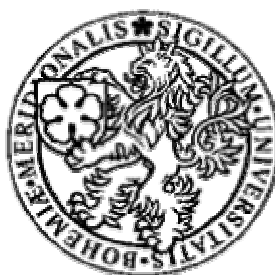


JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH

PEDAGOGICKÁ FAKULTA
KATEDRA MATEMATIKY



Diofantovské rovnice

Bakalářská práce

Autor: Lukáš Frčka

Vedoucí práce: RNDr. Pavel Leischner, Ph.D.

České Budějovice, 2007

Anotace

Název: Diofantovské rovnice

Autor: Lukáš Frčka

Vedoucí práce: RNDr. Pavel Leischner, Ph.D.

Klíčová slova: Diofantovské rovnice, metody řešení diofantovských rovnic, řešené příklady diofantovských rovnic

Hlavním obsahem práce jsou nelineární diofantovské rovnice. Tyto rovnice jsou rozděleny do kategorií: lineární, lineární vzhledem k některé neznámé a pět speciálních typů diofantovských rovnic. Práce se také zabývá elementárními metodami řešení některých typů diofantovských rovnic, které vedou ke správnému řešení. Zmíněna je i problematika řešitelnosti a počet řešení diofantovské rovnice.

Title: Diophantine equations

Autor: Lukáš Frčka

Supervisor: RNDr. Pavel Leischner, Ph.D.

Key words: Diophantine equations, methods of solving diophantine equations, solved diophantine equations

The main purpose of this thesis are nonlinear diophantine equations. These equations are split into categories: linear equations, linear equations in the view of one unknown and five special types of diophantine equation. This thesis is concerned with elementary methods of solving some types of diophantine equations which helps us to find right solution. We can find here answers about solvability and number of solution of diophantine equation.

Děkuji RNDr. Pavlu Leischnerovi, Ph.D. za odborné vedení a pomoc při vypracování bakalářské práce.

Prohlašuji, že jsem bakalářskou práci na téma „Diofantovské rovnice“ vypracoval samostatně a použil jen pramenů, které cituji a uvádím v přiložené bibliografii.

V Českých Budějovicích 24.4.2007

Lukáš Frčka

Obsah:

1 Úvod.....	5
1.1 Historie diofantovských rovnic.....	5
1.2 Diofantos z Alexandrie a jeho rovnice	7
2 Diofantovské rovnice	8
2.1 Klasifikace diofantovských rovnic	8
2.1.1 Lineární diofantovské rovnice	9
2.1.2 Diofantovské rovnice lineární vzhledem k některé neznámé	13
2.1.3 Speciální typy diofantovských rovnic.....	19
2.1.3.1 Diofantovská rovnice $xy = z^2 + 1$	19
2.1.3.2 Diofantovská rovnice tvaru $\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = \frac{1}{x_{n+1}}$	22
2.1.3.3 Pellova rovnice $x^2 - Dy^2 = N$	25
2.1.3.4 Pythagorova diofantovská rovnice $x^2 + y^2 = z^2$	42
2.1.3.5 Diofantovská rovnice tvaru $x^n + y^n = x^p y^q z$	44
2.2 Některé další metody řešení diofantovských rovnic.....	45
2.2.1 Řešení diofantovských rovnic s využitím odhadu nerovností	45
2.2.2 Řešení diofantovských rovnic metodou rozkladu.....	48
2.3 Řešitelnost diofantovských rovnic.....	49
2.3.1 Využití kongruence při důkazu neexistence řešení.....	49
2.3.2 Metoda nekonečného sestupu neboli zmenšování	51
2.3.3 Početnost množiny řešení	52
3 Závěr	54

1 Úvod

Diofantovská rovnice v matematice je neurčitá polynomická rovnice, která připouští za řešení pouze celá čísla. V diofantovských problémech vždy hledáme řešení několika rovnic s větším počtem proměnných než je dáno rovnic. Hledáme jen kořeny z oboru celých čísel. Slovo diofantovské se začíná používat od dob helénské matematiky (3.století n.l.). Diofantos z Alexandrie, který se těmito rovnicemi zabýval a který také jako jeden z matematiků zavedl symboliku do algebry, byl inspirací pro tento název. Matematické odvětví zabývající se diofantovskými problémy, které Diofantos odstartoval, se nazývá „Diofantovskou analýzou.“

Mezi tradiční otázky diofantovské analýzy patří:

- Jsou nějaká řešení?
- Lze nějaká řešení nalézt snadným řešením rovnice?
- Má rovnice konečně nebo nekonečně mnoho řešení?
- Lze teoreticky nalézt všechna řešení?
- Lze v praxi vypočítat všechna řešení této rovnice?

1.1 Historie diofantovských rovnic

Diofantovská analýza v Indii

Indický zájem na základních rozborech diofantovských rovnic můžeme nalézt v díle Sulva Sutras, indický matematický text napsaný mezi 800 př.n.l a 500 př.n.l. matematikem Baudhayanou. Ten popisuje ve svém díle jak našel dva soubory pozitivních základních řešení soustavy rovnic v současné době diofantovských. A také se pokoušel řešit diofantovské rovnice až se čtyřmi neznámými. Apastamba další indický matematik žijící kolem roku 600 př.n.l. se pokoušel řešit současné diofantovské rovnice i s pěti neznámými (viz [7]).

Diofantovské rovnice byly později značně studovány matematiky ve středověké Indii. Tito matematici byli první, kteří začali systematicky vyšetřovat metody na určení základních řešení diofantovských rovnic. Systematické metody, pomocí kterých lze najít celočíselná řešení diofantovských rovnic můžeme nalézt v textech Inda Aryabhata (499 CE). První explicitní vyjádření obecného druhu řešení základní lineární diofantovské rovnice se vyskytuje v jeho díle Aryabhatiya. Tento algoritmus je považován za jeden z významných přínosů Aryabhaty do čisté matematiky. Technika Aryabhaty byla aplikována na problémy v astronomii a dávala základní řešení modelové diofantovské rovnice prvního druhu. Aryabhata popisuje algoritmus pouze ve dvou slokách v díle Aryabhatiy. Jeho myšlenky byly zviditelněny Bhaskarou (6.století) v komentáři Aryabhativa Bhasya. Bhaskara objasnil Aryabhatovo pravidlo pomocí několika příkladů k nimž přidal 24 konkrétních úloh z astronomie. Bez vysvětlení Bhaskary by Aryabhatovy myšlenky šly nesnadno interpretovat. Bhaskara nazval metodu kuttaka (pulverisation – rozmělnění).

Brahmagupta (628) se zabýval složitějšími diofantovskými rovnicemi. On objevil dnes nazývanou Pellovu rovnici a v jeho díle Samasabhayana vyložil metodu jak řešit diofantovské rovnice druhého stupně např. $61x^2 + 1 = y^2$. Tyto metody byly na západě neznámé, rovnici řešil jako problém francouzský matematik Pierre de Fermat kolem roku 1657, nicméně řešení rovnice našel i Euler o sedmdesát let později. Mezi tím bylo toto řešení rovnice zaznamenáno také Bhaskarou II (1150), který používal upravenou verzi Brahmagupotvy metody a také našel řešení Pellovy rovnice.

Diofantovské rovnice se znovu začaly intenzivněji řešit v 17. a 18. století. V roce 1637 si Pierre de Fermat poznamenal na okraj kopie Diofantova díla Arithmetica: „To je nemožné rozdělit krychli na dvě kostky nebo čtvrtou sílu na dvě čtvrté síly nebo obecně nějakou sílu vyšší mocniny na dvě síly stejné vyšší mocniny.“ Řečeno v moderním jazyce: Rovnice tvaru $a^n + b^n = c^n$ nemá řešení pro libovolné n větší než dvě. On pak překvapivě napsal: „Já jsem objevil opravdový důkaz, nicméně okraj není dosti velký, aby ho obsáhl.“ Tento důkaz unikal matematikům celá staletí. Fermatův poslední teorém byl v roce 1994 dokázán britským matematikem Andrew Willesem.

Roku 1900 Hilbert navrhl jako svůj desátý problém řešitelnost všech diofantovských rovnic. V roce 1970 jako výsledek formální logiky Matiyasevichův teorém vyřešil problém negativně: obecně diofantovské problémy jsou neřešitelné (viz [7]).

1.2 Diofantos z Alexandrie a jeho rovnice

Diofantos byl helénský matematik pocházející z Alexandrie. Je nazýván otcem algebry, protože podstatně zjednodušil řecké zapisování čísl a svými pracemi vybudoval základy pro algebraický zápis. Žil kolem roku 250 před naším letopočtem a dochovalo se o něm velmi málo zpráv. Vše, co o tomto slavném matematikovi víme, pochází z jeho nápisu na náhrobku, který má tvar matematické úlohy.

Poutníče! Zde odpočívá popel Diofantův. A čísla poví, je to zázrak, jak dlouhý byl jeho život. Šestina života patřila krásnému dětství. Ještě dvanáctina života uběhla, než se jeho brada pokryla chmýřím. Sedminu života strávil v bezdětném manželství. Uplynulo dalších pět let a radoval se z narození krásného syna, toho, kterému Osud vyměřil veselý a zářící život na této Zemi, ale dlouhý jen polovinu toho, co otcí. A v hlubokém smutku ukončil starý muž svou pout' zde na Zemi, čtyři roky po ztrátě syna.

Z úlohy lze vypočítat kolik bylo Diofantovi let, kdy se oženil, kdy se stal otcem a kdy mu zemřel syn. Z diofantových děl je nejvíce známo dílo Arithmética, ve kterém řeší převážně neurčité rovnice tvaru $Ax^3 + Bx^2 + Cx + D = y^2$ nebo jejich systémy. V tomto díle je patrné, že se zajímá o kladná a racionální řešení. Iracionální řešení nazývá nemocnými. Velmi pečlivě volí koeficienty tak, aby kořeny rovnic byla celá čísla. Rovnice, které mají celočíselné koeficienty a všechny neznámé jsou z oboru celých čísel jsou na jeho počest pojmenovány diofantovské rovnice.

2 Diofantovské rovnice

Diofantovskou rovnicí o n neznámých se rozumí algebraická rovnice s celočíselnými koeficienty s n neznámými, které mohou nabývat pouze celočíselných hodnot. Pro řešení těchto rovnic bohužel neexistuje žádná univerzální metoda. Způsob řešení některých typů využívá Euklidova algoritmu.

2.1 Klasifikace diofantovských rovnic

Třídění diofantovských rovnic může být různé. Jednoduchá klasifikace je v díle Š. Známa [9], který diofantovské rovnice dělí na lineární a rovnice vyššího stupně, kde uvádí pouze některé typy.

Jiné publikace hovoří o klasifikaci z hlediska stupně polynomu, který v rovnici vystupuje, tedy na lineární, kvadratické, kubické, .. , n -tého stupně. V každé rozsáhlejší literatuře se objevují různé typy speciálních diofantovských rovnic jako je např. Pellova diofantovská rovnice. Větší přehled speciálních typů můžeme nalézt například v publikaci J. Sándora [8] včetně způsobů jejich řešení. Dalším hlediskem třídění může být také počet neznámých.

Naše klasifikace bude prostá. Zmíníme se o řešení lineárního typu, v další části pak rozebereme diofantovské rovnice lineární vzhledem k nějaké neznámé. Nejrozsáhlejší bude kapitola zabývající se speciálními typy rovnic s ukázkou některých příkladů a metod řešení.

2.1.1 Lineární diofantovské rovnice

Lineární diofantovské rovnice jsou rovnice tvaru

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b \quad (1)$$

kde $x_1, \dots, x_n$, jsou neznámé, $a_1, \dots, a_n, b$ daná celá čísla. Předpokládejme, že $a_i \neq 0$ pro každé $i = 1, \dots, n$. Při řešení těchto rovnic většinou využíváme kongruencí.

Tento typ, respektive diofantovská rovnice o dvou neznámých $ax + by = c$, je nejznámější a žáci se s ním setkávají již na základní škole a samozřejmě i v praxi. Uvedeme jeden ukázkový příklad.

Příklad 1. Najděte všechna trojčíselná čísla, která při dělení devatenácti dávají zbytek 4 a při dělení třinácti zbytek 2.

Řešení. Označme hledané číslo písmenem x , dále pak písmenem y neúplný podíl při dělení devatenácti a z neúplný podíl při dělení třinácti, platí, že

$$x = 19y + 4 \text{ a zároveň } x = 13z + 2.$$

Dostáváme soustavu dvou rovnic o třech neznámých. Vyloučením neznámé x dostaneme jednu diofantovskou rovnici prvního stupně o dvou neznámých.

$$13z - 19y = 2$$

Tato rovnice má řešení, protože pravá strana je násobkem čísla $D(13, 19) = 1$. Uhodnout některá řešení je poměrně obtížné, proto postupujme takto: Vyjádříme tu neznámou, jejíž koeficient má nejmenší absolutní hodnotu pomocí druhé neznámé. Dostaneme tak

$$z = \frac{19y + 2}{13} = y + \frac{6y + 2}{13}.$$

Číslo z je celé právě tehdy, když číslo $6y + 2$ je násobek třinácti, tedy je-li

$$6y + 2 = 13u,$$

kde $u \in \mathbb{Z}$. Dostali jsme opět diofantovskou rovnici prvního stupně, ale s menšími koeficienty. Postup budeme opakovat s neznámou y .

$$y = \frac{13u - 2}{6} = 2u + \frac{u - 2}{6}$$

Z tohoto výpočtu plyne, že $u - 2$ musí být násobek šesti, tedy musí platit, že

$$u - 2 = 6t,$$

kde $t \in \mathbb{Z}$. Je tedy

$$u = 6t + 2.$$

Dosadíme-li tento výsledek do výrazu pro y , máme

$$y = 2(6t + 2) + t = 13t + 4$$

odkud pak pro z dostaneme

$$z = 13t + 4 + \frac{6(13t + 4) + 2}{13} = 19t + 6$$

a konečně pak

$$x = 19(13t + 4) + 4 = 247t + 80$$

Uvedenou vlastnost mají tedy čísla $247t + 80$, kde $t \in \mathbb{Z}$.

Mezi nimi máme najít všechna, která jsou trojčíferná, proto platí, že $247t + 80 \geq 100$ a

zároveň $247t + 80 < 1000$. Odkud pro t plyne, že $t \geq \frac{20}{247}$ a zároveň $t < \frac{920}{247}$. To splňují

pouze tři čísla 1, 2, 3. Dosadíme-li je do výrazu pro x , dostaneme čísla 327, 574, 821, které jsou řešením této úlohy.

Nyní se zabýváme podrobněji rovnicí (1). Nejprve uvažujeme, kdy vůbec má rovnice (1) řešení. Jestliže číslo b není dělitelné číslem $d = D(a_1, \dots, a_n)$, nemůže mít (1) žádné řešení, protože pro libovolná celá čísla $x_1, \dots, x_n$ je levá strana (1) dělitelná číslem d . Pokud naopak d/b , můžeme celou rovnici (1) vydělit číslem d . Po zjednodušení dostaneme rovnici $a_1'x_1 + a_2'x_2 + \dots + a_n'x_n = b'$, kde $a_i' = a_i/d$ pro $i=1, \dots, n$ a $b' = b/d$. Rovnice (1) má celočíselné řešení, právě když číslo b je dělitelné největším společným dělitelem čísel $a_1, a_2, \dots, a_n$. Předchozí úvahy lze shrnout do následující věty.

Věta 1: Necht' $n \geq 2$. Rovnice

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

kde $a_1, a_2, \dots, a_n, b$, jsou celá čísla taková, že $(a_1, \dots, a_n) = 1$, má vždy celočíselné řešení. Všechna řešení této rovnice je možné popsat pomocí $n-1$ celočíselných parametrů.

Důkaz této věty lze provést indukcí vzhledem k počtu n neznámých x_i v rovnici (1), není však úkolem ani cílem této práce. Metodu z důkazu lze použít při řešení některých příkladů (viz následující).

Věta 2: Nutná a postačující podmínka pro to, aby diofantovská rovnice (1) měla celočíselné řešení, je

$$b = k \cdot D(a_1, a_2, \dots, a_n),$$

kde k je celé číslo.

Příklad 2. Řešte rovnici $12x + 10y + 15z = 1$ v oboru celých čísel.

Řešení. Protože $D(12, 10, 15) = 1$ je dělitel čísla 1 má rovnice celočíselné řešení.

Libovolné řešení této rovnice musí splňovat kongruenci

$$12x + 10y + 15z \equiv 1 \pmod{2}$$

tedy $15z \equiv 1 \pmod{2}$, odkud $z \equiv 1 \pmod{2}$, tj. $z = 1 + 2t$, kde $t \in \mathbb{Z}$. Dosazením do rovnice dostáváme

$$12x + 10y + 15(1 + 2t) = 1$$

po ekvivalentních úpravách

$$12x + 10y = -14 - 30t$$

Tuto rovnici budeme řešit pro libovolné $t \in \mathbb{Z}$. Je-li rovnice splněna musí platit

$$12x + 10y = -14 - 30t \pmod{12},$$

odkud $10y = -14 - 30t \pmod{12}$, tedy $y = 1 - 3t \pmod{12}$, tj. $y = 1 - 3t + 12s$ kde $t, s \in \mathbb{Z}$.

Dosazením do rovnice dostáváme

$$12x + 10(1 - 3t + 12s) + 15(1 + 2t) = 1,$$

odkud vypočítáme $x = -2 - 10s$, kde $t \in \mathbb{Z}$. Tedy řešením zadané lineární diofantovské rovnice o třech neznámých jsou všechna celá čísla pro něž platí

$$x = -2 - 10s, \quad y = 1 - 3t + 12s, \quad z = 1 + 2t, \quad \text{kde } s, t \in \mathbb{Z}$$

2.1.2 Diofantovské rovnice lineární vzhledem k některé neznámé

V této kapitole se budeme zabývat rovnicemi, které lze upravit do tvaru, kdy na jedné straně rovnice bude jedna neznámá, která je v první mocnině a zbytek rovnice bude na druhé straně rovnice. Matematicky zapsáno se jedná o rovnici tohoto tvaru

$$mx_n = F(x_1, \dots, x_{n-1}), \quad (2)$$

kde m je číslo přirozené a $F(x_1, \dots, x_{n-1})$ je mnohočlen s celočíselnými koeficienty. Má-li potom být $x_1, \dots, x_n$ celočíselným řešením rovnice (2), musí platit následující

$$F(x_1, \dots, x_{n-1}) \equiv 0 \pmod{m}. \quad (3)$$

Pokud $x_1, \dots, x_{n-1}$ je řešení kongruence (3), pak pro $x_n = F(x_1, \dots, x_{n-1})/m$ dostaneme celočíselné řešení $x_1, \dots, x_{n-1}, x_n$ rovnice (2). Proto chceme-li vyřešit rovnici (2) postačí nám vyřešit kongruenci (3). V případě, že $n=2$, dostaneme mnohočlen $F(x_1)$ který je mnohočlenem jedné proměnné a jedná se o lineární diofantovskou rovnici. Pro $n > 2$ je možno řešit analogicky podle následující věty.

Věta 3: Pro libovolný mnohočlen $F(x_1, \dots, x_s)$ s celočíselnými koeficienty, přirozené číslo m a celá čísla $a_1, \dots, a_s, b_1, \dots, b_s$ taková, že $a_1 \equiv b_1 \pmod{m}$, ..., $a_s \equiv b_s \pmod{m}$, platí $F(a_1, \dots, a_s) \equiv F(b_1, \dots, b_s) \pmod{m}$.

Abychom mohli nalézt všechna řešení kongruence (3) postačí dosazovat do mnohočlenu $F(x_1, \dots, x_{n-1})$ za $x_1, \dots, x_{n-1}$ nezávisle na sobě postupně čísla $0, 1, \dots, m-1$ (tj. celkem m^{n-1} -krát). Právě tehdy, když pro čísla $a_1, \dots, a_{n-1}$ je splněna podmínka $F(a_1, \dots, a_{n-1}) \equiv 0 \pmod{m}$, dostáváme řešení kongruence (3) ve tvaru

$$x_1 = a_1 + mt_1, \dots, x_{n-1} = a_{n-1} + mt_{n-1},$$

kde $t_1, \dots, t_{n-1}$ mohou nabývat libovolných celočíselných hodnot. Tak dostaneme i řešení rovnice (2).

$$\begin{aligned}
x_1 &= a_1 + mt_1 \\
&\vdots \\
x_{n-1} &= a_{n-1} + mt_{n-1} \\
x_n &= \frac{1}{m} F(a_1 + mt_1, \dots, a_{n-1} + mt_{n-1})
\end{aligned}$$

V předchozí úvaze jsme ukázali metodu jakou lze řešit některé diofantovské rovnice (viz [2]). Obtížnější částí této metody může být řešení kongruence vyššího stupně. Připomeňme proto v následující větě a jejím důsledku jak lze danou kongruenci řešit.

Věta 4: Pro libovolný mnohočlen $F(x)$ s celočíselnými koeficienty, přirozené číslo m a celá čísla a, b taková, že $a \equiv b \pmod{m}$, platí $F(a) \equiv F(b) \pmod{m}$.

Důkaz: Necht' je $F(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$, kde $c_0, c_1, \dots, c_n \in \mathbb{Z}$. Protože $a \equiv b \pmod{m}$, pro každé $i = 1, \dots, n$ platí $c_i a^i \equiv c_i b^i \pmod{m}$ a tedy sečtením těchto kongruencí pro $i = 1, \dots, n$ a kongruence $c_0 \equiv c_0 \pmod{m}$ dostaneme $c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \dots + c_1 b + c_0 \pmod{m}$ tj. $F(a) \equiv F(b) \pmod{m}$.

Důsledek: Jestliže pro žádné celé číslo a , $0 \leq a < m$, neplatí kongruence $F(a) \equiv 0 \pmod{m}$, nemá kongruence

$$F(x) \equiv 0 \pmod{m} \quad (4)$$

řešení. Pokud jsou $a_1, a_2, \dots, a_s$ všechna celá čísla taková, že $0 \leq a_i < m$ a $F(a_i) \equiv 0 \pmod{m}$, pak jsou řešením kongruence (4) právě všechna celá čísla x , vyhovující některé z kongruencí

$$x \equiv a_1 \pmod{m}, x \equiv a_2 \pmod{m}, \dots, x \equiv a_s \pmod{m}.$$

Důkaz: Je-li b libovolné celé číslo, pak platí že existuje právě jedno $a \in \mathbb{Z}$ tak, že $0 \leq a < m$ a platí $b \equiv a \pmod{m}$. Dle věty 3 je pak b řešením kongruence (4), právě když je

a jejím řešením. Při řešení kongruence (4) stačí zjistit, pro která celá čísla a , $0 \leq a < m$, platí $F(a) \equiv 0 \pmod{m}$. Z tohoto lze říci, že jedinou nevýhodou při použití této metody je její pracnost, která se zvyšuje zvětšující se hodnotou m .

Jak řešit konkrétní příklady různé náročnosti si ukážeme na následujících příkladech.

Příklad 3. Řešte v oboru celých čísel $x^2 - 11y - 4 = 0$

Řešení. Rovnici upravíme na rovnici lineární vzhledem k nějaké neznámé v tomto případě k neznámé y . Tedy do tohoto tvaru $11y = -4 + x^2$ a budeme řešit kongruenci

$$-4 + x^2 \equiv 0 \pmod{11}$$

po úpravách dostaneme $x^2 \equiv 4 \pmod{11}$. Dosadíme-li za x čísla 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 a 10, zjistíme že kongruence je splněna pro čísla 2 a 9. Řešením této kongruence jsou tedy dle důsledku věty 3 právě čísla

$$x = 2 + 11t \quad \text{nebo} \quad x = 9 + 11t$$

kde $t \in \mathbb{Z}$. Dosazením dostaneme v prvním případě

$$11y = -4 + (2 + 11t)^2 = 44t + 121t^2$$

a tedy

$$y = 4t + 11t^2,$$

ve druhém případě

$$11y = -4 + (9 + 11t)^2 = 77 + 198t + 121t^2$$

po úpravě

$$y = 7 + 18t + 11t^2.$$

Řešením dané rovnice jsou tedy právě všechny dvojice čísel x, y tvaru

$$x = 2 + 11t, \quad y = 4t + 11t^2 \quad \text{nebo} \quad x = 9 + 11t, \quad y = 7 + 18t + 11t^2,$$

kde t je libovolné celé číslo.

Příklad 4. Řešte v oboru celých čísel $(x^2 + 2)x = 125y - 2$

Řešení. Budeme postupovat stejně jako v předchozím případě. Vyjádříme neznámou y , která je v první mocnině pomocí druhé neznámé, tedy takto

$$125y = (x^2 + 2)x + 2$$

a roznásobením dostaneme tvar

$$125y = x^3 + 2x + 2.$$

Budeme řešit následující kongruenci

$$x^3 + 2x + 2 \equiv 0 \pmod{125}.$$

Stejně jako v předchozím případě budeme hledat celá čísla v tomto příkladě z intervalu $\langle 0; 124 \rangle$, která vyhovují této kongruenci. Logicky lze usoudit, že nemusíme zkoušet dosazovat všechna čísla, ale pouze čísla lichá. Počet možných čísel, který můžou této kongruenci vyhovovat se tak sníží na polovinu. Postupným dosazováním zjistíme, že vyhovuje pouze číslo 113. Řešením této kongruence je tedy

$$x = 113 + 125t,$$

kde $t \in \mathbb{Z}$. Dosazením dostaneme

$$125y = (113 + 125t)^3 + 2(113 + 125t) + 2$$

po úpravách

$$125y = 1442897 + 4788375t + 5296875t^2 + 1953125t^3 + 226 + 250t + 2$$

$$125y = 1443125 + 4788625t + 5296875t^2 + 1953125t^3$$

$$y = 11545 + 38309t + 42375t^2 + 15625t^3$$

Řešením dané rovnice jsou tedy všechny dvojice čísel x, y tvaru

$$x = 113 + 125t, \quad y = 11545 + 38309t + 42375t^2 + 15625t^3.$$

Až dosud jsme řešili pouze diofantovské rovnice o dvou neznámých. V následujícím příkladě si ukážeme, že lze vyřešit i zdánlivě složitou diofantovskou rovnici o čtyřech neznámých druhého stupně. I tuto rovnici lze převést na rovnici, která je lineární vzhledem k některé neznámé, v našem případě k neznámé u .

Příklad 5. Řešte rovnici $x^2 + 4y^2 + 9z^2 = 8u - 1$ v oboru celých čísel

Řešení. Rovnici převedeme na lineární tvar vzhledem k neznámé u . Po úpravách bude rovnice v tomto tvaru

$$8u = x^2 + 4y^2 + 9z^2 + 1.$$

Budeme hledat řešení kongruence

$$x^2 + 4y^2 + 9z^2 + 1 \equiv 0 \pmod{8}.$$

Nyní bychom mohli za uspořádanou trojici (x, y, z) postupně dosazovat uspořádané trojice $(0, 0, 0), (0, 0, 1), (0, 1, 1) \dots (7, 7, 6), (7, 7, 7)$. Museli bychom tak spočítat všech $8^3 = 512$ hodnot výrazu na levé straně. Rychlejší řešení bude využití tvaru kongruence a práci si ulehčit.

Kongruenci si lze přepsat na tento tvar

$$x^2 + (2y)^2 + (3z)^2 \equiv 7 \pmod{8}.$$

Na levé straně je součet tří druhých mocnin celých čísel. Máme tedy dvě možnosti, buď projít všech 72 situací: $x \in \{0, 1, 2, \dots, 6\}$

$$2y \in \{0, 2, 4, 6\}$$

$$3z \in \{0, 3, 6\}$$

nebo prozkoumat zbytky druhých mocnin po dělení osmi:

$$(8k)^2 \equiv 0 \pmod{8}$$

$$(8k \pm 1)^2 \equiv 1 \pmod{8}$$

$$(8k \pm 2)^2 \equiv 4 \pmod{8}$$

$$(8k \pm 3)^2 \equiv 1 \pmod{8}$$

$$(8k \pm 4)^2 \equiv 0 \pmod{8}$$

Z tohoto je patrné, že součet členů umocněných na druhou může dávat pouze zbytky 0, 1, 2, 3, 4, 5, 6. Levá strana rovnice může tedy být pouze 0, 1, 2, 3, 4, 5, 6 (mod 8). Rovnice proto nemá žádné řešení.

2.1.3 Speciální typy diofantovských rovnic

Existuje mnoho speciálních typů diofantovských rovnic. V této práci uvedeme tyto typy:

$$xy = z^2 + 1, \quad \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = \frac{1}{x_{n+1}}, \quad \text{Pellovu rovnici tj. rovnici tvaru } x^2 - Dy^2 = 1,$$

Pythagorejskou diofantovskou rovnici tvaru $x^2 + y^2 = z^2$ a na závěr diofantovskou rovnici $x^n + y^n = x^p y^q z$. Další některé speciální typy diofantovských rovnic lze nalézt v publikaci [8] J. Sándora.

2.1.3.1 Diofantovská rovnice $xy = z^2 + 1$

Tato rovnice se týká problému, zda lze rozhodnout o existenci všech matic $A \in M_2[\mathbb{Z}]$ (tj. matic druhého řádu s celočíselnými koeficienty) takových, pro které platí, že $A^2 = -E$, kde E je jednotková matice.

Nechť $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, pak dostáváme následující systém rovnic:

$$a^2 + bc = -1, \quad ab + bd = 0, \quad ca + cd = 0, \quad cb + d^2 = -1.$$

Tedy $b \neq 0$, $c \neq 0$, $d = -a$ a $a^2 + 1 = -bc$. Nechť $b = -B$ s $B > 0$ a nechť $c > 0$. Dostáváme $a^2 + 1 = Bc$. Jinak řečeno musíme vyřešit rovnici $xy = z^2 + 1$ jejíž řešení budou pouze kladná celá čísla.

Využijeme následující pomocné věty:

Věta 5: Nechť x, z jsou kladná celá čísla. Pokud $x \mid (z^2 + 1)$, pak x můžeme zapsat jako součet dvou druhých mocnin (tj. $x = a^2 + b^2$, kde $a, b \geq 0$)

Věta 6: (Lagrangeova identita)

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Tedy podle věty 5 můžeme položit $x = a^2 + b^2$ a $y = c^2 + d^2$, kde $a, b, c, d \in \mathbb{N}$. Pak tedy z rovnice $xy = z^2 + 1$ dostáváme

$$(a^2 + b^2)(c^2 + d^2) = z^2 + 1$$

Dle Lagrangeovy identity (věty 6) platí, pokud $|ad - bc| = 1$ pak $z = ac + bd$ určuje řešení dané rovnice. Například pokud $D(a, b) = 1$ existují kladná celá čísla (c, d) taková, že $ab - dc = 1$. Proto má daná rovnice nekonečně mnoho řešení. Nyní dokážeme následující tvrzení jak je ukázáno v [8].

Věta 7: Všechna kladná řešení rovnice $xy = z^2 + 1$ mohou být zapsána ve tvaru $x = a^2 + b^2, y = c^2 + d^2, z = ac + bd$, kde $a, b, c, d \in \mathbb{N}$ a $|ad - bc| = 1$.

Důkaz: Předpokládejme, že existuje trojice (x, y, z) vyhovující dané rovnici, která nejde zapsat ve tvaru jako je vyjádřeno v předchozí větě. Necht' (x_0, y_0, z_0) je taková trojice, kde z_0 je nejmenší možné. Předpokládejme, že $x_0 \leq y_0$ (pokud ne, můžeme zaměnit x_0 za y_0). Pak dostáváme $x_0 y_0 = z_0^2 + 1$, $x_0, y_0, z_0 \geq 1$, kde nemáme taková přirozená čísla pro které platí, že $x_0 = a^2 + b^2$, $y_0 = c^2 + d^2$, $z_0 = ac + bd$ s $|ad - bc| = 1$. Můžeme tedy vytvořit další trojici (x, y, z) , která vyhovuje rovnici. Necht' $z = u + x$ pak rovnice je tvaru $xy - x^2 - 2xu - u^2 = 1$, tedy $x(y - x - 2u) = u^2 + 1$. Položíme-li $u = z - x$ dostaneme rovnici tvaru $y - x - 2u = y + x - 2z$. Jinak řečeno, trojice $(x_0, x_0 + y_0 - 2z_0, z_0 - x_0)$ vyhovuje rovnici $xy = z^2 + 1$. Nyní stačí jen ověřit, zda každá proměnná je ≥ 1 . Tedy platí, že $z_0^2 = x_0 y_0 - 1 < x_0 y_0 \leq \left(\frac{x_0 + y_0}{2}\right)^2$, pak $z_0 < \frac{x_0 + y_0}{2}$ což implikuje výraz $x_0 + y_0 - 2z_0 > 0$.

Vezměme to z druhé strany, pokud $z_0 - x_0 \leq 0$ dostáváme $z_0 \leq x_0 \leq y_0$. Musíme rozlišit dva případy:

- 1) Pokud $z_0 = x_0$ pak $x_0(y_0 - x_0) = 1$, tedy $x_0 = 1 = 1^2 + 0^2$, $y_0 = 2 = 1^2 + 1^2$,
 $z_0 = 1 = 1 \cdot 1 + 1 \cdot 0$ a $(1 \cdot 1 - 1 \cdot 0) = 1$ což je ve sporu s uvedeným předpokladem.
- 2) Jestliže $z_0 < x_0$ pak $1 = x_0 y_0 - z_0^2 \geq x_0^2 - z_0^2 \geq (z_0 + 1)^2 - z_0^2 = 2z_0 + 1$ tedy
 $z_0 \leq 0$ což je vyloučené.

Pokud $z_0 > x_0$ z toho jasně plyne, že $z_0 - x_0 \geq 1$.

Nyní má nová trojice člen $z_0 - x_0 < z_0$, potom za námi vysloveného předpokladu existují přirozená čísla m, n, p, q takové, že $x_0 = m^2 + n^2$, $x_0 + y_0 - 2z_0 = p^2 + q^2$,
 $z_0 - x_0 = mp + nq$, kde $|mq - np| = 1$.

Z toho plyne, že

$$z_0 = m^2 + n^2 + mp + nq = m(m + p) + n(n + q)$$

$$y_0 = p^2 + q^2 + 2z_0 - x_0 = p^2 + q^2 + 2mp + m^2 + n^2 = (m + p)^2 + (n + q)^2$$

Proto můžeme psát, že $x_0 = m^2 + n^2$, $y_0 = (m + p)^2 + (n + q)^2$, $z_0 = m(m + p) + n(n + q)$,

kde $|m(n + q) - n(m + p)| = 1$.

Dostáváme tak spor (vybráním $a = m, b = n, c = m + p, d = n + q$).

2.1.3.2 Diofantovská rovnice tvaru $\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = \frac{1}{x_{n+1}}$

Další rovnicí, která je také uvedena v publikaci J. Sándora [8], je následující

$$\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = \frac{1}{x_{n+1}}$$

Necht' $x_i \ (i = \overline{1, n+1})$ jsou kladná celá čísla. Pro $n = 1$ dostáváme rovnici ve tvaru

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

Pro $n = 2$ dostáváme rovnici tvaru

$$\frac{1}{x_1} + \frac{1}{x_2} = \frac{1}{x_3} \quad (5)$$

Tato rovnice je velmi důležitá pro geometrii, teorii čísel, optiku, fyziku,...

Necht' $n \geq 3$. Pro jednoduchost ještě poznamenejme, že $\sum x_1 \dots \hat{x}_i \dots x_n$ je suma $x_1 \dots \hat{x}_i \dots x_n$, kde $\hat{x}_i$ znamená, že člen x_i chybí (pro $n = 3$ je tato suma $x_1 x_3 + x_2 x_3 + x_1 x_2$). Pak pro

$$\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = \frac{1}{x_{n+1}} \quad (6)$$

to znamená, že

$$\sum x_1 \dots \hat{x}_i \dots x_n / x_1 x_2 \dots x_n \quad (7)$$

Necht' $d = (x_1, x_2, \dots, x_n)$ je největší společný dělitel pro $x_1, x_2, \dots, x_n$. Pak $x_1 = dy_1, \dots, x_n = dy_n$, kde $(y_1, y_2, \dots, y_n) = 1$. Po dosazení do (7) a zjednodušení s d^{n-1} dostáváme

$$\sum y_1 \dots \hat{y}_i \dots y_n / y_1 y_2 \dots y_n \quad (8)$$

Necht' $D = (y_1 y_2 \dots y_n \sum y_1 \dots \hat{y}_i \dots y_n)$. Pak z (8) vyplývá, že $\sum y_1 \dots \hat{y}_i \dots y_n / dD$ to znamená, že existuje celé kladné číslo k takové, že $dD = k \sum y_1 y_2 \dots \hat{y}_i \dots y_n$.

Proto

$$\begin{aligned}x_1 &= \frac{k \sum y_1 \dots \hat{y}_i \dots y_n}{(y_1 \dots y_n, \sum y_1 \dots \hat{y}_i \dots y_n)} y_1, \\x_2 &= \frac{k \sum y_1 \dots \hat{y}_i \dots y_n}{(y_1 \dots y_n, \sum y_1 \dots \hat{y}_i \dots y_n)} y_2 \\x_n &= \frac{k \sum y_1 \dots \hat{y}_i \dots y_n}{(y_1 \dots y_n, \sum y_1 \dots \hat{y}_i \dots y_n)} y_n\end{aligned} \quad (9)$$

Zde $\frac{k \sum y_1 \dots \hat{y}_i \dots y_n}{(y_1, \dots, y_n, \sum y_1 \dots \hat{y}_i \dots y_n)} = A$ je kladné celé číslo, takové, že $x_i (i = \overline{1, n})$ jsou kladná

celá čísla, vyhovující rovnici. Naopak z výrazů (9) dostáváme, že

$$\sum x_1 \dots \hat{x}_i \dots x_n = A^{n-1} \sum y_1 \dots \hat{y}_i \dots y_n \quad (10)$$

a

$$x_1 x_2 \dots x_n = A^n \sum y_1 y_2 \dots y_n$$

Odkud $A y_1 \dots y_n = k \cdot \sum y_1 \dots \hat{y}_i \dots y_n \cdot y_1 y_2 \dots y_n / (y_1 y_2 \dots y_n, \sum y_1 \dots \hat{y}_i \dots y_n)$ a

$(y_1 \dots y_n, \sum y_1 \dots \hat{y}_i \dots y_n) / y_1 \dots y_n$ dostáváme $\sum y_1 \dots \hat{y}_i \dots y_n / A y_1 \dots y_n$, pak (10) implikuje (7).

Vše dohromady je obecné řešení rovnice (6) z (9) a $x_{n+1} = \frac{x_1 \dots x_n}{\sum x_1 \dots \hat{x}_i \dots x_n} = \frac{A y_1 \dots y_n}{\sum y_1 \dots \hat{y}_i \dots y_n}$ kde

$y_1 \dots y_n$ jsou libovolná celá kladná čísla, splňující $(y_1, \dots, y_n) = 1$, zatímco k je kladné celé číslo.

Poznámka:

1) Pro $n = 2$ máme

$$x_1 = ky_1(y_1 + y_2)$$

$$x_2 = ky_2(y_1 + y_2)$$

$$x_3 = ky_1y_2$$

a $(y_1, y_2, y_1 + y_2) = 1$ pro $(y_1, y_2) = 1$

2) Pro $n = 3$ je obecný výsledek zapsán:

$$x_1 = ky_1(y_1y_2 + y_1y_3 + y_2y_3) / (y_1y_2y_3, y_1y_2 + y_1y_3 + y_2y_3)$$

$$x_2 = ky_2(y_1y_2 + y_1y_3 + y_2y_3) / (y_1y_2y_3, y_1y_2 + y_1y_3 + y_2y_3)$$

$$x_3 = ky_3(y_1y_2 + y_1y_3 + y_2y_3) / (y_1y_2y_3, y_1y_2 + y_1y_3 + y_2y_3)$$

$$x_4 = \frac{ky_1y_2y_3}{(y_1y_2y_3, y_1y_2 + y_1y_3 + y_2y_3)}$$

kde $k > 0$ je libovolné a $(y_1, y_2, y_3) = 1$

2.1.3.3 Pellova rovnice $x^2 - Dy^2 = N$

Problém řešení této rovnice položil Pierre de Fermat v roce 1657. Lord Brouncker byl ten, kdo našel jako první řešení Pellovy rovnice ovšem bez důkazu. V roce 1685 úplnou odpověď dal J. Wallis. Dalším významným matematikem byl Leopard Ruler, který se také zabýval touto rovnicí a nazval ji Pellova rovnice. Tento termín se v literatuře ustálil a používá se až dodnes.

Rovnice

$$x^2 - Dy^2 = N, \text{ kde } D = a^2 - 1, a > 1, N \in \mathbb{Z} - \{0\} \quad (11)$$

s podmínkou, že řešení x, y jsou z oboru celých čísel, se nazývá Pellova rovnice. Při řešení této rovnice stačí hledat řešení v oboru přirozených čísel, protože s každou dvojicí (x, y) vyhovují i dvojice $(x, -y)$, $(-x, y)$, $(-x, -y)$. Pokud bychom položili $a = 1$ dostaneme triviální rovnici. Pro $a = 0$ dostaneme rovnici $x^2 + y^2 = 1$. Její řešení (ne nutně celočíselné) lze vyjádřit pomocí funkcí sinus a kosinus. Některé kroky při řešení Pellovy rovnice budou připomínat známé vlastnosti funkcí sinus a kosinus, jiné potom vlastnosti Fibonacciho posloupnosti. Není to žádná náhoda, Pellova rovnice s Fibonacciho posloupností souvisí.

Uvažujme nejmenší kladné řešení rovnice $x^2 - Dy^2 = 1$ pro $980 \leq D \leq 1005$ jako jsou ukázána v následující Tabulce č.1 převzaté z publikace [10]. Někdy jsou nejmenší řešení docela malá a někdy velká čísla.

Tabulka č.1

Nejmenší kladná řešení

D	x	y
980	51841	1656
981	158070671986249	5046808151700
982	8837	282
983	284088	9061
984	88805	2831
985	332929	10608
986	49299	1570
987	377	12
988	14549450527	462879684
989	550271588560695	17497618534396
990	881	28
991	379516400906811930638014896080	12055735790331359447442538767
992	63	2
993	2647	84
994	1135	36
995	8835999	280120
996	8553815	271038
997	14418057673	456624468
998	984076901	31150410
999	102688615	3248924
1000	39480499	1248483
1001	1060905	33532
1002	206869247	6535248
1003	9026	285
1004	27009633024199	852416459730
1005	2950149761	93059568

Hlavní metoda, kterou uvedeme jako metodu pro řešení obecné Pellovy rovnice, Lagrange-Matthews-Mollin (LMM) algoritmus, je lehce obsáhlejší než standardní metoda řetězových zlomků pro řešení Pellovy rovnice tvaru $x^2 - Dy^2 = 1$. Pro řešení obecné Pellovy rovnice (pro libovolné $N \neq 0$) uvedeme tři metody:

1. Metoda násilného hledání řešení (tato metoda je vhodná pouze když horní hledaná limita, vyjádřená níže, není moc velká)
2. Lagrange-Matthews-Mollin algoritmus
3. Lagrangeův systém zjemňování

Řešení Pellovy rovnice rozdělíme dle Johna P. Robertsona [10] na tyto části:

- 1) PQa algoritmus
- 2) Řešení rovnice $x^2 - Dy^2 = \pm 1$
- 3) Struktura řešení rovnice $x^2 - Dy^2 = N$
- 4) Řešení rovnice $x^2 - Dy^2 = N$ pro $N^2 < D$
- 5) Řešení rovnice $x^2 - Dy^2 = N$ metodou násilného hledání kořenů
- 6) Řešení rovnice $x^2 - Dy^2 = N$ metodou LMM algoritmu
- 7) Lagrangeův systém zjemňování

PQa algoritmus

Tento algoritmus je srdcem mnoha metod k řešení Pellových rovnice včetně LMM algoritmu. Slouží k počítání řetězových zlomků z iracionálních výrazů $(P_0 + \sqrt{D})/Q_0$ pro proměnné P_0, Q_0, D a také libovolné proměnné.

Nechť P_0, Q_0, D jsou celá čísla taková, že $Q_0 \neq 0, D > 0$, D není čtverec a $P_0^2 \equiv D \pmod{Q_0}$.

Položme

$$A_{-2} = 0, A_{-1} = 1,$$

$$B_{-2} = 0, B_{-1} = 0,$$

$$G_{-2} = -P_0, G_{-1} = Q_0.$$

Pro $i \geq 0$ položme

$$a_i = \left[(P_i + \sqrt{D}) / Q_i \right],$$

$$A_i = a_i A_{i-1} + A_{i-2},$$

$$B_i = a_i B_{i-1} + B_{i-2},$$

$$G_i = a_i G_{i-1} + G_{i-2},$$

a pro $i \geq 1$ položíme

$$P_i = a_{i-1}Q_{i-1} - P_{i-1}$$

$$Q_i = (D - P_i^2)/Q_{i-1}.$$

Každá z těchto proměnných bude z množiny celých čísel pro všechny indexy, které jsou definovány. Důležitým výsledkem algoritmu bude posloupnost $a_0, a_1, a_2, \dots$ díky nimž

vyjádříme řetězový zlomek z $\xi_0 = (P_0 + \sqrt{D})/Q_0$. To jest

$$(P_0 + \sqrt{D})/Q_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

Píšeme $\langle a_0, a_1, a_2, \dots \rangle$ pro tento řetězový zlomek. Proměnné a_i jsou parciální koeficienty pro ξ_0 .

Pak, pro $i \geq 0$, nechť $\xi_i = (P_i + \sqrt{D})/Q_i$ a nechť je $\bar{\xi}_i = (P_i - \sqrt{D})/Q_i$. Položme $\xi = \xi_0$ a $\bar{\xi} = \bar{\xi}_0$. Proměnné ξ_i jsou s i -tým kompletním koeficientem ξ .

Tyto proměnné mají mnoho vlastností, zmiňme některé z nich.

1. Pro $i > 0, a_i > 0$.
2. Každá z posloupností $\{a_i\}, \{P_i\}, \{Q_i\}$ je konečně periodická. Speciálně, je zde nejmenší nezáporné celé číslo i_0 a nejméně kladné celé číslo ℓ , velikosti minimální periody, proto pro jakékoliv celé číslo $i \geq i_0$ a $k > 0$, $a_{i+k\ell} = a_i$, $P_{i+k\ell} = P_i$, $Q_{i+k\ell} = Q_i$, $\xi_{i+k\ell} = \xi_i$.
3. Pro $i \geq i_0, 0 < P_i < \sqrt{D}, 0 < \sqrt{D} - P_i < Q_i < \sqrt{D} + P_i < 2\sqrt{D}$.
4. Pro $i \geq i_0$, pokud $Q_i \neq 1$ pak $a_i < \sqrt{D}$, zatímco pokud $Q_i = 1$ pak $\sqrt{D} < a_i < 2\sqrt{D}$.
5. Pro $i \geq i_0$, $\xi_i = (P_i + \sqrt{D})/Q_i$ je zmenšené, což znamená, že $\xi_i > 1$ a $-1 < \xi_i < 0$.
6. $\xi_i = \langle a_i, a_{i+1}, a_{i+2}, \dots \rangle$ pro $i \geq 0$.
7. $\xi_i = (P_i + \sqrt{D})/Q_i$ jsou odlišné pro $i_0 \leq i \leq i_0 + \ell - 1$.
8. Největší společný dělitel $(A_i, B_i) = 1$ pro $i \geq -2$.
9. Poměr A_i / B_i pro $i \geq 0$ konverguje k rozšířenému řetězovému zlomku $(P_0 + \sqrt{D})/Q_0$.
10. $(P_0 + \sqrt{D})/Q_0 = \lim_{i \rightarrow \infty} \frac{A_i}{B_i}$.
11. $A_i B_{i-1} - A_{i-1} B_i = (-1)^{i-1}$ pro C.
12. $A_i B_{i-2} - A_{i-2} B_i = (-1)^i a_i$ pro $i \geq 0$.
13. $\xi_i = a_i + \frac{1}{\xi_{i+1}}$ pro C
14. $\frac{P_0 + \sqrt{D}}{Q_0} = \frac{A_i \xi_{i+1} + A_{i-1}}{B_i \xi_{i+1} + B_{i-1}}$ pro $i \geq -1$.
15. $P_i^2 \equiv D \pmod{|Q_i|}$ pro $i \geq 0$.

16. $Q_i = Q_{i-2} - a_{i-1}(P_i - P_{i-1})$ pro $i \geq 2$.
17. $G_i = Q_0 A_i - P_0 B_i$ pro $i \geq -2$.
18. $A_i - B_i \xi = \frac{G_i - B_i \sqrt{D}}{Q_0}$; $A_i - B_i \bar{\xi} = \frac{G_i + B_i \sqrt{D}}{Q_0}$ pro $i \geq 0$.
19. $(A_i - B_i \xi)(A_i - B_i \bar{\xi}) = \frac{(-1)^{i+1} Q_{i+1}}{Q_0}$ pro $i \geq -1$.
20. $G_{i-1}^2 - DB_{i-1}^2 = (-1)^i Q_0 Q_i$ pro $i \geq 0$.
21. Největší společný dělitel $D(G_i, B_i) = D(Q_0, B_i)$ pro $i \geq -2$.
22. Největší společný dělitel $D(G_i, B_i)$ dělí Q_{i+1} pro $i \geq -1$.
23. $\frac{1}{B_i + B_{i+1}} \leq \frac{a_{i+2}}{B_{i+2}} < |A_i - B_i \xi| < \frac{1}{B_{i+1}}$ pro $i \geq 0$.
24. $\frac{1}{(a_{i+1} + 2)B_i} \leq \frac{1}{B_i + B_{i+1}}$ pro $i \geq 0$; $\frac{1}{2B_{i+1}} \leq \frac{1}{B_i + B_{i+1}}$ pro $i \geq 0$.
25. $|A_i - \xi B_i| < \frac{1}{2B_i} \Leftrightarrow |Q_{i+1}| < \sqrt{D}$ pro dostatečně velké i .
26. $\left| \frac{G_i - B_i \sqrt{D}}{Q_0} \right| < \frac{1}{2B_i} \Leftrightarrow |G_i^2 - B_i^2 D| < |Q_0| \sqrt{D}$ pro dostatečně velké i .
27. $\lceil \sqrt{D} \rceil + \sqrt{D}$ je zmenšený.

Vztah $G_i^2 - DB_i^2 = (-1)^{i+1} Q_{i+1} Q_0$ bude pro nás velmi důležitý, protože všechny metody, které probereme, budou vyžadovat nastavení $Q_0 = |N|$ a nalezení takových i pro které platí, že $(-1)^{i+1} Q_{i+1} = N / |N|$. Pak G_i, B_i budou řešení uvažované rovnice. Z početního hlediska je žádoucí zmínit, že v některé situaci bude G_i, B_i velmi velké zatímco Q_0 a Q_{i+1} budou malé. Tato rovnice dovoluje přesně spočítat levou stranu výrazu $G_i^2 - DB_i^2 = (-1)^{i+1} Q_{i+1} Q_0$,

když podmínky na levé straně dovolují disponibilní přesnost. To je užitečné vymežit, pokud dosáhneme konce první periody.

Jedna z metod je následující. Když počítáme P_i a Q_i , vymezuje, zda-li $(P_i + \sqrt{D})/Q_i$ se zmenšuje, a nechť i_r je nejmenší i pro které toto nastane. Potom najdeme nejmenší $j > i_r$ pro které platí $P_{i_r} = P_j$ a $Q_{i_r} = Q_j$. Písmeno j označí začátek druhé periody a tedy $j-1$ je konec druhé periody.

Určité P_0 , Q_0 lze vymežit, když nalezneme prostředek první periody, bez toho aniž bychom počítali celou periodu.

Kdykoliv bude $P_0 = 0$ a $Q_0 = 1$ nebo $D \equiv 1 \pmod{4}$, $P_0 = 1, Q_0 = 2$, následující úvaha bude platná. Nechť ℓ je nejmenší index $\ell > 0$ a $Q_\ell = Q_0$ ($=1$ nebo 2). Pokud existuje j takové, že $P_j = P_{j+1}$ a j je nejmenší, pak $\ell = 2j$ a velikost periody je sudá. Jestliže existuje j takové, že $Q_j = Q_{j+1}$ a pokud j je nejmenší, pak $\ell = 2j + 1$ a velikost periody je lichá. Pro jiný případ můžeme ihned vypočítat druhou polovinu první periody za pomoci následujících vztahů, které vyjadřují palindromické vlastnosti posloupnosti P_i , Q_i a a_i : $P_i = P_{\ell+1-i}$ pro $i = 1, 2, 3, \dots, \ell$, $Q_i = Q_{\ell-i}$ pro $i = 0, 1, 2, 3, \dots, \ell$ a $a_i = a_{\ell-i}$ pro $i = 1, 2, 3, \dots, \ell - 1$. Také, $a_\ell = 2a_0$ jestliže $P_0 = 0$ a $Q_0 = 1$, a $a_\ell = 2a_0 - 1$ pokud $P_0 = 1, Q_0 = 2$. Toto nám dává P_i , Q_i a a_i s indexy $i = \ell$, a periodicitu může být použita pro prodloužení těchto posloupností. Jsou zde dodatečné palindromické vlastnosti těchto posloupností, které jsou viditelné uvažíme-li několik málo případů, např. $(P_0, Q_0, D) = (0, 1, 94), (0, 1, 353), (1, 2, 217), (1, 2, 481)$.

Tabulka č.2 z [10] ilustruje PQa algoritmus pro $P_0 = 11, Q_0 = 108, D = 13$. Výpočty jsou uskutečněny pomocí bodu, který je mírně za konce druhé periody. Poznamenejme, že každá posloupnost $\{a_i\}, \{P_i\}$ a $\{Q_i\}$ je periodická pro $i \geq 3$. Uvnitř každé periody zaznamenáváme právě jedno $Q_i = 1$. Pro daná P_0, Q_0 a D nemusí být žádné $Q_i = 1$. Ale pokud je tam nejméně jedno $Q_i = \pm 1$, jako se stalo zde, pak tam bude právě jedno $Q_i = 1$

v každé periodě $\{Q_i\}$. Poznamenejme, jak hodnoty A_i, B_i a G_i rychle rostou při zvyšujícím se i . Pro výpočet $G_i^2 - DB_i^2$ je nejjednodušší vypočítat $(-1)^{i+1} Q_0 Q_{i+1}$, kde Q_0 je pevné a Q_{i+1} zůstává relativně malé.

Tabulka č.2 PQa algoritmus pro $P_0 = 11, Q_0 = 108, D = 13$

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	-11	
-1				1	0	108	
0	11	108	0	0	1	-11	108
1	-11	-1	7	1	7	31	324
2	4	3	2	2	15	51	-324
3	2	3	1	3	22	82	432
4	1	4	1	5	37	133	-108
5	3	1	6	33	244	880	432
6	3	4	1	38	281	1013	-324
7	1	3	1	71	525	1893	324
8	2	3	1	109	806	2906	-432
9	1	4	1	180	1331	4799	108
10	3	1	6	1189	8792	31700	-432
11	3	4	1	1369	10123	36499	324
12	1	3	1	2558	18915	68199	-324
13	2	3	1	3927	29038	104698	432
14	1	4	1	6485	47953	172897	-108
15	3	1	6	42837	316756	1142080	432
16	3	4	1	49322	364709	1314977	-324

Řešení rovnice $x^2 - Dy^2 = \pm 1$

K vyřešení rovnice $x^2 - Dy^2 = \pm 1$ použijeme PQa algoritmus s $P_0 = 0, Q_0 = 1$. Bude zde nejmenší ℓ s $a_\ell = 2a_0$ které také bude menší $\ell > 0$ tak $Q_\ell = 1$. ℓ je délka periody řetězového zlomku rozšířeného o $\sqrt{D}$. Máme dva případy, které je třeba vzít v úvahu: ℓ je liché nebo ℓ je sudé.

Pokud ℓ je liché, rovnice $x^2 - Dy^2 = -1$ má řešení. Minimální kladné řešení je dané výrazem $x = G_{\ell-1}, y = B_{\ell-1}$. Pro nějaké kladné celé číslo k , pokud k je liché pak $x = G_{k\ell-1}, y = B_{k\ell-1}$ je řešení rovnice $x^2 - Dy^2 = -1$ a všechna řešení této rovnice s x a y kladnými jsou generované tímto způsobem. Pokud k je sudé kladné celé číslo, pak $x = G_{k\ell-1}, y = B_{k\ell-1}$ je řešení rovnice $x^2 - Dy^2 = 1$ a všechna řešení této rovnice s x a y kladnými jsou generované tímto způsobem. Nejmenší kladné řešení rovnice $x^2 - Dy^2 = 1$ je $x = G_{2\ell-1}, y = B_{2\ell-1}$.

Pokud ℓ je nejmenší, tak $a_\ell = 2a_0$ je sudé, pak rovnice $x^2 - Dy^2 = -1$ nemá žádné řešení. Pro jakékoliv kladné číslo k , $x = G_{\ell-1}, y = B_{\ell-1}$ je řešení rovnice $x^2 - Dy^2 = -1$ a všechna ostatní řešení x, y této rovnice jsou odvozeny z tohoto vztahu. Nejmenší kladné řešení rovnice $x^2 - Dy^2 = 1$ je $x = G_{\ell-1}, y = B_{\ell-1}$.

Posloupnost P_i a a_i jsou periodické s periodou ℓ po nultém bodě, první perioda je od P_1 do P_i pro posloupnost P_i a a_1 a a_ℓ pro posloupnost a_i . Posloupnost Q_i je periodická začínající v nultém bodě, tj. první perioda je od Q_0 do $Q_{\ell-1}$.

V předchozí úvaze jsme využívali palindromické vlastnosti posloupností P_i, Q_i, a_i a pravidlo poloviční periody.

Je tedy několik metod jak najít všechna řešení rovnice $x^2 - Dy^2 = \pm 1$ pokud známe nejmenší kladné řešení.

Nejprve posuďme rovnici $x^2 - Dy^2 = 1$. Pokud t, u nejmenší kladná řešení rovnice, pak platí pro n -té kladná řešení $x_n + y_n\sqrt{D} = (t + u\sqrt{D})^n$ a $x_n - y_n\sqrt{D} = (t - u\sqrt{D})^n$. Zatímco každé kladné řešení vyhovuje kladným n tyto rovnice dávají smysl i pro $n \leq 0$. Zde je rekurze vyjádřena takto $x_{n+1} = tx_n + uy_n, y_{n+1} = ty_n + ux_n$. Další dvojice rekurze je (necht' $x_0 = 1, y_0 = 0$) $x_{n+1} = 2tx_n - x_{n-1}, y_{n+1} = 2ty_n - y_{n-1}$. Komentář v tomto odstavci platí, bez ohledu na to, zda-li rovnice $x^2 - Dy^2 = -1$ nemá nebo má řešení.

Nyní předpokládejme, že rovnice $x^2 - Dy^2 = -1$ má řešení, necht' t, u jsou nejmenší kladná řešení a definujme x_n, y_n a rovnici $x_n + y_n\sqrt{D} = (t + u\sqrt{D})^n$. Pak také rovnici $x_n - y_n\sqrt{D} = (t - u\sqrt{D})^n$. Pokud n je liché, x_n, y_n jsou řešení rovnice $x^2 - Dy^2 = -1$ a pokud n je sudé pak x_n, y_n jsou řešení rovnice $x^2 - Dy^2 = 1$. Všechna kladná řešení těchto dvou rovnic jsou takto odvozeny. Rekurze $x_{n+1} = tx_n + uy_nD$, $y_{n+1} = ty_n + ux_n$ také umožňují najít řešení pro dané rovnice. Další rekurze je (necht' $x_0 = 1, y_0 = 0$)

$$x_{n+1} = 2tx_n + x_{n-1}, y_{n+1} = 2ty_n + y_{n-1}.$$

Všechna řešení dostaneme pro $\pm x_n, \pm y_n$. Stručné shrnutí řešení těchto rovnic je možno zapsat takto.

Necht' x, y je nějaké řešení rovnice $x^2 - Dy^2 = \pm 1$. Necht' t, u jsou nejmenší kladná řešení rovnice $x^2 - Dy^2 = \pm 1$. Pak pro nějaká znaménka, ± 1 , a nějaké celá n ,

$$x + y\sqrt{D} = \pm (t + u\sqrt{D})^n.$$

Poznamenejme také, že $(t + u\sqrt{D})^{-1} = \pm (t - u\sqrt{D})$.

Příklad: $x^2 - 13y^2 = -1$

Tabulka č.3

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	0	0
-1				1	0	1	1
0	0	1	3	3	1	3	-4
1	3	4	1	4	1	4	3
2	1	3	1	7	2	7	-3
3	2	3	1	11	3	11	4
4	1	4	1	18	5	18	-1
5	3	1	6	119	33	119	4
6	3	4	1	137	38	137	-3
7	1	3	1	256	71	256	3
8	2	3	1	393	109	393	-4
9	1	4	1	649	180	649	1
10	3	1	6	4287	1189	4287	-4
11	3	4	1	4936	1369	4936	3
12	1	3	1	9223	2558	9223	-3
13	2	3	1	14159	3927	14159	4
14	1	4	1	23382	6485	23382	-1
15	3	1	6	154451	42837	154451	4
16	3	4	1	177833	49322	177833	-3
17	1	3	1	332284	92159	332284	3
18	2	3	1	510117	141481	510117	-4
19	1	4	1	842401	233640	842401	1
20	3	1	6	5564523	1543321	5564523	-4

Tabulka č.3 z [10] aplikuje PQa algoritmus na řešení rovnice $x^2 - 13y^2 = \pm 1$. Perioda délky ℓ je 5, což znamená, že rovnice $x^2 - 13y^2 = -1$ má řešení. Nejmenší kladné řešení je $x=18, y=5$. Nejmenší kladné řešení rovnice $x^2 - 13y^2 = 1$ je $x=649, y=180$. Poznamenejme, že $(18+5\sqrt{13})^2 = 649+180\sqrt{13}$, $(18+5\sqrt{13})^3 = 23382+6485\sqrt{13}$ a $(18+5\sqrt{13})^4 = 842401+233640\sqrt{13}$.

Zmiňme se, jak o Pellově rovnici píše Hruša [3]. Rovnici klasifikuje jako diofantovskou rovnici druhého stupně a zaměřuje se na nalezení všech řešení rovnice tvaru

$$x^2 - Dy^2 = 1,$$

kde D je kladné celé číslo.

Má-li rovnice řešení (x_0, y_0) , je zřejmé, že má také další řešení $(x_0, -y_0)$, $(-x_0, y_0)$, $(-x_0, -y_0)$. Proto se můžeme omezit pouze na hledání kladných řešení Pellovy rovnice.

Je-li D druhou mocninou celého čísla, tj. je-li $D = n^2$, kde $n > 0$, má rovnice tvar

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

neboli

$$(x + ny)(x - ny) = 1.$$

Tomu lze vyhovět pouze kladnými čísly tak, že

$$x + ny = 1 \text{ a také } x - ny = 1,$$

a odtud plyne $x = 1$, $y = 0$. Pellova rovnice má v tomto případě jediné nezáporné řešení $(1, 0)$.

Není-li číslo D druhou mocninou celého čísla, lze dokázat, že rovnice má alespoň jedno kladné řešení.

Věta 8: Pellova rovnice má v případě, že číslo D není druhou mocninou celého čísla, nekonečně mnoho kladných řešení.

Důkaz: Nechť je (x_0, y_0) kladné řešení Pellovy rovnice, tj. nechť pro čísla x_0, y_0 je

$$x_0^2 - Dy_0^2 = 1,$$

neboli

$$(x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = 1.$$

Na základě binomické věty dostaneme, že pro každé kladné celé k je

$$(x_0 + y_0\sqrt{D})^k = (x_1 + y_1\sqrt{D}), \quad (x_0 - y_0\sqrt{D})^k = (x_1 - y_1\sqrt{D}),$$

kde x_1, y_1 jsou vhodná kladná celá čísla. Pak je také

$$x_1^2 - Dy_1^2 = (x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}) = (x_0 + y_0\sqrt{D})^k (x_0 - y_0\sqrt{D})^k = (x_0^2 - Dy_0^2)^k = 1^k = 1,$$

takže (x_1, y_1) je další kladné řešení Pellovy rovnice. Pro každé kladné celé číslo k tedy dostaneme další kladné řešení Pellovy rovnice. Podaří-li se nám tedy uhodnout jedno kladné řešení (x_0, y_0) Pellovy rovnice, dostaneme nekonečně mnoho dalších kladných řešení (x_1, y_1) na základě výpočtu

$$(x_0 + y_0\sqrt{D})^k = x_1 + y_1\sqrt{D},$$

kde k je kladné celé číslo. Jestliže čísla x_0, y_0 značí nejmenší kladná celá čísla, která vyhovují Pellově rovnici, dá se dokázat, že uvedeným postupem dostaneme všechna její řešení.

Struktura řešení rovnice $x^2 - Dy^2 = N$

Pokud r, s je řešení rovnice $x^2 - Dy^2 = N$ a t, u je nějaké řešení rovnice $x^2 - Dy^2 = 1$, pak $x = rt + suD, y = ru + st$ je také řešení rovnice $x^2 - Dy^2 = N$. To plyne ze vztahů $(rt + suD)^2 - D(ru + st)^2 = (r^2 - Ds^2)(t^2 - Du^2)$. Tento vztah může být použit k rozdělení řešení rovnice $x^2 - Dy^2 = N$ na rovnocenné třídy. Dvě řešení x, y a r, s jsou ekvivalentní pouze a jen platí-li pro ně $(xr - Dys)/N$ a $(xs - yr)/N$ jsou celá čísla. Je-li $r = -1, s = 0$ vyhovují rovnici $r^2 - Ds^2 = 1$ pro nějaké D , $(-x, -y)$ je vždy ekvivalentní k (x, y) .

Může nám pomoci vidět řešení geometricky. Pokud $N > 0$, pak je rovnice $x^2 - Dy^2 = N$ hyperbola s x -ovou souřadnicí jako její osou a s y -ovou souřadnicí jako osou symetrie. Asymptoty tvoří přímky dané rovnicemi $x \pm y\sqrt{D} = 0$. Necht' t, u jsou nejmenší kladná řešení rovnice $x^2 - Dy^2 = 1$. Nakresleme graf $x^2 - Dy^2 = N$ na množině reálných čísel. Označme bod $(\sqrt{N}, 0)$, který leží na grafu a dále bod $(t\sqrt{N}, u\sqrt{N})$ také ležící na grafu. Pokračujme označováním bodů (x, y) a následně pak body $(xt + yuD, xu + yt)$.

Nyní pro každý bod, který byl vyznačen, vyznačme všechny body $(\pm x, \pm y)$, které ještě nejsou v grafu zaneseny. Vyznačené body rozdělí graf na dva intervaly. Udělejme interval $\left((\sqrt{N}, 0), (t\sqrt{N}, u\sqrt{N})\right]$ polozavřený a pak další každý polozavřený v koncovém bodě.

Pokud jsou celá řešení rovnice $x^2 - Dy^2 = N$ pak platí:

1. Žádná dvě řešení nejsou ze stejného polozavřeného intervalu.
2. Každý interval má právě jedno řešení v každé třídě.
3. Zařazení řešení do třídy je stejné v každém intervalu.

Namísto toho, že začneme s bodem $(\sqrt{N}, 0)$, můžeme začít s libovolným bodem (r, s)

a vyznačit body korespondující k $(r + s\sqrt{D}) \cdot (\pm 1) \cdot (t + u\sqrt{D})^n$. Tři pravidla uvedená nad stáále budou platit.

Situace bude pořád stejná i pro $N < 0$, vyjma toho, že graf bude mít y-ovou osu jako osu a x-ovou jako osu symetrie.

Pokud $x^2 - Dy^2 = -1$ má řešení, pak jakékoliv z těchto řešení může být použito k vytvoření vztahu mezi řešením rovnice $x^2 - Dy^2 = N$ a $-N$.

V rámci třídy je zde jedno řešení, kde x a y jsou nezáporná, ale menší než jakákoliv jiná nezáporná řešení. Toto řešení se nazývá minimální nezáporné řešení třídy. Je možné také najít jedno nebo dvě řešení, kde y je nezáporné a menší nebo rovno jiným nezáporným y nějakého řešení x , y v rámci třídy. Pokud jedno takové řešení najdeme, je nazýváno fundamentální řešení. Pokud taková řešení najdeme dvě, pak budou tato řešení ekvivalentní a jejich x-ové hodnoty budou opačné. V tomto případě řešení s kladnou x-ovou hodnotou je nazýváno fundamentální řešení pro třídu. Pro $N > 0$, fundamentální řešení leží na hyperbole na intervalu

$$(\sqrt{N}, 0) \text{ do } \left(\sqrt{N(r+1)/2}, \sqrt{N(r-1)/2D}\right)$$

a

$$(-\sqrt{N}, 0) \text{ do } \left(-\sqrt{N(r+1)/2}, \sqrt{N(r-1)/2D}\right).$$

V prvním intervalu mohou být koncové body zahrnuty zatímco pro ve druhém intervalu musí být vyloučeny.

Pro $N < 0$ jsou fundamentální řešení v intervalu

$$\left(-\sqrt{N(r+1)/2}, \sqrt{N(r-1)/2D}\right) \text{ do } \left(\sqrt{|N|(r-1)/2}, \sqrt{|N|(r+1)/2D}\right)$$

se středem v bodě $(0, \sqrt{-N/D})$. V tomto intervalu první bod je vyloučen a koncový bod zahrnut.

Když sestavujeme tabulku řešení, je vhodné udělat tabulku tak, aby obsahovala jedno řešení z každé třídy. Často tento výčet bude výčtem nejmenších nezáporných řešení nebo fundamentálních řešení. Máme-li dáno nějaké řešení ve třídě, je pak jednoduché najít fundamentální nebo minimální nezáporné řešení pro tuto třídu.

Obecně, máme-li nějaké řešení z třídy, všechna řešení mohou být nalezena pomocí řešení rovnice $x^2 - Dy^2 = 1$. Pokud r, s je částečné řešení rovnice $x^2 - Dy^2 = N$, x, y je nějaké jiné řešení stejné rovnice ve stejné třídě jako r, s a pokud t, u je nejmenší kladné řešení rovnice $x^2 - Dy^2 = 1$, pak pro libovolný výběr znaménka, ± 1 , a pro nějaké celé číslo n , $x + y\sqrt{D} = \pm(r + s\sqrt{D})(t + u\sqrt{D})^n$.

Jsou zde rekurzní vztahy mezi řešeními podobné těm, při řešení rovnice pro ± 1 . Například pokud $(x_1, y_1), (x_2, y_2)$ a (x_3, y_3) jsou tři řešení rovnice ve stejné třídě na spojitém intervalu a t, u je nejmenší řešení $x^2 - Dy^2 = 1$ pak $x_3 = 2tx_2 - x_1$ a $y_3 = 2ty_2 - y_1$.

Řešení rovnice $x_2 - Dy_2 = N$, $N^2 < D$

Když $1 < N^2 < D$, použijeme PQ algoritmus s $D = D$, $P_0 = 0$, $Q_0 = 1$. Budeme pokračovat v počítání tak dlouho, dokud nenalezneme první $\ell_e > 0$ s $G_{\ell_e-1}^2 - DB_{\ell_e-1}^2 = 1$ (např. $Q_{\ell_e} = 1$ a ℓ je sudé. Poznamenejme, že $\ell_e = \ell$ nebo 2ℓ . Pro $0 \leq i \leq \ell_e - 1$, pokud $G_i^2 - dB_i^2 = N/f^2$ pro $f > 0$, přidejme fG_i , fB_i k řešení rovnice. Pokud budeme postupovat dle tohoto návodu, dostaneme zástupce nejmenší kladné řešení z množiny všech řešení pro každou třídu. Všechna kladná řešení mohou být nalezena pomocí rozšířeného PQa algoritmu.

Řešení $x^2 - Dy^2 = N$ pomocí metody násilného hledání kořenů

Nechť t , u je nejmenší řešení $x^2 - Dy^2 = 1$. Pokud $N > 0$, nechť $L_1 = 0$ a $L_2 = \sqrt{N(t-1)/(2D)}$. Pokud $N < 0$, nechť $L_1 = \sqrt{(-N)/D}$ a $L_2 = \sqrt{N(t+1)/(2D)}$. Pro $L_1 \leq y \leq L_2$, pokud $N + Dy^2$ je čtverec, nechť $x = \sqrt{N + Dy^2}$. Jestliže (x, y) není ekvivalentní s $(-x, y)$, můžeme obě dvojice přidat k řešením rovnice. Pokud nejsou ekvivalentní, řešením je pouze (x, y) . Až dokončíme tuto metodu hledání řešení dostaneme fundamentální řešení.

Tato metoda funguje velmi dobře, pokud L_2 není příliš velké, což znamená, že

$$\sqrt{|N|(t \pm 1)/(2D)}$$

není příliš veliké. Musíme být schopni hledat mezi čísly L_1 a L_2 .

Řešení $x^2 - Dy^2 = N$ pomocí LMM (Lagrange-Matthews-Mollin) algoritmu

Pomocí tohoto algoritmu najdeme právě jednoho zástupce řešení rovnice $x^2 - Dy^2 = N$ pro $N \neq 0$, $D > 0$, D není čtverec.

Udělejme seznam $f > 0$ takových, že f^2 dělí N . Pro každé f ze seznamu, necht' $m = N/f^2$. Najdeme takové z , že $-|m|/2 < y < |m|/2$ a $z^2 \equiv D \pmod{|m|}$. Pro každé z provedme PQa algoritmus s $P_0 = z$, $Q_0 = |m|$, $D = D$. Pokračujeme do té doby, než pro nějaké $i \geq 1$ bude $Q_i = \pm 1$ nebo do té doby, než objevíme konec první periody posloupnosti a_i . Pokud nalezneme i pro něž $Q_i = \pm 1$ pak berme, že $r = G_{i-1}$, $s = B_{i-1}$. Pokud $r^2 - Ds^2 = m$ pak do množiny řešení přidejme $x = fr$, $y = fs$. Jinak $r^2 - Ds^2 = -m$. Pokud rovnice $t^2 - Du^2 = -1$ má řešení a necht' t , u jsou nejmenší kladná řešení, je $x = f(rt + sud)$, $y = f(ru + st)$ řešením rovnice $x^2 - Dy^2 = N$. Jinak postupujeme dále dle PQa algoritmu na další periodu k dalšímu $Q_i = \pm 1$, vezmeme za $r = G_{i-1}$, $s = B_{i-1}$ a $x = fr$, $y = fs$ jsou opět řešením dané rovnice. Poznamenejme, že největší společný dělitel $(r, s) = 1$ tedy generovaná řešení rovnice $x^2 - Dy^2 = m$ jsou primitivní.

Pokud projdeme všechna f a všechna z pro každé f množina řešení bude mít zástupce z každé třídy. Tyto řešení budou buď fundamentální nebo nejmenší kladná řešení ve třídě.

Lagrangeův systém redukce

Tato metoda může být využita při řešení rovnice $x^2 - Dy^2 = N$ když $N^2 > D$. Nejdůležitější poznámka je, že pokud $x \geq 0$, $y \geq 0$ je řešením $x^2 - Dy^2 = N$ s $N^2 > D$ pak jsou zde $0 \leq k \leq |N|/2$, X , Y tak, že $h = (k^2 - D)/N$ je celé číslo, X , Y je řešení $X^2 - DY^2 = h$ a $x = |(kX + DY)/h|$, $y = |(kY + X)/h|$ nebo $x = |(kX - DY)/h|$, $y = |(kY - X)/h|$.

Často je nutné aplikovat tuto metodu rekurzivně. To znamená, že začneme s rovnicí $x^2 - Dy^2 = N$ a pro každé $0 \leq k \leq |N|/2$ s $h = (k^2 - D)/N$ celé číslo a dostaneme rovnici $X^2 - DY^2 = h$. Pokud $h^2 > D$ můžeme použít redukci této poslední rovnice. Pokračujeme dále, dokud máme výsledky, pak dostaneme rovnici s $h^2 < D$ což se stane posléze. To je potom řešeno metodou popsanou v předchozím odstavci. Vezmeme jedno řešení z každé třídy. Projdeme pak vícekrát redukci a dostaneme řešení původní rovnice. K nalezení řešení původní rovnice v každé třídě, vyřešíme každou rovnici $x^2 - Dy^2 = N/f^2$ pro každé $f > 0$ tak, že N/f^2 je celé číslo. Pak dostaneme fx, fy jako řešení původní rovnice.

2.1.3.4 Pythagorova diofantovská rovnice $x^2 + y^2 = z^2$

Jednou z dalších speciálních rovnic je Pythagorova diofantovská rovnice tvaru

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

Omezíme se opět na to, že budeme hledat její kladné řešení. Geometrický význam těchto řešení je zřejmý: jsou to velikosti stran pravoúhlého trojúhelníku, jež se dají vyjádřit celými čísly.

Řešíme tedy v oboru přirozených čísel rovnici

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

Označme $t = (x, y, z)$, $x_1 = \frac{x}{t}$, $y_1 = \frac{y}{t}$, $z_1 = \frac{z}{t}$. Pak platí

$$t^2 x_1^2 + t^2 y_1^2 = t^2 z_1^2,$$

odkud po vydělení číslem $t^2 \neq 0$ vychází

$$x_1^2 + y_1^2 = z_1^2$$

a navíc $(x_1, y_1, z_1) = 1$. Nyní ukažme, že čísla jsou dokonce po dvou nesoudělná. Kdyby nějaké prvočíslo p dělilo dvě z čísel x_1, y_1, z_1 vyšlo by z rovnice $x_1^2 + y_1^2 = z_1^2$, že dělí i třetí,

což vzhledem k $(x_1, y_1, z_1) = 1$ není možné. Z čísel x_1, y_1 je tedy nejvýše jedno sudé.

Připusťme, že obě jsou lichá. Pak z kongruence

$$z_1^2 \equiv x_1^2 + y_1^2 \equiv 1 + 1 \pmod{8}$$

plyne, že z_1^2 je sudé číslo, které není dělitelné 4, což není možné. Je tedy z čísel x_1, y_1 právě jedno sudé. Protože v rovnici $x_1^2 + y_1^2 = z_1^2$ vystupují x_1 a y_1 symetricky, můžeme pro určitost předpokládat, že sudé je $x_1 = 2r, r \in \mathbb{N}$. Z $x_1^2 + y_1^2 = z_1^2$ pak plyne

$$4r^2 = z_1^2 - y_1^2$$

a tedy

$$r^2 = \frac{z_1 + y_1}{2} \cdot \frac{z_1 - y_1}{2}.$$

Označme $u = \frac{1}{2}(z_1 + y_1), v = \frac{1}{2}(z_1 - y_1)$. Pak $z_1 = u + v, y_1 = u - v$. Protože jsou y_1, z_1 přirozená nesoudělná a lichá čísla, jsou i u, v celá nesoudělná čísla. Z rovnice

$$r^2 = u \cdot v$$

pak plyne, že existují nesoudělná přirozená čísla a, b taková, že $u = a^2, v = b^2$, navíc vzhledem k $u > v$ platí $a > b$. Celkem tedy dostáváme

$$\begin{aligned} x &= tx_1 = 2tr = 2tab, \\ y &= ty_1 = t(u - v) = t(a^2 - b^2), \\ z &= tz_1 = t(u + v) = t(a^2 + b^2), \end{aligned}$$

což skutečně pro libovolné $t \in \mathbb{N}$ a libovolná nesoudělná $a, b \in \mathbb{N}$ taková, že $a > b$, vyhovuje dané rovnici. Zbývá řešení dostaneme záměnou x a y (nyní jsme předpokládali, že právě x_1 je sudé):

$$x = t(a^2 - b^2), y = 2tab, z = t(a^2 + b^2),$$

kde opět $t, a, b \in \mathbb{N}$ jsou libovolná taková, že $a > b, (a, b) = 1$.

2.1.3.5 Diofantovská rovnice tvaru $x^n + y^n = x^p y^q z$

Nechť $n \geq 2$, $p, q \geq 1$ jsou kladná čísla taková, že $p + q = n$. Náš záměr je získat všechna netriviální řešení dané rovnice, které jsou z oboru kladných celých čísel. Ve skutečnosti uvedená metoda řešení nám dovoluje získat řešení z oboru celých čísel. K nalezení řešení rovnice využijeme následující dvě pomocné věty. Jejich důkazy lze nalézt v literatuře.

Věta 9: Nechť $x, y > 0$ jsou celá čísla taková, že $D(x, y) = 1$. Pak $D(x + y, xy) = 1$.

Věta 10: Jestliže $a, b > 0$ jsou celá čísla a $D(a, b) = 1$, pak $D(a^n, b) = 1$ pro každé celé číslo $n > 0$.

Nyní označme $D(x, y) = d$ tj. $x = dX$, $y = dY$ kde $D(X, Y) = 1$

Z původní rovnice tedy dostaneme

$$X^n + Y^n = X^p Y^q z \quad (12)$$

použijeme-li Newtonovu binomickou větu, dostáváme

$$X^n + Y^n = (X + Y)^n - \left[\binom{n}{1} X^{n-1} Y + \dots + \binom{n}{n-1} X Y^{n-1} \right] \quad (13)$$

a z rovnice (12) pak

$$\frac{(X + Y)^n}{XY} = \binom{n}{1} X^{n-2} + \dots + \binom{n}{n-1} Y^{n-2} + X^{p-1} Y^{q-1} z \quad (14)$$

kde $p \geq 1$, $q \geq 1$, $n \geq 1$.

Dle dvou pomocných vět (9, 10), levá strana (14) obsahuje ireducibilní zlomek. Z toho plyne, že zlomek může být celé číslo pouze tehdy, když $XY = 1$. Proto tedy $X = Y = 1$, $z = 2$ z čehož plyne, že $x = y = d$, $z = 2$. Tímto tedy dostáváme nekonečný počet řešení dané rovnice, kde d je libovolné celé číslo.

2.2 Některé další metody řešení diofantovských rovnic

V následujících dvou odstavcích si ukážeme další dvě metody, které lze použít celkem velmi často, abychom dosáhli správného výsledku, při řešení diofantovských rovnic. Jedná se o metodu řešení z využitím odhadu nerovnosti a o metodu rozkladu diofantovské rovnice.

2.2.1 Řešení diofantovských rovnic s využitím odhadu nerovností

Metoda je založena na tom, že pro libovolná reálná čísla a, b existuje jen konečně mnoho celých čísel x tak, že $a < x < b$. Proto při řešení dané rovnice hledáme taková čísla a, b , aby nerovnosti $a < x < b$ pro některou neznámou x byly důsledkem této rovnice. Konečně mnoho celých čísel ležících mezi čísly a, b pak můžeme dosadit do rovnice za x a tím ji zjednodušit. Často je možné ukázat sporem, že množina hodnot neznámé x je konečná a omezená nerovnostmi $x \leq a$ (resp. $x \geq b$) je nepravdivé tvrzení. Ve druhém příkladě bude takovým nepravdivým tvrzením dvojice nerovností

$$c^n < d^n < (c+1)^n,$$

kde c, d jsou celá a n přirozené číslo.

Příklad 6. Řešte rovnici v oboru celých čísel $2^x = 1 + 3^y$

Řešení. Je-li $y < 0$, platí $1 < 1 + 3^y < 2$, odkud $0 < x < 1$, což je spor. Je tedy $y \geq 0$ a proto $2^x = 1 + 3^y \geq 2$, odtud $x \geq 1$. Ukážeme, že také platí $x \leq 2$. Kdyby totiž bylo $x \geq 3$, platilo by

$$1 + 3^y = 2^x \equiv 0 \pmod{8},$$

po úpravě bychom dostali

$$3^y \equiv -1 \pmod{8},$$

což však není možné, neboť pro sudá čísla y je $3^y \equiv 1 \pmod{8}$ a pro lichá čísla y platí $3^y \equiv 3 \pmod{8}$. Zbývá tedy vyřešit případ $1 \leq x \leq 2$. Pro $x=1$ dostáváme

$$3^y = 2^1 - 1 = 1,$$

a tedy $y=0$. Z $x=2$ plyne

$$3^y = 2^2 - 1 = 3,$$

takže $y=1$. Rovnice má tedy dvě řešení: $x=1, y=0$ a $x=2, y=1$.

Příklad 7. Řešte diofantovskou rovnici $(x+2)^4 - x^4 = y^3$ v oboru celých čísel.

Řešení. Nejprve rovnici upravíme

$$y^3 = 8x^3 + 24x^2 + 32x + 16 = 8(x^3 + 3x^2 + 4x + 2),$$

odtud plyne, že y je sudé. Položme tedy $y=2z, z \in \mathbb{Z}$. Pak platí, že

$$z^3 = x^3 + 3x^2 + 4x + 2.$$

Je-li $x \geq 0$, platí

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 < x^3 + 3x^2 + 4x + 2 = z^3 < x^3 + 6x^2 + 12x + 8 = (x+2)^3,$$

odkud $x+1 < z < x+2$, což není možné. Daná rovnice tedy nemá řešení $x, y \in \mathbb{Z}$ takové, že $x \geq 0$. Předpokládejme, že má nějaké řešení $x_1, y_1 \in \mathbb{Z}$ takové, že $x_1 \leq -2$. Pak platí

$$(x_1+2)^4 - x_1^4 = y_1^3$$

a dosadíme-li $x_2 = -x_1 - 2, y_2 = -y_1$, dostaneme

$$x_2^4 - (x_2+2)^4 = -y_2^3,$$

a proto x_2, y_2 je také řešení dané rovnice. Ovšem $x_2 = -x_1 - 2 \geq 0$ a z předchozích úvah plyne, že tato situace nastat nemůže. Dohromady tedy $-2 < x < 0$, tj. $x = -1$. Pro $x = -1$ vychází z původní rovnice $y = 0$; dvojice $x = -1, y = 0$ je jediným řešením úlohy.

Při řešení diofantovských rovnic jsou někdy užitečné i některé složitější postupy a nerovnosti (viz následující příklad).

Příklad 8. Řešte rovnici $\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{u^2} = 1$ v oboru přirozených čísel.

Řešení. Jelikož jsou v dané rovnici neznámé x, y, z, u zastoupeny symetricky, můžeme předpokládat, že $x \leq y \leq z \leq u$. Je jasné, že $x > 1$. Kdyby $u \geq 3$, platilo by

$$\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{u^2} \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{9} < 1,$$

a proto $u \leq 2$, a tedy platí $2 \leq x \leq y \leq z \leq u \leq 2$. Dosazením do rovnice lze ověřit, že $x = y = z = u = 2$ je její jediné řešení.

2.2.2 Řešení diofantovských rovnic metodou rozkladu

Další často užívanou metodou je využití rozkladu typu součin.

$$B = A_1 \cdot A_2 \cdot \dots \cdot A_n,$$

kde $A_1 \cdot A_2 \cdot \dots \cdot A_n$ jsou výrazy obsahující neznámé, které pro celočíselné hodnoty neznámých nabývají celočíselných hodnot, a B je číslo popř. výraz, jehož rozklad na prvočísla známe. Pak totiž existuje pouze konečně mnoho rozkladů čísla B na n celočíselných činitelů $a_1, \dots, a_n$. Vyšetříme-li pak pro každý z těchto rozkladů soustavu rovnic

$$A_1 = a_1, A_2 = a_2, \dots, A_n = a_n,$$

získáme všechna řešení rovnice $A_1 \cdot A_2 \cdot \dots \cdot A_n = B$.

Příklad 9. Řešte rovnici $x^4 + 2x^7y - x^{14} - y^2 = 7$ v oboru celých čísel.

Řešení. Nejprve upravme levou stranu rovnice

$$x^4 + 2x^7y - x^{14} - y^2 = x^4 - (x^7 - y)^2 = (x^2 - x^7 + y)(x^2 + x^7 - y)$$

Uvažujme ještě, že číslo sedm lze rozložit čtyřmi způsoby na součin dvou celých čísel a to následujícím způsobem: $7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)$. Proto budeme řešit čtyři soustavy rovnic:

a) $x^2 - x^7 + y = 1$, $x^2 + x^7 - y = 7$ Sečtením obou rovnic dostaneme $x^2 = 4$, odkud

$x = 2$, $y = 125$, nebo $x = -2$, $y = -131$.

b) $x^2 - x^7 + y = 7$, $x^2 + x^7 - y = 1$. V tomto případě $x^2 = 4$, a tedy $x = 2$, $y = 131$ nebo

$x = -2$, $y = -125$.

c) $x^2 - x^7 + y = -7$, $x^2 + x^7 - y = -1$. Což je spor $x^2 = -4$.

d) $x^2 - x^7 + y = -1$, $x^2 + x^7 - y = -7$. Opět dojdeme při výpočtu ke sporu $x^2 = -4$.

Rovnice má tedy čtyři řešení: $(x, y) \in \{(-2; -131), (-2; -125), (2; 125), (2; 131)\}$.

2.3 Řešitelnost diofantovských rovnic

Zabývejme se nyní řešitelností diofantovských rovnic. Uvedeme některé další metody stanovení počtu kořenů diofantovské rovnice.

2.3.1 Využití kongruence při důkazu neexistence řešení

Při důkazu, že řešení neexistuje, je možné využít kongruencí. Má-li totiž řešení diofantovská rovnice $L = P$, kde L, P jsou výrazy obsahující neznámé, nabývající celočíselných hodnot pro libovolné celočíselné hodnoty neznámých, musí mít řešení i kongruence $L \equiv P \pmod{m}$ pro libovolné $m \in \mathbb{N}$, protože řešení této kongruence je například zmíněné řešení rovnice. Odtud plyne, že pokud nalezneme nějaké přirozené číslo m tak, že kongruence $L \equiv P \pmod{m}$ nemá řešení, nemůže mít řešení ani původní diofantovská rovnice $L = P$. Je nutné si však uvědomit, že obrácení této úvahy obecně neplatí. Pokud má kongruence $L \equiv P \pmod{m}$ pro každé přirozené číslo m řešení, neznamená to ještě, že má řešení též diofantovská rovnice $L = P$. Uvidíme ve druhém příkladě.

Příklad 10. Řešte rovnici $1! + 2! + 3! + \dots + x! = y^2$ v oboru celých čísel.

Řešení. Přímým výpočtem se přesvědčíme, že pro $x < 5$ vyhovují rovnici pouze $x = y = 1, x = y = 3$. Ukážeme, že pro $x \geq 5$ rovnice řešení nemá. Protože pro libovolné $n \geq 5$ je $n!$ dělitelné pěti, platí

$$1! + 2! + 3! + \dots + x! \equiv 1! + 2! + 3! + 4! = 33 \equiv 3 \pmod{5}.$$

Ovšem druhá mocnina přirozeného čísla je podle modulu 5 kongruentní s 0 nebo 1 nebo 4. Kongruence $1!+2!+3!+\dots+x!\equiv y^2 \pmod{5}$ pro $x \geq 5$ tedy nemá řešení, a proto nemá pro $x \geq 5$ řešení ani daná rovnice.

Příklad 11. Dokažte, že kongruence $6x^2+5x+1 \equiv 0 \pmod{m}$ má řešení pro každé přirozené číslo m , a přitom rovnice diofantovská $6x^2+5x+1=0$ řešení nemá.

Řešení. Platí $6x^2+5x+1=(3x+1)(2x+1)$, a tak rovnice $6x^2+5x+1=0$ nemá celočíselné řešení. Necht' m je libovolné přirozené číslo a platí $m=2^k$, kde $n \in \mathbb{N}_0$ a k je liché číslo. Protože $(3, 2^n) = (2, k) = 1$, mají obě kongruence soustavy

$$3x \equiv -1 \pmod{2^n}$$

$$2x \equiv -1 \pmod{k}$$

řešení a protože $(2^n, k) = 1$ má řešení i celá soustava. Pro libovolné x vyhovující této soustavě je pak $3x+1$ dělitelné číslem 2^n a $2x+1$ číslem k a proto součin $(3x+1)(2x+1)$ je dělitelný číslem $2^n \cdot k = m$. Je tedy x řešením kongruence

$$6x^2+5x+1 \equiv 0 \pmod{m}.$$

2.3.2 Metoda nekonečného sestupu neboli zmenšování

Zmenšování ad absurdum je metoda důkazu neexistence řešení diofantovské rovnice. Při důkazu touto metodou libovolné řešení dané diofantovské rovnice charakterizujeme nějakým přirozeným číslem (např. největším společným dělitelem hodnot některých neznámých nebo druhou mocninou hodnoty některé neznámé) a ukážeme, že existuje-li řešení charakterizované přirozeným číslem d , musí existovat jiné řešení, charakterizované přirozeným číslem $d' < d$. Pak totiž žádné takové řešení existovat nemůže, o čemž se snadno přesvědčíme sporem: kdyby existovalo, mohli bychom zvolit to řešení, které je ze všech řešení charakterizováno co nejmenším přirozeným číslem d . Pak by ovšem muselo existovat i jiné řešení, charakterizované přirozeným číslem $d' < d$, což však by byl spor s volbou d .

Příklad 12. Řešte rovnici $x^2 + y^2 = 4^z$ v oboru přirozených čísel.

Řešení. Předpokládejme nejprve, že x, y, z je řešením dané rovnice. Pak jistě platí $z \neq 1$, protože je-li $x = y = 1$, platí $x^2 + y^2 = 2 < 4$, a je-li alespoň jedno z čísel x, y větší než jedna, je $x^2 + y^2 > 4$. Je tedy $z > 1$ a platí $x^2 + y^2 = 4^z \equiv 0 \pmod{8}$. Protože druhá mocnina lichého čísla je kongruentní s 1 podle modulu 8 a druhá mocnina sudého čísla je kongruentní s 0 nebo 4 podle modulu 8, plyne z této kongruence, že x, y jsou sudá, a tedy $x = 2x_1, y = 2y_1$ pro vhodná $x_1, y_1 \in \mathbb{N}$. Pak ovšem

$$x_1^2 + y_1^2 = \frac{x^2}{4} + \frac{y^2}{4} = 4^{z-1},$$

a tedy, označíme-li $z_1 = z - 1 \in \mathbb{N}$, čísla x_1, y_1, z_1 splňují danou rovnici, přičemž $z_1 < z$. Zjistili jsme, že ke každé vyhovující trojici přirozených čísel (x, y, z) lze nalézt trojici dalších přirozených kořenů $\left(\frac{x}{2}, \frac{y}{2}, z-1\right)$. To však není možné.

2.3.3 Početnost množiny řešení

V některých případech řešení diofantovských rovnic dojdeme k závěru, že neumíme najít všechna řešení. Ale může se nám podařit rozhodnout, zda řešení je konečně nebo nekonečně mnoho. Konečnost je například zaručena, že hodnoty neznámých jsou v absolutní hodnotě menší než nějaké číslo. Pokud toto číslo nalezneme a je rozumně malé, můžeme pak najít všechna řešení pomocí metody, která využívá nerovností (kap. 2.2.1). To, že daná diofantovská rovnice má řešení nekonečně mnoho, můžeme dokázat třeba tak, že nalezneme pro každou neznámou nějaký výraz s parametrem, a to takový, že po dosazení do rovnice dostaneme rovnost, přitom pro nekonečně mnoho hodnot parametru dostaneme navzájem různé hodnoty neznámých (je to jakási zkouška nekonečně mnoha řešení). Nebo můžeme nalézt jedno řešení rovnice a udat předpis, jak z libovolného řešení spočítat jiné. Máme-li zaručeno, že při další a další aplikaci tohoto předpisu dostáváme stále nová řešení, opět tím dokážeme, že množina všech řešení je nekonečná.

Příklad 13. $(x-1)^2 + (x+1)^2 = y^2 + 1$ Dokažte, že tato rovnice má nekonečně mnoho řešení.

Řešení. Rovnici lze upravit do následujícího tvaru

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

Zkusíme najít nějaká řešení této rovnice. Po několika pokusech lze objevit, že pro $x = 2, y = 3$ vyhovuje dané rovnici. Představme si nyní, že máme k dispozici libovolné řešení $x, y \in \mathbb{Z}$ a pokusme se získat další. Platí tedy

$$(y + \sqrt{2}x)(y - \sqrt{2}x) = 1. \quad (15)$$

Dosazením nalezených hodnot $x = 2, y = 3$ získáme rovnost

$$(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1, \quad (16)$$

vynásobíme-li rovnici (15) rovnicí (16) dostaneme

$$\left[(y + \sqrt{2}x)(3 + 2\sqrt{2}) \right] \cdot \left[(y - \sqrt{2}x)(3 - 2\sqrt{2}) \right] = 1.$$

Výrazy v obou hranatých závorkách upravíme. Platí tedy

$$\begin{aligned} (y + \sqrt{2}x)(3 + 2\sqrt{2}) &= 3y + 3\sqrt{2}x + 2\sqrt{2}y + 4x = (4x + 3y) + (3x + 2y)\sqrt{2}, \\ (y - \sqrt{2}x)(3 - 2\sqrt{2}) &= 3y - 3\sqrt{2}x - 2\sqrt{2}y + 4x = (4x + 3y) - (3x + 2y)\sqrt{2}. \end{aligned}$$

Položíme $u = 4x + 3y, v = 3x + 2y$. Platí tedy

$$(u + \sqrt{2}v)(u - \sqrt{2}v) = 1,$$

odkud

$$u^2 - 2v^2 = 1,$$

a tedy $u, v \in \mathbb{Z}$ je další řešení dané rovnice. Položíme-li $x_1 = 2, y_1 = 3$ a

$$x_{n+1} = 3x_n + 2y_n, y_{n+1} = 4x_n + 3y_n$$

pro libovolné $n \in \mathbb{N}$, dostáváme pro každé $n \in \mathbb{N}$ řešení x_n, y_n dané rovnice. A protože platí $0 < x_1 < x_2 < \dots, 0 < y_1 < y_2 < \dots$, dostáváme pro různé indexy n různá řešení x_n, y_n .

Daná rovnice má tedy nekonečně mnoho řešení.

3 Závěr

Pokusili jsme se vytvořit stručný přehled některých typů diofantovských rovnic a ukázat několik metod, jak lze tyto rovnice řešit. Některé jsou poměrně obtížné a jejich řešení vyžaduje značné úsilí. V některých složitějších případech můžeme alespoň rozhodnout zda-li má rovnice vůbec nějaké řešení a pokud ano, tak zda jich je konečně či nekonečně mnoho. To nám pomáhá rovnice alespoň nějak popsat či zprůhlednit.

V práci jsme též uvedli příklady řešení konkrétních úloh. K jejich řešení jsme používali námi popsané metody. Naše publikace může pomoci studentům při studiu diofantovských úloh a jejich metod řešení a být i přínosem k rozšíření vědomostí či příručkou k přípravě hodin pro učitele matematiky.

.

Literatura:

- [1] Calda, E.: *Rovnice ve škole neřešené*, Prométheus, Praha 1995.
- [2] Herman, J., Kučera, R., Šimša, J.: *Metody řešení matematických úloh I*, skriptum, Masarykova univerzita 2004
- [3] Hruša, K., Dlouhý, Z., Rohlíček, J.: *Úvod do studia matematiky*, SNP, Praha 1977
- [4] <http://www.math.rutgers.edu>
- [5] <http://centaur.maths.qmul.ac.uk>
- [6] Kopka, J.: *Kapitoly o celých číslech*, Univerzita J. E. Purkyně, Ústí nad Labem 2004.
- [7] NAVAJO – otevřená encyklopedie
- [8] Sándor, J.: *Geometric Theorems, Diophantine Equations and Arithmetic functions*, American Research Press Rehoboth, 2002
- [9] Znám, Š.: *Teória čísel*, Alfa, Nitra 1986.
- [10] <http://hometown.aol.com/jpr2718/pell.pdf>