ochotu a věcné rady při psaní této práce. Za velkou podporu bych také chtěl poděkovat mé rodině a přítelkyni.

ABSTRAKT

Tato bakalářská práce pojednává o Pellově rovnici, přičemž srozumitelně podává strukturované informace z prostudovaných tuzemských i zahraničních knih, článků a dalších zdrojů. Cílem práce je vytvořit studijní materiál primárně pro studenty vysokých škol ale také pro zvídavé středoškoláky, a tedy co nejintuitivněji vyložit co je Pellova rovnice, jak najít její řešení a jak souvisí například s řetězovými zlomky, aproximacemi iracionálních čísel, a invertibilními prvky v $\mathbb{Z}[\sqrt{n}]$. Hlavní motivací pro řešení Pellovy rovnice napříč prací je právě to, že její řešení dávají dobré aproximace iracionálních druhých odmocnin. Pellova rovnice je představena v stručném historickém kontextu. Dále je dokázáno, že pro každou Pellovu rovnici existuje netriviální celočíselné řešení, a pro jeho nalezení je využita teorie řetězových zlomků. Pro zjednodušení tvoření řetězových zlomků je představen tzv. Tennerův algoritmus. Konkrétně je hledání řešení Pellovy rovnice odvozeno pomocí sblížených zlomků a periodicity řetězových zlomků iracionálních odmocnin. Následně je popsána struktura řešení: je dokázáno, že existuje tzv. minimální řešení, které generuje všechna kladná řešení, a je popsána množina řešení, která tvoří nekonečnou cyklickou grupu. V závěru práce jsou zmíněna další užití a výskyty Pellovy rovnice, např. tzv. Pellova čísla a jak pomocí nich lze hledat pythagorejské trojice. Tímto jsou podány ucelené informace od odvození přes řešení po užití Pellovy rovnice.

KLÍČOVÁ SLOVA

Pellova rovnice, diofantické aproximace, druhá odmocnina, řetězové zlomky, teorie čísel

ABSTRACT

This bachelor's thesis deals with Pell's equation, while clearly presenting structured information from studied domestic and foreign books, articles, and other sources. The goal of this thesis is to create study material primarily for university students but also for inquisitive high school students, and thus explain as intuitively as possible what Pell's equation is, how to find its solutions, and how it is related, for example, to continued fractions, approximations of irrational numbers, and invertible elements in $Z[\sqrt{n}]$. The main motivation for solving Pell's equation throughout the work is specifically that its solutions give best approximations of irrational square roots. Pell's equation is presented in a brief historical context. Further, it is proved that there is a non-trivial integer solution for every Pell equation, and the theory of continued fractions is used to find it. To make the creation of continued fractions easier, the so-called Tenner's algorithm is introduced. Specifically, the search for a solution to Pell's equation is derived using convergents and the periodicity of continued fractions of irrational roots. Subsequently, the structure of the solution is described: it is proved that there is a so-called minimal solution that generates all positive solutions, and a set of solutions that form an infinite cyclic group is described. At the end of the thesis, other uses and occurrences of the Pell equation are mentioned, e.g. the so-called Pell numbers and how they can be used to search for Pythagorean triples. Thus, comprehensive information is given covering the derivation of the equation, finding its solutions, and its use.

KEYWORDS

Pell’s equation, diophantine approximation, square root, continued fractions, number theory

Obsah

Úvod

Pellova rovnice je předmětem studia matematického oboru známého jako teorie čísel. Jedná se o kvadratickou diofantickou rovnici ve tvaru:

$$x^2 - ny^2 = 1$$

Její význam spočívá především v tom, že pomocí jejích řešení lze velmi dobře aproximovat iracionální odmocniny celých čísel, tj. ty, které nejsou druhou mocninou nějakého celého čísla. Další užití Pellovy rovnice představuje určování invertibilních prvků v číselných oborech $\mathbb{Z}[\sqrt{n}]$, což jsou algebraické struktury tvořené čísly ve tvaru $x + y\sqrt{n}$, kde x a y jsou celá čísla. Invertibilní prvky pak jsou takové, ke kterým existuje inverzní prvek (Stanovský, 2010, s. 20). Zajímavým užitím Pellovy rovnice je hledání čísel, která jsou zároveň čtverci (druhé mocniny celých čísel) a trojúhelníky, což jsou čísla určující počet teček, ze kterých lze sestavit pravidelný rovnostranný trojúhelník. S Pellovou rovnicí také souvisí tzv. Pellova čísla, pomocí kterých lze hledat pythagorejské trojice.

Práce je rozdělena na čtyři kapitoly. První kapitola představuje Pellovu rovnici a uvádí ji v historickém kontextu. V této části je konkrétní Pellova rovnice odvozena z poměru úhlopříčky a strany čtverce jako nástroj pro hledání aproximace $\sqrt{2}$, a následně zobecněna pro hledání aproximací iracionálních odmocnin, což také zůstává její hlavní motivací napříč prací. Tato vlastnost souvisí s několika důkazy a také s řešením pomocí řetězových zlomků.

Druhá kapitola se pak zabývá řetězovými zlomky, pomocí nichž můžeme nalézt libovolné řešení Pellovy rovnice. Nejprve se zde stručně hovoří o řetězových zlomcích racionálních čísel a poté se zbytek kapitoly soustředí na řetězové zlomky iracionálních čísel a jak souvisí s Pellovou rovnicí. Jsou zavedeny tzv. sblížené zlomky, které představují „utnuté“ části řetězových zlomků a je odvozen vztah, určující to, které sblížené zlomky dávají řešení Pellovy rovnice.

Ve třetí kapitole je popsána algebraická struktura, kterou tvoří řešení konkrétní Pellovy rovnice. Je definována množina řešení M a je dokázáno, že splňuje vlastnosti cyklické grupy. Nejdůležitější částí této kapitoly je důkaz, že součinem dvou řešení získáme nové řešení a dále, že všechna kladná řešení jsme schopni generovat tzv. minimálním řešením.

V závěrečné čtvrté kapitole jsou potom zmíněna další využití Pellovy rovnice. Nejprve hledání dalších řešení obecné a negativní Pellovy rovnice, poté hledání invertibilních prvků

v oborech $\mathbb{Z}[\sqrt{n}]$, hledání čísel, která jsou zároveň trojúhelníky a čtverci a v poslední podkapitole této části je představeno, hledat pythagorejské trojice pomocí tzv. Pellových čísel.

V *Elements of Number Theory* Johna Stillwella (2003) se čtenář dočte o dalších zajímavých náhledech na řešení Pellovy rovnice. Další rozšiřující literaturu představují např. Kala (2021), který v textu *Teorie čísel* poskytuje jiný pohled na sblížené zlomky. Hlavním doporučeným textem, pro další čtení je *Pell's Equation* od Edwarda J. Barbeaua, který se věnuje Pellově rovnici z více úhlů a více do hloubky. Pokud by čtenáře zaujaly diofantické aproximace, pak najde další informace např. v diplomové práci Aleny Jaššové (2010) *Diofantické aproximace*.

1 Pellova rovnice a dobré aproximace

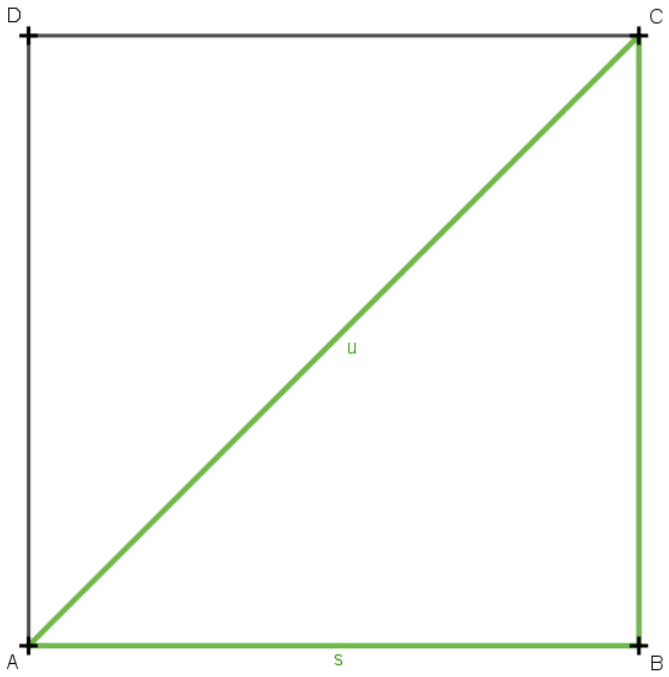
Pellova rovnice je tedy kvadratická diofantická daná předpisem:

$$x^2 - ny^2 = 1$$

Na tuto rovnici lze narazit například při aproximaci iracionální úhlopříčky ve čtverci, či při počítání norem čísel v číselných oborech $\mathbb{Z}[\sqrt{n}]$, kde norma je definována právě jako $|x^2 - ny^2|$, pro dané $x + y\sqrt{n}$.

Touto rovnicí se zabývali už staří Řekové. Mezi velká jména spjatá s Pellovou rovnicí patří Theon ze Smyrny (70-135) nebo Diofantos (3. století n.l.), který se jí zabývá ve svém díle *Arithmetica*. Používali ji především k aproximaci $\sqrt{2}$ a to pomocí tzv. úhlopříčkových a stranových čísel, vztahujících se ke stranám a uhlopříčkám ve čtvercích. (Tattersall, 2005, s. 44)

Už na základních školách se děti učí, že poměr úhlopříčky ve čtverci a jeho strany je právě $\sqrt{2}$. To plyne například z Pythagorovy věty, protože úhlopříčka je přepona v pravoúhlém trojúhelníku, který tvoří spolu se dvěma stranami čtverce.



Obr. 1: Pravoúhlý trojúhelník ve čtverci

(vlastní zpracování, GeoGebra)

Vezměme několik čtverců a pomocí Pythagorovy věty spočtěme jejich úhlopříčky. Mějme čtverce o straně s a úhlopříčce u.

a) $s = 1$. Pak platí, že $1^2 + 1^2 = u^2$a tedy $u = \sqrt{1^2 + 1^2} = \sqrt{2}$

b) $s = 2$. Pak platí, že $2^2 + 2^2 = u^2$ a $u = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2}$

Všimneme si vzorce, že $u = s\sqrt{2}$. To lze odvodit i ze vzorce pro obecný čtverec.

c) Mějme čtverec o nějaké straně s a úhlopříčce u. Platí, že:

$$s^2 + s^2 = u^2$$

$$2s^2 = u^2$$

Z čehož plyne, že $u = \sqrt{2s^2} = s\sqrt{2}$.

Nyní tedy vidíme, že poměr úhlopříčky a strany ve čtverci je skutečně $\sqrt{2}$ a mohli bychom odmocninu ze dvou vyjádřit pomocí $\frac{u}{s}$. Číslo $\sqrt{2}$ je ale iracionální, jak můžeme snadno dokázat.

Tvrzení 1.

$\sqrt{2}$ je iracionální číslo.

Důkaz. Předpokládejme, že $\sqrt{2}$ je racionální, tedy ji můžeme vyjádřit jako zlomek $\frac{p}{q}$, kde p a q jsou nesoudělná celá čísla. Platí, že:

$$\sqrt{2} = \frac{p}{q}$$

$$2q^2 = p^2$$

Z čehož plyne, že p^2 je sudé a tím pádem i p je sudé. Nechť $p = 2m$. Potom $p^2 = 4m^2$. Z toho plyne:

$$2q^2 = 4m^2$$

$$q^2 = 2m^2$$

Číslo q je tedy také sudé, což je ve sporu s předpokladem, že p, q jsou nesoudělná.

(Tattersall, 2009, s. 60) ■

My bychom ale chtěli aby u, s byla čísla celá, a tedy aby $\frac{u}{s}$ bylo racionální. Abychom se zbavili odmocniny ze dvou, umocníme rovnici $\frac{u}{s} = \sqrt{2}$ na druhou. Získáme rovnici $\frac{u^2}{s^2} = 2$. Tento výraz je stále neřešitelný, protože kdyby existovaly dvě druhé mocniny nějakých celých čísel, jejichž podíl je roven dvěma, pak by stačilo obě strany odmocnit a získali bychom podíl celých čísel, který je roven odmocnině ze dvou.

Nelze očekávat, že bychom $\sqrt{2}$ vyjádřili celočíselným podílem přesně. Zkusme proto sestavit rovnici, jejíž řešení budou aproximovat odmocninu ze dvou s co nejmenší chybou. Toho dosáhneme například úpravou umocněné rovnice tak, aby na pravé straně byla nula.

$$\frac{u^2}{s^2} = 2$$

$$u^2 - 2s^2 = 0$$

Z předchozího víme, že tato rovnice nemá řešení v $\mathbb{Z}$. Jelikož uvažujme s, u celá, výsledkem výrazu na pravé straně bude nějaké celé číslo. Když tedy nemůžeme dosáhnout nulového rozdílu, vezměme druhý nejmenší celočíselný rozdíl, tedy ± 1. Nyní řešíme rovnici:

$$u^2 - 2s^2 = \pm 1$$

Na první pohled vidíme, že některá celočíselná řešení existují, například $u = 1, s = 0$ nebo $u = 1, s = 1$ a další.

Obdobnou úvahu lze použít i k aproximaci dalších iracionálních odmocnin. Odpoutejme se tedy od čtverce a značení u, s a označme proměnné obecně x,y. Místo čísla 2 pišme obecně n pro $\sqrt{n}$, kterou chceme aproximovat. Zároveň se prozatím omezme na případ, kdy je pravá strana kladná. Máme tedy $x^2 - ny^2 = 1$. Takové rovnici se říká Pellova, a právě tou se budeme zabývat. Varianta s číslem -1 se nazývá negativní Pellova rovnice, a pokud máme na pravé straně nějaké $c \in \mathbb{Z} \setminus \{0\}$, říkáme takové rovnici obecná Pellova rovnice. Zadefinujme si tedy formálně tyto tři pojmy, ačkoliv zabývat se budeme hlavně Pellovou rovnicí s 1 na pravé straně.

Definice 1. Pellova rovnice

Pellovou rovnicí nazýváme rovnici $x^2 - ny^2 = 1$, kde n je přirozené číslo a zároveň není čtverec, tedy není druhou mocinou žádného celého čísla ($n \in \mathbb{N}, n \neq d^2, d \in \mathbb{N}$). Řešením jsou dvojice $(x; y)$, kde $x, y \in \mathbb{Z}$. (Conrad (a), s. 1)

Poznámka Dále pojmem Pellova rovnice bez dalších přízvisek či specifikací rozumíme právě tuto rovnici.

Definice 2. Negativní Pellova rovnice

Negativní Pellovou rovnicí nazýváme rovnici $x^2 - ny^2 = -1$, kde $n \in \mathbb{N}, n \neq d^2, d \in \mathbb{N}$. (Conrad (a), s. 7)

Tuto rovnici jsme si odvodili na začátku spolu s Pellovou rovnicí. Je jakousi obrácenou stranou mince, protože dává aproximace o něco menší než $\sqrt{n}$, zatímco rovnice s 1 o něco větší. Zároveň je negativní Pellova rovnice speciálním případem obecné.

Definice 3. Obecná Pellova rovnice

Obecnou Pellovou rovnicí nazýváme rovnici $x^2 - ny^2 = c$, kde $n \in \mathbb{N}, n \neq d^2, d \in \mathbb{Z}$ a $c \in \mathbb{Z} \setminus \{0\}$. (Conrad (a), s. 7)

Později si našla Pellova rovnice cestu dále na východ do Indie a Číny. Historické materiály naznačují, že tyto dvě země si vyměňovaly informace ohledně matematických poznatků, ale mnohem větší pokrok učinila Indie, kde Pellovu rovnici zkoumali například Brahmagupta (598-668) nebo Bháskara II. (1114-1185). Ti hledali řešení pro vyšší odmocniny. Brahmagupta sám byl schopen nalézt nekonečně mnoho řešení, protože přišel na to, že součin dvou řešení dává nové řešení. Nebyl ale schopen nalézt řešení pro Pellovy rovnice obecně. K tomu se dobral Bháskara II., ovšem jeho metodu dokázal až Joseph-Loise Lagrange (1736-1813) v 18. století. (Stillwell, 2010, s. 75-76)

Mezi prvními, kdo se v Evropě zabývali Pellovou rovnicí byl například William Brouncker (1620 – 1684). On i další již zakládali své zkoumání na řetězových zlomcích $\sqrt{n}$. (Stillwell, 2010, s. 46) Pozoruhodné je, že přízvisko „Pellova“ dal této rovnici matematik Leonhard Euler (1707 – 1783), který chybně přiřadil zásluhy za studia jejích řešení právě Johnu Pellovi (1611 – 1685). Jak je vidno, studium této rovnice sahá mnohem hlouběji do minulosti a v moderní době se, mnohem více než Pell, jejím řešením zabývali jiní matematici například

William Brouncker, John Wallis (1616-1703) nebo Pierre de Fermat (1607-1665). (Tattersall, 2005, s. 274)

Odvodili jsme tedy Pellovu rovnici přes aproximaci $\sqrt{2}$ jako nástroj pro hledání racionálních čísel $\frac{x}{y}$, pro které platí, že rozdíl $\left|\frac{x}{y} - \sqrt{2}\right|$ je co nejmenší. Dále jsme si rovnici zobecnili, pro různé $\sqrt{n}$, kde n není druhou mocninou nějakého celého čísla $(0, 1, 4, 9, 25, 36, \dots)$. Takovým číslům budeme říkat čtverce a ostatním pak nečtverce, bude-li důležité zdůraznit tuto jejich vlastnost. Teď nás bude zajímat, jak najít řešení Pellovy rovnice. Už v úvodu první kapitoly, kdy jsme řešili aproximaci $\sqrt{2}$, jsme viděli několik řešení na první pohled. Podívejme se na další příklady pro různá n. Schválně zahrneme i rovnice, ve kterých je n čtverec, abychom pochopili, proč se tato n z definice Pellovy rovnice vylučují.

Příklad 1.

Zkuste uhádnout alespoň dvě řešení $(x_1; y_1), (x_2; y_2)$ taková, že $x_1 \neq x_2$ a $y_1 \neq y_2$.

a) $x^2 - y^2 = 1$
b) $x^2 - 2y^2 = 1$
c) $x^2 - 4y^2 = 1$
d) $x^2 - 5y^2 = 1$

Řešení.

a) Zde se jedná o rozdíl dvou čtverců. Jediné dva čtverce, které se liší právě o 1, jsou 0^2 a 1^2 (Jak plyne z posloupnosti čtverců $\{0,1,4,9, \dots\}$). Dostáváme tak pouze dvě řešení $(\pm 1; 0)$.

b) Řešení $(\pm 1; 0)$ platí i pro tuto rovnici. Můžeme si všimnout, že vzhledem k tomu, že $y = 0$ je toto řešení nezávislé na n a tím pádem platí pro všechny Pellovy rovnice. Říkáme mu proto triviální; a zabýváme se případnými dalšími, kterým říkáme netriviální. Můžeme zkusit uhodnout nějaká netriviální řešení, pokud je vidíme. Pokud je nevidíme, můžeme systematicky zkoušet dosazovat, dokud se výsledku nedobereme. Uvažujme následující metodu.

   Vyjádříme x^2 z Pellovy rovnice: $x^2 = 1 + 2y^2$ a poté postupně dosazujeme za y přirozená čísla od 1, protože hledáme y v $\mathbb{Z}$, přičemž nulu neuvažujeme (ta, jak víme, vede na triviální řešení) a vzhledem k druhé mocnině je dosazení například 1 a -1 ekvivalentní. Pokračujeme v dosazování, dokud se pravá strana nerovná nějakému čtverci. Pak jsme našli celočíselné řešení (viz Tab. 1). Hledáme tedy čtverce v posloupnosti čísel tvaru $1 + 2y^2$.

y	$1 + 2y^2 = x^2$
1	3
2	9
3	19
4	33

Tab. 1

(vlastní zpracování)

První čtverec jsme našli už v druhém kroku. Je třeba výsledek odmocnit, protože jsme našli x^2, ne x, a získali jsme nejmenší netriviální řešení $(3; 2)$. Na další řešení bychom narazili pro $y = 12$, další pak až pro $y = 70$ (viz Tab. 3), což vypovídá o tom, jak se tato metoda postupně stává hrubě neefektivní. Zároveň nezaručuje existenci ani počet řešení.

c) V tomto případě je n rovno čtverci, a protože můžeme rovnici upravit následujícím způsobem: $x^2 - (2y)^2 = 1$. Jedná se opět o rozdíl čtverců jako v úloze a), a tedy jediným řešením je triviální řešení $(\pm 1; 0)$.

d) Jako jedno řešení můžeme opět vzít triviální řešení. Abychom našli další můžeme postupovat stejně jako v b). Sestavme následující tabulku:

y	$x^2 = 1 + 5y^2$
1	6
2	21
3	46
4	81

Tab. 2

(vlastní zpracování)

Pro $n = 5$ se první čtverec objevil až ve čtvrtém kroku, nicméně stále relativně brzy a získali jsme řešení $(9; 4)$. Kdybychom chtěli nalézt další netriviální řešení, pokračovali bychom dále, přičemž na další řešení bychom narazili až pro $y = 72$ (viz Tab. 3).

Následující tabulka ilustruje neefektivitu postupného dosazování. Jsou zde uvedena první čtyři řešení, která bychom touto metodou našli. Ta ovšem byla spočtena metodou jinou, konkrétně pomocí vlastnosti, že součin dvou řešení je nové řešení. Tuto vlastnost prozkoumáme ve třetí kapitole.

$x^2 - 2y^2 = 1$	$x^2 - 5y^2 = 1$
$(3; 2)$	$(9; 4)$

$(17; 12)$	$(161; 72)$
$(99; 70)$	$(2889; 1292)$
$(577; 408)$	$(51841; 23184)$

Tab. 3: První čtyři řešení rovnic $x^2 - 2y^2 = 1$ a $x^2 - 5y^2 = 1$.

(vlastní zpracování)

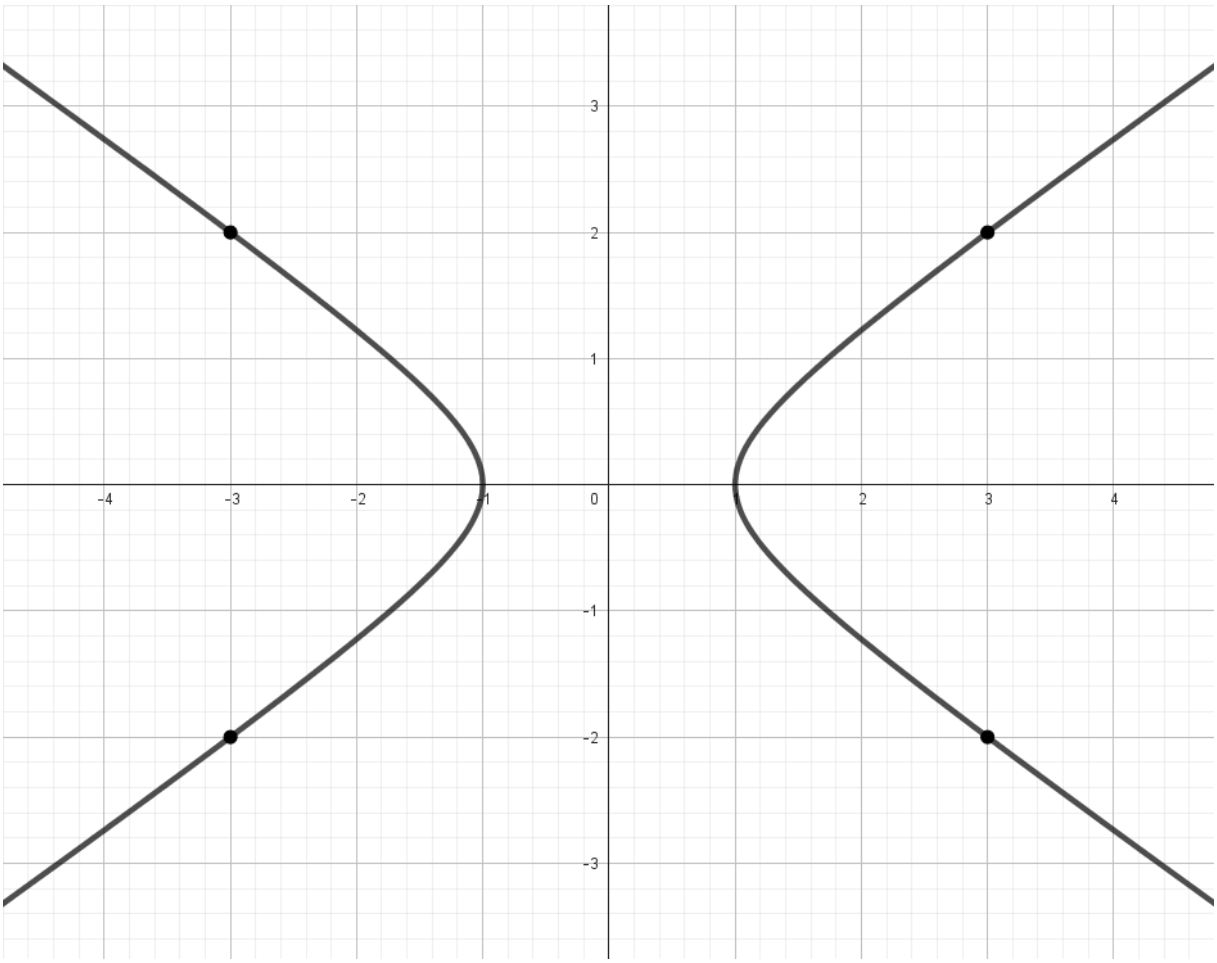
Během řešení předchozích úloh jsme učinili několik důležitých pozorování. Triviální řešení platí pro všechny Pellovy rovnice. Zároveň je jediným řešením těch rovnic, kde $n = d^2, d \in \mathbb{N}$; proto tento případ v definici Pellovy rovnice vylučujeme. Dále si můžeme všimnout, že pokud je řešením nějaké $(x; y)$, pak jsou řešení také všechny znaménkové variace $(x; -y), (-x; y), (-x; -y)$.

To, že triviální řešení platí pro všechny Pellovy rovnice, je zřejmé. Jelikož se druhý člen, jehož je n součástí, vynuluje, je řešení nezávislé na n, tedy na jediném prvku, ve kterém se různé Pellovy rovnice liší. Problém je redukovaný pouze na $x^2 = 1$ pro všechny případy. Ve všech případech bude platit $x = \pm 1$ a tedy triviální řešení $(\pm 1; 0)$ platí pro všechny Pellovy rovnice.

Tvrzení, že rovnici řeší všechny znaménkové variace $(x; y), (x; -y), (-x; y), (-x; -y)$ je také dosti zřejmé. Vzhledem k tomu, že proměnné vstupují do rovnice ve druhé mocnině, je dosazení například $(3; 2), (3; -2), (-3; 2), (-3; -2)$ do rovnice $x^2 - 2y^2 = 1$ ekvivalentní.

$$3^2 - 2 \cdot 2^2 = \ 3^2 - 2(-2)^2 = \ (-3)^2 - 2 \cdot 2^2 = \ (-3)^2 - 2(-2)^2 = 1$$

To je ostatně velmi dobře vidět, pokud se podíváme na graf křivky, kterou Pellova rovnice popisuje. Ten tvoří hyperbola souměrná podle osy x i osy y.



Obr 2. Graf Pellovy rovnice $x^2 - 2y^2 = 1$

(vlastní zpracování, GeoGebra)

Poznámka Pokud nebude specifikováno jinak, budeme se dále bez úhony na obecnosti zabývat pouze kladnými řešeními ($x, y > 0$). Všechna řešení pak dostaneme tak, že přidáme všechny znaménkové variace daného kladného řešení.

Pozorování, které není zcela triviální, je, že v případě kdy n je čtverec, je řešením pouze triviální řešení a žádné netriviální neexistuje. Své pozorování jsme si odůvodnili tím, že jediné dva čtverce, jejichž rozdíl je 1 jsou právě 0 a 1. Pojďme si ale ukázat formálnější důkaz.

Tvrzení 2.

Pokud je n čtverec, pak má Pellova rovnice pouze triviální řešení.

Důkaz. Myšlenku důkazu nejprve ukažme na konkrétní rovnici $x^2 - 4y^2 = 1$. V případě, že n je čtverec, můžeme je napsat jako $d^2, d \in \mathbb{N}$. Číslo 4 tedy zapíšeme jako 2^2 Následně provedeme rozklad podle vzorce $a^2 - b^2 = (a - b) \cdot (a + b)$.

$$x^2 - 2^2y^2 = 1$$

$$(x + 2y) \cdot (x - 2y) = 1$$

Protože $x, y \in \mathbb{Z}$, obě závorky budou ve výsledku celočíselné. Jejich součinem tedy dostaneme 1 pouze tehdy, kdy se a) obě rovnají 1 nebo b) obě rovnají -1. Musí tedy nastat jeden z následujících dvou případů:

a) $x + 2y = 1$
$x - 2y = 1$

b) $x + 2y = -1$
$x - 2y = -1$

V obou případech, když rovnice sečteme, $2y$ se vyruší a dostáváme $2x = 2$ resp. $2x = -2$, a tedy $x = 1$ resp. $x = -1$. Po dosazení zjistíme, že $2y = 0$, a tedy $y = 0$. Jediná řešení tedy skutečně jsou pouze $(1; 0)$ a $(-1; 0)$.

Pro obecný důkaz postupujme stejně. Nechť $x^2 - ny^2 = 1$, kde $n = d^2, d \in \mathbb{N}$. Levou stranu opět rozložíme na součin.

$$x^2 - d^2y^2 = 1$$

$$(x + dy) \cdot (x - dy) = 1$$

A nastává jeden ze dvou případů:

a) $x + dy = 1$
$x - dy = 1$

b) $x + dy = -1$
$x - dy = -1$

Když rovnice sečteme, vyjdou nám rovnice totožné těm v konkrétním příkladu $2x = 2$ resp. $2x = -2$ a $dy = 0$. Případ $d = 0$ neuvažujeme, protože pak už se nejedná o rovnici tvaru $x^2 - ny^2 = 1$ ale pouze triviální kvadratickou rovnici o jedné neznámé $x^2 = 1$. V ostatních případech musí platit $y = 0$ a získáváme jediná řešení $(\pm 1; 0)$ pro rovnice, kde $n = d^2$.

(Kala, 2021, s. 6) ■

Výše jsme si tedy ověřili všechna pozorování, která jsme učinili v příkladu 1. Vraťme se nyní k hledání řešení. Kdybychom hledali metodou postupného dosazování řešení například pro

$n = 13$, velmi dlouho bychom na žádné nenarazili. Je na místě si položit otázku, zda všechna n, která vyhovují definici Pellovy rovnice, skutečně mají i jiné, než triviální řešení. Tedy např., zda nějaké netriviální řešení $x^2 - 13y^2 = 1$ existuje a má vůbec smysl je hledat.

K tomu budeme potřebovat další teorii. Udělejme tedy krátkou odbočku k aproximacím iracionálních čísel. Znalosti z následující podkapitoly nám pomohou při dokazování existence netriviálních řešení.

1.1 Aproximace iracionálních čísel

Iracionální čísla nelze na rozdíl od racionálních vyjádřit jako podíl celých čísel. Proto, abychom s nimi mohli počítat, pracujeme s racionálními čísly, které se danému iracionálnímu číslu pouze přibližují.

S jistou formou aproximace jsme se setkali už na základní škole, kdy jsme se učili zaokrouhlovat. Pokud má dané číslo za desetinnou čárkou číslici pět nebo větší, zaokrouhlíme nahoru, tj. na nejbližší vyšší celé číslo a pokud je číslice za čárkou čtyři a menší, zaokrouhlíme dolu, tj. na nejbližší nižší celé číslo. Můžeme se na tento proces dívat jako na přidávání

a odebírání. Například mějme $\sqrt{2} = 1{,}414213562$ .... Podle pravidel toto číslo zaokrouhlíme na 1, neboli odečteme necelou část odmocniny ze dvou od její celé části. To je o něco přesnější, než kdybychom přičítali $\sim 0{,}586$, abychom se dostali na 2. Jde nám totiž o to, aby rozdíl mezi číslem, které aproximujeme a výslednou aproximací byl co nejmenší, tedy aby hodnota výrazu $\left|\sqrt{2} - p\right|$, kde p je číslo kterým $\sqrt{2}$ aproximujeme, byla minimální.

Poznámka V některých případech je užitečné aproximovat i čísla racionální. Ty sice umíme vyjádřit zlomkem, ale ten může být někdy příliš velký na to, aby se s ním dobře počítalo. Uvažujme například $\frac{29525}{59049}$ na první pohled velký a složitý zlomek, který ovšem můžeme aproximovat třeba jako $\frac{1}{2}$, pokud pro náš účel není překážkou drobná odchylka přibližně $\frac{1}{118098} \approx 0{,}0000085$.

Poznámka Dále v textu budeme značit celou část nějakého čísla α hranatými závorkami $[\alpha]$ a jeho necelou část množinovými závorkami $\{\alpha\}$. Například máme-li číslo $1{,}96$, pak $[\alpha] = 1$ a $\{\alpha\} = 0{,}96$.

Kdybychom se omezili na zaokrouhlování na celá čísla, připouštěli bychom značné odchylky, pokud by původní číslo již nebylo velice blízko nějakému celému. Abychom dosáhli menší odchylky, můžeme zaokrouhlovat na nějaké požadované n-té desetinné místo. Například odmocninu ze dvou zaokrouhlíme nejčastěji na jedno desetinné místo: $1{,}4$, případně na dvě desetinná místa: $1{,}41$. To je ovšem výhodné jen na prvních několik desetinných míst. Praktické počítání např. s $\sqrt{2} \doteq 1{,}4142$ by bylo zbytečně náročné a proto, ačkoliv je odchylka výrazně menší než při zaokrouhlování na celá čísla, není zaokrouhlování na větší počet desetinných míst výhodné. Zamysleme se, zda by nebylo možné aproximovat iracionální čísla lépe, tedy s ještě menší odchylkou, ale aby zároveň konkrétní aproximace měla formát, se kterým se dobře počítá.

Vraťme se zpět k zaokrouhlování na čísla celá a uvažujme násobky iracionálního čísla. Myšlenka je v tom, že nějaký násobek našeho čísla, která chceme aproximovat, bude blízko nějakému celému číslu. Vezměme jako příklad $\sqrt{2}$, o které jsme mluvili:

$$\sqrt{2} = 1{,}414213562 \ldots \qquad 5\sqrt{2} = 7{,}071067811 \ldots$$

$$2\sqrt{2} = 2{,}828427124 \ldots \qquad 6\sqrt{2} = 8{,}485281374 \ldots$$

$$3\sqrt{2} = 4{,}242640687 \ldots \qquad 7\sqrt{2} = 9{,}899494936 \ldots$$

$$4\sqrt{2} = 5{,}656854249 \ldots \qquad 8\sqrt{2} = 11{,}313708498 \ldots$$

Nyní uvažujme následující aproximace:

$$\sqrt{2} \approx 1 \rightarrow \sqrt{2} \approx 1, \qquad 5\sqrt{2} \approx 7 \rightarrow \sqrt{2} \approx \frac{7}{5},$$

$$2\sqrt{2} \approx 3 \rightarrow \sqrt{2} \approx \frac{3}{2}, \qquad 6\sqrt{2} \approx 8 \rightarrow \sqrt{2} \approx \frac{8}{6} = \frac{4}{3},$$

$$3\sqrt{2} \approx 4 \rightarrow \sqrt{2} \approx \frac{4}{3}, \qquad 7\sqrt{2} \approx 10 \rightarrow \sqrt{2} \approx \frac{10}{7},$$

$$4\sqrt{2} \approx 6 \rightarrow \sqrt{2} \approx \frac{6}{4} = \frac{3}{2}, \qquad 8\sqrt{2} \approx 11 \rightarrow \sqrt{2} \approx \frac{11}{8}.$$

Dostáváme se tedy k aproximaci pomocí zlomků. Máme nějaké $q, q \in \mathbb{N}$, kterým násobíme $\sqrt{2}$ a nějaké p, které vznikne zaokrouhlením $q\sqrt{2}$ nahoru nebo dolů podle necelé části. Čísla

p a q tvoří zlomek $\frac{p}{q} \in \mathbb{Q}$, který aproximuje $\sqrt{2}$. Zároveň chceme, aby byly zlomky $\frac{p}{q}$ v základním tvaru (viz $q = 4, q = 6$).

Všimněme si, že některé násobky (např. $2\sqrt{2}, 7\sqrt{2}$) jsou blízko následujícímu celému číslu a některé blízko předcházejícímu číslu (např. $3\sqrt{2}, 5\sqrt{2}$). V těchto případech se při zaokrouhlení dopouštíme jen malé odchylky, zatímco u čísel, jejichž necelá část se pohybuje okolo $0{,}5$ (např. $4\sqrt{2}, 6\sqrt{2}$), je odchylka největší. Z výsledků je vidět, že jen některé násobky se dostanou blízko celému číslu a neplatí tak, že by každá další aproximace, ke které dojdeme touto metodou, byla přesnější než ta předchozí. Proto definujeme dobré aproximace. Dobrá aproximace neříkáme každé aproximaci, která má malou odchylku, ale identifikujeme je dle následující definice.

Definice 4. Dobrá aproximace

Řekneme, že $\frac{p}{q} \in \mathbb{Q}$ je dobrá aproximace daného iracionálního čísla α právě tehdy, když

$$|q\alpha - p| < |s\alpha - r|$$

Pro všechna r, s taková, že $0 < s \leq q$ a $r \neq p$. (Manin a Panchishkin, 2005, s. 50)

Jinými slovy, dobrá aproximace je taková, která má od daného čísla menší odchylku než všechny aproximace s menším jmenovatelem. Intuitivně bychom si mohli myslet, že toto platí vždy. Když zvětšíme jmenovatel, zjemní se rozdělení osy. Ovšem jak jsme viděli, když jsme aproximovali $\sqrt{2}$ pomocí q-násobků, není tomu tak. Rozšiřme naše hledání aproximací z $q = 8$ až na $q = 12$ a podívejme se na dobré aproximace $\sqrt{2}$.

Poznámka Zajímá nás odchylka absolutní, tedy hodnota rozdílu aproximace a původního čísla. Existuje také odchylka relativní, která udává, o jakou část původního čísla se aproximace liší, a běžně se uvádí v procentech. Ekvivalentně by se tedy dobrá aproximace dala definovat s relativní odchylkou, ovšem jednalo by se o pouhý převod rozdílu na procentuální rozdíl, což je navíc v případě iracionálních odmocnin bez kalkulačky početně zbytečně obtížné.

Příklad 2.

Najděte dobré aproximace mezi aproximacemi $\sqrt{2}$ pro $q = 1$ až $q = 12$.

$$\sqrt{2} = 1{,}414213562\ldots \approx 1 \to \frac{1}{1} \qquad 7\sqrt{2} = 9{,}899494936\ldots\ldots \approx 10 \to \frac{10}{7}$$

$$2\sqrt{2} = 2{,}828427124\ldots\ldots \approx 3 \to \frac{3}{2} \qquad 8\sqrt{2} = 11{,}313708498\ldots\ldots \approx 11 \to \frac{11}{8}$$

$$3\sqrt{2} = 4{,}242640687\ldots\ldots \approx 4 \to \frac{4}{3} \qquad 9\sqrt{2} = 12{,}727922061\ldots\ldots \approx 13 \to \frac{13}{9}$$

$$4\sqrt{2} = 5{,}656854249\ldots\ldots \approx 6 \to \frac{1}{4} \qquad 10\sqrt{2} = 14{,}142135623\ldots\ldots \approx 14 \to \frac{7}{5}$$

$$5\sqrt{2} = 7{,}071067811\ldots\ldots \approx 7 \to \frac{7}{5} \qquad 11\sqrt{2} = 15{,}556349186\ldots\ldots \approx 16 \to \frac{16}{11}$$

$$6\sqrt{2} = 8{,}485281374\ldots\ldots \approx 8 \to \frac{4}{3} \qquad 12\sqrt{2} = 16{,}970562748\ldots\ldots \approx 17 \to \frac{17}{12}$$

Řešení.

Podle definice je dobrá ta aproximace, která je blíže $\sqrt{2}$ než všechny předchozí. Zároveň jsme si říkali, že aproximace je lepší, když je q-násobek blíže nějakému celému číslu, na které budeme zaokrouhlovat. Tedy jsou to ty aproximace q-násobků, jejichž necelé části jsou buďto velmi blízko nule nebo velmi blízko jedné. Nejhorší jsou potom aproximace těch, jejichž necelá část je nejblíže $0{,}5$. To lze zjednodušit, když budeme uvažovat rozdíl mezi q-násobkem a číslem, pomocí kterého je aproximujeme. Nejlepší aproximace jsou přirozeně ty, jejichž rozdíl je nejmenší. Vypišme kandidáty z dřívějšího pozorování a uvažujme rozdíly:

1. $\left|\sqrt{2} - 1\right| = 0{,}414213562\ldots$
2. $\left|2\sqrt{2} - 3\right| = 0{,}171572875\ldots$
3. $\left|3\sqrt{2} - 4\right| = 0{,}242640687\ldots$
4. $2 \cdot \left|2\sqrt{2} - 3\right| = 2 \cdot 0{,}171572875\ldots$
5. $\left|5\sqrt{2} - 7\right| = 0{,}071067811\ldots$
6. $2 \cdot \left|3\sqrt{2} - 4\right| = 2 \cdot 0{,}242640687\ldots$
7. $\left|7\sqrt{2} - 10\right| = 0{,}100505063\ldots$
8. $\left|8\sqrt{2} - 11\right| = 0{,}313708498\ldots$
9. $\left|9\sqrt{2} - 13\right| = 0{,}272077938\ldots$
10. $2 \cdot \left|5\sqrt{2} - 7\right| = 2 \cdot 0{,}171572875\ldots$
11. $\left|11\sqrt{2} - 16\right| = 0{,}443650813\ldots$
12. $\left|12\sqrt{2} - 17\right| = 0{,}029437251\ldots$

Poznámka V případech 4., 6. a 10. se číslo, které násobí odchylku se vykrátí s největším společným dělitelem příslušných p, q v absolutní hodnotě. Toto je třeba kvůli následujícím zlomkům $\frac{p}{q}$, které požadujeme v základním tvaru.

První aproximace $\sqrt{2} \approx 1$ je dobrá (ačkoliv ne velmi přesná), protože ji žádná nepředchází, a tak splňuje podmínky z definice. Následující dobrou aproximací je druhá aproximace $\sqrt{2} \approx \frac{3}{2}$, jejíž odchylka je výrazně menší než u první. Další dobrá aproximace je až pátá $\sqrt{2} \approx \frac{7}{5}$ a poté až dvanáctá $\sqrt{2} \approx \frac{17}{12}$.

Ačkoliv neplatí, že každá další aproximace je lepší než předchozí, můžeme nahlédnout, že pro větší q se dostaneme na menší odchylku, než byla u předchozí dobré aproximace. Jinými slovy, pro každou dobrou aproximaci existuje další dobrá aproximace s větším jmenovatelem q. Uvažujme následovně, rozdíl mezi q-násobkem $\sqrt{2}$ a nejbližším celým číslem, je jistě menší než jedna a platí:

a) $q = 2, \left|2\sqrt{2} - 3\right| < 1 \rightarrow \left|\sqrt{2} - \frac{3}{2}\right| < \frac{1}{2}$

b) $q = 3, \left|3\sqrt{2} - 4\right| < 1 \rightarrow \left|\sqrt{2} - \frac{4}{3}\right| < \frac{1}{3}$

c) $q = 5, \left|5\sqrt{2} - 7\right| < 1 \rightarrow \left|\sqrt{2} - \frac{7}{5}\right| < \frac{1}{5}$

d) $q = 7, \left|7\sqrt{2} - 10\right| < 1 \rightarrow \left|\sqrt{2} - \frac{10}{7}\right| < \frac{1}{7}$

Vidíme, že obecně jsme tímto postupem schopni pro nějaké iracionální číslo α vytvořit aproximaci:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}$$

Odchylka je vždy menší, než $\frac{1}{q}$. To určuje horní hranici odchylky. Proto je-li q dostatečně velké, jistě se dostaneme pod odchylku předchozí dobré aproximace.

Obecně tedy existují aproximace, jejichž odchylku můžeme omezit $\frac{1}{q}$. Zamysleme se, zda můžeme odchylku aproximace omezit ještě lépe.

Mějme nějaké $q \in \mathbb{N}$ a rozdělme osu následovně:

Obr. 3: Rozdělení reálné osy

(vlastní zpracování, GeoGebra)

Pak nějaké iracionální číslo α se vyskytuje na ose někde mezi $\frac{i}{q}$ a $\frac{i+1}{q}, i \in \mathbb{Z}$. Označme to z nich, kterému je α blíže, $\frac{p}{q}$. Platí, že rozdíl α a $\frac{p}{q}$ je menší než polovina délky intervalu $\langle \frac{i}{q}; \frac{i+1}{q} \rangle$, tedy polovina $\frac{1}{q}$:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q}$$

(Kala, 2021, s. 7)

Poznámka Jistě se neocitneme v situaci, kdy by se $q\alpha$ vyskytlo přesně v polovině, či v krajních bodech intervalu $\langle \frac{i}{q}; \frac{i+1}{q} \rangle$. Číslo α by se pak dalo vyjádřit jako $\frac{i}{q}$, $\frac{i+1}{q}$ nebo v případě poloviny intervalu $\frac{2i+1}{2q}$, což jsou všechno čísla racionální, a to je ve sporu s iracionalitou α.

Tím jsme zpřesnili náš poznatek ohledně toho, že jistě existují aproximace, jejichž odchylka je menší než $\frac{1}{q}$: $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}$. Následující věta říká, že iracionální čísla lze aproximovat ještě lépe.

Věta 3. Dirichletova věta

Pro každé iracionální číslo α existuje nekonečně mnoho p, q takových, že $\frac{p}{q}$ se liší od α o méně než $\frac{1}{q^2}$.

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

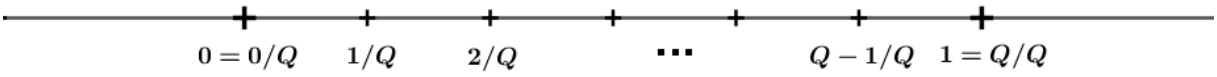
Důkaz. Důkaz je poměrně jednoduchý, využijeme při něm Dirichletova principu, což je tvrzení, nebo spíše pozorování, že máme-li n přihrádek, do kterých náhodně rozmístíme alespoň $n + 1$ věcí, pak v jedné z přihrádek se určitě vyskytují alespoň dvě věci.

Tvrzení 4. Dirichletův princip

Kouzlo čísel: Mějme $n \in \mathbb{N}$. Rozdělíme-li více než n předmětů do právě n přihrádek, pak v alespoň jedné z přihrádek se nachází alespoň dva předměty.

Důkaz. Předpokládejme, že máme více než n předmětů a v každé z přihrádek by byl nejvýše 1. Potom bychom měli ve všech přihrádkách právě n předmětů, což je spor s předpokladem, že máme předmětů více než n. (Křížek a spol., 2018, s. 47) ■

Pokračujme v důkazu Dirichletovy věty. Nechť je α je nějaké iracionální číslo. Pro jakékoliv $Q \in \mathbb{N}, 2 \leq Q$ najdeme $p, q \in \mathbb{N}$, tak, že platí: $1 \leq q < Q$ a $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ}$. Rozdělíme osu na Q intervalů:



Obr. 4: Rozdělení osy na Q intervalů

(vlastní zpracování, GeoGebra)

A mějme čísla $0, 1, \{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots \{(Q-1)\alpha\}$. Zde aplikujeme Dirichletův princip, protože máme Q intervalů a $Q + 1$ různých čísel a můžeme tedy trvdit, že v jednom z intervalů jsou dvě z našich čísel – nechť jsou to třeba $q_1\alpha - p_1$ a $q_2\alpha - p_2$. Rozdíl těchto dvou čísel je jistě menší než délka jednoho intervalu, tedy $\frac{1}{Q}$.

$$|(q_1\alpha - p_1) - (q_2\alpha - p_2)| \leq \frac{1}{Q}$$

Upravme výraz v absolutní hodnotě:

$$|(q_1 - q_2)\alpha - (p_1 - p_2)| \leq \frac{1}{Q}$$

Nyní označme $(q_1 - q_2) = q$ a $(p_1 - p_2) = p$ a vydělme celou nerovnici číslem q. Získáme náš hledaný tvar:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}$$

(Kala, 2021, s. 7)

Nyní můžeme vyměnit Q ve jmenovateli pravé strany za q, protože jak q_1, tak q_2 jsou menší než Q, a tak i jejich rozdíl je menší než Q a platí:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} < \frac{1}{q^2}$$

A tedy přirozeně $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. ■

Závěr Dirichletovy věty nám postačí, abychom dokázali, že řešení Pellovy rovnice vždy existuje, a tedy má smysl pokračovat v našem případu hledání nějakého řešení pro $x^2 - 13y^2 = 1$, který jsme na začátku nechali otevřený.

1.2 Existence netriviálního řešení Pellovy rovnice

Jako první si dokažme, že netriviální řešení existuje pro každou Pellovu rovnici.

Věta 5.
Pokud je n nečtverec, má každá Pellova rovnice netriviální řešení v $\mathbb{Z}$.

Důkaz. Nyní víme, že existuje nekonečně mnoho $\frac{p}{q}$, pro které platí: $\left|\sqrt{n} - \frac{p}{q}\right| < \frac{1}{q^2}$. Z toho usoudíme, že platí:

$$|p^2 - nq^2| = \left|p - q\sqrt{n}\right| \cdot \left|p + q\sqrt{n}\right| < \frac{1}{q^2} < 1$$

$$|p^2 - nq^2| = \left|p - q\sqrt{n}\right| \cdot \left|p - q\sqrt{n} + 2q\sqrt{n}\right| < \frac{1}{q} \cdot \left(\frac{1}{q} + 2q\sqrt{n}\right) < 1 + 2\sqrt{n}$$

Z toho plyne $|p^2 - nq^2| < 1 + 2\sqrt{n}$ a platí:

$$-1 - 2\sqrt{n} < p^2 - nq^2 < 1 + 2\sqrt{n}$$

V intervalu $\langle -1 - 2\sqrt{n};\ 1 + 2\sqrt{n}\rangle$ je jen konečný počet $k \in \mathbb{Z}$ ($k \neq 0$, kdyby se k rovnalo nule, musela by být $\sqrt{n}$ racionální), na které se zobrazí nekonečně různých $p^2 - nq^2$ (Protože $p, q, n \in \mathbb{Z}$ je i $p^2 - nq^2$ celé číslo.). Z toho vyplívá, podobně jako v předchozí větě, že díky Dirichletovu principu se jich na jedno k zobrazí nekonečně mnoho.

Příslušné dvojice $(p; q)$ rozdělíme do kategorií podle hodnot modulo k (tedy podle zbytku po dělení číslem k). Vznikne k^2 možných kategorií, což je stále konečný počet, do kterých budme rozřazovat nekonečně mnoho dvojic $(p; q)$. Alespoň do jedné z kategorií jich bude znovu patřit nekonečně mnoho. Postačí ovšem alespoň dvě. Označme je $(p_1; q_1)$ a $(p_2; q_2)$, přičemž platí: $(p_1; q_1) \neq (p_2; q_2)$, $p^2 - nq^2 = k$ a také $p_1 \equiv p_2\ mod\ k$, $q_1 \equiv q_2\ mod\ k$ (toto

znamená, že p_1 je kongruentní s p_2 modulo k, tedy že mají stejný zbytek po dělení číslem k). Uvažujme následující rovnost:

$$k^2 = (p_1^2 - nq_1^2) \cdot (p_2^2 - nq_2^2) = \left(p_1 - q_1\sqrt{n}\right) \cdot \left(p_1 + q_1\sqrt{n}\right) \cdot \left(p_2 - q_2\sqrt{n}\right) \cdot \left(p_2 + q_2\sqrt{n}\right)$$

Závorky můžeme překombinovat abychom dostali:

$$k^2 = \left[\left(p_1 - q_1\sqrt{n}\right) \cdot \left(p_2 + q_2\sqrt{n}\right)\right] \cdot \left[\left(p_1 + q_1\sqrt{n}\right) \cdot \left(p_2 - q_2\sqrt{n}\right)\right] =$$

$$= \left[(p_1p_2 - q_1q_2n) + (p_1q_2 - p_2q_1)\sqrt{n}\right] \cdot \left[(p_1p_2 - q_1q_2n) - (p_1q_2 - p_2q_1)\sqrt{n}\right]$$

Označme $p_1p_2 - q_1q_2n = A$ a $p_1q_2 - p_2q_1 = B$. Platí, že $A \equiv p_1^2 - nq_1^2 = k \equiv 0\ (mod\ k)$ a $B \equiv p_1q_2 - p_2q_1 = 0\ (mod\ k)$. Máme $k^2 = \left(A - B\sqrt{n}\right) \cdot \left(A + B\sqrt{n}\right)$. Dále mějme následující substituci $X = \frac{A}{k}$ a $Y = \frac{B}{k}$. $Y \neq 0$, protože pak by muselo platit $B = 0$ a tedy:

$$p_1q_2 - p_2q_1 = 0$$

Celou rovnici vydělíme q_1q_2

$$\frac{p_1}{q_1} - \frac{p_2}{q_2} = 0$$

A muselo by platit $p_1 = p_2, q_1 = q_2$ což je ve sporu s tím, že $(p_1; q_1) \neq (p_2; q_2)$. Platí tedy:

$$k^2 = A^2 - nB^2 = k^2 \cdot (X^2 - nY^2)$$

Celá rovnice vydělená k^2 nám dává rovnost $(X^2 - nY^2) = 1$ a $(X; Y)$ je netriviální řešení Pellovy rovnice. (Kala, 2021, s. 8) ■

Můžeme tedy s určitostí říct, že netriviální řešení vždy existuje. Proto má cenu zabývat se hledáním řešení např. pro naše $x^2 - 13y^2 = 1$, pro něž je téměř nemožné řešení uhodnout a postupné zkoušení různých y by trvalo velice dlouho.

Jak tedy budeme hledat netriviální řešení? Víme, že dvojice $(x; y)$ ve tvaru $\frac{x}{y}$ aproximují $\sqrt{n}$. Tak jsme na začátku kapitoly Pellovu rovnici odvodili. Tuto vlastnost také můžeme ukázat následujícím vyjádřením, kde vydělíme celou rovnici y^2 a levou stranu pak rozložíme:

$$\left(\frac{x}{y} - \sqrt{n}\right) \cdot \left(\frac{x}{y} + \sqrt{n}\right) = \frac{1}{y^2}$$

Závorku $\left(\frac{x}{y} + \sqrt{n}\right)$ můžeme zespodu omezit nějakým celým číslem $c > 1$. Prozatím počítejme, že $c = 1$, a tedy:

$$\left(\frac{x}{y} - \sqrt{n}\right) < \frac{1}{y^2}$$

Hledáme tedy taková $\frac{x}{y}$, která splňují tuto nerovnost. (Woods, 2020)

Vezměme například opět $\sqrt{2}$ a uvažujme následovně. Víme, že $\sqrt{2} = 1{,}414213562\ldots$, můžeme tedy tvrdit, že $\sqrt{2}$ leží mezi 1 a 2.

$$1 < \sqrt{2} < 2$$

Naše vymezení můžeme ještě zpřesnit, a to tak, že se pokusíme ohraničit necelou část pomocí nějakých zlomků, a tak shora i zdola lépe odmocninu ze dvou omezit. V případě $\sqrt{2}$ můžeme její necelou část $0{,}414213562\ldots$, ohraničit mezi zlomky $\frac{1}{3} = 0,\overline{33}$ a $\frac{1}{2} = 0{,}5$.

$$1 + \frac{1}{3} < \sqrt{2} < 1 + \frac{1}{2}$$

Můžeme si všimnout, že jsme měli štěstí a horní hranice $1 + \frac{1}{2} = \frac{3}{2}$ je dobrou aproximací a také řešením rovnice. To souhlasí s tím, že během metody postupného dosazování jsme brzy objevili první řešení pro $x^2 - 2y^2 = 1$. Pro jiná n bychom takové štěstí neměli. Otázkou je, jak postupovat dále a $\sqrt{2}$ omezit přesněji. Vezměme naše původní celočíselné omezení a postupujme následovně.

$$1 < \sqrt{2} < 2$$

Číslo 1 na levé straně označme jako a_0 a vyjádřeme $\sqrt{2}$ jako $a_0 + \varepsilon_0$, tedy konkrétně jako $1 + 0{,}414213562\ldots$, to bude náš krok 0.

Krok 0 $\qquad 1 = a_0 < \sqrt{2} < 2 \qquad\qquad \sqrt{2} = 1 + \varepsilon_0$

Jako další krok se pokusíme omezit ε_0. Pro jednoduchost bychom chtěli použít omezení celými čísly, ale vzhledem k tomu, že v tomto kroku se $\varepsilon_0 = \{\sqrt{2}\} = 0{,}414213562\ldots$, můžeme použít jen omezení 0 a 1a ε_0 vyjádřit jako $0 + \varepsilon_1$, kde $\varepsilon_1 = \varepsilon_0$. To nás ovšem nikam neposouvá, krok 1 by se opakoval do nekonečna a dostávali bychom samé nuly nehledě na to, jaké číslo touto metodou aproximujeme, protože každé bychom v nultém kroku rozdělili na celou a necelou část a v prvním a dalších krocích bychom necelou část dokola omezovali zespoda nulou. Zkusme tedy omezit $\frac{1}{\varepsilon_0} = 2{,}414213562$ a spodní hranici označme a_1 a necelou část $\left\{\frac{1}{\varepsilon_0}\right\}$ označme ε_1.

Pro výpočet $\frac{1}{\varepsilon_0}$ použijeme usměrňování zlomků. Víme, že ε_0 je necelá část $\sqrt{2}$. Platí tedy:

$$\varepsilon_0 = \sqrt{2} - 1$$

Kdybychom nyní pouze udělali převrácenou hodnotu: $\frac{1}{\sqrt{2}-1}$ nevěděli bychom, jak tento zlomek omezit. Proto jej rozšíříme jedničkou ve tvaru $\frac{\sqrt{2}+1}{\sqrt{2}+1}$:

$$\frac{1}{\varepsilon_0} = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2}+1$$

Toto číslo nyní můžeme omezit následujícím způsobem:

$$1 < \sqrt{2} < 2$$

$$2 < \sqrt{2} + 1 < 3$$

Vidíme, že celou částí $\sqrt{2}+1$ je 2 a necelou část vyjádříme jako $\sqrt{2}+1-2 = \sqrt{2}-1$. Takto postupujeme i v dalších krocích.

Krok 1 $\quad 2 = a_1 < \frac{1}{\varepsilon_0} < 3 \qquad \sqrt{2} = 1 + \frac{1}{\frac{1}{\varepsilon_0}} = 1 + \frac{1}{2+\varepsilon_1}$

A takto pokračujeme, vždy bereme převrácenou hodnotu čísla $\frac{1}{\varepsilon_i}$, kterou omezíme a vyjádříme jako $a_i + \varepsilon_i, i \in \mathbb{N}$. (Woods, 2020)

Ukážeme si další příklady, abychom lépe pochopili tuto konstrukci. Nejprve pokračujme v aproximaci $\sqrt{2}$.

Krok 0 $\quad 1 = a_0 < \sqrt{2} < 2 \qquad \sqrt{2} = 1 + \varepsilon_0$

Krok 1 $\quad 2 = a_1 < \frac{1}{\varepsilon_0} < 3 \qquad \sqrt{2} = 1 + \frac{1}{\frac{1}{\varepsilon_0}} = 1 + \frac{1}{2+\varepsilon_1}$

Krok 2 $\quad 2 = a_2 < \frac{1}{\varepsilon_1} < 3 \qquad \sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2+\varepsilon_2}}$

Krok 3 $\quad 2 = a_3 < \frac{1}{\varepsilon_2} < 3 \qquad \sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2+\varepsilon_3}}}$

Vidíme že, necelá část ε_i je pokaždé stejná, a tedy se ve zlomku reprezentujícím $\sqrt{2}$ bude také 2 jako a_i opakovat do nekonečna. Nyní se podívejme na $\sqrt{3}$.

Krok 0 $\quad 1 = a_0 < \sqrt{3} < 2 \qquad \sqrt{3} = 1 + \varepsilon_0$

Krok 1 $1 = a_1 < \frac{1}{\varepsilon_0} < 2$ $\sqrt{3} = 1 + \frac{1}{1+\varepsilon_1}$

Krok 2 $2 = a_2 < \frac{1}{\varepsilon_1} < 3$ $\sqrt{3} = 1 + \frac{1}{1+\frac{1}{2+\varepsilon_2}}$

Krok 3 $1 = a_3 < \frac{1}{\varepsilon_2} < 2$ $\sqrt{3} = 1 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\varepsilon_3}}}$

Pokud bychom pokračovali ještě o jeden krok dále, zjistili bychom že $a_4 = 2$ a $\frac{1}{\varepsilon_3} = \frac{1}{\varepsilon_1}$ a v dalších krocích by se střídali $a_{2i+1} = 1$ a $a_{2i} = 2$, tedy lichá a_i by byla 1 a sudá 2. Pro odmocninu z pěti provedeme následující kroky.

Krok 0 $2 = a_0 < \frac{1}{\varepsilon_1} < 3$ $\sqrt{5} = 2 + \varepsilon_0$

Krok 1 $4 = a_1 < \sqrt{5} < 5$ $\sqrt{5} = 2 + \frac{1}{4+\varepsilon_1}$

Krok 2 $4 = a_2 < \frac{1}{\varepsilon_1} < 5$ $\sqrt{5} = 2 + \frac{1}{4+\frac{1}{4+\varepsilon_2}}$

Krok 3 $4 = a_3 < \frac{1}{\varepsilon_2} < 5$ $\sqrt{5} = 2 + \frac{1}{4+\frac{1}{4+\frac{1}{4+\varepsilon_3}}}$

Zde opět jako v případě $\sqrt{2}$ se v každém kroce opakuje stejné a_i a platí, že $\frac{1}{\varepsilon_{i+1}} = \frac{1}{\varepsilon_i}$. Jak si později ukážeme, pro všechny iracionální odmocniny platí, že se čísla a_i dříve či později začnou opakovat.

Někomu již možná tato forma vyjadřování iracionálních odmocnin začala připomínat jistý typ zlomků, a to zlomky řetězové. O těch si v následující kapitole povíme víc, jelikož se jedná o jednu z nejběžnějších metod hledání řešení Pellovy rovnice.

2 Hledání netriviálního řešení a řetězové zlomky

Pojďme řádně definovat konstrukci, ke které jsme se na konci minulé kapitoly dobrali při aproximování iracionálních $\sqrt{n}$. Jak již bylo zmíněno, jedná se o řetězové zlomky. Podívejme se blíže na jejich vlastnosti, abychom pochopili, jak pomocí nich získat řešení Pellovy rovnice.

Definice 4. Řetězový zlomek

Pro jakékoliv reálné číslo α, definujeme jeho řetězový zlomek pomocí posloupností $a_0, a_1, a_2, \dots, a_k, a_i \in \mathbb{Z}$ pro $i = 1, 2, \dots, k$ a $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{k+1}, \varepsilon_i \in \mathbb{R}$ pro $i = 1, 2, \dots, k+1$ daných následovně: $a_o = [\alpha]$, $\varepsilon_0 = \alpha$, $\varepsilon_{i+1} = \frac{1}{\varepsilon_i - a_i}$, $a_{i+1} = [\varepsilon_{i+1}]$. Dostáváme řetězový zlomek:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_k + \cfrac{1}{\varepsilon_{k+1}}}}}$$

Tuto rozsáhlou formulaci můžeme zjednodušeně zapsat jako $\alpha = [a_0; a_1, a_2, \dots a_k, \varepsilon_{k+1}]$. (Manin a Panchishkin, 2005, s. 51).

2.1 Řetězové zlomky racionálních čísel

Pokud je α racionální, pak je řetězový zlomek konečný $\alpha = [a_0; a_1, a_2, \dots a_k]$. (Yang, 2008, s. 1) To lze jednoduše nahlédnout. Pokud máme racionální číslo, je vyjádřitelné nějakým zlomkem, kde čitatel a jmenovatel jsou nějaká celá čísla. Začneme-li upravovat řetězový zlomek odspodu, dostaneme se právě k takovému konkrétnímu zlomku, jak uvidíme v následujících příkladech.

Příklad 3.

Spočtěte řetězové zlomky pro následující racionální čísla.

a) $\frac{3}{2}$ b) $\frac{24}{7}$ c) $\frac{55}{16}$ d) $\frac{345}{113}$

Řešení.

a) Pro $\frac{3}{2}$ je vytvoření řetězového zlomku poměrně jednoduché. Postupujme podle pravidel pro a_i a ε_i z definice. $a_o = \left[\frac{3}{2}\right] = 1$, $\varepsilon_1 = \frac{1}{\frac{3}{2} - \left[\frac{3}{2}\right]} = 2$, $a_1 = [\varepsilon_1] = 2$ a máme:

$$\frac{3}{2} = 1 + \frac{1}{2}$$

Je vidět, že jsme počítali správně, a není třeba provádět zkoušku. Tu provedeme u následujících příkladů, kde nebude správnost výsledku patrná na první pohled.

b) Výpočet pro $\frac{24}{7}$ je o trochu delší, ale postupujeme stejně jako v případu a). Popišme si tentokrát postup trochu jednodušeji, protože pro delší řetězové zlomky může být jejich konstrukce podle definice nepřehledná. Podstatou řešení je, že v každém kroku oddělíme celou část a_i a necelou část $\frac{1}{\varepsilon_i}$, kterou převrátíme abychom získali $\left(\frac{1}{\varepsilon_i}\right)^{-1} = \varepsilon_i$, ale abychom zachovali hodnotu necelé části píšeme $\frac{1}{\left(\frac{1}{\varepsilon_i}\right)^{-1}}$. $a_o = 3$, $\varepsilon_1 = \frac{7}{3}$

$$\frac{24}{7} = 3 + \frac{3}{7} = 3 + \frac{1}{\frac{7}{3}}$$

Hodnotu necelé části tedy převrátíme a zapíšeme do jmenovatele zlomku s čitatelem 1, přičemž se hodnota nezmění a dostaneme ve jmenovateli zlomek větší než 1 a můžeme proces opakovat a znovu ho rozdělit. $a_1 = 2$, $\varepsilon_2 = \frac{3}{1}$

$$\frac{24}{7} = 3 + \frac{3}{7} = 3 + \frac{1}{\frac{7}{3}} = 3 + \frac{1}{2 + \frac{1}{3}}$$

Jelikož poslední zlomek má v čitateli jedna, platí že $\left(\frac{1}{3}\right)^{-1} = \varepsilon_2 = 3$, a tedy rozdělíme na $a_2 = 3$ a necelou část 0, ze které již $\varepsilon_3 = \frac{1}{0}$ nevyjádříme, protože se jedná o nedefinovaný výraz a proces tady končí. Vyjádřili jsme tedy $\frac{24}{7}$ jako:

$$3 + \frac{1}{2 + \frac{1}{3}} = [3,2,3]$$

Proveďme nyní zkoušku abychom si ověřili správnost našeho výpočtu. Budeme postupovat od posledního zlomku a upravíme výraz $2 + \frac{1}{3}$ na $\frac{7}{3}$. Nyní máme:

$$3 + \frac{1}{\frac{7}{3}} = 3 + \frac{3}{7}$$

A upravme $3 + \frac{3}{7}$ na $\frac{24}{7}$. Dostali jsme se k původnímu číslu, čímž jsme dokázali, že náš výsledek byl správný.

c) Postupujeme stejně jako v předchozích případech, proto uvedeme jen jednotlivé kroky. Máme $\varepsilon_0 = \frac{55}{16}$, $a_o = [\varepsilon_0] = 3$ a $\varepsilon_1 = \frac{1}{\frac{55}{16}-3} = \frac{16}{7}$.

$$\frac{55}{16} = 3 + \frac{1}{\frac{16}{7}}$$

V dalším kroku máme $\varepsilon_1 = \frac{16}{7}$, $a_o = [\varepsilon_1] = 2$ a $\varepsilon_2 = \frac{1}{\frac{16}{7}-2} = \frac{7}{2}$.

$$\frac{55}{16} = 3 + \frac{1}{2 + \frac{1}{\frac{7}{2}}}$$

$\varepsilon_2 = \frac{7}{2}$, $a_2 = [\varepsilon_2] = 3$ a $\varepsilon_3 = \frac{1}{\frac{7}{2}-3} = \frac{2}{1}$. Dostali jsme se opět do bodu, kdy ε_i je celé číslo, a tak zde proces končí. Dostali jsme se k vyjádření $\frac{55}{16}$ řetězovým zlomkem.

$$\frac{55}{16} = 3 + \frac{1}{2 + \frac{1}{3+\frac{1}{2}}} = [3,2,3,2]$$

Proveďme nyní zkoušku. Postupujeme stejně jako v předchozím případě.

$$3 + \frac{1}{2 + \frac{1}{3+\frac{1}{2}}} = 3 + \frac{1}{2 + \frac{1}{\frac{7}{2}}} = 3 + \frac{1}{2 + \frac{2}{7}} = 3 + \frac{1}{\frac{16}{7}} = 3 + \frac{7}{16} = \frac{55}{16}$$

Vidíme, že jsme postupovali správně a dobrali se správného výsledku.

d) Pro vyřešení tohoto příkladu bychom postupovali stejným způsobem jako v předchozích. Využijme ho ale k ukázce spojitosti mezi Eukleidovým algoritmem a řetězovými zlomky. Vrátíme se tedy k řešení tohoto příkladu o něco později.

Definice 5. Dělitelnost v $\mathbb{Z}$

Řekneme, že číslo $a \in \mathbb{Z}$ dělí číslo $b \in \mathbb{Z}$, právě tehdy, když platí, že $b = k \cdot a, k \in \mathbb{Z}$ a značíme $a|b$. V opačném případě řekneme že a nedělí b a píšeme $a \nmid b$. Číslo a označujeme jako dělitele čísla b. (Křížek a spol., 2018, s. 29)

Definice 6. Největší společný dělitel

Jako největší společný dělitel nenulových čísel $a, b \in \mathbb{Z}$ označíme největší číslo $k \in \mathbb{N}$ takové, které dělí obě čísla a i b. (Křížek a spol., 2018, s. 32).

Definice 7. Eukleidův algoritmus

Eukleidův algoritmus se používá k nalezení největšího společného dělitele dvou přirozených čísel $a, b, a \geq b$, který značíme (a, b). Pokud b dělí a, největším společným dělitelem je b a případ je triviální. Eukleidova algoritmu užijeme v případě, kdy b nedělí a. Princip tohoto algoritmu spočívá v následujícím tvrzení, kde z je zbytek po dělení čísla a číslem b.

$$(a, b) = (b, z)$$

(Křížek a spol. 2018, s. 36). Toto tvrzení není zřejmé, ale ukázat, že platí, je jednoduché. Uvažujme následovně. Platí, že největší společný dělitel dělí obě čísla. Označme největšího společného dělitele čísel a, b zkratkou D. Dále uvažujme čísla $a, b \in \mathbb{N}, a > b, b \neq 0$.

$$\frac{a}{b} = \frac{\mathrm{D} \cdot k}{\mathrm{D} \cdot l}$$

Čísla k a l jsou nesoudělná, protože všichni společní dělitelé jsou vytknuti jako součást D. Protože $a > b$, musí být číslo k větší než l a tedy lze k vyjádřit jako $m \cdot l + n;\ m, n \in \mathbb{N}$.

$$\frac{a}{b} = \frac{\mathrm{D} \cdot (m \cdot l + n)}{\mathrm{D} \cdot l} = \frac{\mathrm{D} \cdot m \cdot l + \mathrm{D} \cdot n}{\mathrm{D} \cdot l} = m + \frac{\mathrm{D} \cdot n}{\mathrm{D} \cdot l}$$

Všimněme si, že $\mathrm{D} \cdot n$ je zbytek po dělení čísla a číslem b. Označme je z a pamatujme, že $\mathrm{D} \cdot l = b$. Nyní když dokážeme, že n a l jsou nesoudělná, bude platit, že D, jak jsme označili (a, b), bude také největší společný dělitel b a z. Předpokládejme, že l a n nesoudělná nejsou. Pak je můžeme vyjádřit jako násobek nějakého $p, p \in \mathbb{Z}$, tedy $l = p \cdot r,\ n = p \cdot s$. A platí:

$$\frac{a}{b} = \frac{\mathrm{D} \cdot (m \cdot p \cdot r + p \cdot s)}{\mathrm{D} \cdot p \cdot r} = \frac{\mathrm{D} \cdot p \cdot (m \cdot r + s)}{\mathrm{D} \cdot p \cdot r}$$

Potom bychom mohli p vytknout z horní závorky a platilo by, že jak a, tak b mají dalšího společného dělitele p a $(a, b) = p \cdot \mathrm{D}$, což je ve sporu s předpokladem, že D je největší společný dělitel, a musí platit, že $\frac{b}{z} = \frac{\mathrm{D} \cdot l}{\mathrm{D} \cdot n}$, kde $n \geq l$ a jsou nesoudělná. Dokázali jsme, že $(a, b) = (b, z)$.

Příklad 4.

Najděte pomocí Eukleidova algoritmu největšího společného dělitele následujících dvojic čísel.

a) $91; 42$ b) $85; 51$ c) $196; 112$ d) $345; 113$

Řešení.

a) Případ $(91{,}42)$ postupně zjednodušujeme pomocí pravidla $(a, b) = (b, z)$, dokud se nedostaneme do bodu, kdy zbytek dělí předešlého dělitele, a tedy poslední nenulový zbytek, je největším společným dělitelem a a b. Jednoduší příklady můžeme napsat jako sekvenci rovností největších společných dělitelů podle definice.

$$(91{,}42) = (4{,}27) = 7$$

Ukažme si ale i podrobnější postup.

$$91 = 42 \cdot 2 + 7$$
$$42 = 7 \cdot 6 + 0$$

Výsledkem tedy je $(91{,}42) = 7$.

b) Postupujme nejprve podrobně.

$$85 = 51 \cdot 1 + 34$$
$$51 = 34 \cdot 1 + 17$$
$$34 = 17 \cdot 2 + 0$$

Postup můžeme i v tomto případě zapsat jednoduše jako:

$$(85{,}51) = (51{,}34) = (34{,}17) = 17$$

c) Jedná se o stejný princip, ukažme si pouze postup výpočtu.

$$196 = 112 \cdot 1 + 84$$
$$112 = 84 \cdot 1 + 28$$
$$84 = 28 \cdot 3 + 0$$
$$(196{,}112) = (112{,}84) = (84{,}28) = 28$$

d) Vracíme se k podílu, který jsme chtěli vyjádřit řetězovým zlomkem v příkladu 4. Proveďme podrobný postup hledání největšího společného dělitele pomocí Eukleidova algoritmu a nalezněme pomocí něj řetězový zlomek, který vyjadřuje $\frac{345}{113}$. Budeme postupovat stejně jako v předešlých případech, ale dělení budeme psát jako podíl, tj. racionální číslo ve tvaru zlomku.

$$\frac{345}{113} = 3 + \frac{6}{113}$$
$$\frac{113}{6} = 18 + \frac{5}{6}$$

$$\frac{6}{5} = 1 + \frac{1}{5}$$

$$\frac{5}{1} = 5 + 0$$

Vidíme, že podobně jako při výpočtu řetězového zlomku dělíme čísla na celou část a zbytek. Všimněme si, že každý další řádek je vyjádření převrácené hodnoty předešlého zbytku. Vypočítejme nyní řetězový zlomek a podívejme se na paralely mezi řetězovým zlomkem a Eukleidovým algoritmem.

$\varepsilon_0 = \frac{345}{113}$, $a_o = [\varepsilon_0] = 3$ a $\varepsilon_1 = \frac{1}{\frac{345}{113} - 3} = \frac{113}{6}$

$$\frac{345}{113} = 3 + \frac{1}{\frac{113}{6}}$$

$\varepsilon_1 = \frac{113}{6}$, $a_1 = [\varepsilon_1] = 18$ a $\varepsilon_2 = \frac{1}{\frac{113}{6} - 18} = \frac{6}{5}$

$$\frac{345}{113} = 3 + \frac{1}{18 + \frac{1}{\frac{6}{5}}}$$

$\varepsilon_2 = \frac{6}{5}$, $a_2 = [\varepsilon_2] = 1$ a $\varepsilon_3 = \frac{1}{\frac{6}{5} - 1} = \frac{5}{1} = a_3$

$$\frac{345}{113} = 3 + \frac{1}{18 + \frac{1}{1 + \frac{1}{5}}} = [3,18,1,5]$$

Postup Eukleidova algoritmu můžeme přeznačit příslušnými a_i a ε_i.

$$\frac{345}{113} = 3 + \frac{6}{113} \qquad \varepsilon_0 = a_0 + \frac{6}{113}$$

$$\frac{113}{6} = 18 + \frac{5}{6} \qquad \varepsilon_1 = a_1 + \frac{5}{6}$$

$$\frac{6}{5} = 1 + \frac{1}{5} \qquad \varepsilon_2 = a_2 + \frac{1}{5}$$

$$\frac{5}{1} = 5 + 0 \qquad \varepsilon_3 = a_3 + 0$$

Vidíme, že podle obecného popisu vpravo bychom mohli sestavit řetězový zlomek. Zkusme ještě jednou spočítat řetězový zlomek pomocí Euklidova algoritmu v následujícím příkladě.

Příklad 5.

Sestavte řetězový zlomek čísla $\frac{367}{235}$ za pomoci Euklidova algoritmu.

Řešení.

Proveďme algoritmus a pomocí návodu z předchozího příkladu doplňme čísla $a_0, a_1, \dots, a_k$ do řetězového zlomku.

$$367 = 235 \cdot 1 + 132$$

$$235 = 132 \cdot 1 + 103$$

$$132 = 103 \cdot 1 + 29$$

$$103 = 29 \cdot 3 + 16$$

$$29 = 16 \cdot 1 + 13$$

$$16 = 13 \cdot 1 + 3$$

$$13 = 3 \cdot 4 + 1$$

$$3 = 3 \cdot 1 + 0$$

Nyní sestavme řetězový zlomek.

$$\frac{367}{235} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{3}}}}}}}$$

Tento rozsáhlý zápis můžeme zkrátit do podoby posloupnosti a_i. Tedy: $\frac{367}{235} = [1,1,1,3,1,1,4,3]$.

Jelikož se snažíme o aproximaci iracionálních odmocnin, budou nás více zajímat řetězové zlomky iracionálních čísel.

2.2 Řetězové zlomky iracionálních čísel

Je-li α iracionální, pak je řetězový zlomek tohoto čísla nekonečný $\alpha = [a_0; a_1, a_2, \dots]$. (Manin a Panchishkin, 2005, s. 52). Jak můžeme vidět u řetězových zlomků racionálních čísel, pokud by iracionální číslo mělo konečný řetězový zlomek, dal by se upravit a iracionální číslo bychom mohli vyjádřit jako racionální zlomek, což je ve sporu s jeho iracionalitou.

Řetězové zlomky druhých odmocnin, kterými se zabýváme, se dají vypočítat bez předchozí znalosti přesné nebo přibližné hodnoty. Pro třetí odmocniny už je ale výpočet těžší a pro jiná

iracionální čísla, především ta transcendentní již potřebujeme kalkulačku. My se zabýváme pouze druhými odmocninami.

Příklad 6.

Spočtěte řetězové zlomky následujících odmocnin po a_4.

a) $\sqrt{3}$ b) $\sqrt{5}$ c) $\sqrt{7}$ d) $\sqrt{26}$

Řešení.

a) Odmocninu ohraničíme mezi dvě celá čísla vyjádřená jako odmocniny ze čtverců.

$$\sqrt{1} < \sqrt{3} < \sqrt{4}$$

$$1 < \sqrt{3} < 2$$

Nyní víme, že $\sqrt{3}$ leží mezi 1 a 2, tedy její celá část je 1. Necelou část zapíšeme jako $\sqrt{3} - 1$. Poté ji vyjádříme jako převrácenou hodnotu ve jmenovateli a upravíme tak, abychom ji mohli omezit celým číslem.

$$\sqrt{3} = 1 + \left(\sqrt{3} - 1\right) = 1 + \frac{1}{\frac{1}{\sqrt{3}-1}} =$$

$$= 1 + \frac{1}{\frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1}} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}}$$

Nyní budeme omezovat $\frac{\sqrt{3}+1}{2}$. Můžeme využít omezení $\sqrt{3}$ a postupně upravovat, dokud uprostřed nedostaneme kýžený tvar.

$$1 < \sqrt{3} < 2$$

$$2 < \sqrt{3} + 1 < 3$$

$$1 < \frac{\sqrt{3}+1}{2} < \frac{3}{2}$$

Výraz $\frac{\sqrt{3}+1}{2}$ se tedy pohybuje mezi 1 a 1,5 a jeho celou část tvoří 1. Necelou opět výjádříme jako rozdíl původního čísla a celé části, který můžeme rovnou vhodně upravit do jednoho zlomku. Ten jako v předchozím kroku vyjádříme jako převrácenou hodnotu ve jmenovateli, abychom ho mohli omezit nenulovým celým číslem. Za tímto účelem znovu rozšíříme a dále postupujeme v každém kroku analogicky.

$$\sqrt{3} = 1 + \frac{1}{1 + \left(\frac{\sqrt{3}+1}{2} - 1\right)} = 1 + \frac{1}{1 + \frac{\sqrt{3}-1}{2}} = 1 + \frac{1}{1 + \frac{1}{\frac{2}{\sqrt{3}-1}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{\frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1}}} = 1 + \frac{1}{1 + \frac{1}{\frac{2(\sqrt{3}+1)}{2}}} = 1 + \frac{1}{1 + \frac{1}{\sqrt{3}+1}}$$

$$2 < \sqrt{3} + 1 < 3$$

$$1 + \frac{1}{1 + \frac{1}{2+(\sqrt{3}+1-2)}} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{\frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1}}}} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{\frac{\sqrt{3}+1}{2}}}}$$

$$1 < \frac{\sqrt{3}+1}{2} < \frac{3}{2}$$

$$1 + \frac{1}{1 + \frac{1}{2+\frac{1}{\frac{\sqrt{3}+1}{2}}}} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\left(\frac{\sqrt{3}+1}{2}-1\right)}}} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{\sqrt{3}-1}{2}}}} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{1}{\frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1}}}}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{1}{\sqrt{3}+1}}}}$$

$$2 < \sqrt{3} + 1 < 3$$

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{1}{2+(\sqrt{3}+1-2)}}}} = [1; 1,2,1,2, \dots]$$

Dále bychom postupovali stejně, a to nejen stejným algoritmem, ale všimněme si, že třetí a čtvrtý krok jsou identické s prvním a druhým. Výpočet jednoho vždy vede na druhý, a tak by stejné byly i všechny další liché a sudé kroky.

b) Postup pro všechny další příklady je stejný jako v předchozím případě, proto zde budou uvedeny pouze výsledky s komentářem.

$$\sqrt{5} = 2 + \frac{1}{4 + \frac{1}{4+\frac{1}{4+\frac{1}{4+(\sqrt{5}+2-4)}}}} = [2; 4,4,4,4, \dots]$$

Zde byl postup ještě snazší než v a), protože výpočet druhého kroku byl stejný jako výpočet prvního a zacyklil se už na začátku.

c)

$$\sqrt{7} = 2 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{4+(\sqrt{7}+2-4)}}}} = [2; 1,1,1,4, \dots]$$

V tomto případě se zdálo, že se řetězový zlomek $\sqrt{7}$ zacyklí na samé 1. Ovšem v každém kroce vycházely různé výrazy, a proto se o zacyklení nejednalo, což také dokazuje číslo 4 ve čtvrtém kroku. Všimneme si ale, že výraz, který ve čtvrtém kroku zbyl, je stejný jako v kroku nultém, se kterým pak pracujeme v prvním kroku (výpočet a_1), a tak pátý krok bude identický s prvním a budou se opakovat čísla 1,1,1,4.

d)

$$\sqrt{26} = 5 + \cfrac{1}{10 + \cfrac{1}{10 + \cfrac{1}{10 + \cfrac{1}{10 + (\sqrt{26} + 5 - 10)}}}} = [5; 10,10,10,10, \dots]$$

Podobně jako v b), k zacyklení jsme se dostali už v prvním kroku.

Poznámka Na problém bychom mohli narazit, pokud by se mezi horní a dolní hranicí omezení nacházelo nějaké celé číslo, protože nevíme, kde přesně se mezi těmito hranicemi dané číslo nachází. Například:

$$2{,}75 = \frac{11}{4} < \frac{3\sqrt{5} + 5}{4} < \frac{14}{4} = 3{,}5$$

Nelze na první pohled určit, zda se číslo $\frac{3\sqrt{5}+5}{4}$ nachází před nebo za číslem 3, tedy jestli jeho celá část je 2 nebo 3. Existuje několik způsobů, jak tento problém případně vyřešit. První je, že budeme ekvivalentně upravovat následující nerovnost:

$$\frac{3\sqrt{5} + 5}{4} < 3$$

$$3\sqrt{5} < 7$$

Obě strany můžeme umocnit, protože jsou obě kladné.

$$45 < 49$$

Z čehož plyne, že výraz, který chceme omezit, je menší než tři a platí:

$$2{,}75 = \frac{11}{4} < \frac{3\sqrt{5} + 5}{4} < 3$$

A celá část $\frac{3\sqrt{5}+5}{4}$ je 2. Druhou metodou je zvolit číslo větší a pokračovat ve výpočtu. Pokud jsme číslo větší zvolili špatně, během následujícího kroku nám při úpravě necelé části vyjde záporné číslo. To poznáme, když budeme rozšiřovat. Necelá část kladného čísla by měla být

kladná a stejně tak i její převrácená hodnota. Pokud tuto převrácenou hodnotu vynásobíme během úpravy rozšiřováním jedničkou v jakémkoliv tvaru, zůstane nadále kladná.

$$\frac{3\sqrt{5}+5}{4}-3=\frac{3\sqrt{5}-7}{4}$$

$$\frac{4}{3\sqrt{5}-7}\cdot\frac{3\sqrt{5}+7}{3\sqrt{5}+7}=\frac{12\sqrt{5}+28}{45-49}=-3\sqrt{5}-7$$

Vychází číslo záporné, tedy musela být záporná již necelá část. Vidíme, že od původního čísla jsme odečetli příliš velké celé číslo, a výraz omezíme číslem menším. Ačkoliv je tento způsob o něco delší a musíme se v případě chyby vracet, jeho výhodou je, že nemusíme řešit žádné další nerovnosti a v případě správného odhadnutí můžeme pokračovat ve výpočtu. Tímto způsobem se také projeví, odhadneme-li nedopatřením celou část větším číslem. Pokud bychom odhadli číslo menší, bude „necelá“ část větší než jedna a její převrácená hodnota mezi nulou a jedničkou. Nepůjde tedy odhadnout nenulovým celým číslem.

Všimněme si, že řetězové zlomky všech odmocnin, které jsme počítali, jsou od určitého místa periodické. Konkrétně do periody nespadá celá část původní odmocniny a_0. Pro ostatní a_i platí, že $a_n = a_{n+l}$, kde l je délka periody (v kolikátém kroce se proces určování a_i zacyklí). Ve skutečnosti toto platí pro všechny odmocniny a všechna čísla, která jsou kořeny kvadratického polynomu. (Stein, 2017, s. 112)

Věta 6.

Nekonečný řetězový zlomek nějakého čísla α je periodický právě tehdy, když α je kořenem kvadratického polynomu. (Stein, 2017, s. 112)

Dokázat tuto vlastnost je poměrně složité a vyžaduje další poznatky z teorie těles. Důkaz pro čistě periodické řetězové zlomky lze nalézt například v *Elementary Number Theory: Primes, Congruents, and Secrets* od Williama Steina (2017) na stranách 112-114. Vítězslav Kala (2021) pak ve skriptech *Teorie čísel* na straně 15 důkaz rozšiřuje pro čísla, která čistě periodická nejsou (například naše odmocniny). S odkazem na důkazy považujme tvrzení o periodičnosti řetězových zlomků iracionálních odmocnin za pravdivé.

Periodické řetězové zlomky budeme značit podobně jako se značí periodický desetinný rozvoj, a to vodorovnou čarou nad čísly opakujícími se v periodě. Délku periody budeme

značit l a první číslo, které do periody nepatří, oddělíme středníkem. Řetězový zlomek například $\sqrt{7}$ pak vypadá následovně.

$$\sqrt{7} = [2; \overline{1,1,1,4}]$$

Obecně pak: $\sqrt{n} = [a_0; \overline{a_1, a_2, \dots a_l}]$.

Nyní umíme vytvořit řetězové zlomky iracionálních odmocnin a víme, že až na nultý člen jsou periodické. I pro čtvrtý krok je ale proces výpočtu časově náročný, pokud se brzy nezacyklí. Některé odmocniny mají výrazně delší periodu, viz následující tabulka, do které byly vybrány odmocniny s různou periodou.

n	Řetězový zlomek $\sqrt{n}$
22	$[4; \overline{1, 2, 4, 2, 1, 8}]$
31	$\left[5; \overline{1, 1, 3, 5, 3, 1, 1, 10}\right]$
61	$[7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$
67	$\left[8; \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}\right]$
76	$\left[8; \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}\right]$
94	$\left[9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}\right]$

Tab. 4: Řetězové zlomky iracionálních odmocnin (PrimeFan, 2013)

(vlastní zpracování)

Poznámka Všimněme si, jaké vzory se objevují v řetězových zlomcích iracionálních odmocnin krom periodicity. Vidíme, že poslední číslo periody se rovná dvojnásobku čísla a_0. Dále si můžeme všimnout, že čísla mezi a_0 a posledním číslem periody tvoří palindrom, tj. číslo, které je stejné, když ho čteme zleva i zprava. (Yang, 2008, s. 8)

Tvoření řetězových zlomků pro delší periody stále zůstává poněkud časově náročné. Z toho důvodu si představíme algoritmus, který nám umožní rychle a spolehlivě spočítat a_i řetězového zlomku dané odmocniny. Tento algoritmus bude především užitečný v další podkapitole, kde budeme potřebovat tato čísla k výpočtu tzv. sblížených zlomků.

Definice 8. Tennerův algoritmus

Tennerův algoritmus je algoritmus pro výpočet a_i řetězového zlomku $\sqrt{n}$. Mějme $k = \lfloor \sqrt{n} \rfloor$ celou část odmocniny z n a platí $n = k^2 + r$. Sestavíme tabulku o šesti sloupcích, první z nichž nám bude udávat hodnoty a_i.

I	II	III		IV	V	VI
k	$\times$	k	$=$	n	$-$	r
			…			
a	b	c		u	v	w
A	B	C		U	V	W

Každý další řádek pak získáme z předchozího pomocí následujících vztahů:

$$k + c = Aw + B, \text{ kde } 0 \leq B < w$$

$$C = k - B$$

$$U = C^2$$

$$V = n - U$$

$$W = \frac{V}{w}$$

(Barbeau, 2003, s. 69)

Vezměme jako příklad $\sqrt{19}$ $(n = 19)$. Nejprve najdeme celou část $k = \lfloor \sqrt{19} \rfloor$.

$$\sqrt{16} < \sqrt{19} < \sqrt{25}$$

$$4 < \sqrt{19} < 5$$

Z čehož plyne že $k = 4$ a $19 = 4^2 + 3$, tedy $r = 3$. Nyní můžeme sestrojit první řádek tabulky. Ačkoliv se jedná o první z řádků, dále mu budeme říkat nultý řádek, aby název korespondoval s nultým krokem výpočtu řetězového zlomku a indexem získaného a_0.

I	II	III		IV	V	VI
4	$\times$	4	$=$	19	$-$	3

Další řádky tvoříme podle výše definovaných vztahů. Nultý řádek také představuje hodnoty a, b, c, u, v, w, i když některé z hodnot obsazují operační znaménka. To ale nevadí, protože

konkrétní hodnoty b, v k výpočtu dalšího řádku nepotřebujeme. Pro výpočet A, B, C, U, V, W využijeme pouze $c = 4, w = 3$, čísla k a n jsou pevně dána na začátku. Platí tedy:

$$4 + 4 = A \cdot 3 + B$$

Zde se setkáváme s problémem dvou neznámých v jedné rovnici. Ten řeší omezení čísla B, $0 \leq B < w$. B je tedy rozhodně kladné a kdyby $A \cdot 3$ bylo větší než levá strana rovnice, nebylo by možné najít správné B tak, aby rovnice platila. Volíme proto největší A tak, aby $A \cdot 3 < 8$. Kdybychom zvolili číslo A příliš malé, také bychom nenašli v daném omezení vhodné B. Dalo by se také obecně napsat:

$$A = \max\{x \in \mathbb{N}, w \cdot x < k + c\}$$

Rozdíl, který je jistě menší než $w = 3$ je B. B se tedy dá obecně vyjádřit jako:

$$k + c - A \cdot w = B$$

Jedná se o prostou úpravu původní rovnice, ovšem nyní máme dané A. Obě čísla jsou tímto dána jednoznačně. Je možné, že nastane situace, kdy existuje takové A, že $A \cdot w = k + c$, pak z vyjadření B vyplývá, že B je nula, což omezení dovoluje. V našem případě máme tedy následující rovnost.

$$8 = 2 \cdot 3 + 2$$

Získali jsme $A = 2$ a $B = 2$ a můžeme počítat dále.

$$C = 4 - 2 = 2$$

$$U = 2^2 = 4$$

$$V = 19 - 4 = 15$$

$$W = \frac{15}{3} = 5$$

Máme všechny hodnoty pro sestavení „prvního“ řádku (druhého řádku tabulky).

I	II	III		IV	V	VI
4	×	4	=	19	−	3
2	2	4		4	15	5

Čísla v novém řádku se stávají malými a, b, c, u, v, w a hledáme stejně jako v předchozím kroce čísla A, B, C, U, V, W nového řádku a tak dále tolikrát, kolikrát potřebujeme.

Příklad 7.

Spočtěte Tennerovým algoritmem a_0, a_1, a_2 a a_4 řetězového zlomku čísla $\sqrt{11}$.

Řešení.

Postup je stejný jako ve vzorovém příkladě s $\sqrt{19}$, proto zde bude uvedna pouze výsledná tabulka pro kontrolu.

I	II	III		IV	V	VI
3	×	3	=	11	−	2
3	0	3		9	2	1
6	0	3		9	2	2
3	0	3		9	2	1

Všimneme si, že periodičnost řetězových zlomků odmocnin se projevuje i zde. Jak je vidno, první a třetí řádek a druhý a čtvrtý řádek jsou stejné. Do výpočtu dalšího řádku vstupují pouze čísla c, w a k, n, která se od prvního řádku opakují s periodou 2. Můžeme tedy rovnou zapsat celý řetězový zlomek $\sqrt{11}$ pomocí periody.

$$\sqrt{11} = [3; \overline{3,6}]$$

Nyní máme poměrně rychlou metodu pro vytvoření řetězového zlomku iracionálních odmocnin. Nás ovšem nebude zajímat řetězový zlomek jako celek, ale budeme zkoumat pouze části, kterým budeme říkat sblížené zlomky.

2.3 Sblížené zlomky

Pokud chceme vyjádřit iracionální číslo pomocí řetězových zlomků, početně ani graficky nám to nepomůže. Stále se jedná o nekonečný, a tím pádem i neproveditelný zápis. Můžeme tedy jako aproximaci daného čísla konkrétní řetězový zlomek v určitém kroku utnout.

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}} \approx 1 + \frac{1}{2 + \frac{1}{2}}$$

Takovému utnutému zlomku říkáme sblížený zlomek. Ten pak můžeme upravit a vyjde nám zlomek v základním tvaru, který aproximuje, v tomto případě, $\sqrt{2}$.

$$1 + \frac{1}{1 + \frac{1}{2}} = \frac{7}{5} = 1{,}4$$

Neformálně můžeme říci, že jednotlivé sblížené zlomky aproximují dané číslo, protože z něj okrajujeme pouze malé části. Zároveň s každým dalším sblíženým zlomkem (který utneme později) se zmenšuje část, kterou vynecháváme, přesnost aproximace zvětšuje a blížíme se původnímu číslu. Proto se sblíženým zlomkům také někdy říká konvergenty (angl. convergents). V této práci bude používán pojem sblížené zlomky, převzatý ze skript Vítězslava Kaly (2021). Formálně definujeme sblížené zlomky následovně.

Definice 9. Sblížený zlomek

Mějme $\alpha \in \mathbb{R}$, $\alpha = [a_0; a_1, \dots, a_k\,]$. Řetězovému zlomku $[a_0, ; a_1, \dots, a_m\,]$, kde $m \leq k$, říkáme m-tý sblížený zlomek čísla α. Dále definujeme posloupnosti p_m a q_m následujícím rekurzivním předpisem.

$$p_{-1} = 1, p_0 = a_0;\ p_m = a_m p_{m-1} + p_{m-2}$$

$$q_{-1} = 0, q_0 = 1;\ q_m = a_m q_{m-1} + q_{m-2}$$

V následující větě dokážeme, že takto definované posloupnosti dávají zlomky $\frac{p_m}{q_m}$, které odpovídají řetězovým zlomkům $[a_0, ; a_1, \dots, a_m\,]$. (Yang, 2008, s. 1)

Věta 7.

Pro p_m, q_m definovaná výše rekurzivním předpisem, platí, že $\frac{p_m}{q_m} = [a_0; a_1, \dots, a_m\,]$.

Důkaz.

Důkaz provedeme matematickou indukcí. Uvažujme nejprve $\alpha = [a_0, ; a_1]$ $(m = 1)$.

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1}$$

Nyní dosadíme podle definice $p_{-1} = 1, p_0 = a_0, q_{-1} = 0$ a $q_0 = 1$.

$$\frac{a_1 a_0 + 1}{a_1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{p_1}{q_1}$$

První krok máme. Předpokládejme tedy, že věta platí pro nějaké m a budeme řešit, zda pak platí také pro $m+1$. Mějme tedy $[a_0; a_1, \dots, a_m]$;

$$[a_0; a_1, \dots, a_m, a_{m+1}] = \left[a_0; a_1, \dots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right]$$

Vyjádřili jsme $[a_m, a_{m+1}]$ jako jeden člen $"a_m" = a_m + \frac{1}{a_{m+1}}$, tím pádem máme $[a_0; a_1, \dots, "a_m"]$, kde m-tý člen obsahuje i $m+1$ člen. Můžeme nyní aplikovat poznatek z prvního kroku.

$$\left[a_0; a_1, \dots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) \cdot p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) \cdot q_{m-1} + q_{m-2}}$$

Toto vyjádření je hlavní myšlenka důkazu. Odtud dále se jedná pouze o algebraické úpravy. Upravíme výraz na pravé straně. Nejprve v čitateli i jmenovateli převedeme sčítance na stejného jmenovatele a_{m+1}. Protože horní i dolní zlomek budou mít stejný jmenovatel, tyto jmenovatele se pokrátí.

$$\frac{\left(a_m + \frac{1}{a_{m+1}}\right) \cdot p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) \cdot q_{m-1} + q_{m-2}} = \frac{\frac{a_m \cdot a_{m+1} \cdot p_{m-1} + p_{m-1} + a_{m+1} \cdot p_{m-2}}{a_{m+1}}}{\frac{a_m \cdot a_{m+1} \cdot q_{m-1} + q_{m-1} + a_{m+1} \cdot q_{m-2}}{a_{m+1}}}$$

$$= \frac{a_m \cdot a_{m+1} \cdot p_{m-1} + p_{m-1} + a_{m+1} \cdot p_{m-2}}{a_m \cdot a_{m+1} \cdot q_{m-1} + q_{m-1} + a_{m+1} \cdot q_{m-2}}$$

V dalším kroku vytkneme a_{m+1} a poté dosadíme podle definice v čitateli $p_m = a_m p_{m-1} + p_{m-2}$ a jmenovateli $q_m = a_m q_{m-1} + q_{m-2}$.

$$\frac{a_{m+1} \cdot (a_m \cdot p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1} \cdot (a_m \cdot q_{m-1} + q_{m-2}) + q_{m-1}} = \frac{a_{m+1} \cdot p_m + p_{m-1}}{a_{m+1} \cdot q_m + q_{m-1}} = \frac{p_{m+1}}{q_{m+1}}$$

Čímž jsme dokázali, že $[a_0; a_1, \dots, a_m, a_{m+1}] = \frac{p_{m+1}}{q_{m+1}}$. (Yang, 2008, s. 2) ■

Získali jsme nástroj, jak efektivně počítat sblížené zlomky. Čísla $a_0, a_1, \dots, a_m$ získáme Tennerovým algoritmem definovaným v předchozí podkapitole a následně z rekurzivních vztahů vypočteme kýžený sblížený zlomek.

Příklad 8.

Spočtěte m-tý sblížený zlomek následujících čísel. Postupujte metodou rekurze (nikoliv spočtení utnutého zlomku).

a) $m = 3$, $\alpha = \sqrt{2}$ b) $m = 4$, $\alpha = \sqrt{11}$ c) $m = 7$, $\alpha = \sqrt{23}$ d) $m = 9$, $\alpha = \sqrt{13}$

Řešení.

Nejprve sestavíme řetězový zlomek daného čísla až po a_m, protože jako součást rekurzivního vzorce pro výpočet p_m, q_m jsou potřeba čísla $a_0, a_1, \dots, a_m$. Poté budeme dle definice sestavovat sblížené zlomky a z nich pomocí rekurze další.

a) $m = 3, \alpha = \sqrt{2}$

Použijeme Tennerův algoritmus, abychom spočetli potřebné členy řetězového zlomku. Podrobný návod, jak toto provést, najdeme v předchozí podkapitole a jelikož se jedná o mechanický postup, bude zde uveden pouze výsledek.

$$\sqrt{2} = [1; \overline{2}]$$

Máme: $p_{-1} = 1,\ p_0 = a_0$ a $q_{-1} = 0, q_0 = 1$ a vycházíme z rekurzivního vzorce z definice sblíženého zlomku.

$$\frac{p_0}{q_0} = \frac{a_0 = 1}{1} \to \frac{p_1}{q_1} = \frac{2 \cdot 1 + 1}{2 \cdot 1 + 0} = \frac{3}{2} \to \frac{p_2}{q_2} = \frac{2 \cdot 3 + 1}{2 \cdot 2 + 1} = \frac{7}{5} \to \frac{p_3}{q_3} = \frac{2 \cdot 7 + 3}{2 \cdot 5 + 2} = \frac{17}{12}$$

Výsledek tedy je $\frac{p_3}{q_3} = \frac{17}{12}$.

b) $m = 4, \alpha = \sqrt{11}$

Postupujeme stejně jako v a) tím, že začneme určením potřebných a_i.

$$\sqrt{11} = [3; \overline{3,6}]$$

Máme: $p_{-1} = 1,\ p_0 = a_0$ a $q_{-1} = 0, q_0 = 1$

$$\frac{p_0}{q_0} = \frac{a_0 = 3}{1} \to \frac{p_1}{q_1} = \frac{3 \cdot 3 + 1}{3 \cdot 1 + 0} = \frac{10}{3} \to \frac{p_2}{q_2} = \frac{6 \cdot 10 + 3}{6 \cdot 3 + 1} = \frac{63}{19} \to \frac{p_3}{q_3} = \frac{3 \cdot 63 + 10}{3 \cdot 19 + 3}$$
$$= \frac{199}{60} \to \frac{p_4}{q_4} = \frac{6 \cdot 199 + 63}{6 \cdot 60 + 19} = \frac{1257}{379}$$

c) $m = 7, \alpha = \sqrt{23}$

$$\sqrt{23} = [4; \overline{1,3,1,8}]$$

$p_{-1} = 1,\ p_0 = a_0$ a $q_{-1} = 0, q_0 = 1$

$$\frac{p_0}{q_0} = \frac{a_0 = 4}{1} \to \frac{p_1}{q_1} = \frac{1 \cdot 4 + 1}{1 \cdot 1 + 0} = \frac{5}{1} \to \frac{p_2}{q_2} = \frac{3 \cdot 5 + 4}{3 \cdot 1 + 1} = \frac{19}{4} \to \frac{p_3}{q_3} = \frac{1 \cdot 19 + 5}{1 \cdot 4 + 1}$$

$$= \frac{24}{5} \to\to \frac{p_4}{q_4} = \frac{8 \cdot 24 + 19}{8 \cdot 5 + 4} = \frac{211}{44} \to \frac{p_5}{q_5} = \frac{1 \cdot 211 + 24}{1 \cdot 44 + 5} = \frac{235}{49} \to \frac{p_6}{q_6}$$
$$= \frac{3 \cdot 235 + 211}{3 \cdot 49 + 44} = \frac{916}{191} \to \frac{p_7}{q_7} = \frac{1 \cdot 916 + 235}{1 \cdot 191 + 49} = \frac{1151}{240}$$

d) $m = 9, \alpha = \sqrt{13}$

$$\sqrt{13} = [3; \overline{1,1,1,1,6}]$$

$p_{-1} = 1,\ p_0 = a_0$ a $q_{-1} = 0, q_0 = 1$

$$\frac{p_0}{q_0} = \frac{a_0 = 3}{1} \to \frac{p_1}{q_1} = \frac{1 \cdot 3 + 1}{1 \cdot 1 + 0} = \frac{4}{1} \to \frac{p_2}{q_2} = \frac{1 \cdot 4 + 3}{1 \cdot 1 + 1} = \frac{7}{2} \to \frac{p_3}{q_3} = \frac{1 \cdot 7 + 4}{1 \cdot 2 + 1} = \frac{11}{3}$$
$$\to \frac{p_4}{q_4} = \frac{1 \cdot 11 + 7}{1 \cdot 3 + 2} = \frac{18}{5} \to \frac{p_5}{q_5} = \frac{6 \cdot 18 + 10}{6 \cdot 5 + 3} = \frac{119}{33} \to \frac{p_6}{q_6} = \frac{1 \cdot 119 + 18}{1 \cdot 33 + 5} = \frac{137}{38}$$
$$\to \frac{p_7}{q_7} = \frac{1 \cdot 137 + 119}{1 \cdot 38 + 33} = \frac{256}{71} \to \frac{p_8}{q_8} = \frac{1 \cdot 256 + 137}{1 \cdot 71 + 38} = \frac{393}{109} \to$$
$$\to \frac{p_9}{q_9} = \frac{1 \cdot 393 + 256}{1 \cdot 109 + 71} = \frac{649}{180}$$

Procvičili jsme počítání sblížených zlomků a umíme tedy tvořit různé aproximace $\sqrt{n}$. Všimněme si, že v případě a) se mezi sblíženými zlomky objevila řešení Pellovy rovnice. Konkrétně $\frac{p_1}{q_1} = \frac{3}{2}$, $\frac{p_3}{q_3} = \frac{17}{12}$. A kdybychom hledali dál, zjistili bychom, že všechny liché sblížené zlomky nám dávají řešení Pellovy rovnice. Všechny sudé sblížené zlomky pak řeší Pellovu rovnici negativní. Je otázkou, jak je to s ostatními odmocninami. Jako další příklad dosadíme jednotlivé sblížené zlomky, které vyšly v příkladě 6 do Pellovy rovnice a budeme pozorovat, jaké výsledky nám budou vycházet. Vytvoříme tabulky, které vypadají následovně.

$\sqrt{2}$ pro $m = 0$ až $m = 3$

m	$(p_m; q_m)$	${p_m}^2 - 2 \cdot {q_m}^2$
0	$(1; 1)$	-1
1	$(3; 2)$	1

2	$(7;5)$	-1
3	$(17;12)$	1

Tab. 5

(vlastní zpracování)

První řádek určuje m, druhý řádek obsahuje čitatele a jmenovatele příslušných sblížených zlomků ve tvaru řešení Pellovy rovnice $(x;y)$, kde p_m přísluší x a q_m přísluší y. Poslední, třetí řádek, pak udává hodnoty na pravé straně Pellovy rovnice.

Jak jsme vypozorovali již dříve, protože některá řešení pro $n = 2$ známe, řešení Pellovy rovnice se nacházejí na lichých místech a na sudých místech se nacházejí řešení negativní Pellovy rovnice. Všechny liché sblížené zlomky můžeme popsat jako $\frac{p_m}{q_m}, m = k \cdot 2 - 1$, kde $k \in \mathbb{N} \setminus \{0\}$. Zatím se jedná pouze o pozorování. Poté, co naše pozorování doplníme o další příklady, zformulujeme tvrzení.

Příklad 9.

Vytvořte tabulku pro ostatní odmocniny a jejich sblížené zlomky z příkladu 6. Věnujte přitom pozornost, zda a na jakých pozicích (pro jaká m) se objeví řešení Pellovy rovnice.

a) $\sqrt{11}$ b) $\sqrt{23}$ c) $\sqrt{13}$

Řešení.

a) $\sqrt{11}$

Během výpočtu čtvrtého sblíženého zlomku jsme zároveň dostali všechny předchozí sblížené zlomky, takže stačí pouze zapsat a dosadit do Pellovy rovnice.

m	$(p_m; q_m)$	${p_m}^2 - 11 \cdot {q_m}^2$
0	$(3;1)$	-2
1	$(10;3)$	1
2	$(63;19)$	-2
3	$(199;60)$	1

4	$(1257; 379)$	-2

Tab. 6

(vlastní zpracování)

Pozorujeme, že zde opět řešení Pellovy rovnice dávají liché sblížené zlomky $\frac{p_m}{q_m}, m = k \cdot 2 - 1$, kde $k \in \mathbb{N} \setminus \{0\}$.

b) $\sqrt{23}$

Stejně jako v případě a) či vzorovém příkladu dosadíme sblížené zlomky, které nám vyšly do Pellovy rovnice. Proto budou dále uvedeny pouze výsledné tabulky a komentář.

m	$(p_m; q_m)$	${p_m}^2 - 23 \cdot {q_m}^2$
0	$(4; 1)$	-7
1	$(5; 1)$	2
2	$(19; 4)$	-7
3	$(24; 5)$	1
4	$(211; 44)$	-7
5	$(235; 49)$	2
6	$(916; 191)$	-7
7	$(1151; 240)$	1

Tab. 7

(vlastní zpracování)

Řešení se objevila na čtvrtém ($m = 3$) a osmém ($m = 7$) řádku. Předpokládejme stejně jako v předchozích případech, že takto se budou řešení vyskytovat pravidelně. To můžeme popsat jako všechna $\frac{p_m}{q_m}, m = k \cdot 4 - 1$, kde $k \in \mathbb{N} \setminus \{0\}$.

c) $\sqrt{13}$

m	$(p_m; q_m)$	${p_m}^2 - 13 \cdot {q_m}^2$
0	$(3; 1)$	-4
1	$(4; 1)$	3
2	$(7; 2)$	-3
3	$(11; 3)$	4
4	$(18; 5)$	-1
5	$(119; 33)$	4
6	$(137; 38)$	-3
7	$(256; 71)$	3
8	$(393; 109)$	-4
9	$(649; 180)$	1

Tab. 8

(vlastní zpracování)

V tomto případě se vyskytlo pouze jedno řešení na desátém řádku ($m = 9$), čímž jsme vyřešili problém, který nás provázel již od první kapitoly. Předpokládejme tedy znovu, že se bude vyskytovat pravidelně na každém desátém řádku ($m = 9, 19, 29, ...$) a zapišme všechny zlomky, které řeší Pellovu rovnici jako $\frac{p_m}{q_m}, m = k \cdot 10 - 1$, kde $k \in \mathbb{N} \setminus \{0\}$.

Shrňme a porovnejme naše pozorování. Pro $\sqrt{2}$ najdeme řešení jako $2 \cdot k - 1$-ní sblížené zlomky, tedy každý **druhý** sblížený zlomek. Pro $\sqrt{11}$ řešení také dává každý **druhý** sblížený zlomek. Pro $\sqrt{23}$ nacházíme řešení jako $4 \cdot k - 1$-ní, tedy každý **čtvrtý** sblížený zlomek, a pro $\sqrt{13}$ jako $10 \cdot k - 1$-ní, tedy každý **desátý** sblížený zlomek.

Když porovnáme zvýrazněná čísla s délkami period (značíme l) řetězových zlomků příslušných odmocnin, najdeme jistou spojitost. Platí: $\sqrt{2}: l = 1, \sqrt{11}: l = 2, \sqrt{23}: l = 4, \sqrt{13}: l = 5$. Zjistíme, že pro $\sqrt{11}$ a $\sqrt{23}$ se řešení Pellovy rovnice opakují se stejnou periodou (ovšem začínáme od $m = 0$, proto ne $k \cdot l$ ale $k \cdot l - 1$) a pro $\sqrt{2}$ a $\sqrt{13}$

s dvojnásobnou periodou (opět, kvůli $m = 0,\ 2 \cdot l \cdot k - 1$). Na čem tento rozdíl závisí? Jinými slovy, co mají společného $\sqrt{11}$ a $\sqrt{23}$ a co $\sqrt{2}$ a $\sqrt{13}$? Zjistíme, že řetězové zlomky prvních dvou odmocnin mají sudou periodu a zbylých dvou mají lichou. Nyní můžeme naše pozorování zformulovat do tvrzení o závislosti m, pro která $\frac{p_m}{q_m}$ řeší Pellovu rovnici na periodě dané odmocniny.

Tvrzení 8.

Mějme $\sqrt{n} = [a_0; \overline{a_1, a_2, .., a_{l-1}}]$ s periodou l. Pak $(p_m; q_m)$ řeší Pellovu rovnici

$x^2 - n \cdot y^2 = 1$ právě tehdy, když $m = k \cdot l - 1$, pokud l je sudé nebo $m = 2 \cdot l \cdot k - 1$, pokud l je liché ($k \in \mathbb{N} \setminus \{0\}$). (Yang, 2008, s. 12)

Důkaz tohoto tvrzení je složitý a vyžaduje další technické poznatky o vlastnostech řetězových a sblížených zlomků, které jsme zde neuváděli. Poměrně kompletní důkaz poskytuje Yang (2008) ve svém textu *Continued Fractions and Pell's Equation* na stranách 10-12. Kala (2021) i další autoři toto tvrzení uvádí bez důkazu a takto bude uvedeno i zde.

S posledním tvrzením máme kompletní návod, jak hledat řešení Pellovy rovnice, a to jako sblížené zlomky, jejichž index závisí na délce periody l řetězového zlomku dané odmocniny. Můžeme tak uzavřít kapitolu o hledání řešení a podívat se, jakou strukturu množina řešení tvoří. Ačkoliv jsme schopni jakékoliv řešení najít pomocí sblížených zlomků, existuje snazší způsob, který nám odhalí prozkoumání struktury řešení.

3 Struktura řešení Pellovy rovnice a obory $\mathbb{Z}[\sqrt{n}]$

Už z první kapitoly víme, že pro každou Pellovu rovnici je množina netriviálních řešení neprázdná. Nejprve si definujeme reprezentaci řešení Pellovy rovnice pomocí prvků číselného oboru $\mathbb{Z}[\sqrt{n}]$ (viz Definice 15), aby se nám s nimi lépe pracovalo a mohli jsme mezi nimi provádět operace. V následujících tvrzeních si pak ukážeme, že je takto definovaná množina uzavřená na násobení, protože součin dvou řešení (ne nutně různých), je také řešením. Pokud tedy máme jedno řešení, které nám věta 2 zaručuje, můžeme pomocí něj vygenerovat nekonečně mnoho řešení, které budou v podobě mocnin tohoto řešení. To ale nabádá k zamyšlení. Co kdybychom měli jako původní řešení takové, které už mocninou nějakého řešení je? Proto dokážeme, že na množině řešení lze definovat ostré uspořádání a zjistíme, že existuje tzv. minimální nebo fundamentální řešení. To najdeme jako první ze sblížených zlomků, které jsou řešeními, tedy pro $k = 1$. Všechna řešení jsou potom mocniny právě tohoto minimálního řešení. Tento způsob generování řešení je jednodušší než počítat jednotlivé sblížené zlomky.

Na závěr si ukážeme, že množina řešení reprezentované prvky $\mathbb{Z}[\sqrt{n}]$ tvoří s operací násobení tzv. cyklickou grupu. Budeme muset kladná řešení, která jsme doposud uvažovali, rozšířit o řešení tvaru $x - y\sqrt{n}$ pro existenci inverzního prvku a triviální řešení $(1; 0)$ pro existenci neutrálního prvku. Dokážeme, že taková množina s operací násobení splňují všechny vlastnosti cyklické grupy.

3.1 Minimální řešení

Jak je zmíněno v úvodu kapitoly, vyjádření pomocí prvků $\mathbb{Z}[\sqrt{n}]$ nám umožní popsat strukturu a skýtá užitečné vlastnosti. Konkrétně například tu, že všechna kladná řešení jsou mocninou nějakého minimálního řešení, kterému se někdy říká fundamentální. Později si je definujeme formálně. Prozatím mějme představu, že se jedná o řešení s nejmenším jmenovatelem (dokážeme si také, že má i nejmenšího čitatele a řešení lze řadit podle obojího), které není triviální. Vcelku paradoxně je zlomek $\frac{x}{y}$ vytvořený z minimálního řešení největší ze zlomků a nejhruběji aproximuje danou odmocninu. Proto je příhodnější

tomuto řešení říkat fundamentální, což také znamená základní, jelikož tvoří základ pro všechna ostatní řešení. Protože ale budeme toto řešení definovat jako minimum množiny řešení uspořádané podle velikosti x, zůstaneme u přízviska minimální.

Zavedeme nové vyjádření řešení Pellovy rovnice a dokážeme, že lze kladná řešení Pellovy rovnice ostře uspořádat. Tak budeme moci definovat minimální řešení.

Definice 10. Řešení jako prvky $\mathbb{Z}[\sqrt{n}]$

Řekneme, že $x + y\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ je řešením Pellovy rovnice právě tehdy, když platí $x^2 - ny^2 = 1$. (Dudley, 2009, s. 91)

Nyní tedy budeme řešení $(x; y)$ reprezentovat iracionálním číslem ve tvaru $x + y\sqrt{n}$.

Tvrzení 9.

Mějme dvě řešení (x_1, y_1) a (x_2, y_2), $x_1, y_1, x_2, y_2 > 0$. Platí, že $x_1 + y_1\sqrt{\mathrm{n}} < x_2 + y_2\sqrt{\mathrm{n}}$ právě tehdy, když $x_1 < x_2$ (resp. $y_1 < y_2$).

Důkaz.

Pro důkaz první implikace zleva doprava budeme předpokládat, že $x_1 < x_2$. Tím pádem platí také $x_1^2 < x_2^2$, protože x_1, y_1 uvažujeme kladná. Nyní vyjádříme x_1^2, resp. x_2^2 z Pellovy rovnice a provedeme substituci.

$$x_1^2 < x_2^2$$
$$x_1^2 = 1 + ny_1^2$$
$$x_2^2 = 1 + ny_2^2$$
$$1 + ny_1^2 < 1 + ny_2^2$$

Z toho po úpravě vyplývá, že $y_1 < y_2$. Jinými slovy, pokud je x_1 menší než x_2, pak i y_1 je menší než y_2. To platí i obráceně, tedy: $y_1 < y_2$, pak $x_1 < x_2$. Tuto implikaci je snadné dokázat. Postup je stejný, jen vyjadřujeme příslušné y^2.

$$y_1 < y_2 \Rightarrow y_1^2 < y_2^2$$
$$y_1^2 = \frac{1 - x_1^2}{n}$$

$$y_2^2 = \frac{1 - x_2^2}{n}$$

$$\frac{1 - x_1^2}{n} < \frac{1 - x_2^2}{n}$$

Opět po příslušných úpravách dostaneme $x_1^2 < x_2^2$, a tedy $x_1 < x_2$.

Protože k menšímu x_1 přičítáme menší y_1-násobek $\sqrt{n}$, je $x_1 + y_1\sqrt{n}$ menší než $x_2 + y_2\sqrt{n}$.

Opačnou implikaci dokážeme sporem. Předpokládejme, že $x_1 + y_1\sqrt{n} < x_2 + y_2\sqrt{n}$ a zároveň $x_1 \geq x_2$. Stejnými upravami jako v předchozím odstavci dostaneme, že $y_1 \geq y_2$ a $x_1 + y_1\sqrt{n} \geq x_2 + y_2\sqrt{n}$, což je ve sporu s předpokladem, a musí platit, že $x_1 < x_2$.

V předpokladu můžeme zaměnit libovolně x a y. My budeme uvažovat řazení podle x. (Dudley, 2009, s. 92) ■

Definice 11. Minimální řešení

Ukázali jsme, že kladná řešení $x_k + y_k\sqrt{n}$ lze seřadit podle x_k. Jelikož se jedná o neprázdnou množinu přirozených x_k, má tato množina minimum. Toto nejmenší řešení nazveme minimální řešení. (Dudley, 2009, s. 93)

Poznámka Bavíme se o kladných řešeních Pellovy rovnice, mezi které nepočítáme triviální řešení $(1; 0)$, jehož y-ová složka je pouze nezáporná.

Jak je předesláno v úvodu kapitoly, nejdůležitější vlastností minimálního řešení je, že generuje všechna ostatní řešení. Množinu řešení tedy tvoří mocniny tohoto minimálního řešení, které funguje jako generátor, jak si brzy dokážeme. S operací násobení množina řešení tvoří strukturu, kterou popíšeme v následující podkapitole.

3.2 Grupa řešení

Struktura množiny řešení je v úvodu této kapitoly popsána jako cyklická grupa. Nejprve si zadefinujeme, co to cyklická grupa je, a pak ukážeme, že množina řešení dané Pellovy

rovnice, kterou označíme M (obsahující kladná řešení, řešení se záporným y a triviální řešení $(1; 0)$ reprezentované jako $1 + 0\sqrt{n} = 1$), splňuje s násobením nutné vlastnosti, aby byla právě cyklickou grupou. Mezi těmito vlastnostmi je nejdůležitější uzavřenost na násobení, tedy že součin dvou řešení je opět řešení a že mocniny minimálního řešení jsou právě všechna řešení z množiny M.

Definice 12. Grupa a cyklická grupa

Grupa je dvojice $(G,*)$, tvořená neprázdnou množinou G a binární operací $*$ definovanou na množině G, pro kterou platí následující vlastnosti.

a) Je asociativní, tj. $\forall a, b, c \in G: a * (b * c) = (a * b) * c$
b) Existuje vůči ní neutrální prvek $e \in G$, takový, že $\forall a \in G: a * e = e * a = a$
c) Ke každému prvku existuje inverzní prvek a^{-1}, tj. $\forall a \in G\ \exists a^{-1} \in G, a * a^{-1} = a^{-1} * a = e$

Grupu G nazveme cyklickou grupou, pokud existuje nějaký prvek $a \in G, G = \{a^n, n \in \mathbb{Z}\}$, tedy takový prvek, který generuje celou grup G. (Stanovský, 2010, s. 64, 71)

Poznámka V definici nechápejme a^n jako klasickou mocninu vzhledem k násobení. Jedná se o $(n-1)$-krát provedenou operaci $*$ na prvku a, tedy $a * a * a \ldots * a$, kde se operace $*$ vyskytuje právě $(n-1)$-krát. My se ovšem zabýváme operací násobení a volíme multiplikativní zápis grupy. Při použití operace násobení na n stejných prvků a mluvíme o n-té mocnině prvku a.

Definice 13. Množina řešení *M*

Množinou řešení M rozumíme množinu $\{x_k \pm y_k\sqrt{n}, k \in \mathbb{N}: {x_k}^2 - n{y_k}^2 = 1\}$. Triviálnímu $1 \pm 0\sqrt{n}$ zde odpovídá $x_0 \pm y_0\sqrt{n}$.

Nejprve dokažme existenci neutrálního prvku a inverzního prvku. Neutrální prvek nám motivuje zařazení $1 + 0\sqrt{n}$ do množiny M, inverzní prvek pak motivuje zahrnutí $x_k - y_k\sqrt{n}$.

Tvrzení 10.

V množině M existuje prvek e takový, že

$$e \cdot \left(x_k \pm y_k\sqrt{n}\right) = \left(x_k \pm y_k\sqrt{n}\right) \cdot e = x_k \pm y_k\sqrt{n}, k \in \mathbb{N}$$

Důkaz. Protože množinu M jsme definovali tak, že obsahuje triviální řešení $1 + 0\sqrt{n}$, platí, že $1 + 0\sqrt{n} = 1 \in M$. A tedy:

$$1 \cdot \left(x_k \pm y_k\sqrt{n}\right) = \left(x_k \pm y_k\sqrt{n}\right) \cdot 1 = x_k \pm y_k\sqrt{n} \text{ pro všechna } k \in \mathbb{N}.$$

(Stillwell, 2003, s. 82) ■

Tvrzení 11.

Pro každý prvek z množiny M existuje inverzní prvek**.**

$$\forall x_k \pm y_k\sqrt{n} \in M \; \exists \left(x_k \pm y_k\sqrt{n}\right)^{-1} \in M,$$

$$\left(x_k \pm y_k\sqrt{n}\right) \cdot \left(x_k \pm y_k\sqrt{n}\right)^{-1} = \left(x_k \pm y_k\sqrt{n}\right)^{-1} \cdot \left(x_k \pm y_k\sqrt{n}\right) = 1$$

Důkaz. Rozdělíme si případ na $x_i + y_i\sqrt{n}$ a $x_k - y_k\sqrt{n}$. Jednoduchou úpravou získáme:

$$\left(x_k + y_k\sqrt{n}\right)^{-1} = \frac{1}{x_k + y_k\sqrt{n}}$$

Dokážeme, že pro všechna $x_k + y_k\sqrt{n}$ platí, že $\frac{1}{x_k + y_k\sqrt{n}}$ je také řešením.

$$\frac{1}{x_k + y_k\sqrt{n}} = \frac{1}{x_k + y_k\sqrt{n}} \cdot \frac{x_k - y_k\sqrt{n}}{x_k - y_k\sqrt{n}} = \frac{x_k - y_k\sqrt{n}}{{x_k}^2 - n{y_k}^2}$$

Protože $(x_i; y_i)$ je řešení Pellovy rovnice, platí, že ${x_k}^2 - n{y_k}^2 = 1$ a tedy:

$$\left(x_k + y_k\sqrt{n}\right)^{-1} = \frac{1}{x_k + y_k\sqrt{n}} = \frac{x_k - y_k\sqrt{n}}{1} = x_k - y_k\sqrt{n}$$

Z této rovnosti hned vyplývá, že $\left(x_k - y_k\sqrt{n}\right)^{-1} = \frac{1}{x_k - y_k\sqrt{n}} = \frac{x_k + y_k\sqrt{n}}{1} = x_k + y_k\sqrt{n}$. Prvky $x_k + y_k\sqrt{n}$ a $x_k - y_k\sqrt{n}$ jsou si tedy navzájem inverzní. Všimněme si, že pro $1 + 0\sqrt{n}$ platí:

$$1 + 0\sqrt{n} = 1 - 0\sqrt{n}$$

Neutrální prvek je tedy inverzní sám k sobě. (Dudley, 2009, s. 92) ■

Nyní dokážeme, že součin řešení je opět řešením. Je to vlastnost, která je požadována, aby $(M,\cdot)$ byla grupa. Tento požadavek se v definici grupy skrývá ve formulaci, že $*$ je **na** množině G. Chceme tedy ukázat, že násobení je operace na množině M; jinými slovy, chceme dokázat, že M je uzavřená vůči operaci násobení.

Tvrzení 12.

Když $(x_1; y_1)$ a $(x_2; y_2)$ jsou řešení, pak $(x_3; y_3)$, takové, že:

$$(x_3; y_3) = (x_1x_2 + ny_1\,y_2; x_1y_2 + y_1x_2)$$

je také řešení. (Stillwell, 2003, s. 82)

Důkaz. Důkaz provedeme jako cvičení. ■

Příklad 10.

Dokažte tvrzení 12.

Řešení.

Využijeme toho, že jak ${x_1}^2 - n{y_1}^2$, tak ${x_2}^2 - n{y_2}^2$ se rovnají jedné. Jejich součin, se tím pádem také rovná jedné.

$$({x_1}^2 - n{y_1}^2) \cdot ({x_2}^2 - n{y_2}^2) = 1 \cdot 1$$

Oba výrazy na levé straně rozložíme podle vzorce $a^2 - b^2 = (a - b) \cdot (a + b)$ a následně opět vynásobíme, ovšem tak, že soárujeme závorky se stejným znaménkem u y.

$$\left(x_1 - y_1\sqrt{n}\right) \cdot \left(x_1 + y_1\sqrt{n}\right) \cdot \left(x_2 - y_2\sqrt{n}\right) \cdot \left(x_2 + y_2\sqrt{n}\right) = 1$$

$$\left[\left(x_1 - y_1\sqrt{n}\right)\cdot\left(x_2 - y_2\sqrt{n}\right)\right]\cdot\left[\left(x_1 + y_1\sqrt{n}\right)\cdot\left(x_2 + y_2\sqrt{n}\right)\right] = 1$$

$$\left[(x_1x_2 + ny_1y_2) - (x_1y_2 + x_2y_1)\sqrt{n}\right]\cdot\left[(x_1x_2 + ny_1y_2) + (x_1y_2 + x_2y_1)\sqrt{n}\right] = 1$$

Je vidět, že opět můžeme užít vzorce, podle kterého jsme na začátku rozkládali.

$$(x_1x_2 + ny_1y_2)^2 + n(x_1y_2 + x_2y_1)^2 = 1$$

A dostáváme nové řešení $(x_3; y_3)$ ve tvaru $(x_1x_2 + ny_1\,y_2; x_1y_2 + y_1x_2)$, což jsme chtěli dokázat. (Stillwell, 2003, s. 82) ■

Máme tedy uzavřenost množiny řešení M na násobení. Tím jsme nejen ověřili jeden z požadavků na to, aby $(M,\cdot)$ byla grupa, ale hlavně jsme také získali nástroj, jak generovat další řešení jako násobky předchozích dvou.

Uvědomme si, že ve Tvrzení 12 není požadováno, aby byla $(x_1; y_1)$ a $(x_2; y_2)$ různá. Stačí nám tedy jedno řešení a vynásobíme-li ho samo se sebou (druhá mocnina), dostaneme další řešení. To pak můžeme opět vynásobit původním řešením a dostaneme další nové řešení (třetí mocninu). Takto bychom mohli postupovat dále a do nekonečna generovat nová řešení. Co kdybychom ale měli nějaké řešení, které už je mocninou nějakého jiného řešení?

$$x + y\sqrt{n} = \left(x_1 + y_1\sqrt{n}\right)^k$$

Pak umocňováním $x + y\sqrt{n}$ dostaneme pouze k-násobné mocniny $x_1 + y_1\sqrt{n}$.

$$\left(x + y\sqrt{n}\right)^m = \left(x_1 + y_1\sqrt{n}\right)^{m\cdot k}$$

V tom případě nám uniknou některé mocniny řešení $x_1 + y_1\sqrt{n}$, které jsou ovšem také řešeními a nedostaneme kompletní množinu. Například pro $k = 2$ přicházíme o každou lichou mocninu $x_1 + y_1\sqrt{n}$.

Dokážeme, že všechna řešení jsou mocninami minimálního řešení, a to generuje celou množinu řešení M (viz Definice 12).

Tvrzení 13.

Nechť $x_1 + y_1\sqrt{n}$ je minimální řešení dané Pellovy rovnice. Pak všechna další kladná řešení jsou ve tvaru $x_k + y_k\sqrt{n} = \left(x_1 + y_1\sqrt{n}\right)^k$ pro $k \in \mathbb{N}$.

Důkaz. Dokážeme sporem. Předpokládejme, že $x_1 + y_1\sqrt{n}$ je minimální řešení a že existuje nějaké řešení $a + b\sqrt{n}$, které není jeho mocninou. Jelikož není mocninou, pak se vyskytuje někde mezi dvěma mocninami $x_1 + y_1\sqrt{n}$:

$$\left(x_1 + y_1\sqrt{n}\right)^k < a + b\sqrt{n} < \left(x_1 + y_1\sqrt{n}\right)^{k+1}$$

Nyní nerovnosti vynásobíme $\left(x_1 + y_1\sqrt{n}\right)^{-k} = \left(x_1 - y_1\sqrt{n}\right)^k$.

$$1 < \left(a + b\sqrt{n}\right) \cdot \left(x_1 - y_1\sqrt{n}\right)^k < x_1 + y_1\sqrt{n}$$

Protože jak $a + b\sqrt{n}$, tak $\left(x_1 - y_1\sqrt{n}\right)^k$ jsou řešení, je jím podle Tvrzení 12 i jejich součin. To ale znamená, že by existovalo řešení menší než $x_1 + y_1\sqrt{n}$ a tím pádem $x_1 + y_1\sqrt{n}$ by nebylo minimální, což je ve sporu s předpokladem. (Tattersall, 2005, 277) ■

Poznámka Je zřejmé, že $\left(a + b\sqrt{n}\right) \cdot \left(x_1 - y_1\sqrt{n}\right)^k$ nemůže být triviální řešení $1 + 0\sqrt{n}$. Muselo by platit: $\left(a + b\sqrt{n}\right) = \left(x_1 + y_1\sqrt{n}\right)^k$, což je ve sporu s předpokladem, že $\left(a + b\sqrt{n}\right)$ není mocninou minimálního řešení.

Dokázali jsme, že minimální řešení generuje všechna kladná netriviální řešení, která nás zajímají z hlediska aproximací. Zároveň jsme získali efektivnější nástroj hledání dalších řešení Pellovy rovnice. Nyní nám stačí najít pouze minimální řešení a libovolné další dostaneme jako jeho k-tou mocninu. Tento proces je snazší než hledat větší řešení mezi sblíženými zlomky. Z hlediska cyklické grupy ale potřebujeme ukázat, že minimální řešení generuje také $1 + 0\sqrt{n} = 1$ a řešení tvaru $x_k - y_k\sqrt{n}$.

První problém je jednoduchý, protože $x_1 + y_1\sqrt{n}$ je nějaké nenulové iracionální číslo a $\left(x_1 + y_1\sqrt{n}\right)^0 = 1$, tedy neutrální prvek, generuje nultá mocnina minimálního řešení. To, že minimální řešení generuje $x_k - y_k\sqrt{n}$ vyplývá z Tvrzení 11.

$$x_k - y_k\sqrt{n} = \left(x_k + y_k\sqrt{n}\right)^{-1} = \left(x_1 + y_1\sqrt{n}\right)^{-k}$$

Řešení se záporným y_k tedy generují záporné mocniny.

Máme dokázáno, že minimální řešení generuje celou množinu M a že v M existuje prvek neutrální a ke každému prvku inverzní. Pojďme si nyní dokázat zbývající podmínku pro to, abychom mohli $(M,\cdot)$ prohlásit za cyklickou grupu. Poslední vlastností, kterou zbývá ověřit, je asociativita.

Tvrzení 14.
Násobení řešení Pellovy rovnice je asociativní. Platí tedy, že:

$$\left(x_k + y_k\sqrt{\mathrm{n}}\right) \cdot \left[\left(x_l + y_l\sqrt{\mathrm{n}}\right) \cdot \left(x_m + y_m\sqrt{\mathrm{n}}\right)\right] = \left[\left(x_k + y_k\sqrt{\mathrm{n}}\right) \cdot \left(x_l + y_l\sqrt{\mathrm{n}}\right)\right] \cdot \left(x_m + y_m\sqrt{\mathrm{n}}\right)$$

Důkaz. Zapišme řešení jako mocniny minimálního řešení. Jelikož máme mocninu nějakého reálného čísla platí, že $\left(x_1 + y_1\sqrt{\mathrm{n}}\right)^k \cdot \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^l = \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^{k+l}$. Mějme $\left(x_1 + y_1\sqrt{\mathrm{n}}\right)^k, \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^l, \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^m \in M, k, l, m \in \mathbb{Z}$.

$$\left[\left(x_1 + y_1\sqrt{\mathrm{n}}\right)^k \cdot \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^l\right] \cdot \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^m =$$

$$= \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^k \cdot \left[\left(x_1 + y_1\sqrt{\mathrm{n}}\right)^l \cdot \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^m\right]$$

Obě strany upravíme a vyjde nám, že $\left(x_1 + y_1\sqrt{\mathrm{n}}\right)^{k+l+m} = \left(x_1 + y_1\sqrt{\mathrm{n}}\right)^{k+l+m}$ a násobení je asociativní na množině řešení. ■

Tím jsme ověřili, že struktura $(M,\cdot)$ splňuje všechny vlastnosti cyklické grupy. Můžeme nyní

Věta 15. Struktura množiny řešení Pellovy rovnice.
Struktura $(M,\cdot)$, kde $M = \left\{x_k \pm y_k\sqrt{n}, k \in \mathbb{N}: {x_k}^2 - n{y_k}^2 = 1\right\}$ a $\cdot$ je operace násobení, je cyklickou grupu s generátorem $x_1 + y_1\sqrt{\mathrm{n}}$.

Důkaz. Tvrzení 8, 9, 10, 11 a 12. ■

Popsali jsme tedy strukturu množiny M, kde nás především zajímají kladná řešení. Tato množina ovšem neobsahuje všechna řešení Pellovy rovnice. Zbývající řešení ve tvarech $-x_i \pm y_i\sqrt{n}$, dostaneme jako množinu $-M = \left\{-\left(x_i \pm y_i\sqrt{n}\right), i \in \mathbb{N}: {x_i}^2 - n{y_i}^2 = 1\right\}$,

která už ovšem nesdílí vlastnosti námi zkoumané množiny M. Například není uzavřená na násobení.

$$\left(-x_k - y_k\sqrt{n}\right)^2 = \left(x_k + y_k\sqrt{n}\right)^2 = ({x_k}^2 + n{y_k}^2) + 2x_k y_k\sqrt{n}$$

Hlavním poznatkem z této kapitoly je, že můžeme generovat další kladná řešení pomocí kladných mocnin minimálního řešení a ulehčit si tak práci se sblíženými zlomky. Jako záporné mocniny pak získáme řešení ve tvaru $x_i - y_i\sqrt{n}$ a násobením číslem -1 pak dostaneme zbylá řešení dané Pellovy rovnice.

Tímto můžeme uzavřít naše zkoumání Pellovy rovnice jako takové. Ve třech kapitolách jsme zkoumali řešení Pellovy rovnice ve tvaru $x^2 - ny^2 = 1$. Věnovali jsme se kladným netriviálním řešením, protože jsou vhodná k aproximaci $\sqrt{n}$ a jsou snadno generována jedním, minimálním, řešením. Dokázali jsme, že pro všechna n, která nejsou čtvercem, taková řešení existují a odvodili jsme, jak je najít pomocí řetězových zlomků, konkrétně mezi sblíženými zlomky. Poté jsme popsali strukturu, kterou lze v řešeních najít, a usnadnili jsme si tak proces hledání nových řešení. Jsme tedy schopni nalézt všechna řešení Pellovy rovnice pro jakékoliv n.

4 Další užití Pellovy rovnice

Se znalostmi z předchozích kapitol se nyní podívejme na řešení negativní a obecné Pellovy rovnice a další oblasti užití Pellovy rovnice. V úvodu této práce bylo řešení Pellovy rovnice motivováno aproximacemi iracionálních odmocnin, které jsme již probrali jako hlavní motivaci, hledáním invertibilních prvků ve strukturách $\mathbb{Z}[\sqrt{n}]$ a hledáním čísel, která jsou zároveň čtverci a trojúhelníky. Podíváme se tedy krátce i na tato další užití. Jako nový pojem si zavedeme Pellova čísla a učiníme pozorování, jak souvisí s Pellovou rovnicí. Poté si ukážeme, jak pomocí těchto čísel nalézt tzv. pythagorejské trojice.

4.1 Řešení negativní a obecné Pellovy rovnice

Negativní Pellovu rovnici jsme v předchozím textu již několikrát zmínili. Na začátku první kapitoly jsme ji odvodili spolu s Pellovou rovnicí jako rovnice, pomocí jejichž řešení dostaneme co nejmenší odchylku při aproximaci $\sqrt{2}$ a obecně při aproximaci $\sqrt{n}$.

Zabývali jsme se ale hlavně Pellovou rovnicí, a to z toho důvodu, že negativní nemá pro všechna n řešení, což lze ukázat například pomocí kongruencí. To samé platí pro obecnou rovnici, jak ukážeme na následujících příkladech. (Conrad (a), [b.r.], s. 7-8)

Mějme rovnici $x^2 - 3y^2 = -1$ a podívejme se na ni modulo 3. Získáme:

$$x^2 \equiv -1 (\mathrm{mod}\ 3)$$

Jediné dva čtverce $\mathrm{mod}\ 3$, jsou 0 a 1, z čehož plyne že rovnice $x^2 - 3y^2 = -1$ nemá řešení. Stejným způsobem ukažme, že obecná Pellova rovnice $x^2 - 5y^2 = 2$ nemá řešení. Podívejme se na tuto rovnici modulo 5. Máme:

$$x^2 \equiv 2 (\mathrm{mod}\ 5)$$

Jediné čtverce $\mathrm{mod}\ 5$ jsou $0,1,4$ a pro žádný z nich není kongruence splněna. (Conrad (a), [b.r.], s. 8)

Více příkladů lze nalézt v textu Keitha Conrada ([b.r.]) *Pell's Equation I* na straně 8. Kongruence jsme zběžně zmínili při důkazu existence netriviálního řešení Pellovy rovnice pro všechna n. Ten, kdo by se více zajímal o kongruence, najde přehledné informace

například v *Kouzlo čísel* od Křížek a spol. (2018), *Elements of Number Theory* od Johna Stillwella (2003).

Obecně můžeme říct, že řešení $x^2 - 3y^2 = c$, kde $c \in \mathbb{Z} \setminus \{0\}$, neexistuje pro všechna c. Když ale řešení nějaké obecné Pellovy rovnice $x^2 - ny^2 = c$, určené následujícím tvrzením, najdeme, můžeme ostatní řešení této rovnice vygenerovat pomocí řešení příslušné Pellovy rovnice se stejným n, tj. $x^2 - ny^2 = 1$. (Conrad (b), [b.r.], s. 4)

Tvrzení 16.

Mějme $\alpha = x + y\sqrt{n}$ kladné řešení Pellovy rovnice $x^2 - ny^2 = 1$. Pak pro každé $c \in \mathbb{Z} \setminus \{0\}$ jsou všechna řešení $x^2 - ny^2 = c$ rovna mocninám $x + y\sqrt{n}$ násobeným $a + b\sqrt{n}$, takovým že $a^2 - nb^2 = c$ a zároveň $|a| \leq \sqrt{c} \cdot \frac{\sqrt{\alpha}+1}{2}, |a| \leq \sqrt{n} \cdot \frac{\sqrt{\alpha}+1}{2\sqrt{n}}$. (Conrad (b), [b.r.], s.4)

Kompletní důkaz je zdlouhavý a poměrně technický. Celé znění lze nalézt v textu Keitha Conrada ([b.r.]) *Pell's Equation II* na stranách 4-6. My si ukážeme důkaz slabšího tvrzení a to toho, že součin řešení Pellovy rovnice a řešení obecné Pellovy rovnice se stejným n nám dá nějaké nové (ne všechna) řešení obecné rovnice:

Tvrzení 17.

Součin nějakého řešení obecné Pellovy rovnice $x^2 - ny^2 = c$ a nějakého řešení odpovídající Pellovy rovnice $x^2 - ny^2 = 1$ je řešení obecné rovnice $x^2 - ny^2 = c$.

Důkaz. Jedná se o analogii důkazu Tvrzení 12. Postupujeme stejnými úpravami. Máme:

$$(a^2 - nb^2) \cdot (x^2 - ny^2) = c \cdot 1$$

$$\left(a - b\sqrt{n}\right) \cdot \left(a + b\sqrt{n}\right) \cdot \left(x - y\sqrt{n}\right) \cdot \left(x + y\sqrt{n}\right) = c$$

$$\left[\left(a - b\sqrt{n}\right) \cdot \left(x - y\sqrt{n}\right)\right] \cdot \left[\left(a + b\sqrt{n}\right) \cdot \left(x + y\sqrt{n}\right)\right] = c$$

$$\left[(ax + nyb) - (xb + ay)\sqrt{n}\right] \cdot \left[(ax + nyb) + (xb + ay)\sqrt{n}\right] = c$$

$$(ax + nyb)^2 + n(xb + ay)^2 = c$$

A získali jsme nové řešení obecné Pellovy rovnice $x^2 - ny^2 = c$ $(c; d)$ ve tvaru $(ax + nyb; xb + ay)$. ■

Víme tedy, že obecná (a speciálně i negativní) rovnice nemá pro každé $c \in \mathbb{Z} \setminus \{0\}$ na pravé straně řešení. Výjimkou je obecná rovnice s $c = 1$, pro kterou, jak jsme si dokázali, vždy řešení existuje a je užitečná i při generování dalších řešení jiných obecných rovnic.

4.2 Využití Pellovy rovnice při hledání invertibilních prvků v $\mathbb{Z}[\sqrt{n}]$

Nejprve si zadefinujeme, co je invertibilní prvek a struktura $\mathbb{Z}[\sqrt{n}]$. Poté si řekneme, co je to norma čísla ze $\mathbb{Z}[\sqrt{n}]$ a jak souvisí s Pellovou rovnicí, z čehož bude zřejmé, jak pomocí řešení Pellovy rovnice hledat invertibilní prvky v této struktuře.

Definice 14. Invertibilní prvek

Invertibilní prvek je takový prvek a, pro který platí, že $a|1$ a zároveň $1|a$. Z definice dělitelnosti plyne, že existuje nějaké b takové, že $a \cdot b = 1$. Toto b se často označuje a^{-1}. (Stanovský, 2008, s. 20)

Vidíme, že prvek b zde funguje jako inverzní prvek. Můžeme tedy říct, že invertibilní prvek je takový, ke kterému existuje inverzní prvek.

Definice 15. Obor integrity $\mathbb{Z}[\sqrt{n}]$

$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n}: x, y \in \mathbb{Z}\}$ je obor integrity pro všechna n. (Stanovský, 2010, s. 18)

Definici oboru integrity lze nalézt v textu *Základy algebry* Stanovského (2010) na straně 16.

Definice 16. Norma čísla v $\mathbb{Z}[\sqrt{n}]$

Pro $\mathbb{Z}[\sqrt{n}]$, kde n není dělitelné žádnou druhou mocninou prvočísla definujeme zobrazení $v: \mathbb{Z}[\sqrt{n}] \to \mathbb{N}$, kterému říkáme eukleidovská norma. Definici eukleidovské normy nalezneme ve Stanovském (2010) na straně 27. Normou pro tyto obory je zobrazení

$$x + y\sqrt{n} \to |x^2 - ny^2|$$

Bez důkazu uvádíme tvrzení, že prvek v $\mathbb{Z}[\sqrt{n}]$ je invertibilní právě tehdy, když je jeho norma 1. (Stanovský, 2010, s. 31)

Jinými slovy prvek je invertibilní, pokud $|x^2 - ny^2| = 1$, tedy $x^2 - ny^2 = \pm 1$. Hledání invertibilních prvků je tím pádem hledáním řešení Pellovy rovnice a negativní Pellovy rovnice.

4.3 Hledání čísel, která jsou zároveň trojúhelníková čísla a čtverce

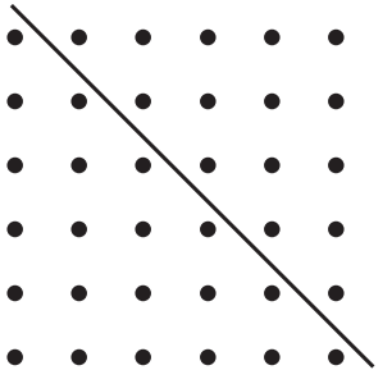
S tzv. čtverci jsme se již setkali. Označovali jsme tak čísla, která jsou druhou mocninou nějakého $d \in \mathbb{N}$. Můžeme je tedy značit d^2. Co jsou tzv. trojúhelníková čísla (zkráceně jim budeme říkat trojúhelníky) říká následující definice:

Definice 17. Trojúhelníková čísla

Trojúhelníková čísla jsou posloupnost čísel, kde n-té číslo určuje počet teček v rovnostranném trojúhelníku, jehož stranu tvoří právě n teček. Jsou to čísla $1, 3, 6, 10, 15, 21, 28, \ldots$ s předpisem pro n-tý člen $t_n = \frac{1}{2}n \cdot (n+1)$.

Obr. 5: Trojúhelníky pro $n = 2,3,4$ (Barbeau, 2003, s. 16)

Můžeme jednoduše vypozorovat, že dva po sobě jdoucí trojúhelníky dávají čtverec.



Obr. 6: Suma dvou po sobě jdoucích trojúhelníků jako čtverec (Barbeau, 2003, s. 17)

(Barbeau, 2003, s. 16, 17)

Příklad 11.

a) Pro trojúhelníky, které jsou zároveň čtverce máme vztah $\frac{1}{2}n \cdot (n+1) = d^2$. Ukažte, že lze tuto rovnost ekvivalentně upravit na $(2n+1)^2 - 8d^2 = 1$.

b) Řešte Pellovu rovnici $x^2 - 8y^2 = 1$ a ze vztahů $x = 2n+1$, $y = d$ určete tři trojúhelníky, které jsou zároveň čtverce.

(Barbeau, 2003, s. 17)

Řešení.

a) Jako první krok můžeme celou rovnici vynásobit číslem 8, abychom na pravé straně dostali $8d^2$.

$$4n \cdot (n+1) = 8d^2$$

Roznásobíme závorku na levé straně a upravíme na čtverec.

$$4n^2 + 4n = 8d^2$$

$$(2n+1)^2 - 1 = 8d^2$$

Nyní stačí jen převést $8d^2$ na pravou stranu a -1 na levou a máme kýžený tvar.

$$(2n+1)^2 - 8d^2 = 1$$

b) Řešme Pellovu rovnici $x^2 - 8y^2 = 1$ tak, jak jsme si ukázali v druhé kapitole. Nejprve sestavíme řetězový zlomek $\sqrt{8}$ a to pomocí Tennerova algoritmu. Pokračujeme, dokud se proces nezacyklí a my neuvidíme, jakou má řetězový zlomek periodu.

I	II	III		IV	V	VI
2	×	2	=	8	−	4
1	0	2		4	4	1
4	0	2		4	4	4
1	0	2		4	4	1
4	0	2		4	4	4

Vidíme, že $\sqrt{8} = [2; \overline{1,4}]$ a má sudou periodu $l = 2$. Podle Tvrzení 8 určíme, že řešení nám dají m-té sblížené zlomky, kde $m = k \cdot l - 1, k \in \mathbb{N} \setminus \{0\}$. Nejmenší s $k = 1$ je $m = 1$, tedy první sblížený zlomek. Pro jeho výpočet není třeba využít rekurzivního předpisu a můžeme ho rovnou spočítat:

$$2 + \frac{1}{1} = \frac{3}{1}$$

Získali jsme jedno řešení $(3; 1)$, a to rovnou řešení minimální, protože jsme zvolili nejmenší k. Když dosadíme do vztahů pro n a d, dostáváme:

$$3 = 2n + 1 \qquad d = 1$$
$$n = 1 \qquad d^2 = 1$$

První trojúhelník, který je zároveň čtverec, je trojúhelník $t_1 = \frac{1}{2} \cdot (1 + 1) = 1$. Jelikož máme minimální řešení, nemusíme počítat další sblížené zlomky, ale můžeme ho použít k vygenerování dalších řešení. Další řešení nám tedy dá druhá mocnina čísla $3 + \sqrt{8}$.

$$\left(3 + \sqrt{8}\right)^2 = 17 + 6\sqrt{8}$$

Ze vztahů vychází:

$$17 = 2n + 1 \qquad d = 6$$
$$n = 8 \qquad d^2 = 36$$

Další trojúhelník, který je také čtverec, je osmý trojúhelník v posloupnosti, tedy číslo $t_1 = \frac{1}{2} \cdot 8 \cdot (8+1) = 36$. Třetí řešení dostaneme jako třetí mocninu minimálního $3 + \sqrt{8}$.

$$\left(3 + \sqrt{8}\right)^3 = 99 + 35\sqrt{8}$$

Ze vztahů dostaneme:

$$99 = 2n + 1$$

$$n = 49$$

$$d = 35$$

$$d^2 = 1225$$

Třetí trojúhelník, který je i čtvercem, je 49-tý trojúhelník z posloupnosti. Vidíme z předchozích případů, že nemusíme počítat trojúhelník pro $n = 49$. Víme totiž, že je zároveň čtvercem 35^2, tedy $t_{49} = 35^2 = 1225$.

Jak jsme si popsali v předchozí kapitole, tímto způsobem bychom mohli vygenerovat nekonečně mnoho řešení. Před tím, než naše studování Pellovy rovnice uzavřeme, podívejme se na Pellova čísla a jak pomocí nich lze hledat pythagorejské trojice.

4.4 Pellova čísla a pythagorejské trojice

V této podkapitole si představíme Pellova čísla jako jisté posloupnosti čísel. Poté si řekneme, co to jsou pythagorejské trojice, a ukážeme si předpis, pomocí kterého lze z Pellových čísel tyto trojice generovat. Pellova čísla definujeme následovně.

Definice 18. Pellova čísla

Pellova čísla P_n a Q_n definujeme následujícími rekurentními předpisy, které vycházejí z tzv. Pellových polynomů, o kterých se dočteme v *Pythagorean Triples with Pell Generators* od Koshyho (2008) na straně 2:

$$P_1 = 1, P_2 = 2, \dots, P_n = 2 \cdot P_{n-1} + P_{n-2}$$

$$Q_1 = 1, Q_2 = 3, \dots, Q_n = 2 \cdot Q_{n-1} + Q_{n-2}$$

Několik prvních Pellových čísel můžeme nahlédnout v tabulce.

n	1	2	3	4	5	6
Q_n	1	3	7	17	41	99
P_n	1	2	5	12	29	70

Tab. 9 (Koshy, 2008, s. 3)

(vlastní zpracování)

(Koshy, 2008, s. 3)

Učiňme pozorování, že dvojice $(Q_n; P_n)$ odpovídají řešením $(x; y)$ rovnice $x^2 - 2y^2 = \pm 1$.

Definice 19. Pythagorejská trojice

Uspořádanou trojici $(a, b, c), a, b, c \in \mathbb{N}$ nazveme pythagorejskou trojicí, pokud platí

$$a^2 + b^2 = c^2$$

Tvoří-li takové trojice strany trojúhelníku, je tento trojúhelník pravoúhlý. (Křížek a spol., 2018, s. 54)

Tyto trojice lze generovat pomocí Pellových čísel podle následujícího předpisu.

$$(a, b, c) = (Q_n Q_{n+1}, 2P_n P_{n+1}, P_{2n+1})$$

(Koshy, 2008, s. 3)

Příklad 12.

Sestrojte pythagorejské trojice pro a) $n = 1$, b) $n = 2$, a ověřte, že splňují $a^2 + b^2 = c^2$.

Řešení.

a) Pouze dosadíme do vzorce čísla z tabulky.

$$(Q_1 Q_2, 2P_1 P_2, P_3) = (1 \cdot 3{,}2 \cdot 1 \cdot 2{,}5) = (3, 4, 5)$$

A ověříme, zda platí $3^2 + 4^2 = 5^2$.

$$9 + 16 = 25$$

Vidíme, že rovnost platí a našli jsme pythagorejskou trojici.

b) Budeme postupovat stejně jako v případě a). Nejprve dosaďme do vzorce.

$$(Q_2Q_3, 2P_2P_3, P_5) = (3 \cdot 7, 2 \cdot 2 \cdot 5, 29\ ) = (21{,}20{,}29)$$

Ověříme, že nám skutečně vyšla pythagorejská trojice.

$$20^2 + 21^2 = 29^2$$

$$400 + 441 = 841$$

Vidíme, že jsme opět dosadili správně a $(21{,}20{,}29)$ opravdu je pythagorejskou trojicí.

Tímto jsme s naší schopností hledat řešení Pellovy rovnice ukázali, jak Pellova rovnice slouží v různých oblastech.

Závěr

Tato práce stručně představila, co je Pellova rovnice, jak najít její řešení, jak souvisí s řetězovými zlomky, aproximacemi iracionálních čísel atd. Text také podává strukturované informace z českých i zahraničních zdrojů a je vhodný k použití jako studijní materiál pro studenty vysokých škol, středních škol a pro kohokoliv, kdo se o toto téma zajímá. Tím byl splněn cíl práce vyložit Pellovu rovnici strukturovaně a srozumitelně pro studenty vysokých škol.

V první kapitole byla představena stručná historie Pellovy rovnice a ta pak byla odvozena ze vztahu úhlopříčky a strany čtverce. Dokázali jsme, že každá Pellova rovnice má řešení, i když jsme je zatím nebyli schopni najít. Ve druhé kapitole jsme se zabývali řetězovými zlomky a sblíženými zlomky. Představili jsme Tennerův algoritmus, který spolu s užitím rekurentního předpisu usnadňuje výpočet sblížených zlomků. Poté jsme odvodili, jak výskyt řešení mezi sblíženými zlomky souvisí s periodou řetězového zlomku dané odmocniny, a získali jsme tak nástroj pro řešení všech Pellových rovnic.

Řešení nám dále usnadnilo prozkoumání struktury množiny řešení ve třetí kapitole, kdy jsme dokázali, že všechna kladná řešení můžeme získat jako mocniny minimálního řešení. Jsme tedy schopni s těmito nástroji úspěšně a poměrně efektivně určit všechna řešení dané Pellovy rovnice.

V poslední kapitole jsme se blíže podívali na řešení Pellovy rovnice negativní a obecné a další užití Pellovy rovnice, čímž jsme uzavřeli naše studium této kvadratické diofantické rovnice.

Seznam použitých informačních zdrojů

BARBEAU, J. Edward, 2003. *Pell's Equation*. New York: Springer. ISBN 0-387-95529-1.

CONRAD (A), Keith, [b.r.]. *Pell'S Equation, I* [online]. Dostupné z: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf

CONRAD (B), Keith, [b.r.]. *Pell'S Equation, II* [online]. Dostupné z: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf

DUDLEY, Underwood, 2009. A Gudie to Elementary Number Theory. USA: The Mathematical Association of America. ISBN 978-0-88385-918-6.

JAŠŠOVÁ, Alena, 2010. *Diofantické aproximace* [online]. Ostrava. Dostupné z: https://theses.cz/id/qua4gk/. Diplomová práce. Ostravská univerzita, Přírodovědecká fakulta. Vedoucí práce prof. RNDr. Jaroslav Hančl, CSc.

KALA, Vítězslav, 2021. *Teorie čísel* [online]. Dostupné z: https://www.karlin.mff.cuni.cz/~kala/1920%20tc/TC%20skripta.pdf

KOSHY, Thomas, 2008. *Pythagorean triples with Pell generators*. In: *The Mathematical Gazette*[online]. B.m.: The Mathematical Association. Dostupné z: https://www.jstor.org/stable/27821836

KŘÍŽEK, Michal, Lawrence SOMER a Alena ŠOLCOVÁ, 2018. *Kouzlo čísel: Od velkých objevů k aplikacím*. 3. vyd. Praha: Academia. ISBN 978-80-200-2840-2.

MANIN, I. Yuri a A. Alexei PANCHISHKIN, 2005. *Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories*. 2. vyd. New York: Springer. ISBN 978-3-540-20364-3.

PRIMEFAN, 2013. *Table of continued fractions of* $\sqrt{n}$ *for* $1 < n < 102$. *PlanetMath.org* [online]. Dostupné z: https://planetmath.org/tableofcontinuedfractionsofsqrtnfor1n102

STANOVSKÝ, David, 2010. *Základy algebry*. 1. vyd. Praha: MatfyzPress. ISBN 978-80-7378-105-7.

STEIN, William, 2017. *Elementary Number Theory: Primes, Congruences, and Secrets* [online]. Dostupné z: https://wstein.org/ent/ent.pdf

STILLWELL, John, 2003. *Elements of Number Theory*. New York: Springer. ISBN 978-1-4419-3066-8.

STILLWELL, John, 2010. *Mathematics and Its History*. 3. vyd. New York: Springer. ISBN 978-1-4419-6052-8.

TATTERSALL, J. James, 2005. *Elementary Number Theory in Nine Chapters*. 2. vyd. New York: Cambridge University Press. ISBN 978-0-5216-1524-2.

WOODS, Billy, 2020. *[ANT08] Continued fractions, Pell's equation, and units of Z[√d]* [online]. YouTube. Dostupné z: https://www.youtube.com/watch?v=3ls3z-UzOSw

YANG, Hyun Seung, 2008. *Continued Fractions and Pell's Equation* [online]. Dostupné z: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Yang.pdf