Univerzita Hradec Králové
Přírodovědecká fakulta

DIPLOMOVÁ PRÁCE

2023 **Bc. Aleš Horáček**

Univerzita Hradec Králové
Přírodovědecká fakulta
Katedra matematiky

Diofantické rovnice

DIPLOMOVÁ PRÁCE

Autor: Bc. Aleš Horáček

Studijní program: N0114A140003

Studijní obor: Učitelství informatiky a matematiky pro střední školy

Vedoucí práce: RNDr. Jitka Kühnová, Ph.D.

Hradec Králové 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, ze kterých jsem vycházel.

V Hradci Králové

Aleš Horáček

Poděkování

Rád bych touto cestou poděkoval RNDr. Jitce Kühnové, Ph.D. nejen za její rady a velmi cenné připomínky, ale především za její trpělivost a ochotu při vedení této práce.
Dále bych rád poděkoval své manželce a rodině za podporu po celou dobu studia.

Anotace

HORÁČEK, A. *Diofantické rovnice* Hradec Králové, 2023. Diplomová práce na Přirodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce RNDr. Jitka Kühnová, Ph.D.

Diplomová práce se zabývá vybranými typy diofantických rovnic. Kromě lineárních diofantických rovnic práce obsahuje i metody řešení některých typu diofantických rovnic vyšších stupňů, Pellovy rovnice a pythagorejské trojúhelníky. Diplomová práce také obsahuje sbírku řešených úloh.

Klíčová slova:

dělitelnost, diofantická rovnice, Pellova rovnice, pythagorejský trojúhelník, řetězové zlomky

Annotation

HORÁČEK, A. *Diophantine equations.* Hradec Králové, 2023. Diploma Thesis at Faculty of Science University of Hradec Králové Thesis Supervisor RNDr. Jitka Kühnová, Ph.D.

The thesis deals with selected types of Diophantine equations. In addition to linear Diophantine equations, the work also includes methods for solving some types of higher-degree Diophantine equations, Pell's equation, and Pythagorean triangles. The thesis also includes a collection of solved problems.

Key words:

divisibility, Diophantine equation, Pell's equation, Pythagorean triangle, continued fractions

Obsah

Seznam použitých symbolů

$\mathbb{N} = \{1,2,3,\dots\}$ ..... množina přirozených čísel
$\mathbb{N}_0 = \{0,1,2,3,\dots,\}$ ..... množina nezáporných celých čísel
$\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ ..... množina celých čísel
$\mathbb{Z}^+ = \{1,2,3,\dots\}$ ..... množina kladných celých čísel
$\mathbb{Q}$ ..... množina racionálních čísel
$\mathbb{I}$ ..... množina iracionálních čísel
$\mathbb{R}$ ..... množina reálných čísel

Úvod

Diofantické rovnice jsou důležitým a zajímavým tématem v teorii čísel. Cílem této diplomové práce je ukázat některé typy diofantických rovnic a názorně demonstrovat metody jejich řešení na příkladech. Protože diofantické rovnice nejsou začleněny v Rámcových vzdělávacích programech pro střední školy, ale vyskytují se v různé míře ve středoškolských matematických soutěžích, může tato diplomová práce být jistou oporou účastníkům takových soutěží.

Práce samotná je rozdělena na tři kapitoly. V první kapitole se zabývá vybranými pojmy z elementární teorie čísel nezbytnými pro řešení vybraných typů diofantických rovnic, především tedy dělitelností celých čísel a řetězovými zlomky.

Druhá kapitola, která tvoří jádro práce, se věnuje pouze vybraným typům diofantických rovnic. Zmíněny jsou metody řešení lineárních diofantických rovnic, ale také i metody řešení některých diofantických rovnic vyššího stupně. Mimo zmíněné se práce věnuje i Pythagorejským trojúhelníkům a způsobům jejich generování.

Třetí kapitolu, tedy praktickou část práce, tvoří sbírka řešených úloh, ve které jsou postupně aplikovány a demonstrovány postupy z teoretické části práce. Většina řešení příkladů je autorská, v opačném případě jsou doplněna o citaci. Postupy řešení úloh jsou zapsány tak, aby mohly být pomůckou dalším studentům ať už střední školy, nebo školy vysoké. Složitější výpočty byly provedeny v tabulkovém procesoru MS Excel, práce je vysázena systémem LaTeX.

Kapitola 1

Vybrané pojmy z teorie čísel

1.1 Dělitelnost celých čísel, největší společný dělitel a prvočísla

Hlavními zdroji pro tuto kapitolu jsou [5] a [8].

Definice 1.1. *Řekneme, že celé číslo a **dělí** celé číslo b (neboli číslo b je dělitelné číslem a, též b je násobek a), právě když existuje celé číslo c tak, že platí $a \cdot c = b$. Píšeme pak $a \mid b$.*

Bez důkazu bude uvedeno několik tvrzení.

Věta 1.1. *Pro libovolná čísla a,b,$c \in \mathbb{Z}$ platí:*

1. $a \mid 0$
2. $0 \mid a \Leftrightarrow a = 0$
3. $a \mid a$.
4. $a \mid b \wedge b \mid c \Rightarrow a \mid c$
5. $(\forall x,y \in \mathbb{Z}) \quad a \mid b \wedge a \mid c \Rightarrow a|bx + cy$
6. $c \neq 0 \Rightarrow (a \mid b \Leftrightarrow ac \mid bc)$
7. $a \mid\Rightarrow |a| \leq |b|$

Poznámka 1.1.

Celá čísla u a v se nazývají sdruženými děliteli čísla w, jestliže platí

$$u \cdot v = w.$$

Věta 1.2. *Každé celé číslo $b \neq 0$ má konečně mnoho dělitelů.*

Věta 1.3. *(Věta o dělení se zbytkem) Ke každému číslu $a \in \mathbb{Z}$ a celému číslu b, $b \neq 0$ existuje právě jedna dvojice celých čísel q, r taková, že $a = bq + r$, kde $0 \leq r < |b|$.*

Důkaz. [8] Nejprve dokážeme existenci čísel q, r. Protože platí $(-q)\cdot(-b) = q\cdot b$, můžeme bez újmy na obecnosti předpokládat, že $b > 0$. Uvažujme čísla:

$$1b, 2b, 3b, \ldots \tag{1.1}$$

Je-li $a \geq 0$, budeme zkoumat množinu M těch čísel v posloupnosti (1.1), která jsou větší než a. Množina M je neprázdná a má nejmenší prvek, který označíme bx'. Jako x si označíme číslo o jednu menší než x', tj. $x + 1 = x'$. Pak

$$bx \leq a < b(x + 1).$$

Je-li $a < 0$, je $-a > 0$ a my můžeme rovnou uvažovat množinu M těch čísel v posloupnosti (1.1), která jsou větší nebo rovna $-a$. Označíme jako by' nejmenší z nich. Potom pro $y = y' - 1$ bude

$$by < a \leq b(y + 1),$$

takže

$$b(-y - 1) \leq a < b(-y).$$

Vidíme, že pro všechna a a $b(b > 0)$ existuje celé číslo q tak, že

$$bq \leq a < b(q + 1). \tag{1.2}$$

Označme jako r rozdíl $a - bq$. Z (1.2) dostáváme $r = a - bq < b(q + 1) - bq = b$ a $r \geq 0$, tedy

$$a = bq + r, \qquad 0 \leq r < b.$$

Dále sporem dokážeme jednoznačnost takových čísel q a r.
Nechť $a = bq + r$ a $a = bq' + r'$, kde $0 \leq r < b$; $0 \leq r' < b$. Předpokládejme, že $r' > r$. Potom je $bq + r = bq' + r'$, a tedy $r' - r = b(q - q')$, kde $0 \leq r < r' < b$, a proto $0 < r' - r < b$ a $q > q'$, tedy zřejmě $q \geq q' + 1$, tj.

$$r' - r = b(q - q') \geq b.$$

Tento vztah ovšem odporuje faktu, že $r' - r < b$. Stejným způsobem dostaneme spor, budeme-li předpokládat, že $r > r'$. To tedy znamená, že musí být $r' = r$, a tedy $b(q - q') = 0$ a protože $b > 0$, tak $q - q' = 0$, tj. $q = q'$.

□

Poznámka 1.2. Číslo q se nazývá **neúplný podíl** a číslo r **zbytek po dělení čísla** a číslem b.

Důsledek. Pro celé číslo $b \neq 0$ platí, že b je dělitelem a právě tehdy, když zbytek po dělení čísla a číslem b je roven nule.

Věta 1.4. *Platí-li pro celá čísla a, b kterýkoliv ze čtyř vztahů $b \mid a$, $-b \mid a$, $-b \mid -a$, $b \mid -a$, pak platí zároveň všechny ostatní.*

Z této věty plyne, že vyšetřování kteréhokoli ze čtyř vztahů v ní uvedených můžeme převést na vyšetřování některého z předchozích vztahů. Díky tomu lze zkoumání vlastností vztahu $a \mid b$ pro celá čísla a,b převést na vyšetřování dělitelnosti v oboru čísel celých nezáporných nebo dokonce často jen v oboru čísel přirozených.

Definice 1.2. ***Společným dělitelem*** *celých čísel* $a_1, a_2, \cdots, a_n$ *se nazývá libovolné celé číslo* d *takové, že* $d \mid a_1$, $d \mid a_2$, $\cdots$, $d \mid a_n$.

Definice 1.3. ***Největším společným dělitelem*** *celých čísel* $a_1, a_2, \cdots, a_n$ *se nazývá ten nezáporný společný dělitel čísel* $a_1, a_2, \cdots, a_n$, *který je dělitelný libovolným jiným společným dělitelem těchto čísel. Označujeme ho zpravidla* $(a_1, a_2, \cdots, a_n)$.

Definice 1.4. ***Společným násobkem*** *celých čísel* $a_1, a_2, \cdots, a_n$ *se nazývá libovolné celé číslo* m *takové, že* $a_1 \mid m$, $a_2 \mid m$,$\cdots$, $a_n \mid m$.

Definice 1.5. ***Nejmenším společným násobkem*** *celých čísel* $a_1, a_2, \cdots, a_n$ *se nazývá nejmenší nezáporné číslo dělitelné všemi čísly* $a_1, a_2, \cdots, a_n$. *Označujeme ho zpravidla* $[a_1, a_2, \cdots, a_n]$.

Věta 1.5. *Jestliže* $b|a$ *a* $b > 0$, *pak* $(a,b) = b$.

Věta 1.6. *Jestliže* $a = bq + r$, *pak* $(a,b) = (b,r)$.

Způsob, jak vypočítat největšího společného dělitele dvou čísel, ukazuje následující věta a její důkaz ze zdroje [8].

Věta 1.7. *(Euklidův algoritmus) K libovolným celým číslům* a,b, $b \neq 0$, *existují celá čísla* $q_0,q_1, \cdots, q_n$ *a* $r_1, r_2, \cdots, r_n$ *taková, že platí:*

$$|b| > r_1 > r_2 > \cdots > r_n > 0,$$

$$\begin{aligned} a &= bq_0 + r_1 \\ b &= r_1q_1 + r_2 \\ r_1 &= r_2q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \\ r_{n-1} &= r_nq_n \end{aligned}$$

a

$$(a,b) = r_n.$$

Důkaz. Podle věty o dělení se zbytkem existují k celým číslům a,b, $b \neq 0$ celá čísla q_0, r_1 tak, že $a = bq_0 + r_1$ a $0 \leq r_1 < |b|$.
Je-li $r_1 = 0$, pak $b|a$ a podle věty 1.5 $(a,b) = b$. Je-li $r_1 > 0$, aplikujeme uvedenou úvahu na dvojici čísel b,r_1, tj. existují celá čísla q_1, r_2 tak, že

$$b = r_1q_1 + r_2$$

a $0 \leq r_2 < r_1$. Je-li $r_2 = 0$, pak $r_1|b$ a $(b,r_1) = r_1$, což podle věty 1.6 znamená, že $r_1 = (b,r_1) = (a,b)$ a můžeme skončit. Je-li $r_2 > 0$, pak pro r_1,r_2 nalezneme q_2 a r_3 tak, že

$$r_1 = r_2q_2 + r_3,$$

atd. Tedy pro r_{k-1} a r_k $(0 < r_k < r_{k-1})$ nalezneme q_k a r_{k+1} tak, že

$$r_{k-1} = r_kq_k + r_{k+1}, \qquad 0 \leq r_{k+1} < r_k.$$

Je-li $r_{k+1} = 0$, pak je postup ukončen. Pokud ale $r_{k+1} \neq 0$, analogicky pokračujeme, a dostáváme vztahy tvaru

$$\begin{aligned} a &= bq_0 + r_1 \\ b &= r_1q_1 + r_2 \\ r_1 &= r_2q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \\ r_{n-1} &= r_nq_n \end{aligned}$$

kde

$$|b| > r_1 > r_2 > \cdots \geq 0.$$

Proces tvoření těchto rovností nemůže být nekonečný. V opačném případě by existovalo nekonečně mnoho přirozených čísel r_k, která by ležela mezi 0 a b. Je ukončen ve chvíli, kdy některé číslo $r_{n+1} = 0$.
Je-li tedy některé $r_{n+1} = 0$, pak je proces tvoření rovností ukončen vztahem $r_{n-1} = r_nq_n$ a platí první část tvrzení věty.
Využijeme-li nyní Větu 1.5 a Větu 1.6, dostáváme

$$r_n = (r_n,r_{n-1}) = (r_{n-1},r_{n-2}) = \cdots = (r_1,r_2) = (b,r_1) = (a,b).$$

□

Největšího společného dělitele dvou čísel najdeme tedy tak, že dělitele opakovaně dělíme zbytkem po předchozím dělení. Jakmile dostaneme nulový zbytek, zbytek v předchozím dělení je největší společný dělitel.

Věta 1.8. *(Bezoutova) Pro libovolná celá čísla a, b existují celá čísla x_0, y_0 tak, že $(a,b) = a \cdot x_0 + b \cdot y_0$.*

Důkaz. Je uveden v [5] (str. 170).

□

Snadno se přesvědčíme, že platí

$$(a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n). \tag{1.3}$$

Největší společný dělitel $(a_1, \ldots, a_n)$ totiž dělí všechna čísla $a_1, \ldots, a_n$, a tedy je společným dělitelem čísel $a_1, \ldots, a_{n-1}$, a proto dělí i největšího společného dělitele $(a_1, \ldots, a_{n-1})$, tj. $(a_1, \ldots, a_n) \mid ((a_1, \ldots, a_{n-1}), a_n)$. Naopak největší společný dělitel čísel $(a_1, \ldots, a_{n-1}), a_n$ musí kromě a_n dělit i všechna čísla $a_1, \ldots, a_{n-1}$, protože dělí jejich největšího společného dělitele, a proto $((a_1, \ldots, a_{n-1}), a_n) \mid (a_1, \ldots, a_n)$. Dohromady dostáváme rovnost (1.3). [5]

Definice 1.6. *Čísla $a_1, \ldots, a_n \in \mathbb{Z}$ se nazývají **nesoudělná**, jestliže platí $(a_1, \ldots, a_n) = 1$. Čísla $a_1, \ldots, a_n \in \mathbb{Z}$ se nazývají **po dvou nesoudělná**, jestliže pro každé i,j takové, že $1 \leq i < j \leq n$, platí $(a_i,a_j) = 1$.*

Poznámka 1.3. V případě $n = 2$ oba pojmy splývají. Pro $n > 2$ plyne z nesoudělnosti po dvou nesoudělnost, ne však naopak.

Věta 1.9. *Pro libovolná přirozená čísla a,b,c platí:*

1. $(ac,bc) = (a,b) \cdot c$,
2. *jestliže* $(a,b) = 1 \wedge a \mid bc$, *pak* $a \mid c$,
3. *jestliže* $d = (a,b)$, *pak* $\left(\frac{a}{d}; \frac{b}{d}\right) = 1$.

Důkaz. Lze najít v [5] (str. 173).

□

Jedním z nejdůležitějších pojmů elementární teorie čísel je pojem prvočíslo především díky větě o jednoznačném rozkladu libovolného přirozeného čísla na součin prvočísel, která bude v práci užita. V další části textu se práce bude zabývat hlavně dělitelností přirozených čísel přirozenými děliteli. Zdrojem jsou [5] a [8].

Definice 1.7. *Každé přirozené číslo* $n \geq 2$ *má alespoň dva kladné celočíselné dělitele:* 1 *a* n. *Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se* ***prvočíslo****. V opačném případě hovoříme o* ***složeném čísle****.*

Prvočísla budou zpravidla značeny písmenem p.

Věta 1.10. *Nejmenší přirozený dělitel libovolného přirozeného čísla* $n > 1$ *různý od jedné je prvočíslo.*

Důkaz. Je uveden v [8] (str. 10).

□

Věta 1.11. *Není-li přirozené číslo* $n > 1$ *dělitelné žádným prvočíslem* $p \leq \sqrt{n}$, *pak je prvočíslo.*

Důkaz. Je uveden v [8] (str. 10).

□

Věta 1.12. *Přirozené číslo* $p \geq 2$ *je prvočíslo, právě když platí:*

$$(\forall a,b \in \mathbb{N}) \quad p|ab \Rightarrow p|a \wedge p|b.$$

Důkaz. Je uveden v [5] (str. 173).

□

Věta 1.13. *(Věta o jednoznačném rozkladu na součin prvočísel.) Libovolné přirozené číslo* $n \geq 2$ *je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li* n *prvočíslo, pak jde o "součin"jednoho prvočísla.)*

Důkaz. Je uveden v [5] (str. 175).

□

Věta 1.14. *Pro libovolné celé číslo* a *a prvočíslo* p *platí:*

$$(a,p) = 1 \Leftrightarrow p \nmid a.$$

Poznámka 1.4. [8] Je-li přirozené číslo $n \geq 2$, pak mezi činiteli součinu

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_l, \tag{1.4}$$

kde p_1,p_2,p_3,$\ldots$ p_k jsou prvočísla taková, že $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_k$ mohou být činitelé navzájem rovní.
Napíšeme-li součin stejných činitelů jako mocninu jednoho z nich s příslušným přirozeným mocnitelem, pak ze vztahu (1.4) dostáváme vztah

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} \cdot, \tag{1.5}$$

kde $m \in \mathbb{N}_{\not\vdash}$ a α_1,α_2,$\ldots$,$\alpha_m \in \mathbb{N}$, p_1,$\ldots$ p_m jsou navzájem různá prvočísla.
Rozklad čísla n podle vztahu (1.5) se nazývá kanonický rozklad na prvočinitele.

1.2 Řetězové zlomky

Definice 1.8. ***Řetězovým zlomkem****, konečným nebo nekonečným, nazýváme výraz*

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}, \tag{1.6}$$

kde a_1 je celé číslo a a_2,a_3,$\ldots$ jsou kladná celá čísla.

Poznámka 1.5.

- Čísla a_1,a_2,a_3,$\ldots$ se nazývají prvky řetězového zlomku.
- Je-li počet prvků konečný, píšeme řetězový zlomek (1.6) ve tvaru $[a_1; a_2,a_3,\ldots,a_n]$. Je-li prvků nekonečně mnoho, píšeme řetězový zlomek (1.6) ve tvaru $[a_1; a_2,a_3,\ldots]$.
- Každý konečný řetězový zlomek vyjadřuje racionální číslo, neboť je výsledkem konečného počtu racionálních operací nad jeho prvky, kterými jsou celá čísla.
- Řetězový zlomek $r_k = [a_k; a_{k+1},\ldots,a_n]$ nazýváme **zbytkem** nekonečného, resp. nekonečného řetězového zlomku.

Definice 1.9. ***Přibližným zlomkem řádu*** *k řetězového zlomku $[a_1; a_2; a_3,\ldots]$ nazýváme zlomek*

$$\frac{P_k}{Q_k} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots + \cfrac{1}{a_k}}}}, \quad k = 1,2,3,\ldots.$$

Označme $\dfrac{P_1}{Q_1} = \dfrac{a_1}{1}$. Vidíme potom, že

$$\frac{P_1}{Q_1} = \frac{a_1}{1}, \quad \frac{P_2}{Q_2} = \frac{a_1a_2+1}{a_2}, \quad \frac{P_3}{Q_3} = \frac{a_1a_2a_3+a_1+a_3}{a_2a_3+1}, \quad \text{atd.}$$

Čísla P_k a Q_k definujeme tak, že je položíme přímo rovno příslušným čitatelům, resp. jmenovatelům.

$$\begin{aligned} P_1 &= a_1, & P_2 &= a_1a_2 + 1, & P_2 &= a_1a_2a_3 + a_1 + a_3, & &\dots \\ Q_1 &= 1, & Q_2 &= a_2, & Q_2 &= a_2a_3 + 1, & &\dots \end{aligned}$$

Věta 1.15. *Pro každé $k \geq 3$ platí*

$$\begin{aligned} P_k &= a_kP_{k-1} + P_{k-2}, \\ Q_k &= a_kQ_{k-1} + Q_{k-2}. \end{aligned}$$

Poznámka 1.6.

- Přibližný zlomek je tedy zcela jednoznačně definován pro konečné i nekonečné řetězové zlomky. Konečný řetězový zlomek má konečný počet sblížených zlomků, nekonečný řetězový zlomek jich má však nekonečně mnoho.
- Pro $n-$členný řetězový zlomek $\alpha = [a_1; a_2, \dots, a_n]$ je zřejmě $\alpha = \dfrac{P_n}{Q_n}$ a tento řetězový zlomek má celkem n přibližných zlomků (řádů $1,2,\dots,n$).

Poznámka 1.7. Věta 1.15 nám snadno umožňuje vypočítat hodnoty přibližných zlomků. Pro rychlý výpočet využijeme tuto tabulku:

i	1	2	3	$\cdots$	$k-1$	k
a_i	a_1	a_2	a_3	$\cdots$	a_{k-1}	a_k
P_i	$P_1 = a_1$	$P_2 = a_1a_2 + 1$	$P_3 = a_3P_2 + P_1$	$\cdots$	P_{k-1}	$a_kP_{k-1} + P_{k-2}$
Q_i	$Q_1 = 1$	$Q_2 = a_2$	$Q_3 = a_3Q_2 + Q_1$	$\cdots$	Q_{k-1}	$a_kQ_{k-1} + Q_{k-2}$

Věta 1.16. *[12] Pro $k \geq 2$ platí*

$$P_kQ_{k-1} - Q_kP_{k-1} = (-1)^k. \tag{1.7}$$

Důsledek. Čitatelé a jmenovatelé sblížených zlomků jsou nesoudělná čísla.

Zdrojem následujících definic a vět uvedených bez důkazu je [8].

Definice 1.10. ***Rozkladem***, *nebo také rozvojem, reálného čísla α v řetězový zlomek rozumíme vyjádření čísla α ve tvaru $\alpha = [a_1; a_2,a_3, \dots]$, kde $a_1,a_2,a_3, \dots$ je konečná nebo nekonečná posloupnost celých čísel taková, že $a_1 \in \mathbb{Z}$ a pro všechna $n \geq 2$ je $a_n \geq 1$. V případě konečného rozkladu je poslední prvek $a_n > 1$.*

Věta 1.17. *Nechť rozklad reálného čísla α v řetězový zlomek má tvar $\alpha = [a_1; a_2,a_3, \dots]$ a nechť $r_k = [a_k; a_{k+1},a_{k+2}, \dots]$ je zbytek daného řetězového zlomku. Pak*

$$\alpha = [a_1; a_2,a_3, \dots ,a_{k-1},r_k]$$

Věta 1.18. *Nechť $\alpha = [a_1; a_2,a_3, \dots]$, nechť r_k (pro $k \geq 3$) je zbytek daného řetězového zlomku. Pak*

$$\alpha = \frac{r_kP_{k-1} + P_{k-2}}{r_kQ_{k-1} + Q_{k-2}} \quad \text{a} \quad r_k = \frac{P_{k-2} - \alpha Q_{k-2}}{\alpha Q_{k-1} - P_{k-1}}, \tag{1.8}$$

kde P_{k-1}, Q_{k-1}, P_{k-2}, Q_{k-2} jsou čitatelé a jmenovatelé sblížených zlomků řádu $(k-1)-$ního a $(k-2)$-ého řetězového zlomku α.

Definice 1.11. *Nekonečný řetězový zlomek* $[a_1; a_2,a_3, \dots]$ *se nazývá* ***konvergentní,*** *existuje-li limita posloupnosti sblížených zlomků, tj. existuje-li*

$$\lim_{k\to\infty} \frac{P_k}{Q_k}.$$

Definice 1.12. ***Hodnotou*** *nekonečného konvergentního řetězového zlomku* $[a_1; a_2,a_3, \dots]$ *rozumíme limitu posloupnosti jeho sblížených zlomků, tj. číslo* α *takové, že*

$$\lim_{k\to\infty} \frac{P_k}{Q_k} = \alpha.$$

Píšeme $\alpha = [a_1; a_2,a_3, \dots]$.

Věta 1.19. *Libovolný nekonečný zlomek konverguje.*

Věta 1.20. *Ke každému reálnému číslu* α *existuje jediný řetězový zlomek, který má za hodnotu toto číslo. Tento řetězový zlomek je konečný, je-li číslo* α *racionální. Je-li číslo* α *iracionální, je tento řetězový zlomek nekonečný.*

V [12] je popsán postup, jak rozvinout libovolné racionální a iracionální číslo v řetězový zlomek.
Každé reálné číslo α lze psát ve tvaru

$$\alpha = [\alpha] + \{\alpha\},$$

kde $[\alpha] \in \mathbb{Z} \wedge [\alpha] \leq \alpha \leq [\alpha] + 1$ a $\{\alpha\} \in \mathbb{R}$, $0 \leq \{\alpha\} < 1$.

1. Nechť je x racionální číslo, $x \notin \mathbb{N}$. Položme $a_1 = [a]$, $x_1 = \dfrac{1}{x}$. Zřejmě pak platí

   $$x = a_1 + \frac{1}{x_1},$$

   kde $x_1 > 1$, $x_1 \in \mathbb{Q}$. Odtud plyne

   $$x_1 = \frac{1}{x - a_1}.$$

   Pro x_1 celý postup zopakujeme. Definujeme tedy číslo

   $$a_2 = [x_1] = \left[\frac{1}{x - a_1}\right]$$

   a číslo

   $$x_2 = \frac{1}{x_1}.$$

   Pak platí

   $$x_1 = a_2 + \frac{1}{x_2},$$

   kde $x_2 > 1$, $x_2 \in \mathbb{Q}$. Z posledního vztahu dostáváme

   $$x_2 = \frac{1}{x_1 - a_2}$$

   a opět definujeme podobným způsobem čísla $a_3,x_3,a_4,x_4, \dots$.
   Postup se zastaví, jakmile je některé x_{n-1} celé číslo. Pak je $a_n = [x_{n-1}]$ poslední prvek řetězového zlomku racionálního čísla x.

2. Nechť je tedy α iracionální číslo. Položíme

$$\alpha = [\alpha] + \{\alpha\}, \quad \alpha_1 = \frac{1}{\{\alpha\}}, \quad \alpha_1 > 1, \quad \alpha_1 \in \mathbb{I}.$$

Položme

$$a_1 = [\alpha].$$

Pokračujeme a dostaneme

$$\begin{aligned}
\alpha_1 &= \frac{1}{\alpha - a_1}, \\
a_2 &= [\alpha_1], \\
\alpha_1 &= a_2 + \frac{1}{\alpha_2}, \quad \alpha_2 = \frac{1}{\{\alpha_1\}}, \quad \alpha_2 > 1, \quad \alpha_2 \in \mathbb{I}, \\
\alpha_2 &= \frac{1}{\alpha_1 - a_2}, \\
a_3 &= [\alpha_2], \\
\alpha_2 &= a_3 + \frac{1}{\alpha_3}, \alpha_3 = \frac{1}{\{\alpha_2\}} \quad \alpha_3 > 1, \quad \alpha_3 \in \mathbb{I}, \\
&\dots
\end{aligned}$$

Čísla $\alpha, \alpha_1, \alpha_2, \alpha_3, \dots,$ jsou iracionální, postup nikdy neskončí, a dostaneme nekonečný řetězový zlomek $[a_1; a_2, \dots]$, ve kterém je $a_1 \in \mathbb{N}_0$, a_2,$a_3, \dots, \in \mathbb{N}$.

Zdrojem pro následující část je opět [8].

Definice 1.13. *Číslo α se nazývá **kvadratická iracionalita**, je-li α iracionálním kořenem některé kvadratické rovnice*

$$ax^2 + bx + c = 0$$

s celočíselnými koeficienty.

Poznámka 1.8.

- Kořeny rovnice $ax^2+bx+c = 0$ jsou čísla $\frac{-b+\sqrt{b^2-4ac}}{2a}, \frac{-b-\sqrt{b^2-4ac}}{2a}$, proto libovolnou kvadratickou iracionalitu α lze vyjádřit ve tvaru

$$\alpha = \frac{M + \sqrt{N}}{O},$$

kde M, N jsou celá čísla a $N(N > 1)$ je celé číslo, které není druhou mocninou celého čísla.
Druhý kořen této rovnice $\alpha' = \frac{M - \sqrt{N}}{O}$ se nazývá iracionalitou sdruženou s α.

- Pro výrazy $\alpha = \sqrt{N}$ a $\alpha' = -\sqrt{N}$ je příslušná kvadratická rovnice $x^2 - N = 0$.

Definice 1.14. *Řekneme, že řetězový zlomek* $\alpha = [a_1; a_2,a_3, \dots]$ *je* ***periodický****, existují-li taková přirozená čísla* s, h, $h \neq 0$, *taková, že pro libovolné* $n \geq s$ *platí*

$$a_{n+h} = a_n.$$

Píšeme $\alpha = [a_1; a_2,a_3, \dots ,a_{s-1},\overline{a_s, \dots ,a_{s+h-1}}]$.

Poznámka 1.9.

- Pro $s = 0$ se řetězový zlomek nazývá ryze periodický a píšeme $[\overline{a_1; a_2, \dots ,a_{h-1}}]$.
- Je-li zároveň $h = 1$, píšeme $[\overline{a_1}]$.
- Je-li $s \geq 0$, nazývá se řetězový zlomek neryze periodický.
- Prvky $a_1,a_2, \dots a_{s-1}$ tvoří předperiodu; prvky $a_s,a_{s+1}, \dots ,a_{s+h-1}$ periodu délky h.
- Každý periodický řetězový zlomek $[a_1; a_2, \dots ,a_{s-1},\overline{a_s, \dots ,a_{s+h-1}}]$, kde $h \geq 2$, lze psát ve tvaru $[a_1; a_2, \dots ,a_{s-1},r_s]$, kde zbytek r_s je ryze periodický řetězový zlomek.

Je-li $\alpha = [a_1; a_2,a_3, \dots ,a_k]$ konečný řetězový zlomek, řetězový zlomek $[a_k; a_{k-1}, \dots ,a_2,a_1]$ se nazývá **inverzní** řetězový zlomek ke zlomku α. Jestliže $[a_1; a_2, \dots ,a_k] = [a_k; a_{k-1}, \dots ,a_1]$, pak platí $\alpha = [a_1; a_2, \dots ,a_m,a_m, \dots ,a_2,a_1]$ nebo $[a_1; a_2, \dots ,a_m,a_{m+1},a_m, \dots ,a_2,a_1]$ a říkáme, že α je **symetrický** řetězový zlomek.

Věta 1.21. *Hodnota libovolného periodického řetězového zlomku je kvadratická iracionalita.*

Věta 1.22. *Každou kvadratickou iracionalitu lze vyjádřit periodickým řetězovým zlomkem.*

Věta 1.23. *Řetězový zlomek čísla* $\sqrt{N}$, $N \in \mathbb{N}$, $\sqrt{N} \in \mathbb{I}$, *má vždy tvar*

$$\sqrt{N} = [a_1; \overline{a_2; a_3; \dots ; a_3; a_2,2a_1}],$$

tj. perioda tohoto zlomku začíná hned po prvním prvku a_1 *a skládá se ze symetrické části* $a_2,a_3, \dots a_3,a_2$, *pro které následuje prvek* $2a_1$.

Kapitola 2

Diofantické rovnice

2.1 Lineární diofantické rovnice

Už ve třetím století našeho letopočtu se řecký matematik Diofantos zajímal o řešení rovnic, kdy za řešení připouštěl pouze celá čísla. Mnoho úloh z běžného života k těmto rovnicím vede, ty se na Diofantovu počest nazývají Diofantické rovnice. Tato práce se zaměří na podmínky řešitelnosti a metody řešení pouze vybraných typů diofantických rovnic. [13]

Definice 2.1. ***Lineární diofantickou rovnicí*** *o dvou neznámých x, y nazveme úlohu nalézt celá čísla x, y tak, aby platilo*

$$ax + by = c, \tag{2.1}$$

kde $a \neq 0$, $b \neq 0$, $c \in \mathbb{Z}$. Dvojice celých čísel x, y, která vyhovuje rovnici (2.1), se nazývá ***řešením*** *této rovnice a píšeme (x,y).*

Poznámka 2.1. V rovnici (2.1) můžeme rozlišit čtyři případy:

$$a > 0, b > 0 \tag{2.2}$$
$$a > 0, b < 0 \tag{2.3}$$
$$a < 0, b > 0 \tag{2.4}$$
$$a < 0, b < 0 \tag{2.5}$$

Všimněme si, že stačí řešit pouze případ (2.2). Pokud by nastal případ (2.5), stačí rovnici (2.1) vynásobit číslem -1, a tím získame případ (2.2). Případy (2.3) a (2.4) jsou symetrické, řeší se tedy analogicky. Stačí vyřešit pouze (2.3) substitucí $y = -z$. Tím opět získáme (2.2), kde rovnici řešíme pro neznámé x,z s kladnými koeficienty s tím, že se vrátíme k substituci. Uvažujme tedy dále rovnici (2.1) pro $a > 0$, $b > 0$.

Zaměříme se nejprve na případ, kdy $c \neq 0$.

Věta 2.1. *Diofantická rovnice*

$$ax + by = c, \tag{2.6}$$

kde $c \neq 0$, je řešitelná právě tehdy když

$$(a,b)|c. \tag{2.7}$$

Důkaz. Důkaz bude proveden ve dvou krocích. Nechť $d = (a,b)$.
Nejprve dokážeme, že pokud je rovnice řešitelná, tak platí (2.7). Předpokládejme, že existují taková celá čísla X a Y, že $aX + bY = c$. Potom, protože $d|a$ a $d|b$ platí $d|aX + bY$, tedy $d|c$ (podle věty 1.1).
Nyní dokážeme, že z (2.7) plyne řešitelnost rovnice (2.1). Uvažujme rovnici

$$ax + by = c.$$

Podle věty 1.8 existují taková celá čísla x_0 a y_0, že

$$ax_0 + by_0 = d.$$

Podle (2.7) platí $c = d \cdot q$, kde q je nějaké celé číslo. Obě strany vynásobíme číslem q a máme $ax_0q + by_0q = dq$. Nechť $x_1 = qx_0$, $y_1 = qy_0$. Potom platí

$$ax_1 + by_1 = qd = c.$$

To znamená, že dvojice (x_1,y_1) je řešením rovnice (2.1).

□

Věta 2.2. *[3] Nechť je dvojice (x_1,y_1) řešením diofantické rovnice*

$$ax + by = c.$$

Pak dvojice celých čísel (x,y) je řešením dané rovnice, právě když je

$$x = x_1 + \frac{b}{(a,b)} \cdot k, \qquad y = y_1 - \frac{a}{(a,b)} \cdot k,$$

kde k je libovolné celé číslo.

Důkaz. Nechť (x_1,y_1) je řešením rovnice $ax + by = c$, tj. $ax_1 + by_1 = c$. Předpokládejme nejprve, že také dvojice (x,y) je řešením dané rovnice. Pak

$$ax + by = c \wedge ax_1 + by_1 = c,$$

tedy

$$ax + by = ax_1 + by_1.$$

Označíme-li $d = (a,b)$, tak po úpravě dostáváme

$$\frac{a}{d} \cdot (x - x_1) = \frac{b}{d} \cdot (y_1 - y). \tag{2.8}$$

Protože $\frac{a}{d} \mid \frac{b}{d}(y_1 - y)$ a $\left(\frac{a}{d},\frac{b}{d}\right) = 1$ (Věta 1.9), je $\frac{a}{d} \mid (y_1 - y)$, což znamená, že existuje $k \in \mathbb{Z}$ tak, že

$$y_1 - y = \frac{a}{d} \cdot k,$$

a tedy $y = y_1 - \frac{a}{d} \cdot k$.

Dále postupujeme analogicky. Protože $\frac{b}{d} \mid \frac{a}{d}(x - x_1)$ a $\left(\frac{a}{d},\frac{b}{d}\right) = 1$, je $\frac{b}{d} \mid (x - x_1)$,

což znamená, že existuje $k' \in \mathbb{Z}$ tak, že $x - x_1 = \frac{b}{d} \cdot k'$, a tedy $x = x_1 + \frac{b}{d} \cdot k'$. Dosadíme-li $x - x_1$ a $y_1 - y$ do vztahu (2.8), máme

$$\frac{a}{d} \cdot \frac{b}{d} \cdot k' = \frac{b}{d} \cdot \frac{a}{d} \cdot k,$$

a proto $k' = k$. Tedy $x = x_1 + \frac{b}{d} \cdot k$, $y = y_1 - \frac{a}{d} \cdot k$, $k \in \mathbb{Z}$.

V dalším předpokládejme, že $x = x_1 + \frac{b}{(a,b)} \cdot k$, $y = y_1 - \frac{a}{(a,b)} \cdot k, k \in \mathbb{Z}$. Pak po dosazení máme

$$\begin{aligned} ax + by &= a \cdot \left(x_1 + \frac{b}{(a,b)} \cdot k \right) + b \cdot \left(y_1 - \frac{a}{(a,b)} \cdot k \right) = \\ &= ax_1 + \frac{ab}{(a,b)} \cdot k + by_1 - \frac{ab}{(a,b)} \cdot k = ax_1 + by_1 = c. \end{aligned}$$

Tedy (x,y) je řešením dané rovnice.

□

Poznámka 2.2.

- Je-li rovnice (2.1) řešitelná, má nekonečně mnoho řešení.
- Speciální případ rovnice (2.1) je rovnice

  $$ax + by = 0.$$

  Dvojice $(x,y) = (0,0)$ je jedním z řešení dané rovnice, nazveme ho triviální řešení. Všechna další celočíselná řešení této rovnice jsou podle věty 2.2 dvojice čísel
  $x = \frac{b}{(a,b)} \cdot k$, $y = -\frac{a}{(a,b)} \cdot k$, kde k je libovolné celé číslo.

2.1.1 Řešení Euklidovým algoritmem

Ukážeme si nyní, jak nalézt jedno řešení (x,y) rovnice $ax + by = c$. Následující část je čerpána z [8].

Euklidovým algoritmem určíme (a,b). Nejdříve nalezneme celá čísla x_0, y_0 taková, že $ax_0 + by_0 = (a,b)$ (Věta 1.8). Dále vyjdeme ze soustavy rovností uvedených ve větě 1.7. Předposlední rovnost lze psát ve tvaru

$$r_{n-2} = r_{n-1}q_{n-1} + r_n = r_{n-1}q_{n-1} + (a,b),$$

z čehož po úpravě dostaneme

$$(a,b) = r_{n-2} - q_{n-1}r_{n-1}. \tag{2.9}$$

Vyjádřili jsme (a,b) ve tvaru $Ar_{n-2} + Br_{n-1}$, kde $A = 1$, $B = q_{n-1}$. Zaměříme se nyní na předcházející rovnost

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}.$$

Odtud je

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$$

a po dosazení do (2.9) dostáváme

$$\begin{aligned}(a,b) &= r_{n-2} - q_{n-1}(r_{n-3} - r_{n-2}q_{n-2}) = \\ &= (-q_{n-1})r_{n-3} + (1 + q_{n-1}q_{n-2})r_{n-2} = \\ &= Cr_{n-3} + Dr_{n-2},\end{aligned}$$

kde $C = -q_{n-1}$, $D = 1 + q_{n-1}q_{n-2}$ atd.
Budeme-li takto "zdola"postupovat "nahoru", dostaneme nakonec největší společný dělitel vyjádřený ve tvaru

$$(a,b) = ax_0 + by_0, \qquad \text{kde } x_0,y_0 \in \mathbb{Z}.$$

Postup řešení rovnice $ax + by = c$ bychom tedy mohli shrnout v těchto bodech.

- Euklidovým algoritmem najdeme $d = (a,b)$.
- Číslo d vyjádříme ve tvaru

$$d = ax_0 + by_0, \qquad x_0,y_0 \in \mathbb{Z}. \tag{2.10}$$

- Je-li rovnice řešitelná, pak existuje $q \in \mathbb{Z}$ tak, že $c = dq$.
- Obě strany rovnice (2.10) vynásobíme číslem q a dostaneme

$$dq = a(x_0q) + b(y_0q).$$

Odtud

$$\begin{aligned}x_1 &= x_0q \\ y_1 &= y_0q.\end{aligned}$$

kde (x_1,y_1) je jedním řešením rovnice $ax + by = c$. Všechna řešení najdeme podle věty 2.2.

2.1.2 Eulerova metoda

Jinou základní metodou, jak najít řešení zejména lineární diofantické rovnice o dvou neznámých je **Eulerova metoda**, která je popsána v [8].
Z rovnice $ax + by = c$ vyjádříme tu neznámou, jejíž koeficient je v absolutní hodnotě menší. Bez újmy na obecnosti uvažujme, že nejmenší je v absolutní hodnotě koeficient a. Dále vyjádříme neznámou x a máme

$$x = \frac{c - by}{a}.$$

Tento podíl lze přepsat do tvaru

$$\frac{c - by}{a} = ky + \frac{c - py}{a}, \quad k \in \mathbb{Z}, |p| \leq |a|.$$

Protože x,$y \in \mathbb{Z}$, musí být číslo $\dfrac{c-py}{a}$ celé, tedy

$$c - py = aq, \quad q \in \mathbb{Z}.$$

Vyjádříme neznámou y:

$$y = \frac{c-aq}{p}.$$

Protože je y celé číslo, lze vyjádřit $c-aq$ ve tvaru násobku čísla p. Dále postupujeme analogicky. Tento proces je konečný, protože koeficienty u neznámých jsou neúplné podíly a zbytky v Euklidově algoritmu pro koeficienty a, b dané rovnice.

2.1.3 Hledání řešení pomocí řetězových zlomků

Při demonstraci **dalšího způsobu** nalezení řešení (x_1,y_1) rovnice (2.1) použijeme řetězové zlomky. Tato metoda je popsána v [12].
Předpokládejme, že $(a,b) = 1$. Vyjdeme ze vztahu

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n. \tag{2.11}$$

Racionální číslo $\dfrac{b}{a}$ rozvineme v řetězový zlomek

$$\frac{b}{a} = [a_1; a_2, \ldots, a_n] = \frac{P_n}{Q_n}.$$

Protože obě čísla $\dfrac{b}{a}$, $\dfrac{P_n}{Q_n}$ jsou v základním tvaru, je $b = P_n$ a $a = Q_n$.
Určíme přibližné zlomky $\dfrac{P_{n-1}}{Q_{n-1}}$, $\dfrac{P_n}{Q_n} = \dfrac{b}{a}$. Z rovnosti (2.11) po dosazení dostáváme

$$bQ_{n-1} - aP_{n-1} = (-1)^n.$$

Vynásobíme obě strany číslem $(-1)^n c$:

$$bc(-1)^nQ_{n-1} - ac(-1)^nP_{n-1} = c,$$

tj.

$$ac(-1)^{n-1}P_{n-1} + bc(-1)^nQ_{n-1} = c, \tag{2.12}$$
$$a[(-1)^{n-1}P_{n-1}c] + b[(-1)^nQ_{n-1}c] = c,$$

odkud srovnáním s rovnicí

$$ax + by = c$$

dostáváme jedno řešení

$$x_1 = (-1)^{n-1}P_{n-1}c, \tag{2.13}$$
$$y_1 = (-1)^nQ_{n-1}c \tag{2.14}$$

rovnice (2.11). Užitím věty 2.2 najdeme všechna řešení diofantické rovnice $ax + by = c$. [12]
Všechny tři metody řešení lineární diofantické rovnice o dvou neznámých jsou názorně demonstrovány na příkladech ve sbírce řešených příkladů.

2.1.4 Lineární diofantické rovnice o n neznámých

Uvažujme dále rovnici

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{2.15}$$

kde a_1,a_2,$\ldots$,a_n,b jsou daná celá čísla, řešením jsou všechny $n-$tice celých čísel $(x_1,\ldots,x_n)$ vyhovující vztahu (2.15). Rovnici (2.15) nazýváme **lineární diofantická rovnici o n neznámých.** Pro řešitelnost rovnice (2.15) lze stejně jako u diofantických rovnic se dvěma neznámými dokázat následující větu.

Věta 2.3. *Rovnice (2.15) je řešitelná právě když $d = (a_1,\ldots,a_n)|b$, přičemž řešení závisí na $n-1$ nezávislých celočíselných parametrech.*

Důkaz. Důkaz věty lze najít v [4].

□

Lze dokázat i následující tvrzení.

Věta 2.4. *[8] Jsou-li a_1,a_2,$\ldots$,a_n celá čísla taková, že alespoň jedno z nich je nenulové, pak existují celá čísla t_1,t_2,$\ldots$,t_n tak, že*

$$(a_1,a_2,\ldots a_n) = a_1t_1 + a_2t_2 + \cdots + a_nt_n.$$

Dále $(a_1,a_2,\ldots,a_n) = 1$, právě tehdy když existují celá čísla t_1,t_2,$\ldots$,t_n taková, že

$$a_1t_1 + a_2t_2 + \cdots + a_nt_n = 1.$$

Poznámka 2.3. [8]

- Při řešení rovnice (2.15) můžeme předpokládat, že všechny koeficienty $a_1,\ldots,a_n$ jsou přirozená čísla, protože nulové koeficienty neovlivňují řešení a je-li některý koeficient $a_i < 0$, $i = 1,2,\cdots,n$, můžeme použít substituci $x_i' = -x_i$.
- Jsou-li si některé koeficienty rovny, např. $a_1 = a_2$, položíme $x_1 + x_2 = x$ a dostaneme rovnici

  $$a_1x + a_3x_3 + \cdots + a_nx_n = b. \tag{2.16}$$

  Z každého řešení $(x,x_3,\ldots x_n)$ rovnice (2.16) můžeme získat řešení rovnice (2.15) tak, že x_1 bude libovolné celé číslo a $x_2 = x - x_1$. Dále můžeme tedy předpokládat, že všechny koeficienty rovnice (2.15) jsou navzájem různé.

Věta 2.5. *[8] Je-li $(y_1,y_2,\ldots,y_n)$ řešením rovnice (2.15) a položíme-li*

$$\begin{aligned} x_i &= y_i + a_ns_i, \quad i = 1,2,\ldots,n-1 \\ x_n &= y_n - a_1s_1 - a_2s_2 - \cdots - a_{n-1}s_{n-1}, \end{aligned}$$

kde s_1,s_2,$\ldots$,s_n jsou libovolná celá čísla, dostaneme celá čísla x_1,x_2,$\ldots$,x_n, která vyhovují rovnici (2.15). Je-li rovnice (2.15) řešitelná, má tedy nekonečně mnoho řešení.

Poznámka 2.4.

K řešení rovnice (2.15) využijeme analogii prvního z popsaných postupů řešení rovnice (2.6) pomocí Euklidova algoritmu:

- Nejprve nalezneme jedno řešení $[y_1,y_2,\ldots,y_n]$ rovnice (2.15) a pak podle vztahů z Věty 2.5 všechna řešení této rovnice.
- Řešení $(y_1,y_2,\ldots,y_n)$ najdeme takto: je-li $d=(a_1,a_2,\ldots,a_n)$ a $d|b$, je $b=dq$, $q\in\mathbb{Z}$. Dále vyjádříme d ve tvaru

$$d=a_1t_1+a_2t_2+\cdots+a_nt_n,\qquad t_1,\cdots,t_n\in\mathbb{Z},$$

a vynásobíme obě strany rovnice číslem q. Dostaneme

$$dq=a_1(t_1q)+a_2(t_2q)+\cdots+a_n(t_nq),$$

tj.

$$b=a_1y_1+a_2y_2+\cdots+a_ny_n,$$

kde $y_i=t_iq_i$, $i=1,2,\ldots,n$.

Poznámka 2.5. Rovnici (2.15) lze řešit také Eulerovou metodou.

2.2 Diofantické rovnice vyšších stupňů - vybrané metody řešení

V další části textu budou zdrojem především knihy [13], [2] a [5]. Řešení diofantických rovnic vyššího stupně je o mnoho náročnější než řešení lineárních diofantických rovnic. Už při přítomnosti druhé mocniny vznikají velké potíže a často nám stačí určit, zda je daná rovnice řešitelná, případně najít několik řešení, málokdy se nám totiž podaří určit všechna řešení. Zmíněny tedy budou pouze vybrané typy rovnic vyššího stupně a vybrané metody řešení. Pro lepší názornost budou přímo u některých metod uvedeny řešené příklady. Pokud nebude řečeno jinak, zadání i řešení budou převzaty z citovaných zdrojů.

Definice 2.2. *Nechť $f(x_1,\ldots,x_n)$ je nenulový polynom s celočíselnými koeficienty o n neznámých, $n\geq 2$, a pro stupeň m polynomu $f(x_1,\ldots,x_n)$ platí $m\geq 1$. Pak se rovnice*

$$f(x_1,\ldots,x_n)=k,$$

kde $k\in\mathbb{Z}$, nazývá ***diofantická rovnice řádu*** *m.*

Definice 2.3. *Rovnice ve tvaru*

$$ax^2+bx+cxy+dy+ey^2=f, \tag{2.17}$$

kde x, y jsou neznámé, $a,b,c,d,e,f\in\mathbb{Z}$ a zároveň $a\neq 0\vee b\neq 0\vee c\neq 0$, se nazývá ***kvadratická diofantická rovnice o dvou neznámých.***

2.2.1 Metoda faktorizace

První metoda, která zde bude zmíněna, se nazývá **metoda faktorizace.** Začněme rovnicemi (2.17). Některé z nich lze totiž přepsat ve tvaru

$$(ax+by)(cx+dy)=k. \tag{2.18}$$

Ukážeme si, jak najít všechna řešení takové rovnice. Jestliže x a y jsou celočíselnými řešeními rovnice (2.18), pak čísla $ax + by$, $cx + dy$ jsou celá čísla a jsou sdruženými děliteli čísla k. Řešení rovnice (2.18) budeme proto hledat tak, že si zvolíme nějakého dělitele k_1 čísla k. Dále nechť je k_2 sdružený dělitel čísla k. Nechť

$$ax + by = k_1$$
$$cx + dy = k_2.$$

Dostaneme tak soustavu dvou lineárních rovnic se dvěma neznámými. Pokud je tato soustava řešitelná a pokud jsou x a y celá čísla, je řešení rovnice (2.18) určeno jednoznačně. Dále z této metody vyplývá, že rovnice typu (2.18) mají konečně mnoho řešení, protože počet dvojic navzájem sdružených dělitelů je konečný a ke každé dvojici sdružených dělitelů náleží buď jedno nebo žádné řešení. Zároveň může být rovnice (2.18) neřešitelná.
Pro diofantickou rovnici řádu m lze metodu faktorizace popsat následujícím způsobem. Danou rovnici upravíme do tvaru

$$A_1 \cdot A_2 \cdot \cdots \cdot A_n = B, \tag{2.19}$$

kde $A_1, \ldots, A_n$ jsou výrazy obsahující neznámé, které pro celočíselné hodnoty neznámých nabývají celočíselných hodnot, a B je číslo (případně výraz), jehož rozklad na prvočísla známe. Pak totiž existuje pouze konečně mnoho rozkladů čísla B na n celočíselných činitelů $k_1, \ldots, k_n$. Vyšetříme-li pak pro každý z těchto rozkladů soustavu rovnic

$$\begin{aligned} A_1 &= k_1, \\ A_2 &= k_2, \\ &\vdots \\ A_n &= k_n, \end{aligned}$$

získáme všechna řešení rovnice (2.19). Pro názornost zde bude uveden řešený příklad.

Příklad 2.1. *Najděte všechna celočíselná řešení rovnice*

$$(x^2 + 1)(y^2 + 1) + 2(x - y)(1 - xy) = 4(1 + xy).$$

Řešení. V rovnici provedeme drobné úpravy a dostaneme

$$x^2y^2 + x^2 + y^2 + 1 + 2(x - y)(1 - xy) = 4 + 4xy.$$

Po přeskupení máme

$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x - y)(1 - xy) = 4,$$

což můžeme napsat jako

$$[xy - 1 - (x - y)]^2 = 4,$$

nebo také

$$(x + 1)(y - 1) = \pm 2.$$

Jestliže $(x + 1)(y - 1) = 2$, dostaneme soustavy rovnic

$$\begin{aligned} x+1&=2 \\ y-1&=1 \end{aligned} \qquad \begin{aligned} x+1&=-2 \\ y-1&=-1 \end{aligned} \qquad \begin{aligned} x+1&=-1 \\ y-1&=-2 \end{aligned} \qquad \begin{aligned} x+1&=1 \\ y-1&=2 \end{aligned}$$

Položíme-li $(x+1)(y-1)=-2$, máme další čtyři soustavy lineárních rovnic.

$$\begin{aligned} x+1&=2 \\ y-1&=-1 \end{aligned} \qquad \begin{aligned} x+1&=-2 \\ y-1&=1 \end{aligned} \qquad \begin{aligned} x+1&=1 \\ y-1&=-2 \end{aligned} \qquad \begin{aligned} x+1&=-1 \\ y-1&=2 \end{aligned}$$

Všechna řešení soustav zapíšeme do tabulky.

x	1	-3	0	-2	1	-3	0	-2
y	2	0	3	-1	0	2	-1	3

Zadání i řešení z [2].

2.2.2 Řešení pomocí nerovností

Metoda řešení diofantických rovnic pomocí nerovností je založena na myšlence, že pro libovolná reálná čísla a, b existuje jen konečně $x \in \mathbb{Z}$ tak, že

$$a < x < b. \tag{2.20}$$

Proto při řešení dané rovnice hledáme taková čísla a, b, aby nerovnosti (2.20) pro některou neznámou x byly důsledkem dané rovnice. Rovnici můžeme zjednošit postupným dosazením konečného počtu celých čísel ležících mezi čísly a, b. Pro přehlednost a názornost zde budou uvedeny dva příklady demonstrující popsanou metodu.

Příklad 2.2. *Najděte všechny celočíselné dvojice* (x,y) *takové, že*

$$x^3+y^3=(x+y)^2.$$

Řešení. Je zřejmé, že každá dvojice tvaru $(k,-k)$, $k \in \mathbb{Z}$ je řešením. Uvažujme tedy dále, že $x+y \neq 0$. Po úpravách máme

$$\begin{aligned} (x+y)(x^2-xy+y^2)&=(x+y)^2 \\ x^2-xy+y^2&=x+y. \end{aligned}$$

V úpravách budeme pokračovat a dostaneme

$$\begin{aligned} 2x^2-2xy+2y^2-2x-2y&=0 \\ x^2-2xy+y^2+x^2-2x+1+y^2-2y+1&=2 \\ (x-y)^2+(x-1)^2+(y-1)^2&=2. \end{aligned}$$

Protože musí být

$$(x-1)^2 \leq 1$$

a zároveň

$$(y-1)^2 \leq 1,$$

je interval, kam náleží neznámé x, y, omezen na $\langle 0,2 \rangle$. Všechna řešení zapíšeme do tabulky

x	0	1	1	2	2
y	1	0	2	1	2

Zadání i řešení z [2].

Příklad 2.3. *Řešte v $\mathbb{Z}$ diofantickou rovnici*

$$6x^2 + 5y^2 = 74.$$

Řešení. Protože pro libovolné $y \in \mathbb{Z}$ platí $5y^2 \geq 0$, musí pro libovolné řešení dané rovnice platit

$$74 = 6x^2 + 5y^2 \geq 6x^2,$$

odkud $x^2 < \frac{37}{3}$, tedy $-3 \leq x \leq 3$, proto x^2 je některé z čísel 0,1,4,9. Dosazením do rovnice postupně dostáváme

$$\begin{aligned} 5y^2 &= 74 \\ 5y^2 &= 68 \\ 5y^2 &= 50 \\ 5y^2 &= 20. \end{aligned}$$

První tři případy jsou ve sporu s podmínkou $y \in \mathbb{Z}$, z posledního dostáváme

$$\begin{aligned} y^2 &= 4 \\ y &= \pm 2. \end{aligned}$$

Rovnice má tedy čtyři řešení zapsané v následující tabulce:

x	3	3	-3	-3
y	2	-2	2	-2

Zadání i řešení z [5].

2.2.3 Další typy rovnic

Zaměříme se nyní na rovnice typu

$$x^2 - y^2 = k. \tag{2.21}$$

Nejprve se zaměříme na řešitelnost. Ověříme, že taková rovnice není řešitelná, jestliže $k = 4t + 2$.
Je-li a libovolné celé číslo, pak je buď $a = 2l$ nebo $a = 2l + 1$, a proto každá druhá mocnina celého čísla a je buď tvaru $a = 4l^2 = 4s$ nebo $a^2 = (2l + 1)^2 = 4s' + 1$. Tedy druhá mocnina žádného celého čísla nemůže mít tvar $a^2 = 4t + 2$.

- Pro $x^2 = 4s$ a $y^2 = 4r$ nebo $x^2 = 4s + 1$ a $y^2 = 4r + 1$, je $x^2 - y^2 = 4t$.
- Pro $x^2 = 4s + 1$ a $y^2 = 4r$ je $x^2 - y^2 = 4t + 1$
- Pokud $x^2 = 4s$ a $y^2 = 4r + 1$, je $x^2 - y^2 = 4t + 3$.

Rozdíl $x^2 - y^2$ nemůže být nikdy tvaru $4t + 2$. Lze naopak i ukázat, že pokud je $k \neq 4t + 2$, pak je rovnice (2.21) řešitelná a dále se použije metoda faktorizace.

Příklad 2.4. *Řešte v oboru celých čísel rovnici*

$$x^2 + xy + y^2 = x^2y^2.$$

Řešení. Nejprve zde bude předveden postup řešení z [13]. Rovnici můžeme přepsat na

$$(2xy + 1)^2 = [2(x + y)]^2 + 1.$$

Položíme-li

$$\begin{aligned} X &= 2xy + 1 \\ Y &= 2(x + y), \end{aligned}$$

dostaneme rovnici typu

$$X^2 - Y^2 = 1.$$

Rozdíl druhých mocnin celých čísel se rovná jedné pouze pro čísla 1 nebo -1 a 0. Nechť

$$\begin{aligned} 2xy + 1 &= 1 \\ 2(x + y) &= 0. \end{aligned}$$

Řešením bude dvojice $x = y = 0$. Jestliže položíme

$$\begin{aligned} 2xy + 1 &= -1 \\ 2(x + y) &= 0, \end{aligned}$$

dostaneme dosazením y z druhé rovnice do první kvadratickou rovnici

$$x^2 = 1,$$

odkud $x = 1$ a $x = -1$ a dostali jsme tak další dvě řešení. Všechna řešení zapíšeme do tabulky.

x	0	1	-1
y	0	-1	1

Pro srovnání bude uvedena metoda řešení stejného příkladu z [5]. Tato metoda je založena již popsaném postupu řešení diofantických rovnic pomocí nerovností. Máme tedy rovnici

$$x^2 + xy + y^2 = x^2y^2.$$

Protože jsou v rovnici neznámé x, y zastoupeny symetricky, můžeme předpokládat, že $x^2 \leq y^2$, odkud plyne $xy \leq y^2$, a proto

$$x^2y^2 = x^2 + xy + y^2 \leq y^2 + y^2 + y^2 = 3y^2.$$

Platí tedy $y = 0$ nebo $x^2 \leq 3$. Dosazením do rovnice dostáváme v prvním případě $x = 0$, ve druhém pro $x = 0$ opět $y = 0$. Pro $x = 1$ je $y = -1$ a pro $x = -1$ je $y = 1$. Rovnice má tedy tři řešení vypsané v tabulce výše.

Předvedeme dále metodu řešení **dalšího typu** diofantické rovnice $n-$tého stupně, která má tvar

$$a_n x^n + \cdots + a_1 x + a_0 = ky, \tag{2.22}$$

kde a_i a k jsou celá čísla. Je důležité si povšimnout, že jedna z neznámých figuruje pouze v první mocnině. Dále je třeba říct, že ne každá taková rovnice je řešitelná. Příkladem rovnice, která není řešitelná, může být rovnice $x^2 + 2 = 4y$.Zmíněná rovnice není řešitelná, protože $x^2 = 4y - 2 = 4y' + 2$. Výše jsme ale ukázali, že žádná druhá mocnina celého čísla nemůže mít tento tvar.
Pro další bude bez důkazu (lze najít v [13]) uvedena následující věta.

Věta 2.6. *Nechť je dvojice* (x_0,y_0) *řešením rovnice* (2.22). *Nechť dále* $t \in \mathbb{Z}$. *Potom ke každému číslu, které má tvar* $x = x_0 + kt$, *existuje takové* y, *že dvojice* (x,y) *je řešením rovnice* (2.22).

Jestliže známe jedno řešení rovnice (2.22), použitím této věty dokážeme najít nekonečně mnoho dalších řešení. Zbývá tedy jen popsat metodu, jak najít jedno řešení rovnice (2.22).

Důsledek. Jestliže je rovnice typu (2.22) řešitelná, pak existují takové její řešení (X,Y), že platí $|X| < |k|$.

Odtud plyne jednoduchá metoda pro nalezení jednoho řešení rovnice. Zjistíme, které z čísel $0,1,\ldots,|k|-1$ dosazené za x dává řešení rovnice. Jestliže pro žádné z nich nedostaneme řešení, rovnice je neřešitelná. Jestliže se naopak přesvědčíme, že k některému x_0 z těchto čísel existuje takové y_0, že dvojice (x_0,y_0) je řešením, pak podle věty 2.6 umíme najít nekonečně mnoho řešení. Specialitou těchto rovnic je, že jsou buď neřešitelné, nebo mají nekonečně mnoho řešení. [13]

2.3 Pythagorejské trojúhelníky

Jedna z nejznámějších diofantických rovnic je rovnice

$$x^2 + y^2 = z^2.$$

Definice 2.4. *Uspořádaná trojice přirozených čísel* (x,y,z), *která splňuje rovnost*

$$x^2 + y^2 = z^2, \tag{2.23}$$

se nazývá ***pythagorejská*** *trojice.*

Definice 2.5. *Trojúhelník, jehož délky stran tvoří pythagorejskou trojici, se nazývá* ***pythagorejský trojúhelník.***

Je zřejmé, že každý pythagorejský trojúhelník je pravoúhlý. Dále můžeme pojmy pythagorejská trojice a pythagorejský trojúhelník pro jejich vzájemnou provázanost libovolně zaměňovat.

Definice 2.6. *Pythagorejský trojúhelník* (x,y,z) *se nazývá* ***primitivní****, jestliže* $(x,y,z) = 1$.

Pomocí každého primitivního pythagorejského trojúhelníku jsme schopni najít nekonečně velké množství pythagorejských trojúhelníků, které primitivní nejsou.

Věta 2.7. *Jestliže je (x,y,z) pythagorejský trojúhelník, tak i trojice (kx,ky,kz) je pythagorejský trojúhelník, kde k je přirozené číslo.*

Opačně, pomocí každého neprimitivního pythagorejského trojúhelníku jsme schopni získat primitivní Pythagorejský trojúhelník.

Věta 2.8. *Každý pythagorejský trojúhelník (x,y,z) lze napsat ve tvaru $(x,y,z) = (kx,ky,kz)$, kde k je přirozené číslo a (x_1,y_1,z_1) je primitivní pythagorejský trojúhelník.*

Důkaz věty 2.8 lze najít v [13]. Najděme nyní všechny primitivní pythagorejské trojúhelníky.

Věta 2.9. *Každý primitivní pythagorejský trojúhelník se sudým y lze napsat ve tvaru*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{2.24}$$

kde m a n jsou nesoudělná přirozená čísla taková, že $m > n$ a součet $m + n$ je lichý.

Důkaz. Jestliže je (x,y,z) primitivní pythagorejský trojúhelník, je jedno z čísel sudé a druhé liché. Čísla x a y nemůžou být obě sudá, protože jsou nesoudělná. Nemůžou být ani lichá, protože by jejich druhá mocnina měla tvar $4k+1$ a součet jejich druhých mocnin by měl tvar $4s + 2$; z^2 ale tento tvar mít nemůže. [13].
Z rovnice

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

vidíme, že trojice daná (2.24) splňuje rovnici (2.23) a y je sudé. Protože x musí být liché, můžeme předpokládat bez újmy na obecnosti, že m je liché a n je sudé. Navíc, je-li největší společný dělitel $d = (m^2 - n^2,2mn,m^2 + n^2) \geq 2$, pak d dělí

$$2m^2 = (m^2 + n^2) + (m^2 - n^2)$$

a

$$2n^2 = (m^2 + n^2) - (m^2 - n^2).$$

Protože m a n jsou nesoudělná, je $d = 2$. Proto m^2+n^2 je sudé, což je v rozporu s předpokladem, že m je liché a n sudé. Z toho vyplývá, že $d = 1$, tedy trojice daná vztahy (2.24) je primitivní.
Nechť je naopak (x,y,z) primitivní pythagorejská trojice, kde $y = 2a$. Potom x a z jsou lichá a v důsledku toho $z + x$ a $z - x$ jsou sudá. Nechť

$$z + x = 2b$$
$$z - x = 2c.$$

Můžeme předpokládat, že b a c jsou nesoudělná, jinak by čísla z a x měla netriviálního společného dělitele. Na druhou stranu

$$4a^2 = y^2 = z^2 - x^2 = (z - x)(z + x) = 4bc,$$

tedy $a^2 = bc$. Protože b a c jsou nesoudělná, je $b = m^2$ a $c = n^2$ pro libovolná přirozená čísla m a n. Dostáváme, že součet $m + n$ je lichý a

$$x = b - c = m^2 - n^2, \quad y = 2mn, \quad z = b + c = m^2 + n^2.$$

Věta i důkaz z [2].

□

Ukážeme si ale i jiné způsoby, kterými se matematici snažili získat pythagorejské trojice. Zdrojem pro následující část je zejména [1]. Za tímto účelem se vrátíme v čase před rok, kdy byla objevena výše popsaná metoda. Traduje se totiž, že dílčí řešení rovnice (2.23) ukázal již sám Pythagoras:

$$a = 2n + 1, \quad b = 2n^2 + 2n, \quad c = 2n^2 + 2n + 1, \quad n \geq 1. \tag{2.25}$$

Ke vztahům (2.25) pravděpodobně došel pomocí vztahu

$$(2k - 1) + (k - 1)^2 = k^2 \tag{2.26}$$

a potom hledáme taková k, která je $(2k - 1)$ dokonalý čtverec, tj. $2k - 1 = m^2$. Protože je m^2 liché, pak m musí být také liché. Takto dostaneme

$$k = \frac{m^2 + 1}{2}$$

a

$$k - 1 = \frac{m^2 - 1}{2}.$$

Proto můžeme vztah (2.26) psát ve tvaru

$$m^2 + \left(\frac{m^2 - 1}{2}\right)^2 = \left(\frac{m^2 + 1}{2}\right)^2,$$

odkud je vidět, že rovnici (2.23) splňují čísla

$$a = m, \quad b = \frac{m^2 - 1}{2}, \quad c = \frac{m^2 + 1}{2}. \tag{2.27}$$

Nakonec pokud ve vztahu (2.27) položíme $m = 2n + 1$, $n \geq 1$, máme (2.25). Všimněme si,že součet délek delší odvěsny a přepony je $4n^2 + 4n + 1 = (2n + 1)^2$, což je druhá mocnina kratší odvěsny. Lze snadno ověřit, že (2.25) skutečně řeší rovnici (2.23). Z faktu, že $c - b = 1$ vyplývá to, že čísla b a c jsou nesoudělná, a v důsledku toho musí být pythagorejské trojice vygenerované (2.25) primitivní. V následující tabulce si ukážeme některé takové trojice.

n	a	b	c
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61
6	13	84	85
7	15	112	113
8	17	144	145
9	19	180	181
10	21	220	221
11	23	264	265
12	25	312	313

V další tabulce si ukážeme pythagorejské trojúhelníky získáné vztahy (2.25), pokud položíme $n = 10{,}10^2, \ldots, 10^5$.

n	a	b	c
10	21	220	221
10^2	201	20200	20201
10^3	2001	2002000	2002001
10^4	20001	200020000	200020001
10^5	200001	20000200000	20000200001

Také je vidět, že Pythagorovo řešení má takovou speciální vlastnost, že generuje trojice, u nichž je přepona vždy o 1 jednotku delší než delší z odvěsen.

Podle řeckého filozofa Proklose, který žil v letech 410 - 485 n.l., našel Platón (žijící v letech 427-347 př. n. l.) metodu kombinující algebru i geometrii. Jeho řešení rovnice (2.23) je

$$a = 2n, \quad b = n^2 - 1, \quad c = n^2 + 1, \quad n \geq 2. \tag{2.28}$$

V následující tabulce jsou vypsány některé z trojic, které takto můžeme získat.

n	a	b	c
2	4	3	5
3	6	8	10
4	8	15	17
5	10	24	26
6	12	35	37
7	14	48	50
8	16	63	65
9	18	80	82
10	20	99	101
11	22	120	122
12	24	143	145

Z (2.28) vyplývá, že délka přepony je delší o dvě jednotky než jedna z odvěsen. Navíc pro $n = 4$ máme pythagorejskou trojici (8,15,17), kterou nelze získat z (2.25). Dále pro $n = 2k + 1$, $k \geq 1$, ze vztahů (2.28) dostaneme

$$a = 2(2k + 1), \quad b = 4k^2 + 4k, \quad c = 4k^2 + 4k + 2, \quad k \geq 1. \tag{2.29}$$

Tedy pro lichá n (2.28) negeneruje primitivní pythagorejské trojice a po vydělení vztahů (2.29) číslem 2 dostaneme vztahy (2.25). Celkem tedy vztahy (2.28) generují trojice již získané (2.25).

Na závěr ukažme pro zajímavost tabulku trojic vygenerované vztahy (2.28) po dosazení $n = 2 \cdot 10$, $2 \cdot 10^2$, atd.

n	a	b	c
20	40	399	401
200	400	39999	40001
2000	4000	3999999	4000001
20000	40000	399999999	400000001

Již tedy víme, že ani vztahy (2.28) negenerovaly všechny pythagorejské trojice a nebylo tomu tak, dokud Eukleidés (325-265 př.n.l.) neformuloval vztahy (2.24), které generují následující trojúhelníky. Písmenem S označíme jejich obsah.

m	n	a	b	c	S
2	1	3	4	5	6
3	2	5	12	13	30
4	1	15	8	17	60
4	3	7	24	25	84
5	2	21	20	29	210
5	4	9	40	41	180
6	1	35	12	37	210
6	5	11	60	61	330
7	2	45	28	53	630
7	4	33	56	65	924
7	6	13	84	85	546
8	1	63	16	65	504
8	3	55	48	73	1320
8	5	39	80	89	1560
8	7	15	112	113	840

Nakonec se zaměříme na spojitost mezi pythagorejskými trojicemi a Fibonacciovou posloupností [10]. Prvních několik členů Fibonacciovy posloupnosti je

$$1,1,2,3,5,8,13,21,34,55,89,144,233,\ldots$$

Obecně ji popíšeme rekurentně tak, že

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_n &= F_{n-1} + F_{n-2}, \quad n > 2. \end{aligned}$$

Dále provedeme následující postup:

1. Označme čísla x, y, $x+y$, $x+2y$ jako čtyři po sobě jdoucí čísla ve Fibonacciově posloupnosti.

2. Položme a rovno součinu prvního a čtvrtého čísla, tj.

$$a = x(x+2y) = x^2 + 2xy$$

3. Dále položíme b rovno dvojnásobku součinu prostředních dvou čísel, tj.

$$b = 2y(x+y) = 2xy + 2y^2$$

4. Vypočítáme

$$\begin{aligned} c = \sqrt{a^2+b^2} &= \sqrt{(x^2+2xy)^2 + (2xy+2y^2)^2} = \\ &= \sqrt{x^4 + 4x^3y + 4x^2y^2 + 4x^2y^2 + 8xy^3 + 4y^4} = \\ &= \sqrt{x^4 + 4x^3y + 8x^2y^2 + 8xy^3 + 4y^4} = \\ &= \sqrt{(x^2+2xy+2y^2)^2} = \\ &= x^2 + 2xy + 2y^2 \end{aligned}$$

Zajímavostí může být, že $c = \sqrt{a^2 + b^2}$ je dokonalým čtvercem nehledě na to, zda čísla x a y jsou členy Fibonacciovy posloupnosti. Navíc ve výpočtech výše je číslo c také členem Fibonacciovy posloupnosti.
Kompletní důkaz v [10] nebo v [1].
V následující tabulce budou vypsány některé z takto získaných trojic, výčet ale není zdaleka úplný.

n	F_n	F_{n+1}	F_{n+2}	F_{n+3}	a	b	c	pozice c
1	1	1	2	3	3	4	5	F_5
2	1	2	3	5	5	12	13	F_7
3	2	3	5	8	16	30	34	F_9
4	3	5	8	13	39	80	89	F_{11}
5	5	8	13	21	105	208	233	F_{13}
6	8	13	21	34	272	546	610	F_{15}
7	13	21	34	55	715	1428	1597	F_{17}
8	21	34	55	89	1869	3740	4181	F_{19}

Poznámka 2.6. V další části budou bez důkazů, případně s krátkým ověřením, uvedeny vybrané zajímavé **vlastnosti** pythagorejských trojúhelníků. Podrobnější výčet včetně důkazů je v [1].

1. Jestliže je O obvod primitivního pythagorejského trojúhelníku (a,b,c), pak O je sudé a $O|a \cdot b$. Tedz $O|2S$, kde S je obsah uvažovaného pythagorejského trojúhelníku. Fermat navíc dokázal, že S nemůže být druhou mocninou celého čísla.

2. V primitivní pythagorejské trojici (a,b,c) je jedna ze stran a, b dělitelná číslem 3.

3. V primitivní pythagorejské trojici (a,b,c) je jedna ze stran a, b dělitelná číslem 4.

4. V primitivní pythagorejské trojici (a,b,c) je jedna ze stran dělitelná pěti. Z těchto tří bodů plyne, že součin ab je dělitelný 12 a součin abc je dělitelný 60.

5. Pro $m = 149$ a $n = 58$ dostaneme pythagorejský trojúhelník (17284,18837,25565). Jeho obsah je 162789354, tedy číslo, kde jsme užili všechny číslice $1, \ldots, 9$. Existují i pythagorejské trojúhelníky, jejichž obsah obsahuje všech 10 číslic.

6. Druhá mocnina libovolného komplexního čísla $u + vi$ dává odvěsny primitivního pythagorejského trojúhelníku. Například $(4 + 3i)^2 = 7 + 24i$, odkud $a = 7$ a $b = 24$. Takto jsme dostali trojici (7,24,25).

2.4 Pellova rovnice

Řešením Pellovy rovnice se zabývá [12], což je společně s [8] a [2] zdroj pro následující část.

Definice 2.7. *Diofantická rovnice druhého stupně tvaru*

$$x^2 - Ny^2 = 1, \quad \text{resp. } x^2 - Ny^2 = -1$$

kde $N \in \mathbb{Z}$, $\sqrt{N} \in \mathbb{I}$, *se nazývá* ***Pellova rovnice****.*

Nejprve se budeme zabývat rovnicí

$$x^2 - Ny^2 = 1 \tag{2.30}$$

. Pro libovolné $N \in \mathbb{Z}^+$ má rovnice vždy řešení $x = 1$, $y = 0$ nebo $x = -1$, $y = 0$. Tato řešení se nazývají triviální řešení.

Hledáme tedy dvojici (x,y), pro kterou platí $x \neq 0$, $y \neq 0$. Pokud jsou čísla x,y přirozená, další řešení rovnice (2.30) jsou pak dvojice $(x,-y)$, $(-x,y)$ a $(-x,-y)$. Abychom našli všechna řešení rovnice (2.30), stačí najít její řešení v přirozených číslech. Omezíme se proto dále na ta řešení (x,y), kde $x,y \in \mathbb{N}$.

Nejprve vyšetříme případ, kdy N je druhou mocninou nějakého celého čísla, tj. $N = a^2$, $a \in \mathbb{Z}^+$. Dosazením do (2.30) dostaneme

$$x^2 - (ay)^2 = \pm 1 \quad \text{tj. } (x + ay)(x - ay) = \pm 1.$$

Pak $(x + ay) \mid 1$, což však není možné, protože předpokládáme, že $x,y,a \in \mathbb{Z}^+$.

Zdroj následující věty je **??**. Ve stejné knize lze najít i její důkaz.

Věta 2.10. *Pro libovolné* $N \in \mathbb{Z}^+$, $\sqrt{N} \in \mathbb{I}$, *má rovnice*

$$x^2 - Ny^2 = 1$$

netriviální řešení (x_0,y_0), $x_0 > 0$, $y_0 > 0$.

Definice 2.8. *Řešení* (x_0,y_0) *rovnice* (2.30) *nazveme* ***nejmenším****, jestliže pro libovolné jiné její řešení* (x',y') *platí* $x' > x_0$, $y' > y_0$.

Věta 2.11. *[12] Rovnice* (2.30) *má nekonečně mnoho řešení. Nechť je* (x_0,y_0) *nejmenší řešení rovnice* (2.30)*. Pak všechna řešení* (x,y) *v přirozených číslech dostaneme ze vzorce*

$$x + y\sqrt{N} = (x_0 + y_0\sqrt{N})^n \tag{2.31}$$

pro $n = 1,2,3,\ldots$.

Poznámka 2.7. [8] Pro nalezení jednoho kladného celočíselného řešení rovnice $x^2 - Ny^2 = 1$ můžeme aplikovat jednoduchý postup.
Ve výrazu $1 + Ny^2$ dosazujeme postupně přirozená čísla $1,2,3,\ldots$ a jako y_0 označíme první y takové, že $1 + Dy_0^2$ je čtvercem přirozeného čísla. Pak položíme $x_0^2 = 1 + Ny_0^2$. Dvojice (x_0,y_0) je tedy nejmenším kladným celočíselným řešením dané rovnice.

Příklad 2.5. *Řešte rovnici* $x^2 - 34y^2 = 1$.

Řešení. K řešení rovnice využijeme Poznámku 2.7. Postup dosazování lze znázornit v následující tabulce.

y	$1+34y_0^2$	x_0^2
1	35	NE
2	137	NE
3	307	NE
4	545	NE
5	851	NE
6	1225	ANO

Nejmenší řešení dané rovnice je $y_0 = 6$, $x_0 = 35$. Všechna řešení můžeme dopočítat podle Věty 2.11.

Jiný způsob, jak nalézt všechna řešení Pellovy rovnice, nabízí následující Věta.

Věta 2.12. *[12] Všechna řešení rovnice (2.30) dostaneme ze vzorců*

$$\begin{aligned} x_{k+1} &= x_0x_k + Ny_0y_k, \\ y_{k+1} &= y_0x_k + x_0y_k, \quad k \in \mathbb{N}_{\not\vdash}, \end{aligned}$$

kde (x_0,y_0) *je nejmenší řešení.*

Důkaz této věty lze najít v [12] str. 149.

Hledejme tedy nyní řešení (x,y) rovnice (2.30). Číslo $\sqrt{N}$ rozvineme v nekonečný řetězový zlomek

$$\sqrt{N} = [a_1; \overline{a_2,a_3\ldots,a_{n+1}}]$$

a nechť je $\dfrac{P_k}{Q_k}$ jeho $k-$tý sblížený zlomek. Řetězový zlomek pro číslo $\sqrt{N}$ má tvar

$$\sqrt{N} = [a_1; \overline{a_2,\ldots,a_n,2a_1}] = [a_1; \overline{a_2,a_3,\ldots,a_3,a_2,2a_1}] = [a_1; a_2,a_3,\ldots,a_n,r_{n+1}],$$

a pro zbytek r_{n+1} platí

$$r_{n+1} = [\overline{2a_1; a_2,a_3,\ldots,a_n}] = a_1 + \sqrt{N}.$$

Ze vztahu (1.8) plyne, že

$$\sqrt{N} = \frac{r_{n+1}P_n + P_{n-1}}{r_{n+1}Q_n + Q_{n-1}} = \frac{(a_1+\sqrt{N})P_n + P_{n-1}}{(a_1+\sqrt{N})Q_n + Q_{n-1}}.$$

Protože je však řetězový zlomek pro číslo $\sqrt{N}$ periodický s $n-$místnou periodou, je také

$$r_n = r_{kn+1}, \quad k = 1,2,3,\ldots.$$

Tedy je

$$\sqrt{N} = \frac{(a_1+\sqrt{N})P_{kn} + P_{kn-1}}{a_1+\sqrt{N}Q_{kn} + Q_{kn-1}}.$$

Z tohoto vztahu dostáváme

$$\sqrt{N}(a_1Q_{kn} + Q_{kn-1}) + NQ_{kn} = \sqrt{N}P_{kn} + (a_1P_{kn} + P_{kn-1}).$$

Protože je $\sqrt{N}$ iracionální číslo, z předchozí rovnosti plyne

$$P_{kn} = a_1 Q_{kn} + Q_{kn-1}$$
$$NQ_{kn} = a_1 P_{kn} + P_{kn-1}.$$

Vynásobíme-li první z těchto rovností číslem P_{kn} a druhou číslem $-Q_{kn}$,dále je sečteme, dostaneme

$$P_{kn}^2 - NQ_{kn}^2 = a_1 Q_{kn} P_{kn} + Q_{kn-1} P_{kn} - a_1 P_{kn} Q_{kn} - P_{kn-1} Q_{kn} =$$
$$= P_{kn} \cdot Q_{kn-1} - Q_{kn} P_{kn-1} = (-1)^{kn}.$$

Je-li n liché, pak z poslední rovnosti plyne

$$P_{kn}^2 - NQ_{kn}^2 = -1, \quad \text{pro } k = 1,3,5,\ldots$$
$$P_{kn}^2 - NQ_{kn}^2 = 1, \quad \text{pro } k = 2,4,6,\ldots.$$

Je-li n sudé, pak

$$P_{kn}^2 - NQ_{kn}^2 = 1, \quad \text{pro libovolné } k = 1,2,3,\ldots.$$

Některé sblížené zlomky nekonečného řetězového zlomku pro číslo $\sqrt{N}$ jsou tedy řešením rovnice $x^2 - Ny^2 = 1$ v kladných celých číslech. Platí i obrácené tvrzení.

Věta 2.13. *Je-li (x,y) libovolné řešení rovnice $x^2 - Ny^2 = 1$ v kladných celých číslech, $\sqrt{N} \in \mathbb{I}$, pak x je čitatel a y jmenovatel jednoho ze sblížených zlomků nekonečného řetězového zlomku pro číslo $\sqrt{N}$.*

Věta 2.14. *Obsahuje-li perioda řetězového zlomku pro číslo $\sqrt{N}$ sudý počet n prvků, potom čitatel a jmenovatel $kn-$tého sblíženého zlomku, $k = 1,2,3,\ldots$, tvoří řešení rovnice $x^2 - Ny^2 = 1$ v kladných celých číslech a všechna kladná celočíselná řešení dané rovnice lze získat právě tímto způsobem.*

Poznámka 2.8. Nejmenší kladné celočíselné řešení je dáno $n-$tým sblíženým zlomkem (pro $k = 1$), tj. $(x_0,y_0) = (P_n,Q_n)$.
Dalšími řešeními jsou dvojice (P_{2n},Q_{2n}), (P_{3n},Q_{3n}), ...

Věta 2.15. *Obsahuje-li perioda řetězového zlomku pro číslo $\sqrt{N}$ lichý počet n prvků, potom čitatel a jmenovatel $2kn-$tého sblíženého zlomku, $k = 1,2,3,\ldots$ tvoří řešení rovnice $x^2 - Ny^2 = 1$ v kladných celých číslech a všechna kladná celočíselná řešení davné rovnice lze získat právě tímto způsobem.*

Narozdíl od Pellovy rovnice, která má řešení pro každé N, rovnice tvaru

$$x^2 - Ny^2 = -1 \tag{2.32}$$

nemusí být pro některá N vůbec řešitelná v oboru celých čísel. Příkladem takové rovnice může být

$$x^2 - 3y^2 = -1.$$

Věta 2.16. *[8] Má-li perioda řetězového zlomku pro číslo $\sqrt{N}$ n prvků a je-li n sudé, pak rovnice (2.32) nemá v přirozených číslech žádné řešení.*
Je-li n liché, pak čitatel a jmenovat každého $2kn$-tého sblíženého zlomku, $k = 1,2,3,\ldots$, tvoří řešení rovnice (2.32) v přirozených číslech a všechna řešení dané rovnice lze získat právě tímto způsobem.

Poznámka 2.9. Nejmenší přirozené řešení v případě lichého n je dáno $2n-$tým sblíženým zlomkem (pro $k = 1$), tj. $(x_0,y_0) = (P_{2n},Q_{2n})$.
Dalšími řešeními jsou dvojice (P_{4n},Q_{4n}), (P_{6n},Q_{6n}), ...

Kapitola 3

Sbírka řešených úloh

Ve sbírce řešených úloh budou demonstrovány některé zmíněné metody řešení problémů z teoretické části. Pokud nebude řečeno jinak, příklady jsou převzaté z citovaných zdrojů a řešení je autorské.

Příklad 3.1. *Určete* (65880,36120).

Řešení. K řešení použijeme Euklidův algoritmus.

$$\begin{aligned} 65880 &= 36120 \cdot 1 + 29760 \\ 36120 &= 29760 \cdot 1 + 6360 \\ 29760 &= 6360 \cdot 4 + 4320 \\ 6360 &= 4320 \cdot 1 + 2040 \\ 4320 &= 2040 \cdot 2 + 240 \\ 2040 &= 240 \cdot 8 + 120 \\ 240 &= 120 \cdot 2 + 0 \end{aligned}$$

Poslední nenulový zbytek je 120, proto (65880,36120) = 120.

Příklad 3.2. *[3] Řešte v* $\mathbb{Z}$ *rovnici* $237x + 416y = 985$.

Řešení. Nejprve Euklidovým algoritmem najdeme $d = (237,416)$.

$$\begin{aligned} 416 &= 237 \cdot 1 + 179 \\ 237 &= 179 \cdot 1 + 58 \\ 179 &= 58 \cdot 3 + 5 \\ 58 &= 5 \cdot 11 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Protože je $d = (237,416) = 1$ a $1|985$, je rovnice řešitelná. Hledejme proto čísla x_0 a y_0 taková, že

$$237x_0 + 416y_0 = 1.$$

Najdeme je "zpětným"chodem Euklidova algoritmu. Po úpravě dostaneme

$$\begin{aligned}1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 58 - 11 \cdot 5 - (179 - 3 \cdot 58) + 58 - 11 \cdot 5 = \\ &= 237 - 1 \cdot 179 - 11 \cdot [179 - 3 \cdot (237 - 1 \cdot 179)] - 179 + 3 \cdot (237 - 1 \cdot 179) + \\ &+ 237 - 1 \cdot 179 - -11[179 - 3 \cdot (237 - 1 \cdot 179)] = \\ &= 71 \cdot 237 - 94 \cdot 179 = 71 \cdot 237 - 94 \cdot (416 - 1 \cdot 237) = 165 \cdot 237 - 94 \cdot 416\end{aligned}$$

Takto jsme našli čísla $x_0 = 165$ a $y_0 = -94$.
Čísla $x_1 = 985 \cdot x_0$ a $y_1 = 985 \cdot y_0$ jsou jedním řešením dané rovnice. Máme-li tedy $x_1 = 162525$ a $y_1 = -92590$, podle věty 2.2 všechna další řešení můžeme vyjádřit ve tvaru

$$\begin{aligned}x &= x_1 + bk = 162525 + 416k = 285 + 390 \cdot 416 + 416k = \\ &= 285 + 416(390 + k) = 285 + 416k' \\ y &= y_1 - ak = -92590 - 237k = -160 - 390 \cdot 237 - 237k = \\ &= -160 - 237(390 + k) = -160 - 239k'.\end{aligned}$$

Příklad 3.3. *Řešte v $\mathbb{Z}$ rovnici $93x - 71y = 25$.*

Řešení. Nejprve položíme $y' = -y$ a dostaneme rovnici

$$93x + 71y' = 25.$$

Euklidovým algoritmem najdeme $d = (93{,}71)$.

$$\begin{aligned}93 &= 71 \cdot 1 + 22 \\ 71 &= 22 \cdot 3 + 5 \\ 22 &= 5 \cdot 4 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0\end{aligned}$$

Protože $(93{,}71)|100$, je rovnice řešitelná. Hledejme nyní čísla x_0, y'_0 taková, že

$$93x_0 + 71y'_0 = 25.$$

Ta nalezneme zpětným chodem Euklidova algoritmu, proto

$$\begin{aligned}1 &= 5 - 2 \cdot 2 = 71 - 3 \cdot 22 - 2 \cdot (22 - 4 \cdot 5) = 71 - 3 \cdot 22 - 2 \cdot 22 + 8 \cdot 5 = \\ &= 71 - 5 \cdot (93 - 71) + 8 \cdot [71 - 3 \cdot (93 - 71)] = \\ &= 71 - 5 \cdot 93 + 5 \cdot 71 + 8 \cdot 71 - 24 \cdot 93 + 24 \cdot 71 = \\ &= -29 \cdot 93 + 38 \cdot 71\end{aligned}$$

tedy $x_0 = -29$, $y'_0 = 38$. Čísla $x_1 = 25 \cdot (-29) = -725$ a $y'_1 = 25 \cdot 38 = 950$ jsou jedním řešení rovnice $93x + 71y' = 25$. Všechna řešení rovnice lze podle věty 2.2 vyjádřit jako

$$\begin{aligned}x &= x_1 + bk = -725 + 71k = -15 - 10 \cdot 71 + 71k = -15 + 71k' \\ y' &= y'_1 - ak = 950 - 93k =',\end{aligned}$$

kde k je libovolné celé číslo. Po návratu do substituce $y' = -y$ máme

$$y = -950 + 93k = -20 + 93k'.$$

Příklad 3.4. *Řešte v* $\mathbb{Z}$ *rovnici* $38x - 106y = 58$.

Řešení. Budeme postupovat Eulerovou metodou. Nejprve ověříme, zda je rovnice řešitelná. Protože (38,106) = 2 a 2|58, je rovnice řešitelná. Z rovnice vyjádříme neznámou, jejíž koeficient je v absolutní hodnotě menší, v tomto případě vyjadřujeme x a dostaneme

$$x = \frac{58 + 106y}{38} = 1 + 2y + \frac{20 + 30y}{38},$$

tedy $x = 1 + 2y + t$, kde $t = \dfrac{20 + 30y}{38}$. Protože jak x, tak y, jsou čísla celá, musí i t být celým číslem. Potom

$$38t = 20 + 30y.$$

Z této rovnice znovu vyjádříme neznámou, jejíž koeficient je v absolutní hodnotě menší, tedy y, a dostaneme

$$y = \frac{-20 + 38t}{30} = t + \frac{20 + 8t}{30},$$

což lze napsat jako $y = t + s$, kde $s = \dfrac{20 + 8t}{30}$. Číslo s musí být celé, proto

$$30s = -20 + 8t,$$

odkud vyjádříme t a máme

$$t = \frac{20 + 30s}{8} = 2 + 3s + \frac{4 + 6s}{8}.$$

To můžeme psát ve tvaru $t = 2 + 3s + r$, kde $r = \dfrac{4 + 6s}{8}$. Analogicky r musí být celé číslo a platí

$$8r = 4 + 6s,$$

odkud

$$s = \frac{-4 + 8r}{6} = r + \frac{-4 + 2r}{6}.$$

Dále $s = r + u$, kde $u = \dfrac{-4 + 2r}{6}$ a

$$\begin{aligned} 6u &= -4 + 2r \\ r &= 3u + 2. \end{aligned}$$

Po postupném dosazení do vztahů

$$\begin{aligned} r &= 3u + 2 \\ s &= r + u \\ t &= 2 + 3s + r \\ y &= t + s \\ x &= 1 + 2y + t \end{aligned}$$

dostaneme

$$s = r + u = 3u + 2 + u = 4u + 2$$
$$t = 2 + 3s + r = 2 + 3(4u + 2) + (3u + 2) = 2 + 12u + 6 + 3u + 2 = 15u + 10$$
$$y = t + s = 15u + 10 + 4u + 2 = 19u + 12$$
$$x = 1 + 2y + t = 1 + 2(19u + 12) + 15u + 10 = 1 + 38u + 24 + 15u + 10 = 35 + 53u$$

kde $u \in \mathbb{Z}$. Máme tedy

$$x = 35 + 53u$$
$$y = 19u + 12.$$

Příklad 3.5. *[13] Kolika způsoby lze beze zbytku rozřezat dřevenou desku dlouhou 5 metrů na kusy 40 cm a 60 cm?*

Řešení. Úloha vede k diofantické rovnici

$$60x + 40y = 500.$$

Nejprve ověříme, zda je rovnice řešitelná. Protože (60,40) = 20 a 20|500, úloha má řešení. To opět najdeme pomocí Eulerovy metody. Stejně jako v předchozím příkladě, z rovnice vyjádříme neznámou, jejíž koeficient je v absolutní hodnotě nejmenší, upravíme, a analogicky budeme postupovat dále. Tedy

$$y = \frac{500 - 60x}{40} = 12 - x + \frac{20 - 20x}{40}.$$

Máme $y = 12 - x + 7$, kde $t = \dfrac{20 - 20x}{40}$ a $t \in \mathbb{Z}$. Proto

$$40t = 20 - 20x,$$

odkud

$$x = \frac{20 - 40t}{20} = 1 - 2t.$$

Celkem máme

$$x = 1 - 2t$$
$$y = 12 - x + t = 12 - (1 - 2t) + t = 11 + 3t.$$

Tím ale řešení nekončí. Musíme zaručit, že $x \geq 0$ a $y \geq 0$. Dostaneme

$$1 - 2t \geq 0$$
$$11 + 3t \geq 0.$$

Odtud musí platit, že $t \leq \dfrac{1}{2} \wedge t \geq -\dfrac{11}{3}$. Jediné přípustné hodnoty t jsou společně s konečným řešením úlohy znázorněny v následující tabulce.

t	-3	-2	-1	0
x	7	5	3	1
y	2	5	8	11

Příklad 3.6. *Řešte v* $\mathbb{Z}$ *rovnici* $47x - 25y = 279$. *[12]*

Řešení. Nejprve zavedeme substituci $y' = -y$ a dostaneme rovnici ve tvaru

$$47x + 25y' = 279.$$

Protože (47,25) = 1 a 1|279, je rovnice řešitelná. Rovnici budeme řešit metodou řetězových zlomků. Rozvineme racionální číslo $\frac{b}{a} = \frac{25}{47}$ v řetězový zlomek:

$$\begin{aligned} 25 &= 47 \cdot 0 + 25 \\ 47 &= 25 \cdot 1 + 22 \\ 25 &= 22 \cdot 1 + 3 \\ 22 &= 3 \cdot 7 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

Je tedy $\frac{25}{47} = [0;1,1,7,3]$, $n = 5$. Dále musíme najít sblížené zlomky $P_{n-1} = P_4$, $Q_{n-1} = Q_4$, k tomu následující schema.

i	1	2	3	4	5
q_i	0	1	1	7	3
P_i	0	1	1	8	25
Q_i	1	1	2	15	47

Odtud $P_4 = 8$ a $Q_4 = 15$. Po dosazení do vztahů (2.13) dostaneme

$$\begin{aligned} x_1 &= (-1)^{n-1} \cdot P_{n-1}c = (-1)^4 \cdot 8 \cdot 279 = 2232 \\ y_1' &= (-1)^n Q_{n-1}c = (-1)^5 \cdot 15 \cdot 279 = -4185. \end{aligned}$$

Všechna řešení dané rovnice vyjádříme ve tvaru

$$\begin{aligned} x &= x_1 + bk = 2232 + 25k \\ y' &= y_1' - ak = -4185 - 47k, \end{aligned}$$

kdy vrácením se do substituce $y' = -y$ dostaneme

$$y = 4185 + 47k.$$

Příklad 3.7. *[5] Řešte v oboru celých čísel rovnici*

$$105x + 119y + 161z = 83.$$

Řešení. V prvním kroce určíme d = (105,119,161) Máme

$$\begin{aligned} 105 &= 119 \cdot 0 + 105 \\ 119 &= 105 \cdot 1 + 14 \\ 105 &= 14 \cdot 7 + 7 \\ 14 &= 7 \cdot 2 + 0 \end{aligned}$$

a

$$161 = 7 \cdot 23 + 0.$$

Z toho vyplývá, že (105,119) = 7, (7,161) = 7, celkem tedy (105,119,161) = 7. Protože číslo 83 není dělitelné sedmi, rovnice není řešitelná.

Příklad 3.8. *[5] Řešte v oboru celých čísel rovnici*

$$63x + 70y + 75z = 91. \tag{3.1}$$

Řešení. Znovu určíme $d = (63{,}70{,}75)$ a dostaneme

$$\begin{aligned} 70 &= 63 \cdot 1 + 7 \\ 63 &= 7 \cdot 9 + 0 \end{aligned}$$

a

$$\begin{aligned} 75 &= 7 \cdot 10 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Vidíme, že $(63{,}70) = 7$ a $(7{,}75) = 1$. Celkem $d = 1$ a protože $1|91$, je rovnice řešitelná. Zpětným chodem Euklidova algoritmu vyjádříme

$$d = a_1x_0 + a_2y_0 + a_3z_0.$$

Máme

$$\begin{aligned} 7 &= 70 - 1 \cdot 63 \\ 5 &= 75 - 10 \cdot 7 \\ 2 &= 7 - 1 \cdot 5 \\ 1 &= 5 - 2 \cdot 2, \end{aligned}$$

proto

$$\begin{aligned} 1 &= 5 - 2 \cdot (7 - 1 \cdot 5) = 5 - 2 \cdot [7 - 1 \cdot (75 - 10 \cdot 7)] = \\ &= 5 - 2 \cdot 7 + 2 \cdot (75 - 10 \cdot 7) = 5 - 2 \cdot 7 + 2 \cdot 75 - 20 \cdot 7 = \\ &= 75 - 10 \cdot (70 - 1 \cdot 63) - 2 \cdot (70 - 1 \cdot 63) + 2 \cdot 75 - 20 \cdot (70 - 1 \cdot 63) = \\ &= 75 - 10 \cdot 70 + 10 \cdot 63 - 2 \cdot 70 + 2 \cdot 63 + 2 \cdot 75 - 20 \cdot 70 + 20 \cdot 63 = \\ &= 32 \cdot 63 - 32 \cdot 70 + 3 \cdot 75 \end{aligned}$$

Odtud

$$\begin{aligned} x_0 &= 32 \\ y_0 &= -32 \\ z_0 &= 3 \quad . \end{aligned}$$

Abychom získali jedno řešení rovnice (3.1), násobíme čísla x_0, y_0 a z_0 číslem 91:

$$\begin{aligned} x_1 &= 32 \cdot 91 = 2912 \\ y_1 &= -32 \cdot 91 = -2912 \\ z_1 &= 3 \cdot 91 = 273 \end{aligned}$$

Všechna řešení lze podle věty 2.5 napsat ve tvaru

$$\begin{aligned} x &= 2912 + 75s_1 \\ y &= -2912 + 75s_2 \\ z &= 273 - 63s_1 - 70s_2 \end{aligned}$$

Stejnou rovnici tentokrát řešíme Eulerovou metodou. Máme

$$63x + 70y + 75z = 91,$$

odkud

$$x = \frac{91 - 70y - 75z}{63} = 1 - y - z + a, \quad a = \frac{28 - 7y - 12z}{63}.$$

Potom

$$\begin{aligned} 63a &= 28 - 7y - 12z \\ y &= \frac{28 - 12z - 63a}{7} = 4 - z - 9a + b, \quad b = \frac{-5z}{7}. \end{aligned}$$

Pokračujeme a dostaneme

$$\begin{aligned} 7b &= -5z \\ z &= -\frac{7b}{5} = -b + c, \quad c = \frac{-2b}{5}. \end{aligned}$$

Dále

$$\begin{aligned} 5c &= -2b \\ b &= -\frac{5c}{2} = -2c + d, \quad d = \frac{-c}{2} \\ 2d &= -c \\ c &= -2d. \end{aligned}$$

Půjdeme-li zpět, postupně dostáváme

$$\begin{aligned} b &= 4d + d = 5d \\ z &= -5d - 2d = -7d \\ y &= 4 + 7d - 9a + 5d = 4 - 9a + 12d \\ x &= 1 - 4 + 9a - 12d + 7d + a = -3 + 10a - 5d. \end{aligned}$$

Příklad 3.9. *Nechť jsou p a q dvě prvočísla. V oboru přirozených čísel řešte rovnici*

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}.$$

Zadání i řešení z [2].

Řešení. Rovnici budeme řešit metodou faktorizace, proto nejprve upravíme a následně k obě stranám rovnice přičteme číslo p^2q^2. Máme pak

$$\begin{aligned} ypq + xpq &= xy \\ xy - xpq - ypq &= 0 \\ xy - xpq - ypq + p^2q^2 &= p^2q^2 \\ (x - pq)(y - pq) &= p^2q^2 \end{aligned}$$

Protože $\frac{1}{x} < \frac{1}{pq}$ je $x > pq$. Uvažujme dále všechny kladné dělitele čísla p^2q^2. Dostaneme následující soustavy rovnic:

$$\begin{aligned} x - pq &= 1 \\ y - pq &= p^2q^2 \end{aligned} \qquad \begin{aligned} x - pq &= p \\ y - pq &= pq^2 \end{aligned} \qquad \begin{aligned} x - pq &= q \\ y - pq &= p^2q \end{aligned}$$

$$\begin{aligned} x - pq &= p^2 \\ y - pq &= q^2 \end{aligned} \qquad \begin{aligned} x - pq &= pq \\ y - pq &= pq \end{aligned} \qquad \begin{aligned} x - pq &= pq^2 \\ y - pq &= p \end{aligned}$$

$$\begin{aligned} x - pq &= p^2q \\ y - pq &= q \end{aligned} \qquad \begin{aligned} x - pq &= q^2 \\ y - pq &= p^2 \end{aligned} \qquad \begin{aligned} x - pq &= p^2q^2 \\ y - pq &= 1 \end{aligned}$$

Z vypsaných soustav dostáváme řešení

$$(1+pq,pq(1+pq)) \quad (p(1+q),pq(1+q)) \quad (q(1+p),pq(1+p))$$

$$(p(p+q),q(p+q)) \quad (2pq,2pq) \quad (pq(1+q),p(1+q))$$

$$(pq(1+p),q(1+p)) \quad (q(p+q),p(p+q)) \quad (pq(1+pq),1+pq)$$

Příklad 3.10. *Klárka měla na papíru napsáno trojmístné číslo. Když ho správně vynásobila devíti, dostala čtyřmístné číslo, jež začínalo touž číslicí, jako číslo původní, prostřední dvě číslice se rovnaly a poslední číslice byla součtem číslic původního čísla. Které čtyřmístné číslo mohla Klárka dostat? Zadání i řešení [9] 57. ročník*

Řešení. Hledáme číslo $x = 100a + 10b + c$, jehož číslice jsou a, b a c. Číslice, která se nachází na obou místech uprostřed výsledného čísla označíme d. Ze zadání úlohy dostaneme

$$9(100a + 10b + c) = 1000a + 100d + 10d + (a + b + c).$$

Výraz $(a + b + c)$ je tedy číslice shodná s poslední číslicí součinu $9c$. To však znamená, že $c \not\geq 5$. Pro $c \geq 5$ končí číslo $9c$ číslicí nepřevyšující 5. Protože navíc platí $a \neq 0$, musí být $a + b + c > c \geq 5$. Rovnici dále upravíme na tvar

$$100(b - a - d) = 10d + a + 11b - 8c.$$

Počet všech možností lze totiž dále omezit odhadem $b \geq a$. Z tabulky níže vybereme správné řešení.

a	1	2	3	4	1	2	3	1	**2**	1
b	7	6	5	4	5	4	3	3	**2**	1
c	1	1	1	1	2	2	2	3	**3**	4
9x	1539	2349	3159	3969	1368	2178	2988	1197	**2007**	1026

Příklad 3.11. *Pomocí nerovností najděte všechna celočíselná řešení rovnice*

$$x^3 + (x+1)^3 + (x+2)^3 + \cdots + (x+7)^3 = y^3.$$

Zadání i řešení převzato z [2], maďarská matematická olympiáda.

Řešení. Označme nejprve

$$A(x) = x^3 + (x+1)^3 + (x+2)^3 + \cdots + (x+7)^3.$$

Po umocnění dostaneme $A(x) = 8x^3 + 84x^2 + 420x + 784$. Jestliže je $x \geq 0$, pak

$$(2x+7)^3 = 8x^3+84x^2+294x+343 < A(x) < 8x^3+120x^2+600x+1000 = (2x+10)^3,$$

potom $2x + 7 < y < 2x + 10$, tudíž y je $2x + 8$ nebo $2x + 9$. Ani jedna z rovnic

$$A(x) - (2x+8)^3 = -12x^2 + 36x + 272 = 0$$
$$A(x) - (2x+9)^3 = -24x^2 - 66x + 55 = 0$$

ale nemá celočíselná řešení, proto pro $x \geq 0$ neexistuje žádné řešení.
Všimněme si, že pro $A(x)$ platí $A(-x-7) = -A(x)$. Potom dvojice (x,y) je řešení právě tehdy když je řešení dvojice $(-x-7, -y)$. Proto neexistují žádná řešení, pro která platí $x \leq -7$. Aby tedy dvojice (x,y) byla řešením, musí platit

$$-6 \leq x \leq -1.$$

Pro $-3 \leq x \leq -1$ máme $A(-1) = 440$ (což není třetí mocnina žádného celého čísla), $A(-2) = 216 = 6^3$ a $A(-3) = 64 = 4^3$, proto dvojice $(-2,6)$ a $(-3,4)$ jsou jediná řešení pro $-3 \leq x \leq -1$. Dvojice $(-4, -4)$ a $(-5, -6)$ jsou jediná řešení pro $-6 \leq x \leq -4$. Všechna řešení zapíšeme do následující tabulky.

x	-2	-3	-4	-5
y	6	4	-4	-6

Příklad 3.12. *[13] V oboru celých čísel řešte rovnici*

$$x^2 - 4 = 11y.$$

Řešení. Podle věty 2.6 do levé strany rovnice budeme postupně dosazovat čísla $0,1,\ldots,10$ a po dosazení pokaždé ověříme, zda je výsledné číslo dělitelné 11. Celý postup je znázorněn v následující tabulce.

x	x^2-4	dělitelné 11
0	-4	NE
1	-3	NE
2	0	ANO
3	5	NE
4	12	NE
5	21	NE
6	32	NE
7	45	NE
8	60	NE
9	77	ANO
10	96	NE

Máme tedy dvě řešení $x_0 = 2$ a $x_1 = 9$. Všechna řešení lze vyjádřit jako

$$x = 11t + 2$$
$$x = 11t + 9,$$

kde $t \in \mathbb{Z}$. Ze zadání musíme dosazením dopočítat i y. Pro $x = 11t + 2$ máme

$$y = \frac{(11t+2)^2 - 4}{11} = \frac{121t^2 + 44t + 4 - 4}{11} = 11t^2 + 4t$$

a pro $x = 11t + 9$

$$y = \frac{(11t+9)^2 - 4}{11} = \frac{121t^2 + 198t + 81 - 4}{11} = 11t^2 + 18t + 7.$$

Řešením je proto každá dvojice tvaru $(11t+2, 11t^2+4t)$ a $(11t+9, 11t^2+18t+7)$, $t \in \mathbb{Z}$.

Příklad 3.13. *[13] Najděte všechna celočíselná řešení rovnice*

$$x^3 + 2x^2 + 5 = 21y.$$

Řešení. Postupovat budeme analogicky, jako v předchozím příkladě podle věty 2.6. Postupně do levé strany rovnice dosadíme čísla 0,1, . . . ,20 a po dosazení každý výsledek ověříme, zda je dělitelný číslem 21. To jest znázorněno v následující tabulce.

x	$x^3 + 2x^2 + 5$	dělitelné 21
0	5	NE
1	8	NE
2	21	ANO
3	50	NE
4	101	NE
5	180	NE
6	293	NE
7	446	NE
8	645	NE
9	896	NE
10	1205	NE
11	1578	NE
12	2021	NE
13	2540	NE
14	3141	NE
15	3830	NE
16	4613	NE
17	5496	NE
18	6485	NE
19	7586	NE
20	8805	NE

Takto jsme našli, že $x_0 = 2$. Obecné řešení lze vyjádřit jako

$$x = 21t + 2, \quad , t \in \mathbb{Z}.$$

Pro $x = 21t + 2$ dopočítáme

$$y = \frac{(21t+2)^3 + 2(21t+2)^2 + 5}{21} = \frac{9261t^3 + 3528t^2 + 420t + 21}{21} =$$
$$= \frac{21(441t^3 + 168t^2 + 20t + 1)}{21} = 441t^3 + 168t^2 + 20t + 1$$

Definice 3.1. ***Mřížovým bodem*** *nazveme bod v rovině, jehož obě souřadnice jsou celočíselné.*

Příklad 3.14. *Určete všechny mřížové body, kterými prochází parabola daná rovnicí*

$$x^2 - 8x - 14y + 5 = 0.$$

Řešení. V podstatě řešíme diofantickou rovnici

$$x^2 - 8x + 5 = 14y.$$

Způsob řešení volíme stejný, jako v předchozí úloze podle věty 2.6. Dostaneme tabulku

x	$x^2 - 8x + 5$	dělitelné 14
0	5	NE
1	-2	NE
2	-7	NE
3	-10	NE
4	-11	NE
5	-10	NE
6	-7	NE
7	-2	NE
8	5	NE
9	14	ANO
10	25	NE
11	38	NE
12	53	NE
13	70	ANO

Našli jsme $x_0 = 9$ a $x_1 = 13$. Z toho vyplývá, že $x = 14t + 9$ nebo $x = 14t + 13$. Pro $x = 14t + 9$ je

$$y = \frac{(14t+9)^2 - 8(14t+9) + 5}{14} = \frac{196t^2 + 140t + 14}{14} = \\ = \frac{14(14t^2 + 10t + 1)}{14} = 14t^2 + 10t + 1$$

a pro $x = 14t + 13$ je

$$y = \frac{(14t+13)^2 - 8(14t+13) + 5}{14} = \frac{196t^2 + 252t + 70}{14} = \\ = \frac{14(14t^2 + 18t + 5)}{14} = 14t^2 + 18t + 5.$$

Všechny mřížové body, který mi prochází parabola v zadání jsou $T_1[14t + 9{,}14t^2 + 10t + 1]$ a $T_2[14t + 13{,}14t^2 + 18t + 5]$, kde $t \in \mathbb{Z}$.

Příklad 3.15. *Pravoúhlý trojúhelník má celočíselné délky stran a obvod 11 990. Navíc víme, že jedna jeho odvěsna má prvočíselnou délku. Určete ji. Zadání i řešení z [9] 71. ročník.*

Řešení. V daném trojúhelníku označíme prvočíselnou délku jedné odvěsny jako p. Písmeny a, b dále označíme celočíselnou délku druhé odvěsny a přepony. Pro zadaný trojúhelník platí

$$p^2 + a^2 = b^2.$$

Tento vztah přepíšeme ve tvaru

$$p^2 = b^2 - a^2 = (b - a)(b + a).$$

Je zřejmé, že jak $(b-a)$, tak i $b+a$ jsou přirozená čísla. Číslo p^2 lze takto rozložit na součin pouze dvěma způsoby. Buď $p^2 = 1 \cdot p^2$ nebo $p^2 = p \cdot p$. Navíc

$$(b - a) < (b + a),$$

odkud vidíme, že musí platit

$$\begin{aligned} b - a &= 1 \\ b + a &= p^2. \end{aligned}$$

Ze zadání obvodu je zřejmé, že

$$p + a + b = 11990,$$

po dosazení hodnotou p^2 za $a + b$ máme

$$p + p^2 = 11990.$$

Kvadratickou rovnici řešíme a dostaneme

$$p_{1/2} = \frac{-1 \pm \sqrt{47960}}{2} = \frac{-1 \pm 219}{2},$$

odkud $p_1 = 109$ a $p_2 = -110$. Z těchto dvou kořenů připadá v úvahu pouze p_1, proto hledaná prvočíselná délka odvěsny zadaného trojúhelníku je $p = 109$.

Příklad 3.16. *Najděte všechny dvojice (a,b) celých čísel, jež vyhovují rovnici*

$$a^2 + 7ab + 6b^2 + 5a + 4b + 3 = 0.$$

Úloha i řešení z [9] - 56. ročník

Řešení. Výraz

$$a^2 + 7ab + 6b^2 + 5a + 4b + c,$$

kde c je vhodně zvolená konstanta, rozložíme na součin. Dostaneme

$$a^2 + 7ab + 6b^2 + 5a + 4b + c = (a + b + x)(a + 6b + y).$$

Na pravé straně roznásobíme

$$a^2 + 7ab + 6b^2 + 5a + 4b + c = a^2 + 7ab + 6b^2 + a(x + y) + b(6x + y) + xy,$$

odkud porovnáním koeficientů u členů a a b vyplývá

$$\begin{aligned} x + y &= 5 \\ 6x + y &= 4. \end{aligned}$$

Z toho vyplývá, že $x = -\frac{1}{5}$, $y = \frac{26}{5}$, proto

$$c = xy = -\frac{26}{25}.$$

Zadanou rovnici proto dále postupně upravíme na tvar

$$\begin{aligned} a^2 + 7ab + 6b^2 + 5a + 4b - \frac{26}{25} &= -3 - \frac{26}{25} \\ \left(a + b - \frac{1}{5}\right)\left(a + 6b + \frac{26}{5}\right) &= -\frac{101}{25} \\ (5a + 5b - 1)(5a + 30b + 26) &= -101. \end{aligned}$$

Pak ale musí být

$$\begin{aligned} 5a + 5b - 1 &= -1 \\ 5a + 30b + 26 &= 101 \end{aligned} \qquad \begin{aligned} 5a + 5b - 1 &= -101 \\ 5a + 30b + 26 &= 1 \end{aligned}$$

nebo

$$\begin{aligned} 5a + 5b - 1 &= 1 \\ 5a + 30b + 26 &= -101 \end{aligned} \qquad \begin{aligned} 5a + 5b - 1 &= 101 \\ 5a + 30b + 26 &= -1 \end{aligned}$$

Z první dvojice soustav dostáváme dvojice $(a,b) = (-3,3)$ a $(a,b) = (-23,3)$, kdy každá z nich vyhovuje zadání. Z druhé dvojice soustav však nedostáváme ani v jednom případě celočíselná řešení. Hledané dvojice jsou tedy $(-3,3)$ a $(-23,3)$.

Příklad 3.17. *Určete počet všech trojic přirozených čísel a, b, c, pro která platí*

$$a + ab + abc + ac + c = 2017.$$

Zadání i řešení [9] 67. ročník.

Řešení. Nejprve upravíme levou stranu rovnice

$$\begin{aligned} a + ab + abc + ac + c = a(1 + b) + ac(1 + b) + c = a(1 + b)(1 + c + c) = \\ = a(1 + b)(1 + c) + (1 + c) - 1 = (1 + c)(a(1 + b) + 1) - 1, \end{aligned}$$

odkud díky tomu máme

$$(1 + c)(a(1 + b) + 1) = 2018.$$

Číslo 2018 lze napsat jako součin dvou přirozených čísel pouze dvěma způsoby:

$$\begin{aligned} 2018 &= 1 \cdot 2018 \\ 2018 &= 2 \cdot 1009. \end{aligned}$$

Protože je

$$\begin{aligned} 1 + c &\geq 2 \\ a(1 + b) + 1 &\geq 3, \end{aligned}$$

může platit pouze

$$1 + c = 2$$
$$a(1 + b) + 1 = 1009,$$

odkud $c = 1$ a $a(1 + b) = 1008$. V každé hledané trojici je tak $c = 1$. Z toho vyplývá, že hledáme počet dvojic (a,b), které splňují rovnici

$$a(1 + b) = 1008.$$

Určíme, že číslo 1008 má celkem 30 různých dělitelů, protože ale musí být $1+b \geq 2$, nemůže být $a = 1008$. Pro každého jiného z 29 dělitelů a čísla 1008 dostaneme jednu dvojici řešení (a,b). Hledaný počet trojic je tedy roven 29.

Příklad 3.18. *Rozviňte v řetězový zlomek číslo* $\sqrt{8}$.

Řešení. Podle věty 1.23 očekáváme periodický řetězovýn zlomek tvaru $[a_1; \overline{a_2; a_3; \ldots; a_3; a_2; 2a_1}]$. Tyto hodnoty získáme postupem popsaným ve stejné kapitole.

$$\alpha = \sqrt{8} = 2 + \frac{1}{\alpha_1} \qquad q_1 = 2$$
$$\alpha_1 = \frac{1}{\sqrt{8} - 2} = \frac{1 + \sqrt{2}}{2} = 1 + \frac{1}{\alpha_2} \qquad q_2 = 1$$
$$\alpha_2 = \frac{1}{\frac{1 + \sqrt{2}}{2} - 1} = 2 + 2\sqrt{2} = 4 + \frac{1}{\alpha_3} \qquad q_3 = 4$$
$$\alpha_3 = \frac{1}{2 + 2\sqrt{2} - 4} = \frac{1 + \sqrt{2}}{2} = \alpha_1 = \frac{1}{\alpha_4} \qquad q_4 = 1$$
$$\alpha_4 = \frac{1}{\frac{1 + \sqrt{2}}{2} - 1} = 2 + 2\sqrt{2} = \alpha_2 = 4 + \frac{1}{\alpha_5} \qquad q_5 = 4$$

Máme $\alpha_1 = \alpha_3$, $\alpha_2 = \alpha_4$, pak ale

$$\alpha_1 = \alpha_3 = \alpha_5 = \cdots = \frac{1 + \sqrt{2}}{2} y$$

tedy $q_2 = q_4 = \cdots = 1$. Dále

$$\alpha_2 = \alpha_4 = \alpha_6 = \cdots = 2 + 2\sqrt{2},$$

proto $q_3 = q_5 = \cdots = 4$. Dostáváme nekonečný periodický řetězový zlomek s jednoprvkovou předperiodou $q_1 = 2$ a dvouprvkovou periodou, tedy $n = 2$ a $\alpha = [2; \overline{1; 4}]$.

Příklad 3.19. *[12] Řešte rovnici*

$$x^2 - 29y^2 = 1.$$

Řešení. Nejprve musíme najít rozvoj čísla $\sqrt{29}$ v řetězový zlomek. Postupovat budeme stejně jako v předchozím příkladu, proto máme

$$\begin{aligned}
\alpha &= \sqrt{29} = 5 + \frac{1}{\alpha_1} && a_1 = 5\\
\alpha_1 &= \frac{1}{\sqrt{29} - 5} = \frac{5 + \sqrt{29}}{4} = 2 + \frac{1}{\alpha_2} && a_2 = 2\\
\alpha_2 &= \frac{1}{\frac{5 + \sqrt{29}}{4} - 2} = \frac{3 + \sqrt{29}}{5} = 1 + \frac{1}{\alpha_3} && a_3 = 1\\
\alpha_3 &= \frac{1}{\frac{3 + \sqrt{29}}{5} - 1} = \frac{2 + \sqrt{29}}{5} = 1 + \frac{1}{\alpha_4} && a_4 = 1\\
\alpha_4 &= \frac{1}{\frac{2 + \sqrt{29}}{5} - 1} = \frac{3 + \sqrt{29}}{4} = 2 + \frac{1}{\alpha_5} && a_5 = 2\\
\alpha_5 &= \frac{1}{\frac{3 + \sqrt{29}}{4} - 2} = 5 + \sqrt{29} = 10 + \frac{1}{\alpha_6} && a_6 = 10\\
\alpha_6 &= \frac{1}{5 + \sqrt{29} - 10} = \frac{5 + \sqrt{29}}{4} = \alpha_1,
\end{aligned}$$

odkud $\sqrt{29} = [5; \overline{2; 1; 1; 2; 10}]$. Délka periody $n = 5$, proto budeme hledat čísla $(x_0,y_0) = (P_{10}, Q_{10})$, k čemuž použijeme následující schema.

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

Je zřejmé, že dvojice $P_{10} = x = 9801$ a $Q_{10} = y = 1820$ je nejmenším dané rovnice. Všechna řešení lze najít podle vztahů z Věty 2.12.

Příklad 3.20. *Řešte rovnici*

$$x^2 - 31y^2 = 1.$$

Řešení. Nejprve musíme najít rozvoj čísla $\sqrt{31}$ v řetězový zlomek. Máme

$$\begin{aligned}
\alpha &= \sqrt{31} = 5 + \frac{1}{\alpha_1} && a_1 = 5\\
\alpha_1 &= \frac{1}{\sqrt{31}-5} = \frac{5+\sqrt{31}}{6} = 1 + \frac{1}{\alpha_2} && a_2 = 1\\
\alpha_2 &= \frac{1}{\frac{5+\sqrt{31}}{6} - 1} = \frac{1+\sqrt{31}}{5} = 1 + \frac{1}{\alpha_3} && a_3 = 1\\
\alpha_3 &= \frac{1}{\frac{1+\sqrt{31}}{5} - 1} = \frac{4+\sqrt{31}}{3} = 3 + \frac{1}{\alpha_4} && a_4 = 3\\
\alpha_4 &= \frac{1}{\frac{4+\sqrt{31}}{3} - 3} = \frac{5+\sqrt{31}}{2} = 5 + \frac{1}{\alpha_5} && a_5 = 5\\
\alpha_5 &= \frac{1}{\frac{5+\sqrt{31}}{2} - 5} = \frac{5+\sqrt{31}}{3} = 3 + \frac{1}{\alpha_6} && a_6 = 3\\
\alpha_6 &= \frac{1}{\frac{5+\sqrt{31}}{3} - 3} = \frac{4+\sqrt{31}}{5} = 1 + \frac{1}{\alpha_7} && a_7 = 1\\
\alpha_7 &= \frac{1}{\frac{4+\sqrt{31}}{5} - 1} = \frac{1+\sqrt{31}}{6} = 1 + \frac{1}{\alpha_8} && a_8 = 1\\
\alpha_8 &= \frac{1}{\frac{1+\sqrt{31}}{6} - 1} = 5 + \sqrt{31} = 10 + \frac{1}{\alpha_9} && a_9 = 10\\
\alpha_9 &= \frac{1}{5+\sqrt{31}-10} = \frac{5+\sqrt{31}}{6} = \alpha_1
\end{aligned}$$

Máme tedy $\sqrt{31} = [5; \overline{1,1,3,5,3,1,1,10}]$, délka periody $n = 8$. Počet prvků v periodě je sudý, budeme proto hledat $(x,y) = (P_8,Q_8)$, k čemuž využijeme následující schema.

i	1	2	3	4	5	6	7	8
a_i	5	1	1	3	5	3	1	1
P_i	5	6	11	39	206	657	863	1520
Q_i	1	1	2	7	37	118	155	273

Ze schematu vidíme, že $x = P_8 = 1520$, $y = Q_8 = 273$. Takto jsme našli nejmenší řešení dané rovnice. Všechna další rovnice určíme pomocí Věty 2.12.

Příklad 3.21. *Popište všechny pravoúhlé trojúhelníky s celočíselnými délkami stran, jejichž obvod má stejnou hodnotu jako obsah. Zadání i řešení z [11].*

Řešení. Nechť jsou odvěsny a, b hledaného pravoúhlého trojúhelníku, nechť je c přepona toho trojúhelníku. Potom platí

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

Bez újmy na obecnosti můžeme předpokládat, že $a \leq b$. Aby měly obvod a obsah stejnou hodnotu, musí platit

$$\frac{1}{2}ab = a + b + c.$$

Po dosazení z prvního vztahu do druhého a následných úpravách dostáváme

$$\begin{aligned} a^2 + b^2 &= \left(\frac{1}{2}ab - a - b\right)^2 \\ a^2 + b^2 &= \frac{1}{4}a^2b^2 - a^2b - ab^2 + a^2 + 2ab + b^2 \\ 0 &= \frac{1}{4}a^2b^2 - a^2b - ab^2 + 2ab \\ 0 &= ab - 4a - 4b + 8 \\ 8 &= (a-4)(b-4) \end{aligned}$$

Rovnici

$$(a-4)(b-4) = 8$$

budeme řešit metodou faktorizace. Protože musí platit $a > 0$, $b > 0$ a zároveň předpokládáme, že $a \leq b$, připadají v úvahu následující možnosti:

$$\begin{aligned} a - 4 &= 1 & \qquad a - 4 &= 2 \\ b - 4 &= 8 & \qquad b - 4 &= 4 \end{aligned}$$

Řešením těchto soustav jsou dvojice (5,12) a (6,8). V prvním případě dostáváme pythagorejský trojúhelník (5,12,13) a ve druhém (6,8,10), což je odpověď.

Zdrojem následujících dvou příkladů a řešení je [2].

Příklad 3.22. *Dokažte, že neexistují žádná dvě kladná celá čísla taková, že součet a rozdíl jejich druhých mocnin jsou druhé mocniny celých čísel.*

Řešení. Budeme se tedy snažit dokázat, že soustava rovnice

$$x^2 + y^2 = z^2 \tag{3.2}$$
$$x^2 - y^2 = w^2 \tag{3.3}$$

nemá v kladných celých číslech řešení. To dokážeme sporem.
Předpokládejme, že daná soustava je řešitelná v oboru kladných celých čísel a nechť je dvojice (x,y) taková, že součet $x^2 + y^2$ je nejmenší možný. Pak největší společný dělitel $(x,y) = 1$.
Sečteme-li dané rovnice, dostaneme

$$2x^2 = z^2 + w^2 \tag{3.4}$$

odkud vyplývá, že čísla z a w mají stejnou paritu. Proto $z + w$ a $z - w$ jsou obě sudá.
Rovnici (3.4) napíšeme ve tvaru

$$x^2 = \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2.$$

Dále je největší společný dělitel $d = \left(x, \frac{z+w}{2}, \frac{z-w}{2}\right) = 1$.
Opravdu: pokud by bylo $d \geq 2$, pak $d \mid x$ a $d \mid \left(\frac{z+w}{2} + \frac{z-w}{2}\right) = z$. Z první rovnice soustavy (3.2) dostaneme, že $d \mid y$, což je spor s tím, že největší společný dělitel $(x,y) = 1$.
Použijeme-li dále větu 2.9, dostaneme buď

$$\frac{z-w}{2} = m^2 - m^2, \quad \frac{z+w}{2} = 2mn,$$

nebo

$$\frac{z-w}{2} = 2mn, \quad \frac{z+w}{2} = m^2 - n^2.$$

Protože $2y^2 = z^2 - w^2$, v obou případech máme

$$2y^2 = 2(m^2 - m^2)4mn,$$

tedy

$$y^2 = 4mn(m^2 - n^2).$$

Z toho vyplývá, že $y = 2k$ pro nějaké kladné celé číslo k, a že

$$k^2 = mn(m+n)(m-n). \tag{3.5}$$

Protože jsou čísla m a n nesoudělná a $m+n$ je sudé, čísla m, n, $m+n$, $m-n$ jsou rovněž po dvou nesoudělná. Proto z rovnice (3.5) můžeme odvodit, že $m = a^2$, $n = b^2$, $m + n = c^2$ a $m - n = d^2$ pro nějaká kladná celá čísla a,b,c,d. Ale $a^2 + b^2 = c^2$ a $a^2 - b^2 = d^2$, tedy čtveřice (a,b,c,d) je také řešením soustavy (3.2). Navíc

$$a^2 + b^2 = m + n < 4mn(m^2 - n^2) = y^2 < x^2 + y^2,$$

což je spor s předpokladem.

Příklad 3.23. *Dokažte, že neexistuje žádná pythagorejská trojice, jejíž obsah je čtverec.*

Řešení. Dokazovat budeme sporem. Předpokládejme, že takový trojúhelník existuje. Pak

$$a^2 + b^2 = c^2 \wedge ab = 2d^2,$$

kde d je kladné celé číslo. Bez újmy na obecnosti můžeme předpokládat, že $a > b$, protože se nemůže stát, že $a = b$, jelikož rovnost $2a^2 = c^2$ není možná. Proto

$$c^2 + (2d)^2 = (a+b)^2 \wedge c^2 - (2d)^2 = (a-b)^2,$$

což je spor s výsledkem předchozího příkladu 3.22.

Závěr

Diplomová práce obsahuje v první kapitole ty nejdůležitější pojmy a vlastnosti, které jsou potřeba pro teorii diofantických rovnic. Zmíněny jsou základní definice a věty doplněné o poznámky často akcentující důsledky, případně podrobněji popisující postupy plynoucí z vět. Nejdůležitější věty jsou rovněž dokázány.

Druhá kapitola je věnována především naplněním jejího cíle, tedy názornému odvození a demonstrování metod řešení jednotlivých typů rovnic. Vybrány byly pouze některé typy rovnic. Diplomová práce se také podrobněji zabývala pythagorejskými trojúhelníky a jejich vlastnostmi.

Ve třetí kapitole, tedy praktické části práce, jsou řešeny některé příklady, včetně příkladů ze středoškolské matematické olympiády. Řešení většiny příkladů v diplomové práci jsou autorská. Kde tomu tak není, je náležitě citován zdroj.

Při tvorbě práce pro mě bylo nejnáročnější porovnávat jednotlivé zdroje a následně zvolit vhodný způsob psaní tak, aby práce byla jednotná a kompaktní. Tvorba diplomové práce pro mě však byla velmi přínosná, konkrétně v práci se zdroji. Shrnout potřebnou teorii v některých úsecích práce, zejména u řetězových zlomků a pojmů s nimi spojených, mi působilo potíže, avšak psaní a dohledávání informací u zajímavějších částí, jako jsou například Pythagorejské trojúhelníky, bylo velmi obohacující.

Literatura

[1] AGARWAL, Ravi P. *Pythagorean Triples before and after Pythagoras.* Computation 2020, 8, 62. https://doi.org/10.3390/computation80300622

[2] ANDREESCU, Titu, Dorin ANDRICA a Ion CUCUREZEANU. *An Introduction to Diophantine Equations: A Problem-Based Approach.* Ilustrované vydání. Springer Science Business Media, 2010. ISBN 0817645497.

[3] DAVYDOV, Jurij Samojlovič a Štefan ZNÁM. *Teória čísel: základné pojmy a zbierka úloh.* Bratislava: Slovenské pedagogické nakladateľstvo, 1972.

[4] HALAŠ, Radomír.: *Teorie čísel.* Olomouc, 1997

[5] HERMAN, Jiří, Radan KUČERA a Jaromír ŠIMŠA. *Metody řešení matematických úloh.* Vyd. 2. přeprac. Brno: Masarykova univerzita, 1996. ISBN 80-210-1202-1.

[6] HUA, Loo Keng *Introduction to Number Theory*. New York: Springer, 1982. ISBN 0-387-10818-1.

[7] CHINČIN, Aleksandr Jakovlevič. *Řetězové zlomky.* Praha: Přírodovědecké vydavatelství, Kruh (Přírodovědecké vydavatelství), 1952.

[8] KÜHNOVÁ, Jitka. *Vybrané partie z teorie čísel.* Hradec Králové: MAFY, 2000. ISBN 80-86148-39-4.

[9] *Matematická olympiáda* [online]. [cit. 2023-04-18]. Dostupné z: https://www.matematickaolympiada.cz/

[10] PAGNI, David. *Fibonacci Meets Pythagoras.* Mathematics in School. 2001, 30, 39-40. Dostupné z: doi:10.2307/30215477

[11] *Rozvíjení matematických talentů na středních školách.* Praha: Matfyzpress, nakladatelství Matematicko-fyzikální fakulty Univerzity Karlovy, 2019. ISBN 978-80-7378-452-2.

[12] VÍT, Pavel. *Řetězové zlomky.* Praha: Mladá fronta, Škola mladých matematiků, 1982.

[13] ZNÁM, Štefan. *Teória čísel.* 2. vyd. Bratislava: Alfa, 1986. Epsilon.