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

DIOFANTICKÉ ROVNICE A SLOVNÍ ÚLOHY

BAKALÁŘSKÁ PRÁCE

Kateřina Fischerová
Matematická studia, obor Matematika - Technická výchova

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

Plzeň 2018

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

V Plzni, dne 25. dubna 2018

Fischerová

.....

Kateřina Fischerová

Chtěla bych poděkovat vedoucímu PhDr. Lukáši Honzíkovi, Ph.D. za cenné rady, trpělivost a pomoc při vypracování mé bakalářské práce.

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Kateřina FISCHEROVÁ**
Osobní číslo:	**P15B0010P**
Studijní program:	**B1001 Přírodovědná studia**
Studijní obor:	**Matematická studia**
Název tématu:	**Diofantické rovnice a slovní úlohy**
Zadávající katedra:	**Katedra matematiky, fyziky a technické výchovy**

Zásady pro vypracování:

1. Představení diofantické rovnice, uvedení jejich typů, krátce z historie.
2. Způsob řešení vybraných typů diofantických rovnic s ilustračními úlohami.
3. Slovní úlohy vedoucí na diofantické rovnice, způsob řešení a diskuze přípustných výsledků.

Rozsah grafických prací:

Rozsah kvalifikační práce: **30 - 50**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

DRÁBEK, Jaroslav. přednášky z KMT/Elementární algebra.
DAŇKOVÁ, Magdaléna. O řešitelnosti některých typů diofantovských rovnic. Plzeň, 2007. Diplomová práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.
MOKRÁ, Tereza. Lineární diofantické rovnice. Brno, 2015. Bakalářská práce. Masarykova univerzita. Vedoucí práce Mgr. Vojtěch Žádník, Ph.D.

Vedoucí bakalářské práce: **PhDr. Lukáš Honzík, Ph.D.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání bakalářské práce: **12. června 2017**

Termín odevzdání bakalářské práce: **30. června 2018**

RNDr. Miroslav Randa, Ph.D.
děkan

L.S.

Doc. PaedDr. Jarmila Honzíková, Ph.D.
vedoucí katedry

V Plzni dne 22. června 2017

DIOFANTICKÉ ROVNICE A SLOVNÍ ÚLOHY

(DIOPHANTINE EQUATION AND WORD PROBLEMS)

OBSAH

SEZNAM ZKRATEK

$=$	rovná se
$\neq$	nerovná se
$>, \geq$	větší, větší nebo rovno
$<, \leq$	menší, menší nebo rovno
$(\ ), \langle\ \rangle, \{\ \}$	kulatá, hranatá, složená závorka
ε	náleží, patří do
$\mathbb{N}$	množina přirozených čísel
$\mathbb{Z}$	množina celých čísel
$\wedge$	a zároveň
mod	modulo
x, y, z, w	neznámé
a, b, c, d	konstanty
r, s, t, u	parametry
$D(a, b)$	největší společný dělitel čísel a, b
$\equiv$	kongruence
$\frac{a}{b}$, $b \mid a$, $a : b$	různé zápisy a děleno b
$b \nmid a$	a nedělí b
FÚSZ	fundamentální úplná soustava zbytků
ÚSZ	úplná soustava zbytků

ÚVOD

Pravděpodobně ve 3. století žil v Alexandrii významný matematik, kterého dnes nazýváme „Otec algebry“. O jeho životě se dochovalo pouze pár informací, avšak nemůžeme s jistotou prohlásit, že jsou pravdivé. S jistotou se neví ani přesné jméno tohoto matematika – existuje několik možných mutací a to: Diofantos, Diofantes nebo dokonce dle [6] Diofantus. Pro přehlednost budeme jméno tohoto matematika uvádět ve tvaru Diofantos, stejně jako česká odborná literatura.

Právě tento matematik se zabýval mimo jiné i neurčitými rovnicemi, které se na jeho počest nazývají diofantické. Téma diofantické rovnice je ale poměrně obsáhlé, a proto se budu v této práci zabývat pouze základním druhem diofantických rovnic – lineárními diofantickými rovnicemi a slovními úlohami. Znalost těchto lineárních diofantických rovnic je nezbytná pro pokračování v této obsáhlé problematice.

Cílem této práce je vytvořit ucelený materiál o lineárních diofantických rovnicích a látku vysvětlit co nejpochopitelněji. Řekneme si, co jsou to diofantické rovnice, jaké druhy diofantických rovnic existují a jakými způsoby je lze počítat. V závěru bych ráda zodpověděla otázku: **Existuje jednotný algoritmus pro výpočet diofantické rovnice? Pokud ne, je nějaký způsob řešení výhodnější než jiný? Kdy je vhodné daný způsob řešení použít?**

Motivace:

Pokud jste o diofantických rovnicích nikdy neslyšeli, věřte, že jste za svůj život již několik lineárních diofantických rovnic spočítali. Lineární diofantické rovnice jsou totiž často pouze přepsané životní situace do světa matematiky. Uvedeme si motivační příklad, který zvládne vyřešit každý z nás.

„V obchodě jsme nakoupili za 300,- korun. Zjistili jsme, že v peněžence máme pouze mince v hodnotách 5, 10 a 20 korun. Jak lze zaplatit nákup?“

1 DIOFANTOS Z ALEXANDRIE A DIOFANTICKÉ ROVNICE

1.1 DIOFANTOS Z ALEXANDRIE

Diofantův život je plný záhad již od jeho počátku, jelikož nemůžeme s jistotou určit ani to, v jakých letech žil. Můžeme alespoň vzdáleně odhadnout století. Diofantos ve svých dílech odkazuje na jména jiných matematiků, o kterých víme přibližné období jejich života – podle zdrojů z [12] cituje například Hypsiklése (190 př. n. l – 120 př. n. l.), kterým je tak určena spodní možná hranice. Horní hranici odhadujeme podle komentáře matematika Theona z Alexandrie, který ve svém díle zmiňuje právě Diofantovo dílo, a proto datujeme jeho možnou smrt přibližně k roku 350 n. l. Toto nepřesně vymezené období se francouzský historik Paul Tannery snažil ještě zpřesnit. To se mu povedlo, a tak na základě všech těchto indicií odhadujeme, že Diofantos žil okolo roku 250 n. l. – 350 n. l.

Diofantos za svůj život napsal mnoho matematických děl, z nichž nejznámějšími jsou dle [9] Arithmetica, Porismata, Moriastika[1] a pojednání o „polygonálních“ číslech. Dochovala se však pouze „polygonální“ čísla a část Arithmeticy. Právě Arithmetica Diofanta nejvíce proslavila. Arithmetica je sbírka třinácti knih, ze kterých se nám jich dochovalo pouze šest. Existují ještě čtyři arabské knihy, které se pokládají za překlad Arithmeticy. Sbírka obsahuje 130 - 189 úloh včetně řešení a vysvětlivek, ve kterých se Diofantos zabýval řešením určitých[2] i neurčitých[3] rovnic a teorií čísel. Avšak základním přínosem pro matematiku byl právě jeho způsob řešení neurčitých rovnic, o kterých se budeme bavit v dalších kapitolách. Podle [9] bylo řešením neurčitých rovnic pouze kladné celé číslo. U Diofanta se nesetkáváme s nulou ani se zápornými čísly – nulu jako výsledné řešení neuznával a záporná řešení mu přišla protismyslná[4]. Diofantos jako první začal používat matematický zápis, který je založený na symbolech[5], jež využíváme dodnes – vybudoval tak základy algebraického zápisu. Používal pouze jednu neznámou x, kterou nazýval „číslo“, a používal pro ni symbol ς´. Zjednodušil řecké zapisování číslic a zavedl například zvláštní označení pro jednotlivé mocniny až do šestého řádu (mocniny vyššího stupně neuvažoval). Například druhou mocninu nazýval dĘnamica - δ^{υ}, třetí kĘboc - κ^{υ} atd. Zabýval se také

[1] Obsah děl Porismata a Moriastika není znám, víme o nich pouze ze zmínky v díle Arithmetica.
[2] Určité rovnice mají jednu proměnnou a jasný počet řešení.
[3] Neurčité rovnice mají 2 či více proměnných a nekonečně mnoho řešení.
[4] Dnes akceptujeme všechna celočíselná řešení.
[5] Za symboly volil počáteční písmena příslušných řeckých názvů.

převrácenou hodnotou neznámé x. Dílo Arithmetica sehrálo důležitou roli pro vznik Velké Fermatovy věty.

Téměř v každé literatuře, ve které je alespoň náznak o Diofantově životě, je uvedena i hádanka, kterou si dle [6] nechal Diofantos vytesat na vlastní náhrobek. Je to jediný zdroj informací o Diofantově osobním životě, který se dochoval, a proto se s tímto zdrojem informací musíme spokojit. Ačkoliv existuje několik variant překladů této hádanky, poselství této zprávy je stejné. Výsledkem této hádanky je věk, kterého se Diofantos údajně dožil.

Zde je znění hádanky v češtině dle [12]:

„ Zde leží Diofantos, jaký to div, algebra poví, jak dlouho byl živ;
Bůh dal mu dětský věk šestinu žití, dvanáctinu pak, než vousy moh míti;
Po další sedmině svou ženu si vzal; a za pět let otcem syna se stal.
Ach, ubohé dítě mudrce a pána! Žil dvakrát míň než otec a už mu zvoní hrana!
Ještě čtyři léta do čísel se nořil, než i jeho čas se konečně završil.“

Nyní zkusíme hádanku vyřešit.

Jestliže označíme Diofantův věk, kterého se dožil jako x, pak rovnice bude vypadat takto

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

Výrazy obsahující x převedeme na levou stranu rovnice

$$x - \frac{x}{6} - \frac{x}{12} - \frac{x}{7} - \frac{x}{2} = 9.$$

Najdeme společného jmenovatele, kterým je číslo $84 = 7 \cdot 12$.

$$\frac{84x - 14x - 7x - 12x - 42x}{84} = 9$$

Upravíme rovnici

$$\frac{9x}{84} = 9.$$

Pro samotné x dostaneme

$$x = 84.$$

Zjistili jsme, že Diofantos žil údajně 84 let. Jeho dětství trvalo 14 let, vousy mu narostly ve 21 letech, ve 33 letech se oženil a ve 38 se mu narodil syn. Ten zemřel ve věku 42 let, to bylo Diofantovi 80 let. O 4 roky později zemřel.

1.2 DIOFANTICKÉ ROVNICE

Stejně jako se neužívá jednotného jména pro Diofanta, ani název této problematiky není jednotný. Různí autoři nazývají tyto rovnice různě: diofantské, diofantovské nebo diofantické. Stále se však jedná o stejný matematický pojem - o neurčité rovnice. V kurzu elementární algebry, jsem se setkala s pojmem diofantické rovnice, a proto tento výraz budu užívat v celé práci. Ačkoliv jsou diofantické rovnice spojovány především s Diofantem, zabývali se tímto problémem dávno před ním i po něm jiní matematici.

Již práce Herona z 1. st. n. l. naznačuje princip počítání neurčitých rovnic, nicméně nejedná se o obecné řešení, nýbrž pouze o řešení s konkrétními čísly. Diofantos také navazuje na staročínské dílo „Matematika v devíti knihách“, ve které jsou řešeny pythagorejské neurčité rovnice. Mezi další zdroje patří také Pellovy rovnice neboli Fermatovy rovnice. Otázkou je. Existuje nějaký obecný algoritmus o konečném počtu kroků k získání řešení u všech typů diofantických rovnic? Tímto problémem se zabýval německý matematik David Hilbert, jehož desátý z dvaceti tří tzv. Hilbertových problémů se této otázce věnuje. Nejen tento, ale i další problémy byly tehdy neřešitelné. Nyní je velká část těchto problémů vyřešena. Desátý problém o diofantických rovnicích vyřešil až v roce 1970 ruský matematik Jurij Vladimirovič Matijasevič, který dokázal, že univerzální algoritmus neexistuje. Také zjistil, že nelze vyřešit každou diofantickou rovnici. Diofantické rovnice tak musíme řešit podle typů, což dělá z diofantických rovnic poměrně obtížný obor.

Takto zní obecná definice diofantické rovnice.

DEFINICE 1.1 (DIOFANTICKÉ ROVNICE)

Diofantickou rovnicí o n neznámých rozumíme neurčitou polynomiální rovnici ve tvaru $f(x_1, x_2, x_3, \dots\dots, x_n) = 0$, která dovoluje proměnným $x_1, x_2, x_3, \dots\dots, x_n$ nabývat pouze hodnot z oboru celých čísel. Řešením této rovnice budeme nazývat každou $n - tici$ $[a_1, a_2, \dots\dots, a_n]$, pro kterou je $f(a_1, a_2, \dots\dots, a_n) = 0$.

1.2.1 TYPY DIOFANTICKÝCH ROVNIC

Existuje široká škála diofantických rovnic. Diofantické rovnice můžeme rozdělit na rovnice lineární[6] a kvadratické[7]. Existuje však i vyšší stupeň diofantických rovnic, které vycházejí z Pythagorovy věty - Velká Fermatova věta. Lineární a kvadratické rovnice se dále dělí podle počtu neznámých, které obsahují. Nyní si uvedeme několik typů diofantických rovnic.

a) Lineární diofantické rovnice

DEFINICE 1.2 (LINEÁRNÍ DIOFANTICKÉ ROVNICE)

Lineární diofantické rovnice o n neznámých jsou algebraické rovnice ve tvaru

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \mathrm{b}, \qquad (1.1)$$

kde koeficienty $a_1, a_2, \dots\dots, a_n \in \mathbb{Z}, b \in \mathbb{Z}$.

S lineárními diofantickými rovnicemi se setkávají i lidé, kteří nikdy tento pojem neslyšeli. Nevědomky se totiž řeší v běžném životě, v mateřských školách, případně až na základní škole – jsou to běžné životní situace přepsané pouze do jazyka matematiky. Běžně lidé řeší lineární diofantické rovnice experimentem neboli „metodou pokus – omyl“.

[6] Lineární rovnice neboli rovnice 1. stupně – alespoň jedna z neznámých je v první mocnině.
[7] Kvadratické rovnice neboli rovnice 2. stupně – alespoň jedna z neznámých je v druhé mocnině.

b) Kvadratické diofantické rovnice

a. Kvadratické diofantické rovnice o dvou neznámých

DEFINICE 1.3 (KVADRATICKÉ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH)

Kvadratickými diofantickými rovnicemi o dvou neznámých x, y rozumíme rovnici ve tvaru $ax^2 + bx + cxy + dy + ey^2 = f$, kde koeficienty $a, b, c, d, e \in \mathbb{Z}, f \in \mathbb{Z}$. Řešením rovnice je každá uspořádaná dvojice $[x_0, y_0] \in \mathbb{Z}^2$, pro kterou platí, že $ax_0^2 + bx_0 + cx_0y_0 + dy_0 + ey_0^2 = f$.

Pro kvadratické diofantické rovnice o dvou neznámých není znám jednotný algoritmus pro získání všech řešení. Pro některé speciální typy taková metoda existuje, případně jsou známy alespoň slabší vlastnosti řešení (např. jak z jednoho řešení nalézt řešení další nebo až nekonečně mnoho řešení.

b. Pellova rovnice

DEFINICE 1.4 (PELLOVA ROVNICE)

Pellova rovnice je jedna z typů kvadratických diofantických rovnic o dvou neznámých x, y, kterou lze zapsat rovnicí ve tvaru $x^2 + Dy^2 = 1$, kde $D \in \mathbb{N}$ a zároveň D není druhou mocninou žádného přirozeného čísla. Řešení x, y hledáme v celých číslech.

Existuje i zobecněný tvar Pellovy rovnice, který se liší pouze hodnotou konstanty na pravé straně – tvar rovnice je tedy $x^2 + Dy^2 = E$, kde $D \in \mathbb{N}, E \in \mathbb{Z}$, a zároveň D není druhou mocninou žádného přirozeného čísla.

Touto rovnicí se zabýval již indický matematik Brahmagupta v 7. století n. l., avšak byla známa pouze určitá řešení pro vybrané typy Pellovy rovnice. První, kdo přišel na obecné řešení této rovnice, byl Pierre de Fermat, který žil v 17. století.

c. Pythagorejská rovnice

DEFINICE 1.5 (PYTHAGOREJSKÁ ROVNICE)

Pythagorejská rovnice patří mezi kvadratické diofantické rovnice. Je to rovnice o třech neznámých x, y, z tak, že $x, y, z \in \mathbb{N}$, kterou lze zapsat rovnicí ve tvaru $x^2 + y^2 = \mathrm{z}^2$. Řešením jsou tzv. pythagorejské trojice, kterých je nekonečně mnoho.

Název této rovnice je odvozen od Pythagorovy věty, se kterou se každý setkal v geometrii na základní škole. Pythagorova věta popisuje podobný vztah, který platí pro strany pravoúhlého trojúhelníka. Řešením jsou pythagorejské trojice[8]. Nejznámější řešení jsou trojice $3, 4, 5$ ($x = 3, y = 4, z = 5$ - x, y lze zaměnit) nebo $5, 12, 13$, které značily celočíselné délky stran. Touto záležitostí se zabývali již antičtí Řekové, ale tehdy ji nenazývaly diofantické rovnice.

d. Velká Fermatova věta

Velká Fermatova věta je ve skutečnosti Pythagorejská rovnice, kde místo druhých mocnin řešíme rovnici pro mocninu n, kde $n \geq 3$. Rovnici lze zapsat ve tvaru $x^n + y^n = z^n$. Přes tři století trvalo velkým matematikům dokázat, že pro tuto rovnici neexistují přirozená řešení.

e. Thueovy rovnice

Rovnice ve tvaru $\sum_{i=0}^{n} a_i\, x^i y^{n-i} = c$, kde $n \geq 3$ a $c \neq 0$. Tyto rovnice jsou zpravidla řešitelné.

f. Erdös-Strassova domněnka

Rovnice ve tvaru $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ neboli v polynomiálním tvaru $4xyz = n(xy + xz + yz)$. Domníváme se, že pro každé číslo $n \geq 2$, $n \in \mathbb{N}$ existuje řešení kladných celých čísel x, y, z.

[8] Pythagorejská trojice – tři celočíselná řešení x, y, z, pro která platí $x^2 + y^2 = \mathrm{z}^2$.

2 DŮLEŽITÉ POJMY

Dříve než se budeme zabývat způsoby řešení lineárních diofantických rovnic, musíme si vysvětlit (případně připomenout) několik pojmů, které budeme potřebovat. Dále je vhodné se orientovat v použitých zkratkách pro správné pochopení všech pojmů (viz Seznam zkratek na straně 3).

2.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

DEFINICE 2.1 (NEJVĚTŠÍ SPOLEČNÝ DĚLITEL)

Nechť čísla $a, b \in \mathbb{N}, D \in \mathbb{N}$. Pak D je společný dělitel čísel a a b, pokud $D|a \wedge D|b$. Číslo D je největší společný dělitel a a b, značíme $D = D\ (a, b)$, pokud navíc platí, že kdykoli k je společný dělitel a a b, pak $k|D$.

Největšího společného dělitele dvou čísel lze určit pomocí prvočíselného rozkladu. Každé číslo můžeme vyjádřit jako součin prvočísel[9]. Největší společný dělitel je součin prvočísel vyskytujících se v obou rozkladech. Tento výpočet je snadno pochopitelný. V praxi je bohužel nepoužitelný s výjimkou velice malých čísel – je pracný a pomalý. Proto využíváme rychlejších algoritmů, hlavně tzv. Eukleidova algoritmu – ten je založený na dělení přirozených čísel se zbytkem.

VĚTA 2.1 (DĚLENÍ PŘIROZENÝCH ČÍSEL SE ZBYTKEM)

Pro libovolná čísla $a, b \in \mathbb{N}$ existují jednoznačně určená čísla $k, z \in \mathbb{N}$ tak, že $b = ka + z$, kde $0 \leq z \leq a$

Důkaz lze najít v [7] na straně 168.

[9] Prvočíslo je přirozené číslo, které kromě jedničky a samo sebe není dělitelné žádným jiným přirozeným číslem.

VĚTA 2.2 (EUKLEIDŮV ALGORITMUS)

Mějme dvě čísla $a, b \in \mathbb{N}$. Hledáme největšího společného dělitele $D(a,b)$ ve dvou krocích. Nechť $a < b$, pak číslo b vydělíme číslem a se zbytkem, dostaneme tedy $b = k_1 a + z_1$, kde $k_1, z_1 \in \mathbb{N} \cup \{0\} \wedge z_1 < a$. Pokud $z_1 = 0$, pak $a|b$, resp. $a = D(a,b) \rightarrow$ **konec algoritmu**

Jinak pokračuji v algoritmu. Čísla a, z_1 mají stejné společné dělitele jako a a b. Číslo a vydělíme číslem z_1 se zbytkem z_2, tedy $a = k_2 z_1 + z_2$, kde $k_2, z_2 \in \mathbb{N} \cup \{0\} \wedge z_2 < z_1$. Pokud je $z_2 = 0$, pak $z_1|a,\ z_1 = D(a, z_1) = D(a,b) \rightarrow$ **konec algoritmu.**

Jestliže je $z_2 \neq 0$, opakuji algoritmus do doby, dokud nezískám $z_n = 0$.

Posloupnost zbytků $z_1, z_2, \dots, z_n$ je klesající, a proto po konečném počtu kroků dojdeme k $z_n = 0$, kde algoritmus skončí. Největším společným dělitelem čísel a, b je poslední nenulový zbytek, tedy z_{n-1}.

Zpětným dosazením do Eukleidova algoritmu získáme tzv. Bezoutovu rovnost, pomocí níž najdeme celočíselnou kombinaci daných čísel.

VĚTA 2.3 (BEZOUTOVA ROVNOST)

Zpětným dosazením do Věty 2.2 můžeme největšího společného dělitele dvou čísel vyjádřit jako lineární celočíselnou kombinaci těchto dvou čísel. Najdeme x, y tak, že $z_{n-1} = z_1 x + z_2 y$. (2.1)

Vycházíme z posledního nenulového zbytku z_{n-1} – největšího společného dělitele. Vyjádříme jej jako celočíselnou kombinaci čísel a a b. Budeme postupovat od z_{n-1} směrem vzhůru a to tak, že z jednotlivých rovností budeme vyjadřovat nalezené zbytky, resp. zbytky budeme osamostatňovat a následně je budeme vyjadřovat pomocí předchozích zbytků. Nyní si tyto pojmy zkusíme v praxi na příkladu.

Příklad 2.1. Pomocí Eukleidova algoritmu nalezněte $D(142, 994)$. Po nalezení největšího společného dělitele budeme chtít vyjádřit jeho celočíselnou kombinaci pomocí zadaných čísel 142 a 994.

Řešení:

Podle Věty 2.2 na straně 12 spustíme algoritmus.

$$142 < 994$$

$$994 = 142 \cdot 7 + \mathbf{0}\ (0 < 142), \qquad 0 = 0$$

Algoritmus skončil hned po prvním kroku. Jelikož je číslo 142 zároveň dělitelem čísla 994, pak je číslo 142 největším společným dělitelem

$$142 \ = \ D\ (142, 994).$$

Nelze najít celočíselnou kombinaci čísel pomocí Věty 2.3 na straně 12 – nemůžeme vycházet z posledního nenulového zbytku, jelikož nám algoritmus skončil po prvním kroku. Nicméně můžeme vyjádřit celočíselnou kombinaci tak, že si půjčíme jednoho dělitele 142 z úplného podílu a celočíselnou kombinaci vyjádříme jako

$$142 \ = \ 994 \cdot 1 - 142 \cdot 6.$$

Příklad 2.2. Pomocí Eukleidova algoritmu nalezněte $D(843, 684)$. Po nalezení největšího společného dělitele budeme chtít vyjádřit jeho celočíselnou kombinaci pomocí zadaných čísel 843 a 684.

Řešení:

Dle Věty 2.2 na straně 12 provedeme algoritmus.

$$684 < 843$$

$$843 = 684 \cdot 1 + \mathbf{159}\ (159 < 684), \qquad 159 \neq 0$$

$$684 = 159 \cdot 4 + \mathbf{48}\ (48 < 159), \qquad 48 \neq 0$$

$$159 = 48 \cdot 3 + \mathbf{15}\ \ (15 < 48), \qquad 15 \neq 0$$

$$48 = 15 \cdot 3 + \boxed{\mathbf{3}}\ (3 < 15), \qquad 3 \neq 0$$

$$15 = 3 \cdot 5 + \mathbf{0}\ (0 < 3), \qquad \mathbf{0} = \mathbf{0}$$

$$konec\ algoritmu.$$

$$D(843, 684) = 3$$

Nyní vycházíme z největšího společného dělitele (zde je jím číslo 3) a vyjádříme jej pomocí Věty 2.3 na straně 12 jako celočíselnou kombinaci čísel 843 a 684. V algoritmu postupujeme odspoda nahoru a osamostatňujeme zbytky

$$3 = 48 \cdot 1 - 15 \cdot 3,$$

$$15 = 159 \cdot 1 - 48 \cdot 3,$$

$$48 = 684 \cdot 1 - 159 \cdot 4,$$

$$159 = 843 \cdot 1 - 684 \cdot 1.$$

Nyní najdeme kombinaci čísel 843 a 684 pomocí výše zmíněných rovností.

$$3 = 48 \cdot 1 - 15 \cdot 3 = 48 \cdot 1 - (159 \cdot 1 - 48 \cdot 3) \cdot 3 = -159 \cdot 3 + 48 \cdot 10 = -159 \cdot 3 +$$
$$+ (684 \cdot 1 - 159 \cdot 4) \cdot 10 = 684 \cdot 10 - 159 \cdot 43 = 684 \cdot 10 - (843 \cdot 1 - 684 \cdot 1) \cdot$$
$$\cdot 43 = 684 \cdot 10 + 684 \cdot 43 - 843 \cdot 43 = 684 \cdot 53 - 843 \cdot 43$$

Hledaná celočíselná kombinace čísel 843 a 684 je ve tvaru

$$3 = 684 \cdot 53 - 843 \cdot 43.$$

Upravíme do tvaru dle (2.1) na straně 12

$$3 = 843 \cdot (-43) + 684 \cdot 53.$$

2.2 KONGRUENCE

Kongruencemi se zabýval matematik Johann Carl Friedrich Gauss. Jen díky němu můžeme dlouhé a komplikované zápisy rovnic zapsat jednoduše a přehledně, a proto jsou v dnešní době hojně užívány.

DEFINICE 2.2 (KONGRUENCE)

Nechť máme čísla $a, b \in \mathbb{Z}$. Jestliže mají tato čísla a, b při dělení přirozeným číslem m, kde $m \geq 2$, stejný zbytek z, kde $0 \leq z < m$, pak se nazývají čísla a, b kongruentní podle modulo m. Zapisujeme

$$a \equiv b \ (mod\ m).$$

Existuje několik možných ekvivalentních zápisů kongruence pro libovolná čísla $a, b \in \mathbb{Z}, m \in \mathbb{N}$:

1. $a \equiv b \ (mod\ m)$
2. $a = b + mk$, kde $k \in \mathbb{Z}$
3. $m \mid (a - b)$

Kongruence podle daného modulo m je na množině celých čísel relací ekvivalence[10]. Tato relace vytváří na množině celých čísel rozklad na tzv. zbytkové třídy[11]. Tyto zbytkové třídy zpravidla značíme:

Z_0 – množina všech celých čísel, která jsou dělitelná číslem m beze zbytku,

Z_1 – množina všech celých čísel, která jsou dělitelná číslem m se zbytkem 1,

…,

Z_{m-1} – množina všech celých čísel, která po dělení číslem m mají zbytek $m - 1$.

Pro znázornění si uvedeme konkrétní příklad zbytkových tříd při kongruenci modulo 4.

$$Z_0 = \{\dots, -12, -8, -4, 0, 4, 8, 12, 16, \dots\}$$
$$Z_1 = \{\dots, -11, -7, -3, 1, 5, 9, 13, 17, \dots\}$$
$$Z_2 = \{\dots, -10, -6, -2, 2, 6, 10, 14, 18, \dots\}$$
$$Z_3 = \{\dots, -9, -5, -1, 3, 7, 11, 15, 19, \dots\}$$

Vybereme-li z každé zbytkové třídy jednoho libovolného zástupce, pak množina těchto zástupců tvoří úplnou soustavu zbytků (ÚSZ) – např. $\{-12, 1, 10, 19\}$. Vybereme-li z každé zbytkové třídy nejmenšího nezáporného zástupce, poté množina těchto zástupců tvoří fundamentální úplnou soustavu zbytků (FÚSZ) - $\{0, 1, 2, 3\}$. Nyní si tyto dva pojmy řádně zavedeme.

[10] Relace ekvivalence = relace reflexivní, relace symetrická a zároveň relace tranzitivní. Důkaz lze najít v [4].

[11] Zbytkovou třídou modulo m rozumíme množinu všech celých čísel, které při dělení přirozeným číslem m dávají stejný zbytek.

DEFINICE 2.3 (ÚPLNÁ SOUSTAVA ZBYTKŮ)

Množina čísel $\{z_1, z_2, \dots, z_m\}$ tvoří úplnou soustavu zbytků (ÚSZ) podle modulo m, právě tehdy, když platí

$$(\forall\, i, j): i \neq j \;\Rightarrow z_i \not\equiv z_j \;(mod\; m)$$

DEFINICE 2.4 (FUNDAMENTÁLNÍ ÚPLNÁ SOUSTAVA ZBYTKŮ)

Množinu čísel $\{0, 1, \dots, m-1\}$ nazýváme fundamentální úplnou soustavu zbytků (FÚSZ) podle modulo m.

2.2.1 ZÁKLADNÍ VLASTNOSTI KONGRUENCÍ

Existuje několik pravidel resp. vlastností, které nám pomohou najít řešení. Neexistuje jediný způsob řešení, cest k výsledku je obvykle více. Pro počítání s kongruencemi je důležitý cvik a představivost, jaké vlastnosti se vyplatí použít. Důkazy těchto vět plynou přímo z definice kongruence a najdeme je např. v [4].

VĚTA 2.4

Nechť máme kongruenci $a \equiv b\; (mod\; m)$.

A) PŘIČTENÍ LIBOVOLNÉHO CELÉHO ČÍSLA

K oběma stranám kongruence můžeme přičíst libovolné číslo $c \in \mathbb{Z}$

$$a + c \equiv b + c\; (mod\; m).$$

B) NÁSOBENÍ LIBOVOLNÝM CELÝM ČÍSLEM

K oběma stranám kongruence můžeme přinásobit libovolné číslo $c \in \mathbb{Z}$

$$a \cdot c \equiv b \cdot c\; (mod\; m).$$

C) UMOCNĚNÍ PŘIROZENÝM ČÍSLEM

Obě strany kongruence lze umocnit o též přirozené číslo $k \in \mathbb{N}$

$$a^k \equiv b^k\; (mod\; m).$$

D) PŘIČTENÍ NÁSOBKU MODULO m

Na jakoukoli stranu kongruence můžeme přičíst libovolný x-násobek modulo m

$$a + x \cdot m \equiv b \ (mod\ m) \text{ nebo } a \equiv b + x \cdot m \ (mod\ m).$$

E) PŘENESENÍ SČÍTANCE Z JEDNÉ STRANY KONGRUENCE NA DRUHOU

Libovolný sčítanec kongruence lze přenést s opačným znaménkem z jedné strany kongruence na druhou stranu

$$a - b \equiv 0 \ (mod\ m).$$

F) KRÁCENÍ KONGRUENCE ČÍSLEM

Jestliže z čísel a i b lze vytknout číslo c, pak obě strany kongruence lze vydělit číslem $c \in \mathbb{Z}$.

Jestliže $m \nmid c$

$$\frac{a}{c} \equiv \frac{b}{c} \ (mod\ m).$$

Jestliže $m|c$, pak musíme vydělit číslem c i modul

$$\frac{a}{c} \equiv \frac{b}{c} \left(mod \frac{m}{c}\right).$$

Nechť máme kongruence $a \equiv b \ (mod\ m)$, $c \equiv d \ (mod\ m)$.

G) SČÍTÁNÍ KONGRUENCÍ PODLE TÉHOŽ MODULU M

Máme-li kongruence podle téhož modulu m, pak je lze sečíst

$$a + c \equiv b + d \ (mod\ m).$$

H) NÁSOBENÍ KONGRUENCÍ PODLE TÉHOŽ MODULU M

Máme-li kongruence podle téhož modulu m, pak je lze vynásobit a platí

$$a \cdot c \equiv b \cdot d \ (mod\ m).$$

2.3 LINEÁRNÍ KONGRUENCE O JEDNÉ NEZNÁMÉ

Lineární diofantické rovnice o dvou neznámých lze transformovat na lineární kongruence o jedné neznámé. Tato metoda se hojně využívá k řešení lineárních diofantických rovnic o dvou neznámých.

DEFINICE 2.5 (LINEÁRNÍ KONGRUENCE O JEDNÉ NEZNÁMÉ)

Lineární kongruencí o jedné neznámé x budeme nazývat rovnici

$$ax \equiv b \ (mod\ m), \tag{2.2}$$

kde $a \not\equiv 0(mod\ m)$(resp. a není dělitelné m); $a, b \in \mathbb{Z}, m \geq 2 \ \wedge m \in \mathbb{N}$

Lineární kongruence o jedné neznámé můžeme řešit několika způsoby – tabulkou, jednoduchými úpravami pomocí základních vlastností kongruence, Eulerovou metodou nebo metodou rozkladu modulu. Způsob řešení musíme volit na základě složitosti příkladu. Eulerova metoda a metoda rozkladu modulu jsou již složitější metody, které pro naše účely nebudeme potřebovat – můžeme je najít např. v [4] nebo v [5].

V dalších podkapitolách se přesvědčíme o tom, že každý příklad může mít jiný počet řešení, případně řešení nemusí existovat. Proto nyní zavedeme větu o řešitelnosti, která je zároveň větou o počtu řešení.

VĚTA 2.5 (ŘEŠITELNOST LINEÁRNÍ KONGRUENCE O JEDNÉ NEZNÁMÉ)

Nechť máme lineární kongruenci $ax \equiv b \ (mod\ m)$. Jestliže platí $D(a, m) = d \ \wedge d|b$, pak je tato kongruence řešitelná a má ve (FÚSZ) a tím i v (ÚSZ) právě d řešení. Jestliže platí $d \nmid b$, pak tato kongruence nemá řešení ve (FÚSZ), tím pádem ani v (ÚSZ).

2.3.1 TABULKOVÁ METODA

Na třech jednoduchých příkladech ukážeme způsob řešení lineárních kongruencí o jedné neznámé pomocí tabulky. Věta 2.5 o řešitelnosti se zpravidla používá jako první krok řešení lineární kongruence – my ji u této metody použijeme až na konci každého příkladu – jako kontrolu, zdali jsme objevili veškerá řešení. U tabulkové metody je velmi malá pravděpodobnost, že by nám některá řešení unikla (za předpokladu, že nemáme

chybu ve výpočtu). U dalších metod bude využití této věty vždy prvním krokem řešení. Řešení pomocí tabulky je intuitivní a lehké, ovšem ne vždy výhodné – není dostatečně rychlé (pro případ vysokého čísla u neznámé x) a není příliš efektivní.

Příklad 2.3. Řešte lineární kongruenci $7x + 1 \equiv 0\ (mod\ 8)$.

Řešení:

Lineární kongruenci o jedné neznámé můžeme řešit pomocí tabulky o třech řádcích. Do prvního řádku zapíšeme veškerá čísla patřící do (FÚSZ) podle daného modulu – v našem případě podle modulo 8 – za x tím pádem zvolíme čísla 0, 1, 2, 3, 4, 5, 6 a 7. Do druhého řádku zapíšeme výslednou hodnotu příslušného výrazu a do třetího řádku zapíšeme výslednou kongruenci, kterou vypočítáme jako redukci druhého řádku do (FÚSZ) – druhý řádek dělíme modulem 8 a do třetího řádku zapisujeme zbytek po dělení.

$\boldsymbol{x}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$\boldsymbol{7x+1}$	1	8	15	22	29	36	43	50
$\boldsymbol{7x+1\ (mod\ 8)}$	1	0	7	6	5	4	3	2

Tabulka 1: Výsledek kongruence $7x + 1 \equiv 0\ (mod\ 8)$

Řešení kongruence $7x + 1 \equiv 0\ (mod\ 8)$ budeme hledat v posledním řádku Tabulka 1. Zajímají nás řešení, kdy v posledním řádku musíme najít hodnotu 0. Kongruence $7x + 1 \equiv 0\ (mod\ 8)$ má řešení pouze jedno a to $x = 1$. Počet všech řešení v množině $\mathbb{Z}$ je nekonečně mnoho (k námi nalezenému řešení přičteme násobky modulu, tedy násobky čísla 8) přesně řečeno $x = 1 + 8t, t \in \mathbb{Z}$.

Kontrola:

Nyní použijeme Větu 2.5 na straně 18 a ověříme, zda má daná kongruence právě jedno řešení

$$D(7,8) = 1\ \wedge 1|1.$$

Ověřili jsme, že existuje právě jedno řešení, jelikož čísla 7 a 8 mají největšího společného dělitele číslo 1, které zároveň dělí 1. Jelikož největší společný dělitel je číslo 1, existuje zároveň právě jedno řešení v (FÚSZ) i v každé libovolně zvolené (ÚSZ).

Příklad 2.4. Řešte lineární kongruenci $2x + 3 \equiv 0\ (mod\ 8)$.

Řešení:

Tuto lineární kongruenci vyřešíme stejným postupem jako Příklad 2.3 na straně 19.

$\boldsymbol{x}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$\boldsymbol{2x+3}$	3	5	7	9	11	13	15	17
$\boldsymbol{2x+3\ (mod\ 8)}$	3	5	7	1	3	5	7	1

Tabulka 2: Výsledek kongruence $2x + 3 \equiv 0\ (mod\ 8)$

Kongruence $2x + 3 \equiv 0\ (mod\ 8)$ nenastane v žádném z případů. Daná kongruence nemá řešení.

Kontrola:

Opět se přesvědčíme pomocí Věty 2.5 na straně 18 o neřešitelnosti této kongruence.

$$D(2,8) = 2\ \wedge 2 \nmid 3$$

Tato kongruence nemá řešení, protože největší společný dělitel čísel 2 a 8 je číslo 2, jenže číslo 2 zároveň nedělí číslo 3. Daná kongruence nemá ve (FÚSZ) řešení (tím pádem nemá řešení ani v (ÚSZ)).

Příklad 2.5. Řešte lineární kongruenci $6x + 4 \equiv (mod\ 8)$.

Řešení:

Opět volíme stejný způsob řešení jako v Příkladu 2.3 na straně 19.

$\boldsymbol{x}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$\boldsymbol{6x+4}$	4	10	16	22	28	34	40	46
$\boldsymbol{6x+4\ (mod\ 8)}$	4	2	0	6	4	2	0	6

Tabulka 3: Výsledek kongruence $6x + 4 \equiv (mod\ 8)$

Daná kongruence má právě dvě řešení $x_1 = 2,\ x_2 = 6$.

Všechna řešení v $\mathbb{Z}$

$$x_1 = 2 + 8t, t \in \mathbb{Z},$$

$$x_2 = 6 + 8t, t \in \mathbb{Z}.$$

Kontrola:

Opět aplikujeme Větu 2.5 na straně 18 a přesvědčíme se o počtu řešení této kongruence.

$$D(6,8) = 2 \ \wedge 2|4$$

Tato kongruence je řešitelná, jelikož největší společný dělitel čísel 6 a 8 je číslo 2. Číslo 2 zároveň dělí číslo 4. Největším společným dělitelem je číslo 2, a proto existují právě dvě řešení v (FÚSZ) i v každé libovolně zvolené (ÚSZ).

2.3.2 ŘEŠENÍ POMOCÍ JEDNODUCHÝCH ÚPRAV

Tento způsob řešení využívá úprav kongruence. Takovýto postup vede k výsledku nejrychleji a nejjednodušeji, lze jej použít i místo tabulkového řešení.

Příklad 2.6. Řešte kongruenci $14x \equiv 8\ (mod\ 10)$.

Řešení:

Nejdříve ověříme, zda má kongruence řešení, případně zjistíme počet řešení

$$D(14,10) = 2 \ \wedge 2|8.$$

Kongruence má dvě řešení v (FÚSZ) i v každé libovolně zvolené (ÚSZ).

Nyní budeme kongruenci upravovat pomocí základních vlastností z Věty 2.4 na straně 16.

Levou stranu kongruence nahradíme číslem, které je s číslem 14 kongruentní podle modulu 10 a patří do (FÚSZ) – číslem 4 (které je zároveň i zbytkem po dělení čísla 14 číslem 10)

$$4x \equiv 8\ (mod\ 10).$$

Obě strany kongruence vydělíme číslem 4 (číslo 10 není dělitelné číslem 4 beze zbytku, ale číslo 4 lze rozložit na $2 \cdot 2$ – musíme dělit modul číslem 2)

$$x \equiv 2\ (mod\ 5).$$

Našli jsme řešení $x_1 = 2$. Další řešení najdeme velmi lehce – stačí k pravé straně přičíst hodnotu modulu, který se nachází u prvního řešení. Druhé řešení bude $x_2 = 7$.

Řešením v $\mathbb{Z}$ jsou veškerá x, pro něž platí

$$x = 2 + 5t, t \in \mathbb{Z}.$$

Příklad 2.7. Řešte kongruenci $21x \equiv 6\ (mod\ 9)$.

Řešení:

Ověříme, zda je kongruence řešitelná

$$D(21,9) = 3 \wedge 3|6.$$

Kongruence má tři řešení v (FÚSZ) i v každé libovolně zvolené (ÚSZ).

Opět budeme kongruenci upravovat pro nalezení řešení.

Levou stranu kongruence nahradíme číslem, které je s číslem 21 kongruentní podle modulu 9 a patří do (FÚSZ) – nahradíme číslem 3 (které je zároveň i zbytkem po dělení čísla 21 číslem 9)

$$3x \equiv 6\ (mod\ 9).$$

Nyní obě strany kongruence vydělíme číslem 3. Pozor – toto číslo dělí i modul, proto jej také budeme dělit

$$x \equiv 2\ (mod\ 3).$$

Našli jsme první řešení $x_1 = 2$.

Podle podmínky řešitelnosti ale víme, že řešení mají být tři. Další řešení najdeme velmi lehce – stačí k pravé straně přičíst hodnotu modulu, který se nachází u prvního řešení (číslo 3)

$$x_2 = 5, x_3 = 8.$$

Řešením v $\mathbb{Z}$ jsou veškerá x, pro která platí

$$x = 2 + 3t, t \in \mathbb{Z}.$$

3 LINEÁRNÍ DIOFANTICKÉ ROVNICE

V této kapitole se budeme zabývat způsoby řešení lineárních diofantických rovnic o dvou; třech a více neznámých.

3.1 ŘEŠENÍ LINEÁRNÍ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH

DEFINICE 3.1 (LINEÁRNÍ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH)

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

$$ax + by = \mathrm{c}, \tag{3.1}$$

kde neznámé $x, y \in \mathbb{Z}$ a koeficienty $a, b, c \in \mathbb{Z}, a \neq 0 \ \wedge \ b \neq 0$.

Tyto rovnice lze řešit mnoha metodami. Pomocí experimentálních výpočtů neboli „metodou pokus – omyl“ nebo grafickým řešením; případně s využitím Eukleidova algoritmu nebo za pomoci kongruence. Dalšími metodami jsou vyjádření členu s nejmenším koeficientem, redukční metoda a metoda podle Nivena a spol. Každá metoda má své silné a slabé stránky, které si řekneme u jednotlivých metod dále. Dříve, než se budeme zabývat jednotlivými metodami, řekneme, kdy je daná diofantická rovnice řešitelná.

Rovnice (3.1) je v oboru celých čísel řešitelná právě tehdy, když je splněna nutná (a postačující) podmínka, o které hovoří následující Věta 3.1. Tu budeme používat jako první krok řešení, pakliže nám bude ihned zřejmý společný dělitel – pokud ne, použijeme ji následně po Eukleidovu algoritmu.

VĚTA 3. 1 (NUTNÁ PODMÍNKA ŘEŠITELNOSTI)

Nutná a zároveň postačující podmínka řešitelnosti rovnice $ax + by = c$ je, aby největší společný dělitel D koeficientů a, b dělil i celé číslo c

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

Jestliže je tato podmínka splněna, existuje alespoň jedna dvojice řešení x_0, y_0, kterou nalezneme pomocí metod vyjmenovaných výše.

Jsou-li a, b nesoudělná přirozená čísla, potom existují celá čísla x, y taková, že platí

$$ax + by = 1$$

Nyní jsme schopni odvodit obecné řešení lineární diofantické rovnice o dvou neznámých dle [4].

Jestliže máme splněnu nutnou podmínku řešitelnosti, existuje alespoň základní řešení x_0, y_0. Rovnici (3.1) na straně 23 dostaneme po dosazení základních řešení ve tvaru

$$ax_0 + by_0 = c. \tag{3.2}$$

Začneme dělením rovnice (3.2) největším společným dělitelem D

$$\left(\frac{a}{D}\right)x_0 + \left(\frac{b}{D}\right)y_0 = \frac{c}{D}. \tag{3.3}$$

Předpokládejme, že existuje nějaké další řešení x^*, y^*

$$\left(\frac{a}{D}\right)x^* + \left(\frac{b}{D}\right)y^* = \frac{c}{D}. \tag{3.4}$$

Nyní od sebe odečteme rovnosti (3.4) a (3.3), dostaneme výraz ve tvaru

$$\left(\frac{a}{D}\right)(x^* - x_0) + \left(\frac{b}{D}\right)(y^* - y_0) = 0.$$

Osamostatníme neznámé x a y převedením jedné neznámé na druhou stranu rovnosti

$$\left(\frac{a}{D}\right)(x^* - x_0) = \left(\frac{b}{D}\right)(y_0 - y^*). \tag{3.5}$$

Z rovnosti (3.5) plyne, že $(y_0 - y^*)$ je dělitelné $\left(\frac{a}{D}\right)$, jelikož víme, že čísla $\left(\frac{a}{D}\right), \left(\frac{b}{D}\right)$ jsou nesoudělná. Proto musí existovat číslo $t \in \mathbb{Z}$, pro které platí

$$y_0 - y^* = \left(\frac{a}{D}\right)t.$$

Vyjádříme y^*

$$y^* = y_0 - \left(\frac{a}{D}\right)t. \tag{3.6}$$

Nyní potřebujeme dostat rovnici pro x^*. Rovnici (3.6) dosadíme do (3.5)

$$\left(\frac{a}{D}\right)(x^* - x_0) = \left(\frac{b}{D}\right)\left[y_0 - \left(y_0 - \left(\frac{a}{D}\right)t\right)\right].$$

Upravíme závorku

$$\left(\frac{a}{D}\right)(x^* - x_0) = \left(\frac{b}{D}\right)\left(\frac{a}{D}\right)t.$$

Vydělíme $\left(\frac{a}{D}\right)$

$$x^* - x_0 = \left(\frac{b}{D}\right) t.$$

Vyjádříme x^*

$$x^* = x_0 + \left(\frac{b}{D}\right) t. \tag{3.7}$$

Rovnice (3.6) na straně 24 spolu s rovnicí (3.7) nám vyjadřují všechna možná řešení rovnice (3.1) na straně 23 pomocí parametrických rovností, kde parametr $t \in \mathbb{Z}$

$$x^* = x_0 + \left(\frac{b}{D}\right) t, \tag{3.7}$$

$$y^* = y_0 - \left(\frac{a}{D}\right) t. \tag{3.6}$$

Nyní, když známe vše potřebné, ukážeme jak řešit diofantické rovnice o dvou neznámých pomocí vybraných metod. Začneme „metodou pokus – omyl“, následně budeme rovnice řešit pomocí grafické metody. Poté budeme řešení počítat za pomoci Eukleidova algoritmu, kongruence a metody vyjádření členu s nejmenším koeficientem.

3.1.1 „METODA POKUS – OMYL“

Ačkoli je tento způsob zjišťování výsledku neoficiální, jedná se o nejpoužívanější „metodu“ řešení diofantických rovnic. Přesněji řečeno jedná se spíše o experiment nežli o metodu[12]. Vystačíme si pouze se základními znalostmi matematiky a selským rozumem. Proto mnoho lidí zvládne tyto rovnice vyřešit, i přesto, že o diofantických rovnicích nemají sebemenší ponětí. U této „metody“ nebudeme využívat podmínku, kdy je rovnice řešitelná, jelikož tento způsob řešení využívají většinou jen lidé, kteří nevědí, že řeší diofantické rovnice – budeme se snažit přiblížit se jejich myšlence řešení. Velmi často nám při použití této „metody“ může uniknout mnoho řešení – proto je tento způsob řešení nepříliš efektivní, zároveň je tato „metoda“ vcelku pomalá a pracná.

[12] Metody jsou univerzální, kdežto zde výsledná řešení pouze hádáme nebo se je snažíme odvodit.

Příklad 3.1. Najděte řešení rovnice $4x + 2y = 47$.

Řešení:

Jako první nás napadne řešit úlohu pouze s x nebo y. Zkusíme tedy jako první vynechat proměnnou y, resp. uvažovat, že $y = 0$. V rovnici tak zůstane $4x = 47$, nyní osamostatníme proměnnou $x \rightarrow x = \frac{47}{4}$. Bohužel se nám nepovedlo dělit číslo 47 číslem 4 beze zbytku – toto řešení tak nepřipadá v úvahu. Zkusíme nyní uvažovat, že $x = 0$. Rovnice bude ve tvaru $2y = 47$. Nyní osamostatníme neznámou $y \rightarrow y = \frac{47}{2}$. Opět se nepovedlo dělit beze zbytku – opět jsme tak nenašli možné řešení. Zjistili jsme, že nelze řešit rovnici pouze za pomoci jedné neznámé – je potřeba zkusit uvažovat nad možnými kombinacemi. Budeme se snažit vymyslet takové kombinace, abychom se s nimi co nejvíce přiblížili číslu 47 – pak je šance, najít co nejrychleji možné řešení. Zkusme uvažovat, že $x = 11, y = 2$, jestliže tato čísla dosadíme do rovnice za neznámé x, y vyjde nám číslo 48. Uvažujme tedy nad jinou kombinací. Např. $x = 12, y = -1 \rightarrow$ nyní dostaneme číslo 46. Takto můžeme zkoušet velké množství kombinací. Můžeme si všimnout, že se vždy pohybujeme v těsné blízkosti čísla 47. Pokud bychom vyzkoušeli pár dalších možností, zjistili bychom (případně jsme již zjistili), že vždy vyjde sudý výsledek. U proměnné x je sudé číslo 4, u proměnné y je také sudé číslo a to číslo 2. Víme, že součet dvou sudých čísel je vždy sudý. Je tedy nemožné, abychom získali liché číslo 47. Můžeme prohlásit, že zadaná úloha nemá řešení.

Příklad 3.2. Najděte řešení rovnice $6x + 9y = 204$.

Řešení:

Opět využijeme stejný postup jako výše. Jako první zkusíme vynechat proměnnou y, resp. uvažovat, že $y = 0$. V rovnici nám tak zůstane $6x = 204$. Zkusíme vydělit číslo 204 číslem 6 $\rightarrow \mathrm{x} = \frac{204}{6} = 34$. Povedlo se nám dělit beze zbytku, našli jsme tedy jednu dvojici řešení $[34; 0]$. Nyní využijeme stejný postup, avšak budeme uvažovat $x = 0$. Rovnice bude ve tvaru $9y = 204$. Opět zkusíme vydělit číslo 204 číslem 9, $y \rightarrow \frac{204}{9} = 22{,}67$. Nepodařilo se nám dělit beze zbytku, neexistuje řešení, kdy $x = 0$. Nyní zkusíme uvažovat, zda je možné vytvořit jiné kombinace x, y tak, abychom dostali při součtu této kombinace číslo 204. Stejně jako v předchozím příkladu, se budeme snažit odhadnout kombinace tak, aby se co nejvíce přibližovaly číslu 204. Kombinace x a y zkusíme najít pomocí tabulky.

Zvolíme libovolné hodnoty pro x (např. od 1 do 7), následně dosadíme za x a dopočítáme zbytek pro hodnotu $9y$, ze které spočteme celočíselné výsledky pro samotné y (pokud existují).

x	$6x + 9y = 204$	$9y = 204 - 6x$	y
1	$6 + 9y = 204$	$9y = 198$	22
2	$12 + 9y = 204$	$9y = 192$	–
3	$18 + 9y = 204$	$9y = 186$	–
4	$24 + 9y = 204$	$9y = 180$	20
5	$30 + 9y = 204$	$9y = 174$	–
6	$36 + 9y = 204$	$9y = 168$	–
7	$42 + 9y = 204$	$9y = 162$	18

Tabulka 4: Některá řešení rovnice $6x + 9y = 204$

V Tabulce 4 jsme našli další tři řešení. Mnoho řešitelů by zde skončilo a spokojilo by se s výsledky, které našli. To je neduh této metody – veškerá řešení nám nejsou ihned známá, resp. netušíme, jak přesně se k nim dostat. Naopak mnozí řešitelé si všimnou, že hodnoty u proměnné x se zvětšují podle nějakého pravidla. Totéž se děje i u proměnné y, zde se ale hodnoty zmenšují.

Vidíme, že pro $x = \{1; 4; 7; \dots\}$ existuje y. Následující hodnota x je vždy o tři větší než předchozí. S velkou pravděpodobností bude posloupnost hodnot x pokračovat dále stejným způsobem. Zkusíme se přesvědčit např. pro $x = 22$.

22	$132 + 9y = 204$	$9y = 72$	8

Tabulka 5: Zkouška řešení pro $x = 22$

Přesvědčili jsme se, že jsme přišli na způsob, jakým se posloupnost hodnot tvoří.

Nyní si vyjádříme všechna řešení pomocí parametrických rovnic. Parametrickou rovnici pro neznámou x jsme si již odvodili v odstavci výše (ovšem i bez odvození těchto rovnic, by šikovnému řešiteli bylo jasné, jak na všechna řešení přijít)

$$x = 1 + 3\mathrm{t}, \mathrm{t} \in \mathbb{Z}.$$

Parametrickou rovnici pro neznámou y si odvodíme stejně jako pro x. Dle Tabulky 4 na straně 27 se hodnota y vždy o dva snižuje, rovnici tak můžeme zapsat ve tvaru

$$y = 22 - 2t, t \in \mathbb{Z}.$$

Pakliže by někdo měl problém s odvozením parametrických rovnic, lze je určit pomocí Věty 3.1 na straně 23 – přesněji podle vzorců (3.6) a (3.7) na straně 25

$$\mathrm{D}(6,9) = 3,$$

$$x^* = 1 + \left(\frac{9}{3}\right)t = 1 + 3t, \tag{3.8}$$

$$y^* = 22 - \left(\frac{6}{3}\right)t = 22 - 2t. \tag{3.9}$$

Došli jsme ke stejnému výsledku – je tedy pouze na nás, kterou metodu zvolíme – metoda dosazení do vzorce (3.6) a (3.7) na straně 25 je samozřejmě rychlejší. Odvozování ovšem může vyhovovat více těm, kteří si nezapamatují vzorce.

Závěr

S touto „metodou“ se učí pracovat již děti na prvním stupni, ačkoliv neví, že řeší diofantické rovnice. Většinou právě děti prvního stupně základní školy jsou řešitelé, kteří se spokojí pouze s jedním řešením, jelikož nemají prostředky, kterými by mohly odvodit další řešení. To se učí až žáci druhého stupně, kteří již umí pracovat s lineárními rovnicemi. Tato metoda se hodí pro malé hodnoty u neznámých x a y, jinak je velmi dlouhá a pracná. Zároveň nám mnohdy mohou nepozorností uniknout mnohá řešení.

3.1.2 GRAFICKÁ „METODA“

Grafickou „metodu“ lze přirovnat k „metodě pokus – omyl“, ale také se nedá považovat za univerzální. Zde ovšem nečteme řešení z tabulky, nýbrž z grafu. Každý žák druhého stupně základní školy ví, že grafem lineární funkce je přímka. Lineární diofantické rovnice lze také vykreslit jako přímku – proto je tato metoda opět vhodná pro běžné lidi, kteří nejsou zasvěceni do problémů diofantických rovnic. Přímku totiž umí vykreslit (snad) každý z nás. Pro sestrojení přímky nám postačí dva body. Tyto body musíme najít, následně stačí vyčíst řešení z grafu. Graf má jednu velkou nevýhodu – nikdy nám neukáže všechna řešení. Musíme doufat v to, že z určitého počtu řešení vyplívajících z grafu, odvodíme všechna řešení.

Nyní plyne otázka. Jak nalezneme řešení diofantické rovnice v grafu? Víme, že hledáme vždy pouze celočíselná řešení, a proto nás budou zajímat místa, kde přímka prochází pouze body s celočíselnými souřadnicemi. Abychom nemuseli složitě hledat, kde se přímka protne s celými čísly na ose x i na ose y, vložíme do grafu mřížkovanou síť, která nám pomůže řešení rychle najít.

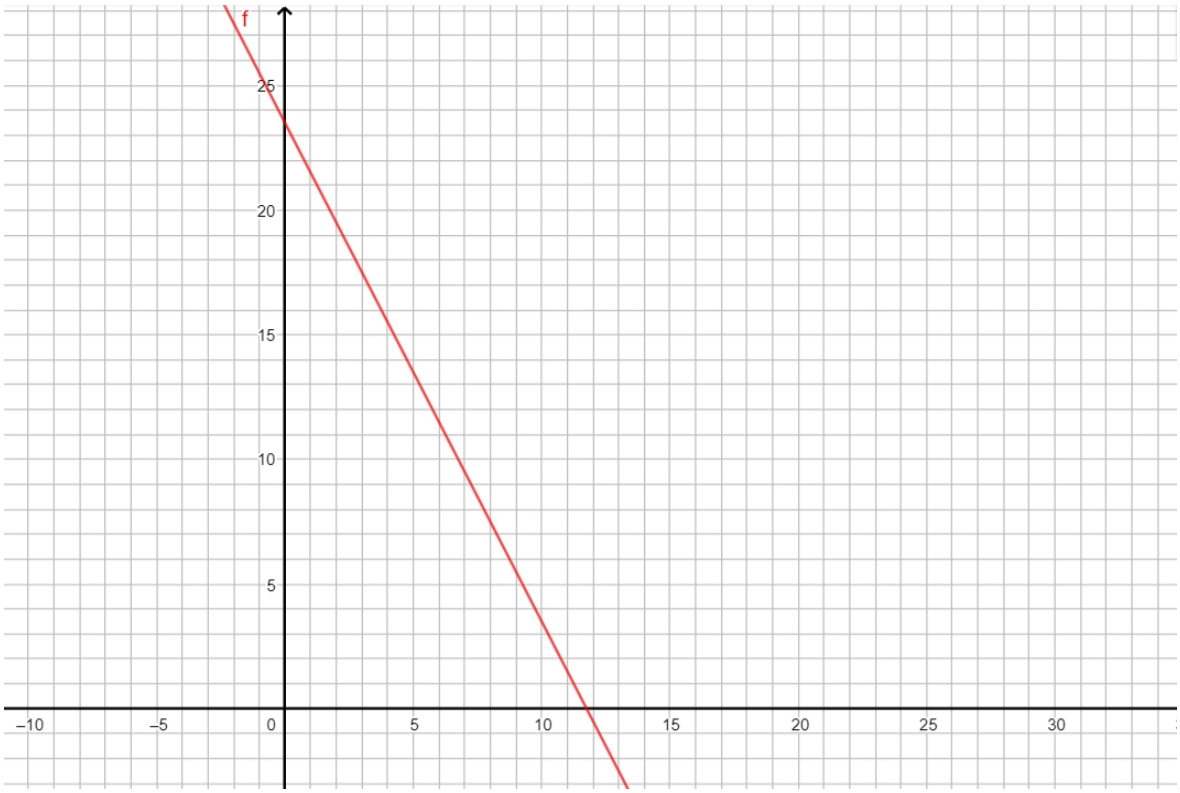
> *Pozn.* Žijeme v moderní době, kdy nám počítače pomáhají s mnohými věcmi. Graf vykreslíme pomocí libovolného matematického softwaru – WolframAlpha, Geogebra, atd. Výhodou těchto programů je snadné uživatelské rozhraní a naprostá přesnost. V celé bakalářské práci budeme grafy vykreslovat pomocí programu Geogebra.

U této metody také nebudeme používat jako první krok podmínku řešitelnosti – ukážeme si totiž, jak z grafu zjistíme, že zadaná rovnice má nebo nemá řešení.

Příklad 3.3. Najděte řešení rovnice ve tvaru $4x + 2y = 47$.

Řešení:

Rovnici zakreslíme do grafu pomocí programu Geogebra.



Graf 1: přímka $4x + 2y = 47$ v mřížkované síti

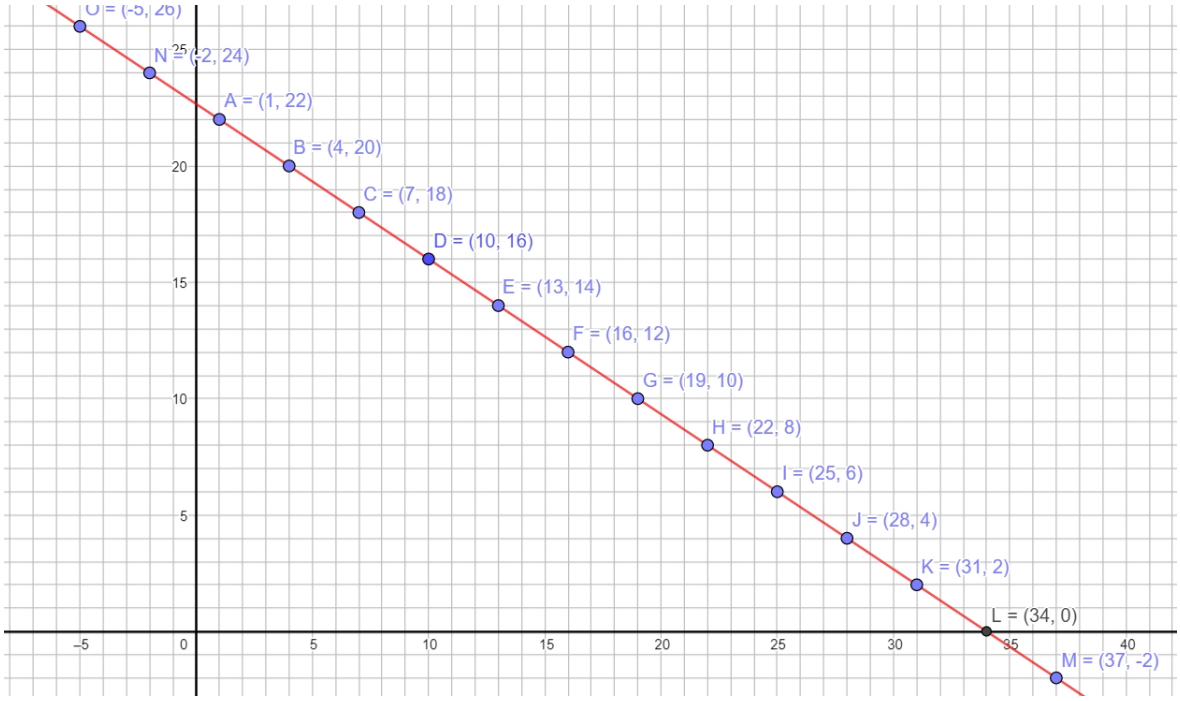
V Grafu 1 můžeme vidět řešení. Řešením, jak jsme řekli, jsou body, v nichž přímka prochází mřížkovými body. Bohužel v této části grafu nevidíme žádný takový bod – vypadá to, že řešení neexistuje. Ovšem pozor – nemusí to tak vždy nutně být. Je možné, že řešení bude existovat a bude pouze mimo naší zobrazenou část.

Jelikož jsme již tento příklad řešili v kapitole 3.1.1 na str. 25 víme, že opravdu řešení nemá. Kdybychom si nebyli jisti, je potřeba zvolit jinou metodu a přesvědčit se o správnosti našeho tvrzení.

Příklad 3.4. Najděte řešení rovnice ve tvaru $6x + 9y = 204$.

Řešení:

Rovnici zakreslíme do grafu pomocí programu Geogebra.



Graf 2: přímka $6x + 9y = 204$ v mřížkované síti

V Grafu 2 vidíme řešení. Našli jsme nyní několik mřížkových bodů. Např.: $\mathrm{A} = [1{,}22]; \mathrm{B} = [4{,}20]; \mathrm{C} = [7{,}18]$ atd. Jak jsme již řekli, graf nám nikdy nezobrazí všechna řešení. Šikovní řešitelé si mohou všimnout určité periody mezi řešením, které jsme našli. Hodnoty souřadnice x rostou vždy o tři body oproti předchozí, naopak hodnoty souřadnice y se vždy o dva body snižují. Opět můžeme určit všechna řešení rovnice pomocí parametrických rovnic stejně jako v předchozí kapitole 3.1.1

$$x = 1 + 3t, t \in \mathbb{Z}, \tag{3.8}$$

$$y = 22 - 2t, t \in \mathbb{Z}. \tag{3.9}$$

Závěr

Tento způsob řešení je podobný „metodě pokus – omyl“ – je velmi pracný. Zároveň nám často mohou nepozorností uniknout mnohá řešení, případně se nám nemusí podařit řešení nalézt i přesto, že řešení existovat mohou.

3.1.3 METODA S VYUŽITÍM EUKLEIDOVA ALGORITMU

V kapitole 2 na straně 12 jsme pojem Eukleidův algoritmus zavedli. Zároveň jsme se jej naučili i počítat s využitím Bezoutovy rovnosti (Příklad 2.1, Příklad 2.2 na straně 13). Nyní se nám tyto nabyté vědomosti budou hodit. Řešení diofantických rovnic budeme opět hledat nejdříve přes Eukleidův algoritmus a následně použijeme Bezoutovu rovnost. Tento způsob řešení je první, který se dá nazývat metodou.

Tato metoda má oproti předcházejícím dvěma řešením jednu velkou výhodu. Řešení nemusíme hádat, přijdeme na něj výpočtem, který je vcelku rychlý a univerzální.

Příklad 3.5. Najděte řešení rovnice ve tvaru $4x + 2y = 47$.

Řešení:

Prvním krokem vždy bude použití nutné podmínky řešitelnosti podle Věty 3.1 na straně 23.

$$D(4,2) = 2 \wedge 2 \nmid 47$$

Tato rovnice není řešitelná, jelikož neplatí nutná podmínka řešitelnosti.

Příklad 3.6. Najděte řešení rovnice ve tvaru $6x + 9y = 204$.

Řešení:

Opět se nejdříve přesvědčíme o řešitelnosti podle Věty 3.1 na straně 23

$$D(6,9) = 3 \wedge 3 | 204.$$

Rovnice je řešitelná.

Můžeme přistoupit k řešení za pomoci Eukleidova algoritmu a Bezoutovy rovnosti

$$6 < 9,$$

$$9 = 6 * 1 + \boxed{\mathbf{3}} (3 < 6), \qquad 3 \neq 0$$

$$6 = 3 * 2 + \mathbf{0}\ (0 < 3), \qquad \mathbf{0} = \mathbf{0}$$

$$konec\ algoritmu.$$

Nyní vycházíme z největšího společného dělitele, zde je jím číslo 3, a vyjádříme jej pomocí Věty 2.3 na straně 12 jako celočíselnou kombinaci čísel 9 a 6. Postupujeme odspoda nahoru

$$3 = 9 \cdot 1 - 6 \cdot 1.$$

Upravíme do základního tvaru dle (1.1) na straně 8

$$6 \cdot (-1) + 9 \cdot 1 = 3. \tag{3.10}$$

Našli jsme základní řešení $x_0 = -1, y_0 = 1$ pro rovnici $6x + 9y = 3$.

Měli jsme ale zadanou rovnici $6x + 9y = 204$, musíme proto rovnici (3.10) vynásobit číslem 68, abychom dostali po vynásobení s číslem 3 číslo 204

$$6 \cdot (-68) + 9 \cdot 68 = 204.$$

Našli jsme základní řešení $x_0^* = -68, y_0^* = 68$ zadané rovnice.

Všechna řešení lze nalézt pomocí základních řešení a parametrických rovnic (3.6) a (3.7) na straně 25

$$x^* = -68 + \frac{9}{3}t, t \in \mathbb{Z},$$

$$y^* = 68 - \frac{6}{3}t, t \in \mathbb{Z}.$$

Zjednodušíme

$$x^* = -68 + 3t, t \in \mathbb{Z}, \tag{3.11}$$

$$y^* = 68 - 2t, t \in \mathbb{Z}. \tag{3.12}$$

Porovnání výsledného řešení Příkladu 3.2, 3.4 a 3.6

Příklad 3.2, 3.4 a 3.6 jsme řešili pomocí tří různých metod. Můžeme si všimnout, že výsledné řešení (3.8), (3.9) na straně 28 „metodou pokus – omyl“ i „metodou“ grafickou na straně 31 vyšlo jinak než výsledné řešení (3.11), (3.12) u metody s využitím Eukleidova algoritmu. Ačkoliv se jedná o dva různé zápisy parametrické rovnice, jedná se o stále stejné řešení. Přesvědčit se o tom můžeme například dosazením několika vybraných hodnot.

Závěr

Tato metoda je univerzální pro lineární diofantické rovnice o dvou neznámých. Jestliže je rovnice řešitelná, pak pomocí této metody lze vždy najít základní řešení, které je následně

možné dosadit do vzorce (3.6) a (3.7) na straně 25 pro zjištění parametrických rovnic, které udávají všechna řešení.

3.1.4 METODA S VYUŽITÍM KONGRUENCE

Tato metoda je spolu s Eukleidovým algoritmem nejpoužívanější. Co to jsou kongruence a jak se počítají, jsme si řekli v kapitole 2.2 na straně 14. Také jsme řekli, co jsou to lineární kongruence v kapitole 2.3 na straně 18. Nyní musíme uvést, jak lze přepsat diofantickou rovnici na kongruence.

Každá lineární diofantická rovnice jde přepsat na kongruenci o jedné neznámé. Můžeme si vybrat, podle kterého modulu budeme chtít počítat (modul volíme podle koeficientu u neznámé x nebo y). Výsledek bude stejný, ať už budeme počítat podle libovolně zvoleného modulu – záleží tedy pouze na nás, co nám vyhovuje více. Často se doporučuje počítat podle menšího modulu.

Jestliže máme diofantickou rovnici

$$ax + by = c,$$

můžeme ji upravit na lineární kongruenci o jedné neznámé

$$ax + by \equiv c \ (mod\ a). \tag{3.13}$$

Budeme počítat neznámou y podle neznámé x. Víme, že $ax \equiv 0 \ (mod\ a)$, proto lze rovnici (3.13) upravit na tvar

$$by \equiv c \ (mod\ a).$$

Pokud bychom se rozhodli počítat neznámou x podle neznámé y, vypadalo by to obdobně – jelikož $by \equiv 0 \ (mod\ b)$, rovnici (3.13) bychom upravili na tvar

$$ax \equiv c \ (mod\ b).$$

Opět použijeme vzorový příklad.

Příklad 3.7. Najděte řešení rovnice $6x + 9y = 204$

Řešení:

Opět se nejdříve přesvědčíme o řešitelnosti podle Věty 2.5 na straně 18 a Věty 3.1 na straně 23.

$$D(6,9) = 3 \wedge 3|204$$

Zjistili jsme, že rovnice je řešitelná. Zároveň víme, že kongruence bude mít 3 řešení v (FÚSZ) i v každé libovolně zvolené (ÚSZ).

Nyní si diofantickou rovnici převedeme na kongruenci. Budeme počítat podle menšího modulu – počítáme neznámou y pomocí neznámé x.

$$6x + 9y \equiv 204\ (mod\ 6) \qquad (3.14)$$

Víme, že $6x \equiv 0\ (mod\ 6)$, kongruenci (3.14) lze upravit na tvar

$$9y \equiv 204\ (mod\ 6).$$

Kongruenci budeme upravovat podle pravidel, která jsme zmínili v kapitole 2.2.1 na straně 16. Pravou stranu kongruence můžeme dělit číslem 6 a dostaneme zbytek 0, který patří do (FÚSZ). Levou stranu budeme dělit také číslem 6 a zde dostaneme zbytek 3, který patří do (FÚSZ)

$$3y \equiv 0\ (mod\ 6).$$

Obě strany kongruence vydělíme číslem 3 – pozor! Číslo 6 je dělitelné číslem 3, a proto dělíme i modul

$$y \equiv 0\ (mod\ 2).$$

Našli jsme první řešení $y_0 = 0$. Dle podmínky řešitelnosti víme, že mají být tři řešení ve (FÚSZ) podle původního modulu 6. Dalšími řešeními jsou $\mathrm{y}_1 = 2, \mathrm{y}_2 = 4$

Řešením v $\mathbb{Z}$ jsou veškerá y, pro která platí

$$y = 0 + 2t, t \in \mathbb{Z}. \qquad (3.15)$$

Nyní dosadíme parametrickou rovnici (3.15) zpět do zadání a následně dopočítáme řešení pro x

$$6x + 9 \cdot (0 + 2t) = 204.$$

$$6x + 18t = 204$$

$$6x = 204 - 18t$$

$$x = \frac{204}{6} - \frac{18}{6}t = 34 - 3t, t \in \mathbb{Z}$$

Řešením zadané rovnice $6x + 9y = 204$ v $\mathbb{Z}$ jsou x a y, pro která platí

$$x = 34 - 3t, t \in \mathbb{Z},$$

$$y = 2t, t \in \mathbb{Z}.$$

Závěr:

Tento způsob řešení bohužel nelze úplně považovat za metodu, jelikož je nekonečně mnoho možností úprav dané kongruence[13]. Pomocí kongruencí lze najít vždy řešení (pokud existuje). Úpravy nejprve pouze zkoušíme a hledáme správné možnosti čísel, až následně zjistíme, zda byla úprava správná nebo ne.

3.1.5 METODA VYJÁDŘENÍ ČLENU S NEJMENŠÍM KOEFICIENTEM

Tato metoda je jedna z nejuniverzálnějších, funguje ale pouze pro hodnoty u neznámých větších než 1. Pomocí této metody se snažíme původní diofantickou rovnici upravovat za předpokladu, že diofantická rovnice má řešení pouze v oboru celých číslech. Jelikož je tato metoda složitější na pochopení, ukážeme postup na cvičném příkladu.

Příklad 3.7. Najděte řešení rovnice $6x + 9y = 213$. (3.16)

Řešení:

U této metody je potřeba nejdříve vyjádřit neznámou s nejnižším koeficientem (zde je to neznámá x). Dostaneme tak zlomek

$$x = \frac{213 - 9y}{6}. \quad (3.17)$$

[13] Pokud bychom zvolili řešení prostřednictvím Eulerovy metody nebo metody rozkladu modulu, které jsme zmínili v kapitole 2.3 na straně 18, pak by kongruence byly algoritmizované.

Nyní budeme upravovat koeficient u neznámé y. Protože $9y = 6y + 3y$ můžeme zlomek (3.17) rozdělit na celou část a „zbylou“ část – ta nás následně bude zajímat.

$$x = -\frac{6y}{6} + \frac{213 - 3y}{6} = -y + \frac{213 - 3y}{6}$$

Dle Definice diofantické rovnice 1.1 víme, že přípustná řešení jsou pouze v oboru celých čísel, a proto čísla x a y musí být čísla celá. Z toho plyne, že zlomek $\frac{213-3y}{6}$ musí být také celé číslo.

Tento zlomek označíme např. jako t

$$t = \frac{213 - 3y}{6}.$$

$$x = -y + t \tag{3.18}$$

Nyní se budeme zabývat pouze rovnicí, kterou tvoří zlomek t a vyjádříme neznámou y.

$$y = \frac{-6t + 213}{3}$$

Opět budeme dělit zlomek na celou a „zbylou“ část, a protože $6t = 3 \cdot 2t$ zlomek bude vypadat takto

$$y = -2t + \frac{213}{3} = -2t + 71.$$

Získali jsme pro rovnici pouze celá čísla. Můžeme začít zpětně dosazovat a vyjadřovat neznámé. Neznámou x vyjádříme z rovnice (3.18), na neznámou y jsme přišli přímo

$$x = -y + t = -(-2t + 71) + t = 3t - 71,$$

$$y = -2t + 71.$$

Obecné řešení v $\mathbb{Z}$ je

$$x = 3t - 71, t \in \mathbb{Z},$$

$$y = -2t + 71, t \in \mathbb{Z}.$$

Závěr

Metoda vyjádření členu s nejmenším koeficientem je stejně jako Eukleidův algoritmus založena na dělení celých čísel a na dělení se zbytkem a následných úpravách. Tato metoda je univerzální a své využití najde převážně v další kapitole 3.2 na straně 38.

3.2 ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC O TŘECH A VÍCE NEZNÁMÝCH

Nyní, když umíme řešit diofantické rovnice o dvou neznámých, naučíme se řešit rovnice o třech a více neznámých. Při řešení těchto diofantických rovnic se můžeme řídit poznatky, které jsme získali z kapitoly 3.1 od strany 23. Bohužel ne všechny metody, které jsme uvedli v kapitole 3.1, lze efektivně použít i pro rovnice o třech a více neznámých.

Efektivními metodami budou stejně jako u rovnic se dvěma neznámými kongruence a metoda vyjádření členu s nejmenším koeficientem. Samozřejmě lze využít i experimentální „metody“, ale řešit pouhým dosazováním bude ještě náročnější než jen pro dvě neznámé. Eukleidův algoritmus, ačkoliv jsme ho označili metodou, nelze použít pro lineární diofantické rovnice o třech a více neznámých. Můžeme totiž narazit na problém, kdy nejsme schopni zjistit, zda jsme našli obecné řešení rovnice, která udává všechna výsledná řešení. V publikaci [11] je uvedena metoda pro rovnice o n neznámých, která využívá Eukleidova algoritmu, největšího společného dělitele $(n-1)$ neznámých a substituce. Více o této metodě najdeme v kapitole 3.2.4 na str. 44.

> *Pozn.* V následujících příkladech budeme mít z důvodu jednoduššího pochopení pouze diofantické rovnice o třech neznámých. Na diofantické rovnice o více než třech neznámých můžeme aplikovat stejné metody a postupy jako na rovnice o třech neznámých. Následující podkapitoly budou stručnější, jelikož využíváme dřívější poznatky.

Obecnou definici (1.1) jsme již uvedli na straně 8, a proto uvedeme, jak vypadá diofantická rovnice o třech neznámých.

DEFINICE 3.2 (LINEÁRNÍ DIOFANTICKÉ ROVNICE O TŘECH NEZNÁMÝCH)

Lineární diofantickou rovnicí o třech neznámých x, y, z rozumíme rovnici ve tvaru

$$ax + by + cz = \mathrm{d},$$

kde neznámé $x, y, z \in \mathbb{Z}$ a koeficienty $a, b, c, d \in \mathbb{Z}, a \neq 0 \wedge b \neq 0 \wedge c \neq 0$.

Opět můžeme zjistit, kdy je diofantická rovnice řešitelná pomocí Věty 3.2.

VĚTA 3. 2 (NUTNÁ PODMÍNKA ŘEŠITELNOSTI)

Nutná a zároveň postačující podmínka řešitelnosti rovnice $ax + by + cz = d$ je, aby největší společný dělitel D koeficientů a, b, c dělil i celé číslo d

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

Jestliže je tato podmínka splněna, existuje alespoň jedna trojice řešení x_0, y_0, z_0, kterou nalezneme pomocí metod.

3.2.1 „METODA POKUS – OMYL“

Stejně jako v kapitole 3.1.1 na straně 25 zkusíme diofantické rovnice vyřešit pomocí experimentu. Čím více neznámých máme, tím těžší je pro nás přijít experimentem na řešení. Tento způsob řešení je velmi pracný a zabere nám mnoho času, ale vždy se k výsledku dostaneme (pokud existuje) a jsme dostatečně trpěliví.

Příklad 3.8. Najděte řešení rovnice $8x + 9y - 11z = 16.$ (3.19)

Řešení:

Jelikož máme tři neznámé o jedné rovnici, budeme za jakékoli dvě neznámé volit libovolná čísla a poslední neznámou zkusíme dopočítat[14].

[14] U n neznámých budeme volit libovolně $n - 1$ neznámých.

Např. zvolíme $x = 0$ a dosadíme do rovnice (3.19).

$$8 \cdot 0 + 9y - 11z = 16$$

$$9y - 11z = 16 \qquad (3.20)$$

Opět zvolíme libovolné číslo za další neznámou, např. $y = 1$ a dosadíme do (3.20).

$$9 \cdot 1 - 11z = 16$$

$$-11z = 7$$

$$z = -\frac{7}{11}, z \notin \mathbb{Z} \rightarrow \text{není řešením}$$

Takto můžeme zkoušet velké množství různých čísel, jelikož jsme se na poprvé netrefili a nemuseli bychom se trefit ani na dalších několik pokusů. Proto zkusíme příklad dořešit pomocí tabulky. V prvním sloupci budeme volit neznámou x, v druhém sloupci budeme upravovat rovnici po dosazení hodnoty za x, ve třetím sloupci budeme volit neznámou y (budeme se snažit dopředu vymýšlet, jakou hodnotu budeme potřebovat, aby nám ve čtvrtém sloupci vyšlo číslo, které je násobkem 11). Ve čtvrtém sloupci budeme upravovat rovnici po dosazení hodnoty za y a v pátém sloupci získáme po úpravě možnou celočíselnou hodnotu neznámé z.

$\boldsymbol{x}$	$\boldsymbol{8x + 9y - 11z = 16}$	$\boldsymbol{y}$	$\boldsymbol{8x + 9y - 11z = 16}$	$\boldsymbol{z}$
1	$9y - 11z = 16 - 8$	7	$-11z = 16 - 8 - 63$	5
2	$9y - 11z = 16 - 16$	0	$-11z = 16 - 16 - 9 \cdot 0$	0
3	$9y - 11z = 16 - 24$	-7	$-11z = 16 - 24 - 9 \cdot (-7)$	-5
4	$9y - 11z = 16 - 32$	-14	$-11z = 16 - 32 - 9 \cdot (-14)$	-10

Tabulka 6: Některá řešení rovnice $8x + 9y - 11z = 16$

Našli jsme několik řešení rovnice (3.19) v Tabulce 6, které tvoří uspořádané trojice $[1,7,5]; [2,0,0]; [3,-7,-5]; [4,-14,-10]$. Zkusíme odvodit parametrické rovnice pro nalezení všech řešení. Z těchto čtyř řešení vidíme, že nám hodnota x roste vždy o hodnotu jedna, parametrická rovnice tak bude např.

$$x = 1 + t.$$

Hodnota u neznámé y se nám vždy snižuje o sedm, parametrická rovnice bude

$$y = 7 - 7t.$$

Hodnota u neznámé z nám vždy klesá o pět, parametrická rovnice bude

$$z = 5 - 5t.$$

Obecným řešením původní rovnice (3.19) na straně 39 je

$$x = 1 + t,$$

$$y = 7 - 7t,$$

$$z = 5 - 5t, t \in \mathbb{Z}.$$

Závěr

Pro neznalce efektivnějších metod, je experimentování opět jedinou možností, jak najít řešení. Stejně jako u rovnic se dvěma neznámými je tato „metoda“ neefektivní – je pracná a můžeme nějaké řešení vynechat.

3.2.2 ŘEŠENÍ POMOCÍ KONGRUENCE

S kongruencemi již umíme řešit diofantické rovnice o dvou neznámých. Při výpočtech příkladů s rovnicemi o třech a více neznámých budeme postupovat obdobně. Za modul můžeme opět volit libovolný koeficient u neznámé – často je výhodné počítat podle nejmenšího modulu. Nově lze za modul zvolit největšího společného dělitele koeficientů u $n - 1$ neznámých (za předpokladu, že největší společný dělitel bude různý od jedné), pak budeme řešit kongruenci o jedné neznámé a následně postupně dopočítáme zbývající proměnné. Pokud je to možné, využijeme možnost volby modulu podle největšího společného dělitele.

Příklad 3.9. Najděte řešení rovnice ve tvaru $8x + 9y - 11z = 16.$ (3.21)

Řešení:

Nejdříve zjistíme, zda je rovnice (3.21) řešitelná za pomoci Věty 3.2 na straně 39.

$$D(8,9,11) = 1 \wedge 1|16$$

Rovnice je řešitelná.

Diofantickou rovnici (3.21) převedeme na kongruenci. Největší společný dělitel dvou koeficientů je vždy roven jedné. Za modul tedy zvolíme nejmenší koeficient u neznámé x

$$8x + 9y - 11z \equiv 16\ (mod\ 8).$$

Upravíme

$$9y - 11z \equiv 16\ (mod\ 8).$$

Na obou stranách budeme dělit číslem 8. Následně dostaneme zbytek, který patří do (FÚSZ)

$$y - 3z \equiv 0\ (mod\ 8),$$

$$y \equiv 3z\ (mod\ 8),$$

$$y = 3z + 8t. \qquad (3.22)$$

Nyní dosadíme (3.22) do (3.21)

$$8x + 9 \cdot (3z + 8t) - 11z = 16,$$

$$8x + 27z + 72t - 11z = 16,$$

$$8x + 16z = 16 - 72t.$$

Vypočítáme neznámou x - osamostatníme a vydělíme rovnici číslem 8

$$x = 2 - 9t - 2z. \qquad (3.23)$$

Jestliže platí rovnice (3.23), musí platit i

$$x \equiv 2 - 9t - 2z\ (mod\ 2),$$

$$x \equiv 2 - 9t\ (mod\ 2),$$

$$x = 2 - 9t + 2s. \qquad (3.24)$$

Do rovnice (3.21) dosadíme řešení (3.22) a (3.24) a najdeme poslední předpis pro neznámou z

$$8(2 - 9t + 2s) + 9(3z + 8t) - 11z = 16,$$

$$16 - 72t + 16s + 27z + 72t - 11z = 16,$$

$$16 + 16s + 16z = 16,$$

$$16z = -16s,$$

$$z = -s.$$

Získali jsme řešení diofantické rovnice (3.21)

$$x = 2 - 9t + 2s,$$

$$y = 8t - 3s,$$

$$z = -s; s, t \in \mathbb{Z}.$$

Závěr:

Řešením je uspořádaná $n - tice$ (v našem případě trojice), kterou lze na základě různých řešitelských postupů zapsat několika možnými správnými způsoby. Tento způsob řešení je jedním z nejrychlejších a zároveň jedním z nejefektivnějších způsobů, jak najít všechna řešení diofantické rovnice o několika neznámých.

3.2.3 METODA VYJÁDŘENÍ ČLENU S NEJMENŠÍM KOEFICIENTEM

Metoda vyjádření členu s nejmenším koeficientem pro rovnice o třech a více neznámých je stejně jako pro rovnice o dvou neznámých univerzální metodou. Tato metoda využívá svůj potenciál právě pro rovnice o více neznámých – jak zjistíme v následujícím příkladu její výhodou je nejen přehlednost a rychlost.

Příklad 3.10. Najděte řešení rovnice ve tvaru $8x + 9y - 11z = 16$.

Řešení:

Vyjádříme neznámou s nejnižším koeficientem a osamostatníme ji. Dostaneme zlomek

$$x = \frac{-9y + 11z + 16}{8}. \qquad (3.25)$$

Protože $9y = 8y + y$ a číslo 16 je dělitelné číslem 8, můžeme zlomek (3.25) rozdělit na celou část a „zbylou“ část

$$x = -\frac{8y}{8} + \frac{-y + 11z + 16}{8} = -y + 2 + \frac{-y + 11z}{8}. \qquad (3.26)$$

Protože x a y jsou celá čísla, tak i zlomek $\frac{-y+11z}{8}$ musí být celé číslo.

Tuto část zlomku označíme např. jako t, zároveň dosadíme t i do (3.26)

$$t = \frac{-y + 11z}{8}, \qquad (3.27)$$

$$x = -y + 2 + t. \tag{3.28}$$

Ze „zbylé“ části (3.27) nyní vyjádříme neznámou y

$$y = -8t + 11z.$$

Dostali jsme rovnici, kterou tvoří pouze celá část. Můžeme začít zpětně dosazovat a vyjadřovat neznámé. Vidíme, že neznámá z je nezávislá, tudíž pro ní zvolíme libovolný parametr, např. $z = u, kde\ u \in \mathbb{Z}$. Neznámou x vyjádříme z rovnice (3.28), na neznámou y jsme přišli přímo.

$$x = -(-8t + 11z) + 2 + t = 8t - 11z + 2 + t = 9t - 11z + 2$$

Obecné řešení diofantické rovnice je

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

$$\mathrm{y} = 11u - 8t,$$

$$z = u, kde\ u, t \in \mathbb{Z}.$$

Závěr:

Metoda vyjádření členu s nejmenším koeficientem je univerzální – stejný postup bychom použili i pro rovnice se čtyřmi a více neznámými. Jak jsme již řekli, tato metoda najde své uplatnění hlavně pro rovnice o více neznámých. Spolu s kongruencemi je tato metoda nejvyužívanější pro diofantické rovnice o třech a více neznámých – je rychlá, přehledná a efektivní.

3.2.4 UPRAVENÁ METODA EUKLEIDOVA ALGORITMU

Tuto metodu můžeme najít v [11] na straně 61. Autor uvádí, že hlavní výhodou této metody je její jednoduchost. Pomocí této metody lze spočítat rovnice o n neznámých a vystačíme si pouze se znalostí Eukleidova algoritmu, největšího společného dělitele koeficientů u $n - 1$ neznámých a se substitucemi. Jestliže nelze najít největšího společného dělitele různého od jedné, nelze tuto metodu použít. Postup metody vysvětlíme na ilustračním příkladu.

Příklad 3.11. Najděte řešení rovnice ve tvaru $8x + 10y + 3z = 7.$ (3.29)

Řešení:

U této metody je potřeba najít největšího společného dělitele koeficientů u $n - 1$ neznámých – v tomto případě u dvou neznámých.

$$D(8, 10) = 2$$

Provedeme úpravu rovnice (3.29) – z koeficientů u neznámých x, y vytkneme největšího společného dělitele – číslo 2

$$2(4x + 5y) + 3z = 7 \quad (3.30)$$

Zavedeme substituci za závorku z (3.30) – substituce bude ve tvaru $4x + 5y = u$ (3.31)

$$2u + 3z = 7 \quad (3.32)$$

Získali jsme rovnici (3.32) o dvou neznámých, kterou již zvládneme vyřešit. Pomocí Eukleidova algoritmu získáme následující Bezoutovu rovnost

$$3 \cdot 1 + 2(-1) = 1,$$

$$3 \cdot 7 + 2(-7) = 7.$$

Řešením rovnice (3.32) jsou parametrické rovnice

$$u = 7 + 3t,$$
$$z = -7 - 2t, t \in \mathbb{Z}.$$

Vrátíme se k substituci (3.31) – musíme vyřešit rovnici $4x + 5y = 7 + 3t$. Tato rovnice má dvě neznámé – opět pomocí Eukleidova algoritmu získáme Bezoutovu rovnost

$$5 \cdot 1 + 4(-1) = 1,$$

$$5(7 + 3t) + 4(-7 - 3t) = 7 + 3t.$$

Řešením jsou parametrické rovnice

$$x = 7 + 3t + 5s,$$

$$y = -7 - 3t - 4s.$$

Řešení původní rovnice (3.29) jsou parametrické rovnice

$$x = 7 + 3t + 5s,$$

$$y = -7 - 3t - 4s,$$

$$z = -7 - 2t; t, s \in \mathbb{Z}.$$

Závěr

Pro rovnice o více než třech neznámých je způsob řešení stejný. Pouze v kroku, kdy se vrátíme k substituci, bude mít substituční rovnice o jednu neznámou méně než rovnice původní (nelze ihned využít Eukleidova algoritmu a Bezoutovy rovnice). Budeme muset substituční rovnici opět redukovat (substituovat). Takto budeme pokračovat, dokud rovnice nebude mít pouze dvě neznámé. Výhodou této metody je jednoduchost, přehlednost a vystačíme si pouze se základními znalostmi Eukleidova algoritmu, společného dělitele a substitucemi. Její nevýhoda spočívá v tom, že pokud nelze nalézt největšího společného dělitele koeficientů u $n - 1$ neznámých, nelze tuto metodu užít.

4 SLOVNÍ ÚLOHY ANEB VYUŽITÍ V PRAXI

V předchozích kapitolách jsme si řekli, co jsou to diofantické rovnice a jaké typy diofantických rovnic existují. Dále jsme se naučili počítat lineární diofantické rovnice o dvou, třech a více neznámých pomocí několika různých metod. Nyní plyne otázka: K čemu jsou diofantické rovnice vlastně dobré? Může se s nimi doopravdy setkat a vyřešit je i obyčejný člověk, který o tomto pojmu nemá ponětí?

Pomocí diofantických rovnic můžeme řešit široké spektrum slovních úloh. Tyto slovní úlohy v běžném životě představují různé situace, které pouze přepisujeme do jazyka matematiky. S diofantickými rovnici se člověk setkává vcelku často, většinou si ani neuvědomíme, že řešíme diofantické rovnice[15]. Každý z nás jistě chodí nakupovat a například při placení máme peněženku plnou drobných mincí. Prodavačka nám řekne cenu nákupu a my v této chvíli v hlavě nevědomky řešíme diofantickou rovnici. Potřebujeme najít jistou kombinaci mincí různých hodnot (od 1 koruny až do 50 koruny) tak, aby součet dával výslednou cenu nákupu. V této situaci nám samozřejmě stačí jedno řešení a přicházíme na něj experimentem.

Avšak můžeme se setkat i se složitějšími situacemi, kdy budeme mít zapeklitější slovní úlohu. Zde budeme muset nějakou metodou použít. Na diofantické rovnice vedou nejčastěji geometrické úlohy – snažíme se zjistit délky stran různých obrazců, jestliže víme jejich obvod; objemové úlohy – máme několik nádob o určitém objemu a potřebujeme je naplnit libovolnou tekutinou; nákupy – nakoupíme několik druhů zboží a víme výslednou částku nákupu atd. U slovních úloh je potřeba stanovit podmínky pro hodnoty parametrů tak, aby dávaly smysl. Nelze koupit záporné množství zboží, ani platit zápornými mincemi (ve skutečnosti placení mincemi se zápornou hodnotou funguje tak, že se jedná o vrácení peněz)[16].

[15] Většinou jsou tyto rovnice lehké, a proto nepotřebujeme znát potřebné aparáty k získání výsledného řešení.

[16] Tyto možnosti je vhodné z řešení vyloučit, jelikož nám mohou vzniknout nesmyslná řešení. Např. chceme zaplatit 2 Kč a použijeme na to 2x 20 Kč, 1x 10 Kč a 1x 2 Kč a bude nám vráceno zpět vše, kromě 1x 2 Kč.

Níže si ukážeme několik příkladů slovních úloh. Některé slovní úlohy jsou omezeny na intervalu podle parametrů, některé mají nekonečně mnoho řešení a některé mohou vést i na soustavu diofantických rovnic[17].

Veškeré metody, jsme vysvětlili v předchozích kapitolách, a proto postup řešení u následujících příkladů nebude tak detailní. Slovní úlohy roztřídíme do podkapitol podle počtu neznámých. Následně můžete na konci každé podkapitoly nalézt několik příkladů pro samostatné vyřešení. V příloze I. na konci této bakalářské práce najdete výsledná řešení.

4.1.1 SLOVNÍ ÚLOHY O DVOU NEZNÁMÝCH

Příklad 4.1. V rodinném obchůdku prodávají ručně vyrobené suvenýry - dva druhy trpaslíků. Jeden druh trpaslíků stojí 330 Kč za kus a druhý 450 Kč za kus. Turisté nakoupili trpaslíky v hodnotě 5670 Kč. Kolik kterých trpaslíků koupili?

Řešení:

První druh trpaslíků označíme jako x, druhý druh trpaslíků jako y a sestavíme rovnici

$$330x + 450y = 5670 \tag{4.1}$$

Nutná podmínka řešitelnosti (pokud si nejsme jistí největším společným dělitelem, najdeme jej pomocí Eukleidova algoritmu)

$$D(330{,}450) = 10 \wedge 10|5670.$$

Rovnice je řešitelná.

Pomocí Eukleidova algoritmu získáme následující Bezoutovu rovnost, kterou upravíme do základního tvaru dle (1.1) na straně 8

$$330(-4) + 450 \cdot 3 = 30. \tag{4.2}$$

Našli jsme základní řešení $x_0 = -4, y_0 = 3$ pro rovnici $330x + 450y = 30$.

Měli jsme ale zadanou rovnici (4.1), a proto rovnici (4.2) vynásobíme číslem 189, abychom dostali po vynásobení s číslem 30 číslo 5670.

$$330 \cdot (-756) + 450 \cdot (567) = 5670$$

[17] Více o soustavách diofantických rovnic můžeme najít v [2] na straně 21.

Našli jsme základní řešení $x_0^* = -756, y_0^* = 567$ zadané rovnice (4.1).

Všechna řešení lze nalézt pomocí základních řešení a vzorců (3.6) a (3.7) na straně 25

$$x = -756 + \frac{450}{30}t,$$

$$y = 567 - \frac{330}{30}t.$$

Zjednodušíme

$$x = -756 + 15t,$$

$$y = 567 - 11t, t \in \mathbb{Z}.$$

Pozor!

Oproti předchozím příkladům, musíme u slovní úlohy stanovit podmínky pro hodnotu parametru t pomocí nerovností, nebo se můžeme snažit nalézt nezáporné hodnoty x, y volbou vhodného parametru t. Hranici intervalu, do které spadnou hodnoty parametru t, zjistíme z parametrické rovnice pro neznámou x a to tak, aby nám vyšlo co nejmenší nezáporné číslo. Druhá hranice intervalu bude určena obdobně – parametrickou rovnicí pro neznámé y, aby nám opět vyšlo co nejmenší nezáporné číslo.

t	51
x	9
y	6

Tabulka 7: Stanovení hodnoty parametru t a hodnot x a y

Horní i dolní hranice je ohraničena stejným parametrem $t = 51$. Existuje pouze jedno řešení.

Turisté koupili 9 trpaslíků prvního druhu a 6 trpaslíků druhého druhu.

Příklad 4.2. Určete délky stran rovnoramenných trojúhelníků, jejichž strany jsou celá čísla a obvod se rovná 50 cm.

Řešení:

Stejně dlouhé strany označíme jako x, zbylou stranu jako y a sestavíme rovnici

$$2x + y = 50. \tag{4.3}$$

Ověříme, zda je rovnice řešitelná

$$D(2,1) = 1 \wedge 1|50.$$

Rovnice je řešitelná. Úlohu budeme řešit pomocí kongruence

Diofantickou rovnici převedeme na kongruenci. Budeme počítat opět podle nejmenšího možného modulu – podle neznámé x.

$$2x + y \equiv 50\ (mod\ 2)$$

$$y \equiv 50\ (mod\ 2)$$

$$y \equiv 0\ (mod\ 2)$$

$$y = 0 + 2t, t \in \mathbb{Z} \tag{4.4}$$

Rovnici (4.4) dosadíme do (4.3) a dopočítáme parametrickou rovnici pro x

$$2x + (0 + 2t) = 50,$$

$$x = 25 - t.$$

Parametrické rovnice vyhovující zadání jsou

$$x = 25 - t, \tag{4.5}$$

$$y = 2t, t \in \mathbb{Z}. \tag{4.6}$$

Stanovíme podmínky parametru t tak, aby mělo řešení smysl. Nesmíme zapomenout, že u trojúhelníku platí, pravidlo, že součet délek dvou stran musí být větší než délka zbývající strany

$$x > 0,$$

$$y > 0,$$

$$2x > y.$$

Zjistíme hodnoty parametru t z parametrických rovnic (4.5) a (4.6).

$$2 \cdot (25 - t) > 2t$$

$$50 - 2t > 2t$$

$$t < \frac{50}{4} = 12{,}5$$

$$t > 0$$

t	12	11	10	…	2	1
x	13	14	15	…	23	24
y	24	22	20	…	4	2

Tabulka 8: Stanovení hodnoty parametru t a hodnot x a y

Existuje mnoho řešení, parametr $t \in \langle 1; 12 \rangle$.

Délky stran rovnoramenného trojúhelníka mohou být např.

[13,13,24]; [14,14,22]; …; [24,24,2].

Cvičení 4.1. Vyřešte následující slovní úlohy.

1. Farmář má na farmě prasata a slepice. Kolik prasat a slepic farmář vlastní, pakliže nám řekl, že mu po zahradě běhá celkem 70 nohou. (*Pozn.* každé zvíře má patřičný počet nohou, tedy prase má čtyři nohy a slepice dvě nohy).
2. Máme stužku dlouhou 50cm a chceme z ní nastříhat proužky – 6 cm a 4 cm dlouhé. Kolika způsoby to můžeme udělat? (*Pozn.* stužku stříháme postupně tak, aby žádný kus nezbyl).
3. Vyrobili jsme 232 litrů jablečného moštu a chceme jej prodat. Máme k dispozici dvě velikosti nádob, do kterých mošt můžeme přelít. První má objem 3 litry, druhá nádoba má objem 5 litrů. Kolik nádob od každého druhu potřebujeme k přelití 232 litrů moštu? (*Pozn.* při přelévání nevylejeme nic mimo nádoby a nádoby plníme až po okraj).

4. Skupina přátel byla v restauraci. Každá žena zaplatila útratu 1000 Kč a každý muž 1500 Kč. Celková útrata byla 12 000 Kč. Kolik žen a kolik mužů bylo ve skupině, když rozdíl mezi počtem mužů a počtem žen byl nejmenší možný?

4.1.2 SLOVNÍ ÚLOHY O TŘECH A VÍCE NEZNÁMÝCH

Příklad 4.3. Ve vodním světě jsme v akváriu viděli 124 zamotaných chapadel červené, modré a fialové barvy. Dle průvodce jsou v akváriu modré chobotnice mající 8 chapadel, červené olihně mající 10 chapadel a fialové chobotnice mající 6 chapadel.

(*Pozn.* Barvy chobotnic i počty chapadel nemusí odpovídat realitě. Není známá žádná chobotnice ani jí příbuzný tvor mající 6 chapadel, ačkoliv oceán je obrovský a je možné, že někde takový tvor existuje).

Řešení:

Modré chobotnice označíme x, červené olihně označíme y a fialové chobotnice z. Dostaneme rovnici

$$8x + 10y + 6z = 124. \tag{4.7}$$

Ověříme, zda je rovnice řešitelná

$$D(8,10,6) = 2 \wedge 2|124.$$

Rovnice je řešitelná. Úlohu budeme řešit pomocí metody vyjádření členu s nejmenším koeficientem.

Nejdříve vyjádříme neznámou s nejnižším koeficientem. Dostaneme zlomek

$$x = \frac{-10y - 6z + 124}{8}. \tag{4.8}$$

Protože $10y = 8y + 2y$ můžeme zlomek (4.8) rozdělit na celou část a „zbylou“ část

$$x = -\frac{8y}{8} + \frac{-2y - 6z + 124}{8} = -y + \frac{-2y - 6z + 124}{8}. \tag{4.9}$$

Zlomek $\frac{-2y-6z+124}{8}$ musí být celé číslo. Tento zlomek označíme např. jako t a dosadíme do (4.9)

$$t = \frac{-2y - 6z + 124}{8},$$

$$x = -y + t. \tag{4.10}$$

Ze „zbylé“ části nyní vyjádříme neznámou y

$$y = -4t - 3z + 62, t \in \mathbb{Z}.$$

Dostali jsme rovnici, kterou tvoří pouze celá část. Neznámou x vyjádříme z rovnice (4.10).

$$x = -(-4\mathrm{t} - 3\mathrm{z} + 62) + t = 5t + 3z - 62$$

Neznámá z je nezávislá, zvolíme libovolný parametr např. $z = u, u \in \mathbb{Z}$.

Řešení diofantické rovnice (4.7) je

$$x = 5t + 3u - 62,$$

$$y = 62 - 4t - 3u,$$

$$z = u;\ kde\ t, u \in \mathbb{Z}.$$

Najdeme podmínky pro parametry t, u tak, aby příklad dával smysl.

$$x > 0, y > 0, u > 0$$

$$\frac{62 - 3u}{5} < t < \frac{62 - 3u}{4}$$

Některá řešení jsou vidět níže v Tabulce 9, avšak je jich mnoho na to, abychom je vypisovali.

u	1	1	1	2	2	3	3	3	…	16
t	12	13	14	12	13	11	12	13	…	3
x	1	6	11	4	9	2	7	12	…	1
y	11	7	3	8	4	9	5	1	…	2
z	1	1	1	2	2	3	3	3	…	16

Tabulka 9: Stanovení hodnot parametrů t, u a hodnot x, y, z

V akváriu může být např. 7 modrých chobotnic, 5 červených olihní a 3 fialové chobotnice.

Příklad 4.4. Vstupenky na školní ples stojí pro žáky 60 Kč, pro jednoho rodiče 160 Kč a pro všechny ostatní návštěvníky 240 Kč. Na vstupném se vybralo přesně 7520 Kč a prodalo se právě 100 vstupenek. Kolik rodičů přišlo na ples?

Řešení:

Žáky označíme jako x, rodiče jako y a ostatní jako z

$$60x + 160y + 240z = 7520. \tag{4.11}$$

Ověříme, zda je rovnice řešitelná

$$D(60,160,240) = 20 \wedge 20|7520.$$

Rovnice je řešitelná. Úlohu budeme řešit za pomocí kongruencí.

Nyní si diofantickou rovnici (4.11) převedeme na kongruenci, podle největšího společného dělitele koeficientů u $y\ a\ z$ – podle čísla 80 a spočítáme neznámou x

$$60x + 160y + 240z \equiv 7520\ (mod\ 80),$$

$$60x \equiv 0\ (mod\ 80),$$

$$x = 0 + 4t, t \in \mathbb{Z}. \tag{4.12}$$

Rovnici (4.12) dosadíme do (4.11)

$$60(0 + 4t) + 160y + 240z = 7520,$$

$$240t + 160y + 240z = 7520. \tag{4.13}$$

Jestliže platí (4.13), musí platit i následující rovnice. Vypočítáme další neznámou

$$240t + 160y + 240z \equiv 7520\ (mod\ 240),$$

$$160y \equiv 7520\ (mod\ 240),$$

$$16y \equiv 752\ (mod\ 24),$$

$$2y \equiv 94\ (mod\ 3),$$

$$y \equiv -1\ (mod\ 3),$$

$$y = -1 + 3s, s \in \mathbb{Z}. \tag{4.14}$$

Do rovnice (4.11) dosadíme parametrické rovnice (4.12) a (4.14) a najdeme poslední parametrickou rovnici pro neznámou z

$$60(0 + 4t) + 160(-1 + 3s) + 240z = 7520,$$

$$60(0 + 4t) + 160(-1 + 3s) + 240z = 7520,$$

$$24t - 16 + 48s + 24z = 752,$$

$$z = 32 - t - 2s; t, s \in \mathbb{Z}.$$

Získali jsme řešení diofantické rovnice (4.11)

$$x = 4t,$$

$$y = 3s - 1,$$

$$z = 32 - t - 2s; t, s \in \mathbb{Z}.$$

Najdeme podmínky pro parametry t, s tak, aby úloha dávala smysl.

$$x \geq 0, y \geq 0, z \geq 0, x + y + z = 100$$

$$-1 + 3s > 0 \rightarrow s > \frac{1}{3}$$

$$0 + 4t > 0 \rightarrow t > 0$$

$$32 - t - 2s > 0 \rightarrow t < 32 - 2s$$

s	**1**	**1**	**1**	**…**	**3**	**…**	**15**
t	1	2	3	…	22	…	2
x	4	8	12	…	88	…	8
y	2	2	2	…	8	…	44
z	29	28	27	…	4	…	0

Tabulka 10: Stanovení hodnot parametrů t, s a hodnot x, y, z

V pátém sloupci Tabulky 10 jsme našli odpověď na naši otázku. Součet vstupenek je zde $100 = 88 + +8 + 4$.

Na ples přišlo 8 rodičů.

Cvičení 4.2. Vyřešte následující slovní úlohy a rovnici.

1. V peněžence máme mince v hodnotách 5, 10 a 20 korun. Jak lze zaplatit nákup v hodnotě 300,- korun, když víme, že každou minci musíme použít alespoň jednou.
2. Do košíku se vejde 48 plodů ovoce. Ovoce máme roztříděné v sáčcích – jablka jsou balena po 2 kusech, hrušky jsou balené po 4 kusech, švestky jsou balené po 16 kusech a třešně po 32 kusech. Kolik sáčků s ovoci bude v košíku? A jakého druhu ovoce budou?
3. Najděte řešení rovnice $2x + 4y + 8z + 16w = 32$.

ZÁVĚR

V této práci jsme se zabývali převážně lineárními diofantickými rovnicemi a slovními úlohami. Zjistili jsme, že každý z nás již před přečtením této práce diofantickou rovnici řešil. A to i přesto, že o problematice diofantických rovnic nikdy neslyšel. S tímto pojmem se totiž setkáme až na vysoké škole i přesto, že slovní úlohy vedoucí na diofantické rovnice, jsou běžné situace, které jsou pouze přepsané do světa matematiky (viz motivace v úvodu). Samozřejmě některé úlohy mohou být, jak jsme zjistili, komplikovanější a poté je nutné znát potřebné aparáty k vyřešení. S těmi lehčími si ale naopak umí poradit i děti na základní škole.

V roce 1970 ruský matematik Jurij Vladimirovič Matijasevič dokázal, že neexistuje univerzální postup, jak řešit diofantické rovnice. Proto musíme šikovně užít nějaký způsob řešení, který jsme v této bakalářské práci uvedli. Nyní bychom měli zvládat efektivně užít jednotlivé metody a vědět, kdy je jaká metoda výhodnější. Tabulky na další straně nám shrnují poznatky, na které jsme přišli – výhody a nevýhody jednotlivých metod a „návod“, kdy je vhodné použít určitou metodu.

Na základě této bakalářské práce bychom měli zvládat problematiku řešení lineárních diofantických rovnic. Tím ale studium diofantických rovnic nekončí. Před námi je stále veliká neznámá v podobě kvadratických diofantických rovnic a Velké Fermatovy věty. Tato práce tak může sloužit jako „odrazový můstek“ do studia složitějších diofantických rovnic.

NÁZEV METODY	VÝHODY	NEVÝHODY
„Metoda pokus – omyl“	- vhodné pro lidi, kteří neznají efektivnější způsoby řešení - lze řešit lineární diofantické rovnice o dvou a více neznámých	- neefektivní „metody“ (nemusíme najít všechna řešení) - příliš pomalé nalezení řešení
Grafická „metoda“		
Metoda s využitím Eukleidova algoritmu	- univerzální metoda pro rovnice o dvou neznámých - rychlá metoda	- nutná znalost algoritmu - nelze řešit rovnice o třech a více neznámých (pro ty můžeme použít upravenou metodu – musí existovat největší společný dělitel $n-1$ neznámých různý od jedné)
Kongruence	- zkrácený zápis pomocí kongruence - rychlý způsob řešení - lze řešit rovnice o dvou a více neznámých	- nutná znalost počítání s kongruencemi
Metoda vyjádření členu s nejnižším koeficientem	- univerzální metoda - rychlý způsob řešení - lze řešit rovnice o dvou a více neznámých	X

Tabulka 11: Přehled použitých metod

DOPORUČENÉ METODY PRO POČÍTÁNÍ S URČITÝM POČTEM NEZNÁMÝCH	
Lineární diofantické rovnice o dvou neznámých	- Eukleidův algoritmus - Kongruence
Lineární diofantické rovnice o třech a více neznámých	- Kongruence - Metoda vyjádření členu s nejnižším koeficientem

Tabulka 12: Doporučené metody pro počítání s určitým počtem neznámých

SHRNUTÍ

Tato bakalářská práce se zabývá diofantickými rovnicemi a slovními úlohami. Práce je členěna do čtyř kapitol. První kapitola popisuje historii Diofanta z Alexandrie a obsahuje úvod do problematiky diofantických rovnic. Druhá kapitola obsahuje důležité pojmy, které je nutné znát – jsou pro počítání s diofantickými rovnicemi nezbytné. Třetí kapitola se zabývá způsoby řešení lineárních diofantických rovnic. V první části této kapitoly řešíme rovnice o dvou neznámých, následně v druhé části kapitoly aplikujeme poznatky na rovnice o třech a více neznámých. V poslední kapitole je uvedeno využití lineárních diofantických rovnic ve slovních úlohách.

RESUMÉ

This bachelor thesis deals with diophantine equations and word problems. The thesis is divided into four chapters. The first chapter describes the history of Diofantos from Alexandria and contains an introduction to the problems of the diophantine equations. The second chapter contains important concepts that need to be known - they are necessary for calculating the diophantine equations. The third chapter deals with ways of solving linear diophantine equations. In the first part of this chapter we solve the equations with two variables, then in the second part of the chapter we apply the knowledge on equations with three and more variables. The last chapter describes the use of linear diophantine equations in word problems.

SEZNAM LITERATURY

[1] BÁBÍČKOVÁ, K. *Soustavy lineárních diofantovských rovnic a Smithův normální tvar matice*. Plzeň: 2017. Diplomová práce. Západočeská univerzita v Plzni. Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

[2] BLÁHOVÁ, M. *Vybrané typy diofantických rovnic a jejich početní využití*. Plzeň: 2015. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce: Mgr. Lukáš Honzík, Ph.D.

[3] DAŇKOVÁ, M. *O řešitelnosti některých typů diofantovských rovnic*. Plzeň: 2007. Diplomová práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

[4] DRÁBEK, J. *Učební texty k předmětu Elementární algebra*. [cit. 2018-Únor-08].

[5] HABALA, P. *Diofantické rovnice*. 2016 [cit. 2018-Březen-06]. Dostupné z: https://math.feld.cvut.cz/habala/teaching/dma/dmkni04.pdf

[6] HEATH, T. L. *Diophantos of Alexandria : A Study in the History of Greek Algebra*. Cambridge: University press warehouse, 1885 [cit. 2018-Únor-13]. Dostupné z: https://archive.org/details/diophantusofalex00heatiala

[7] HERMAN, J. R. KUČERA a J. ŠIMŠA. *Metody řešení matematických úloh I.* 2. vydání. Brno: Masarykovo univerzita, 2011. ISBN 9788021056367.

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

[9] KOLMAN, A. *Dějiny matematiky ve starověku*. Praha: Academia, nakladatelství Československé akademie věd, 1969, 224 s.. ISBN: 507-21-875.

[10] MOKRÁ, T. *Lineární diofantické rovnice*. Brno: 2015. Bakalářská práce. Masarykova univerzita. Vedoucí práce Mgr. Vojtěch Žádník, Ph.D.

[11] STEINSDÖRFER, J. *Metody řešení diofantických rovnic* [Studijní text]. Ústí nad Labem: 2015 [cit. 2018-Duben-12]. Dostupné z: http://physics.ujep.cz/~jmaly/mo/Diofanticke_rovnice.pdf

[12] WILLERS, M. *Algebra bez (m)učení: od arabských matematiků k tajným šifrám: matematika v každodenním životě : …*. Praha: Grada, 2012. ISBN: 978-80-247-4123-9.

SEZNÁM PŘÍKLADŮ A CVIČENÍ

SEZNAM TABULEK

SEZNAM GRAFŮ

PŘÍLOHY

VÝSLEDKY CVIČENÍ

Nechť parametry $r, s, t, u \in \mathbb{Z}$. Řešení budou obsahovat parametrické rovnice jednotlivých neznámých a uspořádané $n-tice$.

Cvičení 4.1.

1. $x = 17 - t,$
   $y = 1 + 2t.$ Řešení jsou $[16; 3], [15; 5], [14; 7], \ldots, [1; 33]$.
2. $x = 1 + 2t,$
   $y = 11 - 3t.$ Stužku můžeme rozstříhat 4 způsoby ([1;11], [3;8], [5;5], [7,2]).
3. $x = 79 - 5t,$
   $y = -1 + 3t.$ Řešení jsou $[74; 2], [69; 5], [64; 8], \ldots, [4; 44]$.
4. $x = 3t,$
   $y = 8 - 2t.$ Ve skupině bylo 6 žen a 4 muži.

Cvičení 4.2.

1. $x = 2u + 2t - 58,$
   $y = 59 - t - 3u,$
   $z = u.$ Řešení jsou $[2,1,14]; [2,3,13]; [2,5,12], [4,2,13], [2,7,11]$.
2. $x = 2t,$
   $y = 4s - t,$
   $z = 1 - s + 2r,$
   $w = 1 - r.$ Řešení je mnoho.
3. $x = 2t,$
   $y = t + 2s,$
   $z = -t - s + 4 - 2u,$
   $w = u.$