ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

ÚLOHY S DIOFANTICKÝMI ROVNICEMI

BAKALÁŘSKÁ PRÁCE

Simona Šourková
Přírodovědná studia, obor Matematická studia

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

Plzeň 2023

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

V Plzni 27. dubna 2023

....

Simona Šourková

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu své bakalářské práce panu PhDr. Lukáši Honzíkovi, Ph.D. za doporučení a připomínky během psaní bakalářské práce. Dále bych chtěla poděkovat své rodině a přátelům za podporu v průběhu celého mého studia.

OBSAH

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

$+$	plus
$-$	mínus
$\cdot$	krát
$:$	děleno
$\frac{x}{y}$	dělící lomítko
$=$	rovná se
$\neq$	nerovná se
$>, \geq$	větší, větší nebo rovno
$<, \leq$	menší, menší nebo rovno
$\equiv$	kongruence
$\mid$	dělí
$\nmid$	nedělí
$(\ )^2, (\ )^n$	na druhou, na n-tou
$\lvert\ \ \rvert$	absolutní hodnota
$(\ \ ), [\ \ ], \{\ \ \}, \langle\ \ \rangle$	kulaté, hranaté, složené, lomené závorky
$\in$	je prvkem
$\wedge$	konjunkce
$\exists$	existuje
$\nexists$	neexistuje
$\forall$	pro všechny
$\Rightarrow$	z toho vyplývá
$\Leftrightarrow$	právě tehdy když
$\mathbb{N}$	množina přirozených čísel
$\mathbb{Z}$	množina celých čísel

x, y, z, v, w	neznámé
a, b, c, d, e, f, k, n	konstanty
r, s, t, u	parametry
i, j	indexy
m	přirozené číslo, které je větší než 1
p	prvočíslo
Z	zbytková třída
$\varphi(n)$	Euklidova funkce
$\mathrm{mod}, (\mathrm{mod}\ m)$	modulo, modulo čísla m
$\mathrm{NSD}, \mathrm{NSD}(a, b)$	největší společný dělitel, největší společný dělitel čísel a a b
Kč	Koruna česká
ml	mililitr
NSN	nejmenší společný násobek
FÚSZ	fundamentální úplná soustava zbytků
ÚSZ	úplná soustava zbytků

ÚVOD

Diofantické rovnice představují fascinující oblast matematiky, která se zaměřuje na hledání celočíselných řešení. Tento problém má své kořeny v antickém Řecku a dodnes zůstává otevřeným tématem pro mnoho matematiků. Diofantické rovnice se vyskytují v různých oblastech matematiky, včetně teorie čísel, algebry, geometrie a teorie grafů.

Cílem této bakalářské práce je představit čtenářům diofantické rovnice a ukázat několik konkrétních úloh, které s nimi souvisí.

V první kapitole se zaměříme na historický vývoj této oblasti matematiky. Budeme pokračovat kapitolou 2, kde čtenáře seznámíme se základními typy diofantických rovnic a následně v kapitole 3 představíme základní pojmy a definice, které jsou potřebné k pochopení této problematiky. V kapitole 4 a 5 se dále budeme věnovat několika typům diofantických rovnic a ukážeme si nejvýznamnější metody a techniky, které se používají k hledání řešení těchto rovnic. V rámci těchto dvou kapitol si uvedeme i cvičné příklady, jejichž řešení nalezneme v příloze.

V rámci těchto kapitol je postupně splněno zadání této bakalářské práce.

1 DIOFANTOS Z ALEXANDRIE

Ačkoliv je Diofantos nazýván „otcem algebry“, jeho život můžeme považovat za jednu z největších hádanek historie matematiky. Místo působení tohoto významného matematika je nám velmi dobře známo, je jím slavná Alexandrie, ovšem období jeho života je předmětem spekulací a domněnek, i když některé aspekty Diofantova života dokážeme určit téměř s přesností.

Diofantos mohl žít kdykoliv v období od 2. stol. př. n. l. až do poloviny 4. stol. n. l. Tato informace je známa díky tomu, že Diofantos v jednom ze svých děl cituje Hypsicla, který působil v Alexandrii ve 2. stol. př. n. l. a na druhou stranu se o Diofantovi zmiňuje Theon, který působil v Alexandrii cca v roce 350 n. l. Toto 500 let dlouhé období bylo zúženo díky práci Tannera, který studoval spisy Michaela Psellusea. Ve svých spisech se Michael Pselluse zmiňuje o Diofantovi a Anattoliim jako o současnících. Jelikož je nám známo, že Anattolii se věnoval vědě a psaní až do doby, kdy se stal biskupem Laodicei, což bylo okolo roku 280 n. l., vyplývá z toho, že pokud byli Diofantos a Anattolii současníci, Diofantos musel v Alexandrii působit v polovině 3. st. n. l., na což poukazují i další informace, které byly předmětem rozsáhlých studií.

I přes to, že nedokážeme s přesností určit rozmezí let jeho života, víme s jistotou kolika let se dožil, a to díky matematické hádance, jež byla vytesána na jeho náhrobní kámen. Existuje nespočet překladů originálního znění této slavné hádanky. My si uvedeme jen jeden z nich, a to překlad ve verších:

„Zde leží Diofantos, jaký to div,
algebra poví, jak dlouho byl živ:
Bůh dal mu dětský věk šestinu žití,
dvanáctinu pak, než vousy mohl míti;
Po další sedmině svou ženu si vzal;
a za pět let otcem syna se stal.
Ach, ubohé to 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.“ [1]

Hádanku vyřešíme sestavením jedné rovnice o jedné neznámé následovně:

- Jako neznámou x zvolíme věk Diofanta;
- Sestavíme rovnici:

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

- Rovnici vyřešíme:

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x \quad /\cdot 84$$

$$14x+7x+12x+42x-84x=-756$$

$$-9x=-756$$

$$x=84$$

Po vypočtení neznámé x se tedy dozvídáme, že jeho život trval 84 let. Po 14 let byl dítětem, ve 21 letech mu narostly vousy a ve 33 letech se oženil. Za dalších 5 let, tedy ve věku 38 se stal otcem syna, který přišel o život, když Diofantovi bylo 80. O další 4 roky později sám Diofantos zemřel. Je zřejmé, že hádanku psal blízký přítel, ne dlouho po Diofantově smrti, který měl také zájem o matematiku.

Další velkou hádankou, možná větší než samotný život Diofanta, jsou jeho díla, jelikož se jejich velká část nedochovala. Za jeho nejvýznamnější práci považujeme „Aritmetiku", v které se setkáváme se zcela jinou algebrou, z jejichž knih vycházeli matematici po celý středověk. Setkáváme se s algebrou založenou na aritmetice, jak napovídá samotný název, a ne na geometrii, jak tomu bylo v případě Euklida. „Aritmetika" původně obsahovala 13 knih, z nichž se dochovalo pouhých šest. Můžeme se tak pouze domnívat o bohatosti a zajímavosti díla jako celku. Na první dojem se může zdát, že „Aritmetika" není ničím průlomové dílo, že se jedná o klasický starověký matematický dokument, tedy že dílo obsahuje vyřešené úlohy, které na sebe nijak nenavazují a čtenář si musí obecný postup řešení složitě vydedukovat. Avšak při hlubším zkoumání tohoto díla vyplývá, že Diofantos se sice držel „normami antiky", ale typově stejné úlohy řadil pečlivě za sebou. Objevuje se zde tedy náznak obecného řešení.

Mylně se o Diofantovi často tvrdí, že neznal záporná čísla stejně jako jeho současníci. On však záporná čísla pouze nepovažoval za výsledek, ale ve svých mezi výpočtech je aktivně využíval. Záporná čísla dokonce označil speciálním termínem $\lambda\varepsilon\iota\psi\iota\varsigma$, který by mohl být přeložen jako „nedostatek". Diofantos zavedl celý systém matematických znaků, které do té doby matematici značili slovními popisy, což samozřejmě nebylo tak efektivní. Pro příklad, zavedl značení pro konstantní člen, který značil jednotu. Dále čtenáře seznámil se symbolikou pro první až šestou mocninou jedné neznáme, a to jak pro mocniny kladné, tak i mocniny záporné. Zavést symboliku pro druhou neznámou se mu však již nepovedlo. [2] [3]

2 DRUHY DIOFANTICKÝCH ROVNIC A NĚKTERÉ MOŽNOSTI JEJICH ŘEŠENÍ

Diofantické rovnice jsou rovnice, které hledají celočíselné řešení. Základní myšlenkou je nalézt všechna taková řešení, nebo dokázat, že taková řešení neexistují. Jelikož se jedná o rozsáhlý, stále otevřený, matematický problém, v mnoha případech obecná řešení nalézt nelze. Pro některé typy těchto rovnic je však možno při řešení aplikovat jednoduché algoritmy. Diofantické rovnice jsou pojmenovány po starověkém matematikovi Diofantovi, kterému byla věnována předchozí kapitola.

Existuje mnoho typů diofantických rovnic, které mají souvislost s různými oblastmi matematiky. Níže uvedené typy těchto rovnic jsou těmi nejčastěji se vyskytujícími.[1]

2.1 LINEÁRNÍ DIOFANTICKÁ ROVNICE VZHLEDEM K NEZNÁMÉ

Lineární diofantická rovnice vzhledem k neznámé má tvar

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

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

Při řešení této rovnice je vhodné použít Euklidův algoritmus, který umožňuje nalézt největší společný dělitel čísel a, b i koeficienty x, y tak, aby platilo:

$$ax + by = d,$$

kde d je největší společný dělitel[2] čísel a, b.

Řešení samotné diofantické rovnice nalezneme následovně:

Pokud c není násobkem d, rovnice nemá celočíselné řešení. V opačném případě lze získat neznámé x a y vynásobením neznámých x' a y', získaných z Euklidova algoritmu, číslem $\frac{c}{d}$. Výsledkem je tedy řešení původní diofantické rovnice (2.1).

[1] Kapitola 2 dle zdrojů: [3] [6] [7] [8] [9]
[2] Největší společný dělitel (NSD) je blíže probírán v kapitole 3.2.1

2.2 LINEÁRNÍ DIOFANTICKÁ ROVNICE O TŘECH NEZNÁMÝCH

Lineární diofantickou rovnici o třech neznámých můžeme obecně zapsat ve tvaru:

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

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

Rovnice má řešení v případě, že $\mathrm{NSD}(a, b, c)$ dělí d beze zbytku. Tedy pokud označíme $\mathrm{NSD}(a, b, c)$ jako d', tak musí platí $d' \mid d$.

> *Pozn.* Pro lineární diofantické rovnice o třech a více neznámých platí obdobné postupy pro nalezení řešení, jako je tomu i u lineárních diofantických rovnic s jednou neznámou.

2.3 KVADRATICKÉ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH

Kvadratická diofantická rovnice o dvou neznámých má tvar

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

kde $a, b, c, d, e, f \in \mathbb{Z}$ a x, y jsou neznámé celočíselné proměnné.
V případě takovéto rovnice je obtížné nalézt celočíselné řešení a není možné použít jednoduché algoritmy jako v případě lineárních diofantických rovnic. Neexistuje univerzální způsob řešení kvadratických diofantických rovnic o dvou neznámých, ale existují metody, jak nalézt alespoň některá z nich. Mezi tyto metody spadá například rozklad na parciální zlomky.

V některých speciálních případech těchto rovnic existují řešení, jež jsou mnohem jednodušší.

2.3.1 $ax^2 + cy^2 = z$

Rovnice tvaru

$$ax^2 + cy^2 = z,$$

kde $a, c, z \in \mathbb{N}$ a $x, y \in \mathbb{Z}$, je řešitelná v případě, že z je násobkem největšího společného dělitele čísel a, c. Jedna z metod řešení je vyjádření neznámých x, y jako lineární kombinaci celých čísel z koeficientů získaných pomocí rozkladu kvadratické formy.

2.3.2 PELLOVA ROVNICE

Dalším příkladem speciálních kvadratických diofantických rovnic je Pellova rovnice, která má tvar

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

kde $x, y \in \mathbb{Z}$ a $\forall d \in \mathbb{Z}, d > 0, (\nexists a \in \mathbb{Z}, a^2 = d) \Rightarrow (\exists x, y \in \mathbb{Z}, x^2 - dy^2 = 1)$. Řešení lze nalézt pomocí Pellova algoritmu.

2.3.3 PYTHAGOREJSKÁ ROVNICE

Tento typ kvadratické diofantické rovnice ve tvaru

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

vzhledem k neznámým x, y, z je všeobecně znám a má velký význam v geometrii a dalších oborech. Řešením jsou např. tzv. Pythagorejské trojice, které jsou tvořeny celočíselnými hodnotami x, y, z, které splňují tuto rovnici.

2.5 DIOFANTOVA ROVNICE S VYŠŠÍM STUPNĚM

Obecně platí, že diofantické rovnice s vyšším stupněm jsou velice obtížné a řešit je lze např. jen pro malé hodnoty exponentu.

Jedním z nejznámějších příkladů je rovnice:

$$x^n + y^n = z^n,$$

kde $n \in \mathbb{N}, n > 2$ a $x, y, z \in \mathbb{Z}$. Tato rovnice je známá jako Velká Fermatova věta a byla vyřešena až po více než 350 letech od jejího zformulování.

2.6 DIOFANTOVA SOUSTAVA ROVNIC

Diofantova soustava rovnic je soustava diofantických lineárních rovnic. Cílem řešení rovnic ve tvaru

$$a_1x + b_1y = c_1,$$
$$a_2x + b_2y = c_2$$

je najít celočíselná řešení (x, y) taková, že platí obě rovnice současně, tj. $x, y \in \mathbb{Z}$.

Existuje několik metod řešení těchto typů rovnic, jako např. metoda Gaussovy eliminace, Euklidův algoritmus nebo metoda zpětné substituce.

3 ZÁKLADNÍ POJMY

Před samotným řešením diofantických rovnic a slovních úloh vedoucí na diofantické rovnice je potřeba připomenout některé důležité základní pojmy týkající se této problematiky.[3]

3.1 DĚLITELNOST

Dělitelnost je vlastnost dvou celých čísel, kdy první číslo lze beze zbytku dělit druhým číslem. Říkáme tedy, že celé číslo a je dělitelné celým číslem b, jestliže existuje celé číslo k takové, že platí $a = b \cdot k$. Tuto vlastnost lze vyjádřit následovně: $b \mid a$, tzn. "b dělí a". Symbol "|" bývá nazýván značkou dělitelnosti. Např. 12 je dělitelné 3, protože $12 = 3 \cdot 4$.

V opačném případě, tedy pokud celé číslo a není dělitelné celým číslem b, říkáme, že a je nedělitelné číslem b.

3.1.1 PRVOČÍSLO

Pro celé číslo $p > 1$ platí, že p je prvočíslo, jestliže má právě dva dělitele, kterými jsou 1 a p samotné, tj. pokud pro žádné jiné celé číslo a neplatí, že a dělí p a zároveň a není 1, ani p samotné. Např. 2, 3, 5, 7, 11, 13, 17.

3.1.2 PRVOČÍSELNÝ ROZKLAD

Prvočíselný rozklad je proces rozkladu přirozeného čísla na součin prvočísel.

Nechť $n \geq 2, n \in \mathbb{Z}$, pak existuje jednoznačný rozklad čísla n na prvočísla takový, že:

$$n = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot \ldots \cdot {p_k}^{a_k},$$

kde $p_1, p_2, \ldots, p_k$ jsou různá prvočísla a $a_1, a_2, \ldots, a_k$ jsou kladné celé exponenty.

Při rozkladu čísla n na součin prvočísel postupujeme následovně:

1. Začneme s prvním prvočíslem, což je $p = 2$. Pokud je p dělitelem čísla n, lze zapsat p jako prvočíselný faktor a podělit n číslem p. Provádíme $\frac{n}{p}$, dokud je to možné.

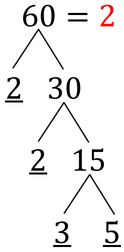
2. Pokračujeme s následujícími prvočísly, tj. 3, 5, 7, 11, 13… a opakujeme postup z 1. kroku, dokud nedostaneme číslo 1. Pokud některé z prvočísel p nedělí n, lze dané prvočíslo p přeskočit.

[3] Kapitola 3 dle zdrojů: [5] [6] [10] [11] [12] [13]

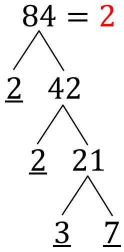
3. Nalezená prvočísla zapíšeme v součinovém tvaru a dostaneme jednoznačný rozklad daného čísla n na prvočísla.

Např. pro čísla 60 a 84 provedeme rozklad následovně:

$60 = 2 \cdot 2 \cdot 3 \cdot 5$



$84 = 2 \cdot 2 \cdot 3 \cdot 7$



3.1.3 KRITÉRIA DĚLITELNOSTI

Kritéria dělitelnosti nám umožňují rychle a efektivně určit, zda je celé číslo dělitelné určitým číslem bez nutnosti provádět samotné dělení. Existuje několik takových kritérii, některá z nich jsou:

Kritérium dělitelnosti 2: Číslo je dělitelné 2, pokud je jeho poslední cifra sudá.
Kritérium dělitelnosti 3: Číslo je dělitelné 3, pokud je součet jeho cifer dělitelný 3.
Kritérium dělitelnosti 4: Číslo je dělitelné 4, pokud je jeho poslední dvojcifra dělitelná 4.
Kritérium dělitelnosti 5: Číslo je dělitelné 5, pokud je jeho poslední cifra 5 nebo 0.
Kritérium dělitelnosti 6: Číslo je dělitelné 6, pokud je dělitelné 2 a 3 současně.
Kritérium dělitelnosti 9: Číslo je dělitelné 9, pokud je součet jeho cifer dělitelný 9.
Kritérium dělitelnosti 11: Číslo je dělitelné 11, pokud je rozdíl součtu jeho cifer na lichých a sudých pozicích dělitelný 11.
Kritérium dělitelnosti 25: Číslo je dělitelné 25, pokud je jeho poslední dvojčíslí 00, 25, 50 nebo 75.

3.1.4 OBECNÁ KRITÉRIA DĚLITELNOSTI

Vysvětlení nejobecnějšího kritéria obsahuje začátek této kapitoly (viz kapitola 3.1). Pro některá čísla však existují speciální kritéria dělitelnosti.

Např. dle Eulerova kritéria dělitelnosti platí pro liché číslo n a prvočíslo p, že n je dělitelné prvočíslem p, právě tehdy, když platí kongruence $n \equiv 1 \pmod{2\,p}$.

Další podobná kritéria existují např. pro sudá čísla, mocniny prvočísel.

3.2 SPOLEČNÝ DĚLITEL

Společný dělitel je číslo, které dělí dvě nebo více čísel beze zbytku. Pokud máme čísla a, b, c, pak číslo d je společným dělitelem těchto čísel, pokud platí:

$d \mid a$ (dělí a beze zbytku),

$d \mid b$ (dělí b beze zbytku),

$d \mid c$ (dělí c beze zbytku).

Např. společným dělitelem čísel 6 a 9 je číslo 3, protože dělí obě z čísel beze zbytku.

Obecně platí, že každá dvě nenulová čísla mají společného dělitele. Dále platí, že každé číslo dělí sebe samo a číslo 1 dělí jakékoliv jiné číslo beze zbytku. Dělení číslem 0 není definováno, tzn. pokud bychom se pokusili dělit nulou, výsledek je neplatný a nelze jej určit.

3.2.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Největší společný dělitel je největší číslo, které dělí dvě nebo více čísel beze zbytku.

Obvykle bývá označován jako $\mathrm{NSD}(a, b)$, kde a, b jsou čísla, pro která hledáme největší společný dělitel.

K nalezení NSD lze využít několik metod, z nichž nejpoužívanější je prvočíselný rozklad (viz kapitola 3.1.2). Po provedení rozkladu všech daných čísel nalezneme prvočísla s nejmenším možným exponentem, která se vyskytují v obou rozkladech. Výsledkem součinu těchto prvočísel je NSD daných čísel.

Tento způsob hledání NSD si ukážeme na následujícím příkladu:

1. Provedeme prvočíselný rozklad čísel 84 a 60:

$$84 = 2^2 \cdot 3 \cdot 7,$$

$$60 = 2^2 \cdot 3 \cdot 5.$$

2. Nalezneme společná prvočísla s nejvyšším možným exponentem vyskytující se v obou rozkladech:

   $p = 2$, nejvyšší mocnina vyskytující se v obou rozkladech je 2^2,

   $p = 3$, nejvyšší mocnina vyskytující se v obou rozkladech je 3^1,

   $p = 5$, vyskytuje se pouze v rozkladu čísla 60,

   $p = 7$, vyskytuje se pouze v rozkladu čísla 84.

3. Největším společným dělitelem čísel 60 a 84 je tedy součin čísel $2^2 \cdot 3 = 12$.

Další velmi známou a efektivní metodou pro nalezení největšího společného dělitele je Euklidův algoritmus.

3.2.2 NESOUDĚLNOST

Pokud $\mathrm{NSD}(a, b) = 1$, neboli pokud neexistuje žádné celé číslo $k > 1$, které by bylo dělitelem obou čísel a, b, pak jsou čísla a, b nesoudělná.

Např. čísla 15 a 28 jsou nesoudělná, jelikož mají jen jednoho společného dělitele, jímž je číslo 1. Naopak čísla 15 a 25 jsou soudělná, jelikož je jejich společný dělitel číslo 5.

3.3 NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Nejmenší společný násobek (NSN) je nejmenší číslo, které je násobkem dvou nebo více daných čísel.

Nejmenší společný násobek dvou a více čísel lze nalézt pomocí prvočíselného rozkladu (viz kapitola 3.1.2). Po provedení rozkladu všech daných čísel určíme nejvyšší mocninu každého prvočísla vyskytující se ve všech rozkladech. Součin těchto prvočísel je nejmenším společným násobkem daných čísel. Tento způsob hledání NSN si ukážeme na následujícím příkladu:

1. Provedeme prvočíselný rozklad čísla 84 a 60:

$$84 = 2^2 \cdot 3 \cdot 7,$$

$$60 = 2^2 \cdot 3 \cdot 5.$$

2. Určíme nejvyšší mocniny každého prvočísla, které se vyskytuje alespoň v jednom z rozkladů:

   $p = 2$, nejvyšší mocnina vyskytující se v obou rozkladech je 2^2,

   $p = 3$, nejvyšší mocnina vyskytující se v obou rozkladech je 3^1,

   $p = 5$, nejvyšší mocnina vyskytující se v rozkladu čísla 60 je 5^1,

   $p = 7$, vyskytující se v rozkladu čísla 84 je 7^1.

3. Nejmenším společným násobkem čísel 60 a 84 je tedy součin čísel:

$$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 420.$$

3.4 EUKLIDŮV ALGORITMUS

Euklidův algoritmus je algoritmus, který využíváme k nalezení NSD dvou celých čísel.

Pro každé $a, b \in \mathbb{Z}, b \neq 0$ existují jednoznačně určené prvky $u, r \in \mathbb{Z}$ takové, že $a = b \cdot u + r, 0 \leq r < |b|$.

Euklidův algoritmus funguje následovně:

1. Dvě celá čísla, pro která hledáme NSD, označíme jako a, b, kde $b \neq 0$.
2. Číslo a dělíme číslem b a zbytek po dělení označíme jako r.
3. Pokud je $r = 0$, pak $\mathrm{NSD}(a, b) = b$ (poslední dělitel).
4. Pokud r není rovno 0, pokračujeme v dělení tak, že nyní číslo b dělíme zbytkem r.
5. Všechny kroky opakujeme, dokud nevyjde nulový zbytek.
6. NSD je poslední nenulový zbytek.

Hledání $\mathrm{NSD}(84, 60)$ pomocí Euklidova algoritmu si ukážeme na následujícím příkladu:

$$\mathrm{NSD}(84, 60) = 12$$

$$a = 84, b = 60$$

$a = u \cdot b + r$	$0 \leq r < \lvert b \rvert \rightarrow 24 < 60$
$84 = 1 \cdot 60 + 24$	$(84/60 = 1 \text{ zb.} 24)$
$b = u_2 \cdot r + r_2$	$0 \leq r_2 < \lvert r \rvert \rightarrow 12 < 24$
$60 = 2 \cdot 24 + 12$	$(60/24 = 2 \text{ zb.} 12)$
$r = u_3 \cdot r_2 + r_3$	$\mathbf{0 \leq r_3 < \lvert r_2 \rvert \rightarrow 0 < 12}$
$24 = 2 \cdot 12 + 0$	$(24/12 = 2 \text{ zb.} 0)$

3.5 BEZOUTOVA ROVNOST

Pro Bezoutovu rovnost platí, že pro libovolná celá čísla a, b existuje lineární kombinace s celými čísly x, y taková, že

$$ax + by = \mathrm{NSD}(a, b).$$

Pro nalezení takové lineární kombinace lze využít rozšířený Euklidův algoritmus.

3.6 KONGRUENCE

Kongruencí rozumíme vztah dvou celých čísel, která se liší o násobek jiného celého čísla, označovaného jako modulo.

Neboli dvě celá čísla a, b jsou kongruentní dle modulo m (kde m je přirozené číslo větší než 1) právě tehdy, když rozdíl $a - b$ je dělitelný m (tedy pokud čísla a, b mají stejný zbytek po dělení m), což lze zapsat jako: $a \equiv b \pmod m$.

Např. 17 je kongruentní s 5 (mod 6), to znamená, že pokud vydělíme $\frac{17}{6}$, zbytek po dělení bude stejný, jako když vydělíme $\frac{5}{6}$. Toto tvrzení ověříme následovně:

$a = 17;$
$b = 5$, podíl těchto čísel musí být dělitelný 6, tedy $17 - 5 = 12$, číslo 12 je násobkem čísla 6.

3.6.1 VLASTNOSTI KONGRUENCÍ

1. Symetrie: Pokud jsou dvě čísla kongruentní vzhledem k určitému modulu, pak můžeme prohodit postavení těchto čísel a výsledek zůstane stejný.
2. Tranzitivita: Pokud jsou dvě dvojice kongruentních čísel dle určitého modulo m a liší se o násobek daného modulu, potom jsou i tyto dvojice vzájemně kongruentní.
3. Reflexivita: Každé číslo je kongruentní samo se sebou vzhledem k libovolnému modulu.
4. Kongruence se chová podobně jako rovnost: Pokud jsou dvě čísla kongruentní vzhledem k modulu m, pak mohou být nahrazeny navzájem v jakémkoli výrazu, aniž by se změnil výsledek.
5. Kongruence je uzavřená vzhledem k základním aritmetickým operacím (sčítání, odčítání a násobení). Pokud jsou dvě čísla kongruentní, pak je kongruentní i jejich součet, rozdíl a součin.

3.6.2 ROZKLAD NA ZBYTKOVÉ TŘÍDY

Relace kongruence modulo m rozkládá množinu celých čísel na zbytkové třídy neboli celá čísla jsou rozdělena do tříd podle toho, jaký mají zbytek po dělení m. Každá třída obsahuje taková celá čísla, která mají při dělení m stejný zbytek.

Zbytkové třídy obvykle značíme jako Z_0 (množina celých čísel, která dají zbytek 0 po dělení m), Z_1 (množina celých čísel, která dají zbytek 1 po dělení m) … Z_{m-1} (množina celých čísel, která dají zbytek $m-1$ po dělení m).

Např. zbytkové třídy modulo 3 můžeme zapsat následovně:

$$Z_0 = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$Z_1 = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$Z_2 = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Podobně bychom mohli definovat zbytkové třídy modulo jakéhokoliv jiného přirozeného čísla.

Pokud vytvoříme množinu obsahující právě jedno číslo z daných zbytkových tříd, dostaneme tzv. úplnou soustavu zbytků (ÚSZ) modulo m, tedy:

Předpokládejme, že máme přirozené číslo m. Množina $\{r_1, r_2, \dots, r_m\}$ je ÚSZ modulo $m \Leftrightarrow \forall i, j$ platí $i \neq j \Rightarrow r_i \not\equiv r_j \pmod m$. Neboli žádná dvě čísla v této množině nemají stejný zbytek po dělení m.

Množinu $\{0, 1, \dots, m-1\}$ nazýváme fundamentální úplnou soustavou zbytků (FÚZS) modulo m. Tato množina obsahuje m různých čísel a každé z nich představuje zbytek po dělení libovolného celého čísla m. Tento soubor je "fundamentální", protože obsahuje základní zbytky modulo m.

3.6.3 SČÍTÁNÍ, NÁSOBENÍ A DĚLENÍ KONGRUENCÍ

Pokud máme dvě kongruence:

$$a \equiv b \pmod m \wedge c \equiv d \pmod m,$$

pak můžeme provést následující operace:

- Sčítání: Pokud sčítáme dvě kongruence, dostaneme:

$$a + c \equiv b + d \pmod m.$$

Tento vztah platí proto, že pokud je a kongruentní s b modulo m, pak existuje celé číslo k takové, že $a = b + k \cdot m$.

Stejně tak, pokud je c kongruentní s d dle modulo m, pak existuje celé číslo l takové, že $c = d + l \cdot m$. Potom můžeme součet $a + c$ napsat jako $(b + k \cdot m) + (d + l \cdot m)$, což po úpravě dává:

$$a + c = b + d + (k + l) \cdot m.$$

To znamená že $a + c$ je kongruentní s $b + d$ modulo m.

- Násobení: Pokud násobíme dvě kongruence, dostaneme:

$$a \cdot c = b \cdot d \pmod{m}.$$

Tento vztah platí proto, že pokud je a kongruentní s b modulo m, pak existuje celé číslo k takové, že $a = b + k \cdot m$. Stejně tomu je v případě, kdy je c kongruentní s d modulo m, pak existuje celé číslo l takové, že $c = d + l \cdot m$. Potom můžeme součin $a \cdot c$ napsat jako $(b + k \cdot m) \cdot (d + l \cdot m)$, což po úpravě dává:

$$a \cdot c = b \cdot d + (b \cdot l + d \cdot k + k \cdot l \cdot m) \cdot m.$$

To znamená, že $a \cdot c$ je kongruentní s $b \cdot d$ modulo m.

> *Pozn.* Výsledek obsahuje další člen $(b \cdot l + d \cdot k + k \cdot l \cdot m) \cdot m$, který zahrnuje zbytky po dělení. To je důvod, proč může být násobení kongruencí složitější než sčítání.

Je důležité poznamenat, že tento vztah platí pouze pro kongruence vzhledem ke stejnému modulu m. Pokud máme kongruence vzhledem k různým modulům, musíme nejprve najít společný modul, abychom je spolu mohli násobit.

- Dělení:

Pro operaci dělení neplatí obecný vztah podobný např. sčítání. Existují však speciální případy, kdy lze provést dělení kongruencí. Jedním z takových případů je, když b a m jsou nesoudělná čísla. V tomto případě lze z kongruencí $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ odvodit:

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{m}.$$

Toto platí pouze pokud existuje číslo x takové, že $a = bx$ a $c = dx$ modulo m.

Příklad 3.1

Nalezněte zbytek po dělení čísla 5^{13} číslem 8.

Řešení

$5^{13} \equiv ?\ (\mathrm{mod}\ 8)$

$5^{1} \equiv 5\ (\mathrm{mod}\ 8)\ /\ (\ )^{2}$

$5^{2} \equiv 25\ (\mathrm{mod}\ 8)$

$5^{2} \equiv 1\ (\mathrm{mod}\ 8)\ /\ (\ )^{6}$ → protože $25 \equiv 1\ (\mathrm{mod}\ 8)$

$5^{12} \equiv 1\ (\mathrm{mod}\ 8)$

$5^{12} \cdot 5^{1} \equiv 1 \cdot 5\ (\mathrm{mod}\ 8)$

$5^{13} \equiv 5\ (\mathrm{mod}\ 8)$

Zbytek po dělení čísla 5^{13} číslem 8 je $\mathbf{5}$.

Příklad 3.2

Dokažte, že číslo 8 dělí číslo $17^{15} + 15^{17}$.

Řešení

Příklad rozdělíme na 2 části:

$17^{15} \equiv ?\ (\mathrm{mod}\ 8)$	$15^{17} \equiv ?\ (\mathrm{mod}\ 8)$
$17 \equiv 1\ (\mathrm{mod}\ 8)$	$15 \equiv -1\ (\mathrm{mod}\ 8)$
$17^{15} \equiv \mathbf{1}\ (\mathrm{mod}\ 8)$	$15^{17} \equiv \mathbf{7}\ (\mathrm{mod}\ 8)$

$\Rightarrow 17^{15} + 15^{17} = 1 + 7 = 8 \equiv 8\ (\mathrm{mod}\ 8) = 0$

Zbytek po dělení čísla $17^{15} + 15^{17}$ číslem 8 je 0, to znamená, že **číslo $\mathbf{8}$ dělí číslo $\mathbf{17^{15} + 15^{17}}$**.

3.7 LINEÁRNÍ KONGRUENCE

Lineární kongruence je speciální typ kongruence, kterou lze zapsat jako $ax \equiv b \pmod m$, kde $a, b, m \in \mathbb{Z}, m \geq 2$ a x je neznámá proměnná.

Lineární kongruence může mít následující možnosti řešení:

1. Pokud $\mathrm{NSD}(a, m)$ není dělitelem b, neexistuje žádné řešení.
2. Pokud $\mathrm{NSD}(a, m) = 1$, existuje právě jedno řešení v (FÚSZ) a tedy i v libovolné (ÚSZ) existuje právě jedno řešení. V tomto případě můžeme k nalezení použít Rozšířený Euklidův algoritmus. Řešení bude vždy modulo m.
3. Pokud $\mathrm{NSD}(a, m) > 1$, existuje více řešení. V tomto případě můžeme rozdělit rovnici $ax \equiv b \pmod m$ na d rovnic $a'x \equiv b' \pmod m$, kde $d = \mathrm{NSD}(a, m)$, $a' = \frac{a}{d}, b' = \frac{b}{d}, m' = \frac{m}{d}$. Pak můžeme použít vztah pro počet řešení lineární kongruence, který zní: rovnice $a'x \equiv b' \pmod{m'}$ má d řešení modulo m', pokud b' dělí d. Tato řešení pak můžeme rozšířit na celá čísla modulo m.

Pokud víme, že má lineární kongruence $ax \equiv b \pmod m$ alespoň jedno řešení, můžeme použít vztah k nalezení všech řešení následovně:

Nejprve spočítáme $\mathrm{NSD}(a, m)$. Pokud $\mathrm{NSD}(a, m)$ nedělí b, pak rovnice nemá řešení. Pokud $\mathrm{NSD}(a, m)$ dělí b, potom existuje alespoň jedno řešení.

Najdeme inverzní prvek k číslu a modulo m. To znamená, že najdeme celé číslo x, pro které platí $ax \equiv 1 \pmod m$.

Nyní můžeme použít vztah dle [4] k nalezení všech řešení:

$$x = bx_0 \pmod m,$$

kde x_0 je libovolné řešení rovnice $ax \equiv b \pmod m$. Všechna řešení pak jsou dána vztahem:

$$x \equiv x_0 + km \pmod m,$$

kde k je celé číslo.

Příklad 3.3

Vyřešte následující lineární kongruenci:

$$5x \equiv 3 \pmod 8$$

Řešení

$\mathrm{NSD}(5, 8) = 1 \wedge 1 \mid 3$ ⇒ právě 1 řešení v (ÚSZ)

$5x \equiv 3 \pmod 8$

$5x \equiv -5 \pmod 8$

$x \equiv -1 \pmod 8$

$x \equiv 7 \pmod 8$

Všechna řešení v oboru celých čísel vyjádříme následovně: $x = 7 + 8k; k \in \mathbb{Z}$.

Příklad 3.4

Vyřešte následující lineární kongruenci:

$$6x \equiv 2 \pmod{10}$$

Řešení

$\mathrm{NSD}(6, 10) = 2 \wedge 2 \mid 2$ ⇒ právě 2 řešení v (ÚSZ)

$6x \equiv 2 \pmod{10}$

$6x \equiv 12 \pmod{10}$

$x \equiv 2 \pmod{10}$

Vyjádříme vzorec pro řešení v (ÚSZ) → $x = 2 + 10k; k = 0; 1$

$k = 0; x_1 = 2 + 10 \cdot 0$

$\boldsymbol{x_1 = 2}$

$k = 1; x_2 = 2 + 10 \cdot 1$

$\boldsymbol{x_2 = 12}$

Kongruence má 2 řešení v (FÚSZ) → $\boldsymbol{x_1 = 2}$

$\boldsymbol{x_2 = 12}$

3.8 EULEROVA FUNKCE

Eulerova funkce je funkce $\varphi(n)$ definovaná pro každé kladné celé číslo n takto:

$\varphi(n) =$ počet kladných celých čísel menších nebo rovných n, která jsou nesoudělná s n.

Např. pro $n = 10$, Eulerova funkce $\varphi(10)$ je rovna 4, protože existují 4 kladná celá čísla menší nebo rovná 10, která jsou nesoudělná s 10 (1, 3, 7 a 9).

3.8.1 EULEROVA VĚTA

Pokud jsou celá čísla a a n nesoudělná, pak platí Eulerova věta:

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

kde $\varphi(n)$ je Eulerova funkce z čísla n a "≡" označuje kongruenci modulo n.

3.8.2 MALÁ FERMATOVA VĚTA

Malá Fermatova věta je speciální případ Eulerovy věty, kdy n je prvočíslo. Pro každé prvočíslo p a celé číslo a, které není dělitelné p, platí:

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Tento vztah lze také zapsat jako:

$$a^{p} \equiv a \pmod{p}.$$

4 ŘEŠENÉ ÚLOHY NA DIOFANTICKÉ ROVNICE

V kapitolách 4.1 a 4.2 se zaměříme na řešení lineárních diofantických rovnic o dvou a třech neznámých. K řešení využijeme 5 různých metod, které jsou vypsané v Tab. 1. V kapitole 4.3 se zaměříme na řešení soustav lineárních diofantických rovnic.

Tab. 1: Druhy metod používaných pro řešení diofantických rovnic

Metoda	**Název metody**
a)	Metoda „pokus-omyl“
b)	Grafická metoda
c)	Metoda Euklidova algoritmu
d)	Metoda kongruence
e)	Metoda vyjádření členu s nejmenším koeficientem

4.1 ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC O DVOU NEZNÁMÝCH

Příklad 4.1

Najděte řešení pro rovnici:

$$9x + 27y = 23$$

Řešení

Lineární diofantická rovnice je řešitelná, pokud $\mathrm{NSD}(a, b) \mid c$, tedy $\mathrm{NSD}(9, 27) \mid 23$.

NSD nalezneme rozkladem na prvočísla:

$$\begin{array}{l} 27 = 3 \cdot 3 \cdot 3 \\ 3 \cdot 9 \\ \quad 3 \cdot 3 \end{array} \qquad\qquad \begin{array}{l} 9 = 3 \cdot 3 \\ 3 \cdot 3 \end{array}$$

$\mathrm{NSD}(9, 27) = 3 \cdot 3 = 9$, jelikož $9 \nmid 23$ rovnice nemá řešení.

Příklad 4.2

Najděte řešení pro rovnici:

$$3x + 7y = 1 \tag{4.1}$$

Řešení

Opět ověříme podmínku řešitelnosti, tedy $\mathrm{NSD}(7,3) \mid 1$.

NSD tentokrát nalezneme pomocí Euklidova algoritmu:

$$7 = 2 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

$\mathrm{NSD}(7,3) = 1$, jelikož $1 \mid 1 \Rightarrow$ rovnice je řešitelná.

Pro nalezení řešení takovéto rovnice existuje mnoho metod, my si na tomto příkladu demonstrujeme metodu „pokus-omyl" a grafickou metodu:

a) Metoda „pokus-omyl"

Metoda „pokus-omyl" není systematická a obvyklá metoda pro řešení těchto rovnic, nicméně v některých případech může být použita. Tuto metodu lze využít, pokud jsou hodnoty neznámých malé a jednoduše se dají zkoušet různé možnosti řešení. V takovém případě se pokoušíme dosazovat různé kombinace hodnot neznámých, dokud nenalezneme tu, která splňuje danou rovnici. Pro složitější rovnice a vyšší hodnoty je vhodnější použít spolehlivější způsoby řešení.

Pokračování řešení Příkladu 4.2

Zkusíme kombinaci např.: $\left.\begin{array}{r} x = -1 \\ y = 2 \end{array}\right\} 3 \cdot (-1) + 7 \cdot 2 \neq 1$

Zkusíme tedy jinou kombinaci, např.: $\left.\begin{array}{r} x = -2 \\ y = 1 \end{array}\right\} 3 \cdot (-2) + 7 \cdot 1 = 1$

Uspořádaná dvojice $[-2; 1]$ je tedy jedním z výsledků této rovnice. Jelikož známe jedno z řešení, dokážeme nalézt všechna zbývající řešení následovně:

Za předpokladu, že a, b jsou nesoudělná čísla a známe jedno z řešení rovnice, platí následující vztah dle [5] pro vyjádření všech řešení:

$$x = x_0 - b \cdot t\ ;\ t \in \mathbb{Z} \tag{4.2}$$

$$y = y_0 + a \cdot t\ ;\ t \in \mathbb{Z} \tag{4.3}$$

Dosadíme $[x; y] = [-2; 1]$ do rovnic (4.2) a (4.3), tím nalezneme všechna řešení:

$$x = -2 - 7t\ ;\ t \in \mathbb{Z}$$

$$y = 1 + 3t\ ;\ t \in \mathbb{Z}$$

Pozn. Za předpokladu, že $\mathrm{NSD}(a, b) > 1$ a známe jedno z řešení rovnice, platí následující vztah pro vyjádření všech řešení:

$$x = x_0 - \left(\frac{b}{\mathrm{NSD}(a,b)}\right) \cdot t \,;\; t \in \mathbb{Z} \tag{4.4}$$

$$y = y_0 + \left(\frac{a}{\mathrm{NSD}(a,b)}\right) \cdot t \,;\; t \in \mathbb{Z} \tag{4.5}$$

b) Grafická metoda

Grafická metoda, stejně jako metoda „pokus-omyl“, není obvyklá, protože ne vždy lze z grafu vyčíst dané řešení, ale přesto ji lze v některých případech použít.

Pro rovnici $ax + by = c$ postupujeme následovně:

1. Sestrojíme graf funkce ve tvaru $y = ax + b$.
2. Nalezneme bod grafu s celočíselnými souřadnicemi. Tento bod je jedním z řešení. Pokud žádný takový neexistuje, rovnice nemá řešení.
3. Pomocí nalezeného bodu najdeme všechna řešení dané rovnice.

Tento postup lze využít pro rovnice s dvěma neznámými, ale je obtížné ho využít pro rovnice s více než dvěma neznámými, a to z toho důvodu, že grafem vždy nemusí být přímka, ale např. i křivka. Pro složitější rovnice s více neznámými by bylo dokonce potřeba vytvořit vícerozměrný graf, což by bylo složité a zdlouhavé. V takovém případě by bylo opět vhodnější využít jiné metody řešení dané rovnice.

Pozn. V rámci této bakalářské práce používáme, k řešení příkladů grafickou metodou, aplikaci GeoGebra.

Pokračování řešení Příkladu 4.2

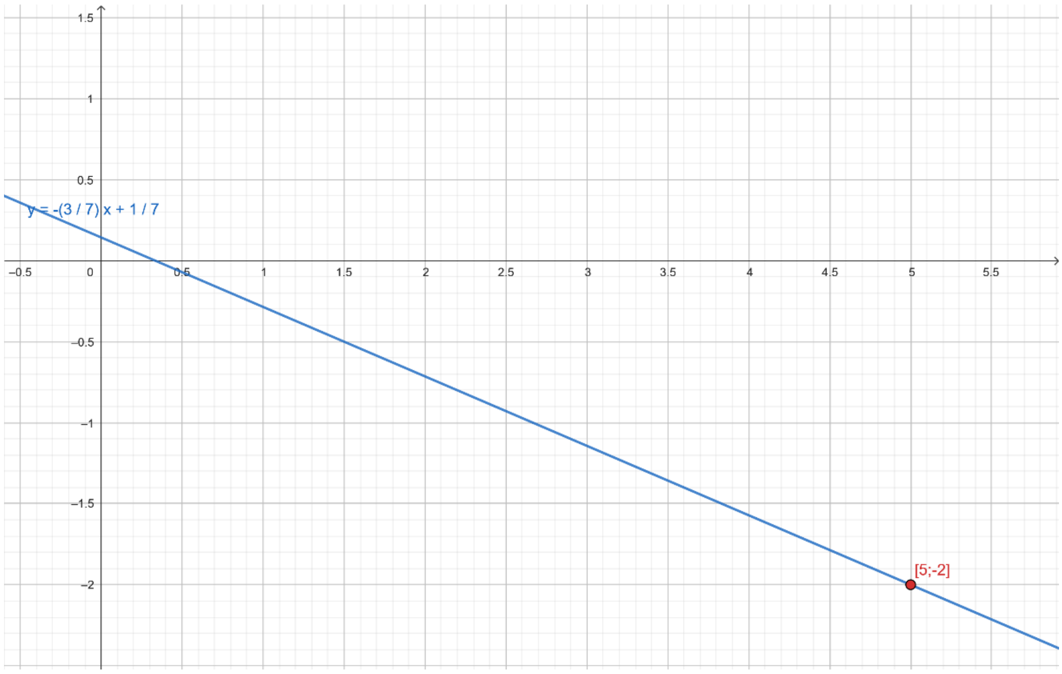
Rovnici (4.1) upravíme na tvar $y = ax + b$:

$$3x + 7y = 1$$

$$7y = 1 - 3x$$

$$y = -\frac{3}{7}x + \frac{1}{7}$$

Sestrojíme graf pro $y = -\frac{3}{7}x + \frac{1}{7}$ a pokusíme se nalézt bod grafu s celočíselnými souřadnicemi. Pokud takový bod existuje, je řešením rovnice.
Je jím např. $[\mathbf{5}; -\mathbf{2}]$, viz Graf 1:



Graf 1: Funkce y – Příklad 4.2

Všechna řešení získáme dosazením do rovnic (4.2) a (4.3):

$$x = 5 - 7t\ ;\ t \in \mathbb{Z}$$

$$y = -2 + 3t\ ;\ t \in \mathbb{Z}$$

Příklad 4.3

Najděte řešení pro rovnici:

$$21x + 15y = 3 \tag{4.6}$$

Řešení

Nejdříve ověříme podmínku řešitelnosti:

$\mathrm{NSD}(21, 15) \mid 3$

$\mathrm{NSD}(21, 15) = 3\ \wedge 3 \mid 3 \Rightarrow$ rovnice je řešitelná.

Pro řešení lze využít např. následující metody:

c) Metoda Euklidova algoritmu

Euklidův algoritmus je vhodný k nalezení NSD dvou celých čísel (viz kapitola 3.4), jeho rozšířenou verzi však lze využít k nalezení řešení diofantické rovnice následovně:

Pokračování řešení Příkladu 4.3

Euklidův algoritmus	**Úprava**
$21 = 1 \cdot 15 + 6$	$6 = 21 - 1 \cdot 15$
$15 = 2 \cdot 6 + 3$	$3 = 15 - 2 \cdot 6$
$6 = 2 \cdot 3 + 0$	$0 = 6 - 2 \cdot 3$

Následně využijeme Bezoutovu rovnost (viz kapitola 3.5):

$6 = 21 - 15$

$3 = 15 - 2 \cdot (21 - 15) = -2 \cdot 21 + 3 \cdot 15$

Jedním z řešení je $[-2; 3]$.

Po dosazení $[-2; 3]$ do rovnic (4.4) a (4.5) získáváme obecné řešení:

$$x = -2 - 5t\ ;\ t \in \mathbb{Z}$$

$$y = 3 + 7t\ ;\ t \in \mathbb{Z}$$

d) Metoda kongruence

Metoda kongruencí je často používána pro řešení diofantických rovnic. Tato metoda spočívá v nalezení řešení rovnice dle modulo nějakého čísla a poté využívá vlastností kongruencí pro nalezení řešení původní rovnice.

Převod diofantické rovnice ve tvaru $ax + by = c$ na kongruenci se provádí následovně:

$$ax + by = c$$

$$ax = c - by$$

$$ax \equiv c \pmod{b}$$

To znamená, že pokud jsou a, b, c a y dané, můžeme hledat řešení x pomocí kongruence $ax \equiv c \pmod{b}$.

Pokračování řešení Příkladu 4.3

Nejprve převedeme rovnici (4.6) na ekvivalentní rovnici využitím kongruencí modulo následovně:

$$21x \equiv 3 \pmod{15}$$

$$6x \equiv 18 \pmod{15} \quad /:3$$

$$2x \equiv 6 \pmod 5$$

$$x \equiv 3 \pmod 5$$

Takže x lze zapsat ve tvaru:

$$\boldsymbol{x = 3 + 5k}; k \in \mathbb{Z}$$

Nyní dosadíme x do původní rovnice:

$$21(3 + 5k) + 15y = 3$$

$$63 + 105k + 15y = 3$$

$$15y = -105k - 60$$

$$\boldsymbol{y = -7k - 4}; k \in \mathbb{Z}$$

Řešením je tedy $[\boldsymbol{3 + 5k};\ \boldsymbol{-4 - 7k}]; k \in \mathbb{Z}$

e) Metoda vyjádření členu s nejmenším koeficientem

Výhodou této redukční metody je, že nepotřebujeme žádné pokročilé matematické vědomosti, vystačíme si se znalostmi matematiky na úrovni základní školy. Tuto metodu považujeme za univerzální a lze ji využít i pro rovnice s více neznámými. Postup řešení si ukážeme na následujícím příkladu:

Pokračování Příkladu 4.3

Z rovnice (4.4) vyjádříme neznámou s nejmenším koeficientem, což je v našem případě y:

$$15y = 3 - 21x$$

$$y = \frac{3 - 21x}{15}$$

Zjednodušíme:

$$y = \frac{3 \cdot (1 - 7x)}{15} = \frac{1 - 2x - 5x}{5}$$

$$\boldsymbol{y = -x + \frac{1 - 2x}{5}}$$

Jelikož víme, že řešením musí být pouze celá čísla, i pro zlomek $\frac{1-2x}{5}$ musíme najít hodnotu x takovou, aby výsledkem bylo celé číslo. Je jím nejspíše $x = -2$, ale tvrzení ještě ověříme.

Využijeme substituci $u = \frac{1-2x}{5}$, tedy:

$$y = -x + u$$

Dále si vyjádříme x z $u = \frac{1-2x}{5}$:

$$u = \frac{1-2x}{5}$$

$$x = \frac{-5+1}{2} = \frac{-4u \cdot u + 1}{2} = -2u + \frac{1-u}{2}$$

⇒ např. po dosazení $u = 1$ vychází x jako celočíselné řešení, proto lze $u = 1$ považovat za výsledek. Nyní začneme zpětně dosazovat:

$u = 1$ dosadíme zpět do $x = \frac{-5u+1}{2}$:

$$x = \frac{-5 \cdot 1 + 1}{2} = -2$$

Řešením je tedy opravdu $x = -2$ a dosazením do původní rovnice dostáváme $y = 3$. Všechna řešení dostáváme dosazením do rovnic (4.4) a (4.5):

$$x = -2 - 5t\,;\ t \in \mathbb{Z}$$

$$y = 3 + 7t\,;\ t \in \mathbb{Z}$$

Příklad 4.4

Nalezněte řešení rovnice:

$$27x + 18y = 162 \tag{4.7}$$

Řešení

$\mathrm{NSD}(27, 18) = 9 \wedge 9 \mid 162$ ⇒ rovnice je řešitelná

Rovnici (4.7) vyřešíme dvěma způsoby:

a) Metoda „pokus-omyl“

V případě rovnice s vyššími koeficienty už je poměrně obtížné odhadnout celočíselné řešení.

Budeme postupovat následovně:

1. Vyzkoušíme do rovnice (4.7) dosadit $x = 1$:

$$27 \cdot 1 + 18y = 162$$

$$18y = 162 - 27$$

$$18y = 135 \quad /:18$$

$$y = 7{,}5$$

Jelikož pro řešení připouštíme pouze celočíselné výsledky, $y = 7{,}5$ není řešením rovnice a tedy ani $x = 1$ není řešením rovnice.

2. Vyzkoušíme dosadit do rovnice (4.7) $x = 2$:

$$27 \cdot 2 + 18y = 162$$

$$18y = 162 - 54$$

$$18y = 108 \quad /:18$$

$$\boldsymbol{y = 6}$$

Jelikož výsledek rovnice po dosazení $x = 2$ je celé číslo, uspořádanou dvojici [2; 6] můžeme považovat za jeden z výsledků.

Vyjádříme všechna řešení dosazením do rovnic (4.4) a (4.5):

$$x = 2 - 2t\,;\ t \in \mathbb{Z}$$

$$y = 6 + 3t\,;\ t \in \mathbb{Z}$$

b) Grafická metoda

Rovnici (4.7) upravíme na tvar $y = ax + b$:

$$27x + 18y = 162$$

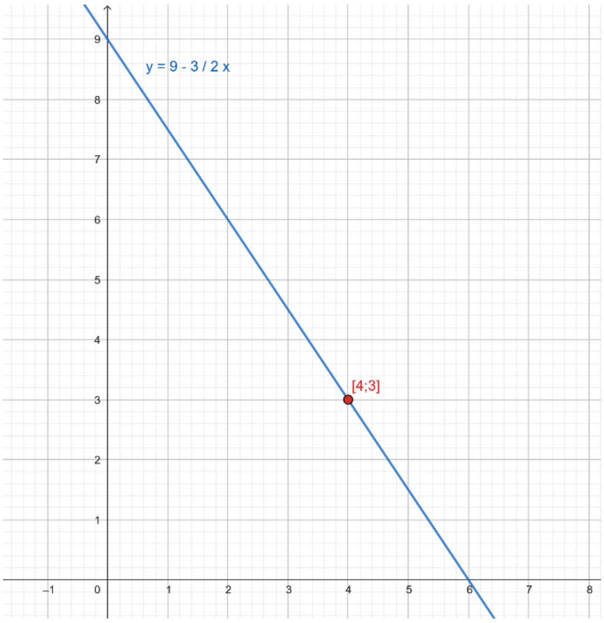
$$18y = 162 - 27x \quad /:18$$

$$y = \frac{162-27x}{18}$$

$$y = 9 - \frac{3}{2}x$$

Pokusíme se nalézt bod s celočíselnými souřadnicemi. Pokud takový bod existuje, bude jedním z řešení.

Je jím např. $[\mathbf{4}; \mathbf{3}]$, viz Graf 2:



Graf 2: Funkce y – Příklad 4.4

Po dosazení řešení do rovnic (4.4) a (4.5) získáváme všechna řešení:

$$x = 4 - 2t\ ;\ t \in \mathbb{Z}$$

$$y = 3 + 3t\ ;\ t \in \mathbb{Z}$$

Příklad 4.5

Nalezněte řešení rovnice:

$$492x + 308y = 84 \tag{4.8}$$

Řešení

$\mathrm{NSD}(492, 308) = 4 \wedge 4 \mid 84 \Rightarrow$ rovnice je řešitelná

Rovnici (4.8) vyřešíme opět dvěma způsoby:

c) Metoda Euklidova algoritmu

Euklidův algoritmus	**Úprava**
$492 = 1 \cdot 308 + 184$	$184 = 492 - 1 \cdot 308$
$308 = 1 \cdot 184 + 124$	$124 = 208 - 1 \cdot 184$
$184 = 1 \cdot 124 + 60$	$60 = 184 - 1 \cdot 124$
$124 = 2 \cdot 60 + 4$	$4 = 124 - 2 \cdot 60$
$60 = 15 \cdot 4 + 0$	$0 = 60 - 15 \cdot 4$

Využijeme Bezoutovu rovnost (viz kapitola 3.5):

$184 = 492 - 1 \cdot 308$

$124 = 308 - 1 \cdot 184 = 308 - 1 \cdot (492 - 1 \cdot 308) = 2 \cdot 308 - 1 \cdot 492$

$60 = 184 - 1 \cdot 124 = 492 - 1 \cdot 308 - 1 \cdot (2 \cdot 308 - 1 \cdot 492) = -3 \cdot 308 + 2 \cdot 492$

$4 = 124 - 2 \cdot 60 = 2 \cdot 308 - 1 \cdot 492 - 2 \cdot (-3 \cdot 308 + 2 \cdot 492) = 8 \cdot 308 - 5 \cdot 492$

Z rovnice $4 = 8 \cdot 308 - 5 \cdot 492$ plyne řešení $[\mathbf{-5}; \mathbf{8}]$.

Pravá strana původní rovnice se ale rovnala číslu 84. Proto rovnici $4 = 8 \cdot 308 - 5 \cdot 492$ vynásobíme číslem 21 a dostaneme:

$84 = 168 \cdot 308 - 105 \cdot 492 \Rightarrow [\mathbf{-105}; \mathbf{168}]$.

Vyjádříme obecné řešení dosazením do rovnic (4.4) a (4.5):

$$x = -105 - 77t;\ t \in \mathbb{Z}$$

$$y = 168 + 123t;\ t \in \mathbb{Z}$$

e) Metoda vyjádření členu s nejmenším koeficientem

Z rovnice (4.8) si vyjádříme y:

$$308y = 84 - 492x$$

$$y = \frac{84-492x}{308} \qquad (4.9)$$

Rovnici (4.9) dále upravíme:

$$y = \frac{21 - 123x}{77} = \frac{21 - 46x - 77x}{77} = -x + \frac{21 - 46x}{77}$$

Využijeme substituci $u = \frac{21-46x}{77}$, tedy:

$$y = -x + u \qquad (4.10)$$

Dále vyjádříme x z $u = \frac{21-46x}{77}$:

$$u = \frac{21-46x}{77}$$

$$21 - 46x = 77u$$

$$-46x = 77u - 21$$

$$x = \frac{-77u+21}{46} \tag{4.11}$$

Rovnici (4.11) dále upravíme:

$$x = \frac{-31u - 46u + 21}{46} = -u + \frac{21 - 31u}{46}$$

Využijeme substituci $s = \frac{21-31u}{46}$, tedy:

$$x = -u + s \tag{4.12}$$

Dále vyjádříme u z $s = \frac{21-31u}{46}$:

$$s = \frac{21-31u}{46}$$

$$21 - 31u = 46s$$

$$-31u = 46s - 21$$

$$u = \frac{21-46s}{31} \tag{4.13}$$

Rovnici (4.13) dále upravíme:

$$u = \frac{-15s - 31s + 21}{31} = -s + \frac{21 - 15s}{31}$$

Využijeme substituci $z = \frac{21-15s}{31}$, tedy:

$$u = -s + z \tag{4.14}$$

Dále vyjádříme s z $z = \frac{21-15s}{31}$:

$$z = \frac{21-15s}{31}$$

$$21 - 15s = 31z$$

$$-15s = 31z - 21$$

$$s = \frac{21-31z}{15} \tag{4.15}$$

Rovnici (4.15) dále upravíme:

$$s = \frac{21 - 30z - z}{15} = -2z + 1 + \frac{6 - z}{15}$$

⇒ např. po dosazení $z = 6$ vychází s jako celočíselné řešení, proto lze $z = 6$ považovat za výsledek. Nyní začneme zpětně dosazovat:

$z = 6$ dosadíme do rovnice (4.15), abychom získali hodnotu s:

$$s = \frac{21 - 31 \cdot 6}{15} = \mathbf{-11}$$

$z = 6$, $s = -11$ dosadíme do rovnice (4.14), abychom získali hodnotu u:

$$u = 11 + 6 = \mathbf{17}$$

$u = 17$, $s = -11$ dosadíme do rovnice (4.12), abychom získali hodnotu x:

$$x = -17 - 11 = \mathbf{-28}$$

$x = -28$, $u = 17$ dosadíme do rovnice (4.10), abychom získali hodnotu y:

$$y = 28 + 17 = \mathbf{45}$$

Po dosazení $[-28; 45]$ do rovnic (4.4) a (4.5) získáváme obecné řešení:

$$x = -28 - 77t\ ;\ t \in \mathbb{Z}$$

$$y = 45 + 123t\ ;\ t \in \mathbb{Z}$$

Cvičení 4.1

Najděte řešení rovnice:

$$125x + 225y = 113$$

4.2 ŘEŠENÍ LINEÁRNÍCH DIOFANTICKÝCH ROVNIC O TŘECH NEZNÁMÝCH

Příklad 4.6

Vyřešte rovnici:

$$3x + 6y + 9z = 45 \tag{4.16}$$

Řešení

Podobně jako v předchozích příkladech ověříme nejprve podmínku řešitelnosti:

$\mathrm{NSD}(3, 6, 9) = 3 \wedge 3 \mid 45 \Rightarrow$ rovnice je řešitelná

Pro řešení této rovnice použijeme dvě metody:

a) Metoda „pokus-omyl“

Stejně jako u diofantické rovnice se dvěma neznámými se budeme pokoušet odhadem nalézt takové metody neznámých, které budou splňovat danou rovnici.

V případě diofantické rovnice se třemi neznámými bude ale celý proces hledání řešení o něco složitější a zdlouhavější.

Pokračování řešení Příkladu 4.6

Upravíme rovnici (4.16):

$$3x + 6y + 9z = 45 \;\; /:3$$

$$x + 2y + 3z = 15$$

Pro přehlednost sestavíme tabulku (viz Tab. 2). V prvním sloupci se nachází konstanty, které dosazujeme za neznámou x. Ve druhém sloupci se vyskytuje upravená rovnice po dosazení konstanty x. Ve třetím sloupci najdeme hodnoty, které dosadíme za neznámou y a ve čtvrtém sloupci upravenou rovnici po takovém dosazení. V posledním, pátém sloupci, najdeme řešení pro neznámou z.

> *Pozn.* Ve třetím sloupci se snažíme volit hodnoty y tak, aby neznámá z následně vyšla jako celé číslo.

Tab. 2: Metoda „pokus-omyl" – Příklad 4.6

x	$x + 2y + 3z = 15$	y	$x + 2y + 3z = 15$	z
0	$2y + 3z = 15$	3	$3z = 9$	3
1	$2y + 3z = 14$	4	$3z = 6$	2
2	$2y + 3z = 13$	5	$3z = 3$	1
3	$2y + 3z = 12$	6	$3z = 0$	0
4	$2y + 3z = 11$	7	$3z = -3$	-1

Z tabulky lze vyčíst hned několik řešení, např. $[0; 3; 3], [1; 4; 2], [2; 5; 1]$ ...

Nyní se pokusíme nalézt všeobecné řešení. Vyjádříme jej parametricky, např. pro řešení $[0; 3; 3]$:

Parametrickou rovnici x vyjádříme:

$$x = 0 + t; \; t \in \mathbb{Z}$$

Parametrickou rovnici y vyjádříme:

$$y = 3 + t;\ t \in \mathbb{Z}$$

→ Jelikož z tabulky dedukujeme, že hodnota y vždy o 1 stoupá

Parametrickou rovnici z vyjádříme:

$$z = 3 - t;\ t \in \mathbb{Z}$$

→ Jelikož z tabulky dedukujeme, že hodnota z vždy o 1 klesá

Tedy: $x = t;\ t \in \mathbb{Z}$

$y = 3 + t;\ t \in \mathbb{Z}$

$z = 3 - t;\ t \in \mathbb{Z}$

c) Metoda Euklidova algoritmu

Pro řešení rovnice (4.16) budeme využívat upravený Euklidův algoritmus. Pro tento způsob řešení není potřeba zavádět žádné nové algoritmy či věty, ale vystačíme si pouze se znalostmi substituce, Euklidova algoritmu a NSD.

Řešení (dle [4] *str. 62)*

$$3x + 6y + 9z = 45$$

$\mathrm{NSD}(3, 6) = 3$, potom

$$3 \cdot (x + 2y) + 9z = 45$$

Zavedeme substituci $x + 2y = u$

$$3u + 9z = 45 \tag{4.17}$$

Rovnici (4.17) vyřešíme pomocí Euklidova algoritmu a řešení vyjádříme Bezoutovou rovností, kterou poté upravíme:

$$(4) \cdot 3 + (-1) \cdot 9 = 3\ \ /\cdot 15$$
$$(60) \cdot 3 + (-15) \cdot 9 = 45$$

Vyjádříme všechna řešení:

$$u = 60 + 9t$$

$$z = -15 - 3t$$

Nyní $z = -15 - 3t$ dosadíme do substituce a vyřešíme ji:

$$x + 2y = 60 + 9t$$

Dostáváme lineární diofantickou rovnici o 2 neznámých, kterou opět vyřešíme pomocí Euklidova algoritmu a vyjádříme Bezoutovou rovností:

$$1 \cdot (-1) + 2 \cdot 1 = 1 \ \ /\cdot (60 + 9t)$$

$$1 \cdot (-60 - 9t) + 2 \cdot (60 + 9t) = 60 + 9t$$

Vyjádření všech řešení je potom:

$$x = -60 - 9t + 2s;\ t, s \in \mathbb{Z}$$

$$y = 60 + 9t - s;\ t, s \in \mathbb{Z}$$

$$z = -15 - 3t;\ t \in \mathbb{Z}$$

Příklad 4.7

Vyřešte rovnici:

$$8x + 4y + 15z = 13 \tag{4.18}$$

Řešení

Nejdříve ověříme podmínku řešitelnosti:

$\mathrm{NSD}(8, 4, 15) = 1 \wedge 1 \mid 13 \Rightarrow$ rovnice je řešitelná

Vyřešíme ji metodou:

d) Metoda kongruence

Určíme NSD $n - 1$ koeficientů za předpokladu, že je toto číslo různé od 1, použijeme modul dán tímto NSD pro řešení kongruence o jedné neznámé. Poté postupně dopočítáme zbývající neznámé:

$$8x + 4y + 15z = 13 \qquad\qquad \mathrm{NSD}(8, 4) = 4$$

$$8x + 4y + 15z \equiv 13 \pmod 4$$

$$3z \equiv 21 \pmod 4$$

$$z \equiv 7 \pmod 4$$

$$z = 7 + 4t; t \in \mathbb{Z} \tag{4.19}$$

Rovnici (4.19) dosadíme do původní rovnice (4.18):

$$8x + 4y + 105 + 60t = 13$$

$$8x + 4y = -60t - 92 \quad /:4$$

$$2x + y = -15t - 23 \tag{4.20}$$

Nyní řešíme diofantickou rovnici o dvou neznámých:

$$2x + y \equiv -15t - 23 \ (\mathrm{mod}\ 2)$$

$$y \equiv t + 1 \ (\mathrm{mod}\ 2)$$

$$y = t + 1 + 2s;\ t, s \in \mathbb{Z} \tag{4.21}$$

Rovnici (4.21) dosadíme do (4.20):

$$2x + t + 1 + 2s = -15t - 23$$

$$2x = -16t - 24 - 2s$$

$$x = -8t - 12 - s$$

Všechna řešení tedy lze vyjádřit:

$$x = -12 - 8t - s;\ t, s \in \mathbb{Z}$$

$$y = 1 + t + 2s;\ t, s \in \mathbb{Z}$$

$$z = 7 + 4t;\ t \in \mathbb{Z}$$

Příklad 4.8

Vyřešte rovnici:

$$3x + 5y + 7z = 41 \tag{4.22}$$

Řešení

Nejdříve ověříme podmínku řešitelnosti:

$\mathrm{NSD}(3, 5, 7) = 1 \wedge 1 \mid 41 \Rightarrow$ rovnice je řešitelná

Vyřešíme ji metodou:

e) Metoda vyjádření členu s nejmenším koeficientem

Rovnici (4.22) upravíme a vyjádříme neznámou s nejmenším koeficientem:

$$3x = 41 - 5y - 7z$$

$$x = \frac{41-5y-7z}{3} \tag{4.23}$$

Rovnici (4.23) dále upravíme:

$$x = \frac{39+2-3y-2y-6z-z}{3} = 3-y-2z+\frac{2-2y-z}{3}$$

Použijeme substituci $s = \frac{2-2y-z}{3}$:

$$x = 3-y-2z+s$$

Dále vyjádříme y z $s = \frac{2-2y-z}{3}$:

$$s = \frac{2-2y-z}{3}$$

$$3s = 2-2y-z$$

$$3s-2+z = -2y$$

$$y = \frac{2-z-3s}{2} \tag{4.24}$$

Rovnici (4.24) dále upravíme:

$$y = \frac{2-z-2s-s}{2} = 1-s+\frac{-z-s}{2}$$

Využijeme substituci $k = \frac{-z+s}{2}$:

$$y = 1-s+k$$

Dále vyjádříme z z $k = \frac{-z+s}{2}$:

$$k = \frac{-z+s}{2}$$

$$2k = -z+s$$

$$2k-s = -z$$

$$z = s-2k$$

Nyní začneme zpětně dosazovat. Dosadíme $z = s-2k$ do rovnice (4.24):

$$y = \frac{2-s+2k-3s}{2}$$

$$y = 1-2s+k$$

Dosadíme $y = 1 - 2s + k$ a $z = s - 2k$ do rovnice (4.23):

$$x = \frac{41 - 5 + 10s - 5k - 7s + 14k}{3}$$

$$x = 12 + s + 3k$$

Všechna řešení tedy lze vyjádřit následovně:

$$x = 12 + s + 3k;\ s, k \in \mathbb{Z}$$

$$y = 1 - 2s + k;\ s, k \in \mathbb{Z}$$

$$z = s - 2k;\ s, k \in \mathbb{Z}$$

Cvičení 4.2

Najděte řešení rovnice:

$$4x + 8y + 9z = 23$$

4.3 ŘEŠENÍ SOUSTAV LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

K řešení soustav lineárních diofantických rovnic budeme využívat sčítací a dosazovací metody, které si představíme přímo na příkladech. Tyto metody můžeme znát již ze střední školy, jelikož se využívají při řešení soustav lineárních rovnic.

Z vlastností lineárních diofantických rovnic víme, že je nutné ověřit podmínku řešitelnosti. Pokud alespoň jedna z rovnic soustavy nebude řešitelná, pak celá soustava nemá řešení.

Příklad 4.9

Vyřešte soustavu:

$$4x + 2y - z = 5$$

$$8x - 2y = 3$$

Řešení

Nejprve ověříme podmínku řešitelnosti:

Soustava je řešitelná v případě, že jsou řešitelné obě rovnice:

$\mathrm{NSD}(4, 2, 1) = 1 \wedge 1 \mid 5$

$\mathrm{NSD}(8, 2) = 2 \wedge 2 \nmid 3$

Druhá rovnice nesplňuje podmínky řešitelnosti ⇒ soustava nemá řešení.

Příklad 4.10

Vyřešte soustavu:

$$2x + 3y - 4z = -10$$
$$x - 6y + 7z = 4$$

Řešení

Ověříme podmínky řešitelnosti:

$$\left.\begin{array}{l}\mathrm{NSD}(2,3,4) = 1 \wedge 1 \mid -10 \\ \mathrm{NSD}(1,6,7) = 1 \wedge 1 \mid 4\end{array}\right\}$$ ⇒ soustava má řešení a k jeho nalezení použijeme sčítací metodu:

A) Sčítací metoda

Obě rovnice sečteme, ale ještě předtím druhou rovnici vynásobíme číslem -2, abychom se „zbavili“ jedné neznámé:

$$2x + 3y - 4z = -10$$
$$x - 6y + 7z = 4 \quad / -2$$

$$2x + 3y - 4z = -10$$
$$-2x + 12y - 14z = -8$$

$$15y - 18z = -18$$

Po sečtení rovnic dostáváme lineární diofantickou rovnici o dvou neznámých. K řešení takové rovnice použijeme metodu **e) Metoda vyjádření členu s nejmenším koeficientem**:

$$15y = 18z - 18$$
$$y = \frac{18z - 18}{15} = z - 1 + \frac{3z - 3}{15}$$

Použijeme substituci $u = \frac{3z-3}{15}$, tedy:

$$y = z - 1 + u$$

Dále vyjádříme z z $u = \frac{3z-3}{15}$:

$$u = \frac{3z - 3}{15}$$
$$15u = 3z - 3$$
$$z = 5u + 1$$

Jedním z řešení je tedy $z = 5u + 1$, kde $u \in \mathbb{Z}$. Zpětným dosazením získáme všechna řešení:

$$x = u - 3;\ u \in \mathbb{Z}$$
$$y = 6u;\ u \in \mathbb{Z}$$
$$z = 5u + 1;\ u \in \mathbb{Z}$$

Příklad 4.11

Řešte soustavu:

$$3x - y - 2z = 5$$
$$2x - 4y + 3z = -7$$

Řešení

Nejprve opět ověříme řešitelnost:

$\left.\begin{array}{l}\mathrm{NSD}(3,1,2) = 1 \wedge 1 \mid 5 \\ \mathrm{NSD}(2,4,3) = 1 \wedge 1 \mid -7\end{array}\right\} \Rightarrow$ soustava je řešitelná. Při řešení použijeme dosazovací metodu:

B) Dosazovací metoda

Při řešení dosazovací metodou budeme postupovat následovně:

Vyjádříme si např. z první rovnice neznámou y a poté dosadíme do druhé:

$$3x - y - 2z = 5 \Rightarrow y = 3x - 2z - 5$$
$$2x - 4y + 3z = -7$$
$$\overline{}$$
$$2x - 4 \cdot (3x - 2z - 5) + 3z = -7$$
$$-10x + 11z = -27$$

Dostáváme diofantickou rovnici o dvou neznámých, kterou vyřešíme pomocí metody: **d) Metoda kongruence**

$$-10x + 11z \equiv -27 \pmod{10}$$
$$z \equiv 3 \pmod{10}$$
$$z = 3 + 10t;\ t \in \mathbb{Z}$$

Po zpětném dosazení získáváme všechna řešení:

$$x = 6 + 11t;\ t \in \mathbb{Z}$$
$$y = 7 + 13t;\ t \in \mathbb{Z}$$
$$z = 3 + 10t;\ t \in \mathbb{Z}$$

Cvičení 4.3

Najděte řešení soustavy:

$$3x + 5y + 6z = 4$$
$$2x - y + 4z = 7$$

5 SLOVNÍ ÚLOHY VEDOUCÍ NA DIOFANTICKÉ ROVNICE

Nyní, když za sebou máme objasnění řešení lineárních diofantických rovnic o dvou a třech neznámých, lineárních diofantických soustav a několik metod jejich řešení, je na čase zodpovědět otázku využití v praxi.

I když si to neuvědomujeme, diofantické rovnice řešíme v různých každodenních situacích. Jedním z příkladů může být hledání nejmenšího počtu mincí při placení v obchodě, řešení problémů v oblasti logistiky při hledání nejkratší cesty mezi dvěma body s omezením na maximální hmotnost nákladu, nebo dokonce i při vaření, kdy hledáme ideální poměr ingrediencí. Některé z těchto problémů lze řešit velmi jednoduše, bez jakýkoliv metod a algoritmů, dokonce i bez uvědomění si, že řešíme diofantickou rovnici. Avšak některé z nich je nutné převést do matematického jazyka a pro jejich řešení aplikovat různé metody vysvětlované v předchozích kapitolách.

Slovní úlohy budeme rozdělovat do podkapitol podle toho, na který druh diofantické rovnice povedou.

5.1 ŘEŠENÍ ÚLOH VEDOUCÍCH NA LINEÁRNÍ DIOFANTICKÉ ROVNICE O DVOU NEZNÁMÝCH

Příklad 5.1

Bořek se v rámci letního úklidu rozhodl pro vyklizení své sklepní kóje. V té nalezl mimo jiné i celkem 110 knih po svém dědečkovi. Rozhodl se je nevyhodit, ale převézt je k rodičům na chatu, avšak pro převoz má k dispozici pouze 2 velikosti kartonových krabic, přičemž menší z nich pojme 6 knih a ta větší 8 knih. Kolik Bořek využije menších a větších kartonových krabic?

Řešení

Krabice, které pojmou 6 knih označíme proměnou x a krabice, které pojmou 8 knih, označíme proměnou y.

Následně sestavíme lineární diofantickou rovnici o dvou neznámých.

$$6x + 8y = 110 \tag{5.1}$$

Ověříme podmínku řešitelnosti:

$\mathrm{NSD}(6, 8) = 2 \wedge 2 \mid 110 \Rightarrow$ rovnice je řešitelná a vyřešíme ji všemi pěti metodami z Tab.1:

a) Metoda „pokus-omyl“

Do rovnice (5.1) za neznámou x budeme postupně dosazovat celočíselné hodnoty $1 - 18$ (1 je minimální počet menších krabic a 18 je maximální počet). Za správný výsledek budeme považovat celočíselné hodnoty neznámé y. Pro přehlednost sestavíme tabulku (viz Tab. 3):

Tab. 3: Metoda „pokus-omyl“ – Příklad 5.1

x	$6x + 8y = 110$	y
1	$8y = 104$	13
2	$8y = 98$	12,25
3	$8y = 92$	11,5
4	$8y = 86$	10,75
5	$8y = 80$	10
6	$8y = 74$	9,25
7	$8y = 68$	8,5
8	$8y = 62$	7,75
9	$8y = 54$	7
$\vdots$	$\vdots$	$\vdots$
18	$8y = 2$	0,25

Z tabulky lze vyčíst hned několik řešení, např. $[1; 13]$; $[5; 10]$; $[9; 7]$. Podle toho, jak se tabulka vyvíjí předpokládejme, že další řešení by mohla být $[13; 4]$; $[17; 1]$.

Výsledná odpověď:

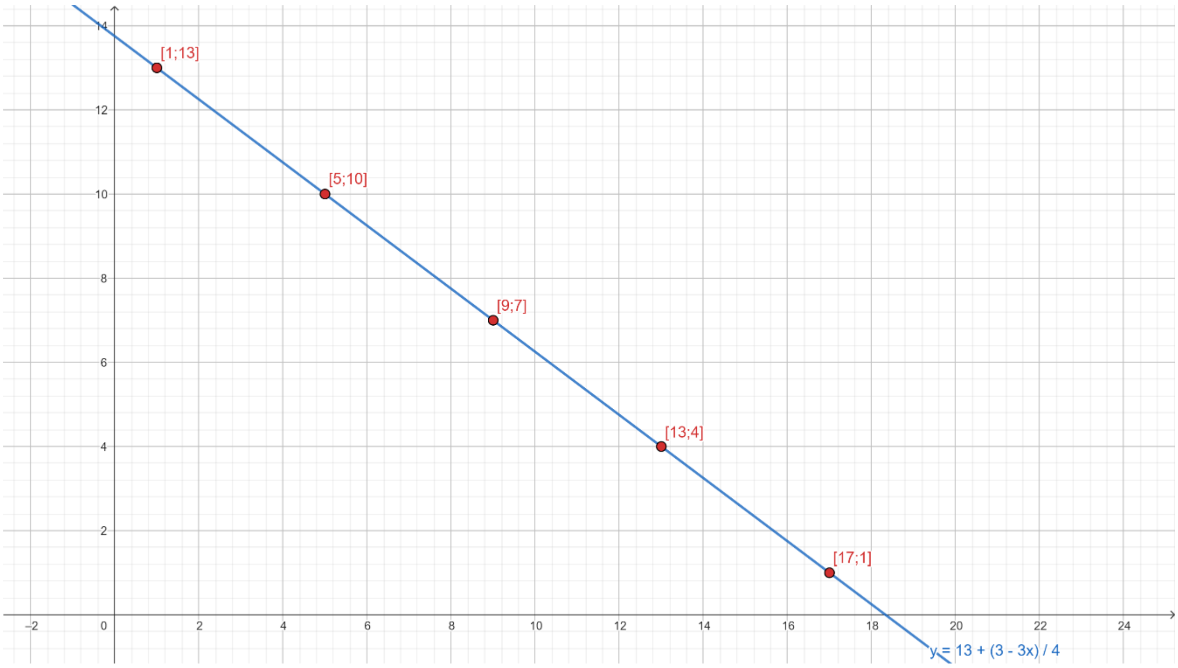
Bořek má 5 možností, jak dané krabice využít, např. všech 110 knih může odvést k rodičům v 1 menší krabici a 13 větších.

b) Grafická metoda

Rovnici (5.1) upravíme na tvar $y = ax + b$:

$$6x + 8y = 110$$
$$8y = 110 - 6x$$
$$y = \frac{104 + 6 - 6x}{8} = 13 + \frac{3 - 3x}{4}$$

Pokusíme se nalézt body s celočíselnými souřadnicemi. Pokud takové body existují, jsou řešením. Jelikož nejsou přípustná záporná řešení, za výsledek považujeme pouze 5 bodů znázorněných v Grafu 3. Jsou to body: $[1; 13]$; $[5; 10]$; $[9; 7]$; $[13; 4]$; $[17; 1]$.



Graf 3: Funkce y – Příklad 5.1

Výsledná odpověď:

Bořek má 5 možností, jak dané krabice využít, např. všech 110 knih může odvést k rodičům v 9 menších krabicích a 7 větších.

c) Metoda Euklidova algoritmu

Euklidův algoritmus	**Úprava**	
$8 = 1 \cdot 6 + 2$	$2 = 8 - 1 \cdot 6$	(5.2)
$6 = 2 \cdot 3 + 0$		

Jelikož se pravá strana původní rovnice (5.1) rovná 110, musíme rovnici (5.2) vynásobit 55:

$$55 \cdot 8 - 55 \cdot 6 = 110$$

Všeobecným řešením je tedy:

$$x = -55 - 4t;\ t \in \mathbb{Z}$$
$$y = 55 + 3t;\ t \in \mathbb{Z}$$

Všechna tato řešení ovšem nesplňují zadání, jelikož výsledek nesmí být záporné číslo (počet krabic nemůže být záporný), proto musíme parametr t omezit intervalem $t \in \langle -18; -14 \rangle$, tedy $t \in \{-18; -17; -16; -15; -14\}$.

Výsledná odpověď:

Bořek má 5 možností, jak dané krabice využít, např. všech 110 knih může odvést k rodičům v 13 menších krabicích a 4 větších.

d) Metoda kongruence

$$6x + 8y \equiv 110 \text{ (mod 6)}$$
$$2y \equiv 2 \text{ (mod 6)}$$
$$y = 1 + 6t$$

Do rovnice (5.1) dosadíme $y = 1 + 6t$:

$$6x + 8 + 48t = 110$$
$$6x = 102 - 48t$$
$$x = 17 - 8t$$

Po zpětném dosazení získáváme všechna řešení:

$$x = 17 - 4t;\ t \in \mathbb{Z}$$
$$y = 1 + 3t;\ t \in \mathbb{Z}$$

Všechna tato řešení ovšem opět nesplňují zadání, jelikož výsledek ani zde nesmí být záporné číslo, proto musíme parametr t omezit intervalem $t \in \langle 0; 4 \rangle$, tedy $t \in \{0; 1; 2; 3; 4\}$.

Výsledná odpověď:

Bořek má 5 možností, jak dané krabice využít, např. všech 110 knih může odvést k rodičům v 17 menších krabicích a 1 větší.

e) Metoda vyjádření členu s nejmenším koeficientem

Z rovnice (5.1) si vyjádříme x:

$$6x = 110 - 8y$$
$$x = \frac{108 + 2 - 2y - 6y}{6} = 18 - y + \frac{1 - y}{3}$$

Využijeme substituci $u = \frac{1-y}{3}$:

$$x = 18 - y + u \tag{5.3}$$

Dále vyjádříme y:

$$u = \frac{1 - y}{3}$$
$$y = 1 - 3u$$

Do rovnice (5.3) dosadíme $y = 1 - 6u$:

$$x = 18 - 1 + 3u + u$$
$$x = 4u + 17$$

Tím získáváme:

$$x = 4u + 17;\ u \in \mathbb{Z}$$
$$y = 1 - 3u;\ u \in \mathbb{Z}$$

Všechna tato řešení, ale nejsou řešením úlohy (např. pro $u = 1 \rightarrow y = -2$). Proto musíme parametr u omezit $u \in \langle -4; 0 \rangle$, tedy $u \in \{-4; -3; -2; -1; 0\}$.

Výsledná odpověď:

Bořek má 5 možností, jak dané krabice využít, např. všech 110 knih může odvést k rodičům v 5 menších krabicích a 10 větších.

Příklad 5.2

Restaurace v centru Plzně se rozhodla, že v poledních hodinách bude nabízet zvýhodněné jídelní menu. Zákazník si každý den může vybrat z 5 hlavních jídel a 2 druhů polévek. Za celé menu (hlavní jídlo + polévka) zákazník zaplatí 112 Kč, přičemž samotná polévka zákazníka vyjde na 19 Kč. Kolik restaurace prodala celých menu a kolik samostatných polévek během jednoho poledne, když celková tržba byla 17 750 Kč?

Řešení

Počet samostatně prodaných polévek označíme neznámou x a počet celých menu označíme neznámou y.

Následně sestavíme lineární diofantickou rovnici o dvou neznámých.

$$19x + 112y = 17750 \tag{5.4}$$

Ověříme podmínku řešitelnosti:

$\mathrm{NSD}(19, 112) = 1 \wedge 1 \mid 17750 \Rightarrow$ rovnice je řešitelná

Použijeme metodu:

d) Metoda kongruence

$$19x + 112y \equiv 17750 \text{ (mod 19)}$$
$$17y \equiv 4 \text{ (mod 19)}$$
$$-2y \equiv 4 \text{ (mod 19)}$$
$$y \equiv -2 \text{ (mod 19)}$$
$$y \equiv 17 \text{ (mod 19)}$$
$$y = 17 + 19t$$

Do rovnice (5.4) zpětně dosadíme $y = 17 + 19t$:

$$19x + 1904 + 2128t = 17750$$
$$19x = -2128t + 15846$$
$$x = -112t + 834$$

Všeobecné řešení lze zapsat následovně:

$$x = 834 - 112t; t \in \mathbb{Z}$$
$$y = 17 + 19t; t \in \mathbb{Z}$$

Ovšem parametr t musíme omezit na interval $t \in \langle 0; 7\rangle$, jelikož výsledek nemůže být záporné číslo. Pro přehlednost zapíšeme všechna přípustná řešení do tabulky (viz Tab. 4). V prvním sloupci jsou přípustné hodnoty parametru t, v druhém sloupci počet samostatně zakoupených polévek a ve třetím sloupci počet zakoupených celých menu.

Tab. 4: Metoda kongruence – Příklad 5.2

t	Polévka	Celé menu
0	834	17
1	722	36
2	610	55
3	498	74
4	386	93
5	274	112
6	162	131
7	50	150

Restaurace tedy mohla prodat polévky a menu v 8 různých kombinacích.

Výsledná odpověď:

Restaurace během jednoho odpoledne prodala např. 50 samostatných polévek a 150 celých menu.

Cvičení 5.1

Vyřešte následující slovní úlohu:

Ondřej vyprodukoval za loňský rok 23,55 litrů domácí pálenky. Pálenku rozlil do dvou typů lahví. První typ měl objem 550 ml a druhý typ 800 ml. Do kolika 550 ml a 800 ml lahví rozlil celý objem pálenky?

5.2 ŘEŠENÍ ÚLOH VEDOUCÍCH NA LINEÁRNÍ DIOFANTICKÉ ROVNICE O TŘECH A VÍCE NEZNÁMÝCH

Příklad 5.3

Maminka poslala Aničku do obchodu, aby nakoupila ovoce a zeleninu. U pokladny zjistila, že nákup stojí 87 Kč. Anička má v peněžence k dispozici mince v hodnotě 1 Kč, 2 Kč, 5 Kč, 10 Kč, 20 Kč. Jaký je nejmenší počet mincí, který může Anička použít?

Řešení

Můžeme sestavit rovnici:

$$1x + 2y + 5z + 10v + 20w = 87, \tag{5.5}$$

kde neznámé x, y, z, v, w představují počet jednotlivých mincí, tedy:

x .... počet 1 Kč mincí,

y .... počet 2 Kč mincí,

z .... počet 5 Kč mincí,

v .... počet 10 Kč mincí,

w .... počet 20 Kč mincí.

Postupně budeme dosazovat počty jednotlivých mincí do rovnice. Začneme od mince s nejvyšší hodnotou, tedy s neznámou w. Maximálně tuto neznámou můžeme použít čtyřikrát, jelikož $4 \cdot 20 = 80 < 87$; dosadíme $w = 4$ do rovnice (5.5):

$$1x + 2y + 5z + 10v + 20 \cdot 4 = 87$$

$$1x + 2y + 5z + 10v = 7 \tag{5.6}$$

Potom co budou použity čtyři dvacetikoruny, zbývá doplatit 7 Kč.

Pokračujeme k neznámé v. Ta nemůže být použita ani jedna, jelikož $10 > 7$, tudíž by byla částka přeplacena. Dosadíme $v = 0$ do rovnice (5.6):

$$1x + 2y + 5z + 10 \cdot 0 = 7$$

$$1x + 2y + 5z = 7 \tag{5.7}$$

Stále tedy zbývá doplatit 7 Kč.

Pokračujeme k neznámé z. Tu použijeme právě jednou, jelikož $1 \cdot 5 = 5 < 7$; dosadíme $z = 1$ do rovnice (5.7):

$$1x + 2y + 5 \cdot 1 = 7$$

$$1x + 2y = 2 \tag{5.8}$$

Zbývá doplatit 2 Kč, tudíž neznámou y použijeme opět právě jednou, a tím pokryjeme celou částku. Dosadíme tedy $y = 1$ do rovnice (5.8):

$$1x + 2 \cdot 1 = 2$$

$$x = 0$$

Celkem tedy potřebujeme pro zaplacení částky 87 Kč 6 mincí, tj. 4 dvacetikoruny, 1 pětikorunu a 1 dvoukorunu.

Výsledná odpověď:

Nejmenší počet mincí, který může Anička použít je 6 mincí (4 dvacetikoruny, 1 pětikoruna a 1 dvoukoruna).

Příklad 5.4

Babička a její vnuk sklidili svou úrodu polních okurek. Babička šla poté vařit oběd a vnukovi dala za úkol, aby okurky přepočítal. Vnuk spočítal, že jich nasbírali celkem 267 kusů, avšak dědeček 2 z nich snědl. Po obědě šla babička zbylé okurky zavařit, přičemž k dispozici měla 3 druhy zavařovacích sklenic. Do velké sklenice se vešlo 24 okurek, do střední 15 okurek a do malé sklenice 11 okurek. Kolik, kterých sklenic při zavařování babička použila?

Řešení

Nejprve si ke všem druhům sklenic přiřadíme neznámé následovně:

x .... počet velkých sklenic,

y .... počet středních sklenic,

z .... počet malých sklenic.

Nyní můžeme sestavit rovnici:

$$24x + 15y + 11z = 265 \tag{5.9}$$

A poté ověříme podmínky:

$\mathrm{NSD}(24, 15, 11) = 1 \wedge 1 \mid 265 \Rightarrow$ úloha je řešitelná

Rovnici vyřešíme metodou:

d) Metoda kongruence

$\mathrm{NSD}(24, 15) = 3$

$$24x + 15y + 11z \equiv 265 \pmod 3$$
$$11z \equiv 265 \pmod 3$$
$$-1z \equiv 1 \pmod 3$$
$$z \equiv -1 \pmod 3$$
$$z = -1 + 3t$$

Do rovnice (5.9) dosadíme $z = -1 + 3t$:

$$24x + 15y - 11 + 33t = 265$$
$$24x + 15y = 276 - 33t; t \in \mathbb{Z}$$

Dostáváme lineární diofantickou rovnici o dvou neznámých, kterou budeme opět řešit metodou kongruence:

$$24x + 15y \equiv 276 - 33t \pmod{24}$$
$$15y \equiv 12 - 9t \pmod{24} \ /: 3$$
$$5y \equiv 4 - 3t \pmod 8$$
$$-3y \equiv 12 - 3t \pmod 8 \ \ /: (-3)$$
$$y \equiv t - 4 \pmod 8$$
$$y = -4 + t + 8s$$

Do původní rovnice (5.9) dosadíme $y = -4 + t + 8s$ a vyjádříme x:

$$24x - 60 + 15t + 120s - 11 + 33t = 265$$
$$24x = -48t - 120s + 336$$
$$x = 14 - 2t - 5s$$

Následně vyjádříme všechna řešení:

$$x = 14 - 2t - 5s; t, s \in \mathbb{Z}$$
$$y = -4 + t + 8s; t, s \in \mathbb{Z}$$
$$z = -1 + 3t; t, s \in \mathbb{Z}$$

Musíme nalézt parametry s, t tak, aby následná řešení dávaly smysl:

$$x \geq 0 \wedge y \geq 0 \wedge z \geq 0.$$

I.

$$14 - 2t - 5s \geq 0$$
$$-2t \geq 5s - 14$$
$$t \leq 7 - \frac{5}{2}s$$

II.

$$-4 + t + 8s \geq 0$$
$$t \geq 4 - 8s$$

III.

$$-1 + 3t \geq 0$$
$$3t \geq 1$$
$$t \geq \frac{1}{3}$$

Možná řešení pro parametry t, s, která odpovídají podmínkám, zaneseme do tabulky:

Tab. 5: Metoda kongruence – Příklad 5.4

t	s	x	y	z
1	1	7	5	2
1	2	2	13	2
2	1	5	6	5
2	2	0	14	5
3	1	3	7	8

Babička může při zavařování použít 5 různých kombinací sklenic.

Výsledná odpověď:

Babička pro zavařování okurek může využít např. 5 malých, 6 středních a 5 velkých zavařovacích sklenic.

Cvičení 5.2

Vyřešte následující slovní úlohu:

Dominik se rozhodl, že si po celý rok bude dávat na stranu peníze a bude šetřit na novou stavebnici Lego Star Wars, která stojí 15 999 Kč. Od rodičů dostává každý měsíc 1000 Kč a od babičky 200 Kč. Zbytek peněz by již měl mít našetřený v kasičce, kde má k dispozici mince v hodnotě 1 Kč, 2 Kč, 5 Kč, 10 Kč, 20 Kč a 50 Kč. Jaký nejmenší počet mincí může mít Dominik v kasičce, aby si na konci roku mohl koupit vysněnou stavebnici?

5.3 ŘEŠENÍ ÚLOH VEDOUCÍCH NA SOUSTAVU LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

Příklad 5.5

František dostal od babičky 100 Kč k svátku. Při cestě domů se rozhodl, že se zastaví v cukrárně a dá si zmrzlinový pohár, který ho stál 53 Kč. Při platbě mu obsluha cukrárny vrátila 20 mincí v hodnotě 1 Kč, 2 Kč a 5 Kč. Kolika mincemi daných hodnot František disponuje?

Řešení

Pro jednotlivé mince zavedeme značení:

x .... 1 Kč,

y .... 2 Kč,

z .... 5 Kč.

Úloha vede na soustavu rovnic. Jednotlivé rovnice sestavíme následovně:

$$1x + 2y + 5z = 47$$
$$x + y + z = 20$$

Nyní ověříme řešitelnost soustavy:

$$\left.\begin{array}{l}\mathrm{NSD}(1,2,5) = 1 \wedge 1 \mid 47 \\ \mathrm{NSD}(1,1,1) = 1 \wedge 1 \mid 20\end{array}\right\} \Rightarrow \text{soustava je řešitelná}$$

Při řešení využijeme dosazovací metodu:

$$1x + 2y + 5z = 47$$
$$x + y + z = 20 \rightarrow x = 20 - y - z$$

$$20 - y - z + 2y + 5z = 47$$

$$y + 4z = 27$$
$$y = 27 - 4z$$

z nahradíme parametrem $t; t \in \mathbb{Z}$, tedy $z = t$.

Nyní zpětně dosadíme $y = 27 - 4t$ do $x = 20 - y - z$.

$$x = 20 - y - z$$
$$x = -7 + 3t$$

Všechna řešení jsou ve tvaru:

$$x = -7 + 3t; t \in \mathbb{Z}$$
$$y = 27 - 4t; t \in \mathbb{Z}$$
$$z = t; t \in \mathbb{Z}$$

Parametr t musíme omezit, jelikož je pro nás nepřípustný záporný výsledek (mincí nemůže být záporné množství), tedy $t \in \mathbb{Z}; t \in \langle 3; 6 \rangle$. Úloha má 4 různá řešení.

Výsledná odpověď:

František disponuje např. dvěma 1 Kč, patnácti 2 Kč a třemi 5 Kč.

Příklad 5.6

Na stole stojí 3 nádoby, přičemž v každé je neznámý počet kuliček. Pokud do první nádoby přidáme 10 kuliček, pak ve druhé a třetí bude dohromady o polovinu méně kuliček než v první nádobě. Pokud ale do první nádoby přidáme 20 kuliček, pak bude ve druhé a třetí nádobě dohromady třetinové množství kuliček první nádoby. Kolik kuliček bylo v každé z nádob původně?

Řešení

Nejprve si zavedeme značení:

První nádobu označíme neznámou x, druhou nádobu neznámou y a třetí nádobu neznámou z.

Úloha vede na soustavu rovnic. Jednotlivé rovnice sestavíme dle zadání:

$$x + 10 = 2 \cdot (y + z)$$
$$x + 20 = 3 \cdot (y + z)$$

Provedeme úpravu:

$$x - 2y - 2z = -10$$
$$x - 3y - 3z = -20$$

Nyní můžeme ověřit řešitelnost soustavy:

$\left.\begin{array}{l} \mathrm{NSD}(1,2,2) = 1 \wedge 1 \mid -10 \\ \mathrm{NSD}(1,3,3) = 1 \wedge 1 \mid -20 \end{array}\right\}$ ⇒ soustava je řešitelná a při řešení využijeme sčítací metodu:

$$x - 2y - 2z = -10$$
$$x - 3y - 3z = -20$$

$$y + z = 10$$
$$y = 10 - z$$

z nahradíme parametrem $t; t \in \mathbb{Z}$, tedy $z = t$.

Nyní zpětně dosadíme $y = 10 - t$ do jedné z původní rovnic:

$$x - 20 + 2t - 2t = -10$$
$$x = 10$$

Všechna řešení jsou ve tvaru:

$$x = 10$$
$$y = 10 - t; t \in \mathbb{Z}$$
$$z = t; t \in \mathbb{Z}$$

Parametr t opět musíme omezit, jelikož je pro nás nepřípustný záporný výsledek (kuliček nemůže být záporné množství), tedy $t \in \mathbb{Z}; t \in \langle 0; 9 \rangle$.

Úloha má 10 různých řešení, ale v první nádobě bude při každém řešení 10 kuliček, jelikož neznámá x není závislá na parametru t.

Výsledná odpověď:

Původně bylo např. v první nádobě 10 kuliček, v druhé nádobě 9 kuliček a ve třetí 1 kulička.

Cvičení 5.3

Vyřešte následující slovní úlohu:

Otec je o 24 let starší než jeho syn. Za 6 let bude otec dvakrát starší než jeho syn. Jaký je věk otce a jaký syna?

ZÁVĚR

Cílem bakalářské práce bylo představit čtenářům diofantické rovnice a ukázat několik konkrétních úloh, které s nimi souvisí.

V bakalářské práci jsme prozkoumali některé základní pojmy, typy a metody řešení diofantických rovnic. V první kapitole jsme se zabývali historickým vývojem této oblasti matematiky, který sahá až do velkolepé Alexandrie. V kontextu historie jsme se zaměřili převážně na slavného Diofanta, po kterém jsou tyto rovnice pojmenovány.

V druhé kapitole jsme představili některé typy diofantických rovnic, jako jsou například lineární a kvadratické rovnice.

V třetí kapitole jsme definovali základní pojmy související s diofantickými rovnicemi, jsou jimi např. největší společný dělitel, nejmenší společný násobek, či kongruence. Vysvětlili jsme, jak lze tyto pojmy početně využít, jelikož jsme je následně využívali při řešení diofantických rovnic.

V čtvrté kapitole jsme se zaměřili na konkrétní příklady lineárních diofantických rovnic o dvou a třech neznámých a soustav lineárních diofantických rovnic. Pokud to bylo možné, ukázali jsme, jak lze tyto rovnice řešit pomocí 5 metod, tj. metoda „pokus-omyl“, grafická metoda, metoda Euklidova algoritmu, metoda kongruence a metoda vyjádření členu s nejmenším koeficientem.

V páté kapitole jsme se pak věnovali slovním úlohám, které vedou na lineární diofantické rovnice o dvou, třech neznámých a jejich soustav. Řešení jsme prováděli opět pomocí 5 již zmiňovaných metod.

V průběhu práce jsme se naučili, jak efektivně řešit různé typy diofantických rovnic a jak tyto znalosti aplikovat na praktické úlohy. Lze shrnout, že práce na téma úlohy s diofantickými rovnicemi nám umožnila prohloubit naše znalosti v této oblasti matematiky a představit nám mnoho zajímavých problémů, které lze řešit pomocí těchto rovnic.

Celkově můžeme konstatovat, že jsme splnili cíl této bakalářské práce a případné pokračování by se mohlo soustředit na řešení dalších typů diofantických rovnic pomocí většího množství metod, či na otestování znalostí studentů základních a středních škol právě na téma diofantické rovnice.

RESUMÉ

Tato bakalářská práce se zabývá úlohami s diofantickými rovnicemi. Celkově je práce členěna do 5 hlavních kapitol. První kapitola se zaměřuje na historický vývoj této oblasti matematiky. Druhá kapitola seznamuje čtenáře se základními typy diofantických rovnic. Následně třetí kapitola představuje základní pojmy a definice, jež jsou potřebné k pochopení této problematiky. V posledních dvou kapitolách jsou využívány nejvýznamnější metody a techniky, které se používají k hledání řešení těchto rovnic. Součástí těchto dvou kapitol jsou i řešené a cvičné příklady.

This bachelor's thesis deals with problems involving Diophantine equations. The thesis is divided into 5 main chapters. The first chapter focuses on the historical development of this area of mathematics. The second chapter introduces readers to the basic types of Diophantine equations. Subsequently, the third chapter presents the fundamental concepts and definitions that are necessary for understanding this issue. In the last two chapters, the most significant methods and techniques used to find solutions to these equations are employed. These two chapters also include solved and practice examples.

SEZNAM LITERATURY

[1] **WILLERS, Michael.** *Algebra bez (m)učení.* [překl.] Marek Čtrnáct. Praha : Grada, 2012. str. 64. ISBN 978-80-247-4123-9.

[2] **BASHMAKOVA, Isabella G. a SILVERMAN, Joseph H.** *Diophantus and Diophantine Equations.* místo neznámé : The Mathematical Association of America, 1997. stránky 1–10. ISBN 978-1-4704-5048-9.

[3] **HEATH, Thomas L.** *Diophantus of Alexandria: A Study in the History of Greek Algebra.* místo neznámé : Martino Pub, 2009. stránky 1–7. ISBN 978-1578987542.

[4] **STEINSDÖRFER, Jan.** *Metody řešení diofantických rovnic.* [Online] 2015. [Citace: 18. 4. 2023.] Dostupné z: http://physics.ujep.cz/~jmaly/mo/Diofanticke_rovnice.pdf.

[5] **RÁKOSNÍK, Jiří.** *Základy teorie čísel.* 2. vydání. Praha : Matfyzpress, 2010. ISBN 978-80-7378-141-6.

[6] **HRÁZSKÝ, Jaroslav.** *Dělitelnost čísel a diofantické rovnice.* Brno : KPÚ - kabinet matematiky, 1969.

[7] **RIEMEL, Tomáš.** Diofantovské rovnice a jejich soustavy. [Online] 2017. [Citace: 7. 4. 2023.] Diplomová práce. Univerzita Palackého v Olomouci, Přírodovědecká fakulta. Vedoucí práce RNDr. Jaroslav Švrček, CSc. Dostupné z: https://theses.cz/id/pykxqb/.

[8] **ANDREESCU, Titu et al.** *An Introduction to Diophantine Equations.* New York : Springer Science+Business Media, 2010. ISBN 978-0-8176-4548-9.

[9] **GEL'FOND, Aleksandr O.** *Neurčité rovnice.* [překl.] Karel WINKELBAUER. Praha : STNL – Státní nakladatelství technické literatury, 1954.

[10] **HABALA, Petr.** *Počítání modulo.* [Online] 2019. [Citace: 7. 4. 2023.] České vysoké učení v Praze. Přednáška z předmětu Diskrétní matematika. Dostupné z: shorturl.at/oFGKW.

[11] —. *Rovnice a celá čísla.* [Online] 2019. [Citace: 7. 4. 2023.] České vysoké učení v Praze. Přednáška z předmětu Diskrétní matematika. Dostupné z: shorturl.at/av589.

[12] **HONZÍK, Lukáš.** *Kongruence a neurčité rovnice.* [Online] [Citace: 7. 4. 2023.] Západočeská univerzita v Plzni, Fakulta pedagogická. Přednáška z předmětu Elementární algebra. Dostupné z: shorturl.at/DQUV0.

[13] **JARKOVSKÝ, Jaroslav.** *Dělitelnost a prvočísla.* Praha : Prometheus, 1995. ISBN 80-7196-029-1.

SEZNAM TABULEK, GRAFŮ, PŘÍKLADŮ A CVIČENÍ

PŘÍLOHY

VÝSLEDKY CVIČENÍ

Cvičení 4.1

Nemá řešení, jelikož není splněna podmínka řešitelnosti:

$\mathrm{NSD}(125, 225) = 25 \wedge 25 \nmid 113.$

Cvičení 4.2

$x = 1 + t + 2s; t, s \in \mathbb{Z}$

$y = -1 - 5t - s; t, s \in \mathbb{Z}$

$z = 3 + 4t; t \in \mathbb{Z}$

Cvičení 4.3

$x = 3 - 2t; t \in \mathbb{Z}$

$y = -1$

$z = t; t \in \mathbb{Z}$

Cvičení 5.1

$x = 5 + 16t$

$y = 26 - 11t$

To platí pro $t = \{0; 1; 2\}$

Např. pálenku rozlil do pěti 550 ml lahví a dvaceti šesti 800 ml lahví.

Cvičení 5.2

36 mincí (31 · 50 Kč, 2 · 20 Kč, 1 · 5 Kč, 2 · 2 Kč).

Cvičení 5.3

Otcovi je 42 let a synovi 18 let.