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

SOUSTAVY LINEÁRNÍCH DIOFANTOVSKÝCH ROVNIC A SMITHŮV NORMÁLNÍ TVAR MATICE

DIPLOMOVÁ PRÁCE

Bc. Kateřina Bábíčková
Učitelství pro základní školy, obor Učitelství matematiky pro základní školy

Vedoucí práce: Doc. RNDr. Jaroslav Hora, CSc.

Plzeň 2017

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

V Plzni, 29. června 2017

.....

vlastnoruční podpis

Děkuji vedoucímu bakalářské práce Doc. RNDr. Jaroslavovi Horovi, CSc. za cenné rady a připomínky při vedení mé diplomové práce a v neposlední řadě za trpělivost, kterou mi věnoval.

ZDE SE NACHÁZÍ ORIGINÁL ZADÁNÍ KVALIFIKAČNÍ PRÁCE.

OBSAH

SEZNAM ZKRATEK

Značka a její význam:

$(\ ),\langle\ \rangle;\{\ \}$	kulatá, resp. hranatá, resp. složená závorka
$<\ ;\ \leq$	je menší, resp. je menší nebo rovno
$>\ ;\ \geq$	je větší, resp. je větší nebo rovno
$=$	rovná se
$\equiv$	kongruence
$:, -, \mid$	děleno; v textu píšeme $\frac{a}{b}$ nebo $a\mid b$ místo $a:b$
$\wedge$	a současně
$\triangle, det$	determinant
$\in$	je prvkem, patří do; např. $x \in \langle a, b\rangle$ znamená: *x* patří do intervalu $\langle a, b\rangle$
$\sum$	součet, suma; $\sum_{n=1}^{\infty} a_n$ je nekonečná řada utvořená z členů posloupnosti $\{a_n\}$
$A, B, D, \ldots$	matice
A^T	transponovaná matice k matici A
a^n	*n*-tá mocnina
$a_{i,j}$	prvek v *i*-tém řádku a v *j*-tém sloupci matice A
$diag$	diagonála
hod	hodnost
$n!$	*n*-faktoriál $(1\cdot 2\cdot 3\cdot \ldots \cdot n)$
$m \times n$	matice o m řádcích a n sloupcích
mod	modulo
$x_0 \neq x_1$	x_0 se nerovná x_1
$\vec{x}$	vektor x
$\mathbb{Z}$	obor celých čísel

ÚVOD

Diplomová práce na téma „Soustava lineárních diofantických rovnic a Smithův normální tvar matic“ je věnována lineárním diofantickým rovnicím, jejich soustavám a nakonec i Smithovým normálním tvarem matice.

Mnoho lidí si neumí představit, co se skrývá pod těmito pojmy, i když jsme se určitě všichni na prvním stupni základní školy s lineárními diofantickými rovnicemi setkali. Jediné, s čím jsme se setkat vůbec nemuseli, je Smithův normální tvar matic, neboť s maticemi se setkáváme až na vysokých školách, nebo možná již dříve, na gymnáziích. Cílem této práce bude seznámit čtenáře s těmito pojmy a předvést je na příkladech. Je kladen také důraz na pochopení teoretické podstaty rovnic a soustav. Na základě této práce bychom si měli osvojit i určité početní metody.

V diplomové práci nalezneme čtyři hlavní kapitoly. V první kapitole si povíme, kdo to byl Diofantos z Alexandrie. Než začneme řešit soustavy lineárních diofantických rovnic, měli bychom něco vědět o lineárních diofantických rovnicích, její základní pojmy a početní úkony. Proto další kapitola bude o lineárních diofantických rovnicích, kde si ukážeme vhodné metody potřebné k výpočtu. V třetí kapitole přejdeme k soustavě lineárních diofantických rovnic a způsobům jejich řešení. V poslední kapitole si povíme, kdo to byl Henry John Stephen Smith, a zaměříme se na Smithův normální tvar matice.

1 DIOFANTOS Z ALEXANDRIE

„Otec algebry“, tak nazýváme záhadného muže ze starověkého světa, pana Diofanta z Alexandrie, obzvlášť za jeho dílo Aritmetika. Sepsal i další díla a menší spisky jako například o „polygonálních“ číslech a na jeho počest se rovnicím, jejichž řešení jsou celočíselná, říká diofantické.

1.1 HÁDANKA

O Diofantovi toho víme velice málo. Už jen určit, kdy přesně žil, je pro historiky problém. Ví se, že strávil podstatnou část svého života v Alexandrii. Období, ve kterém žil, odhadujeme podle toho, koho on ve svých pracích cituje a kteří autoři citují jeho. Našly se zmínky, v nichž Diofantos cituje řeckého matematika Hypsiklése, žijícího v době 190 – 120 př. n. l., a kdy řecký matematik a otec Hypatie Theón Alexandrijský (335 – 405 př. n. l.) citoval Diofanta. Tudíž musel žít mezi rokem 150 př. n. l. až do roku 350 n. l. Proto si myslíme, že se narodil kolem roku 200 n. l. a zemřel o nějakých osmdesát čtyři let později.

Věk osmdesát čtyři let známe z tzv. „Diofantovy hádanky“, kterou si Diofantos nechal vytesat na vlastní náhrobek. Je v podobě početní úlohy, a i když existuje několik různých překladů, dostaneme se ke stejnému výsledku. Například tato:

„ 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 tuto hádanku rozluštit.
Pokud označíme za *x* věk Diofanta, kterého se dožil, pak by rovnice byla ve tvaru:

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

Převedeme si výrazy obsahující *x* na levou stranu rovnice:

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

Najdeme společného jmenovatele zlomků, kterým je číslo 84:

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

Upravíme čitatel a dostaneme:

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

Nakonec obě strany vynásobíme 84 a vydělíme 9.

$$x = 84$$

Po vyřešení této rovnice jsme zjistili, že Diofantos žil 84 let. Tato úloha se vyskytovala i v některých středoškolských učebnicích, užívaných v ČR.

1.2 DÍLO

Největším a nejvýznamnějším Diofantovým dílem je Arithmetica [Aritmetika]. Obsahuje 130 až 189 úloh, které se zabývají numerickým řešením určitých i neurčitých rovnic. Arithmetika je složena z třinácti knih, kde bylo shromážděno vše, co znali matematici za dob Diofantova života o řešení lineární a kvadratické rovnice. Dochovalo se ale pouze šest z nich a existují ještě čtyři arabské knihy pokládající se za překlady. Diofantos ignoroval nulu a záporná čísla, tudíž se věnoval kladným racionálním řešením. Dílo Arithmetika sehrálo mnohem později důležitou roli pro formulaci a důkaz Velké Fermatovy věty.

Další díla, která v Arithmetice Diofantos odkazuje, „Porismy“ a „Moriastika“, jsou úplně ztracena. Existují však zlomky jiného díla, tzv. O mnohoúhelníkových číslech.

2 LINEÁRNÍ DIOFANTICKÉ ROVNICE

Definice 1: Lineární diofantické rovnice

Lineární diofantická rovnice je rovnice ve tvaru

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

kde $a_1, a_2, \dots, a_n, b$ jsou celá čísla a $x_1, x_2, \dots, x_n$ jsou neznámé. Pro rovnici o n neznámých předpokládáme, že $a_i \neq 0$ pro každé $i = 1, \dots, n$.

2.1 LINEÁRNÍ DIOFANTICKÉ ROVNICE SE DVĚMA NEZNÁMÝMI

Definice 2:

Lineární neurčitou rovnici o dvou neznámých *x, y* rozumíme rovnici

$$ax + by = c, \qquad a \neq 0 \wedge b \neq 0,$$

kde koeficienty *a, b, c* této rovnice jsou celá čísla a neznámé *x, y* jsou též prvky množiny celých čísel.

Definice 3: Největší společný dělitel

Nechť jsou kladná celá čísla $a_1, a_2, \dots, a_n$. Číslo $u \in \mathbb{Z}$ nazýváme společným dělitelem čísel $a_1, a_2, \dots, a_n$, pokud $u|a_i$ pro každé $i = 1, 2, \dots, n$. Kladné celé číslo d nazýváme největším společným dělitelem čísel $a_1, a_2, \dots, a_n$ a zapisujeme $d = (a_1, a_2, \dots, a_n)$, jestliže d je společným dělitelem těchto čísel a je-li $u \in \mathbb{Z}$ libovolný společný dělitel čísel $a_1, a_2, \dots, a_n$, pak $u|d$.

Věta 1: Nutná podmínka řešitelnosti

Nutnou podmínkou řešitelnosti rovnice $ax + by = c$ je, že největší společný dělitel d koeficientů *a, b* musí dělit celé číslo *c*.

Předpokladem je, že rovnice má řešení x_0, y_0. Potom platí $d|(ax_0 + by_0)$, protože $d|a \wedge d|b$. Tím je dokázáno, že $d|c$.

Lemma 1:

Nechť $a|b$ a $b|c$, potom pro libovolná celá čísla *x* a *y* platí $a|(bx + cy)$.

Důkaz věty o nutné podmínce řešitelnosti

Nejprve dokazujeme, že rovnice $ax + by = c$ je řešitelná, pokud platí $(a, b)|c$. Předpokládáme, že existují celá čísla x a y pro $ax + by = c$. Pak na základě vlastnosti největšího společného dělitele a lemmatu 1 platí $d|(ax + by) = c$.

Řešitelnost rovnice vyplývá z podmínky $(a, b)|c$ a označme si $(a, b) = d$. Pak zkoumáme diofantickou rovnici ve tvaru $ax + by = d$. Euklidovým algoritmem umíme nalézt čísla x_0, y_0, která leží v oboru celých čísel. Potom platí $ax_0 + by_0 = 1$. Pak $(a, b)|c$ a $c = de$, kde $e \in \mathbb{Z}$.

Nechť je $x_1 = ex_0$ a $y_1 = ey_0$, zřejmě pak platí

$$ax_1 + by_1 = e(ax_0 + by_0) = ed = c.$$

To znamená, že dvojice (x_1, y_1) je řešením diofantické rovnice.

Věta 2: Nesoudělná čísla

Mějme čísla $a_1, a_2, \dots, a_n$ nazývaná nesoudělná, právě když $d = (a_1, a_2, \dots, a_n) = 1$. Ke každým dvěma nesoudělným přirozeným číslům a, b existují celá čísla x, y taková, že platí $ax + by = 1$.

Věta 3: Euklidův algoritmus

Nechť a, b jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{n-1} = (a, b)$.

Věta 4: Bezoutova rovnost

Pro libovolná celá čísla a, b a $d = (a, b)$ je jejich největší společný dělitel, přitom existují celá čísla u, v tak, že $d = au + bv$. To nazýváme Bezoutova rovnost.

Jsou-li čísla a, b nesoudělná, existují celá čísla u, v, pro která je

$$au + bv = 1.$$

Na příkladu si ukážeme nelezení jednoho řešení lineární diofantické rovnice s využitím Euklidova algoritmu.

Příklad: Nalezněte jedno řešení diofantické rovnice $32x + 14y = 2$.

Řešení:

Podle věty o nutné podmínce řešitelnosti je tato rovnice řešitelná, tj. $d = (32, 14) = 2$ a ta dělí pravou stranu rovnice. Euklidův algoritmus pro $a = 32$, $b = 14$ dává

$$32 = 14 \cdot 2 + 4$$

$$14 = 4 \cdot 3 + 2$$

$$4 = 2 \cdot 2 + 0.$$

Protože největší společný dělitel je 2, pak ji vyjádříme z předposlední rovnice

$$2 = 14 - 4 \cdot 3 = 14 + 4 \cdot (-3).$$

Z první rovnice máme

$$4 = 32 - 14 \cdot 2 = 32 + 14 \cdot (-2)$$

a dosazením dostaneme

$$2 = 14 + \big(32 + 14 \cdot (-2)\big) \cdot (-3) = 14 + 32 \cdot (-3) + 14 \cdot 6 = 32 \cdot (-3) + 14 \cdot 7.$$

Tímto jsme vypočetli Bézoutovu identitu a nalezli řešení $x_0 = -3$ a $y_0 = 7$.

Nechť celá čísla $x_0\left(\frac{c}{d}\right), y_0\left(\frac{c}{d}\right)$ představují již řešení rovnice $ax + by = c$. Nyní se pokusíme nalézt všechna řešení rovnice $ax + by = c$, když jsme nalezli již pevné řešení x_0, y_0. Předpokládejme nějaké další řešení x', y'. Potom bude platit:

$$\left(\frac{a}{d}\right) x_0 + \left(\frac{b}{d}\right) y_0 = \frac{c}{d}$$

a platí také

$$\left(\frac{a}{d}\right) x' + \left(\frac{b}{d}\right) y' = \frac{c}{d}.$$

Odečtením obou rovností dostáváme

$$\left(\frac{a}{d}\right)(x_0 - x') + \left(\frac{b}{d}\right)(y_0 - y') = 0,$$

upravíme tak, abychom měli na každé straně zvlášť neznámé x_0, x' a y_0, y'

$$\left(\frac{a}{d}\right)(x_0 - x') = \left(\frac{b}{d}\right)(y' - y_0).$$

Odtud plyne dělitelnost$\left(\frac{a}{d}\right) / (y_0 - y')$ a také existence celého čísla *t*, pro které platí

$$y_0 - y' = \left(\frac{a}{d}\right) t.$$

Nyní si vyjádříme *y'*:

$$y' = y_0 - \left(\frac{a}{d}\right) t.$$

Tuto rovnost dosadíme do rovnice $\left(\frac{a}{d}\right)(x_0 - x') + \left(\frac{b}{d}\right)(y_0 - y') = 0$, a dostaneme

$$\left(\frac{a}{d}\right)(x_0 - x') + \left(\frac{b}{d}\right)\left[y_0 - \left(y_0 - \left(\frac{a}{d}\right) t\right)\right] 0.$$

Upravíme závorky

$$\left(\frac{a}{d}\right)(x_0 - x') + \left(\frac{b}{d}\right)\left(\frac{a}{d}\right) t = 0,$$

rovnici vydělíme $\left(\frac{a}{d}\right)$ a vyjádříme *x'*:

$$x' = x_0 + \left(\frac{b}{d}\right) t.$$

Zkouškou se přesvědčíme, že celá čísla *x', y'*, pro která platí

$$x' = x_0 + \left(\frac{b}{d}\right) t$$

$$y' = y_0 - \left(\frac{a}{d}\right) t$$

kde $t \in \mathbb{Z}$, jsou řešením této rovnice. Tímto dostáváme větu o nutné a postačující podmínce, která výše vyjádřené poznatky shrnuje.

Věta 5: Nutná a postačující podmínka

Nutnou a postačující podmínkou pro to, aby neurčitá rovnice $ax + by = c,\ a \neq 0 \wedge b \neq 0$, měla aspoň jednu dvojici řešení x_0, y_0 je, aby největší společný dělitel *d* koeficientů *a, b* této rovnice dělil celé číslo *c*. Jestliže celá čísla x_0, y_0 jsou řešením rovnice $ax + by = c$, $a \neq 0 \wedge b \neq 0$, potom všechna řešení rovnice jsou dána parametrickými rovnostmi:

$$x = x_0 + \left(\frac{b}{d}\right) t$$

$$y = y_0 - \left(\frac{a}{d}\right) t,$$

kde parametr *t* probíhá množinou celých čísel Z.

2.1.1 PŘÍKLAD

Zadání:

Malý Vašík moc toužil po autíčku, které stálo 99 korun. Musel si ale na něj našetřit. Od babičky dostával pětikoruny a od maminky dvoukoruny a vše si schovával do kasičky. Kolik dvoukorun a pětikorun dá v obchodě, aby zaplatit autíčko?

1. **Řešení úsudkem**

Pokud zadáme tuto úlohu žákovi, určitě se ji pokusí vyřešit logickým uvažováním. Vystačí si se základními početními operacemi, aniž by sestavoval rovnici. Bohužel se tak nedozví, že řešil lineární diofantickou rovnici. Jak by žák mohl danou úlohu vyřešit?

První co žáka asi napadne, je zkusit zaplatit pomocí velkého množství pětikorun. Číslo 99 není dělitelné pěti beze zbytku. Zjistíme, že 99 děleno pěti dává neúplný podíl 19 a zbytek čtyři. To znamená, že bychom částku 99 korun mohli zaplatit devatenácti pětikorunami a dvěma dvoukorunami. Nacházíme tak první řešení tohoto příkladu. Musíme ale pokračovat, nezískali jsme všechna řešení.

Nemůžeme počet pětikorun snížit? O jednu pětikorunu rozhodně ne, protože ji nedokážeme nahradit samými dvoukorunami. Ze stejného důvodu nemůžeme ubrat lichý počet pětikorun. Kdybychom ale ubrali dvě pětikoruny, tak bychom ztrátu vyrovnali pěti dvoukorunami. Nacházíme další řešení, postačí nám 17 pětikorun a sedm dvoukorun.

Mohli jsme ale ubrat čtyři pětikoruny a tuto ztrátu dohnat deseti dvoukorunami. Tím už máme třetí řešení, zaplatíme pomocí 15 pětikorun a dvanácti dvoukorun.

Nacházet další řešení je již snadné. Snížíme vždy počet pětikorun o dvě a zároveň musíme přidat pět dvoukorun. Skončíme tím, že k zaplacení použijeme jednu pětikorunu a 47 dvoukorun. Řešení zapisujeme do tabulky

Počet pětikorun	Počet dvoukorun
19	2
17	7
15	12
13	17
11	22

Počet pětikorun	Počet dvoukorun
9	27
7	32
5	37
3	42
1	47

Tabulka 1

2. Řešení s využitím Euklidova algoritmu:

Chceme-li počítat lineární diofantické rovnice, měli bychom je umět řešit i jinými způsoby. Jedním možným řeším je pomocí Euklidova algoritmu.

Označíme si:

Počet dvoukorun … *x*

Počet pětikorun … *y*

Tato slovní úloha vede k rovnici: $2x + 5y = 99$. Řešením dané diofantické rovnice je každá uspořádaná dvojice $[x, y]$ celých nebo přirozených čísel. Vzhledem k zadání příkladu nás budou zajímat pouze čísla přirozená.

Nalezneme si alespoň jednu dvojici x_0, y_0, která by byla řešením rovnice $2x + 5y = 99$. Jelikož čísla 5 a 2 jsou čísla nesoudělná, je d = (5, 2) = 1. Podle věty 2 o nesoudělných číslech platí $2x' + 5y' = 1$. Tato čísla nalezneme pomocí Euklidova algoritmu. Protože jsou v tomto příkladu čísla nízká, dokážeme tyto čísla uhodnout.

Podle Euklidova algoritmu platí:

$$5 = 2 \cdot 2 + 1$$

Nemusíme psát zpětný zápis pomocí jedničky, protože již z úpravy vidíme, jak rovnice bude vypadat:

$$2 \cdot (-2) + 5 \cdot 1 = 1$$

Našli jsme čísla x', y', pro která platí:

$$x' = -2$$

$$y' = 1$$

Rovnost $2 \cdot (-2) + 5 \cdot 1 = 1$ vynásobíme 99 a dostáváme

$$2 \cdot (-198) + 5 \cdot 99 = 99.$$

Celá čísla $x_0 = -198$, $y_0 = 99$ představují řešení původní rovnice.

Pokud $d|c$ a jsou-li celá čísla x_0, y_0, jsou řešením rovnice $ax + by = c, a \neq 0 \wedge b \neq 0$, potom všechna řešení rovnice jsou dána parametrickými rovnicemi

$$x = x_0 + \left(\frac{b}{d}\right)t$$

$$y = y_0 - \left(\frac{a}{d}\right)t, t \in \mathbb{Z}$$

$$2 \cdot (-198) + 5 \cdot 99 = 99$$

$$a(x_0) + b(y_0) = 99$$

Všechna řešení rovnice $2x + 5y = 99$ jsou po dosazení dána parametrickými rovnicemi:

$$x = -198 + \left(\frac{5}{1}\right)t$$

$$y = 99 - \left(\frac{2}{1}\right)t, t \in \mathbb{Z}$$

$$x = -198 + 5t$$

$$y = 99 - 2t$$

Dále řešíme pomocí nerovnic, kterými omezíme hodnotu parametru *t*. Podle zadání musí platit nerovnice $x \geq 0$, $y \geq 0$, $x + y = -99 + 3t$.

1.) $x \geq 0$ $\quad -198 + 5t \geq 0$ $\quad$ 2.) $y \geq 0$ $\quad 99 - 2t \geq 0$

$$t \geq 39\frac{3}{5} \qquad\qquad t \leq 49\frac{1}{2}$$

Řešením těchto nerovnic dostáváme nerovnice, kterým vyhovuje deset hodnot parametru *t*. Dosadíme *t* do rovnic $x = -198 + 5t$ a do $y = 99 - 2t$.

t	40	41	42	43	44	45	46	47	48	49
x	2	7	12	17	22	27	32	37	42	47
y	19	17	15	13	11	9	7	5	3	1

Tabulka 2

3. Řešení s využitím kongruence:

Pomocí lineární kongruence lze také řešit lineární diofantické rovnice.

Definice 4: Kongruence

Nechť $a, b \in \mathbb{Z}$. Jestliže čísla *a*, *b* mají při dělení přirozeným číslem *m* stejný zbytek *r*, kde $0 \leq r \leq m$, pak se nazývají *a*, *b* kongruentní podle modulu *m*. Zapisujeme:

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

Lemma 2:

Nechť $a, b \in \mathbb{Z},\ m \in \mathbb{N}$, pak jsou následující podmínky ekvivalentní:

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

b) $a = b + mt$ pro vhodné $t \in \mathbb{Z}$,

c) $m \mid a - b$.

Věta 6: Základní vlastnosti kongruencí

1.) Můžeme sčítat kongruence podle téhož modulu. Můžeme přenést libovolný sčítanec s opačným znaménkem z jedné strany kongruence na druhou. Můžeme přičíst jakýkoliv násobek modulu na libovolnou stranu kongruence.

2.) Můžeme násobit kongruence podle téhož modulu. Obě strany kongruence je možné umocnit na totéž přirozené číslo či vynásobit stejným celým číslem.

3.) Můžeme vydělit jejich společným dělitelem obě strany kongruence, jestliže je tento dělitel nesoudělný s modulem.

4.) Obě strany kongruence i její modul můžeme současně vynásobit stejným přirozeným číslem nebo vydělit jejich společným kladným dělitelem.

Nyní se pokusíme vyřešit předchozí úlohu podle této metody. Měli jsme rovnici
$2x + 5y = 99$ a tu můžeme rozdělit na dva případy.

a) Pokud vyjádříme x z kongruence $2x \equiv 99\ (mod\ 5)$ a dosadíme do diofantické rovnice, získáme řešení.

$$2x \equiv 99\ (mod\ 5)$$

$$2x \equiv 4\ (mod\ 5)$$

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

$$x = 2 + 5t.$$

Dosadíme x do původní rovnice

$$2(2 + 5t) + 5y = 99$$

$$4 + 10t + 5y = 99$$

$$10t + 5y = 95$$

$$y = 19 - 2t$$

Řešením je každá uspořádaná dvojice $[2 + 5t;\ 19 - 2t]$, kde $t \in \mathbb{Z}$. Do tabulky jsou uvedena všechna $[x, y]$ řešení, jejichž složkami jsou výhradně přirozená čísla:

t	0	1	2	3	4	5	6	7	8	9
x	2	7	12	17	22	27	32	37	42	47
y	19	17	15	13	11	9	7	5	3	1

Tabulka 3

b) Vyjádříme-li y z kongruence $5y \equiv 99\ (mod\ 2)$ a dosadíme do diofantické rovnice, řešení by se nemělo změnit.

$$5y \equiv 99\ (mod\ 2)$$

$$y \equiv 1\ (mod\ 2)$$

$$y = 1 + 2t$$

Dosadíme *y* do původní rovnice a vyřešíme

$$2x + 5(1 + 2t) = 99$$

$$2x + 5 + 10t = 99$$

$$2x + 10t = 94$$

$$x + 5t = 47$$

$$x = 47 - 5t$$

Řešením jsou uspořádané dvojice $[47 - 5t;\ 1 + 2t]$, kde $t \in \mathbb{Z}$. Pokud dosadíme *t* do uspořádaných dvojic, pak dostáváme stejnou tabulku, ale v opačném pořadí.

2.2 LINEÁRNÍ DIOFANTICKÉ ROVNICE O VÍCE NEZNÁMÝCH

Zjistili jsme, že řešení lineárních diofantických rovnic o dvou neznámých není nic složitého a tomu nebude jinak i při řešení lineárních diofantických rovnic o více neznámých. Využíváme stejné poznatky, avšak ne všechny metody jsou vhodné pro řešení. Jak jsme si již uvedli, při řešení těchto rovnic používáme Euklidův algoritmus a kongruenci. Dalšími metodami jsou například vyjádření členu s nejmenším koeficientem, redukční metoda nebo grafické znázornění. Těmito metodami se v této práci zabývat nebudeme.

Definice 5: Lineární diofantická rovnice o *n* neznámých

Lineární neurčitou rovnici o *n* neznámých rozumíme rovnici

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

kde koeficienty $a_1, a_2, \ldots, a_n$ této rovnice jsou celá čísla, $a_i \neq 0$ pro všechna $i = 1, 2, \ldots, n$ a neznámé $x_1, x_2, \ldots, x_n$ jsou též z množiny celých čísel.

Věta 7: Nutná podmínka

Nutnou podmínkou řešitelnosti rovnice $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ je, že největší společný dělitel *d* koeficientů $a_1, a_2, \ldots, a_n$ musí dělit celé číslo *b:*

$$d = (a_1, a_2, \ldots, a_n) \wedge d|b.$$

2.2.1 PŘÍKLAD

Zadání:

Maminka si chce pořídit album na fotografie. Má tři druhy fotografií – formát 10x13, formát 15x15 a formát 20x30. Na jednu stranu alba se vejde formát 10x13 9krát, formát 15x15 4krát a formát 20x30 2krát. Kolika stránkové album si maminka musí pořídit, když má 108 fotografií?

Označíme si:

Počet fotografií formátu 10x13 … *x*

počet fotografií formátu 15x15 … *y*

počet fotografií formátu 20x30 … *z*

Pro tuto slovní úlohu rovnice bude vypadat takto:

$$9x + 4y + 2z = 108.$$

Než začneme tuto rovnici řešit, prověříme, zda má vůbec nějaká řešení. Jinak řečeno, ověříme si nutnou podmínku řešitelnosti. Máme čísla 9, 4, 2 a jejich největším společným dělitelem je číslo 1. Číslo 1 dělí číslo 108 a proto je úloha řešitelná.

1. **Řešení s využitím Euklidova algoritmu**

Rovnice je v základním tvaru se třemi neznámými. Nejprve si najdeme největšího společného dělitele dvou čísel a následně provedeme substituci.

Největším společným dělitelem dvou čísel v této rovnici je d = (4, 2) roven dvěma a tu vytkneme před závorku.

$$9x + 4y + 2z = 108$$

$$9x + 2 \cdot (2y + z) = 108,$$

Substituce bude pro $u = 2y + z$ a dostaneme rovnici $9x + 2u = 108$. Ta musí stále splňovat podmínku řešitelnosti. Největší společný dělitel 9 a 2 je 1 a 1 dělí číslo 108, takže je řešitelná. Nyní pomocí Euklidova algoritmu nalezneme čísla x_0, u_0, která lze snadno uhodnout.

Euklidův algoritmus je $9 = 2 \cdot 4 + 1$ a zpětným zápisem pomocí 1 dostáváme rovnost:

$$9 \cdot 1 + 2 \cdot (-4) = 1$$

Tu musíme vynásobit 108:

$$9 \cdot 108 + 2 \cdot (-432) = 108.$$

Celá čísla $x_0 = 108$, $u_0 = -432$ představují řešení původní rovnice.

Pokud $d|c$ a jsou-li celá čísla x_0, u_0 jsou řešením rovnice $ax + bu = c, a \neq 0 \wedge b \neq 0$, potom všechna řešení rovnice jsou dána parametrickými rovnicemi

$$x = x_0 + \left(\frac{b}{d}\right) t$$

$$u = u_0 - \left(\frac{a}{d}\right) t;\ t \in \mathbb{Z}$$

$$a(x_0) + b(u_0) = 108.$$

Všechna řešení rovnice $9x + 2u = 108$ jsou po dosazení dána parametrickými rovnicemi:

$$x = 108 + \left(\frac{2}{1}\right) t$$

$$u = -432 - \left(\frac{9}{1}\right)t;\ t \in \mathbb{Z}$$

$$x = 108 + 2t$$

$$u = -432 - 9t;\ t \in \mathbb{Z}.$$

Nyní se vraťme k substituci $u = 2y + z$ a vyřešíme rovnici $2y + z = -432 - 9t$.
Použijeme znova Euklidův algoritmus a získáme Bezoutovu rovnost

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

$$2 \cdot (-432 - 9t) + 1 \cdot (432 + 9t) = -432 - 9t.$$

Všechna řešení rovnice jsou dána dalšími parametrickými rovnicemi

$$y = y_0 + \left(\frac{b}{d}\right)s$$

$$z = z_0 - \left(\frac{a}{d}\right)s;\ s \in \mathbb{Z}$$

$$a(y_0) + b(z_0) = -432 - 9t$$

a pro rovnici $2y + z = -432 - 9t$ platí

$$y = -432 - 9t + \left(\frac{1}{1}\right)s$$

$$z = 432 + 9t - \left(\frac{2}{1}\right)s;\ t, s \in \mathbb{Z}$$

$$y = -432 - 9t + s$$

$$z = 432 + 9t - 2s;\ t, s \in \mathbb{Z}.$$

Řešením jsou trojice čísel $[x, y, z]$ ve tvaru

$$x = -108 + 2t$$

$$y = -432 - 9t + s$$

$$z = 432 + 9t - 2s,$$

kde *s* a *t* jsou celá čísla.

Trojice obsahující výhradně přirozená čísla nalezneme z nerovnic $x \geq 0$, $y \geq 0$, $z \geq 0$:

1.) $x \geq 0$ $\quad -108 + 2t \geq 0$ $\quad$ 2.) $y \geq 0$ $\quad -432 - 9t + s \geq 0$

$t \geq 54$ $\quad$ 3.) $z \geq 0$ $\quad 432 + 9t - 2s \geq 0$

Vyřešit tyto nerovnice není vůbec jednoduché. Vypomůžeme si s počítačovým programem Mathematica, která vypíše všechna možná řešení.

Zadáme-li

Solve[9x+4y+2z==108&&x>0 &&y>0&&z>0,{x,y,z},Integers]

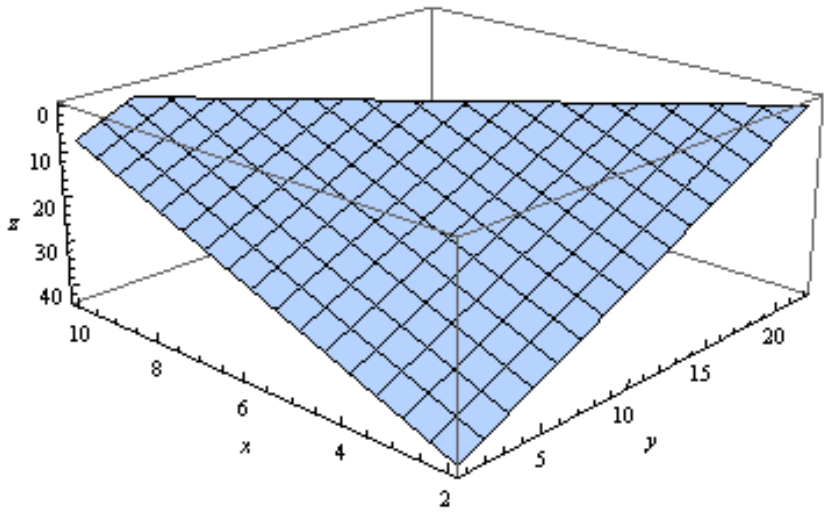
dostaneme uspořádané trojice

{{x->2,y->1,z->43},{x->2,y->2,z->41},{x->2,y->3,z->39},{x->2,y->4,z->37},
{x->2,y->5,z->35},{x->2,y->6,z->33},{x->2,y->7,z->31},{x->2,y->8,z->29},
{x->2,y->9,z->27},{x->2,y->10,z->25},{x->2,y->11,z->23},{x->2,y->12,z->21},
{x->2,y->13,z->19},{x->2,y->14,z->17},{x->2,y->15,z->15},{x->2,y->16,z->13},
{x->2,y->17,z->11},{x->2,y->18,z->9},{x->2,y->19,z->7},{x->2,y->20,z->5},
{x->2,y->21,z->3},{x->2,y->22,z->1},{x->4,y->1,z->34},{x->4,y->2,z->32},
{x->4,y->3,z->30},{x->4,y->4,z->28},{x->4,y->5,z->26},{x->4,y->6,z->24},
{x->4,y->7,z->22},{x->4,y->8,z->20},{x->4,y->9,z->18},{x->4,y->10,z->16},
{x->4,y->11,z->14},{x->4,y->12,z->12},{x->4,y->13,z->10},{x->4,y->14,z->8},
{x->4,y->15,z->6},{x->4,y->16,z->4},{x->4,y->17,z->2},{x->6,y->1,z->25},
{x->6,y->2,z->23},{x->6,y->3,z->21},{x->6,y->4,z->19},{x->6,y->5,z->17},
{x->6,y->6,z->15},{x->6,y->7,z->13},{x->6,y->8,z->11},{x->6,y->9,z->9},
{x->6,y->10,z->7},{x->6,y->11,z->5},{x->6,y->12,z->3},{x->6,y->13,z->1},
{x->8,y->1,z->16},{x->8,y->2,z->14},{x->8,y->3,z->12},{x->8,y->4,z->10},
{x->8,y->5,z->8},{x->8,y->6,z->6},{x->8,y->7,z->4},{x->8,y->8,z->2},
{x->10,y->1,z->7},{x->10,y->2,z->5},{x->10,y->3,z->3},{x->10,y->4,z->1}}.

Lineární rovnice o dvou neznámých je rovnicí přímky a lineární rovnice o třech neznámých je rovnice roviny. Sestrojit přímku bychom jednoduše zvládli, ale zakreslit rovinu je přece jen náročnější. Proto tyto uspořádané trojice znova zapíšeme do programu Mathematica. Protože hledáme celočíselná řešení rovnice, bude rovina procházet mřížovými body ze získané mřížkované sítě.

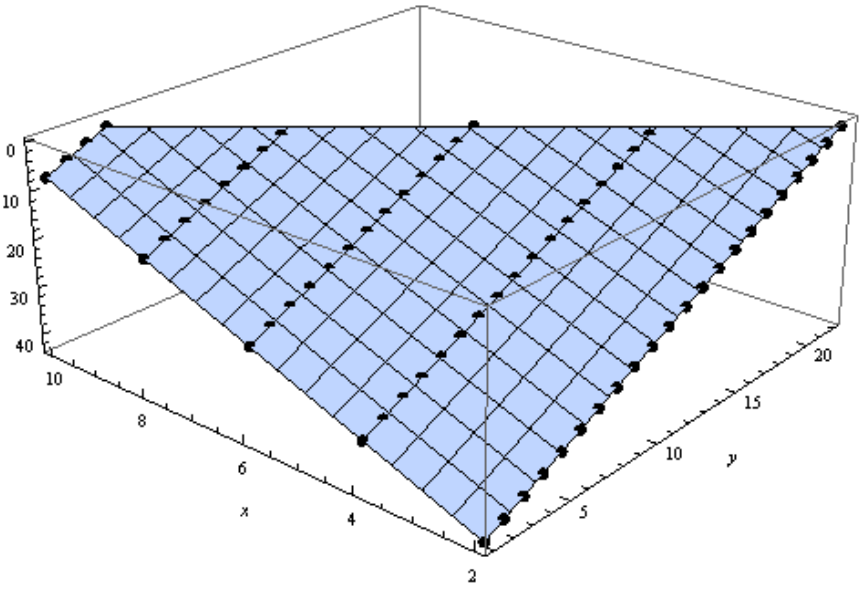
Celý soubor bodů si označme jako body. Pak do programu zadáme:

ListPlot3D[{body}, AxesLabel→{x, y, z}], čímž dostaneme



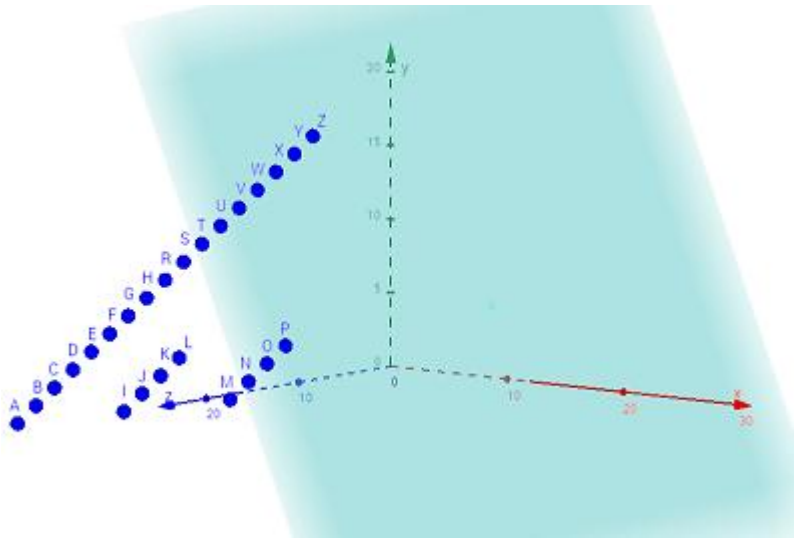
Graf 1 – grafické řešení lineární diofantické rovnice v programu Mathematica

Po zvýraznění bodů dostáváme tento graf.



Graf 2 – grafické řešení lineární diofantické rovnice v programu Mathematica

Ještě jsem se pokusila o grafické znázornění v programu Geogebra, kam jsem vypsala jen pár bodů (z 64 bodů jen 27). Bohužel, z grafu není moc dobře vidět, že body leží v jisté rovině.



Graf 3 - grafické řešení lineární diofantické rovnice v programu GeoGebra

2. Řešení s využitím kongruence

Pokud máme řešit předchozí úlohu pomocí kongruence, pak bychom měli vědět, že to není univerzální metoda. Sami si vybíráme vhodný modul tak, abychom dostali co nejméně neznámých.

Ze slovní úlohy jsme dostali rovnici $9x + 4y + 2z = 108$.

Jelikož největší společný dělitel čísel 2 a 4 je 2, pak tohle číslo bude nejvhodnější modulo.

$$9x + 4y + 2z \equiv 108 \ (mod\ 2)$$

Dostáváme kongruenci upravenou na tvar

$$x \equiv 0 \ (mod\ 2),$$

nahradíme *x* parametrem *s*

$$x = 2s, \text{ kde } s \in \mathbb{Z}.$$

Zpětně dosadíme, upravíme a dostáváme

$$9 \cdot 2s + 4y + 2z = 108$$

$$4y + 2z = 108 - 18s.$$

Dostali jsme se k lineární diofantické rovnici o dvou neznámých, kterou již umíme řešit z předchozí podkapitoly. Nyní nahradíme neznámou *z* pomocí modulo 4 parametrem *t*

$$4y + 2z \equiv (108 - 18s) \ (mod\ 4)$$

$$2z \equiv 2s \ (mod\ 4)$$

Tuto rovnici upravíme podle věty, která zní: Je-li $ac \equiv bc\ (mod\ n)$ a $d = (c, n)$ je největší společný dělitel čísel c a n, potom $a \equiv b\ (mod\ m)$, kde $n = dm$. Tedy jestliže c a n jsou nesoudělná čísla, pak $a \equiv b\ (mod\ n)$.

Proto dostáváme rovnici ve tvaru

$$z \equiv s\ (mod\ 2)$$

$$z = s + 2t, \text{ kde } s, t \in \mathbb{Z}.$$

Znova zpětně dosadíme, upravíme a dostáváme neznámou y

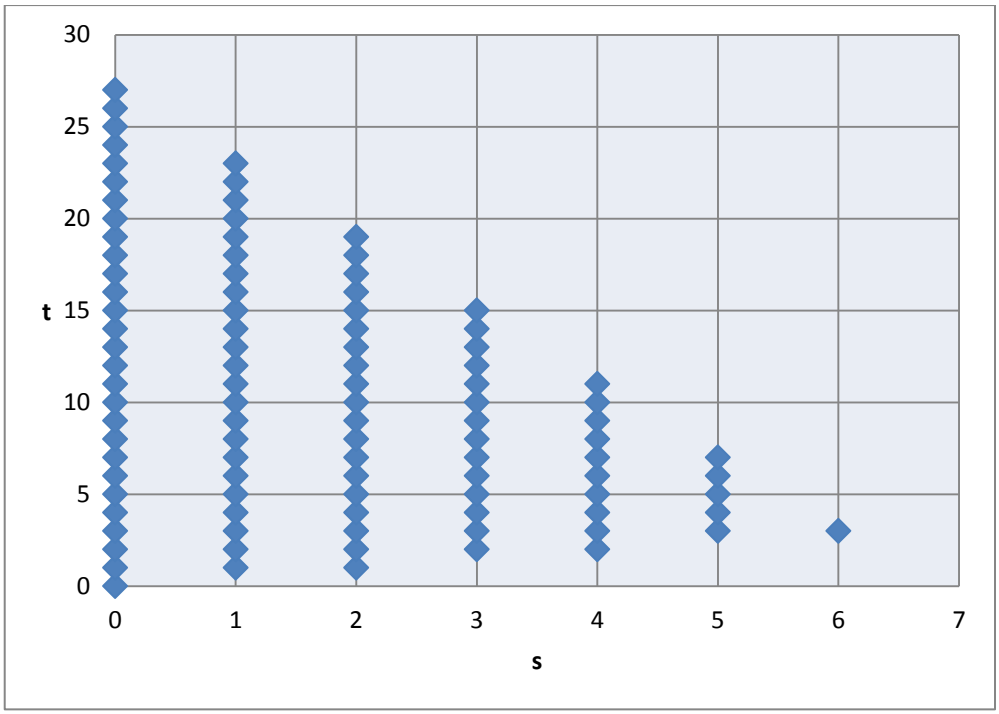
$$4y - 2(s + 2t) = 108 - 18s$$

$$4y - 2s - 4t = 108 - 18s$$

$$4y = 108 - 16s + 4t$$

$$y = 27 - 4s + t, \text{ kde } s, t \in \mathbb{Z}.$$

Řešením rovnice $9x + 4y + 2z = 108$ je uspořádaná trojice $[2s; 27 - 4s + t; s + 2t]$, kde $s, t \in \mathbb{Z}$. Jak již víme, dostaneme 64 možností řešení. Zakresleme si tedy graf závislý na parametru s a t.



Graf 4 – graf závislý na parametru s a t

Pro lepší přehled jsem v Excelu vypočítala hodnoty pro neznámé *x*, *y* a *z* a parametry *s* a *t*.

x	*y*	*z*	*s*	*t*
2	22	1	1	1
2	21	3	1	2
2	20	5	1	3
2	19	7	1	4
2	18	9	1	5
2	17	11	1	6
2	16	13	1	7
2	15	15	1	8
2	14	17	1	9
2	13	19	1	10
2	12	21	1	11
2	11	23	1	12
2	10	25	1	13
2	9	27	1	14
2	8	29	1	15
2	7	31	1	16
2	6	33	1	17
2	5	35	1	18
2	4	37	1	19
2	3	39	1	20
2	2	41	1	21
2	1	43	1	22
4	17	2	2	2
4	16	4	2	3
4	15	6	2	4
4	14	8	2	5
4	13	10	2	6
4	12	12	2	7
4	11	14	2	8
4	10	16	2	9
4	9	18	2	10
4	8	20	2	11

x	*y*	*z*	*s*	*t*
4	7	22	2	12
4	6	24	2	13
4	5	26	2	14
4	4	28	2	15
4	3	30	2	16
4	2	32	2	17
4	1	34	2	18
6	13	1	3	2
6	12	3	3	3
6	11	5	3	4
6	10	7	3	5
6	9	9	3	6
6	8	11	3	7
6	7	13	3	8
6	6	15	3	9
6	5	17	3	10
6	4	19	3	11
6	3	21	3	12
6	2	23	3	13
6	1	25	3	14
8	8	2	4	3
8	7	4	4	4
8	6	6	4	5
8	5	8	4	6
8	4	10	4	7
8	3	12	4	8
8	2	14	4	9
8	1	16	4	10
10	4	1	5	3
10	3	3	5	4
10	2	5	5	5
10	1	7	5	6

Tabulka 4

Tímto způsobem můžeme řešit i další lineární diofantické rovnice o více než třech neznámých, kde najdeme alespoň obecné řešení pro všechny neznámé. Budeme se ale muset vzdát naděje, že výsledky zakreslíme do grafu – ten by musel být čtyřrozměrný a více.

3 SOUSTAVY LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

V předchozích kapitolách jsme si ukázali, co to je a jak se řeší lineární diofantické rovnice. Pokud máme zadáno více lineárních diofantických rovnic s několika neznámými, pak hovoříme o soustavě lineárních diofantických rovnic. Takováto soustava se formálně od běžných soustav lineárních rovnic nad tělesem reálných čísel nijak neliší a využíváme stejné metody.

Definice 6: Soustava lineárních diofantických rovnic

Soustavou lineárních rovnici o *n* neznámých rozumíme soustavu rovnic

$$a_{11}x_1 + a_{12}x_2 + \cdots a_{1n}x_n = c_1$$

$$a_{21}x_1 + a_{22}x_2 + \cdots a_{2n}x_n = c_2$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + \cdots a_{mn}x_n = c_m \ ,$$

kde koeficienty a_{ij} jsou celá čísla pro všechna $i, j = 1, 2, \dots, n,$ a $c_1, c_2, \dots, c_n$ jsou absolutní členy soustavy také celá čísla a neznámé $x_1, x_2, \dots, x_n$ jsou též množiny celých čísel. Pro čísla $m, n \in \mathbb{N}$ platí $m \geq 1$ a $n \geq 1$. Řešením všech rovnic soustavy je každá uspořádaná *n*-tice $[x_1, x_2, \dots, x_n] \in \mathbb{Z}$, která vyhovuje každé z rovnic dané soustavy.

Tuto soustavu lineárních diofantických rovnic o *n* neznámých můžeme také zapsat do maticového tvaru $A\vec{x} = \vec{c}$. Zde máme celočíselnou matici $A = (a_{ij})$ typu $m \times n$, celočíselný vektor $\vec{c}$ a hledáme všechna celočíselná řešení $\vec{x}$.

Podmínky řešitelnosti rovnic jsou stejné jako v předchozí kapitole, ale je i tak soustava sama o sobě řešitelná? Může toto řešit Frobeniova věta?

Věta 8: Frobeniova věta

Soustava lineárních rovnic je řešitelná právě tehdy, když hodnost matice $hod(A)$ je stejná jako hodnost matice rozšířené $hod(A|\mathrm{c})$. Zapisujeme:

$$hod(A) = hod(A|\mathrm{c}).$$

Definice 7: Hodnost matice

Nechť maticový zápis soustavy rovnic je $A\vec{x} = \vec{c}$. Pak hodnost matice je číslo, které udává počet lineárně nezávislých řádků matice.

Frobeniova věta platí pro soustavy lineárních (ale ne diofantických) rovnic. Uvažme příklad, kdy máme soustavu obsahující jen jedinou diofantickou rovnici $2x + 4y = 7$. Je jasné, že tato diofantická rovnice nemá řešení. Pokud ale napíšeme matici soustavy $(2, 4)$ a rozšířenou matici soustavy $(2, 4 \mid 7)$, mají obě hodnost 1 nad tělesem reálných čísel a podle Frobeniovy věty má soustava řešení. Těch je dokonce nekonečně mnoho (geometricky jde o všechny body přímky o rovnici $2x + 4y = 7$). Jenže na této přímce neleží žádný mřížový bod roviny s celočíselnými souřadnicemi a příslušná diofantická rovnice nemá řešení.

3.1 ZPŮSOBY ŘEŠENÍ SOUSTAV LINEÁRNÍCH DIOFANTICKÝCH ROVNIC

Uvedená soustava se dá řešit několika metodami. Než se začneme zabývat maticemi, zkusíme počítat bez nich. Využijeme početní metody, které jsou založeny na postupné eliminaci (vyloučení) neznámé z rovnic soustavy.

3.1.1 SČÍTACÍ METODA (ADIČNÍ)

U sčítací metody se rovnice soustavy násobí čísly zvolenými tak, aby se po sečtení rovnic jedna neznámá vyloučila.

Příklad:

Pomocí sčítací metody řešte soustavu lineárních diofantických rovnic.

$$12x + 3y - z = 4$$

$$6x - 2y = 3$$

Řešení:

Stejně jako u lineárních diofantických rovnic, tak i zde musíme ověřit nutnou podmínku řešitelnosti u každé rovnice zvlášť. V první rovnici máme koeficienty 12, 3 a 1, jejichž největším společným dělitelem je číslo 1. Číslo 1 dělí číslo 4 a tak první rovnice je řešitelná. U druhé rovnice máme tři koeficienty 6, 2 a 0. Bereme však největší společný dělitel čísel 6 a 2 a to je číslo 2 a ta nedělí číslo 3, tudíž není řešitelná a není řešitelná i celá soustava.

Příklad:

Pomocí sčítací metody řešte soustavu lineárních diofantických rovnic.

$$4x + 9y = -3$$

$$7x + 3y + z = 1$$

Řešení:

Již víme, že musíme ověřit nutnou podmínku řešitelnosti u každé rovnice zvlášť. V první rovnici máme koeficienty 4, 9 a 0, kde největším společným dělitelem čísel 4 a 9 je číslo 1. Číslo 1 dělí číslo -3 a tak první rovnice je řešitelná. U druhé rovnice máme tři koeficienty 7, 3 a 1. Největší společný dělitel těchto čísel je číslo 1 a ta dělí číslo 1, tudíž je také řešitelná.

Nevíme ovšem, zda je řešitelná celá soustava a zatím nemáme žádnou teorii, která by to rozhodla. Ani známá Frobeniova věta, platná pro řešení soustav nad tělesem (např. tělesem reálných čísel), nám mnoho nepomůže.

Daná soustava je řešitelná nad tělesem reálných čísel právě tehdy, pokud $hod\begin{pmatrix}4 & 9 & 0\\ 7 & 3 & 1\end{pmatrix} = hod\left(\begin{array}{ccc|c}4 & 9 & 0 & 3\\ 7 & 3 & 1 & 1\end{array}\right)$ a to je splněné. Hodnost obou matic je rovna 2. Tímto víme, že soustava je řešitelná a bude mít jednu neznámou volitelnou. Soustava tedy má nekonečně mnoho řešení, jejichž souřadnicemi jsou reálná čísla. Vůbec ale není jasné, zda má celočíselná řešení.

Pokusíme se postupovat zatím bez teorie, jen s elementárními postupy. Najít řešení první diofantické rovnice je snadné. Je $4 \cdot (-2) + 9 \cdot 1 = 1$, takže po vynásobení číslem -3 máme $4 \cdot 6 + 9 \cdot (-3) = -3$ a nalezli jsme jedno řešení první rovnice soustavy

$$x_0 = 6, y_0 = -3.$$

Obecné řešení této rovnice pak je

$$x = 6 + 9t$$

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

Třetí souřadnici řešení určíme z druhé rovnice. Platí

$$z = 1 - 7x - 3y = 1 - 7 \cdot (6 + 9t) - 3 \cdot (-3 - 4t) = -32 - 51t.$$

Vidíme, že tentokrát má soustava lineárních diofantických rovnic nekonečně mnoho řešení v $\mathbb{Z}^3$, a to každou trojici celých čísel $[x, y, z]$, kde

$$x = 6 + 9t$$

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

$$z = -32 - 51t, t \in \mathbb{Z}.$$

V kapitole 2.1 Lineární diofantické rovnice se dvěma neznámými jsme si také uváděli způsob řešení s využitím kongruence. Vypočtěme si soustavu rovnic touto metodou.

Po sčítací metodě jsme dostali rovnici $17x + 3z = 6$. Nyní vyjádříme x z kongruence $17x \equiv 6\ (mod\ 3)$ a dosadíme do diofantické rovnice.

$$17x \equiv 6\ (mod\ 3)$$

$$2x \equiv 0\ (mod\ 3)$$

$$x = 0 + 3t, t \in \mathbb{Z}.$$

Dosadíme x do původní rovnice a vyřešíme

$$17(3t) + 3z = 6$$

$$51t + 3z = 6$$

$$3z = 6 - 51t$$

$$z = 2 - 17t, t \in \mathbb{Z}.$$

Vypočítáme y tak, že do první nebo druhé rovnice v soustavě rovnic dosadíme hodnoty x a z. Dosadíme do první rovnice:

$$4(3t) + 9y = -3$$

$$12t + 9y = -3$$

$$9y = -3 - 12t$$

Již vidíme, že opět nedostaneme celočíselné řešení. Můžeme říct, že sčítací metoda při výpočtu soustav lineárních diofantických rovnic není vhodná, i když by se určitě našel nějaký příklad, kde to využít lze.

Zkusme tento příklad vypočítat jinak. Z rovnice $4x + 9y = -3$ uhodneme jedno řešení:

$$x_0 = -3, y_0 = 1.$$

Pak je snadné zapsat obecné řešení první rovnice:

$$x = -3 + 9t$$

$$y = 1 - 4t, t \in \mathbb{Z}.$$

Dosadíme za x a za y do druhé rovnice a vyjádříme neznámou z:

$$7(-3 + 9t) + 3(1 - 4t) + z = 1$$

$$z = 1 + 21 - 3 - 63t + 12t = 19 - 51t, t \in \mathbb{Z}.$$

Řešením původní soustavy jsou všechny trojice $[x, y, z] \in \mathbb{Z}^3$, kde

$$x = -3 + 9t$$

$$y = 1 - 4t,$$

$$z = 19 - 51t, t \in \mathbb{Z}.$$

3.1.2 DOSAZOVACÍ METODA (SUBSTITUČNÍ)

U dosazovací metody se vyjádří jedna neznámá z jedné rovnice a dosadí do druhé rovnice. Případně pokud máme více rovnic, tak dosadíme do zbývajících rovnic, čímž se jedna neznámá vyloučí. Rovnice se upraví a pak se vyjádří další neznámá a dosazujeme do dalších rovnic pro vyloučení další neznámé. Takto postupujeme dál, dokud nedostaneme jednu rovnici o jedné neznámé.

Příklad:

Vypočítejte soustavu dvou rovnic pomocí dosazovací metody:

$$2x - y = 1$$

$$x + 3y + 4z = 11$$

Řešení:

Ověříme si nutnou podmínku řešitelnosti. V první rovnici největší společný dělitel čísel 2 a 1 je 1 a ta dělí 1. Rovnice je řešitelná. Další rovnice má koeficienty 1, 3 a 4 a ty mají také největšího společného dělitele 1. Číslo 1 dělí 11 a tak je rovnice také řešitelná. Zkusíme využít postup z předchozího příkladu, kdy jsme uhádli jedno řešení z první rovnice. Zde by to bylo velmi jednoduché: $x_0 = 1$ a $y_0 = 1$.

Obecné řešení první rovnice zapíšeme

$$x = 1 - t$$

$$y = 1 - 2t, t \in \mathbb{Z}.$$

Za *x* a za *y* dosadíme do druhé rovnice a vyjádříme neznámou *z*.

$$1 - t + 3(1 - 2t) + 4z = 11$$

$$1 - t + 3 - 6t + 4z = 11$$

$$4z = 7 + 7t$$

Nyní vidíme, že nemůžeme rovnou vypočítat *z*, protože to vychází jako zlomek a my potřebujeme celočíselné řešení. Pomůžeme si tím, že na rovnici $4z - 7t = 7$ opět díváme jako na diofantickou rovnici s neznámými *z*, *t*. Snadno uhodneme jedno její řešení

$$z_0 = 7, t_0 = 3.$$

Obecné řešení pak vyjde

$$z = 7 - 7u$$

$$t = 3 - 4u, u \in \mathbb{Z}.$$

Pak již snadno dopočteme

$$x = 1 - t = 1 - (3 - 4u) = -2 + 4u,$$

$$y = 1 - 2t = 1 - 2 \cdot (3 - 4u) = 1 - 6 + 8u = -5 + 8u, u \in \mathbb{Z}.$$

Poté můžeme provést zkoušku.

Nyní zkusme soustavu rovnic řešit dosazovací metodou. Nejlepší bude, když si z první rovnice vyjádříme neznámou y:

$$y = 2x - 1.$$

Tuto vyjádřenou neznámou dosadíme do druhé rovnice, a tak vyloučíme jednu neznámou. Rovnice bude ve tvaru

$$x + 3(2x - 1) + 4z = 11$$

a po úpravě

$$7x + 4z = 14.$$

Tato rovnice je lineární diofantická rovnice o dvou neznámých, kterou jsme se už naučili řešit. Rovnici můžeme řešit buď Euklidovým algoritmem, nebo kongruencí. My provedeme výpočet přes kongruenci.

Pomocí modulo 4 nahradíme neznámou *z* parametrem *t*.

$$7x \equiv 14 (mod\ 4)$$

Protože 7 dělí 14, pak lze obě strany rovnice vydělit číslem 7 a získáme tak rovnici

$$x \equiv 2 (mod\ 4).$$

Kongruenci upravíme na tvar rovnice

$$x = 2 + 4t, t \in \mathbb{Z}.$$

Tento tvar dosadíme do původní rovnice a dopočítáme neznámou *z*:

$$7(2+4t)+4z=14$$

$$14+28t+4z=14$$

$$4z=-28t$$

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

Nyní když známe hodnoty neznámých *x* a *z*, tak dosadíme do vyjádřené *y* a vypočítáme:

$$y=2x-1$$

$$y=2(2+4t)-1$$

$$y=3+8t,$$

kde $t\in\mathbb{Z}$. Řešením soustavy rovnic jsou celá čísla tvaru

$$x=2+4t$$

$$y=3+8t$$

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

Snadno ověříme, že množiny řešení nalezené oběma postupy jsou si rovny. K tomu stačí v prvním řešení položit $u=t+1$.

3.1.3 ŘEŠENÍ S VYUŽITÍM MATICOVÉ INTERPRETACE

Na úvod o soustavách lineárních diofantických rovnic jsme uvedli, že se taková soustava dá zapsat i pomocí matice. Nyní si ukážeme, jak můžeme aplikovat maticovou interpretaci pro soustavu rovnic

$$a_{11}x_1+a_{12}x_2+\cdots a_{1n}x_n=c_1$$

$$a_{21}x_1+a_{22}x_2+\cdots a_{2n}x_n=c_2$$

$$\vdots$$

$$a_{m1}x_1+a_{m2}x_2+\cdots a_{mn}x_n=c_m.$$

Matice, se kterou budeme pracovat, rozdělíme na levou a pravou část. Do levé části sepíšeme koeficienty rovnic do sloupců odpovídající matici transponované A^T. V části pravé se nachází jednotková matice vhodné velikosti, která bude sloužit k zápisu řádkových úprav prováděných na řádky matice soustavy.

$$\left(\begin{array}{ccc|cccc} a_{11} & \cdots & a_{m1} & 1 & 0 & \cdots & 0 \\ a_{12} & \cdots & a_{m2} & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & 1 \\ a_{1n} & \ldots & a_{mn} & 0 & 0 & \cdots & 1 \end{array}\right).$$

Matici vlevo redukujeme řádkovými úpravami. Spočítáme si největší společný dělitel $d = (a_{11}, \ldots, a_{1n})$ prvků v prvním sloupci a v tomto sloupci provádíme úpravy tak, abychom na místě prvku a_{11} měli $d = (a_{11}, \ldots, a_{1n})$ a pod ním nuly. Další sloupce upravujeme tak, abychom na levé straně dostali řádkově schodovitý tvar. Jelikož máme n řádků a m sloupců a pokud $m \leq n$, budeme mít o $n - m$ nulových řádků. Matici vlevo lze celočíselnými řádkovými úpravami převést na řádkově redukovaný tvar

$$\left(\begin{array}{ccc|cccc} d = (a_{11}, \ldots, a_{1n}) & \cdots & * & A_1 & A_2 & \cdots & A_n \\ 0 & \cdots & * & B_1 & B_2 & \cdots & B_n \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & & & \end{array}\right).$$

Pokud číslo $d = (a_{11}, \ldots, a_{1n})$ dělí pravou stranu řešené rovnice c_{11}, pak první řádek vynásobíme tak, abychom c_{11} dostali.

V dalších sloupcích to jednoduché není. V prvním řádku v prvním sloupci matice jsme už použili c_{11}. Nyní vypočítáme c_{22} pomocí prvního a druhého řádku v druhém sloupci. Pokud to bude možné, vynásobíme druhý řádek takovým číslem, abychom po sečtení prvků v druhém sloupci dostali c_{22}. Ve třetím sloupci a třetím řádku chceme dostat c_{33}. Třetí řádek vynásobíme takovým číslem, abychom po sečtení prvního, druhého a třetího řádku ve třetím sloupci tento prvek dostali. Takto pokračujeme dál. Pokud nebude možné získat tato čísla, pak soustava nemá řešení.

$$\left(\begin{array}{ccc|cccc} c_{11} & \cdots & * & A_{p1} & A_{p2} & \cdots & A_{pn} \\ 0 & c_{22} & * & B_{p1} & B_{p2} & \cdots & B_{pn} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & & & \end{array}\right).$$

Co se týče řešení, tak partikulární řešení hledáme v nenulových řádcích z levé části. Homogenní řešení zas v nulových řádcích. Řádky matic si označíme vektory $\vec{r_i}$, pro které platí $\overrightarrow{x_p} = \sum_{i=1}^{N} \vec{r_i}$. Pro obecné řešení soustavy bychom dostali vzorec $\overrightarrow{x_p} + \sum t_i \vec{r_i}$ pro $t_i \in \mathbb{Z}$. Pro ujasnění si vytvoříme algoritmus:

Algoritmus

Mějme soustavu lineárních homogenních rovnic $A\vec{x} = \vec{c}$, kde A je celočíselná matice $m \times n$ a $\vec{c} \in \mathbb{Z}$ a očekáváme, že dostaneme $\vec{x} \in \mathbb{Z}$.

1. Vytvoříme si matici $(A^T|E_n)$ a celočíselnými řádkovými úpravami ji převedeme do řádkově schodovitého tvaru $(D|S)$.

2. Celočíselným násobením řádků matice $(D|S)$ upravíme do tvaru $(B|R)$. Pro každé $j = 1, \dots, m$ je součet prvků ve sloupci j matice B roven c_j. Není-li toto možné, pak daná soustava řešení nemá.

3. Pokud platí krok 2., pak si označíme řádky matice R vektory $\vec{r_i}$. Bude platit

$$\overrightarrow{x_p} = \sum_{i=1}^{N} \vec{r_i}.$$

4. Nakonec obecné řešení dané soustavy je dáno vzorcem $\overrightarrow{x_p} + \sum t_i \vec{r_i}$ pro $t_i \in \mathbb{Z}$.

1. Příklad

Najděte obecná řešení soustavy rovnic

$$6k - 3l + 5m + 2n = 9$$

$$-3k - 12l + 7m + 8n = 21$$

Řešení:

Sestrojíme si matici, kterou budeme redukovat.

$$\left(\begin{array}{rr|cccc} 6 & -3 & 1 & 0 & 0 & 0 \\ -3 & -12 & 0 & 1 & 0 & 0 \\ 5 & 7 & 0 & 0 & 1 & 0 \\ 2 & 8 & 0 & 0 & 0 & 1 \end{array}\right)$$

Matici upravíme do řádkově schodovitého tvaru pomocí celočíselnými řádkovými operacemi. Nejprve zredukujeme první sloupec. Vybereme si nejmenší číslo v absolutní hodnotě a odečítáme vhodné násobky od ostatních řádků. V prvním sloupci tak získáme co nejmenší čísla.

$$\left(\begin{array}{rr|cccc} 0 & -27 & 1 & 0 & 0 & -3 \\ 1 & 4 & 0 & 1 & 0 & 2 \\ 1 & -9 & 0 & 0 & 1 & -2 \\ 2 & 8 & 0 & 0 & 0 & 1 \end{array}\right)$$

Nyní je nejmenším číslem 1 ve druhém a třetím řádku. Vidíme však, že druhý řádek je dvojnásobek čtvrtého řádku a proto vyrobíme nuly v prvním sloupci pomocí druhého řádku. Dostaneme matici

$$\left(\begin{array}{cc|cccc} 0 & -27 & 1 & 0 & 0 & -3 \\ 1 & 4 & 0 & 1 & 0 & 2 \\ 0 & -13 & 0 & -1 & 1 & -4 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right).$$

Teď budeme upravovat v druhém sloupci první a třetí řádek.

$$\left(\begin{array}{cc|cccc} 0 & -1 & 1 & -2 & 2 & -11 \\ 1 & 4 & 0 & 1 & 0 & 2 \\ 0 & -13 & 0 & -1 & 1 & -4 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 0 & -1 & 1 & -2 & 2 & -11 \\ 1 & 4 & 0 & 1 & 0 & 2 \\ 0 & 0 & -13 & 25 & -25 & 139 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right)$$

Nakonec zaměníme první řádek s druhým. Zůstali nám dva nenulové řádky, to znamená, že vznikne jeden generující vektor pro homogenní řešení.

$$\left(\begin{array}{cc|cccc} 1 & 4 & 0 & 1 & 0 & 2 \\ 0 & -1 & 1 & -2 & 2 & -11 \\ 0 & 0 & -13 & 25 & -25 & 139 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right)$$

Nyní budeme upravovat matici tak, abychom dostali v prvním sloupci výsledek 9. To znamená, že první řádek číslem 9 vynásobíme

$$\left(\begin{array}{cc|cccc} 9 & 36 & 0 & 9 & 0 & 18 \\ 0 & -1 & 1 & -2 & 2 & -11 \\ 0 & 0 & -13 & 25 & -25 & 139 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right).$$

V druhém sloupci potřebujeme dostat součet 21, takže druhý řádek vynásobíme číslem 15

$$\left(\begin{array}{cc|cccc} 9 & 36 & 0 & 9 & 0 & 18 \\ 0 & -15 & 15 & -30 & 30 & -165 \\ 0 & 0 & -13 & 25 & -25 & 139 \\ 0 & 0 & 0 & -2 & 0 & -3 \end{array}\right).$$

Vidíme, že první dva řádky v levé části jsou nenulové a tak dostáváme partikulární řešení

$$\overrightarrow{x_p} = (0, 9, 0, 18) + (15, -30, 30, -165) = (15, -21, 30, -147).$$

Přidružené homogenní rovnice jsou

$$\overrightarrow{x_h} = s(-13, 25, -25, 139) + t(0, -2, 0, -3).$$

Obecné řešení naší soustavy máme

$$k = 15 - 13s$$

$$l = -21 + 25s - 2t$$

$$m = 30 - 25s$$

$$n = -147 + 139s - 3t \text{ pro } s, t \in \mathbb{Z}.$$

Pokud provedeme zkoušku, pak zjistíme, že to tak vychází.

Tento postup se dříve používal a možná ještě dnes používá pro výpočet soustav lineárních diofantických rovnic. Jenže v nedávno vydané knize zvané Od Aritmetiky k abstraktní algebře jsem se dozvěděla jiný způsob řešení, kde počítání s maticemi by nebylo tak náročné. Počítání vychází z následující věty:

Věta 9:

Nechť máme celočíselnou matici $A = (a_{ij})$ typu $m \times n$. Nechť d je největší společný dělitel všech čísel (a_{ij}), kde $i = 1$ nebo $j = 1$, tj. prvků prvního řádku a prvního sloupce matice *A*. Potom existují matice *L* řádu *m* a *R* řádu *n* takové, že

$$B = LAR = (b_{ij}),$$

kde $b_{11} = d, b_{1j} = 0$ pro $2 \leq j \leq n$ a $b_{i1} = 0$ pro $2 \leq i \leq m$. Navíc det *L* = det *R* = 1, tj. *L* a *R* jsou tzv. unimodulární matice.

Ujasněme si pár pojmů, abychom plně pochopili tuto větu.

Lemma 3:

Nechť *a, b* jsou celá čísla a *d* je jejich největší společný dělitel. Pak existuje celočíselná matice *A* druhého řádu, pro kterou je det *A* = 1,

$$A\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}, \qquad \text{tj.} \qquad (a, b)A^T = (d, 0).$$

Definice 8: Determinant

Determinant matice *A* *n*-tého řádu ($n \in \mathbb{N}$) je součet $n!$ součinů *n* prvků vybraných tak, že z každého řádku a každého sloupce vybereme právě jeden prvek. Determinant matice *A* *n*-tého řádu označujeme

$$\Delta = \det A = \det\begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1}, & \dots, & a_{nn} \end{pmatrix} = \sum_{\pi \epsilon S_n} zn(\pi) \cdot a_{1r_1} \cdot a_{2r_2} \cdot \dots \cdot a_{nr_n},$$

kde sčítáme přes všechny permutace π množiny $1,2,\dots,n$. S_n je množina těchto permutací a značení $zn(\pi) = (-1)^k$ je znaménko permutace, kde k udává počet všech inverzí permutace π.

Definice 9: Unimodulární matice

Unimodulární maticí rozumíme čtvercovou matici s celočíselnými prvky, jejíž determinant je roven číslu 1 nebo -1.

Je zde také řečeno, že nemusíme využít celé tvrzení této věty, ale stačí použít matice L. Předveďme si to na příkladu.

2. Příklad

Ze soustavy lineárních rovnic najděte celočíselná řešení

$$7k - 4l + m + 20n = 17$$

$$2k + l + 3m + 9n = 5$$

$$-4k + 8l + 7m - 2n = -18.$$

Řešení:

Nejprve si tuto soustavu převedeme do matice, kterou budeme zatím řešit bez pravé strany. Máme ji ve tvaru $A\vec{x} = \vec{c}$

$$A = \begin{pmatrix} 7 & -4 & 1 & 20 \\ 2 & 1 & 3 & 9 \\ -4 & 8 & 7 & -2 \end{pmatrix}, \vec{c} = \begin{pmatrix} 17 \\ 5 \\ -18 \end{pmatrix}$$

Matici A budeme postupně násobit matici zleva unimodulární maticí L_1, tak abychom na místě a_{11} dostali číslo 1.

$$L_1 = \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$L_1 A = \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & -4 & 1 & 20 \\ 2 & 1 & 3 & 9 \\ -4 & 8 & 7 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -7 & -8 & -7 \\ 2 & 1 & 3 & 9 \\ -4 & 8 & 7 & -2 \end{pmatrix} = A_1$$

Pokračujeme unimodulární maticí L_2, díky které vynulujeme první sloupec kromě prvního členu:

$$L_2 A_1 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -7 & -8 & -7 \\ 2 & 1 & 3 & 9 \\ -4 & 8 & 7 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -7 & -8 & -7 \\ 0 & 15 & 19 & 23 \\ 0 & -20 & -25 & -30 \end{pmatrix} = A_2$$

Unimodulární maticí L_3 upravíme prostřední řádek, tak abychom další unimodulární maticí L_4 vynulovali člen a_{32}. Pokračujeme následovně:

$$L_3A_2 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & -7 & -8 & -7\\ 0 & 15 & 19 & 23\\ 0 & -20 & -25 & -30\end{pmatrix} = \begin{pmatrix}1 & -7 & -8 & -7\\ 0 & -5 & -6 & -7\\ 0 & -20 & -25 & -30\end{pmatrix} = A_3$$

a pak

$$L_4A_3 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -4 & 1\end{pmatrix}\begin{pmatrix}1 & -7 & -8 & -7\\ 0 & -5 & -6 & -7\\ 0 & -20 & -25 & -30\end{pmatrix} = \begin{pmatrix}1 & -7 & -8 & -7\\ 0 & -5 & -6 & -7\\ 0 & 0 & -1 & -2\end{pmatrix} = A_4$$

Pro lepší interpretaci si druhý a třetí řádek vynásobíme -1 unimodulární maticí L_5 abychom dostali kladná čísla.

$$L_5A_4 = \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}\begin{pmatrix}1 & -7 & -8 & -7\\ 0 & -5 & -6 & -7\\ 0 & 0 & -1 & -2\end{pmatrix} = \begin{pmatrix}1 & -7 & -8 & -7\\ 0 & 5 & 6 & 7\\ 0 & 0 & 1 & 2\end{pmatrix} = A_5$$

Vypočítáme součin unimodulárních matic $L = L_5L_4L_3L_2L_1$

$$L = \begin{pmatrix}1 & -3 & 0\\ -2 & 5 & -1\\ 4 & -8 & 3\end{pmatrix}.$$

Pokud jsme počítali správně, pak můžeme tuto matici *L* vynásobit zleva matici *A*.

Zbývá nám pravá strana soustavy rovnic, kterou převedeme do matice a tu pak zleva vynásobíme maticí L:

$$L\vec{c} = \begin{pmatrix}1 & -3 & 0\\ -2 & 5 & -1\\ 4 & -8 & 3\end{pmatrix}\begin{pmatrix}17\\ 5\\ -18\end{pmatrix} = \begin{pmatrix}2\\ 9\\ -26\end{pmatrix} = \overrightarrow{c_1}.$$

Dostáváme ekvivalentní soustavu rovnic z matice A_5 a $\overrightarrow{c_1}$ ve tvaru

$$k - 7l - 8m - 7n = 2$$

$$5l + 6m + 7n = 9$$

$$m + 2n = -26.$$

Nejprve si vezmeme rovnici $m + 2n = -26$, kde dostaneme obecné řešení pro

$$n = u \in \mathbb{Z}$$

a pak po dosazení a úpravě máme

$$m = -26 - 2u.$$

To dosadíme do druhé rovnice

$$5l + 6(-26 - 2u) + 7u = 9$$

$$5l - 156 - 12u + 7u = 9$$

$$5l - 5u = 165$$

$$l - u = 33.$$

Pokud l bude roven parametru t, pak si můžeme vyjádřit u a dosadit zpětně do n a m. Odtud platí:

$$l = t \in \mathbb{Z}, \quad u = n = l - 33 = t - 33$$

$$m = -26 - 2u = -26 - 2(t - 33) = 40 - 2t.$$

Nakonec tyto vypočtené hodnoty dosadíme do první rovnice a dopočteme neznámou k

$$k - 7t - 8(40 - 2t) - 7(t - 33) = 2$$

$$k - 7t - 320 + 16t - 7t + 231 = 2$$

$$k = 91 - 2t.$$

Dostali jsme obecné řešení soustavy, pro které platí:

$$k = 91 - 2t$$

$$l = t$$

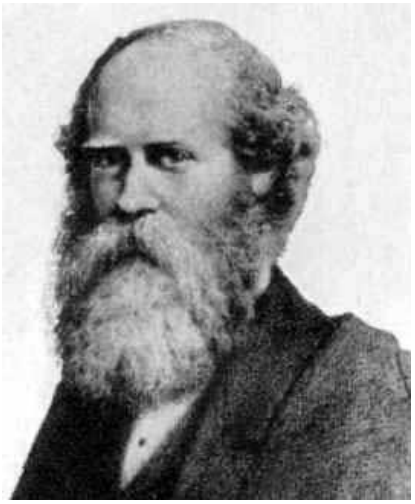
$$m = 40 - 2t$$

$$n = -33 + t, t \in \mathbb{Z}.$$

Správnost řešení zjistíme tak, že obecné řešení soustavy dosadíme do zadání soustavy lineárních rovnic. Celočíselné řešení najdeme například pro $t = 2$ dostáváme řešení $k = 87, l = 2, m = 36, n = -31$.

4 SMITHŮV NORMÁLNÍ TVAR MATICE

4.1 HENRY JOHN STEPHEN SMITH



Obrázek 1 – „H. J. S. Smith“, [1]

Henry John Stephen Smith se narodil 2. listopadu 1826 v irském Dublinu a zemřel 9. února 1883 v Oxfordu. Byl nejmladší ze čtyř dětí. Smith studoval v Oxfordu a v roce 1844 získal stipendium na Balliol College. Kvůli nemoci musel přerušit toto studium, ale bylo mu umožněno studovat na Sorbonně a ve Francii s některými z nejlepších matematiků. Poté, co se uzdravil, se vrátil do Oxfordu. V roce 1851 byl vysokoškolským matematickým učencem na univerzitě a stal se lektorem na Balliol. V roce 1860 byl jmenován profesorem geometrie v Oxfordu.

Smith byl ovlivněn Gaussem a jeho nejvýznamnějším příspěvkem v teorii čísel bylo, když pracoval v teorii elementárních dělitelů. Dokázal, že každé celé číslo může být rozloženo do součtu 5 čtverců a do součtu 7 čtverců. Kromě řešení těchto případů dal metodu, která udává počet způsobů, jak lze celé číslo vyjádřit jako součet k čtverců pro všechna pevná k. Své výsledky v řádech a rodech kvadratických formulářů obsahujících více než tři neurčitosti publikoval ve sborníku Královské společnosti v roce 1867. Předtím dokázal výsledek na 3 čtverce Eisenstein a Jacobi na 2, 4 a 6 čtverců.

Smithova matematická práce byla rozsáhlá a překlenula mnoho různorodých oblastí matematiky. V období 1859 – 1865 se věnoval práci v teorii čísel a jeho „Zpráva o teorii čísel“ obsahující pět částí je popisována jako nejkomplexnější a elegantní památka, která byla kdy postavena na teorii čísel. Smithova vlastní práce v teorii čísel a algebry byla velmi považována. V roce 1861 Smith prokázal existenci a jedinečnost toho, co nyní

nazýváme Smithovým normálním tvarem matice s celočíselnými prvky. První uplatnění tohoto výsledku bylo zjistit, kdy lineární diofantická rovnice má řešení. To nejprve studovali staří Řekové.

Smith také psal témata na geometrii, přičemž první dva dokumenty „Certain cubic and biquadratic problems“ („Určité krychlové a bivadratické problémy“) mu dopomohly získat Steiner cenu v Berlíně (1868).

Přispíval i k oboru matematická analýza, kde jeho práce nejsou dobře známé a plně doceněné. Sepsal článek „O integraci nespojitých funkcí“, ve které opravil chybu Riemannovy práce o teorii Riemannova integrálu.

Za svůj život získal řadu ocenění včetně čestných titulů z univerzit Cambridge a Dublinu. Byl i jmenován do dvou královských komisí. Dva měsíce po jeho smrti mu Academie věd udělila dvě ceny.

4.2 SMITHŮV NORMÁLNÍ TVAR MATICE

Symboly:

Z – obor celých čísel

$M_{m,n}(\mathbb{Z})$, $1 \leq m \leq n$ – obor všech celých čísel $m \times n$ matic

$SL_k(\mathbb{Z})$ – množina všech čtvercových matic $k \times k$ s celočíselnými položkami, který má determinant 1 nebo -1 (zvaná unimodulární matice)

$D = diag(d_1, d_2, \dots, d_m) \in M_{m,n}(\mathbb{Z})$ – diagonální matice, která má celé číslo d_i na místě (i, i) pro $i = 1, \dots, m$ a nuly jsou mimo diagonálu

Věta 10: Smithův normální tvar matice *A*

Nechť je matice *A* z oboru celých čísel $m \times n$ matic. Existuje $L \in SL_m(\mathbb{Z})$ a $R \in SL_n(\mathbb{Z})$ tak, že

$$LAR = D = diag(d_1, d_2, \dots, d_s, 0, \dots, 0),$$

kde $d_i > 0, i = 1, \dots, s$, a $d_i | d_{i+1}$, $i = 1, \dots, s-1$. *D* se nazývá Smithovým normálním tvarem matice *A*.

Příklad:

Řešte soustavu diofantických rovnic $A\vec{x} = \vec{c}$, kde

$$3x_1 + 2x_2 + 6x_3 = 7$$

$$-2x_1 - 4x_2 + x_3 = -4.$$

Řešení:

Soustavu rovnic převedeme do matic $A\vec{x} = \vec{c}$, kde

$$A = \begin{pmatrix} 3 & 2 & 6 \\ -2 & -4 & 1 \end{pmatrix}, \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \vec{c} = \begin{pmatrix} 7 \\ -4 \end{pmatrix}.$$

Postupnými elementárními řádkovými a sloupcovými úpravami matice A získáme řešení. Úpravy lze realizovat násobením matice A unimodulárními maticemi (definice unimodulární matice). Pokud budeme matici A násobit zprava, pak budeme tyto matice označovat písmeny R_i. Pokud budeme matici A násobit zleva, pak budeme tyto matice označovat písmeny L_i.

V prvním kroku bychom chtěli mít na pozici a_{11} získat číslo 1 pro lepší výpočet. To dostaneme vynásobením matice A unimodulární maticí zleva L_1 a tak se přičte druhý řádek k řádku prvnímu.

$$L_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$L_1 A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 & 6 \\ -2 & -4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 7 \\ -2 & -4 & 1 \end{pmatrix}$$

Tuto upravenou matici budeme unimodulární maticí R_2 násobit zprava, abychom vynulovali pozici a_{12}, ve tvaru:

$$R_2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Výslednou matici si označíme A_1.

$$AR_2 = \begin{pmatrix} 1 & -2 & 7 \\ -2 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 7 \\ -2 & -8 & 1 \end{pmatrix} = A_1$$

Dále budeme nulovat člen a_{13} tím, že budeme násobit unimodulární maticí zprava ve tvaru:

$$R_3 = \begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Násobíme-li tuto rovnici maticí R_3A_1, pak získáme

$$A_1R_3 = \begin{pmatrix} 1 & 0 & 7 \\ -2 & -8 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & -8 & 15 \end{pmatrix} = A_2.$$

V prvním řádku máme již vše vynulované, co jsme potřebovali. Dále budeme pokračovat druhým řádkem násobením unimodulární maticí zleva pro vynulování pozice a_{21}. Ta bude ve tvaru:

$$L_4 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Rovnice pak bude ve tvaru:

$$L_4A_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -2 & -8 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -8 & 15 \end{pmatrix} = A_3.$$

Ještě nám zbývá pozice a_{23} a tu vynulujeme postupně. Nejprve využijeme unimodulární matici zprava R_5 ve tvaru:

$$R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pak platí

$$A_3R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -8 & 15 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -8 & -1 \end{pmatrix} = A_4.$$

Vidíme, že jsme tuto pozici nevynulovali, tak musíme upravit pozici a_{22}unimodulární maticí zprava R_6, která je:

$$R_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -7 & 1 \end{pmatrix}.$$

Dále platí:

$$A_4R_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -8 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -7 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix} = A_5.$$

Nakonec použijeme unimodulární matici zprava R_7 ve tvaru

$$R_7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Poslední úprava pro vynulování pozice a_{23} bude vypadat takto:

$$A_5 R_7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} = A_6.$$

Jelikož na diagonále musí být čísla větší než nula, pak upravíme unimodulární maticí zleva

$$L_8 A_6 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Označme si

$$L = L_8 L_4 L_1 = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix}$$

a

$$R = R_2 R_3 R_5 R_6 R_7 = \begin{pmatrix} 1 & 23 & -26 \\ 0 & -13 & 15 \\ 0 & -7 & 8 \end{pmatrix}.$$

Když máme vypočtené *L* a *R*, pak můžeme dosadit do $D = LAR$:

$$D = LAR = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix} \begin{pmatrix} 3 & 2 & 6 \\ -2 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 23 & -26 \\ 0 & -13 & 15 \\ 0 & -7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Vidíme, že matice *D* vypadá jako diagonální matice, to znamená má nenulové prvky pouze v hlavní diagonále a jinde jsou nuly.

Původní soustava rovnic je ve tvaru $A\vec{x} = \vec{c}$. Vynásobením matice L zleva máme $LA\vec{x} = L\vec{c} = \vec{b}$, a máme označení $\vec{x} = R\vec{y}$ pro matici zprava. Pak platí $LA\vec{x} = LAR\vec{y} = D\vec{y} = \vec{b}$. Vypočítáme si součin $\vec{b} = L\vec{c} = \begin{pmatrix} 1 & 1 \\ -2 & -3 \end{pmatrix} \begin{pmatrix} 7 \\ -4 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$. Na výpočet $D\vec{y} = \vec{b}$ musíme dávat velký pozor, jak ovlivní pravou stranu provedené řádkové a sloupcové úpravy:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}.$$

Jde o soustavu $y_1 = 3, y_2 = -2, y_3 = t, t \in \mathbb{Z}$.

Nakonec

$$\vec{x} = R\vec{y} = \begin{pmatrix} 1 & 23 & -26 \\ 0 & -13 & 15 \\ 0 & -7 & 8 \end{pmatrix}\begin{pmatrix} 3 \\ -2 \\ t \end{pmatrix} = \begin{pmatrix} -43 - 26t \\ 26 + 15t \\ 14 + 8t \end{pmatrix}.$$

Správnost výpočtu provedeme zkouškou:

$$A\vec{x} = \begin{pmatrix} 3 & 2 & 6 \\ -2 & -4 & 1 \end{pmatrix}\begin{pmatrix} -43 - 26t \\ 26 + 15t \\ 14 + 8t \end{pmatrix} = \begin{pmatrix} 7 \\ -4 \end{pmatrix} = \vec{c}.$$

Věta 11.

Nechť *A, L, R, D* jsou ve větě 1, $\vec{c} \in \mathbb{Z}^n$a $\vec{b} = L\vec{c}$. Pak následující čtyři výroky jsou ekvivalentní:

a) Systém lineárních rovnic $A\vec{x} = \vec{c}$ má celočíselné řešení.

b) Systém lineárních rovnic $D\vec{y} = \vec{b}$ má celočíselné řešení.

c) Pro každý racionální vektor $\vec{u}$, kde $\vec{u}A$ představuje celé číslo vektoru, je číslo $\overrightarrow{uc}$ celé číslo.

d) Pro každý racionální vektor $\vec{v}$, kde $\vec{v}D$ představuje celé číslo vektoru, je číslo $\overrightarrow{vb}$ celé číslo.

Tvrzení 1.

Nechť $A \in M_{m,n}(\mathbb{Z})$ a $\vec{c} \in \mathbb{Z}^n$. Potom soustava lineárních rovnic $A\vec{x} = \vec{c}$ má řešení celé číslo tehdy a jen tehdy, když odpovídající systém kongruence $A\vec{x} = \vec{c}\ (mod\ n)$ má řešení pro každé celé kladné číslo *n*.

Příklad:

Řešte soustavu diofantických rovnic, kde

$$x_1 - 3x_2 + x_3 = 3$$

$$8x_1 - 2x_2 + x_3 = 5$$

$$5x_1 + 9x_2 - 4x_3 = 9.$$

Řešení:

Soustavu diofantických rovnic zapíšeme do matic, která je ve tvaru $A\vec{x} = \vec{c}$:

$$A = \begin{pmatrix} 1 & -3 & 1 \\ 8 & -2 & 1 \\ 5 & 9 & -4 \end{pmatrix}, \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \vec{c} = \begin{pmatrix} 3 \\ 5 \\ 9 \end{pmatrix}.$$

Matici *A* budeme upravovat unimoduálrními maticemi, abychom dostali diagonální matici *D*. Tu dostaneme provedením posloupností elementárními řádkovými a sloupcovými úpravami matice *A*.

Jelikož již známe postup z předchozího příkladu, budeme postupovat rychleji. Čísla -3 a 1 v prvním řádku se zbavíme tak, že přičteme trojnásobek prvního sloupce ke druhému sloupci a ke třetímu sloupci připočteme sloupec první vynásobený číslem -1. Použijeme unimodulární matici zprava, která bude vypadat:

$$R_1 = \begin{pmatrix} 1 & 3 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pak máme

$$AR_1 = \begin{pmatrix} 1 & -3 & 1 \\ 8 & -2 & 1 \\ 5 & 9 & -4 \end{pmatrix}\begin{pmatrix} 1 & 3 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & 22 & -7 \\ 5 & 24 & -9 \end{pmatrix} = A_1$$

Nyní se zbavíme z prvního sloupce čísla 8 a 5. To provedeme tak, že ke druhému řádku připočteme -8násobek prvního řádku a ke třetímu řádku -5násobek prvního řádku. Musíme použít unimodulární matici zleva, kterou vynásobíme s maticí A_1

$$L_2 = \begin{pmatrix} 1 & 0 & 0 \\ -8 & 1 & 0 \\ -5 & 0 & 1 \end{pmatrix}.$$

Platí

$$L_2A_1 = \begin{pmatrix} 1 & 0 & 0 \\ -8 & 1 & 0 \\ -5 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 8 & 22 & -7 \\ 5 & 24 & -9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 22 & -7 \\ 0 & 24 & -9 \end{pmatrix} = A_2.$$

Bylo by vhodné, kdybychom změnili pozici a_{22}. Číslo 22 nahradíme jedničkou tak, že ke druhému sloupci přičteme trojnásobek sloupce třetího. Proto unimodulární matice zprava je

$$R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}.$$

Pak

$$A_2R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 22 & -7 \\ 0 & 24 & -9 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & -3 & -9 \end{pmatrix} = A_3.$$

Dále vezmeme unimodulární matici zleva

$$L_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$$

a ověříme, že

$$L_4A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & -3 & -9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & 0 & -30 \end{pmatrix} = A_4.$$

Nakonec položíme

$$R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{pmatrix}$$

a dostáváme

$$A_4R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & 0 & -30 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -30 \end{pmatrix} = D.$$

Nalezli jsme Smithův normální tvar D matice A.

Označíme si

$$L = L_4\, L_2 = \begin{pmatrix} 1 & 0 & 0 \\ -8 & 1 & 0 \\ -29 & 3 & 1 \end{pmatrix}$$

a

$$R = R_1R_3R_5 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 7 \\ 0 & 3 & 22 \end{pmatrix}.$$

Musíme dávat pozor, v jakém pořadí násobíme matice.

Dále vypočítáme součin

$$\vec{b} = L\vec{c} = \begin{pmatrix} 1 & 0 & 0 \\ -8 & 1 & 0 \\ -29 & 3 & 1 \end{pmatrix}\begin{pmatrix} 3 \\ 5 \\ 9 \end{pmatrix} = \begin{pmatrix} 3 \\ -19 \\ -63 \end{pmatrix}.$$

Pro $D\vec{y} = \vec{b}$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -30 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -19 \\ -63 \end{pmatrix},$$

kde $y_1 = 3, y_2 = -19, -30 \cdot y_3 = -63$, zjišťujeme, že díky y_3 soustava nemá celočíselné řešení.

Kdybychom změnili v zadání vektor pravé strany na $\vec{c} = \begin{pmatrix} 3 \\ 7 \\ 6 \end{pmatrix}$, dostali bychom

$$\vec{b} = L\vec{c} = \begin{pmatrix} 1 & 0 & 0 \\ -8 & 1 & 0 \\ -29 & 3 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 7 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ -17 \\ -60 \end{pmatrix}.$$

Pro $D\vec{y} = \vec{b}$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -30 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -17 \\ -60 \end{pmatrix}$$

vychází $y_1 = 3, y_2 = -17, y_3 = 2$.

Nakonec

$$\vec{x} = R\vec{y} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 7 \\ 0 & 3 & 22 \end{pmatrix} . \begin{pmatrix} 3 \\ -17 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ -3 \\ -7 \end{pmatrix},$$

Dostáváme jediné řešení soustavy pro$x_1 = 1, x_2 = -3, x_3 = -7$. Správnost výpočtu můžeme provést zkouškou, kdy vynásobíme matici A s hledaným $\vec{x}$ a musí vyjít $\vec{c}$. Nebo soustavu rovnic zadáme do programu Mathematica.

Zadáme-li soustavu rovnic v tomto tvaru:

$\text{Solve}[x - 3y + z == 3\&\&8x - 2y + z == 5\&\&5x + 9y - 4z == 9, \{x, y, z\}, \text{Integers}]$,

pak program to vypočítá takto {}. To znamená, že soustava nemá řešení.

Pokud zadáme upravenou soustavu rovnic s pravou stranou do programu:

$\text{Solve}[x - 3y + z == 3\&\&8x - 2y + z == 7\&\&5x + 9y - 4z == 6, \{x, y, z\}, \text{Integers}]$,

dostáváme řešení $\{\{x \to 1, y \to -3, z \to -7\}\}$, které je v souladu s výpočty.

ZÁVĚR

V diplomové práci jsme získali teoretické znalosti o lineárních diofantických rovnicích a jejich soustavách a také o Smithovo normálním tvaru matic. Osvojili jsme si určité početní metody a na základě toho vypočítali příklady.

Práce je rozdělena do čtyř kapitol, které jsou dále členěny na podkapitoly. V první kapitole je krátce popsána historie Diofanta z Alexandrie a jeho díla. Kapitola druhá pojednává o lineárních diofantických rovnicích a je rozdělena do dvou podkapitol. V první se zabýváme lineárními diofantickými rovnicemi se dvěma neznámými a v druhé podkapitole o více neznámých. V této kapitole si uvádíme potřebnou teorii a následně názorné příklady řešené různými metodami.

Ve třetí kapitole se věnujeme soustavám lineárních diofantických rovnic a jejich způsobům řešení. Následně v podkapitolách se věnujeme způsobům řešení metodou sčítací, dosazovací a řešení s využitím maticové interpretace.

Poslední kapitola je zaměřena na Smithův normální tvar matice, kde v první podkapitole sepisujeme krátce život Henryho Johna Stephena Smitha. V druhé podkapitole se zabýváme teorií Smithova normálního tvaru matice dokončená příklady.

RESUMÉ

This Diploma thesis is folows the teoretical knowledge about linear diofantic equations and their systems, as well as about Smith's normal form of a matrix.

The thesis is divided into four chapters and chapters are subdivided into subchapters. The first chapter briefly described the history of Mr. Diofante from Alexandria and his works. The second chapter deals with linear deiofantic equations and is divided into two subchapters. In the first we deal with linear diofantic equations with two unknowns and in the second subchapter with more unknowns.

In the third chapter is deals with the systems of linear diofantic equations and their solution. Is made focus on methods of adding, settling and solving solutions using matrix interpretation in next subchapters.

The last chapter is focused on Smith's normal shape of the matrix. The first subchapter is briefly describe life of Mr. Henry John Stephen Smith. The theory of Smith's normal form of a matrix of completed examples is described in last subchapters.

SEZNAM LITERATURY

[1] BAYLOR.edu. Copyright © Baylor® University. 11. 2. 2010, online: http://www.baylor.edu/math/news.php?action=story&story=68917

[2] BICAN, Ladislav. *Lineární algebra a geometrie*. Vyd. 2. Praha: Academia, 2009. ISBN 978-80-200-1707-9.

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

[4] BULANT, Michal. *Algebra 2 – Teorie čísel*. Brno: Masarykova univerzita, 2008, online: http://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-screen.pdf

[5] ČADEK, Martin; Vokřínek, Lukáš. *Lineární algebra a geometrie III*, Brno, 2016, online: http://www.math.muni.cz/~koren/LA3.pdf

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

[7] DLAB, Vlastimil a Jindřich BEČVÁŘ. *Od aritmetiky k abstraktní algebře*. Praha: vydali V. Dlab a J. Bečvář vlastním nákladem, 2016. ISBN 978-80-260-9838-6.

[8] DRÁBEK, Jaroslav. *Základy elementární aritmetiky pro učitelství 1. stupně ZŠ*. Praha: Státní pedagogické nakladatelství, 1985. Učebnice pro vysoké školy (Státní pedagogické nakladatelství).

[9] HABALA, Petr. *Diskrétní matematika*, 2. Dělitelnost - 2016, online: https://math.feld.cvut.cz/habala/teaching/dma/dmkni02.pdf

[10] HABALA, Petr. *Diskrétní matematika*, 3a. Kongruence, počítání modulo - 2016, online: https://math.feld.cvut.cz/habala/teaching/dma/dmkni03.pdf

[11] HABALA, Petr. *Diskrétní matematika*, 4a. Diofantické rovnice - 2016, online: https://math.feld.cvut.cz/habala/teaching/dma/dmkni04.pdf

[12] HAVEL, V. a J. HOLENDA. *Lineární algebra*. Praha: SNTL - Nakladatelství technické literatury, 1984. Učebnice pro vysoké školy.

[13] HENRY John Stephen Smith. JOC/EFR© February 1999, online: http://www-groups.dcs.st-and.ac.uk/history/Biographies/Smith.html

[14] HORA, Jaroslav. *Algebra I.* Vyd. 1. Plzeň: Pedagogická fakulta v Plzni, 1991. ISBN 80-7043-030-3.

[15] HORA, Jaroslav. *Soustavy lineárních diofantickýh rovnic a Smithův normální tvar matice*. Plzeň : South Bohemia Mathematical Letters, 2011.

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

[17] KALA, Víťa. *Diofantické rovnice*, online: https://mks.mff.cuni.cz/library/DiofantickeRovniceVK/DiofantickeRovniceVK.pdf

[18] KRYČ, Jiří. *Diplomová práce:* Vybrané kapitoly z elementární algebry. Plzeň: Západočeská univerzita, 2013. Vedoucí práce: Mgr. Lukáš Honzík.

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

[20] PLHÁK, Jan. *Bakalářská práce:* Algoritmy pro výpočet Smithova normálního tvaru. Brno: Masarykova univerzita, 2015. Vedoucí práce: Bc. Lukáš Vokřínek, PhD.

[21] STEINSDÖRFER, Jan. *Studijní text:* Metody řešení diofantických rovnic. Ústí nad Labem: Univerzita Jana Evangelisty Purkyně, 2015.

[22] VELÍŠKOVÁ, Barbora. *Bakalářská práce:* Soustavy lineárních rovnic nad okruhy. Plzeň: Západočeská univerzita, 2014. Vedoucí práce: Mgr. Martina Kašparová, Ph.D.

[23] WILLERS, Michael. *Algebra bez (m)učení: od arabských matematiků k tajným šifrám: matematika v každodenním životě: fascinující čísla a rovnice*. 1. vyd. Praha: Grada, 2012. ISBN 978-80-247-4123-9.

ZDROJE OBRÁZKŮ A PROGRAMŮ

Obrázky:

[1] HENRY John Stephen Smith. JOC/EFR© February 1999, online:
http://www-groups.dcs.st-and.ac.uk/history/Biographies/Smith.html

Programy:

[2] GeoGebra. © 2017 International GeoGebra Institute, online:
http://www.geogebra.org

[3] WolframAlpha. © 2017 Wolfram Alpha LLC, online:
http://www.wolframalpha.com

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

Grafy:

Obrázky:

Tabulky:

PŘÍLOHY

CD s diplomovou prací ve formátu PDF