ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

VYBRANÉ TYPY DIOFANTICKÝCH ROVNIC A JEJICH POČETNÍ VYUŽITÍ

BAKALÁŘSKÁ PRÁCE

Martina Bláhová
Matematická studia, obor Ma-Fy

Vedoucí práce: Mgr. Lukáš Honzík, Ph.D.

Plzeň, 2015

Prohlášení:

„Prohlašuji tímto, že jsem bakalářskou práci na téma „Vybrané typy diofantických rovnic a jejich početní využití“ zpracovala sama a využila pouze pramenů uvedených v seznamu literatury této bakalářské práce.”

V Plzni, dne 15. dubna 2015

....

Martina Bláhová

Poděkování:

Ráda bych poděkovala vedoucímu práce Mgr. Lukáši Honzíkovi, Ph.D. za inspirativní podněty a odbornou pomoc při psaní bakalářské práce.

VYBRANÉ TYPY DIOFANTICKÝCH ROVNIC A JEJICH POČETNÍ VYUŽITÍ

SELECTED TYPES OF DIOPHANTINE EQUATIONS AND THEIR NUMERICAL USE

OBSAH

Úvod

V bakalářské práci na téma „Vybrané typy diofantických rovnic a jejich početní využití“ se budeme věnovat typům diofantických rovnic, které byly v historii objeveny. Jednotlivé typy teoreticky popíšeme, větší část práce bude obsahovat řešení konkrétních příkladů, aplikaci v praxi a jejich použitelnost ve výuce na školách. Cílem bakalářské práce je pochopit teoretickou podstatu jednotlivých typů diofantických rovnic a osvojit si základní principy řešení příkladů, jež se pokusíme zkonstruovat.

V úvodu práce se seznámíme s řeckým matematikem Diofantem, který přinesl základy těchto rovnic. Následně projdeme nejjednodušší typ diofantických rovnic, a to lineární diofantické rovnice, ke kterým nás dovedou slovní úlohy ze základních škol. Jako motivační příklad můžeme uvést: „Na parkovišti parkují motorky a auta, přičemž hlídač spočítal, že se na parkovišti nachází celkem 28 kol. Zjistěte, kolik hlídal aut a kolik motorek.“ V další kapitole nás budou zajímat diofantické rovnice 2. stupně, tedy kvadratické diofantické rovnice, mezi něž patří speciální typy jako pythagorejská rovnice, Pellova rovnici a zobecněná Pellova rovnice. U vyšších stupňů diofantických rovnic se zmíníme pouze o problému zvaném Velká Fermatova věta.

1 POJEM DIOFANTICKÉ ROVNICE

Diofantická rovnice byla pojmenována po Diofantu Alexandrijském, který žil ve starověkém Řecku kolem 3. století před naším letopočtem. Původně řešil rovnice v oboru racionálních čísel. Dnešní název diofantické rovnice představuje neurčité polynomiální rovnice, které jsou řešitelné v oboru celých (přirozených) čísel.

Obecně lze diofantickou rovnici napsat ve tvaru

$$f(x_1, x_2, \dots, x_n) = 0,$$

kde f je polynom $x_1, x_2, \dots, x_n$ s celočíselnými koeficienty. Řešením bude každá n-tice $[a_1, a_2, \dots, a_n]$, která nuluje polynom f.

1.1 DIOFANTŮV ŽIVOT

Diofantos Alexandrijský (Διόφαντορ ὁ Ἀλεξανδπεύρ), po kterém jsou diofantické rovnice pojmenované, žil dle dochovaných děl a pozůstatků kolem roku 250 n. l. ve starověkém Řecku. O jeho životě toho příliš nevíme, dochoval se však náhrobek, z kterého lze spočítat délku jeho života.

Epigram: (Kolman, 1969)

… Šestinu života dopřál mu bůh být chlapcem.

Za dvanáctinu života pak narostly mu vousy.

K tomu sedmina, když uzavřel sňatek manželský.

Po pěti letech vzešel z toho spojení syn.

Běda, dítě tak milované dožilo se poloviny let otcových,

Když ho Hades strašlivý povolal k sobě.

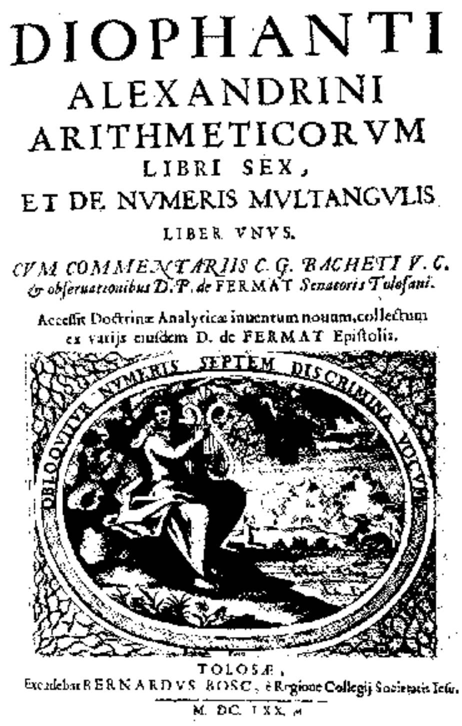
Ještě čtyři léta snášel Diofantos bolest, věnuje se vědě…

Jestliže délku Diofantova života označíme x, potom lze sestavit rovnici ve tvaru

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x,$$

jejímž řešením je $x = 84$ let.

1.2 DIOFANTOVO DÍLO


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Obrázek 1 - "Aritmetika", [1]

Diofantovo nejrozsáhlejší matematické dílo s názvem „Aritmetika“ se skládalo z 13 knih, z nichž se dochovalo pouze šest. V tomto souboru knih definuje neurčené množství jednotek jako neznámou x, kterou nazývá „číslo“. Zabýval se také převrácenou hodnotou neznámé x, a jejími až šestými mocninami. Ve své symbolice neměl znak pro sčítání, násobení ani dělení, speciální znak používal pro odčítání. V knize řeší obecné určité rovnice, lineární rovnice, kvadratické rovnice a speciální typ kubické rovnice. Ve svých propočtech se věnoval pouze kladným racionálním číslům, což je v rozporu s tím, že dnes při řešení „diofantických rovnic“ hledáme celočíselné řešení. Není jasné, zda o záporných kořenech některých rovnice věděl. V díle „Aritmetika“ řeší Diofantos také konstrukční úlohy o pravoúhlých trojúhelnících.

Mezi další díla patří pojednání o „polygonálních číslech“, „Porismata“ a „Moriastika“, o kterých se autor zmínil pouze v díle „Aritmetika“ a obsah není znám.

Mezi rozsáhlé zdroje Diofantova aritmeticko-algebraického poznání se dá zařadit práce Herona, jenž žil v 1. st. n. l. Ten ve svém díle naznačuje myšlenku počítání neurčitých rovnic, nicméně řešení vždy provádí na konkrétních číslech. Ve svém díle navazuje také na staročínskou literaturu, konkrétně na dílo „Matematika v devíti knihách“, kde jsou řešeny pythagorejské neurčité rovnice. Dále na Pellovy rovnice (později Fermatovy rovnice) a na známou Archimedovu úlohu o dobytku. Všechny tyto typy úloh budou probrány v následujících kapitolách mé práce.

1.3 ZÁKLADNÍ TYPY DIOFANTICKÝCH ROVNIC

Existuje mnoho typů diofantických rovnic a problémů:

a) Lineární diofantické rovnice (diofantické rovnice 1. stupně)

Rovnice mají tvar $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, kde koeficienty $a_1, a_2, \dots, a_n, c \in Z$. S lineárními diofantickými rovnicemi se lidé setkávají denně. Nevědomky je řeší i děti v mateřských školách a jsou pouze přepisem běžných situací do jazyka matematiky.

b) Diofantické rovnice 2. stupně

b.1) kvadratická diofantická rovnice

Kvadratickou diofantickou rovnicí o dvou neznámých x, y rozumíme rovnici $ax^2 + bx + cxy + dy + ey^2 = f$, kde $a, b, c, d, e, f \epsilon Z$. Řešením rovnice je každá uspořádaná dvojice $[x, y] \epsilon Z^2$. Pro rovnice tohoto typu neexistuje jednotný algoritmus pro získání řešení.

b.2) Pellova rovnice

Pellova rovnice je speciálním typem kvadratické diofantické rovnice o 2 neznámých. Má tvar $x^2 - Ay^2 = 1$, kde A je přirozené číslo, které není přirozenou mocninou žádného přirozeného čísla.

b.3) zobecněná Pellova rovnice

Obecný tvar zobecněné Pellovy rovnice je $\mathrm{x}^2 - \mathrm{Ay}^2 = \mathrm{C}$, kde A je přirozené číslo, které není přirozenou mocninou žádného přirozeného čísla a $C \epsilon Z$.

b.4) Pythagorejská rovnice

Pythagorejská rovnice má tvar $x^2 + y^2 = z^2$, kde $x, y, z \epsilon Z$; $x, y, z > 0$; $D(x, y) = 1$ a x je sudé. V praxi hledá celočíselné délky stran pravoúhlého trojúhelníka. Výsledkem je tzv. pythagorejská trojice, která je popsána jako $x = 2ab$, $y = b^2 - a^2$, $z = a^2 + b^2$, kde $0 < a < b$; $a, b \epsilon N$; a, b jsou nesoudělná čísla různé parity.

c) <u>Vyšší stupně diofantických rovnic</u>

c.1) Velká Fermatova věta

Velká Fermatova věta je vlastně Pythagorejská rovnice tvaru $x^n + y^n = z^n$, kde $n \geq 3, x \geq 1, y \geq 1, z \geq 1$. Přes 350 let trvalo matematikům dokázat, že neexistují přirozená čísla, která tuto rovnici řeší.

1.4 DESÁTÝ HILBERTŮV PROBLÉM

Obrázek 2 - David Hilbert, [2]

David Hilbert (1862 – 1943) byl profesorem matematiky a působil na přelomu 19. a 20. století v Německu. V bakalářské práci se o něm zmiňujeme proto, že na druhém mezinárodním kongresu matematiků v Paříži v roce 1900 předložil 23 tzv. Hilbertových problémů, z nichž desátý se věnuje diofantickým rovnicím. Hilbertovy problémy jsou otázky různých matematických oblastí, na něž bylo potřeba odpovědět. Desáty Hilbertův problém se zabývá otázkou, zda existuje obecný algoritmus o konečném počtu kroků jak určit, zda jakákoli diofantická rovnice má či nemá řešení. Problémem se zabývalo mnoho matematiků, avšak až v roce 1970 dokázal ruský matematik Jurij Vladimirovič Matijasevič, že obecný algoritmus neexistuje.

2 LINEÁRNÍ DIOFANTICKÉ ROVNICE

Obecná lineární diofantická rovnice má tvar

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \qquad (2.1)$$

kde koeficienty $a_1, a_2, \dots, a_n \in Z$, stejně jako $c \in Z$. Řešením je uspořádaná n-tice $[x_1, x_2, \dots, x_n] \in Z \times Z \times \dots \times Z$, která nuluje levou stranu rovnice (2.1). Nutnou podmínku řešitelnosti rovnice (2.1) v oboru celých čísel definujme vztahem

$$D = D(a_1, a_2, \dots, a_n) \wedge D|c,$$

neboli číslo c musí být dělitelné největším společným dělitelem čísel $a_1, a_2, \dots, a_n$.

2.1 LINEÁRNÍ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH

Lineární neurčitou rovnicí o 2 neznámých x, y (Bezoutovou rovnicí, tj. obecnou lineární diofantickou rovnici pro $n = 2$) budeme rozumět rovnici ve tvaru

$$ax + by = c, \qquad (2.1.1)$$

kde $a, b, c \in Z - \{0\}$; $x, y \in Z$. Aby rovnice (2.1.1) měla řešení v oboru celých čísel, musí být splněna nutná podmínka řešitelnosti a to, aby největší společný dělitel čísel a, b dělil zároveň číslo c. Matematicky zapsáno předpisem (2.1.2).

$$D = D(a, b) \wedge D|c \qquad (2.1.2)$$

Příkladem lineární diofantovské rovnice, která nemá řešení je $12x - 6y = 7$ (v tomto případě je $D = 6$ a $6 \nmid 7$).

Pokud vezmeme v úvahu rovnici (2.1.1) a splníme-li předpoklady vztahu (2.1.2), jsme schopni odvodit obecné řešení lineární diofantovské rovnice o dvou neznámých. Odvození začneme vydělení rovnice (2.1.1) největším společným dělitelem D a získáme tvar

$$(a:D)x + (b:D)y = c:D.$$

Pro určité x', y' platí, že rovnici lze zapsat jako

$$(a:D)x' + (b:D)y' = 1. \qquad (2.1.3)$$

Pokud vynásobíme vztah (2.1.3) číslem $(c:D)$, existují konkrétní řešení x_0, y_0, která vyhovují rovnici (2.1.4).

$$(a:D)(c:D)x' + (b:D)(c:D)y' = c:D \qquad (2.1.4)$$

Po vynásobení číslem D dostaneme

$$(a:D)cx' + (b:D)cy' = c.$$

Po dalších úpravách vznikne rovnice ve tvaru

$$a(c:D)x' + b(c:D)y' = c,$$

která v případě, že $x_0 = (c:D)x'$ a $y_0 = (c:D)y'$ je obecným řešení lineární neurčité rovnice. Tedy

$$ax_0 + by_0 = c. \qquad (2.1.5)$$

<u>Věta 1:</u> (další řešení)

V případě, že bychom hledali další řešení x, y; $x \neq x_0, y \neq y_0$, platí věta 1: Mějme neurčitou lineární rovnici $ax + by = c$; $a, b, c \in Z; x, y \in Z$, známe-li alespoň jednu dvojici x_0, y_0, která je řešením, potom všechna ostatní řešení popisuje soustava

$$y = y_0 - (a:D)t,$$

$$x = x_0 + (b:D)t,$$

kde $t \in Z$.

<u>Důkaz 1:</u>

Po odečtení rovnice (2.1.5) od rovnice (2.1.1) a vydělením číslem D, získáváme rovnici ve tvaru

$$(a:D) \cdot (x - x_0) = (b:D) \cdot (y_0 - y). \qquad (2.1.6)$$

Z teorie víme, že čísla $(a:D), (b:D)$ jsou nesoudělná. Z toho plyne, že $(y_0 - y)$ musí být dělitelné $(a:D)$. Musí proto existovat nějaké $t \in Z$, pro které platí

$$y_0 - y = t(a:D). \qquad (2.1.7)$$

Tento vztah dosadíme do (2.1.6) a dostaneme

$$(a:D) \cdot (x - x_0) = (b:D) \cdot t(a:D),$$

což lze upravit na tvar

$$x - x_0 = (b:D)t. \qquad (2.1.8)$$

Ze vztahů (2.1.7) a (2.1.8) nyní jednoduše vyjádříme všechna řešení rovnice jako

$$y = y_0 - (a:D)t, \text{ kde } t \in Z,$$

$$x = x_0 + (b:D)t, \text{ kde } t \in Z.$$

Lineární diofantické rovnice o dvou neznámých lze řešit pomocí lineární kongruence, jak je uvedeno v metodách jejich řešení. Souvislost udává následující definice a tvrzení (Demlová, 2005).

Definice:

Je dáno přirozené číslo $b > 1$. Řekneme, že celá čísla a, c jsou kongruentní modulo b, píšeme $a \equiv c \pmod{b}$, právě tehdy, když jejich rozdíl $a - c$ je dělitelný číslem b.

Tvrzení:

Kongruence $a \equiv c \pmod{b}$ má řešení právě tehdy, když číslo c je násobkem největšího společného dělitele čísel a a b. V takovém případě najdeme všechna čísla x jako řešení diofantické rovnice $ax + by = c$.

Příklad 1: (lineární diofantická rovnice – kongruence)

Řešte rovnici $15x + 16y = 20$ pomocí kongruence.

Řešení 1:

Rovnici $15x + 16y = 20$ lze rozdělit na dva případy a každý řešit zvlášť pomocí kongruence. Pokud vyjádříme y z kongruence $16y \equiv 20 \pmod{15}$ podle předchozího tvrzení o kongruenci a dosadíme do diofantické rovnice, získáme řešení.

$$16y \equiv 20 \pmod{15}$$
$$y \equiv 5 \pmod{15}$$
$$y = 5 + 15k$$

$$15x + 16(5 + 15k) = 20$$
$$15x + 240k = -60$$
$$x = -4 - 16k$$

Řešením je uspořádaná dvojice $[-4 - 16k; 5 + 15k]$; kde $k \in Z$.

k	x	y
…	…	…
-1	12	-10
0	-4	5
1	-20	20
…	…	…

Tabulka 1

2.2 LINEÁRNÍ DIOFANTICKÉ ROVNICE O TŘECH NEZNÁMÝCH

Analogicky jako pro dvě neznámé lze ukázat, že podmínkou řešitelnosti lineární diofantické rovnice o třech neznámých ve tvaru

$$ax + by + cz = d,$$

kde $a, b, c, d \in Z$; $x, y, z \in Z$ a a, b, c jsou nenulová čísla v oboru celých čísel, je, aby největší společný dělitel čísel a, b, c dělil zároveň číslo d. Matematicky zapsáno

$$D = D(a, b, c) \wedge D|d.$$

2.3 METODY ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

2.3.1 ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC O 2 NEZNÁMÝCH

Metod pro řešení lineárních diofantovských rovnic o dvou neznámých existuje mnoho. Od experimentálních výpočtů, přes řešení pokusem, dosazovací metodou či klasické algebraické řešení. Možnosti řešení takových rovnic si ukážeme na následujícím příkladu 2.

Příklad 2: (lineární diofantická rovnice – slovní úloha)

Mějme dva druhy akvárií. První akvárium má objem menší než 10 litrů, označme ho x. Druhé akvárium je větší, jeho objem označme y. Závislost jejich objemů má tvar lineární diofantovské rovnice: $12x - 7y = 10$.

Řešení 2:

Řešení pokusem pomocí tabulky:

Do tabulky zaneseme možné hodnoty čísla x, spočteme dvanáctinásobek x, dopočítáme zbytek pro hodnotu $7y$, ze které odvodíme možné celočíselné výsledky.

x<10	1	2	3	4	5	6	7	8	9
12x	12	24	36	48	60	72	84	96	108
7y	2	14	26	38	50	62	74	86	98
y	-	2	-	-	-	-	-	-	14

Tabulka 2

Z tabulky 2 vidíme, že dle všech zadaných parametrů vyhovují pouze $x = 9; y = 14$. Dvojice $x = 2; y = 2$ nemůže být řešením zadané úlohy, neboť má být $y > x$.

Řešení kongruencí:

Rovnici $12x - 7y = 10$ lze rozdělit na dva případy a každý řešit zvlášť pomocí kongruence. První kongruence bude mít tvar $-7y \equiv 10\, mod(12)$ a druhá $12x \equiv 10\, mod(7)$.

$$12x - 7y = 10$$
$$-7y \equiv 10\, mod(12)$$
$$5y \equiv 10\, mod(12)$$
$$y = 2 + 12k$$

Výsledek dosadíme do zadané rovnice a dostaneme

$$12x - 7(2 + 12k\ ) = 10,$$
$$x = 2 + 7k.$$

Řešením je uspořádaná dvojice $[2 + 7k; 2 + 12k]$; kde $k \in Z$.

$\boldsymbol{k}$	$\boldsymbol{x}$	$\boldsymbol{y}$
$k < 0$	$x < 0$	$y < 0$
$k = 0$	2	2
$k = 1$	9	14
$k = 2$	16	26

Tabulka 3

Zadání vyhovuje pouze hodnota $k = 1$, řešení je tedy $x = 9; y = 14$.

Řešení dosazovací metodou:

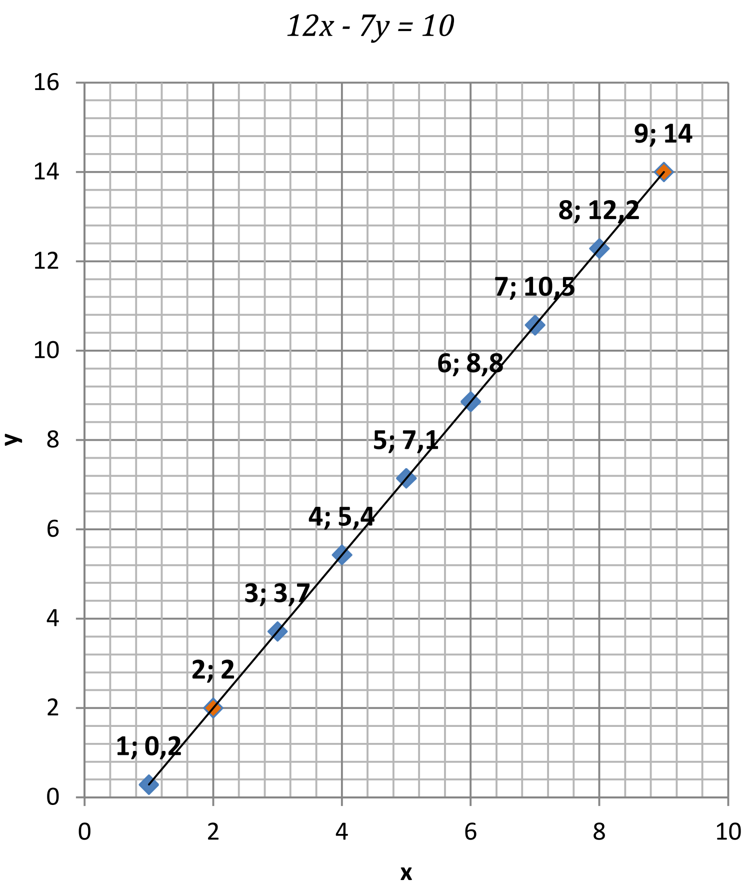
V případě dosazovací metody je potřeba ověřit nutnou podmínku řešitelnosti (2.1.2) z kapitoly Lineární diofantické rovnice o dvou neznámých. Řešení existuje, neboť $D(12,7) = 1 \wedge 1|10$. Rovnici $12x - 7y = 10$ upravíme tak, aby každá její strana obsahovala pouze jednu neznámou. Tvar této rovnice je $12x = 10 + 7y$. Za y nyní budeme zkoušet dosazovat celá čísla do té doby, než výsledek pravé strany rovnice bude celočíselným násobkem dvanáctky. Tento princip je zobrazen v následující tabulce, ze které je vidět, že výsledkem je uspořádaná dvojice $x = 9; y = 14$. Uspořádaná dvojice $x = 2; y = 2$ jsou sice řešením dané rovnice, nevyhovují však zadané podmínce, že $y > x$.

y	$10 + 7y$	dělitelnost	x
1	17	$12 \nmid 17$	–
2	24	$12 \mid 24$	2
3	31	$12 \nmid 31$	–
4	38	$12 \nmid 38$	–
5	45	$12 \nmid 45$	–
6	52	$12 \nmid 52$	–
7	59	$12 \nmid 59$	–
8	66	$12 \nmid 66$	–
9	73	$12 \nmid 73$	–
10	80	$12 \nmid 80$	–
11	87	$12 \nmid 87$	–
12	94	$12 \nmid 94$	–
13	101	$12 \nmid 101$	–
14	108	$12 \mid 108$	9

Tabulka 4

Grafické řešení:

Pokud znázorníme rovnici $12x - 7y = 10$ do grafu, jsou výsledky v místech, kde souřadnice bodu x, y současně náleží oboru přirozených čísel. Jak můžeme vidět, jsou to dvojice $x = 9; y = 14$ a $x = 2; y = 2$. Dvojice o souřadnicích $x = 2; y = 2$ nevyhovuje podmínce $y > x$, proto není tato dvojice řešením zadané úlohy. V grafu jsou vidět i jiná řešení, která však nesplňují definici diofantických rovnic, jejichž řešení náleží oboru celých čísel (potažmo v takto zadané slovní úloze přirozeným číslům).



Graf 1 – grafické řešení lineární diofantické rovnice

Algebraické řešení:

Nejprve ověříme nutnou podmínku řešitelnosti, tj. vztah (2.1.2) z předchozí kapitoly. Rovnice je řešitelná, protože $D(12,7) = 1 \wedge 1|10$. Provedeme Euklidův rozklad čísel a, b.

$$12 = 1 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Číslo 1 lze tedy zapsat následovně.

$$1 = 5 - 2 \cdot 2 = 1 \cdot 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 = 3(12 - 1 \cdot 7) - 2 \cdot 7$$
$$1 = 3 \cdot 12 - 5 \cdot 7$$

Číslo c z diofantické rovnice je desetkrát větší než číslo 1, vynásobíme tedy rozklad číslem 10.

$$10 = 30 \cdot 12 - 50 \cdot 7$$

Koeficienty x_0, y_0 před čísly a, b jsou jedním řešením zadané rovnice.

$$x_0 = 30, y_0 = 50$$

Obecné řešení získáme dosazením do rovnic $x = x_0 + (b : D)t$, $y = y_0 - (a : D)t$, kde $t \in Z$:

$$x = 30 - (7 : 1)t,$$

$$y = 50 - (12 : 1)t.$$

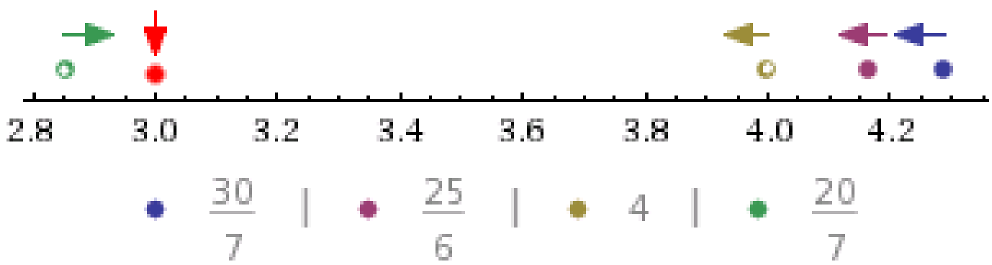
Tyto rovnice musí dle zadání splňovat následující vztahy, ze kterých jsme schopni určit hodnotu celočíselného parametru t.

$$x \geq 0: \qquad 30 - 7t \geq 0 \qquad t \leq \frac{30}{7}$$

$$y \geq 0: \qquad 50 - 12t \geq 0 \qquad t \leq \frac{50}{12}$$

$$x < y: \qquad 30 - 7t < 50 - 12t \qquad t < \frac{20}{5}$$

$$x < 10: \qquad 30 - 7t < 10 \qquad t > \frac{20}{7}$$



Obrázek 3 - číselná osa, [3]

Z grafického znázornění vyplývá, že parametr t musí být roven 3. Parametr dosadíme do předpisů a získáme výsledné hodnoty $x = 9; y = 14$. Menší akvárium má objem 9 litrů a větší akvárium 14 litrů.

Řešení vyjádřením členu s nejmenším koeficientem:

Lineární diofantickou rovnici o dvou neznámých lze řešit osamostatněním členu s menším z koeficientů, v našem případě y. Dostaneme tedy vyjádření

$$y = \frac{12x-10}{7} = 1 - x + \frac{19x-17}{7}.$$

Protože řešením diofantické rovnice jsou celá čísla, musí $\frac{19x-17}{7} \in Z$ a lze tedy položit $\frac{19x-17}{7} = t$, kde $t \in Z$. Z tohoto vztahu vidíme, že $x = \frac{7t+17}{19}$, což můžeme dosadit do původního vztahu. Získáme rovnici

$$y = 1 - \frac{7t+17}{19} + t.$$

Pokud tento vztah upravíme, získáme $y = \frac{12t+2}{19}$. Řešením rovnice je množina uspořádaných dvojic $\left[\frac{7t+17}{19}; \frac{12t+2}{19}\right]; t \in Z$.

t	**x**	**y**
1	$\frac{23}{19}$	$\frac{14}{19}$
2	$\frac{31}{19}$	$\frac{26}{19}$
3	$\frac{38}{19} = 2$	$\frac{38}{19} = 2$
4	$\frac{45}{19}$	$\frac{50}{19}$
5	$\frac{52}{19}$	$\frac{62}{19}$
6	$\frac{59}{19}$	$\frac{74}{19}$
7	$\frac{66}{19}$	$\frac{86}{19}$
8	$\frac{73}{19}$	$\frac{98}{19}$
9	$\frac{80}{19}$	$\frac{110}{19}$
10	$\frac{87}{19}$	$\frac{122}{19}$
11	$\frac{94}{19}$	$\frac{134}{19}$
12	$\frac{101}{19}$	$\frac{146}{19}$
13	$\frac{108}{19}$	$\frac{158}{19}$
14	$\frac{115}{19}$	$\frac{170}{19}$
15	$\frac{122}{19}$	$\frac{182}{19}$
16	$\frac{129}{19}$	$\frac{194}{19}$
17	$\frac{136}{19}$	$\frac{218}{19}$
18	$\frac{143}{19}$	$\frac{2}{19}$
19	$\frac{150}{19}$	$\frac{230}{19}$
20	$\frac{157}{19}$	$\frac{242}{19}$
21	$\frac{164}{19}$	$\frac{254}{19}$
22	$\frac{171}{19} = 9$	$\frac{266}{19} = 14$

Tabulka 5

Výsledkem v souladu se zadáním je $x = 9; y = 14$.

2.3.2 ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC O 3 A 4 NEZNÁMÝCH

Stejně jako Bezoutovy rovnice mají lineární diofantické rovnice o 3 či 4 neznámých několik metod pro získání řešení. Řešení se dá samozřejmě získat metodou „pokus-omyl“, algebraickým řešením za pomoci Euklidova rozkladu čísel, řešením pomocí kongruence, nebo osamostatňováním členu s nejmenším koeficientem. Níže uvádím dvě nejzajímavější metody získání výsledků.

<u>Příklad 3:</u> (lineární diofantické rovnice o 3 neznámých)

Mějme k dispozici mince v hodnotách 5, 10 a 20 korun. Najděte možnosti zaplacení částky 300,- Kč, kdy každou musíme alespoň jednou použít.

Označení:
x … počet pětikorun
y … počet desetikorun
z … počet dvacetikorun

<u>Řešení 3:</u>

Příklad 3 budeme řešit metodou vyjádření členu s nejmenším z koeficientů. Sestavená rovnice bude mít tvar $5x + 10y + 20z = 300$. Podmínka řešitelnosti této rovnice v oboru celých čísel je splněna, neboť $D(5, 10, 20) = 5 \wedge 5|300$.

V našem případě je nejmenším koeficientem číslo 5, budeme tedy vyjadřovat neznámou x jako

$$x = \frac{300 - 10y - 20z}{5} = -y - z + 1 + \frac{-5y - 15z + 295}{5}.$$

Protože výsledek hledáme v oboru celých čísel, lze rovnici zapsat ve tvaru

$$x = -y - z + 1 + t, \qquad (2.3.2.1)$$

kde $t = \frac{-5y-15z+295}{5}$, $t \in Z$. Pokud z této substituce vyjádříme neznámou y a dosadíme do rovnice (2.3.2.1), získáme rovnici

$$x = 2z + 2t - 58.$$

Řešením je množina uspořádaných trojic $[2z + 2t - 58; -3z - t + 59; z]; t, z \in Z$, kdy všechna řešení jsou zobrazena v Tabulce 6.

t	z	x	y
16	14	2	1
17	13	2	3
18	12	2	5
18	13	4	2
19	11	2	7

Tabulka 6

Příklad 4: (lineární diofantické rovnice o 4 neznámých)

Do ovocného košíku se vejde 48 plodů jakéhokoli ovoce, které je však roztříděno po balíčcích. Do koše můžeme vkládat jablka balená po 2 kusech, hrušky zabalené po čtveřicích, švestek je v každém balení 16 kusů a třešní se do jednoho pytlíku vešlo 32 kusů. Kolik bude v košíku balení od každého druhu ovoce?

Označení:
x … počet balení jablek
y … počet balení hrušek
z … počet balení švestek
w … počet balení třešní

Řešení 4:

V tomto případě použijeme způsob řešení pomocí kongruence, aplikovanou na rovnici $2x + 4y + 16z + 32w = 48$. Podmínka řešitelnosti rovnice v oboru celých čísel je splněna, protože $D(2, 4, 16, 32) = 2 \ \wedge 2|48$.
V řešení budeme postupně eliminovat neznámé a nahrazovat parametry. Pokud bude v rovnici kongruence n neznámých, za modulo budeme považovat největší společný dělitel z $n - 1$ koeficientů, jejichž velikost je největší.

1. nahrazení x parametrem t a zpětné dosazení

$$2x + 4y + 16z + 32w = 48$$
$$2x + 4y + 16z + 32w \equiv 48 \ (\mathrm{mod}\ 4)$$
$$2x \equiv 0 \ (\mathrm{mod}\ 4)$$
$$2x = 4t$$
$$x = 2t, \text{kde } t \in Z$$
$$4t + 4y + 16z + 32w = 48$$
$$4y + 16z + 32w = 48 - 4t$$

2. nahrazení y parametry t a s a zpětné dosazení

$$4y + 16z + 32w \equiv (48 - 4t)(\mathrm{mod}\ 16)$$
$$4y \equiv -4t \ (\mathrm{mod}\ 16)$$
$$4y = -4t + 16s$$
$$y = -t + 4s, \text{kde } t, s \in Z$$
$$-4t + 16s + 16z + 32w = 48 - 4t$$
$$16z + 32w = 48 - 16\, s$$

3. nahrazení z parametry r a s a zpětné dosazení

$$16z + 32w \equiv (48 - 16\, s)(\mathrm{mod}\ 32)$$
$$16z \equiv (48 - 16\, s)(\mathrm{mod}\ 32)$$
$$16z = 16 - 16s + 32r$$
$$z = 1 - s + 2r, \text{kde } r, s \in Z$$
$$16 - 16s + 32r + 32w = 48 - 16\, s$$
$$w = 1 - r, \text{kde } r \in Z$$

Řešením rovnice $2x + 4y + 16z + 32w = 48$ je uspořádaná čtveřice $[x, y, z, w]$ dána předpisy

$x = 2t,$

$y = -t + 4s,$

$z = 1 - s + 2r,$

$w = 1 - r,$ kde $t, s, r \in Z.$

Množina všech řešení je uvedena v následující tabulce.

t	s	r	x	y	z	w
0	0	0	0	0	1	1
0	1	0	0	4	0	1
0	0	1	0	0	3	0
1	1	0	2	3	0	1
1	1	1	2	3	2	0
0	1	1	0	4	2	0
2	1	0	4	2	0	1
2	2	1	4	6	1	0
3	2	1	6	5	1	0
2	3	1	4	10	0	0
3	3	1	6	9	0	0
4	1	0	8	0	0	1
4	2	1	8	4	1	0
4	1	1	8	0	2	0

t	s	r	x	y	z	w
4	3	1	8	8	0	0
5	2	1	10	3	1	0
5	3	1	10	7	0	0
6	2	1	12	2	1	0
6	3	1	12	6	0	0
7	2	1	14	1	1	0
7	3	1	14	5	0	0
8	2	1	16	0	1	0
8	3	1	16	4	0	0
9	3	1	18	3	0	0
10	3	1	20	2	0	0
11	3	1	22	1	0	0
12	3	1	24	0	0	0

Tabulka 7

2.3.3 OBECNÉ ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

Jak již bylo uvedeno v kapitole číslo 2, obecná lineární diofantická rovnice má tvar $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, kde koeficienty $a_1, a_2, \ldots, a_n, c \in Z$. Nutná podmínka řešitelnosti v oboru celých čísel je splněna, když číslo c je dělitelné největším společným dělitelem koeficientů $a_1, a_2, \ldots, a_n$. K řešení lineárních diofantických rovnic, kde $n > 3$ se většinou užívá kongruencí, při kterých jsou neznámé vyjadřovány pomocí parametrů. Pokud si pečlivě prohlédneme příklady 2 a 4 řešené pomocí kongruencí, zjistíme, že pro $n = 2$ získáme uspořádanou dvojici s jedním parametrem. V příkladu 4 (lineární diofantické rovnice o 4 neznámých, tedy $n = 4$) jsme výslednou uspořádanou čtveřici $[x, y, z, w]$ dokázali vyjádřit pomocí třech celočíselných parametrů. Tyto poznatky můžeme shrnout tak, že výsledkem lineární diofantické rovnice je množina uspořádaných n-tic popsaná $n - 1$ celočíselnými parametry.

Náznak řešení:

Podmínky:

- $a_1, a_2, \dots, a_n, c \in Z$
- $D(a_1, a_2, \dots, a_n) = D$ je největší společný dělitel koeficientů
- platí nutná podmínka řešitelnosti v oboru celých čísel
- $a_1 < a_2 < \dots < a_n$

Označme:

$D_1 = D(a_2, \dots, a_n)$

$D_2 = D(a_3, \dots, a_n)$

…

Postup:

Nejprve provedeme kongruenci původní rovnice podle modulo D_1. Vyjádříme neznámou x_1 pomocí parametru t_1, dosadíme do původní rovnice a převedeme tento člen na druhou stranu rovnice.

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

$$a_1x_1 + a_2x_2 + \dots + a_nx_n \equiv c \ (\mathrm{mod}\ D_1)$$

$$a_1x_1 \equiv c \ (\mathrm{mod}\ D_1)$$

$$a_1x_1 = c \ (\mathrm{mod}\ D_1) + t_1D_1$$

$$x_1 = \frac{c \ (\mathrm{mod}\ D_1) + t_1D_1}{a_1}, \text{kde } t \in Z$$

$$a_2x_2 + \dots + a_nx_n = c - c \ (\mathrm{mod}\ D_1) - t_1D_1$$

Nyní bychom použili stejný postup podruhé. Dostali bychom vyjádřený člen a_2x_2 pomocí parametrů t_1 a t_2. Po použití tohoto postupu $(n-1)$-krát, bychom získali uspořádanou n-tici $[x_1, x_2, \dots, x_n]$ z oboru celých čísel vyjádřenou pomocí $n-1$ parametrů, tj. pomocí parametrů $t_1, t_2, \dots, t_{n-1}$.

2.4 SOUSTAVY LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

Slovní úlohy vedoucí na lineární diofantické rovnice mohou být omezeny více podmínkami. V takovém případě ze zadání vytvoříme soustavu lineárních diofantických rovnic, kterou lze zapsat v maticovém tvaru $A\vec{x} = \vec{c}$, kde

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \vec{c} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix},$$

kde m je počet lineárních diofantických rovnic o n neznámých $x_1, x_2, \dots, x_n$. Dále $a_{mn} \in Z$, $c_n \in Z$ a řešením je každá uspořádaná n-tice $[x_1, x_2, \dots, x_n] \epsilon Z^n$, kde $m < n.$

Metody řešení naznačíme v následujícím příkladu. Řešitelnost rovnic je hodnocena dle podmínek určených v předchozích kapitolách. Soustava je řešitelná v případě, že $hod(A) = hod(A|c)$.

Příklad 5: (soustava lineárních diofantických rovnic)
Mějme následující soustavu diofantických rovnic.

$$x + 6y + 12z = 4 \qquad (2.4.1)$$

$$2x + 10y + 14z = 6 \qquad (2.4.2)$$

Určete všechna řešení soustavy.

Řešení 5:
Rovnice soustavy jsou řešitelné, neboť je splněna podmínka řešitelnosti první rovnice $D(1, 6, 12) = 1 \wedge 1|4$ a zároveň rovnice druhé $D(2, 10, 14) = 2 \wedge 2|6$. Soustava je také řešitelná, protože $hod \begin{pmatrix} 1 & 6 & 12 \\ 2 & 10 & 14 \end{pmatrix} = hod \left(\begin{matrix} 1 & 6 & 12 \\ 2 & 10 & 14 \end{matrix}\middle|\begin{matrix} 4 \\ 6 \end{matrix}\right)$.

Dosazovací metoda:

Z rovnice (2.4.2) vyjádříme neznámou x: $x = -5y - 7z + 3$ a dosadíme do (2.4.1): $y + 5z = 1$. Pokud z této rovnice vyjádříme y, bude řešením množina uspořádaných trojic $[18z - 2;\ 1 - 5z; z]$, kde $z \epsilon Z$.

Sčítací metoda:

Rovnici (2.4.1) a (2.4.2) upravíme tak, aby po jejich sečtení se odečetla jedna neznámá. Sčítáme tedy například rovnice

$$-2x - 12y - 24z = -8,$$
$$2x + 10y + 14z = 6.$$

Po sečtení dostaneme stejnou uspořádanou trojici jako z dosazovací metody.

Maticový počet: (Hora, 2011)

$A = \begin{pmatrix} 1 & 6 & 12 \\ 2 & 10 & 14 \end{pmatrix}$; $\vec{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$; $\vec{c} = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$

Nejprve se budeme snažit upravit matici A do diagonálního tvaru. Nediagonální členy matice A převedeme elementárními řádkovými a sloupcovými úpravami matice, což je matematicky stejné jako násobení matice A zprava unimodulárními maticemi R_i a zleva unimodulárními maticemi L_i, což jsou čtvercové matice s celočíselnými prvky a jejichž determinant je buď 1, nebo -1.

a) vynulování členu a_{12}

$$R_1 = \begin{pmatrix} 1 & -6 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 6 & 12 \\ 2 & 10 & 14 \end{pmatrix} \cdot \begin{pmatrix} 1 & -6 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 12 \\ 2 & -2 & 14 \end{pmatrix}$$

b) vynulování členu a_{13}

$$R_2 = \begin{pmatrix} 1 & 0 & -12 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 12 \\ 2 & -2 & 14 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -12 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -2 & -10 \end{pmatrix}$$

c) vynulování členu a_{21}

$$L_3 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 2 & -2 & -10 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -10 \end{pmatrix}$$

d) vynulování členu a_{23}

$$R_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -10 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \end{pmatrix}$$

Násobení unimodulárními maticemi šlo nahradit v jednotlivých krocích:

a) přičíst -6násobek prvního sloupce k druhému sloupci

b) přičíst -12násobek prvního sloupce ke třetímu sloupci

c) přičíst -2násobek prvního řádku k druhému řádku

d) přičíst -5násobek druhého sloupce ke třetímu sloupci

Označme:

$$L = L_3 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \qquad R = R_1 \cdot R_2 \cdot R_4 = \begin{pmatrix} 1 & -6 & 18 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix}$$

Potom Smithův normální tvar matice A je definován jako $D = LAR = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 6 & 12 \\ 2 & 10 & 14 \end{pmatrix} \cdot \begin{pmatrix} 1 & -6 & 18 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \end{pmatrix}$. V důsledku změny matice A se musely změnit i prvky matice $\vec{c}$, konkrétně o násobek matice L. Pravá strana rovnice má tedy tvar $\vec{c'} = L\vec{c} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 4 \\ -2 \end{pmatrix}$. Původní matici jsme zleva vynásobili maticí L a zprava maticí R. Nové řešení můžeme napsat ve tvaru $LAR\vec{x'} = D\vec{x'} = \vec{c'}$, po dosazení $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 4 \\ -2 \end{pmatrix}$. Řešením těchto rovnic je $x' = 4$, $y' = 1$, $z' = t, t \in Z$. Původní řešení se od tohoto liší o násobek matice R zleva. Tzn.: $\vec{x} = R\vec{x'} = \begin{pmatrix} 1 & -6 & 18 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 1 \\ t \end{pmatrix} = \begin{pmatrix} 18t - 2 \\ -5t + 1 \\ t \end{pmatrix}$, kde $t \in Z$, což koresponduje s výsledky předchozích způsobů řešení.

2.5 PRAKTICKÉ UŽITÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

Představme si, že stojíme v obchodě u pokladny, máme peněženku plnou mincí, prodavačka sečte cenu zboží a co se děje dál? Každý člověk v podvědomí řeší diofantickou rovnici. Potřebuje zkombinovat mince různých hodnot tak, aby se součet co nejvíce přibližoval ceně nákupu. Proč se ale této rovnici říká diofantická? Odpověď je jednoduchá. Diofantická rovnice je rovnice řešená v oboru celých čísel, tzn. v rámci celých mincí. Metodu řešení diofantických rovnic v těchto situacích nazýváme „pokus-omyl" a učí se s ní pracovat již děti na prvním stupni základní školy za pomoci základních aritmetických operací. Touto metodou bohužel nedokážeme najít všechny možnosti řešení. Všechna řešení mohou získat žáci druhého stupně základní školy, kteří absolvovali výuku o lineárních rovnicích. Žáci vysokých škol mohou k řešení využít nejrychlejší způsob řešení pomocí kongruence modulo n, které bylo již dříve vysvětleno. Tato metoda je vhodná především na složitější rovnice o více proměnných a výsledkem je množina všech řešení. Stejně tak soustavy lineárních diofantických rovnic pomocí Smithova normálního tvaru matice mohou řešit až studenti vysokých škol. Na lineární diofantické úlohy vedou i některé geometrické úlohy (možnosti délek stran trojúhelníka v závislosti na obvodu), objemové úlohy (přesné naplnění sudu o určitém objemu různě objemnými nádobami) a mnoho dalších.

3 DIOFANTICKÉ ROVNICE 2. STUPNĚ

Kvadratickou diofantickou rovnicí o dvou neznámých x, y rozumíme rovnici ve tvaru

$$ax^2 + bx + cxy + dy + ey^2 = f, \qquad (3.1)$$

kde $a, b, c, d, e, f \in Z$. Řešením rovnice je každá uspořádaná dvojice $[x, y] \in Z^2$. Pro rovnice tohoto typu neexistuje jednotný algoritmus pro získání řešení. Koeficienty v rovnici (3.1) lze pokládat rovné 0 nebo jiným konstantám, čímž vznikají různé typy kvadratických diofantických rovnic. Základním typem je tvar

$$ax^2 + ey^2 = f, \qquad (3.2)$$

kde koeficienty b, c, d z rovnice (3.2) jsou rovny nule. Rovnice (3.2) je řešitelná právě tehdy, když největší společný dělitel a, e dělí f. Matematicky zapsáno $D(a, e)|f$. Metody řešení si ukážeme na následujícím příkladu.

Příklad 6: (kvadratická diofantická rovnice)

Sedm čtverců s délkou strany x a šestnáct čtverců s délkou strany y mají dohromady obsah 23j^2. Příklad je velmi jednoduchý a umělý, aby mohly být metody řešení vysvětleny jasně.

Řešení 6:

Rovnice bude mít tvar $7x^2 + 16y^2 = 23$. Podmínka řešitelnosti je splněna, neboť $D(7, 16) = 1 \land 1|23$.

Metoda pokus-omyl:

V této metodě zkoušíme volit za x nebo y libovolné přirozené číslo. Pokud druhá z dvojice neznámých bude náležet také oboru přirozených čísel, je tato uspořádaná dvojice výsledkem příkladu 6. Obecně bereme za obor řešení diofantických rovnic čísla celá. V tomto příkladu uvažujeme pouze o číslech přirozených, protože uspořádaná dvojice představuje délky stran. Pokud zvolíme například $x = 1$, $y = \pm 1$. Za řešení můžeme považovat uspořádanou dvojici $[1, 1]$.

Řešení vyjádřením členu s nejmenším koeficientem:

Z rovnice $7x^2 + 16y^2 = 23$ vyjádříme x^2 jako

$$x^2 = \frac{23-16y^2}{7} = 3 - 2y^2 + \frac{2-2y^2}{7} = 3 - 2y^2 + t,$$

kde $\frac{2-2y^2}{7} = t$ a $t \in Z$.

Víme, že $y^2 = \frac{2-7t}{2}$, což dosadíme do rovnice $x^2 = 3 - 2y^2 + t = 1 + 8t$. Pokud vyjádříme x a y, dostaneme uspořádané dvojice $x = \pm\sqrt{1+8t}$, $y = \pm\sqrt{\frac{2-7t}{2}}$, které dávají smysl například pro $t = 0$. Řešení hledáme v oboru celých kladných čísel, takže výsledkem je uspořádaná dvojice $[1, 1]$.

Řešení kongruencí:

Zadanou rovnici rozdělíme na dva případy řešení.

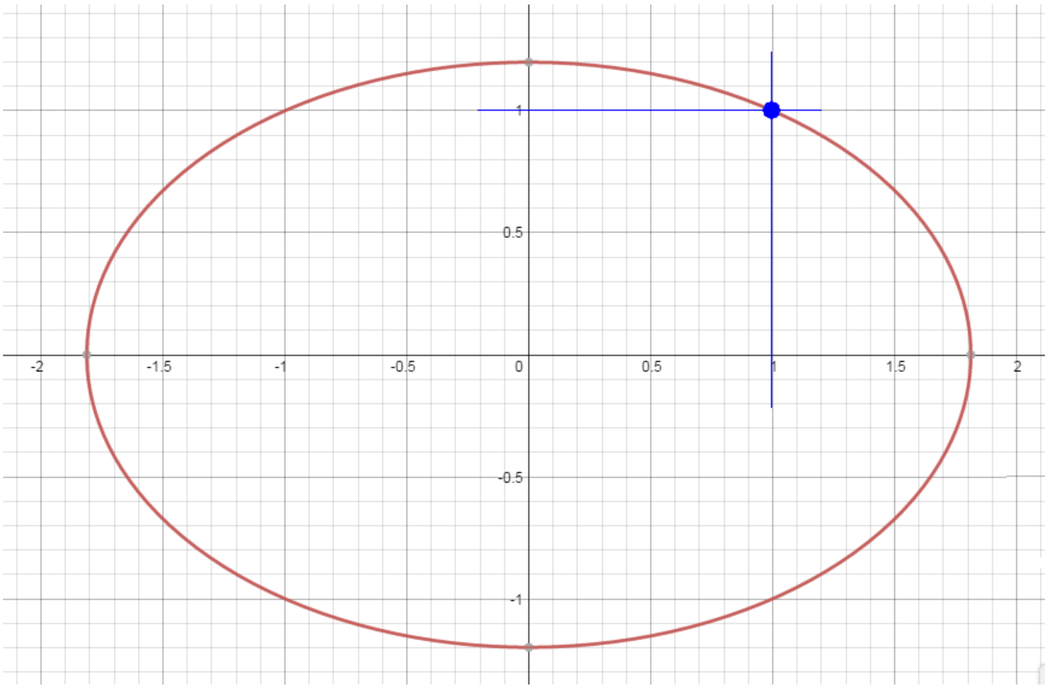
$$7x^2 + 16y^2 \equiv 23 \; mod \; 7$$
$$2y^2 \equiv 2 \; mod \; 7$$
$$y^2 \equiv 1 \; mod \; 7$$
$$y^2 = 1 + 7t$$
$$y = \pm\sqrt{1+7t}$$

$$7x^2 + 16y^2 \equiv 23 \; mod \; 16$$
$$7x^2 \equiv 23 \; mod \; 16$$
$$7x^2 \equiv 7 \; mod \; 16$$
$$x^2 \equiv 1 \; mod \; 16$$
$$x^2 = 1 + 16t$$
$$x = \pm\sqrt{1+16t}$$

V úvahu bereme jen kladné hodnoty, například pro $t = 0$. Výsledkem je uspořádaná dvojice $[1, 1]$. Místo použití druhého řešení pomocí modulo 16, šlo $y = \pm\sqrt{1+7t}$ dosadit přímo do $7x^2 + 16y^2 = 23$ a úpravami zjistit rovnici pro x, což je matematicky korektní.

Grafické řešení:

Pokud bychom zadanou rovnici sledovali z hlediska geometrie, vyjadřoval by předpis rovnici elipsy se středem v počátku. Jestliže výsledkem jsou délky stran, musíme řešení hledat v prvním kvadrantu. Výsledkem je uspořádaná dvojice, pro niž jsou hodnoty x a y z přirozených čísel, tj. bod $[1, 1]$.



Obrázek 4 - kvadratická diofantická rovnice, [4]

S těmito typy rovnic se setkávají žáci již na základní škole. Řešení se pokouší najít buď metodou pokus-omyl, či vyjádřením členu s nejmenším koeficientem a následným parametrizováním. Slovních úloh vedoucích k vyjádření kvadratických diofantických rovnic typu $ax^2 + ey^2 = f$ není mnoho. Jedná se především o geometrické příklady v návaznosti na Pythagorovu větu. Nejvýhodnější metodu řešení pomocí kongruence (získáme všechna řešení) využijí až žáci vysokých škol. Je potřeba znát teorii elementární algebry a základy kongruence modulo n. Ve většině případů je obtížné najít celočíselné řešení a pokud existuje, najdeme pouze několik málo uspořádaných dvojic.

Soustavy kvadratických diofantických rovnic se dají stejně jako soustavy lineárních diofantických rovnic řešit sčítací či dosazovací metodou, kdy pro každou z rovnic musí být splněna podmínka řešitelnosti.

3.1 PELLOVA ROVNICE

Speciálním typem kvadratické diofantické rovnice o 2 neznámých je Pellova rovnice, která má tvar

$$x^2 - Ay^2 = 1, \qquad (3.1.1)$$

kde A je přirozené číslo, které není přirozenou mocninou žádného přirozeného čísla (například $A \neq 4$). Triviálním řešením rovnice (3.1.1) jsou uspořádané dvojice $[1, 0]$ a $[-1, 0]$, kterými se automaticky nebudeme zabývat.

Vysvětlení, proč A nemůže být přirozenou mocninou žádného přirozeného čísla je jednoduché. Pokud by $A = a^2$, pro $a \in N$ pak rovnice $x^2 - (ay)^2 = 1$ nemá celočíselné řešení, protože rozdíl dvou čtverců nemůže být roven jedné. Pokud tuto větu znegujeme, dostaneme, že pro každé $A > 0$, kde $A \neq a^2$, má rovnice (3.1.1) alespoň jedno celočíselné řešení.

Na příkladu 7 si ukážeme principy řešení použité u předchozích typů diofantických rovnic. Pomocí nich získáme alespoň jedno řešení. Všechna řešení získáme ze vztahů

$$x = \frac{(p + q\sqrt{A})^n + (p - q\sqrt{A})^n}{2}, \qquad (3.1.2)$$

$$y = \frac{(p + q\sqrt{A})^n - (p - q\sqrt{A})^n}{2\sqrt{A}}. \qquad (3.1.3)$$

přičemž předpokládáme, že rovnici (3.1.1) vyhovuje řešení $(x, y) = (p, q)$, pro $p, q \in N$, kde $n \in N$. Potom všechny dvojice celých čísel (x, y) jsou řešením Pellovy rovnice.

Odvození:

Jestliže (p, q) řeší rovnici (3.1.1), je $1 = p^2 - Aq^2 = \left(p + q\sqrt{A}\right)\left(p - q\sqrt{A}\right)$. Pokud obě strany umocníme na n-tou, dostaneme $1 = 1^n = \left(p + q\sqrt{A}\right)^n\left(p - q\sqrt{A}\right)^n$. Tyto výrazy se musí rovnat původnímu zadání, tedy

$$x + y\sqrt{A} = \left(p + q\sqrt{A}\right)^n,$$

$$x - y\sqrt{A} = (p - q\sqrt{A})^n.$$

Pokud z této soustavy vyjádříme x, y dostaneme vztahy (3.1.2) a (3.1.3).

Příklad 7: (Pellova rovnice)

Řešte rovnici $x^2 - 2y^2 = 1$.

Řešení 7:

Rovnice je řešitelná, neboť $D(1, -2) = 1 \wedge 1|1$.

Metoda pokus-omyl:

Stejně jako v obecném případě kvadratických diofantických rovnic lze řešení zkoušet dosazováním. Zkusíme znovu zvolit $x = 3$, vyjde $y = \pm 2$. Řešením tedy budou uspořádané dvojice $[3, 2]$ a $[3, -2]$.

Řešení vyjádřením členu s nejmenším koeficientem:

Pro získání řešení Pellovy rovnici lze samozřejmě použít i metodu, kdy vyjadřujeme neznámou s nejmenším koeficientem. Po úpravách získáme $x^2 = 1 + 2y^2$. Pokud $y^2 = t$, $t \in Z$ bude $x^2 = 1 + 2t$. Vyjádříme-li x, y: $x = \pm\sqrt{1 + 2t}$, $y = \pm\sqrt{t}$. Může být řešením například uspořádaná dvojice $[3, 2]$, $[-3, -2]$, $[-3, 2]$ nebo $[3, -2]$ pro $t = 4$.

Řešení kongruencí:

Stejně jako v kapitole 3, lze zadanou rovnici řešit pomocí kongruence.

$$x^2 - 2y^2 \equiv 1 \ mod\ 2$$

$$x^2 \equiv 1 \ mod\ 2$$

$$x^2 = 1 + 2t$$

$$x = \pm\sqrt{1 + 2t}$$

Nyní dosadíme $x = \pm\sqrt{1 + 2t}$ do původní rovnice a vyjádříme $y = \pm\sqrt{t}$.

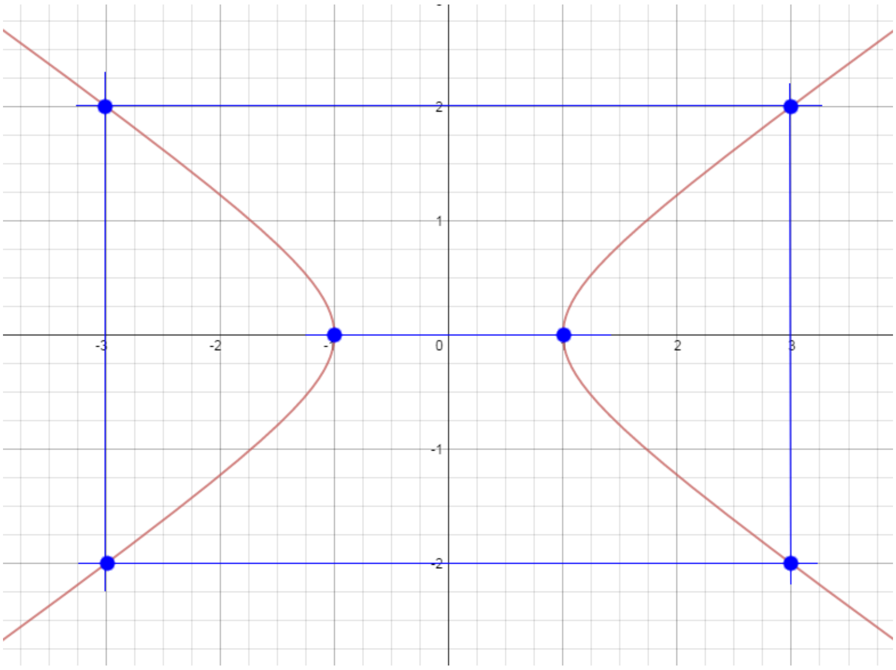
Možnosti výsledků jsou uvedeny v následující tabulce.

t	uspořádaná dvojice [x, y]
4	$[3, 2]$, $[-3, -2]$, $[-3, 2]$, $[3, -2]$

Tabulka 8

Grafické řešení:

Na obrázku 5 jsou vidět jak 2 triviální řešení, tak i 4 netriviální uspořádané dvojice celých čísel, které jsou výše vypočteným řešením. Pellova rovnice je předpisem hyperboly se středem v počátku.



Obrázek 5 - Pellova rovnice, [4]

Další řešení:

Ve všech metodách nám jedním z řešení vyšla uspořádaná dvojice $[3, 2]$. Všechna řešení získáme dosazením do vztahů (3.1.2) a (3.1.3):

$$x = \frac{\left(p + q\sqrt{A}\right)^n + \left(p - q\sqrt{A}\right)^n}{2} = \frac{\left(3 + 2\sqrt{2}\right)^n + \left(3 - 2\sqrt{2}\right)^n}{2},$$

$$y = \frac{\left(p + q\sqrt{A}\right)^n - \left(p - q\sqrt{A}\right)^n}{2\sqrt{A}} = \frac{\left(3 + 2\sqrt{2}\right)^n - \left(3 - 2\sqrt{2}\right)^n}{2\sqrt{2}}.$$

n	x	y
1	3	2
2	17	12
3	99	70
...	...	...

Tabulka 9

V následujících odstavcích čtenáře seznámíme s potřebnou teorií a definujeme pojmy podstatné pro upřesnění principu počítání Pellových rovnic pomocí řetězových zlomků. Tato teorie byla čerpána ze zdroje uvedeného v seznamu literatury (Petrová, 2012).

Definice: (řetězový zlomek)

Konečným řetězovým zlomkem rozumíme výraz

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

kde $a_0 \epsilon Z$; $a_1, a_2, \dots, a_k \epsilon N$; $a_k > 1$. Zapíšeme jako $[a_0, a_1, a_2, \dots, a_k]$ a používá se pro racionální čísla.

Nekonečným řetězovým zlomkem rozumíme výraz

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

kde $a_0 \epsilon Z$; $a_1, a_2, \dots \epsilon N$. Zapíšeme jako $[a_0, a_1, a_2, \dots]$ a používá se pro iracionální čísla. 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 $k \epsilon N, s \epsilon N^0$. Nejmenší přirozené číslo k, pro které lze nekonečný řetězový zlomek napsat v tomto tvaru, se nazývá jeho periodou.

Definice: (pomocné posloupnosti P_n, Q_n)

Pomocné posloupnosti P_n, Q_n celých čísel definujeme vztahy:

$P_{-1} = 1$	$P_0 = a_0$	$P_n = a_n P_{n-1} + P_{n-2}$	$n \geq 1$
$Q_{-1} = 0$	$Q_0 = 1$	$Q_n = a_n Q_{n-1} + Q_{n-2}$	$n \geq 1$

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

Věta 3: Budou-li $j = \bar{x} + \bar{y}\sqrt{A}$ nejmenší kladné řešení Pellovy rovnice. Potom platí $j^{n+2} = 2\bar{x}j^{n+1} - j^n, n = 0, 1, 2, \dots$

Věta 4: Buď $[a_0, a_1, a_2, \dots, a_{k-1}, 2a_0, a_1, \dots]$ nekonečný periodický řetězový zlomek k číslu $\sqrt{A}$. Pak výraz $P_{kn-1} + Q_{kn-1} \cdot \sqrt{A}$, kde $n \in N$, kde kn je sudé jsou všechna kladná řešení Pellovy rovnice. Jestliže je k sudé, je $P_{k-1} + Q_{k-1} \cdot \sqrt{A}$ nejmenší kladné řešení této rovnice. Pro liché k je nejmenším kladným řešením rovnice výraz $P_{2k-1} + Q_{2k-1} \cdot \sqrt{A}$.

Příklad 8: (Pellova rovnice – řetězové zlomky)

Nalezněte první 4 kladná řešení Pellovy rovnice $x^2 - 15y^2 = 1$.

Řešení 8:

1. Nalezneme řetězový zlomek k číslu $\sqrt{15}$
2. Nalezneme nejmenší kladné řešení (podle věty 4)
3. Najdeme mocniny $j^n = x_n + y_n\sqrt{A}$ (podle věty 3)

1. ŘETĚZOVÝ ZLOMEK

$a_0 = 3$	$\sqrt{15} = 3 + \frac{1}{\alpha_1}$	$\alpha_1 = \frac{\sqrt{15}+3}{6}$
$a_1 = 1$	$\frac{\sqrt{15}+3}{6} = 1 + \frac{1}{\alpha_2}$	$\alpha_2 = \sqrt{15} - 3$
$a_2 = 0$	$\sqrt{15} - 3 = 0 + \frac{1}{\alpha_3}$	$\alpha_3 = \frac{\sqrt{15}+3}{6}$

Nekonečný periodický řetězový zlomek k číslu $\sqrt{15}$ je $[3, 1, 0, \dots]$ s periodou $k = 2$.

2. NEJMENŠÍ KLADNÉ ŘEŠENÍ

$$P_1 = a_1P_0 + P_{-1} = a_1a_0 + 1 = 1 \cdot 3 + 1 = 4$$

$$Q_1 = a_1Q_0 + Q_{-1} = a_1 1 + 0 = 1 \cdot 1 + 0 = 1$$

$$P_2 = a_2P_1 + P_0 = a_2P_1 + a_0 = 0 \cdot 4 + 3 = 3$$

$$Q_2 = a_2Q_1 + Q_0 = a_2Q_1 + 1 = 0 \cdot 1 + 1 = 1$$

$$P_3 = a_3P_2 + P_1 = a_1P_2 + P_1 = 1 \cdot 3 + 4 = 7$$

$$Q_3 = a_3Q_2 + Q_1 = a_1Q_2 + Q_1 = 1 \cdot 1 + 1 = 2$$

$\boldsymbol{n}$	**-1**	**0**	**1**	**2**	**3**	**4**
$\boldsymbol{a_n}$		3	1	0	1	…
$\boldsymbol{P_n}$	1	3	4	3	7	…
$\boldsymbol{Q_n}$	0	1	1	1	2	…

Tabulka 10

Nejmenší kladné řešení rovnice má tvar $j = \bar{x} + \bar{y}\sqrt{A}$. Protože je perioda sudé číslo, použijeme vzorec

$$j = P_{k-1} + Q_{k-1}\sqrt{A} = P_1 + Q_1\sqrt{15} = \bar{x} + \bar{y}\sqrt{A} = 4 + \sqrt{15}.$$

3. PRVNÍ 4 KLADNÁ ŘEŠENÍ

Další řešení najdeme pomocí vzorce $j^n = x_n + y_n\sqrt{A} = 2\bar{x}j^{n-1} - j^{n-2}$.

$$j^2 = x_n + y_n\sqrt{A} = 2\bar{x}j - j^0 = 2 \cdot 4 \cdot \left(4 + \sqrt{15}\right) - 1 = \mathbf{31} + \mathbf{8}\sqrt{15}$$

$$j^3 = x_n + y_n\sqrt{A} = 2\bar{x}j^2 - j^1 = 2 \cdot 4 \cdot \left(31 + 8\sqrt{15}\right) - \left(4 + \sqrt{15}\right) = \mathbf{244} + \mathbf{63}\sqrt{15}$$

$$j^4 = x_n + y_n\sqrt{A} = 2\bar{x}j^3 - j^2 = 8 \cdot \left(244 + 63\sqrt{15}\right) - \left(31 + 8\sqrt{15}\right) = \mathbf{1921} + \mathbf{496}\sqrt{15}$$

$\boldsymbol{n}$	**0**	**1**	**2**	**3**	**4**
x_n	1	4	31	244	1921
y_n	0	1	8	63	496

Tabulka 11

Tím byla první 4 kladná řešení zadané rovnice nalezena.

3.1.1 ARCHIMÉDOVA ÚLOHA O DOBYTKU

Archimédova úloha o dobytku pravděpodobně vznikla ve starém Řecku přibližně ve 3. stolení před naším letopočtem. Mezi historiky však panují 2 názory ohledně jejího autorství. Jedním názorem je, že autorem byl právě Archimédes, druhý zastává myšlenku, že úlohu vymyslel Eratosthenes z Kyrény a zaslal ji Archimédovi k vyřešení, neboť byla napsána ve verších, což neodpovídalo Archimédovu stylu. Zadání se zdá být jednoduché a řešení se dá rozdělit do 2 částí. V prvních krocích je potřeba vyřešit sedm lineárních diofantických rovnic o osmi neznámých, v druhé části musíme vyřešit Pellovu rovnici, na kterou zadání vede.

Archimédova úloha o dobytku (Bártlová, 2012):

„Řekni mi, příteli, přesný počet Héliova skotu. Pečlivě mi vypočítej, není-li ti moudrost cizí, kolik ho bylo, když se jednou pásl na nivách ostrova Sicílie, rozděleno do čtyř stád. Každé stádo bylo jinak zbarveno; první bylo mléčně bílé, ale druhé zářilo zcela tmavou černí. Třetí pak bylo hnědé, čtvrté strakaté; v každém měli býci v počtu velikou převahu. A tito [býci] byli nyní v takovémto poměru:bílí se rovnali v počtu hnědým vzatým dohromady s třetinou a polovinou černých, o příteli. Dále množství černých bylo rovno čtvrtině a pětině strakatých zvětšených o všechny hnědé. Nakonec musíš počet strakatých býků položit rovny, příteli, šestině a sedmině bílých s přičteným ještě množstvím hnědých. Jinak však tomu bylo s kravami: ty s bílou srsti byly rovny třetině a čtvrtině černého skotu, krav i býků. Dále černé krávy byly rovny čtvrtině a pětině strakatého stáda, když byli počítáni jak býci, tak krávy. Právě tak byly strakaté krávy pětinou a šestinou všeho [skotu] s hnědou srsti, když šel na pastvu. Nakonec hnědé krávy byly šestinou a sedminou celého stáda s bílou srstí. Můžeš-li mi říci přesně, můj příteli, kolik skotu tam bylo dohromady a také kolik bylo krav každé barvy a dobře živených býků, pak tě věru právem nazývají zdatným v počtech.

Ještě tě však nepočítají k mudrcům; nuže pojď tedy a řekni mi, jak se to má dále: Když se spojil celkový počet černých a bílých býků, pak zde stali uspořádáni stejně do šířky jako do hloubky; šíře sicilské nivy byly zcela zaplněny tím množstvím býků. Když se však postavili dohromady hnědí a strakatí, pak byl vytvořen trojúhelník, jeden stal na špičce a nechyběl žádný z hnědých a strakatých býků, ani jeden jiné barvy se mezi nimi nenašel. Když jsi to také vypátral a v duchu pochopil a uvedeš mi poměr, příteli, *který se nalézá v každém stádu, pak můžeš pyšně vykračovat jako vítěz, protože teď tvá vědecká sláva jasně září.“*

Úkolem je vypočítat, jaké množství bílých, černých, strakatých a hnědých krav a býků se pase ve čtyřech stádech na ostrově Sicílie boha Hélia.

Označme:

B…počet bílých býků

b…počet bílých krav

C…počet černých býků

c…počet černých krav

S…počet strakatých býků

s…počet strakatých krav

H…počet hnědých býků

h…počet hnědých krav

V první části ze zadání vytvoříme lineární diofantické rovnice

$$B = \left(\frac{1}{2} + \frac{1}{3}\right) C + H,$$

$$C = \left(\frac{1}{4} + \frac{1}{5}\right) S + H,$$

$$S = \left(\frac{1}{6} + \frac{1}{7}\right) B + H,$$

$$b = \left(\frac{1}{3} + \frac{1}{4}\right) (C + c),$$

$$c = \left(\frac{1}{4} + \frac{1}{5}\right) (S + s),$$

$$s = \left(\frac{1}{5} + \frac{1}{6}\right) (H + h),$$

$$h = \left(\frac{1}{6} + \frac{1}{7}\right) (B + b).$$

Výpočet provedeme dosazovací metodou.

$$B = \frac{5}{6}C + H = \frac{5}{6}\left(\frac{9}{20}S + H\right) + H = \frac{5}{6}\left(\frac{9}{20}\left(\frac{13}{42}B + H\right) + H\right) + H = \frac{13}{112}B + \frac{53}{24}H$$

$$297 \cdot B = 742 \cdot H$$

Platí

$$B = 742k,$$

$$H = 297k,$$

$$S = \frac{1580}{3}k,$$

$$C = 534k, \text{kde } k \in N.$$

Po úpravě

$$B = 2226k,$$

$$H = 891k,$$

$$S = 1580k,$$

$$C = 1602k, \text{kde } k \in N.$$

Pokud tyto výsledky dosadíme do zbylých 4 rovnic, získáme

$$b = \frac{7}{12}\left(1602k + \frac{9}{20}\left(1580k + \left(\frac{11}{30}\left(891k + \left(\frac{13}{42}(2226k + b)\right)\right)\right)\right)\right) = \frac{7206360}{4657}k,$$

$$h = \left(\frac{13}{42}\right)\left(2226k + \frac{7206360}{4657}k\right) = \frac{5439213}{4657}k,$$

$$s = \left(\frac{11}{30}\right)\left(891k + \frac{5439213}{4657}k\right) = \frac{3515820}{4657}k,$$

$$c = \left(\frac{9}{20}\right)\left(1580k + \frac{3515820}{4657}k\right) = \frac{4893246}{4657}k,$$

kde $k \in N$.

Pokud vynásobíme všechny neznámé číslem 4657, dostaneme množinu výsledků ($k \in N$).

<table>
<tr><th>barva a pohlaví dobytka (viz označení)</th><th>počet kusů dobytka dle barvy</th><th>počet kusů dobytka dle pohlaví</th></tr>
<tr><td>B</td><td>$10\,366\,482k$</td><td rowspan="4">$29\,334\,443k$</td></tr>
<tr><td>C</td><td>$7\,460\,514k$</td></tr>
<tr><td>S</td><td>$7\,358\,060k$</td></tr>
<tr><td>H</td><td>$4\,149\,387k$</td></tr>
<tr><td>b</td><td>$7\,206\,360k$</td><td rowspan="4">$21\,054\,639k$</td></tr>
<tr><td>c</td><td>$4\,893\,246k$</td></tr>
<tr><td>s</td><td>$3\,515\,820k$</td></tr>
<tr><td>h</td><td>$5\,439\,213k$</td></tr>
<tr><td colspan="2">CELKEM kusů dobytka</td><td>$50\,389\,082k$</td></tr>
</table>

Tabulka 12

Nyní se podíváme na druhou část úlohy.

„Když se spojil celkový počet černých a bílých býků, pak zde stali uspořádáni stejně do šířky jako do hloubky; šíře sicilské nivy byly zcela zaplněny tím množstvím býků.“

Matematický zápis této podmínky zní $C + B = x^2$, kde $x \in N$ (černé a bílé býky lze uspořádat do čtverce). Do rovnice můžeme dosadit.

$$7\,460\,514k + 10\,366\,482k = x^2$$

$$17\,826\,996k = x^2$$

Provedeme rozklad na prvočísla.

$$2 \cdot 2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657k = x^2$$

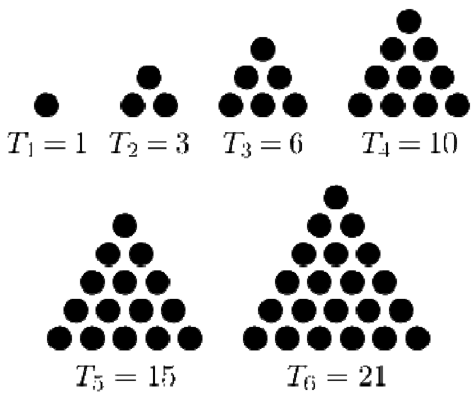
Aby toto číslo bylo čtvercem, musí být $k = 3 \cdot 11 \cdot 29 \cdot 4657n^2 = 4\,456\,749n^2$, kde $n \in N$.

„Když se však postavili dohromady hnědí a strakatí, pak byl vytvořen trojúhelník, jeden stal na špičce a nechyběl žádný z hnědých a strakatých býků, ani jeden jiné barvy se mezi nimi nenašel.“

Na tuto doplňující podmínku využijeme tzv. trojúhelníkové číslo, což je součet k přirozených čísel od 1 do k. Trojúhelníkové číslo tedy uvádí počet hnědých a strakatých býků. Trojúhelníkové číslo je definováno jako

$$T_k = 1 + 2 + 3 + \cdots + (k-1) + \ k = \tfrac{k(k+1)}{2}, \text{ kde } n \in N.$$

K pochopení trojúhelníkového čísla a představě o uspořádání býků nám pomůže obrázek 6.



Obrázek 6 - trojúhelníkové obrazce, [5]

Ze zadání tedy odvodíme rovnici $S + H = \frac{y(y+1)}{2}$, kde $y \in N$. Pokud dosadíme, dostaneme následující vztahy.

$$7\,358\,060k + 4\,149\,387k = \frac{y(y+1)}{2}$$

$$11\,507\,447k = \frac{y(y+1)}{2}$$

Nyní můžeme dosadit $k = 4\,456\,749n^2$.

$$102\,571\,605\,819\,606n^2 = \frac{y(y+1)}{2}$$

Definujeme $A = 102\,571\,605\,819\,606$.

$$An^2 = \frac{y(y+1)}{2}$$

Tento výraz upravíme na kvadratickou rovnici

$$y^2 + y - 2An^2 = 0.$$

Vypočteme diskriminant $D = 1 + 8An^2$ a získáme kořeny

$$y_{1,2} = \frac{-1 \pm \sqrt{D}}{2}.$$

Aby řešení bylo z oboru přirozených čísel, musí být $\sqrt{D}$ záporné celé liché číslo, to zapíšeme jako $\sqrt{D} = \sqrt{1 + 8An^2} = p$, umocníme $D = 1 + 8An^2 = p^2$ a upravíme do tvaru Pellovy rovnice.

$$p^2 - 8An^2 = 1$$

$$p^2 - 820\,572\,846\,556\,848n^2 = 1$$

Nyní bychom mohli začít hledat řetězový zlomek k číslu $\sqrt{820\,572\,846\,556\,848}$, následně bychom našli nejmenší kladné řešení a všechna další. Počítáním této rovnice bychom obsahově naplnili další bakalářskou práci, takže se do těchto výpočtů nebudeme pouštět. Je však zřejmé, že i přes zdánlivě triviální zadání není jednoduché k výsledku dojít. Přesné řešení bylo provedeno až po nástupu počítačové techniky, neboť výsledek je složen z 206 545 cifer.

Výsledek je pro čtenáře k náhledu na webovských stránkách http://www.math.nyu.edu/~crorres/Archimedes/Cattle/computer2/computer_output.html.

3.2 ZOBECNĚNÁ PELLOVA ROVNICE

Rozdíl mezi zobecněnou Pellovou rovnicí a Pellovou rovnicí je v absolutním členu na pravé straně rovnice. Takže obecný tvar je dán

$$x^2 - Ay^2 = C, \qquad (3.2.1)$$

kde A je přirozené číslo, které není přirozenou mocninou žádného přirozeného čísla a $C \in Z$. Triviálním řešením rovnice (3.2.1) jsou uspořádané dvojice $[\sqrt{C}, 0]$ a $[-\sqrt{C}, 0]$.

Dále definujeme základní vztahy potřebné k výpočtu řešení. Některé vztahy byly přebrány z předchozí kapitoly, vše bylo čerpáno ze zdroje uvedeného v seznamu literatury této bakalářské práce (Petrová, 2012).

$j = \bar{x} + \bar{y}\sqrt{A}$ … nejmenší kladné řešení Pellovy rovnice

$j^{-1} = \bar{x} - \bar{y}\sqrt{A}$ … inverzní číslo k j

$$j.j^{-1} = 1$$

$\alpha = x + y\sqrt{A}$ … libovolné řešení zobecněné Pellovy rovnice

$\alpha \cdot j^n$, pro $n \epsilon Z$ … další řešení zobecněné Pellovy rovnice

$\alpha \cdot j^{-1}$ … levé řešení k řešení α

$\alpha \cdot j^1$ … pravé řešení k řešení α

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

Věta 5: 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. Potom platí

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

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

Příklad 9: (zobecněná Pellova rovnice)

Řešte zobecněnou Pellovu rovnici $x^2 - 15y^2 = 106$.

Řešení 9:

1. Nalezneme nejmenší kladné řešení Pellovy rovnice (viz předchozí kapitola)
2. Odhadneme y podle věty 5
3. Najdeme rovnici řešení ve tvaru $\alpha = x + y\sqrt{A}$, kdy ke každému y splňující nerovnosti z věty 5 existuje x
4. Vytvoříme sérii $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$ ke každému řešení a tím získáme všechna nezáporná řešení zadané rovnice.

1. NEJMENŠÍ KLADNÉ ŘEŠENÍ PELLOVY ROVNICE

Pellova rovnice má tvar řešeného příkladu 8 předchozí kapitoly, tedy $x^2 - 15y^2 = 1$. Zjistili jsme, že nejmenším kladným řešení byla uspořádaná dvojice [4, 1].

2. ODHAD y

Podle věty 5 použijeme pro odhad neznámé $y \leq \sqrt{\frac{C(\bar{x}-1)}{2A}}$, neboť $C = 106$.

$$y \leq \sqrt{\frac{106(4-1)}{2\cdot 15}} \rightarrow y \leq \sqrt{\frac{53}{5}}$$

Z toho plyne, že $y = \{1, 2, 3\}$.

3. ŘEŠENÍ VE TVARU $\alpha = x + y\sqrt{A}$

Ze zadané rovnice vyjádříme x: $x = \sqrt{106 + 15y^2}$ a dosazujeme možné hodnoty y.

y	x
1	11
2	$\sqrt{166}$
3	$\sqrt{241}$

Tabulka 13

Celočíselné řešení lze zapsat jako: $\alpha = 11 + \sqrt{15}$.

Kdyby neexistoval žádná celočíselná uspořádaná dvojice $[x, y]$ neměla by zadaná rovnice žádné řešení.

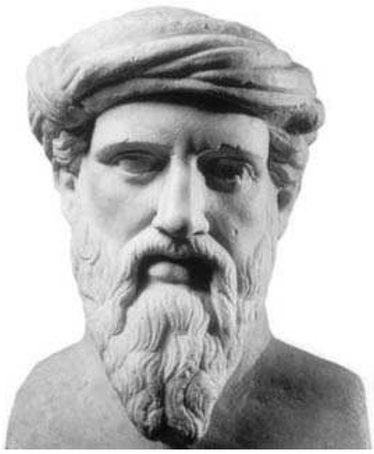
4. SÉRIE ŘEŠENÍ $\{\alpha, |\alpha j^{-1}|\}_{n=0}^{\infty}$

$$\alpha j^{-1} = \left(11 + \sqrt{15}\right) \cdot \left(4 - \sqrt{15}\right) = (29 - 7\sqrt{15})$$

Všechna nezáporná řešení zadané rovnice jsou

$$\left\{11 + \sqrt{15}, 29 + 7\sqrt{15}\right\}_{n=0}^{\infty}.$$

3.3 PYTHAGOREJSKÁ ROVNICE



Obrázek 7 - Pythagoras, [6]

Pythagorejská rovnice 2. stupně je dalším speciálním typem kvadratických diofantických rovnic. Její tvar je podobný Pythagorově větě ($a^2 + b^2 = c^2$), která popisuje vztah stran pravoúhlého trojúhelníka a má nekonečně mnoho řešení tzv. pythagorejských trojic. Pythagorejská diofantická rovnice hledá celočíselné délky stran pravoúhlého trojúhelníka. Tyto celočíselné trojice splňují rovnici

$$x^2 + y^2 = z^2, \qquad (3.3.1)$$

kde $x, y, z \in Z; x > 0, y > 0, z > 0; D(x, y) = 1$ a x je sudé. Výrazy x, y a z jsou popsány následovně

$$x = 2ab,$$

$$y = b^2 - a^2,$$

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

kde $0 < a < b; a, b \in N; a, b$ jsou nesoudělná čísla různé parity.

Důkaz pythagorejské věty je dlouhý a mimo rozsah této bakalářské práce. Naznačíme pouze, že se opírá o znalost Gaussových celých čísel, kdy rovnici (3.3.1) můžeme přepsat do tvaru nesoudělných Gaussových celých čísel jako $(x + iy) \cdot (x - iy) = z^2$. Po mnoha operacích bychom došli k uvedené větě.

V tabulce 14 jsou uvedeny možné výsledky vzhledem k náhodně zvoleným parametrům a, b, které vyhovují požadovaným podmínkám.

$(\boldsymbol{a}, \boldsymbol{b})$	$(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ **– pythagorejská trojice**
$(1, 2)$	$(4, 3, 5)$
$(2, 3)$	$(12, 5, 13)$
$(3, 4)$	$(24, 7, 25)$
$(4, 5)$	$(40, 9, 41)$
…	…

Tabulka 14

4 VYŠŠÍ STUPNĚ DIOFANTICKÝCH ROVNIC

4.1 VELKÁ FERMATOVA VĚTA

V 17. století žil slavný matematik Pierre de Fermat. V roce 1670 byla jeho synem vydána Diofantova Aritmetika doplněna o otcovo pozorování. Na stánkách této knihy vzešlo 48 problémů, z nichž některé z nich byly dokázány a některé vyvráceny. V jedné z poznámek bylo uvedeno, že neexistují přirozená čísla $n \geq 3, x \geq 1, y \geq 1, z \geq 1$ taková, že $x^n + y^n = z^n$. Toto tvrzení bylo nazváno Velká Fermatova věta a Fermat ji uvedl bez důkazu, i když mu prý byl znám a neuvedl ho, protože by se mu do Diofantovy Aritmetiky nevešel. Vyjádřil se takto (Algoritmy.net):

„Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigitas non caperet.“

„Je nemožné rozdělit krychli do dvou krychlí, či čtvrtou mocninu do dvou čtvrtých mocnin, nebo obecně jakoukoli mocninu vyšší než druhou do dvou stejných mocnin. Objevil jsem opravdu tak podivuhodný důkaz, že tento okraj je příliš malý, aby se do něj vešel.“

To způsobilo vlnu matematického bádání. Přes 350 let se matematici celého světa snažili tuto větu dokázat. Úspěšný byl až v roce 1994 Andrew Wiles. Na důkazu pracoval řadu let, je rozsáhlý přes 200 stran, využívá různé části matematiky a na světě existuje velmi malé množství matematiků, kteří jsou mu schopni porozumět.

Obrázek 8 - Velká Fermatova věta na české poštovní známce, [7]

ZÁVĚR

Je jasné, že existuje ještě mnoho typů diofantických rovnic, protože v oboru celých čísel lze řešit jakoukoliv rovnici. Neexistuje však jednotný postup, jak toto řešení nalézt. Je zajímavé, že ačkoliv slovní úlohy vedoucí na diofantické rovnice jsou vytvářeny z praxe (počítáme celé kusy zvěře, lidí, ovoce, předmětů…), s názvem diofantické rovnice se setkáváme až na vysoké škole a děti na základní, potažmo střední škole o tomto názvosloví nevědí. Velmi zajímavé by bylo zkoumat hlouběji kvadratické diofantické úlohy nebo Pellovu rovnici v souvislosti s geometrií.

Řešení diofantických rovnic je možné získat pomocí programu Mathematica, či webového rozhraní Wolframu Alpha. Pokud používáme program Mathematica, je nutné k získání řešení znát přesné názvy příslušných povelů. Můžeme se pokusit vyřešit úvodní příklad, který lze přepsat do matematického vyjádření $4x + 2y = 28$. Zadání v programu by bylo ve tvaru

$$\textbf{Reduce}[4x + 2y == 28, \{x, y\}, \textbf{Integers}],$$

kdy povel „**Reduce**“ se dá přeložit jako „vypočítat“ a povel „**Integers**“ udává, že hledání řešení má být v oboru celých čísel. Z programu dostaneme výsledek

$$C[1] \in Integers \mathbin{\&\&} x = C[1] \mathbin{\&\&} y == 14 - 2C[1],$$

kde C[1] je celočíselný parametr.

Pokud zadáme lineární diofantickou rovnici z úvodního příkladu do webového rozhraní Wolfram Alpha, jedno z nabídnutých řešení je i v oboru celých čísel a je parametricky vyjádřeno následovně

$$x = 7 - n, \qquad y = 2n, \qquad \text{kde } n \in Z.$$

Vzhledem k zadání příkladu však musí $[x, y] \in N$, takže $C[1], n = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Množinou řešení příkladu „Na parkovišti parkují motorky a auta, přičemž hlídač spočítal, že se na parkovišti nachází celkem 28 kol. Zjistěte, kolik hlídal aut a kolik motorek.“, kde v uspořádané dvojici $[x, y]$ odpovídá neznámá x počtu aut a y počtu motorek, jsou uspořádané dvojice [0,14], [1,12], [2,10], [3,8], [4,6], [5,4], [6,2], [7,0].

SHRNUTÍ

Cílem bakalářské práce s názvem Vybrané typy diofantických rovnic a jejich početní využití bylo získání teoretických znalostí o jednotlivých typech rovnic a osvojení si základních metod jejich řešení. V první části práce byla krátce popsána historie slavného Diofanta z Alexandrie a jeho dílo. V průběhu práce jsme probrali lineární diofantické rovnice, kvadratické diofantické rovnice a Pellovu rovnici, v rámci níž jsme vyřešili Archimedovu úlohu o dobytku. V druhé části jsme rozebrali teorii pythagorejských rovnic a Velké Fermatovy věty. Práce obsáhla velké množství slovních úloh z běžného života. Při řešení byly použity metody, které znalostně mohou řešit žáci a studenti na základních, středních i vysokých školách. Ačkoliv je složité najít k diofantickým rovnicím jednotnou literaturu a většina zdrojů je cizojazyčných, podařilo se nám tuto problematiku komplexně shrnout.

RESUMÉ

The aim of the thesis titled “Selected types of diophantine equations and their numerical use” is to gain theoretical knowledge about the different types of equations and to learn the basic methods of solving them. The first section briefly describes the history of the famous Diophantus of Alexandria and his work. During the work we discussed the linear diophantine equations, quadratic equations and Diophantine Pell's equation, within which we solved Archimedes' cattle problem. In the second part, we analyzed the theory of Pythagorean diophantine equations and Fermat's Last theorem. The work contains a lot of verbal tasks in everyday life. In solving this we used that knowledge pupils and students in primary, secondary and high schools. Although it is difficult to find equations diophantine in literature and most of them we drew from foreign-language resources. We were successful in comprehensively summarizing this issue.

SEZNAM LITERATURY

1. Algoritmy.net. Copyright (C) 2008-2015 Algoritmy.net, online: http://www.algoritmy.net/article/48513/Velka-Fermatova-veta

2. BÁRTLOVÁ, T. Archimedova úloha o dobytku. Archimedes' cattle problem. Praha : MATFYZPRESS, Vydavatelství Matematicko-fyzikální fakulty, 2012, online: http://dml.cz/bitstream/handle/10338.dmlcz/402381/DejinyMat_54-2012-1_11.pdf

3. BICAN, L. O řešení Pellovy rovnice. *Rozhledy matematicko-fyzikální*. 1977-1978, roč. 56, č. 5, s. 193-199.

4. BICAN, L. Zobecněná Pellova rovnice. *Rozhledy matematicko-fyzikální*. 1977-1978, roč. 56, č. 6, s. 258-261.

5. DAŇKOVÁ, M. *Diplomová práce:* O řešitelnosti některých typů diofantických rovnic. Plzeň : Západočeská univerzita, 2007. Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

6. DEMLOVÁ, M. Diskrétní matematika a logika, Přednáška 10 – 5/12/2005, online: http://math.feld.cvut.cz/demlova/teaching/dml/pred10.pdf

7. Diophantus of Alexandria. JOC/EFR© February 1999, online: http://www-history.mcs.st-and.ac.uk/history/Biographies/Diophantus.html

8. DRÁBEK, J. *učební texty k předmětu Elementární algebra*.

9. ĎURIŠ, V. a Sovišová, M. Diofantické rovnice a metódy ich riešenia. Nitra : Univerzita Konštantína Filozofa v Nitre, 2011. ISBN 978-80-8094-896-2.

10. HALAS, Z. Archimédes: několik pohledů do jeho života a díla. Praha : Matfyzpress, 2012. stránky 99-108. ISBN 978-80-7378-228-3.

11. Hilbert David, 2014, JOC/EFR © NOVEMBER, online: http://www-history.mcs.st-andrews.ac.uk/Biographies/Hilbert.html

12. HORA, J. Soustavy lineárních diofantickcýh rovnic a Smithův normální tvar matice. Plzeň : South Bohemia Mathematical Letters, 2011.

13. JANSOVÁ, P. *Bakalářská práce:* Diofantické rovnice. Praha : Univerzita Karlova, 2010. Vedoucí práce: Doc. RNDr. Jarmila Novotná, CSc.

14. KOLMAN, A. Dějiny matematiky ve starověku. Praha : Academia, nakladatelstvé Československé akademie věd, 1969. str. 224. ISBN 507-21-875.

15. PETROVÁ, I. *Diplomová práce:* Diofantovské rovnice v úlohách MO a v historii matematiky. Plzeň : Západočeská univerzita, 2012. Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

16. Sciences, Courant Institute of Mathematical. ARCHIMEDES IN THE 21ST CENTURY. New York University, online: http://www.mcs.drexel.edu/~crorres/Archimedes/Cattle/computer2/computer_output.html

17. Wolfram MathWorld. © 1999-2015 Wolfram Research, Inc. | Terms of Use, online: http://mathworld.wolfram.com/

ZDROJE OBRÁZKŮ:

1. Diophantus of Alexandria. JOC/EFR© February 1999, online: http://www-history.mcs.st-and.ac.uk/history/Bookpages/Diophantus4a.gif

2. Hilbert, D. 2014, JOC/EFR © NOVEMBER, online: http://www-history.mcs.st-andrews.ac.uk/PictDisplay/Hilbert.html

3. Wolfram Aplha. © 2015 Wolfram Alpha LLC - A Wolfram Research Company, onine: http://www.wolframalpha.com/

4. Copyright © 2014 Desmos, Inc., online: www.desmos.com/calculator

5. Creative Commons Attribution-Share Alike 3.0 Unported, online: http://commons.wikimedia.org/wiki/File:First_six_triangular_numbers.svg

6. Pythagoras of Samos. JOC/EFR © January 1999, online: http://www-history.mcs.st-andrews.ac.uk/Biographies/Pythagoras.html

7. Filaso.cz ... aneb filatelisté sobě. © 2008-2011 Filaso.cz, online: http://www.filaso.cz/katalog-rocnik/cr/2000

SEZNAM OBRÁZKŮ

SEZNAM PŘÍKLADŮ A JEJICH ŘEŠENÍ

SEZNAM GRAFŮ A TABULEK