Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

DIOFANTOVSKÉ ROVNICE V ÚLOHÁCH MO A V HISTORII MATEMATIKY

DIPLOMOVÁ PRÁCE

Bc. Ivana Petrová

Učitelství pro 2. stupeň ZŠ, obor M-Bi

léta studia (2010 - 2012)

Vedoucí práce: *doc. RNDr. Jaroslav Hora, CSc.*

Plzeň, 16. červen 2012

Prohlašuji, že jsem diplomovou práci vypracovala samostatně
s použitím uvedené literatury a zdrojů informací.

Plzeň, 16. červen 2012

……………………………………………
vlastnoruční podpis

Chtěla bych velmi poděkovat za pomoc a odbornou práci při vypracování vedoucímu mé diplomové práce, doc. RNDr. Jaroslavu Horovi, CSc.

OBSAH

1 ÚVOD

Tato diplomová práce se zabývá diofantovskými rovnicemi. Nepojednává o nich však obecně. Podrobněji se věnuje některým významným typům diofantovských rovnic a odhaluje i způsob jejich řešení pomocí počítačového programu Mathematica. Hlavním cílem práce je rozšířit soubor řešených rovnic o některé historicky významné rovnice a seznámit čtenáře s postupy jejich řešení.

Na úvod je zde nejprve uvedeno několik příkladů z matematické olympiády, ve kterých se počítá s diofantovskými rovnicemi. Další kapitola je nejobsáhlejší a je věnována historicky významným diofantovským rovnicím. Je zde představena Pellova rovnice, zobecněná Pellova rovnice a pythagorejská rovnice. Popisuje se zde i postup řešení, což je asi nejdůležitější částí kapitoly. Kapitola o desátém Hilbertově problému ukazuje na jeho souvislost s diofantovskými rovnicemi. Jeho podstata je ve snaze nalézt algoritmus, který by určil řešitelnost těchto rovnic. Poslední kapitola této práce závěrem ukazuje řešitelnost zmíněných rovnic v programu Mathematica.

2 DIOFANTOVSKÉ ROVNICE V ÚLOHÁCH MO

Diofantovskou rovnicí nazýváme neurčitou polynomiální rovnici, která dovoluje proměnným, aby nabývaly pouze hodnot z oboru celých čísel. Diofantovské problémy mají méně rovnic než proměnných a zahrnují nalezení celých čísel, která jsou řešením pro všechny rovnice dané soustavy rovnic. V této práci se postupně zaměříme na některé významné diofantovské rovnice. Na úvod si však uvedeme několik příkladů z matematické olympiády.

Sbírka [5] obsahuje i určitý soubor úloh na diofantovské rovnice. Protože jde o soubor příkladů k samotnému studiu, nacházíme v ní i jednodušší příklady. Jeden z nich je tento:

<u>Příklad 1:</u> Student obdržel soubor dvaceti úloh. Za každou správně rozřešenou dostal 8 bodů, za špatně rozřešenou se strhlo 5 bodů, za úlohu, kterou vůbec neřešil, bylo 0 bodů. Student dostal 13 bodů. Kolik úloh se pokusil řešit?

<u>Řešení:</u> Nechť x je počet správně vyřešených příkladů a y počet nesprávně řešených úloh. Platí

$$8x - 5y = 13. \qquad (1)$$

To je ovšem lineární diofantovská rovnice se dvěma neznámými a můžeme použít obecnou teorii. Není těžké uhodnout jedno řešení rovnice (1), je jím $x_0 = 1, y_0 = -1$. Obecné řešení rovnice (1) je pak $x = 1 + 5t,\ y = -1 + 8t,\ t \in Z$. Pro počet všech úspěšně či neúspěšně řešených úloh pak platí $x + y = 13t,\ t \in Z$ a samozřejmě je $x + y \leq 20$. Odtud plyne $t = 1, x + y = 13$ a snadno dopočítáme, že $x = 6,\ y = 7$.

Student tedy vyřešil 6 úloh správně a 7 špatně.

Vzhledem k tomu, že jde o sbírku úloh určenou pro talentované studenty, jsou vedeni k tomu, aby leccos vymysleli sami. Kdybychom k oběma stranám rovnice (1) přičetli $13y$, mohli bychom psát

$$8(x + y) = 13(1 + y)$$

a teď vidíme, že číslo 13 musí dělit $x+y$. Opět ovšem je $x+y \leq 20$ a my vidíme, že šikovný student se v daném případě obejde i bez naučené teorie.

V ruském časopise Kvant se často vyskytují mnohem náročnější úlohy. Mnohdy jde sice o řešení nějaké diofantovské rovnice, ale ještě je nutné znát něco navíc. V následujícím případě se od studentů, zřejmě špičkových řešitelů úloh matematické olympiády, vyžaduje, aby znali méně obvyklou identitu

$$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca). \qquad (2)$$

Poznamenejme, že od běžných studentů našich škol se vyžaduje znalost rozkladu dvojčlenu a^2-b^2, úspěšný řešitel MO musí umět více.

<u>Příklad 2</u>: (Kvant, roč. 2011, číslo 5 – 6.): V množině celých čísel řešte rovnici

$$x^3+y^3+6xy=8.$$

<u>Řešení:</u> Danou rovnici přepíšeme ve tvaru

$$x^3+y^3+(-2)^3-3\,.\,(-2)\,.\,x.\,y=0.$$

Využijeme identitu (2) a položíme v ní $a=x, b=y, c=-2$. Ze vztahu (2) dostaneme dva možné případy:

1) $a+b+c=0$, potom při našem označení $x+y=2$;

2) $a^2+b^2+c^2-ab-bc-ca=0 \Leftrightarrow 2a^2+2b^2+2c^2-2ab-2bc-2ca= =0 \Leftrightarrow (a-b)^2+(b-c)^2+(c-a)^2=0 \Leftrightarrow a=b=c$, tj. v tomto případě $x=y=-2$. Je tedy $P=\{[-2,-2],[x,2-x],x\in Z\}$.

<u>Příklad 3:</u> Řešte rovnici $x^3-y^3= xy+61$ v přirozených číslech. (3)

<u>Řešení:</u> Jestliže jsou x,y přirozená čísla, je výraz vpravo kladný, vlevo tedy též a proto platí $x>y$. Můžeme tedy psát $x=y+d$, kde d je zatím neurčené přirozené číslo. Po dosazení do (3) a roznásobení dostaneme

$$(3d-1)y^2+(3d^2-d)y+d^3=61. \qquad (4)$$

Ale všechny výrazy vlevo jsou kladné, takže jistě je $d^3 < 61$ a $d < 4$. V úvahu tudíž připadají možnosti $d = 1, 2, 3$.

I. Dosadíme-li do (4) hodnotu $d = 1$, řešíme rovnici $2y^2 + 2y = 60$, tj. $y^2 + y = 30$ a dostáváme $y = 5$, což je jediné přirozené číslo vyhovující dané rovnici. Nahlížíme, že uspořádaná dvojice $[6, 5]$ je řešením původní rovnice (3).

II. Dosadíme-li do (4) hodnotu $d = 2$, řešíme rovnici $5y^2 + 10y + 8 = 61$, která nemá celočíselné kořeny.

III. Stejný závěr učiníme i pro $d = 3$. Shrňme: rovnice (3) má v $N \times N$ jediné řešení, a to dvojici $[6, 5]$.

Několik ukázek již postačuje k závěru, že diofantovské rovnice v úlohách matematické olympiády mohou představovat značně náročné příklady. Někdy se od zadavatelů vyžaduje prokázání dodatečných algebraických znalostí, jako jsou vzorce pro rozklad polynomů či prokázání schopnosti takový rozklad objevit, jindy se využívají fakta o dělitelnosti atd. I nalezený obor pravdivosti může být velice různorodý, případně se můžeme dobrat i závěru, že zadaná rovnice řešení nemá.

3 HISTORICKY VÝZNAMNÉ DIOFANTOVSKÉ ROVNICE

3.1 PELLOVA ROVNICE

Tato rovnice je jedním z typů diofantovských rovnic a je zapsána ve tvaru

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

kde A je přirozené číslo, které není druhou mocninou žádného přirozeného čísla. Řešení některých speciálních typů této rovnice bylo známo už daleko dříve. Víme totiž, že se jí zabýval už v 7. století indický matematik Brahmagupta. Také rovnice ve tvaru $x^2 - 2y^2 = 1$ se vyskytovala již ve 4. století před n. l. u některých řeckých a indických matematiků. Avšak první, kdo znal obecnou metodu řešení této rovnice, byl P. Fermat (1601 – 1665).

3.1.1 O ŘEŠENÍ PELLOVY ROVNICE

V této kapitole si uvedeme některé základní věty a pojmy důležité pro řešení Pellovy rovnice. Hlavním cílem této kapitoly je seznámit čtenáře s postupem řešení této rovnice.

Při řešení budeme pracovat s řetězovými zlomky, proto si tento pojem definujeme a zvolíme vhodný zápis.

<u>Definice 1:</u> *Konečným řetězovým zlomkem* rozumíme výraz

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}},$$

kde a_0 je celé číslo a $a_1, a_2, \dots, a_k$ jsou přirozená čísla a $a_k > 1$. Podobně *nekonečným řetězovým zlomkem* rozumíme výraz

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

kde a_0 je celé číslo a $a_1,\ a_2, \dots$ jsou přirozená čísla.

Protože budeme s těmito pojmy při výpočtu pracovat, zvolíme si pro ně vhodný zápis. První zlomek budeme zapisovat ve tvaru $[a_0; a_1, a_2, \dots, a_k]$ a druhý zlomek zapíšeme ve tvaru $[a_0; a_1, a_2, \dots]$.

V dalším textu v případě konečného řetězového zlomku bude n značit celé nezáporné číslo, $n \leq k$. V případě nekonečného řetězového zlomku bude n značit libovolné nezáporné celé číslo. Číslo $A_n = [a_0, a_1, a_2, \dots, a_n]$ se nazývá n-tým sblíženým zlomkem řetězového zlomku.

Definice 2: Definujeme-li posloupnosti P_n, Q_n celých čísel vztahy

$$P_{-1} = 1, P_0 = a_0, P_n = a_n P_{n-1} + P_{n-2}, n \geq 1,$$

$$Q_{-1} = 0, Q_0 = 1, Q_n = a_n Q_{n-1} + Q_{n-2}, n \geq 1,$$

pak je možné dokázat, že $A_n = P_n/Q_n$, $n = 0, 1, \dots$.

Když počítáme sblížené zlomky, je vhodné zapisovat vypočtené hodnoty do tabulky.

	$\boldsymbol{a_0}$	$\boldsymbol{a_1}$	$\boldsymbol{a_2}$	**…**
$\boldsymbol{P_{-1}}$	P_0	P_1	P_2	…
$\boldsymbol{Q_{-1}}$	Q_0	Q_1	Q_2	…

Tabulka 1

Definice 3: Nekonečný řetězový zlomek se nazývá *periodický*, jestliže jej lze napsat ve tvaru $[a_0; a_1, a_2, \dots, a_s, a_{s+1}, \dots, a_{s+k-1}, a_{s+1}, \dots, a_{s+k-1}, a_{s+1}, \dots]$, kde k je přirozené číslo a s je celé nezáporné číslo. Nejmenší přirozené číslo k, pro které lze nekonečný řetězový zlomek napsat v tomto tvaru, se nazývá jeho *periodou.*

Nyní si ukažme, jak lze každému reálnému číslu α přiřadit řetězový zlomek. (Symbolem $[\alpha]$ je označena celá část čísla α, tj. největší celé číslo menší nebo rovné α). Položme $a_0 = [\alpha]$ a zapišme α ve tvaru $\alpha = a_0 + \frac{1}{\alpha_1}$. Dále položme $a_1 = [\alpha_1]$ a zapišme $\alpha_1 = a_1 + \frac{1}{\alpha_2}$. Dále postupujeme stejným způsobem a získáme postupně $a_2 = [\alpha_2]$, $\alpha_2 = a_2 + \frac{1}{\alpha_3}$, atd. Při takovémto postupu dostaneme k danému reálnému číslu α nějaký řetězový zlomek (konečný či nekonečný). Dá se dokázat, že je-li A přirozené číslo, které není druhou mocninou žádného přirozeného čísla, pak řetězový zlomek příslušný číslu $\sqrt{A}$ je nekonečný periodický řetězový zlomek ve tvaru

$$[a_0; a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, \dots, a_{k-1}, 2a_0, \dots].$$

Už víme, že Pellova rovnice má tvar $x^2 - Ay^2 = 1$, kde A je přirozené číslo, které není druhou mocninou žádného přirozeného čísla. Pro řešení této rovnice (tj. dvojice $[x, y]$ celých čísel) budeme využívat následující zápis:

$$x + y\sqrt{A}.$$

Tento zápis je praktický pro naše další počítání, jeho vhodnost uvidíme později. Řešení nazveme kladným, je-li $x > 0, y > 0$. Při hledání řešení Pellovy rovnice se stačí omezit na hledání kladných řešení.

Mějme dvě kladná řešení rovnice:

$$\alpha = x + y\sqrt{A},$$

$$\beta = z + u\sqrt{A}.$$

Platí, že α je menší než β (tj. $\alpha \prec \beta$), jestliže $x < z$ a $y < u$. Lze dokázat, že pro každá dvě různá kladná řešení rovnice platí buď $\alpha \prec \beta$ nebo $\beta \prec \alpha$.

Už jsme si uvedli důležité pojmy a definice potřebné pro výpočet řešení Pellovy rovnice. K výpočtu však budeme také potřebovat následující tři základní věty:

<u>Věta 1:</u> Označme $j = \bar{x} + \bar{y}\sqrt{A}$ nejmenší kladné řešení Pellovy rovnice. Pak $j^n, n = 1,2, \dots$ jsou právě všechna kladná řešení této rovnice.

Věta 2: Buď $j = \bar{x} + \bar{y}\sqrt{A}$ nejmenší kladné řešení Pellovy rovnice. Pak

$$j^{n+2} = 2\bar{x}j^{n+1} - j^n$$

pro všechna celá nezáporná čísla n.

Věta 3: Buď $[a_0; a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, \dots]$ nekonečný periodický řetězový zlomek příslušný číslu $\sqrt{A}$. Pak $P_{kn-1} + Q_{kn-1}\sqrt{A}$, kde n je přirozené číslo takové, že kn je sudé, jsou právě všechna kladná řešení Pellovy rovnice. Speciálně pro k sudé je $P_{k-1} + Q_{k-1}\sqrt{A}$ nejmenší kladné řešení této rovnice a pro k liché je $P_{2k-1} + Q_{2k-1}\sqrt{A}$ nejmenší kladné řešení této rovnice.

Při samotném řešení rovnice budeme postupovat takto:

1) nalezneme řetězový zlomek příslušný číslu $\sqrt{A}$,
2) podle věty 3 nalezneme nejmenší kladné řešení $j = \bar{x} + \bar{y}\sqrt{A}$ rovnice,
3) najdeme mocniny j^n pomocí věty 2 a jednotlivé mocniny j^n budeme zapisovat do tabulky, kde $x_n + y_n\sqrt{A} = j^n$.

x_0	x_1	x_2	…
y_0	y_1	y_2	…

Tabulka 2

Nyní už máme znalosti potřebné pro řešení Pellovy rovnice. Uvedeme tedy již konkrétní příklad, ve kterém bude vše postupně popsáno pro lepší pochopení a orientaci čtenáře.

Názorný příklad: Najděme prvních pět kladných řešení Pellovy rovnice

$$x^2 - 5y^2 = 1.$$

Řešení:

1) Nejprve nalezneme řetězový zlomek příslušný číslu $\sqrt{5}$.

$\boldsymbol{a_0 = 2}$ $\quad$ $\sqrt{5} = 2 + \frac{1}{\alpha_1}$

$$\alpha_1 = \frac{1}{\sqrt{5}-2} = \frac{1}{\sqrt{5}-2} \cdot \frac{\sqrt{5}+2}{\sqrt{5}+2} = \frac{\sqrt{5}+2}{5-4} = \sqrt{5} + 2$$

$$\underline{\alpha_1 = \sqrt{5} + 2}$$

$\boldsymbol{a_1 = 4}$ $\quad$ $\sqrt{5} + 2 = 4 + \frac{1}{\alpha_2}$

$$\sqrt{5} - 2 = \frac{1}{\alpha_2}$$

$$\alpha_2 = \frac{1}{\sqrt{5}-2} = \frac{1}{\sqrt{5}-2} \cdot \frac{\sqrt{5}+2}{\sqrt{5}+2} = \frac{\sqrt{5}+2}{5-4} = \sqrt{5} + 2$$

$$\underline{\alpha_2 = \sqrt{5} + 2}$$

$\boldsymbol{a_2 = 4}$ $\quad$ Vidíme, že by byl další výpočet stejný.

→ Nekonečný periodický zlomek příslušný číslu $\sqrt{5}$ je $[\mathbf{2}; \mathbf{4}, \mathbf{4}, \dots]$, perioda $\boldsymbol{k = 1}$.

2) Nyní nalezneme nejmenší kladné řešení. Použijeme větu 3. Pro přehlednost si všechny potřebné hodnoty budeme zapisovat do tabulky. V následující tabulce jsou zapsány hodnoty, které už víme.

$\boldsymbol{n}$	**-1**	**0**	**1**	**2**	**3**	**4**
$\boldsymbol{a_n}$		2	4	4	4	…
$\boldsymbol{P_n}$	1	2				…
$\boldsymbol{Q_n}$	0	1				…

Tabulka 3

$P_{-1} = 1 \qquad P_0 = a_0$

$Q_{-1} = 0 \qquad Q_0 = 1$

Dále potřebujeme vypočítat ostatní chybějící hodnoty. Použijeme dříve uvedené vzorce:

$$P_n = a_n P_{n-1} + P_{n-2}, n \geq 1,$$

$$Q_n = a_n Q_{n-1} + Q_{n-2}, n \geq 1.$$

Získáme:

$P_1 = a_1 P_0 + P_{-1} = 4 . 2 + 1 = \underline{9}$

$Q_1 = a_1 Q_0 + Q_{-1} = 4 . 1 + 0 = \underline{4}$

$P_2 = a_2 P_1 + P_0 = 4 . 9 + 2 = \underline{38}$

$Q_2 = a_2 Q_1 + Q_0 = 4 . 4 + 1 = \underline{17}$

$P_3 = a_3 P_2 + P_1 = 4 . 38 + 9 = \underline{161}$

$Q_3 = a_3 Q_2 + Q_1 = 4 . 17 + 4 = \underline{72}$

Tyto hodnoty již můžeme zapsat do připravené tabulky.

$\boldsymbol{n}$	**-1**	**0**	**1**	**2**	**3**	**4**
$\boldsymbol{a_n}$		2	4	4	4	...
$\boldsymbol{P_n}$	1	2	9	38	161	...
$\boldsymbol{Q_n}$	0	1	4	17	72	...

Tabulka 4

Nyní přejdeme k samotnému výpočtu nejmenšího kladného řešení rovnice, které má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Využijeme k tomu větu 3. Víme, že perioda nekonečného periodického řetězového zlomku je 1, tj. $k = 1$. Číslo k je liché, použijeme tedy vzorec:

$$j = P_{2k-1} + Q_{2k-1}\sqrt{A}.$$

Získáme tedy nejmenší kladné řešení rovnice:

$$\boldsymbol{j} = P_1 + Q_1\sqrt{5} = \underline{\mathbf{9 + 4\sqrt{5}}}.$$

3) Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$. Využijeme k tomu větu 2, kde je uveden vzorec

$$j^{n+2} = 2\bar{x}j^{n+1} - j^n.$$

Získáme:

$$\begin{aligned} j^2 = 2\bar{x}j^1 - j^0 \qquad &= 2\,.\,9\,.\left(9 + 4\sqrt{5}\right) - 1 \\ &= 18\,.\left(9 + 4\sqrt{5}\right) - 1 \\ &= 162 + 72\sqrt{5} - 1 \\ &= \underline{161 + 72\sqrt{5}} \end{aligned}$$

$$\begin{aligned} j^3 = 2\bar{x}j^2 - j^1 \qquad &= 2\,.\,9\,.\left(161 + 72\sqrt{5}\right) - \left(9 + 4\sqrt{5}\right) \\ &= 18\,.\left(161 + 72\sqrt{5}\right) - 9 - 4\sqrt{5} \\ &= 2898 + 1296\sqrt{5} - 9 - 4\sqrt{5} \\ &= \underline{2889 + 1292\sqrt{5}} \end{aligned}$$

$$\begin{aligned} j^4 = 2\bar{x}j^3 - j^2 \qquad &= 2\,.\,9\,.\left(2889 + 1292\sqrt{5}\right) - \left(161 + 72\sqrt{5}\right) \\ &= 18\,.\left(2889 + 1292\sqrt{5}\right) - 161 - 72\sqrt{5} \\ &= \underline{51841 + 23184\sqrt{5}} \end{aligned}$$

$$\begin{aligned} j^5 = 2\bar{x}j^4 - j^3 \qquad &= 2\,.\,9\,.\left(51841 + 23184\sqrt{5}\right) - \left(2889 + 1292\sqrt{5}\right) \\ &= \underline{930249 + 416020\sqrt{5}} \end{aligned}$$

Našli jsme prvních pět kladných řešení zadané Pellovy rovnice a nyní je zapíšeme do tabulky pro přehlednost.

n	0	1	2	3	4	5
x_n	1	9	161	2889	51841	930249
y_n	0	4	72	1292	23184	416020

Tabulka 5

Podívejme se nyní na další konkrétní příklady, které již nemusíme tak podrobně rozepisovat. Budeme postupovat stejným způsobem.

<u>Příklad 1:</u> Nalezněte první čtyři kladná řešení Pellovy rovnice $x^2 - 12y^2 = 1$.

<u>Řešení:</u>

1) Nejprve nalezneme řetězový zlomek příslušný číslu $\sqrt{12}$.

$\boldsymbol{a_0 = 3}$ $\qquad \sqrt{12} = 3 + \frac{1}{\alpha_1}$

$$\alpha_1 = \frac{1}{\sqrt{12}-3} = \frac{\sqrt{12}+3}{3}$$

$$\underline{\alpha_1 = \frac{\sqrt{12}+3}{3}}$$

$\boldsymbol{a_1 = 2}$ $\qquad \frac{\sqrt{12}+3}{3} = 2 + \frac{1}{\alpha_2}$

$$\frac{\sqrt{12}+3-6}{3} = \frac{1}{\alpha_2}$$

$$\alpha_2 = \frac{3}{\sqrt{12}-3} = \frac{3(\sqrt{12}+3)}{3} = \sqrt{12} + 3$$

$$\underline{\alpha_2 = \sqrt{12} + 3}$$

$\boldsymbol{a_2 = 6}$ $\qquad \sqrt{12} + 3 = 6 + \frac{1}{\alpha_3}$

$$\alpha_3 = \frac{1}{\sqrt{12}-3} = \frac{\sqrt{12}+3}{3}$$

$$\underline{\alpha_3 = \frac{\sqrt{12}+3}{3}}$$

→ Nekonečný periodický zlomek příslušný číslu $\sqrt{12}$ je $[\mathbf{3}; \mathbf{2}, \mathbf{6}, \dots]$, perioda $\boldsymbol{k} = \mathbf{2}$.

2) Nyní nalezneme nejmenší kladné řešení.

Získáme:

$$P_1 = a_1 P_0 + P_{-1} = 2 \,.\, 3 + 1 = \underline{7}$$

$$Q_1 = a_1 Q_0 + Q_{-1} = 2 \,.\, 1 + 0 = \underline{2}$$

$$P_2 = a_2 P_1 + P_0 = 6 \,.\, 7 + 3 = \underline{45}$$

$$Q_2 = a_2 Q_1 + Q_0 = 6 \,.\, 2 + 1 = \underline{13}$$

$$P_3 = a_3 P_2 + P_1 = 2 \,.\, 45 + 7 = \underline{97}$$

$$Q_3 = a_3 Q_2 + Q_1 = 2 \,.\, 13 + 2 = \underline{28}$$

$\boldsymbol{n}$	-1	0	1	2	3	4
$\boldsymbol{a_n}$		3	2	6	2	...
$\boldsymbol{P_n}$	1	3	7	45	97	...
$\boldsymbol{Q_n}$	0	1	2	13	28	...

Tabulka 6

Nyní přejdeme k výpočtu nejmenšího kladného řešení rovnice, které má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Číslo k je sudé, použijeme tedy vzorec:

$$j = P_{k-1} + Q_{k-1}\sqrt{A}.$$

$$\boldsymbol{j} = P_1 + Q_1\sqrt{12} = \underline{\mathbf{7 + 2\sqrt{12}}}$$

3) Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$.

Získáme:

$$j^2 = 2\bar{x}j^1 - j^0 \qquad = 2\,.\,7\,.\left(7 + 2\sqrt{12}\right) - 1$$
$$= 14\,.\left(7 + 2\sqrt{5}\right) - 1$$
$$= \underline{97 + 28\sqrt{12}}$$

$$j^3 = 2\bar{x}j^2 - j^1 \qquad = 2\,.\,7\,.\left(97 + 28\sqrt{12}\right) - \left(7 + 2\sqrt{12}\right)$$
$$= 1358 + 392\sqrt{12} - 7 - 2\sqrt{12}$$
$$= \underline{1351 + 390\sqrt{12}}$$

$$j^4 = 2\bar{x}j^3 - j^2 \qquad = 2\,.\,7\,.\left(1351 + 390\sqrt{12}\right) - \left(97 + 28\sqrt{12}\right)$$
$$= 18914 + 5460\sqrt{12} - 97 - 28\sqrt{12}$$
$$= \underline{18817 + 5432\sqrt{12}}$$

n	0	1	2	3	4
x_n	1	7	97	1351	18817
y_n	0	2	28	390	5432

Tabulka 7

Příklad 2: Nalezněte první čtyři kladná řešení Pellovy rovnice $x^2 - 24y^2 = 1$.

Řešení:

1) Nejprve nalezneme řetězový zlomek příslušný číslu $\sqrt{24}$.

$\boldsymbol{a_0 = 4}$ $\qquad \sqrt{24} = 4 + \frac{1}{\alpha_1}$

$$\alpha_1 = \frac{1}{\sqrt{24}-4} = \frac{\sqrt{24}+4}{8}$$

$$\underline{\alpha_1 = \frac{\sqrt{24}+4}{8}}$$

$\boldsymbol{a_1 = 1}$

$$\frac{\sqrt{24}+4}{8} = 1 + \frac{1}{\alpha_2}$$

$$\frac{\sqrt{24}+4-8}{8} = \frac{1}{\alpha_2}$$

$$\alpha_2 = \frac{8}{\sqrt{24}-4} = \frac{8(\sqrt{24}+4)}{8} = \sqrt{24} + 4$$

$$\underline{\alpha_2 = \sqrt{24} + 4}$$

$\boldsymbol{a_2 = 8}$

$$\sqrt{24} + 4 = 8 + \frac{1}{\alpha_3}$$

$$\alpha_3 = \frac{1}{\sqrt{24}-4} = \frac{\sqrt{24}+4}{8}$$

$$\underline{\alpha_3 = \frac{\sqrt{24}+4}{8}}$$

→ Nekonečný periodický zlomek příslušný číslu $\sqrt{24}$ je $[\mathbf{4}; \mathbf{1}, \mathbf{8}, \dots]$, perioda $\boldsymbol{k} = \mathbf{2}$.

2) Nyní nalezneme nejmenší kladné řešení.

Získáme:

$$P_1 = a_1 P_0 + P_{-1} = 1\,.\,4 + 1 = \underline{5}$$

$$Q_1 = a_1 Q_0 + Q_{-1} = 1\,.\,1 + 0 = \underline{1}$$

$$P_2 = a_2 P_1 + P_0 = 8\,.\,5 + 4 = \underline{44}$$

$$Q_2 = a_2 Q_1 + Q_0 = 8\,.\,1 + 1 = \underline{9}$$

$$P_3 = a_3 P_2 + P_1 = 1\,.\,44 + 5 = \underline{49}$$

$$Q_3 = a_3 Q_2 + Q_1 = 1\,.\,9 + 1 = \underline{10}$$

n	-1	0	1	2	3	4
a_n		4	1	8	1	...
P_n	1	4	5	44	49	...
Q_n	0	1	1	9	10	...

Tabulka 8

Nyní přejdeme k výpočtu nejmenšího kladného řešení rovnice, které má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Číslo k je sudé, použijeme tedy vzorec:

$$j = P_{k-1} + Q_{k-1}\sqrt{A}.$$

$$\boldsymbol{j} = P_1 + Q_1\sqrt{24} = \underline{\mathbf{5 + 1\sqrt{24}}}$$

3) Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$.

Získáme:

$$j^2 = 2\bar{x}j^1 - j^0 \qquad = 2\,.\,5\,.\left(5 + 1\sqrt{24}\right) - 1$$

$$= 10\,.\left(5 + 1\sqrt{24}\right) - 1$$

$$= \underline{49 + 10\sqrt{24}}$$

$$j^3 = 2\bar{x}j^2 - j^1 \qquad = 2\,.\,5\,.\left(49 + 10\sqrt{24}\right) - \left(5 + 1\sqrt{24}\right)$$

$$= 490 + 100\sqrt{24} - 5 - 1\sqrt{24}$$

$$= \underline{485 + 99\sqrt{24}}$$

$$j^4 = 2\bar{x}j^3 - j^2 \qquad = 2\,.\,5\,.\left(485 + 99\sqrt{24}\right) - \left(49 + 10\sqrt{24}\right)$$

$$= 4850 + 990\sqrt{24} - 49 - 10\sqrt{24}$$

$$= \underline{4801 + 980\sqrt{24}}$$

n	0	1	2	3	4
x_n	1	5	49	485	4801
y_n	0	1	10	99	980

Tabulka 9

Příklad 3: Nalezněte první dvě kladná řešení Pellovy rovnice $x^2 - 71y^2 = 1$.

Řešení:

1) Nejprve nalezneme řetězový zlomek příslušný číslu $\sqrt{71}$.

$\boldsymbol{a_0 = 8}$ $$\sqrt{71} = 8 + \frac{1}{\alpha_1}$$

$$\alpha_1 = \frac{1}{\sqrt{71}-8} = \frac{\sqrt{71}+8}{7}$$

$$\underline{\alpha_1 = \frac{\sqrt{71}+8}{7}}$$

$\boldsymbol{a_1 = 2}$ $$\frac{\sqrt{71}+8}{7} = 2 + \frac{1}{\alpha_2}$$

$$\frac{\sqrt{71}+8-14}{7} = \frac{1}{\alpha_2}$$

$$\alpha_2 = \frac{7}{\sqrt{71}-6} = \frac{7(\sqrt{71}+6)}{35} = \frac{\sqrt{71}+6}{5}$$

$$\underline{\alpha_2 = \frac{\sqrt{71}+6}{5}}$$

$\boldsymbol{a_2 = 2}$ $$\frac{\sqrt{71}+6}{5} = 2 + \frac{1}{\alpha_3}$$

$$\alpha_3 = \frac{5}{\sqrt{71}-4} = \frac{\sqrt{71}+4}{11}$$

$$\underline{\alpha_3 = \frac{\sqrt{71}+4}{11}}$$

$\boldsymbol{a_3 = 1}$ $$\frac{\sqrt{71}+4}{11} = 1 + \frac{1}{\alpha_4}$$

$$\alpha_4 = \frac{11}{\sqrt{71}-7} = \frac{\sqrt{71}+7}{2}$$

$$\underline{\alpha_4 = \frac{\sqrt{71}+7}{2}}$$

$\boldsymbol{a_4 = 7}$

$$\frac{\sqrt{71}+7}{2} = 7 + \frac{1}{\alpha_5}$$

$$\alpha_5 = \frac{2}{\sqrt{71}-7} = \frac{\sqrt{71}+7}{11}$$

$$\underline{\alpha_5 = \frac{\sqrt{71}+7}{11}}$$

$\boldsymbol{a_5 = 1}$

$$\frac{\sqrt{71}+7}{11} = 1 + \frac{1}{\alpha_6}$$

$$\alpha_6 = \frac{11}{\sqrt{71}-4} = \frac{\sqrt{71}+4}{5}$$

$$\underline{\alpha_6 = \frac{\sqrt{71}+4}{5}}$$

$\boldsymbol{a_6 = 2}$

$$\frac{\sqrt{71}+4}{5} = 2 + \frac{1}{\alpha_7}$$

$$\alpha_7 = \frac{5}{\sqrt{71}-6} = \frac{\sqrt{71}+6}{7}$$

$$\underline{\alpha_7 = \frac{\sqrt{71}+6}{7}}$$

$\boldsymbol{a_7 = 2}$

$$\frac{\sqrt{71}+6}{7} = 2 + \frac{1}{\alpha_8}$$

$$\alpha_8 = \frac{7}{\sqrt{71}-8} = \sqrt{71} + 8$$

$$\underline{\alpha_8 = \sqrt{71} + 8}$$

$\boldsymbol{a_8 = 16}$

$$\sqrt{71} + 8 = 16 + \frac{1}{\alpha_9}$$

$$\alpha_9 = \frac{1}{\sqrt{71}-8} = \frac{\sqrt{71}+8}{7}$$

$$\underline{\alpha_9 = \frac{\sqrt{71}+8}{7}}$$

→ Nekonečný periodický zlomek příslušný číslu $\sqrt{71}$ je $[\mathbf{8}; \mathbf{2}, \mathbf{2}, \mathbf{1}, \mathbf{7}, \mathbf{1}, \mathbf{2}, \mathbf{2}, \mathbf{16}, \dots]$, perioda $\boldsymbol{k} = \mathbf{8}$.

2) Nyní nalezneme nejmenší kladné řešení.

Získáme:

$$P_1 = a_1P_0 + P_{-1} = 2\,.\,8 + 1 = \underline{17}$$

$$Q_1 = a_1Q_0 + Q_{-1} = 2\,.\,1 + 0 = \underline{2}$$

$$P_2 = a_2P_1 + P_0 = 2\,.\,17 + 8 = \underline{42}$$

$$Q_2 = a_2Q_1 + Q_0 = 2\,.\,2 + 1 = \underline{5}$$

$$P_3 = a_3P_2 + P_1 = 1\,.\,42 + 17 = \underline{59}$$

$$Q_3 = a_3Q_2 + Q_1 = 1\,.\,5 + 2 = \underline{7}$$

$$P_4 = a_4P_3 + P_2 = 7\,.\,59 + 42 = \underline{455}$$

$$Q_4 = a_4Q_3 + Q_2 = 7\,.\,7 + 5 = \underline{54}$$

$$P_5 = a_5P_4 + P_3 = 1\,.\,455 + 59 = \underline{514}$$

$$Q_5 = a_5Q_4 + Q_3 = 1\,.\,54 + 7 = \underline{61}$$

$$P_6 = a_6P_5 + P_4 = 2\,.\,514 + 455 = \underline{1483}$$

$$Q_6 = a_6Q_5 + Q_4 = 2\,.\,61 + 54 = \underline{176}$$

$$P_7 = a_7P_6 + P_5 = 2\,.\,1483 + 514 = \underline{3480}$$

$$Q_7 = a_7Q_6 + Q_5 = 2\,.\,176 + 61 = \underline{413}$$

n	-1	0	1	2	3	4	5	6	7	8
a_n		8	2	2	1	7	1	2	2	16
P_n	1	8	17	42	59	455	514	1483	3480	…
Q_n	0	1	2	5	7	54	61	176	413	…

Tabulka 10

Nyní přejdeme k výpočtu nejmenšího kladného řešení rovnice, které má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Číslo k je sudé, použijeme tedy vzorec:

$$j = P_{k-1} + Q_{k-1}\sqrt{A}.$$

$$\boldsymbol{j} = P_7 + Q_7\sqrt{71} = \underline{\mathbf{3480 + 413\sqrt{71}}}$$

3) Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$.

Získáme:

$$j^2 = 2\bar{x}j^1 - j^0 \qquad = 2\,.\,3480\,.\left(3480 + 413\sqrt{71}\right) - 1$$

$$= \underline{24220799 + 2874480\sqrt{71}}$$

n	0	1	2
x_n	1	3480	24220799
y_n	0	413	2874480

Tabulka 11

<u>Příklad 4:</u> Nalezněte první čtyři kladná řešení Pellovy rovnice $x^2 - 15y^2 = 1$.

<u>Řešení:</u>

1) Nejprve nalezneme řetězový zlomek příslušný číslu $\sqrt{15}$.

$\boldsymbol{a_0 = 3}$ $\quad \sqrt{15} = 3 + \frac{1}{\alpha_1}$

$\alpha_1 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6}$

$\underline{\alpha_1 = \frac{\sqrt{15}+3}{6}}$

$\boldsymbol{a_1 = 1}$ $\quad \frac{\sqrt{15}+3}{6} = 1 + \frac{1}{\alpha_2}$

$\frac{\sqrt{15}+3-6}{6} = \frac{1}{\alpha_2}$

$\alpha_2 = \frac{6}{\sqrt{15}-3} = \frac{6(\sqrt{15}+3)}{6} = \sqrt{15} + 3$

$\underline{\alpha_2 = \sqrt{15} + 3}$

$\boldsymbol{a_2 = 6}$ $\quad \sqrt{15} + 3 = 6 + \frac{1}{\alpha_3}$

$\alpha_3 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6}$

$\underline{\alpha_3 = \frac{\sqrt{15}+3}{6}}$

→ Nekonečný periodický zlomek příslušný číslu $\sqrt{15}$ je $[\mathbf{3}; \mathbf{1}, \mathbf{6}, \dots]$, perioda $\boldsymbol{k} = \mathbf{2}$.

2) Nyní nalezneme nejmenší kladné řešení.

Získáme:

$P_1 = a_1 P_0 + P_{-1} = 1 \,.\, 3 + 1 = \underline{4}$

$Q_1 = a_1 Q_0 + Q_{-1} = 1 \,.\, 1 + 0 = \underline{1}$

$P_2 = a_2 P_1 + P_0 = 6 \,.\, 4 + 3 = \underline{27}$

$Q_2 = a_2 Q_1 + Q_0 = 6 \,.\, 1 + 1 = \underline{7}$

$P_3 = a_3 P_2 + P_1 = 1 \,.\, 27 + 4 = \underline{31}$

$$Q_3 = a_3Q_2 + Q_1 = 1\,.\,7 + 1 = \underline{8}$$

n	-1	0	1	2	3	4
a_n		3	1	6	1	6
P_n	1	3	4	27	31	...
Q_n	0	1	1	7	8	...

Tabulka 12

Nyní přejdeme k výpočtu nejmenšího kladného řešení rovnice, které má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Číslo k je sudé, použijeme tedy vzorec:

$$j = P_{k-1} + Q_{k-1}\sqrt{A}.$$

$$\boldsymbol{j} = P_1 + Q_1\sqrt{15} = \underline{\mathbf{4 + 1\sqrt{15}}}$$

3) Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$.

Získáme:

$$j^2 = 2\bar{x}j^1 - j^0 \qquad = 2\,.\,4\,.\left(4 + 1\sqrt{15}\right) - 1$$

$$= \underline{31 + 8\sqrt{15}}$$

$$j^3 = 2\bar{x}j^2 - j^1 \qquad = 2\,.\,4\,.\left(31 + 8\sqrt{15}\right) - \left(4 + 1\sqrt{15}\right)$$

$$= 248 + 64\sqrt{15} - 4 - 1\sqrt{15}$$

$$= \underline{244 + 63\sqrt{15}}$$

$$j^4 = 2\bar{x}j^3 - j^2 \qquad = 2\,.\,4\,.\left(244 + 63\sqrt{15}\right) - \left(31 + 8\sqrt{15}\right)$$

$$= 1952 + 504\sqrt{15} - 31 - 8\sqrt{15}$$

$$= \underline{1921 + 496\sqrt{15}}$$

n	0	1	2	3	4
x_n	1	4	31	244	1921
y_n	0	1	8	63	496

Tabulka 13

3.1.2 ZOBECNĚNÁ PELLOVA ROVNICE

V předešlém textu jsme se zabývali řešením Pellovy rovnice $x^2 - Ay^2 = 1$, kde A je přirozené číslo, které není druhou mocninou žádného přirozeného čísla. Uvedli jsme si základní definice a věty, které jsme k řešení rovnice potřebovali. Nyní se s těmito získanými znalostmi můžeme seznámit se zobecněnou Pellovou rovnicí

$$x^2 - Ay^2 = C,$$

kde A je přirozené číslo, které není druhou mocninou žádného přirozeného čísla a C je libovolné celé číslo. V následujícím textu se zaměříme opět na postup řešení uvedené rovnice, ale nejprve se seznámíme s potřebnými pojmy. Je zřejmé, že se opět stačí omezit na hledání všech kladných řešení této rovnice, tj. řešení $\alpha = x + y\sqrt{A}$, kde $x > 0$, $y > 0$.

Již víme, že $j = \bar{x} + \bar{y}\sqrt{A}$ je nejmenší kladné řešení Pellovy rovnice. Označíme-li $j^{-1} = \bar{x} - \bar{y}\sqrt{A}$, je zřejmě $jj^{-1} = 1$. Buď dále $\alpha = x + y\sqrt{A}$ libovolné řešení zobecněné Pellovy rovnice. Přímým výpočtem lze snadno ověřit, že číslo αj^n je pro každé celé číslo n také řešením rovnice. Levým řešením k řešení α budeme rozumět řešení αj^{-1} a pravým řešením budeme rozumět řešení αj. Je-li $\alpha = x + y\sqrt{A}$ libovolné řešení rovnice (nemusí být kladné), pak absolutní hodnotou α budeme rozumět $|\alpha| = |x| + |y|\sqrt{A}$. Řešení $\alpha = x + y\sqrt{A}$ nazýváme nezáporným, jestliže $x \geq 0$, $y \geq 0$.

<u>Definice 1:</u> Nechť je $\alpha = x + y\sqrt{A}$ nezáporné řešení zobecněné Pellovy rovnice. Posloupností řešení určenou prvkem α budeme rozumět posloupnost $\{\alpha j^n\}_{n=0}^{\infty}$. Pokud je α takové kladné řešení rovnice, že levé řešení αj^{-1} už není nezáporné, pak dvojici posloupností $\{\alpha j^n, |\alpha j^{-1}| j^n\}_{n=0}^{\infty}$ nazveme sérií řešení rovnice. Budeme používat zkrácené označení $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$.

Může se stát, že je α nezáporné řešení rovnice, které není kladné (tj. alespoň jedna ze složek x, y je rovna nule). Potom sérií řešení rozumíme posloupnost $\{\alpha j^n\}_{n=0}^{\infty}$, a to vzhledem k tomu, že v tomto případě $|\alpha j^{-1}| = \alpha j$.

Dále si vzpomeňme na předchozí kapitolu o Pellově rovnici. Také i pro zobecněnou Pellovu rovnici platí, že pro každá dvě různá nezáporná řešení α, β platí buď $\alpha \prec \beta$, nebo $\beta \prec \alpha$.

Nyní již přejděme k samotnému postupu řešení zobecněné Pellovy rovnice. Opět si řekneme několik kroků, které pak uvedeme v konkrétním příkladě.

1) Nejprve použijeme metodu z minulé kapitoly a najdeme nejmenší kladné řešení Pellovy rovnice.
2) Najdeme odhad pro y pomocí následujících vzorců uvedených ve větě 1.

<u>Věta 1:</u> Buď $j = \bar{x} + \bar{y}\sqrt{A}$ nejmenší kladné řešení Pellovy rovnice a buď $\alpha = x + y\sqrt{A}$ nejmenší nezáporné řešení z libovolné série řešení zobecněné Pellovy rovnice. Pak platí

$$y \leq \sqrt{\frac{C(\bar{x}-1)}{2A}} \text{ pro } C > 0,$$

$$\sqrt{-\frac{C}{A}} \leq y \leq \sqrt{\frac{-C(\bar{x}+1)}{2A}} \text{ pro } C < 0.$$

3) Najdeme všechna y vyhovující daným nerovnostem, k nimž existují x tak, že $\alpha = x + y\sqrt{A}$ je řešením rovnice.
4) Ke každému získanému řešení utvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$. Tím dostaneme všechna nezáporná řešení zadané rovnice.

<u>Názorný příklad:</u> Řešme rovnici $x^2 - 120y^2 = 721$.

<u>Řešení:</u>

1) Nejprve najdeme nejmenší kladné řešení rovnice $x^2 - 120y^2 = 1$. Jelikož jsme podobné příklady počítali v minulé kapitole, není třeba zde postup podrobně rozepisovat. Získáme tedy nekonečný periodický zlomek příslušný $\sqrt{120}$, který je zapsán ve tvaru $[\mathbf{10}; \mathbf{1}, \mathbf{20}, \mathbf{1}, \dots], s \text{ periodou } \boldsymbol{k} = \mathbf{2}$. Dalšími výpočty se dostaneme ke hledanému výsledku $\boldsymbol{j} = \mathbf{11} + \sqrt{\mathbf{120}}$.

2) Najdeme odhad pro y. Jelikož je číslo 721 větší než nula, použijeme nerovnost

$$y \leq \sqrt{\frac{C(\bar{x} - 1)}{2A}}.$$

$$\boldsymbol{y} \leq \sqrt{\frac{721(11 - 1)}{2 \,.\, 120}} < 6$$

3) Ze získané nerovnosti vidíme, že můžeme uvažovat o $y = 1, 2, 3, 4$ a 5. Ze zadané rovnice si vyjádříme

$$x = \sqrt{721 + 120y^2}.$$

Postupně dosazujeme y a zjišťujeme, zda vyjde celočíselný výsledek. Pokud se tak stane, $\alpha = x + y\sqrt{A}$ je řešením rovnice.

$y = 1$ $\qquad x = \sqrt{721 + 120 \,.\, 1^2} = \mathbf{29}$

$y = 2$ $\qquad x = \sqrt{721 + 120 \,.\, 2^2} \cong 34{,}66$

$y = 3$ $\qquad x = \sqrt{721 + 120 \,.\, 3^2} \cong 42{,}44$

$y = 4$ $\qquad x = \sqrt{721 + 120 \,.\, 4^2} \cong 51{,}39$

$y = 5$ $\qquad x = \sqrt{721 + 120 \,.\, 5^2} = \mathbf{61}$

Získali jsme tedy dvě řešení: $\boldsymbol{\alpha} = \mathbf{29} + \mathbf{1}\sqrt{\mathbf{120}}$, $\boldsymbol{\beta} = \mathbf{61} + \mathbf{5}\sqrt{\mathbf{120}}$.

4) K získaným řešením utvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$.

$\alpha j^{-1} = (29 + 1\sqrt{120})(11 - 1\sqrt{120}) = \underline{199 - 18\sqrt{120}}$

$\beta j^{-1} = (61 + 5\sqrt{120})(11 - 1\sqrt{120}) = \underline{71 - 6\sqrt{120}}$

Získáme všechna nezáporná řešení zadané rovnice:

$$\{\mathbf{29 + \sqrt{120}, 199 + 18\sqrt{120}}\}_{\boldsymbol{n=0}}^{\infty},$$

$$\{\mathbf{61 + 5\sqrt{120}, 71 + 6\sqrt{120}}\}_{\boldsymbol{n=0}}^{\infty}.$$

Příklad 1: Řešte rovnici $x^2 - 12y^2 = 25$.

Řešení:

1) Opět nejprve hledáme nejmenší kladné řešení. Rovnici $x^2 - 12y^2 = 1$ jsme řešili v předchozí kapitole, uvedeme tedy jen výsledky bez podrobného výpočtu.

→ nekonečný periodický zlomek příslušný $\sqrt{12}$ je $[\mathbf{3}; \mathbf{2}, \mathbf{6}, \dots], s$ periodou $\boldsymbol{k} = \mathbf{2}$

→ $\boldsymbol{j} = \mathbf{7 + 2\sqrt{12}}$

2) Najdeme odhad pro y.

$$y \leq \sqrt{\frac{C(\bar{x} - 1)}{2A}}$$

$$\boldsymbol{y} \leq \sqrt{\frac{25(7 - 1)}{2\,.\,12}} < 3$$

3) Hledáme x.

$$x = \sqrt{25 + 12y^2}$$

Protože je na pravé straně rovnice číslo 25, které je druhou mocninou, testujeme i $y = 0$.

$y = 0$ $\quad x = \sqrt{25 + 12\,.\,0^2} = \mathbf{5}$

$y = 1$ $\quad x = \sqrt{25 + 12\,.\,1^2} \cong 6{,}08$

$y = 2$ $\quad x = \sqrt{25 + 12\,.\,2^2} \cong 8{,}54$

Získali jsme řešení: $\boldsymbol{\alpha} = \mathbf{5} + \mathbf{0}\sqrt{\mathbf{12}}$.

4) K získanému řešení utvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$. Jelikož je α řešení nezáporné a zároveň není kladné (tj. $y = 0$), sérií řešení rozumíme posloupnost $\{\alpha j^n\}_{n=0}^{\infty}$, zkráceně $\{\alpha\}_{n=0}^{\infty}$.

Získáme všechna nezáporná řešení zadané rovnice:

$$\left\{\mathbf{5} + \mathbf{0}\sqrt{\mathbf{12}}\right\}_{\boldsymbol{n}=\mathbf{0}}^{\infty}.$$

<u>Příklad 2:</u> Řešte rovnici $x^2 - 24y^2 = -71$.

<u>Řešení:</u>

1) Nejprve hledáme nejmenší kladné řešení. Rovnici $x^2 - 24y^2 = 1$ jsme také řešili v předchozí kapitole, uvedeme tedy opět jen výsledky bez podrobného výpočtu.

→ nekonečný periodický zlomek příslušný $\sqrt{24}$ je $[\mathbf{4}; \mathbf{1}, \mathbf{8}, \dots], s$ periodou $\boldsymbol{k} = \mathbf{2}$

→ $\boldsymbol{j} = \mathbf{5} + \mathbf{1}\sqrt{\mathbf{24}}$

2) Najdeme odhad pro y.

$$\sqrt{-\frac{C}{A}} \leq y \leq \sqrt{\frac{-C(\bar{x} + 1)}{2A}}$$

$$1 < \sqrt{-\frac{(-71)}{24}} \leq \boldsymbol{y} \leq \sqrt{\frac{71(5 + 1)}{2\,.\,24}} < 3$$

3) Hledáme x.

$$x = \sqrt{-71 + 24y^2}$$

$y = 2$ $\qquad$ $x = \sqrt{-71 + 24 \,.\, 2^2} = \mathbf{5}$

Získali jsme řešení: $\boldsymbol{\alpha} = \mathbf{5} + \mathbf{2}\sqrt{\mathbf{24}}$**.**

4) K získanému řešení utvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$.

$\alpha j^{-1} = \left(5 + 2\sqrt{24}\right)\left(5 - 1\sqrt{24}\right) = \underline{-23 + 5\sqrt{24}}$

Získáme všechna nezáporná řešení zadané rovnice:

$$\left\{\mathbf{5} + \mathbf{2}\sqrt{\mathbf{24}}, \mathbf{23} + \mathbf{5}\sqrt{\mathbf{24}}\right\}_{\boldsymbol{n}=\mathbf{0}}^{\infty}.$$

<u>Příklad 3:</u> Řešte rovnici $x^2 - 71y^2 = 2$.

<u>Řešení:</u>

1) Opět nejprve hledáme nejmenší kladné řešení. Rovnici $x^2 - 71y^2 = 1$ jsme řešili v předchozí kapitole, uvedeme tedy jen výsledky bez podrobného výpočtu.

→ nekonečný periodický zlomek příslušný $\sqrt{71}$ je $[\mathbf{8}; \mathbf{2}, \mathbf{2}, \mathbf{1}, \mathbf{7}, \mathbf{1}, \mathbf{2}, \mathbf{2}, \mathbf{16}, \dots]$, s periodou $\boldsymbol{k} = \mathbf{8}$

→ $\boldsymbol{j} = \mathbf{3480} + \mathbf{413}\sqrt{\mathbf{71}}$

2) Najdeme odhad pro y.

$$y \leq \sqrt{\frac{C(\bar{x} - 1)}{2A}}$$

$$\boldsymbol{y} \leq \sqrt{\frac{2(3480-1)}{2\,.\,71}} = 7$$

3) Hledáme x.

$$x = \sqrt{2 + 71y^2}$$

$y = 1$ $\quad x = \sqrt{2 + 71\,.\,1^2} \cong 8{,}5$

$y = 2$ $\quad x = \sqrt{2 + 71\,.\,2^2} \cong 16{,}9$

$y = 3$ $\quad x = \sqrt{2 + 71\,.\,3^2} \cong 25{,}3$

$y = 4$ $\quad x = \sqrt{2 + 71\,.\,4^2} \cong 33{,}7$

$y = 5$ $\quad x = \sqrt{2 + 71\,.\,5^2} \cong 42{,}2$

$y = 6$ $\quad x = \sqrt{2 + 71\,.\,6^2} \cong 50{,}6$

$y = 7$ $\quad x = \sqrt{2 + 71\,.\,7^2} = \mathbf{59}$

Získali jsme řešení: $\boldsymbol{\alpha} = \mathbf{59} + \mathbf{7}\sqrt{\mathbf{71}}$.

4) K získanému řešení utvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$.

$\alpha j^{-1} = (59 + 7\sqrt{71})(3480 - 413\sqrt{71}) = \underline{59 - 7\sqrt{71}}$

Získáme všechna nezáporná řešení zadané rovnice:

$$\{\mathbf{59} + \mathbf{7}\sqrt{\mathbf{71}}, \mathbf{59} + \mathbf{7}\sqrt{\mathbf{71}}\}_{\boldsymbol{n}=\mathbf{0}}^{\infty}.$$

Nalezněme ještě další kladná řešení. Vypočteme-li

$\alpha j = (59 + 7\sqrt{71})(3480 + 413\sqrt{71}) = \underline{410581 + 48727\sqrt{71}}$, resp.

$\alpha j^2 = (59 + 7\sqrt{71})(3480 + 413\sqrt{71})^2 = \underline{2857643701 + 339139913\sqrt{71}}$,

vidíme, že jde o řešení již značně veliká.

Příklad 4: Řešte rovnici $x^2 - 15y^2 = 48$.

Řešení:

1) Opět nejprve hledáme nejmenší kladné řešení. Rovnici $x^2 - 15y^2 = 1$ jsme řešili v předchozí kapitole, uvedeme tedy jen výsledky bez podrobného výpočtu.

→ nekonečný periodický zlomek příslušný $\sqrt{15}$ je $[\mathbf{3}; \mathbf{1}, \mathbf{6}, \dots]$, s periodou $\boldsymbol{k} = \mathbf{2}$

→ $\boldsymbol{j} = \mathbf{4} + \mathbf{1}\sqrt{\mathbf{15}}$

2) Najdeme odhad pro y.

$$y \leq \sqrt{\frac{C(\bar{x} - 1)}{2A}}$$

$$\boldsymbol{y} \leq \sqrt{\frac{48(4-1)}{2 \,.\, 15}} < 3$$

3) Hledáme x.

$$x = \sqrt{48 + 15y^2}$$

$y = 1$ $\qquad$ $x = \sqrt{48 + 15 \,.\, 1^2} \cong 7{,}9$

$y = 2$ $\qquad$ $x = \sqrt{48 + 15 \,.\, 2^2} \cong 10{,}4$

Zjistili jsme, že **rovnice nemá řešení**.

3.2 PYTHAGOREJSKÁ ROVNICE

Pythagorejská trojice je trojice přirozených čísel a, b, c takových, že platí $a^2 + b^2 = c^2$. Této rovnici říkáme pythagorejská a patří také mezi diofantovské rovnice. Název je odvozen od Pythagorovy věty, která uvádí podobný vztah pro strany pravoúhlého trojúhelníka.

<u>Platí následující věta:</u>

Obecné řešení diofantovské rovnice $x^2 + y^2 = z^2$ celými čísly $x,\ y,\ z,\ x > 0$, $y > 0,\ z > 0,\ D(x, y) = 1$ a celé číslo x je sudé, je dané výrazy

$$x = 2ab, y = b^2 - a^2, z = a^2 + b^2,$$

kde $0 < a < b$ jsou přirozená a nesoudělná čísla různé parity.

Existuje mnoho důkazů této věty. Budeme sledovat variantu důkazu ze [4], využívající našich znalostí o celých Gaussových číslech. Víme, že obor integrity $(Z[i], +, .)$ je eukleidovský a že v něm existují čtyři jednotky, kterými jsou $1, i, -1, -i$. Tyto čtyři prvky lze zapsat jako $i^r, r = 0{,}1{,}2{,}3$. Připomeňme si ještě, že typicky je Gaussovo celé číslo asociováno se čtveřicí Gaussových celých čísel (např. $2 + 3i$ samo se sebou, s $-2 - 3i$, s $-3 + 2i$ a $3 - 2i$).

Víme také, že každé Gaussovo celé číslo α s normou $N(\alpha) > 1$ lze zapsat jako součin konečného počtu Gaussových prvočísel

$$\alpha = \pi_1 \pi_2 \cdots \pi_r,$$

přičemž tento rozklad je až na pořadí činitelů a asociovanost jednoznačný.

Budeme ještě potřebovat toto tvrzení, které bezprostředně plyne z předchozího.

<u>Lemma:</u> Jestliže je součin dvou nesoudělných celých Gaussových čísel $\alpha\,.\,\beta$ roven n-té mocnině nějakého celého Gaussova čísla γ, tj. platí-li

$$\alpha\,.\,\beta = \gamma^n,$$

potom je každý z činitelů α, β asociován s n-tou mocninou celého Gaussova čísla.

Důkaz lemmatu je jasný z toho, že γ lze zapsat jakožto součin Gaussových prvočísel $\gamma = \pi_1 \cdots \pi_s$. Potom $\gamma^n = \pi_1^n \cdots \pi_s^n = \alpha \, . \, \beta$ a vzhledem k nesoudělnosti α, β musí každé π_i^n dělit právě jedno z α, β. Odtud již tvrzení lemmatu plyne.

Nyní se vrátíme k rovnici $x^2 + y^2 = z^2$ a rozvážíme, že pokud $D(x, y) = 1$, pak jsou x, y přirozená čísla různé parity (tj. jedno je sudé, druhé je liché). Je zřejmé, že x, y nemohou být obě sudá, neboť $D(x, y) = 1$. Nemohou být ani obě lichá. Kdyby bylo $x = 2k + 1$, je dále $x^2 = 4k^2 + 4k + 1$ a $x^2 \equiv 1 \ (mod 4)$. Obdobně pak $y^2 \equiv 1 \ (mod 4)$ a $x^2 + y^2 \equiv 2 \ (mod 4)$. Avšak $z^2 \equiv 2 \ (mod 4)$ neplatí pro žádné $z \in N$. Je totiž pro z sudé $z^2 \equiv 0 \ (mod 4)$ a pro z liché, jak jsme ukázali výše, $z^2 \equiv 1 \ (mod 4)$.

Rovnici $x^2 + y^2 = z^2$ lze v $Z[i]$ přepsat ve tvaru $(x + iy)(x - iy) = z^2$. Snadno nahlédneme, že $x + iy$ a $x - iy$ jsou nesoudělná Gaussova celá čísla.

Při řešení uvedené rovnice můžeme využít výše zmíněné lemma. Součin dvou nesoudělných čísel se rovná druhé mocnině z^2, tedy je $x + iy$ asociované s druhou mocninou nějakého celého Gaussova čísla. Můžeme napsat

$$x + iy = i^r (a + bi)^2,$$

kde a, b jsou celá čísla a r se rovná některému z čísel 0, 1, 2, 3. Nyní si rovnici dále upravíme a porovnáváním reálné a imaginární části dostaneme následující výpočty.

$$x + iy = i^r (a + bi)^2$$

$$x + iy = i^r (a^2 + 2abi + b^2 i^2)$$

$$x + iy = i^r (a^2 + 2abi - b^2)$$

$$x + iy = i^r (a^2 - b^2) + i^r i \, . \, 2ab$$

$$\boldsymbol{x + iy = i^r (a^2 - b^2) + i^{r+1} \, . \, 2ab}$$

$\boldsymbol{r = 0}$ → $x + iy = (a^2 - b^2) + i \, . \, 2ab$

$\underline{x = (a^2 - b^2)}$

$\underline{y = 2ab}$

$\boldsymbol{r = 1}$ → $x + iy = i(a^2 - b^2) + i^2 \, . \, 2ab$

$x + iy = i(a^2 - b^2) - 2ab$

$\underline{x = -2ab}$

$\underline{y = (a^2 - b^2)}$

$\boldsymbol{r = 2}$ → $x + iy = i^2(a^2 - b^2) + i^3 \,.\, 2ab$

$x + iy = -(a^2 - b^2) - i \,.\, 2ab$

$\underline{x = -(a^2 - b^2)}$

$\underline{y = -2ab}$

$\boldsymbol{r = 3}$ → $x + iy = i^3(a^2 - b^2) + i^4 \,.\, 2ab$

$x + iy = -i(a^2 - b^2) + 2ab$

$\underline{x = 2ab}$

$\underline{y = -(a^2 - b^2)}$

Zjistili jsme tedy, že porovnáním reálné a imaginární části získáme

$$\boldsymbol{x = \pm(a^2 - b^2), y = \pm 2ab}$$

nebo

$$\boldsymbol{x = \pm 2ab, y = \mp(a^2 - b^2)}.$$

Dále z rovnice $x + iy = i^r(a + bi)^2$ dostáváme přechodem k číslům komplexně sdruženým

$$x - iy = i^{-r}(a - bi)^2.$$

Poznámka: Jestliže $a + ib = 0$, kde jsou a, b reálná čísla, potom je $a = 0, b = 0$. Tedy také platí $a - ib = 0$. V našem případě například pro $r = 0$ vyplývá

$$x + iy = (a^2 - b^2) + i \,.\, 2ab,$$

$$[x - (a^2 - b^2)] + i[y - 2ab] = 0.$$

Tedy je $x - (a^2 - b^2) = 0, y - 2ab = 0$. A proto také platí

$$[x - (a^2 - b^2)] - i[y - 2ab] = 0,$$

tj.

$$x - iy = (a^2 - b^2) - i\,.\,2ab.$$

Dále si uvědomme, že $i^{-r} = (-i)^r$.

Nyní nám ještě zbývá najít vyjádření pro z. Pomocí rovnice $x + iy = i^r(a + bi)^2$ a rovnice $x - iy = i^{-r}(a - bi)^2$ získáváme

$$z^2 = (x - iy)(x - iy) = [i^r(a + bi)^2][i^{-r}(a - bi)^2].$$

Odtud konečně vyplývá

$$z = \pm(a^2 + b^2).$$

Pro přehlednost se podívejme na výpočty, které nás k tomuto výsledku dovedly.

$$z^2 = [i^r(a + bi)^2][i^{-r}(a - bi)^2]$$

pro $r = 0$ → $z^2 = (a + bi)^2(a - bi)^2$

$$z^2 = (a^2 + b^2)^2$$

$$\underline{z = \pm(a^2 + b^2)}$$

pro $r = 1$ → $z^2 = [i(a + bi)^2][i^{-1}(a - bi)^2]$

$$z^2 = [i(a^2 + 2abi - b^2)][-i(a^2 - 2abi - b^2)]$$

$$z^2 = (a^2 + b^2)^2$$

$$\underline{z = \pm(a^2 + b^2)}$$

pro $r = 2$ → $z^2 = [i^2(a + bi)^2][i^{-2}(a - bi)^2]$

$$z^2 = [-(a^2 + 2abi - b^2)][-(a^2 - 2abi - b^2)]$$

$$z^2 = (a^2 + b^2)^2$$

$$\underline{z = \pm(a^2 + b^2)}$$

pro $r = 3$ → $z^2 = [i^3(a + bi)^2][i^{-3}(a - bi)^2]$

$$z^2 = [-i(a^2 + 2abi - b^2)][i(a^2 - 2abi - b^2)]$$

$$z^2 = (a^2 + b^2)^2$$

$$\underline{z = \pm(a^2 + b^2)}$$

Shrneme tedy získané výsledky. Pokud má rovnice $x^2 + y^2 = z^2$ řešení takové, že x, y, z jsou celá čísla žádaných vlastností, musí být čísla x, y, z ve tvaru:

$$\boldsymbol{x = \pm(a^2 - b^2), y = \pm 2ab, z = \pm(a^2 + b^2)}$$

nebo

$$\boldsymbol{x = \pm 2ab, y = \mp(a^2 - b^2), z = \pm(a^2 + b^2)},$$

kde a, b jsou celá čísla. Přímým dosazením se můžeme přesvědčit, že každá z výše napsaných trojic opravdu vyhovuje dané rovnici.

Zbývá nám vyřešit, jak je třeba volit čísla a, b, aby byly splněny podmínky $x > 0, y > 0, z > 0, D(x, y) = 1$. Víme, že čísla x, y musí mít různou paritu, a navíc dále žádáme, aby x bylo sudé. Může tedy nastat jen případ druhý, tedy

$$x = \pm 2ab, y = \mp(a^2 - b^2), z = \pm(a^2 + b^2).$$

Nyní se tedy omezme na případ horního znaménka.

$$\boldsymbol{x = 2ab, y = b^2 - a^2, z = a^2 + b^2}$$

Aby platilo $x > 0, y > 0$, stačí volit $0 < a < b$. A dále aby platilo $D(x, y) = 1$, je nutné a stačí, aby čísla a, b byla nesoudělná a měla různou paritu, což nyní dokážeme.

<u>Důkaz:</u>

1) Podmínka je nutná. Kdyby platilo $D(a, b) > 1$, nebyla by čísla $x = 2ab, y = b^2 - a^2, z = a^2 + b^2$ nesoudělná. Zároveň musí mít čísla a, b různou paritu, protože jinak by nebylo y liché.

2) Podmínky jsou postačující. Máme ukázat, že pokud jsou čísla a, b volena uvedeným způsobem, je $D(x, y) = 1$. Pokud by platilo $D(x, y) = d > 1$, platilo by také $d|z$, tj. $d|b^2 - a^2, d|b^2 + a^2$. Také by tedy platilo $d|2a^2, d|2b^2$. A pokud $D(a, b) = 1$, bylo by $d|2$, tj. $d = 2$. To je ale nemožné, protože y se rovná rozdílu dvou čísel různé parity, tudíž y je liché.

Zároveň vidíme, že různým hodnotám a, b odpovídají různé hodnoty x, y, z. Neboť jestliže je y, z dáno, jsou čísla $a > 0, b > 0$ určené rovnicemi $y = b^2 - a^2, z = a^2 + b^2$ jednoznačně.

Tím jsme tedy konečně dokázali větu uvedenou na začátku kapitoly.

Věta 1: Nejobecnější řešení rovnice $x^2 + y^2 = z^2$ celými čísly x, y, z, které splňují podmínky $x > 0,\ y > 0,\ z > 0,\ D(x, y) = 1,\ 2|x$, je dané výrazy

$$x = 2ab, y = b^2 - a^2, z = b^2 + a^2,$$

kde $0 < a < b$ jsou celá a nesoudělná čísla různé parity.

Podle zmíněné věty můžeme sestavit například následující tabulku výsledků.

(*a*, *b*)	**(*x*, *y*, *z*)**
(1, 2)	(4, 3, 5)
(2, 3)	(12, 5, 13)
(1, 4)	(8, 15, 17)
(3, 4)	(24, 7, 25)
(2, 5)	(20, 21, 29)
(4, 5)	(40, 9, 41)
…	…

Tabulka 14

Po úspěšném vyřešení rovnice $x^2 + y^2 = z^2$ se pojďme podívat na další problém. Zkusme najít všechna řešení rovnice $x^2 + y^2 = z^n, n \geq 2$, kde x, y, z jsou celá čísla a platí $D(x, y) = 1, z > 0$. Postup bude velmi podobný postupu při řešení předešlé rovnice. I v tomto případě musí mít čísla x, y různou paritu. Číslo z je pak liché.

Předpokládejme, že trojice x, y, z je řešením rovnice $x^2 + y^2 = z^n$ žádaných vlastností, a opět tuto rovnici zapíšeme jako v předchozím příkladě ve tvaru

$$(x + iy)(x - iy) = z^n.$$

Víme, že stejně jako v případě rovnice $x^2 + y^2 = z^2$ jsou čísla $x + iy$, $x - iy$ nesoudělná. Užijeme výše zmíněné lemma. Potom existují dvě celá čísla a, b a číslo $r, 0 \leq r \leq 3$, že platí

$$x + iy = i^r (a + bi)^n,$$

$$x - iy = i^{-r} (a - bi)^n.$$

Jestliže má platit $z > 0$, vynásobením získáme

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

U výše zmíněné rovnice $x + iy = i^r (a + bi)^n$ opět porovnáme imaginární a reálnou část a získáme následující výpočty.

$$x + iy = \left[a^n - \binom{n}{2} a^{n-2} b^2 + \binom{n}{4} a^{n-4} b^4 + \cdots\right] i^r +$$

$$+ \left[\binom{n}{1} a^{n-1} b - \binom{n}{3} a^{n-3} b^3 + \cdots\right] i^{r+1}$$

$$\pm x = a^n - \binom{n}{2} a^{n-2} b^2 + \cdots$$

$$\pm y = \binom{n}{1} a^{n-1} b - \binom{n}{3} a^{n-3} b^3 + \cdots$$

Přímým dosazením se můžeme přesvědčit, že uvedené výrazy vyjadřující x, y, z opravdu vyhovují rovnici $x^2 + y^2 = z^n$. Zbývá zjistit, jak je třeba volit čísla a, b, aby byly výrazy $\pm x = a^n - \binom{n}{2} a^{n-2} b^2 + \cdots$ a $\pm y = \binom{n}{1} a^{n-1} b - \binom{n}{3} a^{n-3} b^3 + \cdots$ nesoudělné. Lze dokázat, že čísla a, b musí být opět nesoudělná a musí mít různou paritu. Platí tedy následující věta.

<u>Věta 2:</u> Všechna řešení rovnice $x^2 + y^2 = z^n, n \geq 2$, pro která je $z > 0, D(x, y) =$ $= 1$, získáme z rovnice

$$x + iy = i^r (a + bi)^n,$$

kde a, b jsou celá nesoudělná čísla různé parity.

Příklad: Nalezněte řešení rovnice $x^2 + y^2 = z^3$.

Řešení: Řešení této rovnice získáme z vyjádření $x + iy = i^r(a + bi)^3$, jak je uvedeno ve větě 2 výše. Víme, že každá jednotka sama je třetí mocninou.

$$1 = 1^3, i = (-i)^3, -i = i^3, (-1) = (-1)^3.$$

Můžeme tedy i^r vsunout do závorky a zjednodušit zápis (podrobněji rozepíšeme dále). Zapíšeme tedy takto:

$$x + iy = (a + bi)^3,$$

tj.

$$x = a^3 - 3ab^2, y = 3a^2b - b^3, z = a^2 + b^2.$$

Dostaneme například následující hodnoty.

(*a*, *b*)	**(*x*, *y*, *z*)**
(2, 3)	(-46, 9, 13)
(3, 2)	(46, -9, 13)
(2, 5)	(-142, -65, 29)
...	...

Tabulka 15

Nyní si podrobněji vysvětlíme uvedené zjednodušení zápisu. Řešení rovnice $x^2 + y^2 = z^3$ dostaneme z vyjádření

$$x + iy = i^r(a_1 + ib_1)^3,\ r = 0, 1, 2, 3. \qquad (*)$$

Postupně ukážeme, že pro všechna $r = 0, 1, 2, 3$ lze vztah $(*)$ přepsat ve tvaru

$$x + iy = (a + ib)^3, \qquad (**)$$

kde a, b jsou celá čísla.

Pro $r = 0$ je to velice jednoduché. Vztah $(*)$ má tvar $x + iy = (a_1 + ib_1)^3$ a píšeme-li místo a_1 jen a, místo b_1 pouze b, dostáváme $(**)$.

Pro $r = 1$ máme $x + iy = i(a_1 + ib_1)^3$. Je ale $i = (-i)^3$, tj. $x + iy = (-i)^3(a_1 + ib_1)^3 = (a_1(-i) - i^2b_1)^3 = (b_1 + i(-a_1))^3$. Píšeme-li nyní a místo b_1, b místo $-a_1$, máme $x + iy = (a + ib)^3$, tj. vztah $(**)$.

Pro $r = 2$ dostaneme z $(*)$ vztah $x + iy = (-1)(a_1 + ib_1)^3 = (-1)^3(a_1 + ib_1)^3 = (-a_1 + i(-b_1))^3$. Nyní místo $-a_1$ pišme a, místo $-b_1$ zase b a máme $x + iy = (a + ib)^3$, což je opět $(**)$.

Nakonec pro $r = 3$ je $x + iy = i^3(a_1 + ib_1)^3 = (ia_1 - b_1)^3 = (-b_1 + ia_1)^3$. Označme $-b_1 = a, a_1 = b$ a máme $x + iy = (a + ib)^3$, čili i teď jsme dostali vztah $(**)$.

Porovnáním reálných složek dostaneme $x = a^3 - 3ab^2$, analogicky z komponent obsahujících i máme $y = 3a^2b - b^3$ a dopočteme $z = a^2 + b^2$. Tím je sice rovnice $x^2 + y^2 = z^3$ vyřešena, ale neřekneme-li nic dalšího, nezískali bychom příliš elegantní popis všech řešení, jak dále uvidíme.

První, co si uvědomíme, je toto: Je-li uspořádaná trojice $[x_0, y_0, z_0]$ řešením rovnice $x^2 + y^2 = z^3$, pak také trojice $[-x_0, y_0, z_0]$, $[x_0, -y_0, z_0]$, $[-x_0, -y_0, z_0]$ jsou řešeními téže rovnice.

V případě „pythagorejské“ rovnice $x^2 + y^2 = z^2$, kdy jsme vyžadovali nejen nalezení řešení dané rovnice, ale i zachycení faktu, že má jít o délky stran pravoúhlého trojúhelníka, nám ovšem vyšla výraznější omezení na celá čísla ve vzorci generujícím „pythagorejské“ trojice. Nyní budeme za x i y brát celá čísla jakéhokoli znaménka. Číslo z vyskytující se na pravé straně rovnice $x^2 + y^2 = z^3$ ovšem může být jen kladné.

Nyní vyzkoušíme významnější věc. Volme na ukázku např. $a = 2, b = 1$. Dostáváme $x = 2, y = 11, z = 5$ a snadno ověříme, že uspořádaná trojice $[2, 11, 5]$ je řešením, neboť $2^2 + 11^2 = 5^3$.

Kdybychom dále volili např. dvojnásobné parametry, tj. $a = 4, b = 2$, dostali bychom $x = 16, y = 88, z = 20$. Jenže trojice $[16, 88, 20]$ je, jak tušíme, jen „namnožena“ z trojice $[2, 11, 5]$ tím způsobem, že první dvě složky jsou vynásobeny osmi, třetí čtyřmi.

Kdybychom volili trojnásobné hodnoty, tj. $a = 6, b = 23$, dostali bychom $x = 54, y = 297, z = 45$. Vidíme, že první dvě složky v původní trojici $[2, 11, 5]$ bychom vynásobili $3^3 = 27$, kdežto třetí složku $3^2 = 9$.

Obecněji, kdybychom přecházeli od původních parametrů a, b k dvojici $a' = k.a, b' = k.b$, pak bychom zřejmě místo původní trojice $[x_0, y_0, z_0]$ získali „nové" řešení $[k^3 x_0, k^3 y_0, k^2 z_0]$. To ale není příliš zajímavá hra. Tímto způsobem můžeme vygenerovat celé série řešení, ale postačilo by znát jen původní „primitivní" trojici $[x_0, y_0, z_0]$, kde čísla x_0, y_0 jsou nesoudělná.

Dostáváme se tedy k tomu, jak najít všechna řešení $[x, y, z]$ rovnice $x^2 + y^2 = z^3$ taková, že $z > 0$ a x, y jsou nesoudělná. Ukazuje se, že to nastane právě tehdy, když a, b budou celá nesoudělná čísla různé parity (tj. jedno z nich je liché a druhé sudé).

<u>Věta 3</u>: Všechna řešení rovnice $x^2 + y^2 = z^3$ taková, že $z > 0$ a x, y jsou nesoudělná, dostaneme z vyjádření $x = a^3 - 3ab^2$, $y = 3a^2b - b^3$, $z = a^2 + b^2$, kde a, b jsou nesoudělná celá čísla různé parity.

<u>Důkaz:</u>

a) Nejprve dokažme tuto implikaci: Jsou-li x, y nesoudělná, pak $D(a, b) = 1$ a celá čísla a, b jsou různé parity. Postupujme sporem a předpokládejme, že čísla $x = a^3 - -3ab^2$, a $y = 3a^2b - b^3$ jsou nesoudělná a přitom $D(a, b) = d > 1$. Pak existovala celá čísla k_1, k_2 taková, že $a = k_1.d, a = k_2.d$ a dosazením do vzorců pro x, y ihned dostaneme, že $d^3|x, d^3|y$. To je ovšem spor s nesoudělností čísel x, y. Snadno také nahlédneme, že celá čísla a, b jsou různé parity. Pokud by totiž byla obě sudá, je $D(a, b) = 2$ a dostaneme spor zcela stejně jako v předchozí úvaze. Ať tedy a, b jsou obě lichá, pak jsou zřejmě čísla $x = a^3 - 3ab^2$ a $y = 3a^2b - b^3$ obě sudá a tedy soudělná, což je spor.

b) Zbývá dokázat, že z předpokladů $D(a, b) = 1$ a celá čísla a, b jsou různé parity již vyplývá, že $D(x, y) = 1$. Postupujme opět sporem a předpokládejme, že čísla $x = a(a^2 - 3b^2)$ a $y = b(3a^2 - b^2)$ jsou soudělná. Existuje tedy prvočíslo $p \in N$ takové, že $p|x, p|y$. Nyní si připomeneme prvočíselnou vlastnost: jestliže prvočíslo $p|u.v$, pak $p|u$ nebo $p|v$.

Víme, že $p|a(a^2 - 3b^2)$ a $p|b(3a^2 - b^2)$, takže rozebereme čtyři příklady:

1. Jestliže $p|a$ a $p|b$, pak čísla a, b nejsou nesoudělná a to je spor s předpokladem $D(a,b) = 1$.

2. Jestliže $p|a$ a $p|(3a^2 - b^2)$, pak také $p|a^2$, $p|3a^2$ a tedy nutně $p|b^2$. Z toho plyne $p|b$ a dostáváme spor s předpokladem $D(a,b) = 1$ zcela stejně jako v závěru části 1.

3. Pokud $p|(a^2 - 3b^2)$ a $p|b$, je postup obdobný jako v části 2. a nebudeme jej již provádět.

4. Pokud $p|(a^2 - 3b^2)$ a $p|(3a^2 - b^2)$, pak $p|[-3.(a^2 - 3b^2) + (3a^2 - b^2)]$, tj. $p|8b^2$. Nyní poprvé využijeme faktu, že čísla a, b jsou různé parity. Odtud snadno plyne, že jedno z čísel x, y je liché a druhé sudé, a protože $p|x$ a zároveň $p|y$, není $p = 2$, tj. p je liché prvočíslo. Z toho a z $p|8b^2$ máme $p|b^2$ a odtud $p|b$. Analogicky ukážeme, že $p|a$ a získáme opět spor s $D(a,b) = 1$, což dokončuje důkaz.

Dalším zajímavým typem diofantovské rovnice je rovnice $x^2 + 4 = y^3$. Pojďme se zamyslet nad jejím řešením. Rovnici si přepišme do tvaru

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

<u>1) Nejprve hledejme řešení s lichým x.</u> Potom jsou čísla $x + 2i, x - 2i$ nesoudělná. Kdyby totiž δ dělilo $x + 2i$ i $x - 2i$, pak $\delta|2x \wedge \delta|4i$, ale $2 = -i(1+i)^2$, takže $\delta| - i(1+i)^2 x$, $4 = -(1+i)^4$, $\delta| - i(1+i)^4$. Z posledního vyjádření je vidět, že eventuelní dělitel δ by musel být asociován s jistou mocninou $(1+i)^k, k = 1, 2, 3, 4$. Ukážeme ale, že $x + 2i$ není dělitelné ani $1 + i$, takže nemůže být dělitelné ani žádnou další mocninou Gaussova prvočísla $(1+i), k = 2, 3, 4$. Snadno se ověří, že $\frac{x+2i}{1+i} \notin Z[i]$ (x je podle předpokladu liché).

Podle již dříve zmíněného lemmatu můžeme psát:

$$x + 2i = i^r (a_1 + i b_1)^3,$$

$$x - 2i = i^{-r}(a_1 - ib_1)^3.$$

Ale i^r je vždy samo třetí mocninou, proto lze psát jednodušeji:

$$x + 2i = (a + bi)^3,$$

$$x - 2i = (a - bi)^3,$$

kde a, b jsou celá čísla. Odtud porovnáním reálné a imaginární části dojdeme k následujícím výsledkům.

$$\begin{aligned} x + 2i &= (a + bi)^3 \\ &= a^3 + 3a^2bi + 3ab^2i^2 + b^3i^3 \\ &= a^3 - 3ab^2 + 3a^2bi - b^3i \\ &\Rightarrow \boldsymbol{x = a^3 - 3ab^2, 2 = b(3a^2 - b^2)} \\ x - 2i &= (a - bi)^3 \\ &= a^3 - 3a^2bi + 3ab^2i^2 - b^3i^3 \\ &= a^3 - 3ab^2 - 3a^2bi + b^3i \\ &\Rightarrow \boldsymbol{x = a^3 - 3ab^2, 2 = b(3a^2 - b^2)} \end{aligned}$$

Ze získané rovnice $2 = b(3a^2 - b^2)$ plyne buď $b = \pm 1, 3a^2 - b^2 = \pm 2$, nebo $b = \pm 2, 3a^2 - b^2 = \pm 1$. Pojďme se podrobněji podívat na obě tyto možnosti.

a) $3a^2 - b^2 = \pm 2$

$3a^2 - 1 = \pm 2$

$a^2 = \frac{\pm 2 + 1}{3}$

$\Rightarrow a = \pm 1, b = \pm 1$

Toto však po dosazení do vzorce $x = a^3 - 3ab^2$ vede k sudému x.

b) $3a^2 - b^2 = \pm 1$

$3a^2 - 4 = \pm 1$

$a^2 = \frac{\pm 1 + 4}{3}$

$\Rightarrow a = \pm 1, b = \pm 2$

Toto po dosazení do vzorce $x = a^3 - 3ab^2$ vede k lichému x. Po provedení zkoušky dosazením hodnot a, b do vzorce $2 = b(3a^2 - b^2)$ zjišťujeme, že vyhovuje pouze řešení $a = \pm 1, b = -2$. Dosazením jsme získali $\boldsymbol{x = \pm 11, y = 5}$.

<u>2) Nyní hledejme řešení se sudým x.</u> Proto tedy položme $x = 2u$. Potom musí být i y sudé, tedy zapíšeme $y = 2v$. Původní rovnice tedy přejde v rovnici $u^2 + 1 = 2v^3$, kde u musí být liché.

$$x^2 + 4 = y^3$$

$$(2u)^2 + 4 = (2v)^3$$

$$u^2 + 1 = 2v^3$$

Můžeme pak psát:

$$\left(\frac{u+1}{2}\right)^2 + \left(\frac{u-1}{2}\right)^2 = v^3.$$

Nyní vlastně řešíme rovnici $x^2 + y^2 = z^3$. Čísla $\frac{u+1}{2}, \frac{u-1}{2}$ jsou nesoudělná. Postupujeme podobně jako v předchozím příkladu. Můžeme psát $(x + iy)(x - iy) = z^3$, odtud odvodíme $x + iy = (a + bi)^3$. Získáme $x = a^3 - 3ab^2, y = 3a^2b - b^3, z = a^2 + b^2$, kde a, b jsou nesoudělná čísla různé parity. V našem případě tedy:

$$\frac{u+1}{2} = p^3 - 3pq^2,$$

$$\frac{u-1}{2} = 3p^2q - q^3,$$

kde p, q jsou nesoudělná čísla různé parity. Tyto rovnice dále upravíme a od sebe odečteme.

$$u + 1 = 2p^3 - 6pq^2$$

$$\underline{u - 1 = 6p^2q - 2q^3}$$

$$p^3 + q^3 - 3pq^2 - 3p^2q = 1$$

$$\boldsymbol{(p + q)(p^2 - 4pq + q^2) = 1}$$

Odtud plyne, že musí platit buď:

$$p + q = 1, p^2 - 4pq + q^2 = 1,$$

nebo:

$$p + q = -1, p^2 - 4pq + q^2 = -1.$$

Tyto dvě možnosti nyní podrobněji rozepíšeme.

a) $p + q = 1, p^2 - 4pq + q^2 = 1$

$\Rightarrow p = 0, q = 1$: $\frac{u+1}{2} = p^3 - 3pq^2$

$\frac{u+1}{2} = 0 - 3 . 0 . 1$

$u = -1$

$\Rightarrow \boldsymbol{x = -2, y = 2}$

$\Rightarrow p = 1, q = 0$: $\frac{u+1}{2} = p^3 - 3pq^2$

$\frac{u+1}{2} = 1 - 0$

$u = 1$

$\Rightarrow \boldsymbol{x = 2, y = 2}$

b) $p + q = -1, p^2 - 4pq + q^2 = -1$

→ Neexistuje celočíselné řešení.

Zjistili jsme tedy, že rovnice $x^2 + 4 = y^3$ má přesně čtyři dvojice řešení celými čísly, a to: $[\mathbf{11}, \mathbf{5}], [-\mathbf{11}, \mathbf{5}], [\mathbf{2}, \mathbf{2}], [-\mathbf{2}, \mathbf{2}]$.

4 DESÁTÝ HILBERTŮV PROBLÉM

Nejprve si pojďme stručně říci pár vět o známé osobnosti, jejíž jméno tento problém nese.

Obrázek 1 - David Hilbert, [6]

David Hilbert (1862 – 1943) studoval na gymnáziu v jeho rodném městě Kaliningradu (Königsberg). Po maturitě nastoupil na univerzitu v Königsbergu, kde pokračoval ve studiu pod vedením Lindemanna. V roce 1885 pak obdržel doktorát za práci s názvem *Über invariante Eigenschaften specieller binärer Formen, insbesondere der Kugelfunctionen*. Hilbert působil na této univerzitě jako soukromý docent až do roku 1892. Dále byl jmenován mimořádným profesorem, poté v roce 1893 se stal řádným profesorem. V roce 1895 odešel na univerzitu v Göttingenu, kde učil po zbytek své kariéry. Hilbert přispěl k mnoha oblastem matematiky a obdržel také mnoho vyznamenání.

Tato kapitola je však věnována desátému Hilbertovu problému, který patří mezi dalších 23 matematických problémů. Seznam těchto 23 takzvaných Hilbertových problémů předložil David Hilbert v roce 1900 ve své přednášce *Problémy matematiky* na druhém mezinárodním kongresu matematiků v Paříži. Uvedené problémy představovaly tehdy největší nevyřešené otázky v matematice. Dnes je již většina vyřešena a jejich řešení významně ovlivnilo matematiku 20. století.

Jak už jsme zmínili výše, Hilbert zformuloval 23 matematických problémů, které bylo třeba zodpovědět. Jelikož je ale tato práce věnována diofantovským rovnicím, je zřejmé, že nás bude zajímat právě desátý Hilbertův problém. V předešlých kapitolách jsme se věnovali různým typům diofantovských rovnic, při jejichž řešení jsme využívali složitějšího a možná tedy i zdlouhavého postupu. Pro jednodušší práci s těmito rovnicemi by bylo vhodné nejprve zjistit, jestli daná rovnice řešení má či naopak. Postup, který by nám umožnil zjistit existenci či neexistenci řešení, by nám usnadnil mnohdy zbytečné a dlouhé výpočty. Této problematice se věnuje zmíněný desátý Hilbertův problém. Týká se otázky, zda existuje obecný algoritmus, který je schopen určit pro libovolnou diofantovskou rovnici, zda má řešení v celých číslech. Ačkoliv byly diofantovské rovnice důkladně studovány už od starověku, nebyl takový algoritmus znám ani na sklonku 19. století.

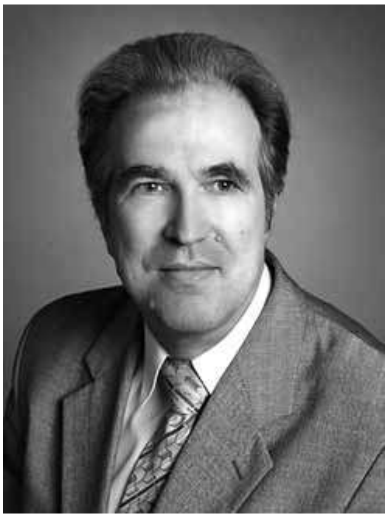
Podle [3] může být problém zformulován například takto: Požaduje se udání metody, která by pro každou diofantickou rovnici umožnila po konečném počtu kroků rozhodnout, zda daná rovnice má řešení. Diofantickou rovnicí míníme rovnici tvaru

$$P(x_1, \dots, x_n) = 0,$$

kde P je polynom s celočíselnými koeficienty v proměnných $x_1, \dots, x_n$. Řešením rovnice pak rozumíme každou n-tici celých čísel $(x_1, \dots, x_n)$, která anuluje polynom P.

Podívejme se například na rovnici $xy^2 - 2y + x^2 - 1 = 0$, která řešení má, a to například $x = 1, y = 2$. Dále například rovnice $u^4 + u^2v^2 + 1 = 0$ žádné řešení nemá.

Desátý Hilbertův problém byl vyřešen v roce 1970, tedy celkem nedávno. Postupně rozvíjející se matematická logika a teorie algoritmů a rekursivních funkcí přinesly potřebné pojmy i důkazové postupy. Tím dále umožnily matematicky se zabývat podobnými otázkami o existenci algoritmů pro řešení různých úloh. Vyřešení tohoto problému by tedy nebylo možné bez práce různých matematiků, kteří podstatně přispěli k rozvoji matematické logiky a teorie rekursivních funkcí. Velkého pokroku dosáhli například američtí matematikové J. Robinsonová, M. Davis a H. Putnam. Poslední krok důležitý pro úplné vyřešení problému udělal mladý matematik J. V. Matijasevič. Mimo jiné se stal držitelem první ceny mezinárodní matematické olympiády z r. 1964.



Obrázek 2 – J. V. Matijasevič (*1947), [10]

Stručně řečeno z prací ostatních zmíněných matematiků vyplývalo, že k negativní odpovědi na desátý problém stačí odpovědět kladně na tuto otázku:

Je pravda, že pro nějaké m existuje polynom $P(x, y, z, u_1, \dots, u_m)$ s celočíselnými koeficienty takový, že pro všechna přirozená x, y, z platí

$$z = x^y \Leftrightarrow (\exists u_1, \dots, u_m)\, P(x, y, z, u_1, \dots, u_m) = 0\ ?$$

Jinými slovy: je predikát $z = x^y$ diofantický?

Tuto otázku se Matijasevičovi podařilo zodpovědět kladně a tak se mnohaleté úsilí matematiků pracujících na vyřešení desátého problému dobralo k závěru. K vysvětlení jeho důkazu bychom zde museli definovat mnoho pojmů, což by přesahovalo tuto diplomovou práci. Čtenář, který se o tuto problematiku více zajímá, se může o tomto důkazu více dočíst např. na WWW:

http://dml.cz/bitstream/handle/10338.dmlcz/138822/PokrokyMFA_18-1973-4_2.pdf.

5 ŘEŠENÍ DIOFANTOVSKÝCH ROVNIC V PROGRAMU MATHEMATICA

V předchozí kapitole jsme pochopili, že spoléhat se na pomoc počítačových programů při řešení diofantovských rovnic obecně nemůžeme. Desátý Hilbertův problém totiž skončil překvapivým závěrem: neexistuje ani algoritmus, který by umožnil rozhodnout o řešitelnosti zadané diofantovské rovnice, natož o tom, jak případně vypadá množina jejích řešení. Můžeme si ale aspoň otestovat několik jednodušších diofantovských rovnic studovaných v této práci a zjistit, jak to vypadá s řešením těchto konkrétních ukázek.

V programu <u>*Mathematica 8*</u> je k dispozici povel **`Reduce`**. Ten obecně slouží k řešení rovnic a nerovnic a je zde možnost zadat si obor, ve kterém má být zadaný problém řešen. Možností využití tohoto povelu je mnoho, nás však bude zajímat, že volba **`Reduce[`*`expr`*`, `*`vars`*`, Integers]`** zkusí vyřešit diofantovskou rovnici nad množinou celých čísel. Právem ovšem můžeme očekávat, že dostaneme obecné řešení lineární diofantovské rovnice o dvou neznámých. Kupř. po zadání

```
Reduce[2x+3y==7,{x,y},Integers]
```

obdržíme

```
C[1]∈ Integers &&x== 2 + 3 C[1]&&y==1 - 2 C[1].
```

To je ve shodě s „lidským“ výpočtem, možná je jen někdo zvyklý značit celočíselný parametr písmenem *t* a nikoli `C[1]`. Poznamenejme, že volbou **`Integers`** si zadáme, že se má daný problém řešit v množině celých čísel.

Ve značné části diplomové práce jsme řešili příklady na Pellovu rovnici. Všimli jsme si, že množina řešení je nekonečná. Jak se tedy vyrovná program Mathematica kupř. s rovnicí $x^2 - 5y^2 = 1$, kterou jsme řešili na str. 12 - 16? Zadáme-li

```
Reduce[x^2-5y^2==1,{x,y},Integers],
```

dostaneme dosti nepřehlednou formuli:

$$(C[1]\in \text{Integers} \&\& C[1]\geq 0 \&\& x==1/2\ \ (-(9-4\sqrt{5})^{C[1]}-(9+4\sqrt{5})^{C[1]})$$

&&y==-(((9-4$\sqrt{5}$)$^{C[1]}$-(9+4$\sqrt{5}$)$^{C[1]}$)/(2$\sqrt{5}$)))||(C[1]∈ Integers &&C[1]≥0&&x==1/2(-(9-4$\sqrt{5}$)$^{C[1]}$-(9+4$\sqrt{5}$)$^{C[1]}$)&&y==((9-4$\sqrt{5}$)$^{C[1]}$-(9+4$\sqrt{5}$)$^{C[1]}$)/(2$\sqrt{5}$))||(C[1]∈ Integers &&C[1]≥0 &&x==1/2 ((9-4$\sqrt{5}$)$^{C[1]}$+(9+4$\sqrt{5}$)$^{C[1]}$)&&y==-(((9-4$\sqrt{5}$)$^{C[1]}$-(9+4$\sqrt{5}$)$^{C[1]}$)/(2$\sqrt{5}$))) ||(C[1]∈Integers &&C[1]≥0&&x== 1/2 ((9-4$\sqrt{5}$)$^{C[1]}$+(9+4$\sqrt{5}$)$^{C[1]}$) &&y==((9-4$\sqrt{5}$)$^{C[1]}$-(9+4$\sqrt{5}$)$^{C[1]}$)/(2$\sqrt{5}$))

a ani se nedivíme. Zapsat onu nekonečnou množinu řešení není jednoduché a zpětně luštit obdobnou formuli také ne. Můžeme alespoň projít náš výpočet a nechat si zkontrolovat, zda jsme vyčíslili dobře periodický řetězový zlomek pro $\sqrt{5}$:

ContinuedFraction[Sqrt[5]]

{2,{4}}.

To je v pořádku, souhlasí to s našimi výpočty ze str. 13. Nekonečný řetězový zlomek příslušný číslu $\sqrt{5}$ je periodický s periodou $k = 1$ a má tvar $[2;\ 4, 4, \dots]$.

Dále nám nevyhovuje výše zmiňovaná „nepřehledná" formule. Pokusme se tedy najít relativně „malá" řešení jinak:

FindInstance[x^2-5y^2==1 &&1 < x < 100,{x,y},Integers]

{{x→9,y→4}}.

Řekněme si, co v daném případě vykoná povel **FindInstance.** Nachází jedno řešení předepsané Pellovy rovnice, vyhovující daným podmínkám, tj. s relativně malou souřadnicí x. Chceme řešení víc? Zapišme např.

Reduce[x^2 - 5y^2 == 1 && 0 < x < 2 000 000 && y > 0, {x,y}, Integers]

a dostaneme (symbol || značí logickou spojku pro disjunkci $\vee$)

(x==9&&y==4)||(x==161&&y==72)||(x==2889&&y==1292)||(x==51841&&y==23184)||(x==930249&&y==416020).

Můžeme si tak zkontrolovat výsledky z tab. 5.

Pro zajímavost ještě zkontrolujme jedno naše řešení zobecněné Pellovy rovnice. Nepůjde nám o zápis pomocí obecné a nepřehledné formule, ale o nalezení jistého počtu řešení.

```
Reduce[x^2 - 20y^2==721&&0<x<2000000&&y>0,{x,y},Integers]
```

```
(x==29&&y==1)||(x==61&&y==5)||(x==71&&y==6)||(x==199&&y==18)||(x==4
39&&y==40)||(x==1271&&y==116)||(x==1501&&y==137)||(x==4349&&y==39
7)||(x==9629&&y==879)||(x==27901&&y==2547)||(x==32951&&y==3008)||
(x==95479&&y==8716)||(x==211399&&y==19298)||(x==612551&&y==55918)
||(x==723421&&y==66039)
```

Vidíme, že Mathematica ve verzi 8 „umí“ řešit i diofantovské rovnice druhého stupně ve dvou neznámých. Obecné řešení však zapisuje poměrně komplikovanou formulí a chceme-li poznat více, je dobré znát teorii.

V případě diofantovských rovnic vyšších stupňů bychom někdy mohli být zklamáni získaným výsledkem, kdybychom ovšem nevěděli, jak je řešení obdobných rovnic obtížné:

```
Reduce[x^2+y^2==z^3,{x,y,z},Integers]
```

(x|y|z)∈Integers&&z==Root[$-x^2-y^2+\#1^3$&,1]

Dostali jsme nic neříkající odpověď. Zkusme proto

```
FindInstance[x^2+y^2==z^3&&10<x<20,{x,y,z},Integers]
```

a dostaneme alespoň

{{x→11,y→2,z→5}}.

Připomeňme, že na str. 45 - 48 jsme řešili rovnici $x^2 + 4 = y^3$ a zjistili jsme, že má právě čtyři řešení. Jedno z nich jsme nalezli výše (a je ovšem možné experimentovat dále).

6 ZÁVĚR

Hlavním cílem této diplomové práce je rozšíření souboru řešených rovnic a některé historicky významné diofantovské rovnice. V první části je nejprve uvedeno několik úloh z matematické olympiády, které se řeší pomocí diofantovských rovnic.

Druhá část představuje Pellovu rovnici, zobecněnou Pellovu rovnici a pythagorejskou rovnici a naplňuje tak hlavní cíl práce. Postup řešení každého zmíněného typu rovnic je vždy podrobně vysvětlen. Nejprve jsou uvedeny potřebné věty a definice, poté je vše demonstrováno na konkrétních příkladech. Vysvětlení je na úrovni, které by měl rozumět i čtenář, jenž se v minulosti diofantovskými rovnicemi nezabýval.

Další část práce představuje desátý Hilbertův problém. Kapitola se zmiňuje o znění tohoto problému, o významných osobnostech s ním spjatých a také o jeho vyřešení. Problém žádal nalezení obecného algoritmu, který by určil, zda je jakákoliv diofantovská rovnice řešitelná či nikoliv. Jak se po čase zjistilo, je tento problém neřešitelný a algoritmus, který by práci s řešením usnadnil, tedy neexistuje.

Poslední kapitola představuje počítačový program Mathematica jako nástroj k řešení diofantovských rovnic. Na jednoduchých ukázkách čtenář pozná, jak si pomocí tohoto programu své výpočty kontrolovat.

7 SEZNAM OBRÁZKŮ

8 SEZNAM TABULEK

9 SEZNAM LITERATURY

[1] BICAN, L.: ***O řešení Pellovy rovnice.*** Rozhledy matematicko fyzikální, roč. 56, (1977 - 1978), č. 5, str. 193 – 198.

[2] BICAN, L.: ***Zobecněná Pellova rovnice.*** Rozhledy matematicko fyzikální, roč. 56, (1977 - 1978), č. 6, str. 257 – 261.

[3] HAVEL, Ivan M.: ***O desátém Hilbertově problému.*** [online]. [cit. 2012-04-22] Dostupné na WWW: <http://dml.cz/bitstream/handle/10338.dmlcz/138822/Pokroky MFA_18-1973-4_2.pdf>.

[4] SCHWARZ, Štefan: ***Algebraické čísla.*** Praha: Přírodovědecké nakladatelství, 1950.

[5] Vasiljev, N. B., Gutenmacher, V. L., Rabbot, Ž. M., Toom, A. L.: ***Zaočnyje matematičeskije olympiády***. Bibliotečka Kvant, Moskva, 2012.

[6] ***David Hilbert*****.** [online]. [cit. 2012-04-22] Dostupné na WWW: <http://www-history.mcs.st-and.ac.uk/Biographies/Hilbert.html>.

[7] ***Diofantovská rovnice*****.** [online]. [cit. 2012-06-12] Dostupné na WWW: <http://cs.wikipedia.org/wiki/Diofantick%C3%A1_rovnice>.

[8] ***Hilbertovy problémy*****.** [online]. [cit. 2012-04-22] Dostupné na WWW: <http://cs.wikipedia.org/wiki/Hilbertovy_probl%C3%A9my>.

[9] ***Pythagorejská trojice*.** [online]. [cit. 2012-04-01] Dostupné na WWW: <http://cs.wikipedia.org/wiki/Pythagorejsk%C3%A1_trojice>.

[10] ***Yuri Vladimirovich Matiyasevich*.** [online]. [cit. 2012-05-10] Dostupné na WWW: <http://www-history.mcs.st-and.ac.uk/Mathematicians/Matiyasevich.html>.

10 RESUMÉ

The main object of this diploma thesis is acquainting the reader with some historically significant Diophantine equations. There is explained Pell's equation, generalized Pell's equation and Pythagorean equation. All facts are presented with examples. This thesis deals with examples of mathematical Olympiad, where the Diophantine equations are used. It describes the tenth Hilbert's problem and its solution too. The last part of this thesis explains work with computer program Mathematica and it is devoted to practical examples of solutions to equations with this program.