Univerzita Jana Evangelisty Purkyně v Ústí nad Labem

Přírodovědecká fakulta

Metody řešení diofantických rovnic

STUDIJNÍ TEXT

Vypracoval: Jan Steinsdörfer

Ústí nad Labem 2015

Obsah

Úvod

Diofantickou rovnicí rozumíme jakoukoliv rovnici tvaru

$$P(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

kde $P(x_1, x_2, \ldots, x_n)$ je polynom n proměnných x_1, x_2, …, x_n s celočíselnými koeficienty. Vyřešit rovnici (1) znamená najít všechny n-tice x_1, x_2, …, x_n, kde x_i jsou celá čísla, pro $i = 1, 2, \ldots, n$, která této rovnici vyhovují.

David Hilbert v roce 1900 představil seznam 23 nevyřešených matematických problémů, kterými by se matematikové měli ve 20. století zabývat. Jeden z nich, tzv. desáty Hilbertův problém se týkal nalezení algoritmu, který by rozpoznal, zda má rovnice (1) řešení. Tento problém negativně řeší Matijaševičova věta[1)] z roku 1970, ze které již snadno vyplývá: *„Neexistuje algoritmus, který by rozhodl, zda daná diofantická rovnice má řešení.“* Důsledkem této věty je, že neexistuje univerzální metoda, pomocí níž bychom našli řešení libovolné diofantické rovnice.

Proto se musíme pokusit nalézt algoritmy, které řeší alespoň nějaké speciální případy rovnice (1).

Cílem práce je vytvoření studijního textu, který se bude zabývat přesným teoretickým odvozením metod řešení některých typů diofantických rovnic.

Teoretický výklad je doprovázen mnoha příklady, ať už se jedná o řešení nějaké konkrétní rovnice či příklad pro ujasnění nově definovaného pojmu. V textu je také několik cvičení k samostatnému vyřešení s výsledky uvedenými na konci textu. Všechna cvičení a řešené příklady jsou autorova.

Text neobsahuje žádné slovní úlohy, které jsou velmi často s tématem diofantické rovnice spojovány. Slovním úlohám, vedoucím na lineární diofantické rovnice o dvou neznámých, je věnována diplomová práce [11].

[1)] Přesné znění a důkaz čtenář nalezne v [1, kapitola 23].

V práci jsou až nezvykle podrobně prováděny důkazy vět za účelem úplné srozumitelnosti pro čtenáře. Proto jsem naprostou většinu důkazů a pomocných vět v celém textu vypracoval sám nebo s pomocí vedoucího práce.

Práce je určena především vysokoškolským studentům, kteří se o tuto problematiku zajímají. Některé části práce by byly přístupné také nadaným studentům středních škol.

Kapitola 1

Vznik diofantických rovnic

Diofantické rovnice jsou pojmenované podle řeckého starověkého matematika Diofanta z Alexandrie. Bohužel o něm víme jen velmi málo, neboť se nezachovaly žádné přímé životopisné údaje.

Zcela bezpečně se jeho život dá zadařit mezi roky 150 př. n. l. – 350 n. l., vše ostatní jsou jen spekulace, nicméně se odhaduje, že žil v letech 200 – 284 n. l. Ikdyž nevíme, kdy přesně žil, je známa jeho délka života, která je řešením početního rébusu, který si nechal vytesat na náhrobek. Ve volném překladu zní asi takto:

„Bůh mu dopřál, aby byl hochem šestinu svého života a přidav k této době dvanáctinu, ozdobil jeho líce vousem. Po další sedmině prozářil jeho život světlem manželství, po dalších pěti letech pak daroval mu syna. Však běda, sotva ubohé dítě dosáhlo polovinu délky otcova života, neúprosné sudičky vzaly si jej zpět. Když bůh utěšil jeho hoře učením o číslech, po dalších čtyřech letech ukončil dobu jeho života.“

Rébus vede na rovnici

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x.$$

Její řešení je $x = 84$. Víme tedy, že žil 84 let a měl syna.

Diofantos bývá často označován jako *„otec algebry“*. Podstatnou část života strávil v Alexandrijské knihovně. Jeho nejvýznamější spis se jmenuje *Aritmetika*. Jde o spis třinácti knih, ve kterých sepsal vše, co se v té době vědělo o řešení lineárních a kvadratických rovnic. Bohužel se dochovalo pouze šest knih a čtyři se časem nalezly v arabských překladech. Jeho spis společně s Euklidovým spisem *Základy* se staly základním kamenem pro studium matematiky po celý středověk.

Zabýval se rovnicemi typu

$$ax + by = c,$$

kde a, b, c jsou kladné celé konstanty a proměnné x, y mají být také kladná celá čísla. Připouštěl tedy jen kladné celočíselné řešení, neboť ještě neznal záporná čísla ani nulu. Například rovnici

$$8x + 20 = 4$$

nazýval absurdní, protože vede na záporné, tzn. nesmyslné, řešení.

Protože byl první, kdo se zabýval jen celočíselným řešením rovnic (navíc kladným), jsou po něm tyto rovnice pojmenovány jako *diofantické* nebo *diofantovské rovnice*.[1)] Dnes ovšem při řešení těchto rovnic připouštíme celočíselné řešení.[2)]

[1)] Ve starší literatuře je možno narazit na pojmenování *neurčité rovnice*.

[2)] Více o historii antické matematiky například viz [10, str. 34 – 69].

Kapitola 2

Diofantické rovnice o jedné neznámé

Kapitolu Diofantické rovnice o jedné neznámé zde uvádím pouze pro úplnost. Mnohem větší význam pro nás budou mít diofantické rovnice o více neznámých. V této kapitole vycházím především z [3, kapitola 1], v druhé části kapitoly využívám poznatků o polynomech z [4, kapitola 1.3 a 3.10].

Nejprve si zadefinujme pojem dělitelnost, se kterým se mnohokrát setkáme.

Definice 2.1. *Nechť a, b jsou celá čísla. Budeme říkat, že číslo a dělí číslo b právě tehdy, když existuje celé číslo k tak, že platí*

$$b = k \cdot a.$$

Tuto skutečnost budeme symbolicky zapisovat

$$a \mid b.$$

V opačném případě budeme říkat, že číslo a nedělí číslo b a psát $a \nmid b$.

Začněme řešit nejjednodušší případ diofantické rovnice o jedné neznámé a sice lineární.

Definice 2.2. *Lineární diofantickou rovnicí o jedné neznámé budeme rozumět každou rovnici ve tvaru*

$$a_1 x + a_0 = 0, \tag{2.1}$$

kde x je neznámá, a_1, a_0 jsou celá čísla, $a_1 \neq 0$.

Ptáme se, kdy bude řešení rovnice (2.1) tvaru

$$x = -\frac{a_0}{a_1}$$

celým číslem. To bude právě tehdy, když číslo a_0 bude dělitelné číslem a_1, neboli $a_1 \mid a_0$. To ovšem podle definice 2.1 znamená, že $a_0 = k \cdot a_1$, kde k je celé číslo. Potom je

$$x = -\frac{k \cdot a_1}{a_1} = -k$$

řešení rovnice (2.1).

Příklad 2.1. $3x - 27 = 0$

Jelikož platí, že $3 \mid 27$, má rovnice řešení v celých číslech a sice $x = 9$.

Příklad 2.2. $5x + 21 = 0$

Protože $5 \nmid 21$, nemá rovnice celočíselné řešení.

Přejděme nyní od lineární rovnice hned k rovnici n-tého stupně.

Definice 2.3. *Diofantickou rovnicí n-tého stupně o jedné neznámé budeme rozumět každou rovnici ve tvaru*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0, \tag{2.2}$$

kde x je neznámá, a_n, $a_{n-1}, \ldots, a_1$, a_0 jsou celá čísla, $a_n \neq 0$, n je kladné celé číslo.

Budeme hledat řešení rovnice (2.2). Všimněme si, že volbou $n = 1$ obdržíme přesně rovnici (2.1). Uvažujme tedy rovnici (2.2) pro $n \geq 2$. Nechť celé číslo c je řešením této rovnice. Pak musí platit, že

$$\begin{aligned} a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c + a_0 &= 0 \\ a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c &= -a_0 \\ c \cdot (-a_n c^{n-1} - a_{n-1} c^{n-2} - \ldots - a_1) &= a_0. \end{aligned}$$

Podle definice 2.1 z poslední rovnosti plyne, že $c \mid a_0$. Tedy každý celočíselný kořen rovnice (2.2) musí dělit absolutní člen a_0 této rovnice. Je ovšem důležité si uvědomit, jestliže nějaké celé číslo z dělí absolutní člen rovnice (2.2), tak to neznamená, že z je kořenem. Uvažujme například kvadratickou rovnici $x^2 + 5x + 6 = 0$. Víme, že pokud

má kvadratická rovnice v reálných číslech řešení, pak jsou řešení dvě[1)], pro tento konkrétní příklad jsou to čísla -3 a -2. Ovšem podmínka $c \mid a_0$ nám nedává pouze tato dvě čísla, ale množinu čísel $\{-6,\ -3,\ -2,\ -1,\ 1,\ 2,\ 3,\ 6\}$. Tedy podmínka $c \mid a_0$ nám vlastně určuje pouze množinu potenciálních kořenů, označme ji $\mathbb{M}$ a platí

$$\mathbb{M} = \{m \in \mathbb{Z}; m \mid a_0\}. \tag{2.3}$$

Řešením rovnice (2.2) jsou potom taková $m \in \mathbb{M}$, která po dosazení do (2.2) dávají identitu[2)].

Příklad 2.3. $x^5 - 2x^4 + 2x^3 - 4x^2 + x - 2 = 0$

Množina potenciálních kořenů je $\mathbb{M} = \{-2,\ -1,\ 1,\ 2\}$. Po dosazení prvků množiny $\mathbb{M}$ do naší rovnice dostáváme identitu pouze pro číslo 2. Tedy číslo 2 je jediný celočíselný kořen.

Příklad 2.4. $x^4 + 2x^2 + 1 = 0$

Množinou potenciálních kořenů je dvouprvková množina $\mathbb{M} = \{-1,\ 1\}$. Po dosazení těchto prvků do zadané rovnice ovšem nikdy nedostaneme identitu. Rovnice tedy nemá žádný celočíselný kořen.

Co kdyby v (2.2) bylo $a_0 = 0$? Pak by množina potenciálních kořenů $\mathbb{M}$ z (2.3) byla rovna množině všech celých čísel $\mathbb{Z}$, neboť všechna celá čísla dělí nulu. Tím bychom tedy nic nezískali. Jak v takovém případě postupovat si ukážeme na příkladě.

Příklad 2.5. $3x^5 - 5x^3 + 2x = 0$

V takovém případě můžeme vytknout x a dostáváme

$$x \cdot (3x^4 - 5x^2 + 2) = 0.$$

Odtud pak máme, že musí být

$$x = 0 \quad \vee \quad 3x^4 - 5x^2 + 2 = 0,$$

[1)] Dvojnásobný kořen bereme jako dvě řešení.

[2)] Tuto identitu je výhodné ověřit pomocí Hornerova schématu, např. viz [7, kapitola 4.6.4.]

tím máme jedno řešení $x = 0$ a ve druhé rovnici už máme nenulový absolutní člen a postupujeme stejně jako v předchozích příkladech. Tedy $\mathbb{M} = \{-2,\ -1,\ 1,\ 2\}$. Po dosazení dostáváme identitu pro 1 a -1. Řešením rovnice jsou čísla: $0,\ 1,\ -1$.

Obecněji, budou-li čísla $a_0, a_1, \ldots, a_k$ v (2.2) rovna nule a $a_{k+1} \neq 0$, kde k je celé číslo, $0 \leq k < n$, tak vytknutím x^{k+1} dostaneme

$$x^{k+1} \cdot (a_n x^{n-(k+1)} + \cdots + a_{k+1}) = 0,$$

odkud máme jedno řešení $x = 0$ a zbývající řešení získáme řešením rovnice

$$a_n x^{n-(k+1)} + \cdots + a_{k+1} = 0,$$

kde už máme číslo a_{k+1} nenulové a můžeme k řešení použít výše uvedený postup.

Jistě bychom teď byli schopni vyřešit jakoukoliv diofantickou rovnici n-tého stupně o jedné neznámé. Je jasné, že bude-li mít číslo a_0 v rovnici (2.2) mnoho dělitelů, tak bude množina $\mathbb{M}$ obsahovat velký počet prvků, my pak musíme všechny tyto prvky otestovat, zda jsou kořeny či nikoliv. Například uvažujme rovnici

$$3x^4 + 21x^3 + 28x^2 - 14x - 20 = 0,$$

množina potenciálních kořenů této rovnice je $\mathbb{M} = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 5,\ \pm 10,\ \pm 20\}$, museli bychom tedy dosazením testovat 12 čísel, což je pro ruční počítání jistě nepohodlné. Následující věta nám dá jiný návod jak nalézt celočíselné kořeny diofantické rovnice n-tého stupně o jedné neznámé. Nejprve jedno lemma.

Lemma 2.1. *Nechť n je kladné celé číslo. Nechť A, B jsou čísla. Platí*

$$A^n - B^n = (A - B) \cdot \sum_{0 \leq i \leq n-1} A^{n-1-i} B^i.$$

Důkaz.

Identitu dokážeme přímým výpočtem.

$$\begin{aligned}
(A - B) \cdot \sum_{0 \leq i \leq n-1} A^{n-1-i} B^i &= A \cdot \sum_{0 \leq i \leq n-1} A^{n-1-i} B^i - B \cdot \sum_{0 \leq i \leq n-1} A^{n-1-i} B^i \\
&= \sum_{0 \leq i \leq n-1} A^{n-i} B^i - \sum_{0 \leq i \leq n-1} A^{n-1-i} B^{i+1} \\
&= A^n + \sum_{1 \leq i \leq n-1} A^{n-i} B^i - B^n - \sum_{0 \leq i \leq n-2} A^{n-1-i} B^{i+1} \\
&= A^n - B^n + \sum_{1 \leq i \leq n-1} A^{n-i} B^i - \sum_{1 \leq j \leq n-1} A^{n-j} B^j \\
&= A^n - B^n
\end{aligned}$$

□

Věta 2.1. *Nechť $f(x)$ je polynom n-tého stupně s celočíselnými koeficienty a celé číslo c je kořenem tohoto polynomu. Pak pro libovolné celé číslo m platí*

$$(c-m) \mid f(m).$$

Důkaz.

Nechť $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, kde a_i je celé číslo, pro všechna $i = 1, 2, \ldots, n$. Protože c je kořen polynomu $f(x)$, platí

$$0 = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0. \tag{2.4}$$

Dále je

$$f(m) = a_n m^n + a_{n-1}m^{n-1} + \cdots + a_1 m + a_0. \tag{2.5}$$

Odečtěme rovnost (2.5) od rovnosti (2.4).

$$-f(m) = a_n(c^n - m^n) + a_{n-1}(c^{n-1} - m^{n-1}) + \cdots + a_1(c-m)$$

V této rovnosti lze podle lemmatu 2.1 z každé závorky na pravé straně vytknou $c-m$.

$$-f(m) = (c-m)\left[a_n \sum_{0\le i\le n-1} c^{n-1-i}m^i + a_{n-1} \sum_{0\le i\le n-2} c^{n-2-i}m^i + \cdots + a_1\right]$$

$$f(m) = (c-m)\left[-a_n \sum_{0\le i\le n-1} c^{n-1-i}m^i - a_{n-1} \sum_{0\le i\le n-2} c^{n-2-i}m^i - \ldots - a_1\right]$$

Odtud máme $(c-m) \mid f(m)$. □

Při hledání řešení rovnice (2.2) budeme postupovat takto:

(I) Stanovíme množinu potenciálních kořenů $\mathbb{M}$ podle (2.3).

(II) Zvolíme si celé číslo m, $m \neq 0$, a stanovíme množinu $\mathbb{M}_m$ následujícím způsobem:

$$\mathbb{M}_m = \{z \in \mathbb{Z}; z \mid f(m)\}$$

(III) Vytvoříme množinu $\mathbb{M}'_m$ takto:

$$\mathbb{M}'_m = \{z + m; z \in \mathbb{M}_m\}$$

(VI) Uděláme průnik $\mathbb{M} \cap \mathbb{M}'_m$.

Pokud by náhodou zvolené číslo m bylo jedno z celočíselných řešení, tak by množina $\mathbb{M}_m$ z bodu (II) výše uvedeného postupu byla rovna množině všech celých čísel, neboť bude-li m řešením, je $f(m) = 0$ a platí, že každé celé číslo dělí nulu. Výsledkem průniku $\mathbb{M} \cap \mathbb{M}'_m$ by pak byla množina $\mathbb{M}$ a tím bychom nic nezískali. V takovém případě si buď můžeme vytvořit jinou volbou m nové množiny $\mathbb{M}_m$, $\mathbb{M}'_m$, nebo dosadit m do Hornerova schématu, které nám dá polynom, který vznikne z podílu polynomů $f(x)$ a $x - m$ a na něm pak můžeme celý proces opakovat.

Pokud ovšem číslo m nebude celočíselným řešením, pak průnik $\mathbb{M} \cap \mathbb{M}'_m$ již bude obsahovat méně prvků než množina $\mathbb{M}$. Musíme pak testovat menší počet čísel než na počátku.[3)]

Často je výhodné volit m rovno 1 a -1, neboť

$$f(1) = \sum_{0 \le i \le n} a_i \qquad f(-1) = \sum_{0 \le i \le n} (-1)^i a_i.$$

Ukažme si výše uvedený postup na příkladě.

Příklad 2.6. $3x^4 + 21x^3 + 28x^2 - 14x - 20 = 0$

Volme např. $m = 1$, potom je $f(1) = 18$.

(I) $\mathbb{M} = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 5,\ \pm 10,\ \pm 20\}$

(II) $\mathbb{M}_1 = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm 9,\ \pm 18\}$

(III) $\mathbb{M}'_1 = \{-17,\ -8,\ -5,\ -2,\ -1,\ 0,\ 2,\ 3,\ 4,\ 7,\ 10,\ 19\}$

(IV) $\mathbb{M} \cap \mathbb{M}'_1 = \{-5,\ -2,\ -1,\ 2,\ 4,\ 10\}$

Je vidět, že došlo k výraznému zjednodušení, místo dvanácti kandidátů na celočíselný kořen máme již pouze šest. Zkusme tuto množinu ještě zúžit tak, že postup provedeme ještě pro $m = -1$, $f(-1) = 4$, kde ovšem místo původní $\mathbb{M}$ použijeme již zúženou množinu získanou v bodu (IV).

(I) $\mathbb{M} \cap \mathbb{M}'_{-1} = \{-5,\ -2,\ -1,\ 2,\ 4,\ 10\}$

(II) $\mathbb{M}_{-1} = \{\pm 1,\ \pm 2,\ \pm 4\}$

[3)] Ne vždy tento postup musí být výhodnější, neboť sestavení množin $\mathbb{M}_m$, $\mathbb{M}'_m$ může být také pracné pokud číslo $f(m)$ má mnoho dělitelů.

(III) $\mathbb{M}'_{-1} = \{-5, -3, -2, 0, 1, 3\}$

(IV) $\mathbb{M} \cap \mathbb{M}'_1 \cap \mathbb{M}'_{-1} = \{-5, -2\}$

Po dosazení zjistíme, že obě tato čísla jsou celočíselnými kořeny.

Zde je několik příkladů na procvičení.

Cvičení 2.1. Vyřešte následující diofantické rovnice.

(a) $3x^3 - x^2 - 2 = 0$

(b) $15x^4 + 61x^3 + 47x^2 - 5x - 6 = 0$

(c) $x^3 - 4x^2 + 5x - 2 = 0$

(d) $3x^3 - x^2 + 3x - 1 = 0$

Kapitola 3

Lineární diofantické rovnice o dvou neznámých

V této kapitole budeme řešit často se vyskytující typ diofantické rovnice, který bývá spojován se slovními úlohami. Proto se jím budeme detailně zabývat a ukážeme si hned více různých metod řešení.

Při sepisování této kapitoly jsem vycházel hlavně ze zdrojů [3, kapitola 2], [2, kapitola 2,4,5 a 6].

Definice 3.1. *Lineární diofantickou rovnicí o dvou neznámých nazveme každou rovnici ve tvaru*

$$ax + by + c = 0, \tag{3.1}$$

kde x,y jsou neznámé, a, b, c jsou celá čísla, $a \neq 0$, $b \neq 0$.

Řešení rovnice (3.1) můžeme rozdělit na čtyři případy:

(I) $a > 0$, $b > 0$

(II) $a > 0$, $b < 0$

(III) $a < 0$, $b > 0$

(IV) $a < 0$, $b < 0$

Uvědomme si, že stačí vyřešit pouze případ (I), neboť budeme-li řešit (IV), pak stačí rovnici (3.1) vynásobit číslem -1 a tím dojde k převedení na (I). Problémy (II) a (III) jsou symetrické, tak nám stačí vyřešit například jen (II). Budeme-li uvažovat

případ (II), tak substitucí $y = -z$ opět dochází k převedení na případ (I), kde vyřešíme rovnici pro neznámé x, z s kladnými koeficienty a na závěr se stačí vrátit k substituci. Od této chvíle uvažujeme rovnici (3.1) pro $a > 0$, $b > 0$.

Definice 3.2. *Nechť a, b jsou kladná celá čísla. Budeme říkat, že kladné celé číslo d je největším společným dělitelem čísel a, b právě tehdy, když platí:*

(I) $d \mid a \wedge d \mid b$,

(II) *pro všechna kladná celá e platí:* $(e \mid a \wedge e \mid b) \Rightarrow e \mid d$.

Skutečnost, že d je největším společným dělitelem čísel a, b budeme zapisovat

$$d = gcd(a, b).$$

Pokud platí pouze (I)*, nazýváme číslo d společným dělitelem čísel a, b.*

Rozšířený Euklidův algoritmus

Čtenář se pravděpodobně již setkal s Euklidovým algoritmem na výpočet největšího společného dělitele dvou kladných celých čísel. Nyní uvedeme rozšířenou verzi tohoto algoritmu, který nám mnohokrát v tomto textu poslouží jako nástroj, například pro důkaz některé z vět nebo pro řešení lineárních diofantických rovnic o dvou neznámých.[1)]

Jsou-li dána dvě kladná celá čísla a, b, $a > b$, algoritmus vypočte jejich největšího společného dělitele $d = gcd(a, b)$ a současně najde dvě celá čísla α, β, pro která platí

$$a\alpha + b\beta - d = 0. \tag{3.2}$$

Podívejme se na jednotlivé kroky tohoto algoritmu:

E1: [**Inicializace.**] Přiřaďte $\alpha' \leftarrow \beta \leftarrow 1$, $\alpha \leftarrow \beta' \leftarrow 0$, $\gamma \leftarrow a$, $d \leftarrow b$.

E2: [**Dělení.**] Nechť q a r jsou po řadě neúplný podíl a zbytek po dělení γ číslem d. (To znamená, že $\gamma = qd + r$, $0 \leq r < d$.)

E3: [**Je zbytek nulový?**] Pokud je $r = 0$, algoritmus končí, v tom případě je $a\alpha + b\beta - d = 0$.

[1)] S návodem k důkazu správnosti rozšířeného Euklidova algoritmu se čtenář může seznámit např. v [6, str. 13-17].

E4: [**Nový cyklus.**] Přiřaďte $\gamma \leftarrow d$, $d \leftarrow r$, $t \leftarrow \alpha'$, $\alpha' \leftarrow \alpha$, $\alpha \leftarrow t - q\alpha$, $t \leftarrow \beta'$, $\beta' \leftarrow \beta$, $\beta \leftarrow t - q\beta$ a jděte zpět na krok E2.

Definice 3.3. *Rovnost* (3.2) *se nazývá Bezoutova rovnost a číslům* α, β *říkáme Bezoutovy koeficienty.*

Příklad 3.1. Najděte největšího společného dělitele d čísel 1729, 551 a najděte čísla α, β tak, aby

$$1769\alpha + 551\beta - d = 0.$$

Průběh algoritmu zaznamenáme následující tabulkou.

α'	α	β'	β	γ	d	q	r
1	0	0	1	1769	551	3	116
0	1	1	−3	551	116	4	87
1	−4	−3	13	116	87	1	29
−4	5	13	−16	87	29	3	0

Tedy $d = 29$, $\alpha = 5$, $\beta = -16$ a skutečně platí, že

$$1769 \cdot 5 + 551 \cdot (-16) - 29 = 0.$$

Tento algoritmus hned využijeme v důkazu následujícího lemmatu, na které se budeme mnohokrát v textu odvolávat.

Lemma 3.1. *Nechť* a, b, c *jsou kladná celá čísla. Jestliže* $gcd(a, b) = 1$ *a zároveň* $a \mid bc$, *pak* $a \mid c$.

Důkaz.
Protože $gcd(a, b) = 1$, rozšířený Euklidův algoritmus nám pro čísla a, b nalezne celá čísla α, β a platí

$$a\alpha + b\beta - 1 = 0$$

$$ac\alpha + bc\beta - c = 0.$$

Dle předpokladů $a \mid bc$, to podle definice 2.1 znamená, že existuje kladné celé číslo k a platí $bc = ka$.

$$ac\alpha + ak\beta - c = 0$$

$$a(c\alpha + k\beta) = c$$

Z poslední rovnosti vidíme, že $a \mid c$. □

Podívejme se nejprve na otázku řešitelnosti rovnice (3.1). Intuitivně asi tušíme, že bude mít celočíselné řešení pouze za nějaké podmínky. O ní hovoří následující věta.

Věta 3.1. *Nechť je dána rovnice* (3.1). *Nechť* $d = gcd(a, b)$. *Rovnice* (3.1) *má celočíselné řešení právě tehdy, když* $d \mid c$.

Důkaz.

Protože věta je vyslovená ve formě ekvivalence, budeme muset dokázat dvě věci:

(I) Jestliže má rovnice (3.1) celočíselné řešení, pak $d \mid c$.

(II) Jestliže $d \mid c$, pak má rovnice (3.1) řešení v celých číslech.

ad(I) Označme x_0, y_0 celočíselné řešení rovnice (3.1); pak platí

$$ax_0 + by_0 + c = 0.$$

Protože $d = gcd(a, b)$ existují celá čísla a_1, b_1 tak, že $a = a_1 d$, $b = b_1 d$. Potom

$$a_1 d x_0 + b_1 d y_0 + c = 0$$
$$d \cdot (-a_1 x_0 - b_1 y_0) = c.$$

Odtud musí $d \mid c$, což jsme chtěli dokázat.

ad(II) Protože $d \mid c$, existuje celé číslo c_1 tak, že $c = c_1 d$. Vezměme koeficienty a, b z rovnice (3.1) a aplikujme na ně rozšířený Euklidův algoritmus. Ten nám najde celá čísla α, β tak, že je splněná následující Bezoutova rovnost

$$a\alpha + b\beta - d = 0.$$

Nyní získanou rovnost vynásobíme číslem c_1 a dostáváme

$$a\alpha c_1 + b\beta c_1 - dc_1 = 0$$
$$a\alpha c_1 + b\beta c_1 - c = 0$$
$$a(-\alpha c_1) + b(-\beta c_1) + c = 0.$$

Porovnáním s rovnicí (3.1) obdržíme

$$x_0 = -\alpha c_1 \qquad y_0 = -\beta c_1$$

a to je nějaké celočíselné řešení, které jsme měli najít. Tím je tedy celý důkaz proveden. □

Věta 3.1 má velmi zajímavý důsledek. Bude-li $d = gcd(a, b) = 1$, bude mít rovnice (3.1) vždy celočíselné řešení, neboť vždy platí, že $1 \mid c$ pro všechna c. Navíc každou celočíselně řešitelnou rovnici (to podle věty 3.1 znamáná, že $d \mid c$) lze vydělit číslem d a tedy převést na případ, kdy už máme $gcd(a, b) = 1$.

Definice 3.4. *Budeme říkat, že rovnice* (3.1) *je v základním tvaru právě tehdy, když* $gcd(a, b) = 1$.

Příklad 3.2. $2x + 4y + 7 = 0$

Protože $gcd(2, 4) = 2$ a $2 \nmid 7$, nemá tato rovnice řešení v celých číslech.

Příklad 3.3. $3x + 8y - 5 = 0$

Rovnice má celočíselné řešení, neboť $gcd(3, 8) = 1$ a platí, že $1 \mid -5$.

Někdy se pro praktické použití může hodit také následující věta, která plyne z věty 3.1.

Věta 3.2. *Nechť je dána rovnice* (3.1). *Nechť je dáno kladné celé číslo* e *takové, že* $e \mid a$, $e \mid b$. *Jestliže* $e \nmid c$, *pak nemá rovnice* (3.1) *celočíselné řešení.*

Důkaz.
Dokážeme obměnu věty: Jestliže má rovnice (3.1) celočíselné řešení, pak $e \mid c$. To je ovšem (I) z důkazu věty 3.1, kde nyní neuvažujeme největšího společného dělitele, ale pouze společného dělitele čísel a, b. □

Příklad 3.4. $2586x + 4210y + 2361 = 0$

Tato rovnice nemá podle věty 3.2 řešení v celých číslech, neboť koeficienty u neznámých jsou sudá čísla, mají tedy společného dělitele 2, ovšem číslo 2361 je liché a tedy není dělitelné 2.

Věta 3.3. *Nechť je rovnice* (3.1) *dána v základním tvaru. Nechť celá čísla* x_0, y_0 *jsou nějakým řešením této rovnice. Pak celá čísla* x, y *jsou také řešením této rovnice právě tehdy, když*

$$x = x_0 - bt \qquad y = y_0 + at, \tag{3.3}$$

kde t *je celé číslo.*

Důkaz.

Věta je opět vyslovená ve formě ekvivalence, musíme tedy dokázat následující:

(I) Jestliže $x = x_0 - bt$ a $y = y_0 + at$, kde x_0, y_0 je celočíselné řešení rovnice (3.1), t je celé číslo, pak x, y je také řešení.

(II) Jestliže x, y je celočíselné řešení rovnice (3.1), pak

$$x = x_0 - bt \qquad y = y_0 + at,$$

kde t je celé číslo.

ad(I) Chceme ověřit, že čísla tvaru x, y jsou řešením rovnice (3.1), dosaďme a počítejme.

$$\begin{aligned} ax + by + c &= a(x_0 - bt) + b(y_0 + at) + c \\ &= ax_0 - abt + by_0 + abt + c \\ &= ax_0 + by_0 + c \\ &= 0 \end{aligned}$$

Poslední rovnost plyne z toho, že x_0, y_0 je řešení.

ad(II) Víme, že x_0, y_0 a x, y jsou řešení rovnice (3.1), platí tedy rovnosti

$$ax + by + c = 0 \qquad ax_0 + by_0 + c = 0.$$

Odečtěme druhou rovnost od první a počítejme.

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ b(y - y_0) &= a(x_0 - x) \end{aligned} \tag{3.4}$$

Protože uvažujeme rovnici (3.1) v základním tvaru, tj. $gcd(a, b) = 1$, musí podle lemmatu 3.1 $b \mid (x_0 - x)$. To opět podle definice 2.1 znamená, že existuje celé číslo t tak, že platí $x_0 - x = bt$. Odtud máme

$$x = x_0 - bt.$$

Dosazením bt za $x_0 - x$ do rovnice (3.4) obdržíme

$$\begin{aligned} y - y_0 &= \frac{a}{b}\, bt \\ y - y_0 &= at \\ y &= y_0 + at. \end{aligned}$$

□

Rád bych zdůraznil důležitost této věty. Říká, že nám vlastně stačí nalézt pouze jedno libovolné řešení rovnice (3.1) v základním tvaru a ihned známe všechna další řešení této rovnice a jsou tvaru (3.3).

Nyní si zvlášť vyřešíme případ $a = b$. Pokud budou oba koeficienty stejné, lze rovnici (3.1), za předpokladu že má řešení, převést na tvar

$$x + y + e = 0,$$

kde e je celé číslo, pro které platí $c = a \cdot e$. Řešení této rovnice je velice snadné, stačí zvolit jednu neznámou, např. y, jako celočíselný parametr, $y = t$, kde t je celé číslo a druhou neznámou dopočítat. Celkem

$$x = -e - t \qquad y = t.$$

Stačí nám už vyřešit případ, kdy $a > b$. Speciálně ještě může nastat, že $b = 1$, pak ovšem řešíme rovnici

$$ax + y + c = 0.$$

Řešení této rovnice je opět jednoduché;

$$x = t \qquad y = -c - at,$$

kde t je celé číslo.

Budeme se tedy zabývat rovnicemi, kde bude $a > b > 1$.

3.1 Metoda řešení rozšířeným Euklidovým algoritmem

Využijeme nám již známý rozšířený Euklidův algoritmus. Ještě jednou pro přehled připomenu, co je naším úkolem.

Chceme vyřešit rovnici

$$ax + by + c = 0, \tag{3.5}$$

kde a, b, c jsou celá čísla, $a > b > 1$.

Aplikujme rozšířený Euklidův algoritmus na koeficienty a a b. Výsledkem bude Bezoutova rovnost

$$a\alpha + b\beta - d = 0, \tag{3.6}$$

kde α, β jsou celá čísla, $d = gcd(a, b)$. Nyní se rozhodne o tom, zda má rovnice celočíselné řešení podle toho, jestli $d \mid c$. Pokud tomu tak nebude, nemá podle věty 3.1 rovnice řešení v celých číslech. Pokud naopak bude platit $d \mid c$, bude existovat celé číslo k tak, že $c = kd$. Obdrženou rovnost (3.6) budeme chtít porovnat s rovnicí (3.5), musíme jí proto vynásobit číslem $-k$ a dostáváme

$$a(-k\alpha) + b(-k\beta) + kd = 0$$
$$a(-k\alpha) + b(-k\beta) + c = 0.$$

Odtud porovnáním s rovnicí (3.5) vidíme jedno celočíselné řešení

$$x_0 = -k\alpha \qquad y_0 = -k\beta.$$

K popisu všech řešení využijeme větu 3.3. Jejím předpokladem je ovšem nesoudělnost koeficientů stojících u neznámých. Musíme je proto vydělit jejich největším společným dělitelem d a dostáváme všechna řešení rovnice (3.5) tvaru

$$x = -k\alpha - \frac{b}{d}t \qquad y = -k\beta + \frac{a}{d}t,$$

kde t je celé číslo.

Pokud bude rovnice (3.5) v základním tvaru, tzn. $d = 1$, pak řešením této rovnice jsou čísla tvaru

$$x = -c\alpha - bt \qquad y = -c\beta + at,$$

kde t je celé číslo.

Ukažme si tento postup na konkrétních příkladech.

Příklad 3.5. $25x + 17y + 4 = 0$

Dle návodu aplikujme rozšířený Euklidův algoritmus na čísla 25, 17. Průběh algoritmu budeme vždy zaznamenávat tabulkou.

α'	α	β'	β	γ	d	q	r
1	0	0	1	25	17	1	8
0	1	1	−1	17	8	2	1
1	−2	−1	3	8	1	8	0

Spočítali jsme, že $\alpha = -2$ a $\beta = 3$; dostáváme tak následující Bezoutovu rovnost

$$25(-2) + 17 \cdot 3 - 1 = 0,$$

kterou stačí už jen vynásobit číslem -4.

$$25 \cdot 8 + 17(-12) + 4 = 0$$

Našli jsme jedno celočíselné řešení

$$x_0 = 8 \qquad y_0 = -12,$$

což nám podle věty 3.3 stačí k tomu, abychom popsali všechna další řešení a sice

$$x = 8 - 17t \qquad y = -12 + 25t,$$

kde t je celé číslo.

Příklad 3.6. $1025x - 241y - 26 = 0$

Protože koeficient u neznámé y je záporný, musíme zavést substituci $y = -z$ a dostáváme tak rovnici

$$1025x + 241z - 26 = 0,$$

kde už ale máme oba koeficienty kladné a můžeme na ně aplikovat rozšířený Euklidův algoritmus.

α'	α	β'	β	γ	d	q	r
1	0	0	1	1025	241	4	61
0	1	1	−4	241	61	3	58
1	−3	−4	13	61	58	1	3
−3	4	13	−17	58	3	19	1
4	−79	−17	336	3	1	3	0

Dostáváme tak Bezoutovu rovnost

$$1025(-79) + 241 \cdot 336 - 1 = 0,$$

kterou nám stačí vynásobit číslem 26.

$$1025(-2054) + 241 \cdot 8736 - 26 = 0$$

Vidíme, že

$$x_0 = -2054 \qquad z_0 = 8736,$$

a podle věty 3.3

$$x = -2054 - 241t \qquad z = 8736 + 1025t.$$

Musíme se ale vrátit k substituci $y = -z$, abychom našli řešení původní rovnice. Celkem

$$x = -2054 - 241t \qquad y = -8736 - 1025t,$$

kde t je celé číslo.

Příklad 3.7. $136x + 85y - 187 = 0$

Opět provedeme rozšířený Euklidův algoritmus pro koeficienty 136, 85.

α'	α	β'	β	γ	d	q	r
1	0	0	1	136	85	1	51
0	1	1	−1	85	51	1	34
1	−1	−1	2	51	34	1	17
−1	2	2	−3	34	17	2	0

Dostáváme Bezoutovu rovnost

$$136(2) + 85(-3) - 17 = 0 \tag{3.7}$$

a vidíme, že $gcd(136, 85) = 17$. Musíme zjistit, zda má rovnice celočíselné řešení, musí platit, že $17 \mid 187$, což platí, neboť $187 = 11 \cdot 17$. Rovnost (3.7) musíme násobit číslem 11.

$$136(22) + 85(-33) - 187 = 0$$

Jedním řešením jsou čísla $x_0 = 22$, $y_0 = -33$. Abychom popsali všechna řešení, musíme použít větu 3.3, ovšem předpoklad této věty je, že $gcd(a, b) = 1$, což v našem

příkladě nemáme. Musíme proto čísla 136, 85 vydělit jejich největším společným dělitelem, tj. 17 a dostáváme čísla 8, 5. Tedy všechna řešení jsou tvaru

$$x = 22 - 5t \qquad y = -33 + 8t,$$

kde t je celé číslo.

Cvičení 3.1. Pomocí rozšířeného Euklidova algoritmu vyřešte následující rovnice:

(a) $27x - 34y - 5 = 0$

(b) $-51x - 221y - 85 = 0$

(c) $2432x + 237y + 3 = 0$

(d) $65x + 156y + 11 = 0$

3.2 Metoda řešení řetězovým zlomkem

Ukažme si jiný způsob vyřešení rovnice (3.5). Tuto metodu budeme používat tehdy, bude-li rovnice (3.5) v základním tvaru, nebo dokážeme-li jí snadno na tento tvar převést, tzn. že na první pohled budeme znát $gcd(a,\, b)$, nebo si ho dokážeme rychle spočítat, např. pomocí rozkladu na prvočísla. Pak ihned dokážeme rozhodnout o řešitelnosti této rovnice a pokud bude mít řešení, dokážeme rovnici vydělením číslem $gcd(a,b)$ převést na základní tvar.

Postupujme obdobně jak je tomu v [3, kapitola 2]. Na příkladu provedeme motivační výpočet a následně si všechny úvahy teoreticky vysvětlíme s využitím některých poznatků o tzv. kontinuantech z [7, str. 356–359]. Proč při výpočtu následujícího příkladu postupujeme právě takto, nebude komentováno, ikdyž se některé úpravy na první pohled mohou jevit podivně.

Uvažujme rovnici $37x + 24y - 5 = 0$. Proveďme následující úpravy s poměrem koeficientů:

$$\begin{aligned}
\frac{37}{24} &= 1 + \frac{13}{24} = 1 + \cfrac{1}{\cfrac{24}{13}} \\
&= 1 + \cfrac{1}{1 + \cfrac{11}{13}} = 1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{13}{11}}} \\
&= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{11}}} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{11}{2}}}} \\
&= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2}}}}
\end{aligned}$$

Výraz, který jsme obdrželi, nazýváme řetězovým zlomkem. Odstraňme z něj jednu

polovinu a zpětně dopočítejme zlomek jednoduchý.

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5}}}=1+\cfrac{1}{1+\cfrac{1}{\frac{6}{5}}}=1+\cfrac{1}{1+\frac{5}{6}}=1+\cfrac{1}{\frac{11}{6}}=1+\frac{6}{11}=\frac{17}{11}$$

Získaný zlomek odečteme od původního poměru koeficientů.

$$\frac{37}{24}-\frac{17}{11}=\frac{407-408}{24\cdot 11}=\frac{-1}{24\cdot 11}$$

Získanou rovnost upravujme:

$$37\cdot 11+24\cdot(-17)=-1$$
$$37\cdot 11+24\cdot(-17)+1=0$$
$$37\cdot(-55)+24\cdot 85-5=0$$

Porovnáme-li poslední rovnost se zadanou rovnicí, vidíme, že

$$x_0=-55 \qquad y_0=85$$

a opět podle věty 3.3 jsou všechna řešení tvaru

$$x=-55-24t \qquad y=85+37t,$$

kde t je celé číslo.

Zaveďme si matematický aparát potřebný k obecnému popisu úvodního příkladu.

Definice 3.5. *Konečným řetězovým zlomkem budeme rozumět výrazy tvaru*

$$x_1+\cfrac{y_1}{x_2+\cfrac{y_2}{x_3+\cfrac{y_3}{\ldots\cfrac{}{x_{n-1}+\cfrac{y_{n-1}}{x_n}}}}}, \tag{3.8}$$

kde n je kladné celé číslo.

Definice 3.6. *Kanonickým nebo regulérním řetězovým zlomkem nazveme výraz* (3.8)*, kde pro všechna y_i, $i=1,\ 2,\ \ldots,\ n-1$, platí, že $y_i=1$.*

Pro zjednodušení zápisu kanonických řetězových zlomků si zaveďme následující značení

$$x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\cdots \cfrac{}{x_{n-1} + \cfrac{1}{x_n}}}}} = //x_1, x_2, \ldots, x_n//.$$

Například můžeme psát:

$$\begin{aligned} //x_1// &= x_1 \\ //x_1, x_2// &= x_1 + \frac{1}{x_2} = \frac{x_1x_2 + 1}{x_2} \\ //x_1, x_2, x_3// &= x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3}} = \frac{x_1x_2x_3 + x_1 + x_3}{x_2x_3 + 1} \end{aligned} \tag{3.9}$$

Definice 3.7. *Je dán kanonický řetězový zlomek $//x_1, x_2, \ldots, x_n//$. Nechť k je kladné celé číslo, $k \leq n$. Pak k-tým sblíženým zlomkem ke kanonickému řetězovému zlomku $//x_1, x_2, \ldots, x_n//$ rozumíme zlomek*

$$//x_1, x_2, \ldots, x_k//.$$

Značíme $\delta_k(//x_1, x_2, \ldots, x_n//)$.

Uveďme si pro ujasnění několik příkladů, pro $n \geq 3$:

$$\begin{aligned} \delta_1(//x_1, x_2, \ldots, x_n//) &= //x_1// = x_1 \\ \delta_2(//x_1, x_2, \ldots, x_n//) &= //x_1, x_2// = \frac{x_1x_2 + 1}{x_2} \\ \delta_3(//x_1, x_2, \ldots, x_n//) &= //x_1, x_2, x_3// = \frac{x_1x_2x_3 + x_1 + x_3}{x_2x_3 + 1} \end{aligned} \tag{3.10}$$

Ještě si uvědomme, že

$$\delta_n(//x_1, x_2, \ldots, x_n//) = //x_1, x_2, \ldots, x_n//.$$

Kanonický řetězový zlomek lze také definovat následujícím rekurentním vzorcem

$$//x_1, x_2, \ldots, x_n, x_{n+1}// = //x_1, x_2, \ldots, x_{n-1}, x_n + \frac{1}{x_{n+1}}//, \tag{3.11}$$

kde $//x_1// = x_1$.

Definice 3.8. *Definujme kontinuanty $K_n(x_1, x_2, \ldots, x_n)$ v n proměnných, $n \geq 0$, předpisem:*

$$K_n(x_1, x_2, \ldots, x_n) = \begin{cases} 1, & n = 0 \\ x_1, & n = 1 \\ x_n K_{n-1}(x_1, x_2, \ldots, x_{n-1}) + K_{n-2}(x_1, x_2, \ldots, x_{n-2}), & n > 1 \end{cases}$$

Opět několik příkladů:

$$\begin{aligned} K_0 &= 1 \\ K_1(x_1) &= x_1 \\ K_1(x_2) &= x_2 \\ K_2(x_1, x_2) &= x_2 K_1(x_1) + K_0 = x_2 x_1 + 1 \\ K_2(x_2, x_3) &= x_3 K_1(x_2) + K_0 = x_3 x_2 + 1 \\ K_3(x_1, x_2, x_3) &= x_3 K_2(x_1, x_2) + K_1(x_1) = x_3 x_2 x_1 + x_3 + x_1 \end{aligned} \tag{3.12}$$

Zkoumejme rovnosti (3.10) a (3.12); zjistíme, že

$$\begin{aligned} \delta_1(//x_1, x_2, \ldots, x_n//) &= \frac{K_1(x_1)}{K_0} \\ \delta_2(//x_1, x_2, \ldots, x_n//) &= \frac{K_2(x_1, x_2)}{K_1(x_2)} \\ \delta_3(//x_1, x_2, \ldots, x_n//) &= \frac{K_3(x_1, x_2, x_3)}{K_2(x_2, x_3)}. \end{aligned}$$

Vyvstává nyní otázka, zda je

$$\delta_k(//x_1, x_2, \ldots, x_n//) = \frac{K_k(x_1, x_2, \ldots, x_k)}{K_{k-1}(x_2, x_3, \ldots, x_k)}?$$

Věta 3.4. *Nechť je dán kanonický řetězový zlomek $//x_1, x_2, \ldots, x_n//$. Dále nechť k je kladné celé číslo takové, že $k \leq n$. Sblížený zlomek $\delta_k(//x_1, x_2, \ldots, x_n//)$ lze vyjádřit následujícím podílem dvou kontinuantů*

$$\delta_k(//x_1, x_2, \ldots, x_n//) = \frac{K_k(x_1, x_2, \ldots, x_k)}{K_{k-1}(x_2, x_3, \ldots, x_k)}. \tag{3.13}$$

Důkaz.

Dohodněme se, že budeme pro stručnost místo $\delta_k(//x_1, x_2, \ldots, x_n//)$ psát pouze δ_k. Větu dokážeme pomocí matematické indukce vzhledem ke k.

(I) Dokážeme, že rovnost (3.13) platí pro $k = 1$, tj. že

$$\delta_1 = \frac{K_1(x_1)}{K_0}$$

(II) Budeme předpokládat, že rovnost (3.13) platí pro celé číslo k, $1 \leq k < n$ a dokážeme, že platí také pro $k+1$.

ad(I) To už jsme dokázali výše, při porovnávání rovnic (3.10) a (3.12).

ad(II) Dokážeme, že platí:

$$\delta_{k+1} = \frac{K_{k+1}(x_1, x_2, \ldots, x_{k+1})}{K_k(x_2, x_3, \ldots, x_{k+1})}$$

Dle indukčního předpokladu věta platí pro k, můžeme tedy psát

$$\delta_k = \frac{K_k(x_1, x_2, \ldots, x_k)}{K_{k-1}(x_2, x_3, \ldots, x_k)} = \frac{x_k K_{k-1}(x_1, \ldots, x_{k-1}) + K_{k-2}(x_1, \ldots, x_{k-2})}{x_k K_{k-2}(x_2, \ldots, x_{k-1}) + K_{k-3}(x_2, \ldots, x_{k-2})}.$$

Druhá rovnost je pouze rozepsání kontinuantů podle definice 3.8. Musíme dát ovšem pozor, toto rozepsání můžeme použít jen v případě, že bude $k \geq 3$, viz definici 3.8. Než budeme pokračovat, musíme ještě navíc dokázat platnost věty pro $k = 2$ a pro $k = 3$. To jsme už ale udělali, viz porovnávání rovnic (3.10) a (3.12).

Nyní je důležité si uvědomit, jak získáme sblížený zlomek δ_{k+1}, když známe δ_k. Pomocí rovnosti 3.11 lze psát

$$\delta_{k+1}(//x_1, x_2, \ldots, x_n//) = //x_1, x_2, \ldots, x_{k+1}// = //x_1, x_2, \ldots, x_k + \frac{1}{x_{k+1}}//.$$

Takže sblížený zlomek δ_{k+1} získáme z δ_k tak, že ve výrazu pro δ_k nahradíme proměnnou x_k výrazem $x_k + \frac{1}{x_{k+1}}$, pak dostáváme:

$$\delta_{k+1} = \frac{\left(x_k + \dfrac{1}{x_{k+1}}\right) K_{k-1}(x_1, \ldots, x_{k-1}) + K_{k-2}(x_1, \ldots, x_{k-2})}{\left(x_k + \dfrac{1}{x_{k+1}}\right) K_{k-2}(x_2, \ldots, x_{k-1}) + K_{k-3}(x_2, \ldots, x_{k-2})}$$

Získaný zlomek rozšíříme výrazem x_{k+1}.

$$\begin{aligned}
\delta_{k+1} &= \frac{x_k x_{k+1} K_{k-1}(x_1, \ldots, x_{k-1}) + K_{k-1}(x_1, \ldots, x_{k-1}) + x_{k+1} K_{k-2}(x_1, \ldots, x_{k-2})}{x_k x_{k+1} K_{k-2}(x_2, \ldots, x_{k-1}) + K_{k-2}(x_2, \ldots, x_{k-1}) + x_{k+1} K_{k-3}(x_2, \ldots, x_{k-2})} = \\
&= \frac{x_{k+1}\left(x_k K_{k-1}(x_1, \ldots, x_{k-1}) + K_{k-2}(x_1, \ldots, x_{k-2})\right) + K_{k-1}(x_1, \ldots, x_{k-1})}{x_{k+1}\left(x_k K_{k-2}(x_2, \ldots, x_{k-1}) + K_{k-3}(x_2, \ldots, x_{k-2})\right) + K_{k-2}(x_2, \ldots, x_{k-1})} = \\
&= \frac{x_{k+1} K_k(x_1, \ldots, x_k) + K_{k-1}(x_1, \ldots, x_{k-1})}{x_{k+1} K_{k-1}(x_2, \ldots, x_k) + K_{k-2}(x_2, \ldots, x_{k-1})} = \\
&= \frac{K_{k+1}(x_1, \ldots, x_{k+1})}{K_k(x_2, \ldots, x_{k+1})}
\end{aligned}$$

Což jsme měli dokázat.[2)]

□

Stručnost zápisu z důkazu předchozí věty budeme využívat i nadále. Nebude-li tedy řečeno jinak, tak symbolem δ_k budeme rozumět $\delta_k(//x_1, \ldots, x_n//)$.

Věta 3.5. *Nechť je dán kanonický řetězový zlomek $//x_1, \ldots, x_n//$, kde $n \geq 2$. Nechť k je kladné celé číslo, $2 \leq k \leq n$. Pak rozdíl dvou sousedních sblížených zlomků je*

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{K_{k-1}(x_2, \ldots, x_k)K_{k-2}(x_2, \ldots, x_{k-1})}. \tag{3.14}$$

Důkaz.

Podle věty 3.4 víme, že

$$\delta_k = \frac{K_k(x_1, \ldots, x_k)}{K_{k-1}(x_2, \ldots, x_k)} \qquad \delta_{k-1} = \frac{K_{k-1}(x_1, \ldots, x_{k-1})}{K_{k-2}(x_2, \ldots, x_{k-1})}.$$

Spočítejme rozdíl těchto sblížených zlomků.

$$\begin{aligned} \delta_k - \delta_{k-1} &= \frac{K_k(x_1, \ldots, x_k)}{K_{k-1}(x_2, \ldots, x_k)} - \frac{K_{k-1}(x_1, \ldots, x_{k-1})}{K_{k-2}(x_2, \ldots, x_{k-1})} \\ &= \frac{K_k(x_1, \ldots, x_k)K_{k-2}(x_2, \ldots, x_{k-1}) - K_{k-1}(x_2, \ldots, x_k)K_{k-1}(x_1, \ldots, x_{k-1})}{K_{k-1}(x_2, \ldots, x_k)K_{k-2}(x_2, \ldots, x_{k-1})} \end{aligned} \tag{3.15}$$

Kontinuanty $K_k(x_1, \ldots, x_k)$, $K_{k-1}(x_1, \ldots, x_{k-1})$ rozepíšeme podle definice 3.8

$$K_k(x_1, \ldots, x_k) = x_k K_{k-1}(x_1, \ldots, x_{k-1}) + K_{k-2}(x_1, \ldots, x_{k-2})$$
$$K_{k-1}(x_2, \ldots, x_k) = x_k K_{k-2}(x_2, \ldots, x_{k-1}) + K_{k-3}(x_2, \ldots, x_{k-2})$$

a dosadíme.

Abychom mohli kontinuanty takto rozepsat, musí opět být $k \geq 2$. Budeme tedy později muset dokázat platnost rovnosti (3.14) také pro $k = 2$.

Po dosazení rozepsaných kontinuantů do čitatele (3.15) a následném roznásobení zjistíme, že se nám některé členy odečtou. Navíc po vytknutí -1 získáme

$$\delta_k - \delta_{k-1} = (-1)\cdot\frac{K_{k-1}(x_1, \ldots, x_{k-1})K_{k-3}(x_2, \ldots, x_{k-2}) - K_{k-2}(x_2, \ldots, x_{k-1})K_{k-2}(x_1, \ldots, x_{k-2})}{K_{k-1}(x_2, \ldots, x_k)K_{k-2}(x_2, \ldots, x_{k-1})}.$$

Všimněme si, že získaný výraz se od výrazu (3.15) liší pouze tím, že přibyla -1 a v čitateli jsme všude místo k napsali $k-1$. Podle výše uvedeného postupu můžeme

[2)] Poslední dvě rovnosti plynou z definice (3.8).

pokračovat, až dostaneme

$$\begin{aligned}\delta_k - \delta_{k-1} &= (-1)^{k-2} \cdot \frac{K_2(x_1,x_2)K_0 - K_1(x_2)K_1(x_1)}{K_{k-1}(x_2,\ldots,x_k)K_{k-2}(x_2,\ldots,x_{k-1})} \\ &= (-1)^{k-2} \cdot \frac{x_2x_1 + 1 - x_2x_1}{K_{k-1}(x_2,\ldots,x_k)K_{k-2}(x_2,\ldots,x_{k-1})} \\ &= (-1)^{k-2} \cdot \frac{1}{K_{k-1}(x_2,\ldots,x_k)K_{k-2}(x_2,\ldots,x_{k-1})} \\ &= (-1)^{k} \cdot \frac{1}{K_{k-1}(x_2,\ldots,x_k)K_{k-2}(x_2,\ldots,x_{k-1})}.\end{aligned}$$

To jsme měli dokázat. Ještě nám ovšem zbývá ověřit platnost věty pro $k = 2$. Počítejme tedy:

$$\delta_2 - \delta_1 = //x_1, x_2// - //x_1// = x_1 + \frac{1}{x_2} - x_1 = \frac{1}{x_2}$$

$$\frac{(-1)^2}{K_1(x_2)K_0} = \frac{1}{x_2}$$

Tím je tedy celý důkaz proveden. □

Díky zavedeným pojmům a větám, jsme schopni obecně vyřešit rovnici (3.5) postupem, který jsme použili při řešení úvodního příkladu.

Vezmeme koeficienty a, b z rovnice (3.5), připomínám, že máme $a > b > 1$. Přeznačme $a = r_{-1}$, $b = r_0$. Vydělme se zbytkem číslo r_{-1} číslem r_0:

$$r_{-1} = q_1 r_0 + r_1,$$

kde q_1, r_1 jsou celá čísla, $q_1 > 0$, $0 \leq r_1 < r_0$. Protože $r_1 > 0$[3)], vydělíme se zbytkem číslo r_0 číslem r_1:

$$r_0 = q_2 r_1 + r_2,$$

kde q_2, r_2 jsou celá čísla, $q_2 > 0$, $0 \leq r_2 < r_1$. Pokud je $r_2 > 0$ budeme stejným způsobem pokračovat. Uvedený postup je známý Euklidův algoritmus. Zbytky po dělení vyhovují nerovnostem

$$r_0 > r_1 > r_2 > r_3 > \ldots,$$

což je klesající posloupnost nezáporných celých čísel. Protože nezáporných celých čísel menších než dané kladné celé číslo je konečný počet, musí tato posloupnost někdy skončit nulou, tedy existuje kladné celé číslo n takové, že

$$r_0 > r_1 > r_2 > r_3 > \cdots > r_n = 0.$$

[3)] Neboť je $a > b > 1$ a $gcd(a, b) = 1$.

Je tedy

$$r_{n-2} = q_n r_{n-1} \qquad r_n = 0.$$

Celkem jsme tedy obdrželi

$$\begin{aligned} r_{-1} &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1}, \end{aligned} \tag{3.16}$$

což můžeme upravit

$$\begin{aligned} \frac{a}{b} = \frac{r_{-1}}{r_0} &= q_1 + \frac{r_1}{r_0} \\ \frac{r_0}{r_1} &= q_2 + \frac{r_2}{r_1} \\ \frac{r_1}{r_2} &= q_3 + \frac{r_3}{r_2} \\ &\vdots \\ \frac{r_{n-3}}{r_{n-2}} &= q_{n-1} + \frac{r_{n-1}}{r_{n-2}} \\ \frac{r_{n-2}}{r_{n-1}} &= q_n \end{aligned}$$

a postupným dosazováním obdržíme

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\cdots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} = //q_1, q_2, \ldots, q_n// = \delta_n(//q_1, q_2, \ldots, q_n//).$$

Nyní vytvoříme

$$\delta_{n-1}(//q_1, q_2, \ldots, q_n//) = //q_1, q_2, \ldots, q_{n-1}//,$$

to má ale smysl pouze pro $n \geq 2$. Protože uvažujeme $gcd(a, b) = 1$ a $a > b > 1$, je $r_1 \neq 0$, proto vždy bude $n \geq 2$. Odečteme $\delta_{n-1}(//q_1, q_2, \ldots, q_n//)$ od původního

poměru koeficientů, což je $\delta_n(//q_1, q_2, \ldots, q_n//)$. To ovšem není nic jiného, než rozdíl dvou sousedních sblížených zlomků, který je podle věty 3.5 roven

$$\delta_n(//q_1, q_2, \ldots, q_n//) - \delta_{n-1}(//q_1, q_2, \ldots, q_n//) = \frac{(-1)^n}{K_{n-1}(q_2, \ldots, q_n)K_{n-2}(q_2, \ldots, q_{n-1})}. \quad (3.17)$$

Navíc podle věty 3.4 je

$$\begin{aligned} \delta_{n-1}(//q_1, q_2, \ldots, q_n//) &= \frac{K_{n-1}(q_1, q_2, \ldots, q_{n-1})}{K_{n-2}(q_2, q_3, \ldots, q_{n-1})} \\ \delta_n(//q_1, q_2, \ldots, q_n//) = \frac{a}{b} &= \frac{K_n(q_1, q_2, \ldots, q_n)}{K_{n-1}(q_2, q_3, \ldots, q_n)} \end{aligned} \quad (3.18)$$

Z poslední rovnosti je

$$aK_{n-1}(q_2, q_3, \ldots, q_n) = bK_n(q_1, q_2, \ldots, q_n),$$

protože čísla a, b jsou kladná celá, jsou kladná celá také čísla q_i, pro $i = 1, 2, \ldots, n$, pak ale i $K_{n-1}(q_2, q_3, \ldots, q_n)$, $K_n(q_1, q_2, \ldots, q_n)$ jsou kladná celá čísla. Protože je $gcd(a, b) = 1$, musí podle lemmatu 3.1 z poslední rovnosti $b \mid K_{n-1}(q_2, q_3, \ldots, q_n)$, existuje tedy celé číslo d tak, že platí

$$K_{n-1}(q_2, q_3, \ldots, q_n) = d \cdot b, \quad (3.19)$$

ovšem z kladnosti čísel $K_{n-1}(q_2, q_3, \ldots, q_n)$, b plyne kladnost čísla d.

Dosaďme vztahy (3.18) do (3.17).[4)]

$$\frac{a}{b} - \frac{K_{n-1}(q_1, q_2, \ldots, q_{n-1})}{K_{n-2}(q_2, q_3, \ldots, q_{n-1})} = \frac{(-1)^n}{K_{n-1}(q_2, \ldots, q_n)K_{n-2}(q_2, \ldots, q_{n-1})}$$

Dosadíme za $K_{n-1}(q_2, q_3, \ldots, q_n)$ podle (3.19).

$$\frac{a}{b} - \frac{K_{n-1}(q_1, q_2, \ldots, q_{n-1})}{K_{n-2}(q_2, q_3, \ldots, q_{n-1})} = \frac{(-1)^n}{b \cdot d \cdot K_{n-2}(q_2, \ldots, q_{n-1})}$$

$$a \cdot d \cdot K_{n-2}(q_2, \ldots, q_{n-1}) - b \cdot d \cdot K_{n-1}(q_1, q_2, \ldots, q_{n-1}) = (-1)^n$$

$$d \cdot [a \cdot K_{n-2}(q_2, \ldots, q_{n-1}) - b \cdot K_{n-1}(q_1, q_2, \ldots, q_{n-1})] = (-1)^n$$

Odtud $d \mid (-1)^n$, je tedy $d = \{-1, 1\}$. Protože d musí být kladné, je $d = 1$ a dostáváme

$$a \cdot K_{n-2}(q_2, q_3, \ldots, q_{n-1}) - b \cdot K_{n-1}(q_1, q_2, \ldots, q_{n-1}) = (-1)^n$$

$$a \cdot K_{n-2}(q_2, q_3, \ldots, q_{n-1}) - b \cdot K_{n-1}(q_1, q_2, \ldots, q_{n-1}) + (-1)^{n+1} = 0$$

$$a \cdot (-1)^{n+1}K_{n-2}(q_2, q_3, \ldots, q_{n-1}) + b \cdot (-1)^n K_{n-1}(q_1, q_2, \ldots, q_{n-1}) + 1 = 0$$

$$a \cdot (-1)^{n+1}cK_{n-2}(q_2, q_3, \ldots, q_{n-1}) + b \cdot (-1)^n cK_{n-1}(q_1, q_2, \ldots, q_{n-1}) + c = 0$$

[4)] Znova si uvědomme, že čísla $K_{n-1}(q_1, q_2, \ldots, q_{n-1})$, $K_{n-2}(q_2, q_3, \ldots, q_{n-1})$ jsou kladná celá, neboť q_i je kladné celé číslo, pro všechna $i = 1, 2, \ldots, n$.

a konečným srovnáním s rovnicí (3.5) získáváme řešení

$$x_0 = (-1)^{n+1} cK_{n-2}(q_2, q_3, \ldots, q_{n-1}) \qquad y_0 = (-1)^n cK_{n-1}(q_1, q_2, \ldots, q_{n-1}). \quad (3.20)$$

S použitím věty 3.3 jsou všechna řešení rovnice (3.5) tvaru

$$x = (-1)^{n+1} cK_{n-2}(q_2, q_3, \ldots, q_{n-1}) - bt \qquad y = (-1)^n cK_{n-1}(q_1, q_2, \ldots, q_{n-1}) + at,$$

kde t je celé číslo.

Uvědomme si, že vzorec pro x_0 se vztahuje k té neznámé, jejíž koeficient je větší, neboť jsme před rozvinutím poměru koeficientů u neznámých uvažovali $a > b$.

Zde končí teoretické zdůvodnění postupu, který jsme použili při řešení úvodního příkladu této kapitoly. Při praktickém řešení diofantických rovnic touto metodou je vhodnější využívat postup, který byl proveden v úvodním příkladu, neboť vzorce (3.20) jsou těžké pro zapamatování a opírají se navíc o znalost rekurentních vzorců pro kontinuanty. Na příkladech si však ukážeme oba postupy.

Příklad 3.8. $72x + 13y + 5 = 0$

Aby bylo možné dosadit do vzorců (3.20) je nutné znát číslo n, tj. počet členů řetězového zlomků vzniklého rozvojem poměru daných koeficientů a dále potřebujeme znát čísla q_i, $i = 1, 2, \ldots, n$, tj. čísla tohoto řetězového zlomku.

$$\frac{72}{13} = 5 + \frac{7}{13} = 5 + \cfrac{1}{\cfrac{13}{7}}$$

$$= 5 + \cfrac{1}{1 + \cfrac{6}{7}} = 5 + \cfrac{1}{1 + \cfrac{1}{\cfrac{7}{6}}}$$

$$= 5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6}}} = //5, 1, 1, 6//$$

Víme tedy, že

$$n = 4,\ q_1 = 5,\ q_2 = 1,\ q_3 = 1,\ q_4 = 6.$$

Dosazením do vzorců (3.20) máme

$$\begin{aligned} x_0 &= (-1)^5 \cdot 5 \cdot K_2(1,1) = -5 \cdot [1 \cdot K_1(1) + K_0] = -5 \cdot [1 \cdot 1 + 1] = -10 \\ y_0 &= (-1)^4 \cdot 5 \cdot K_3(5,1,1) = 5 \cdot [1 \cdot K_2(5,1) + K_1(5)] \\ &= 5 \cdot [1 \cdot K_1(5) + K_0 + 5] = 5 \cdot [5 + 1 + 5] = 55 \end{aligned}$$

Celkem

$$x = -10 - 13t \qquad y = 55 + 72t,$$

kde t je celé číslo.

Využijeme postup z úvodního příkladu. Již máme spočítáno

$$\frac{72}{13} = 5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6}}}.$$

Vynecháním $\frac{1}{6}$ získáme

$$5 + \cfrac{1}{1 + \cfrac{1}{1}} = 5 + \frac{1}{2} = \frac{11}{2}$$

Obdržený zlomek odečteme od původního poměru koeficientů.

$$\frac{72}{13} - \frac{11}{2} = \frac{144 - 143}{2 \cdot 13} = \frac{1}{2 \cdot 13}$$

Postupnými úpravami získané rovnosti dojdeme k výsledku.

$$\begin{aligned} \frac{72}{13} - \frac{11}{2} &= \frac{1}{2 \cdot 13} \\ 72 \cdot 2 - 13 \cdot 11 &= 1 \\ 72 \cdot 2 - 13 \cdot 11 - 1 &= 0 \\ 72 \cdot (-10) + 13 \cdot (55) + 5 &= 0 \end{aligned}$$

Odtud

$$x_0 = -10 \qquad y_0 = 55.$$

Příklad 3.9. $25x - 37y - 12 = 0$

Substitucí $y = -z$ převedeme příklad na případ, kdy máme oba koeficienty kladné, tj.

$$25x + 37z - 12 = 0.$$

Opět rozvineme poměr koeficientů v řetězový zlomek.

$$\frac{37}{25} = //1, 2, 12//$$

Nyní stačí dosadit do vzorců 3.20, kde si jen musíme uvědomit, že pro z_0 musíme použít vypočet odpovídající v těchto vzorcích x_0, neboť u neznámé z je vyšší koeficient.

$$z_0 = (-1)^4 \cdot (-12) \cdot K_1(2) = -24$$
$$x_0 = (-1)^3 \cdot (-12) \cdot K_2(1, 2) = 36$$

Všechna řešení jsou ve tvaru

$$x = 36 + 37t \qquad z = -24 - 25t,$$

kde t je celé číslo. Ještě se musíme vrátit zpět k substituci, řešením zadané rovnice jsou čísla tvaru

$$x = 36 + 37t \qquad y = 24 + 25t.$$

Příklad ještě vyřešíme druhým postupem. Vycházíme z rovnice po substituci. Již víme $\frac{37}{25} = //1, 2, 12//$ a vypočítáme $//1, 2// = \frac{3}{2}$. Rozdílem těchto zlomků a upravami obdržené rovnosti dostáváme

$$\frac{37}{25} - \frac{3}{2} = \frac{-1}{25 \cdot 2}$$
$$37 \cdot 2 - 25 \cdot 3 = -1$$
$$37 \cdot 2 - 25 \cdot 3 + 1 = 0$$
$$37 \cdot (-24) + 25 \cdot (36) - 12 = 0,$$

odkud porovnáním $x_0 = 36$, $z_0 = -24$.

Cvičení 3.2. Vyřešte následující diofantické rovnice s využitím řetězových zlomků.

(a) $19x + 5y - 4 = 0$

(b) $180x - 23y + 12 = 0$

(c) $182 + 104y + 29 = 0$

(d) $4x + 11y - 16 = 0$

3.3 Metoda řešení kongruencí

Bohužel se opět neobejdeme bez zavedení potřebného aparátu, kterému musíme věnovat větší pozornost, neboť jej využijeme i později při řešení lineárních diofantických rovnic o n neznámých, ale také u rovnic, které jsou lineární vzhledem k alespoň jedné neznámé. Nejprve si zavedeme pojem kongruence, následně si ukážeme, jak s kongruencemi počítat. Vycházím hlavně z [2].

Definice 3.9. *Jestliže dvě celá čísla a, b mají po dělení kladným celým číslem m stejný zbytek r, kde $0 \leq r < m$, říkáme, že a je kongruentní s b modulo m a píšeme symbolicky*

$$a \equiv b \pmod{m}.$$

V opačném případě řekneme, že a není kongruentní s b modulo m a píšeme

$$a \not\equiv b \pmod{m}.$$

Číslo a nazýváme levou stranou kongruence, číslo b pravou stranou kongruence.

Věta 3.6. *Nechť a, b jsou celá čísla a m je kladné celé číslo. Pak následující podmínky jsou ekvivalentní:*

(I) $a \equiv b \pmod{m}$.

(II) $m \mid (a - b)$.

(III) $a = b + mk$, *kde k je celé číslo.*

Důkaz.
Provedeme ho tak, že dokážeme následující tři tvrzení:

(i) Jestliže (I), pak (II).

(ii) Jestliže (II), pak (III).

(iii) Jestliže (III), pak (I).

ad(i) $a \equiv b \pmod{m}$ podle definice 3.9 znamená

$$a = q_1 m + r$$
$$b = q_2 m + r,$$

kde q_1, q_2 jsou celá čísla. Odečtením druhé rovnice od první dostaneme $a-b = (q_1 - q_2)m$, což ovšem znamená, že $m \mid (a-b)$.

ad(ii) Protože $m \mid (a-b)$, musí existovat celé číslo k tak, že $a - b = km$, úpravou získáme $a = b + mk$.

ad(iii) Vydělíme-li se zbytkem číslo b číslem m dostaneme $b = qm + r$, kde q, r jsou celá čísla a $0 \leq r < m$. Dosazením do předpokladu $a = b + mk$ dostáváme $a = (q+k)m+r$, tedy číslo a má po dělení číslem m stejný zbytek jako číslo b, což jsme měli dokázat.

□

Věta 3.7. *Nechť a, b, c jsou celá čísla. Pak pro každé kladné celé číslo m platí:*

(I) $a \equiv a \pmod{m}$.

(II) *Jestliže* $a \equiv b \pmod{m}$, *pak* $b \equiv a \pmod{m}$.

(III) *Jestliže* $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$, *pak je také* $a \equiv c \pmod{m}$.

Důkaz.

ad(I) Pro každé kladné celé číslo platí $m \mid 0$, což můžeme zapsat $m \mid (a-a)$, to podle věty 3.6 je $a \equiv a \pmod{m}$.

ad(II) Podle předpokladu $a \equiv b \pmod{m}$, musí $m \mid (a-b)$, to znamená, že existuje celé číslo k tak, že platí $a - b = km$. Po vynásobení této rovnosti číslem -1 dostaneme $b - a = -km$, to znamená, že $m \mid (b-a)$, tedy $b \equiv a \pmod{m}$.

ad(III) Podle předpokladů $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, existují celá čísla k, l tak, že platí

$$a - b = km$$
$$b - c = lm.$$

Po sečtení těchto rovnic dostaneme $a - c = (k+l)m$, tedy $a \equiv c \pmod{m}$.[5)]

□

[5)] Dokázali jsme, že relace kongruence podle libovolného kladného celého modulu m je reflexivní, symetrická a trantzitivní, tzn. že tato relace je typu ekvivalence.

O tom jak s kongruencemi počítat hovoří následující věty.

Věta 3.8. *Nechť a, b, c, m jsou celá čísla, $m > 0$. Jestliže je $a \equiv b \pmod{m}$, pak je také*

(I) $a + c \equiv b + c \pmod{m}$,

(II) $a - c \equiv b - c \pmod{m}$,

(III) $ac \equiv bc \pmod{m}$.

Důkaz.

ad(I) Dle předpokladu $m \mid (a - b)$. To je totéž, jako $m \mid (a + c - c - b)$. Po úpravě máme $m \mid [(a + c) - (b + c)]$, což ovšem znamená, že $a + c \equiv b + c \pmod{m}$.

ad(II) Dle předpokladu $m \mid (a - b)$. To je totéž, jako $m \mid (a - c + c - b)$. Po úpravě máme $m \mid [(a - c) - (b - c)]$, což ovšem znamená, že $a - c \equiv b - c \pmod{m}$.

ad(III) Protože $m \mid (a - b)$, platí $m \mid (a - b)c$, tedy $m \mid (ac - bc)$, odtud $ac \equiv bc \pmod{m}$.

□

Máme-li danou kongruenci s daným modulem m, můžeme k ní přičíst, resp. od ní odečíst, libovolné celé číslo nebo vynásobit obě strany kongruence libovolným celým číslem, stejně jako u rovnosti.

Věta 3.9. *Nechť a, b, c, d jsou celá čísla. Nechť m je kladné celé číslo. Jestliže je $a \equiv b \pmod{m}$ a zároveň $c \equiv d \pmod{m}$ pak je také*

(I) $a + c \equiv b + d \pmod{m}$,

(II) $a - c \equiv b - d \pmod{m}$,

(III) $ac \equiv bd \pmod{m}$.

Důkaz.

ad(I) Z kongruencí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ získáme podle (I) ve větě 3.8

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

Nyní stačí použít (III) z věty 3.7 a dostáváme $a + c \equiv b + d \pmod{m}$.

ad(II) Z kongruencí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ získáme podle (II) ve větě 3.8

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

Kongruenci vpravo vynásobíme podle (III) z věty 3.8 číslem -1. Získáváme tak kongruenci $b - c \equiv b - d \pmod{m}$ a teď už stačí opět použít (III) z věty 3.7.

ad(III) Z kongruencí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ získáme podle (III) ve větě 3.8

$$ac \equiv bc \pmod{m} \qquad cb \equiv db \pmod{m}.$$

Nyní stačí použít (III) z věty 3.7 a dostáváme $ac \equiv bd \pmod{m}$. □

Kongruence podle stejného modulu tedy lze spolu sčítat, odčítat a násobit. Důsledkem této věty je také to, že můžeme libovolný sčítanec přenést z jedné strany kongruence na druhou, ovšem s opačným znaménkem a také na každou stranu kongruence můžeme přičíst jiný a libovolný násobek modulu.

Věta 3.10. *Jestliže $a \equiv b \pmod{m}$, pak pro každé kladné celé k platí*

$$a^k \equiv b^k \pmod{m}.$$

Důkaz.

Větu dokážeme matematickou indukcí. Musíme dokázat následující:

(I) Dokážeme, že věta platí pro $k = 1$.

(II) Dokážeme, že platí $a^{k+1} \equiv b^{k+1} \pmod{m}$, za předpokladu $a^k \equiv b^k \pmod{m}$.

ad(I) Pro $k = 1$ dostáváme $a^1 \equiv b^1 \pmod{m}$, což je ovšem předpoklad věty.

ad(II) Předpokládejme, že věta platí pro k, tzn. $a^k \equiv b^k \pmod{m}$. Položíme-li ve větě 3.9 $c = a^k$ a $d = b^k$, dostaneme podle bodu (III) této věty

$$a \cdot a^k \equiv b \cdot b^k \pmod{m},$$

což je

$$a^{k+1} \equiv b^{k+1}.$$

□

Tedy obě strany kongruence můžeme umocnit kladným celým číslem, podobně jako rovnost.

Věta 3.11. *Nechť a, b, c, m jsou celá čísla, $m > 0$. Nechť $gcd(c, m) = 1$. Nechť konečně je $ac \equiv bc \pmod{m}$. Pak je také $a \equiv b \pmod{m}$.*

Důkaz.
Protože $ac \equiv bc \pmod{m}$, platí $m \mid (ac-bc)$, tj. $m \mid (a-b)c$ a protože $gcd(c, m) = 1$, musí $m \mid (a - b)$, což znamená $a \equiv b \pmod{m}$. □

Můžeme tedy kongruenci krátit číslem, které je nesoudělné s modulem dané kongruence.

Věta 3.12. *Nechť a, b, c, m jsou celá čísla, $c > 0$, $m > 0$. Kongruence $a \equiv b \pmod{m}$ je ekvivalentní s kongruencí $ac \equiv cb \pmod{mc}$.*

Důkaz.
Musíme dokázat dvě věci:

(I) $a \equiv b \pmod{m} \Rightarrow ac \equiv cb \pmod{mc}$,

(II) $ac \equiv cb \pmod{mc} \Rightarrow a \equiv b \pmod{m}$.

ad(I) Protože $a \equiv b \pmod{m}$, existuje celé číslo k takové, že platí $a - b = km$, tuto rovnost můžeme vynásobit kladným celým číslem c, $ac - bc = k(mc)$, odtud $ac \equiv cb \pmod{mc}$.

ad(II) Protože $ac \equiv cb \pmod{mc}$, existuje celé číslo k takové, že platí $ac-bc = kmc$, tuto rovnost můžeme vydělit kladným celým číslem c, $a-b = km$, odtud $a \equiv b \pmod{m}$.

□

Ukážeme si, jak nám kongruence pomůžou při řešení lineárních diofantických rovnic o dvou neznámých. Vrátíme se opět k řešení rovnice (3.5), jen se nám bude více hodit tuto rovnici uvažovat v následujícím tvaru

$$ax + by = c, \tag{3.21}$$

navíc již nevyžadujeme $a > b > 1$, čísla a, b jsou libovolná, ovšem nenulová celá čísla a také různá od 1. Libovolné řešení x, y po dosazení do rovnice (3.21) musí nutně splňovat kongruenci podle libovolného modulu m, kde m je kladné celé číslo, tj.

$$ax + by \equiv c \pmod{m}.$$

Vezměme za modul absolutní hodnotu jednoho z koeficientů, např. nechť $m = |b|$, obdržíme

$$ax + by \equiv c \pmod{|b|},$$

protože můžeme přičítat, resp. odečítat od kongruence násobky modula, dostáváme

$$ax \equiv c \pmod{|b|}. \tag{3.22}$$

Obdrželi jsme lineární kongruenci o jedné neznámé.

Věta 3.13. *Nechť m je kladné celé číslo, u, v jsou celá čísla. Nechť $gcd(u, m) = d$. Jestliže $d \mid v$, pak kongruence*

$$ux \equiv v \pmod{m} \tag{3.23}$$

má řešení.

Důkaz.
Protože $d \mid v$, je $v = k \cdot d$, kde k je celé číslo. Pomocí rozšířeného Euklidova algoritmu můžeme nalézt celá čísla α, β tak, že platí:

$$\begin{aligned} \alpha u + \beta m &= d \\ (\alpha k)u + (\beta k)m &= kd \\ (\alpha k)u + (\beta k)m &= v \\ (\beta k)m &= v - (\alpha k)u \end{aligned}$$

Odtud $m \mid (v - (\alpha k)u)$, což je

$$(\alpha k)u \equiv v \pmod{m}. \tag{3.24}$$

Srovnáním s rovnicí (3.23) vidíme řešení $x = \alpha k$. □

Rád bych jen čtenáře upozornil, na existenci následující věty, jejíž důkaz je k nalezení v [4, str. 189].

Věta 3.14. *Nechť m je kladné celé číslo, u, v jsou celá čísla. Nechť $gcd(u, m) = d$. Kongruence*

$$ux \equiv v \pmod{m} \tag{3.25}$$

je řešitelná, jen když $d \mid v$. V tomto případě je x řešením kongruence (3.25)*, právě když*

$$x \equiv v_1 \cdot u_1^{\varphi(m_1)-1} \pmod{m_1}, \tag{3.26}$$

kde $u_1 = \frac{u}{d}$, $v_1 = \frac{v}{d}$, $m_1 = \frac{m}{d}$ a φ je Eulerova funkce[6]*.*

Tato věta nám oproti větě 3.13 ukazuje, jak lze kongruenci (3.25) převést na (3.26), odkud je podle věty 3.6 vidět řešení kongruence (3.25) tvaru $x = v_1 \cdot u_1^{\varphi(m_1)-1} + tm_1$, kde t je celé číslo. Pracuje se zde ovšem s Eulerovou funkcí, pro níž neexistuje žádný efektivní algoritmus jejího vyčíslení, pokud neznáme prvočíselný rozklad jejího argumentu a navíc číslo ${u_1}^{\varphi(m_1)-1}$ bývá zpravidla velmi vysoké. Z těchto důvodů si vystačíme s větou 3.13, která nám zaručuje existenci řešení kongruence (3.23), kterou se naučíme převést na tvar $x \equiv q \pmod{m}$, kde q je celé číslo, pomocí povolených úprav.

Příklad 3.10. $5x \equiv 36 \pmod{7}$

Nejprve vypíšeme celý výpočet a následně okomentujeme jednotlivé kroky. Tato kongruence má podle věty 3.13 řešení, neboť je $gcd(5, 7) = 1$ a $1 \mid 36$.

$$\begin{aligned} 5x &\equiv 36 \pmod{7} \\ 5x &\equiv 15 \pmod{7} \\ x &\equiv 3 \pmod{7} \\ x &= 3 + 7t, \end{aligned}$$

kde t je celé číslo. Při výpočtu jsme postupně použili odečtení trojnásobku modula od levé strany kongruence (důsledek věty 3.9), dělení pěti, což lze, neboť $5 \nmid 7$ (věta 3.11) a nakonec ekvivalentní zápis (věta 3.6).

[6] Hodnota Eulerovy funkce v kladném celém čísle n, tj. $\varphi(n)$, udává počet nezáporných celých čísel, která jsou menší než n a jsou s n nesoudělná. Definici a některé základní vlastnosti čtenář muže nalézt v [4, str. 182-185].

Na dvou následujících příkladech si konkrétně ukážeme, využití kongruencí při řešení rovnice (3.21).

Příklad 3.11. $14x + 23y = 17$

Nechť x, y je řešení, pak splňují kongruenci

$$14x + 23y \equiv 17 \pmod{14},$$

často je výhodné volit nejmenší možný modul, tj. menší z koeficientů. Úpravami postupně získáváme:

$$\begin{aligned} 23y &\equiv 17 \pmod{14} \\ 9y &\equiv 3 \pmod{14} \\ 3y &\equiv 1 \pmod{14} \\ 3y &\equiv 15 \pmod{14} \\ y &\equiv 5 \pmod{14} \end{aligned}$$

V úpravách jsme postupně použili odečtení jednanásobku modula, dělení číslem 3, což lze neboť číslo 3 není soudělné s modulem, přičtení jednanásobku modula na levou stranu kongruence, další dělení číslem 3.

Poslední kongruence nám podle věty 3.6 dává $y = 5 + 14t$, kde t je celé číslo. Dosazením do zadané rovnice dopočítáme neznámou x.

$$\begin{aligned} 14x + 23(5 + 14t) &= 17 \\ 14x &= -98 - 23 \cdot 14t \\ x &= -7 - 23t \end{aligned}$$

Celkem tedy

$$x = -7 - 23t \qquad y = 5 + 14t,$$

kde t je celé číslo.

Příklad 3.12. $18x - 25y = -8$

Jsou-li čísla x, y řešením, musí vyhovovat například kongruenci

$$18x - 25y \equiv -8 \pmod{18}$$

a postupnými úpravami dostáváme:

$$\begin{aligned} -25y &\equiv -8 \pmod{18} \\ 25y &\equiv 8 \pmod{18} \\ 25y &\equiv -10 \pmod{18} \\ 5y &\equiv -2 \pmod{18} \\ 5y &\equiv -20 \pmod{18} \\ y &\equiv -4 \pmod{18} \end{aligned}$$

Odtud $y = -4 + 18t$, kde t je celé číslo. Dosazením do zadání získáme

$$18x - 25 \cdot (-4 + 18t) = -8.$$

Celkem tedy

$$x = -6 + 25t \qquad y = -4 + 18t,$$

kde t je celé číslo.

Na těchto dvou příkladech je vidět, jak je řešení snadné a téměř bezpracné, stačí pouze uchopit pojem kongruence a umět řešit lineární kongruence o jedné neznámé. Komplikace nastává, pokud zadaná diofantická rovnice má velké koeficienty, pak modul kongruence je také velký a nalezení řešení se stává obtížnějším.

Následující věty nám pomohou s případem, kdy modul nebude prvočíselný, tj. půjde napsat jako součin několika kladných celých čísel. Ukáže se, že pak můžeme tuto kongruenci převést na soustavu více kongruencí podle modulů, které jsou činiteli původního modulu.

Musíme tedy dokázat ekvivalenci původní kongruence a vzniklé soustavy kongruencí a následně dát návod, jak řešit soustavu lineárních kongruencí o jedné neznámé. Nejprve dvě pomocné věty.

Lemma 3.2. *Nechť x, y, z jsou celá čísla. Jestliže $x \mid y$ a zároveň $y \mid z$, pak $x \mid z$.*

Důkaz.

Chceme dokázat, že $x \mid z$, což znamená, že musíme najít celé číslo t tak, aby platilo $z = t \cdot x$. Podle předpokladů platí $x \mid y$ a $y \mid z$, musí tedy existovat celá čísla k, l tak, že $y = k \cdot x$ a $z = l \cdot y$. Dosazením do posledního vztahu za y dostáváme $z = l \cdot k \cdot x$, odtud volbou $t = k \cdot l$ jsme našli hledané t. □

Definice 3.10. *Nechť a, b jsou kladná celá čísla. Budeme říkat, že kladné celé číslo c je nejmenším společným násobkem čísel a, b právě tehdy, když platí:*

(I) $a \mid c \wedge b \mid c$,

(II) *pro všechna kladná celá e platí:* $(a \mid e \wedge b \mid e) \Rightarrow c \mid e$.

Skutečnost, že c je nejmenším společným násobkem čísel a, b budeme zapisovat

$$c = lcm(a, b).$$

Pokud platí pouze (I)*, nazýváme číslo c společným násobkem čísel a, b.*

Věta 3.15. *Nechť u, v jsou celá čísla. Nechť k je kladné celé číslo. Nechť m_i jsou kladná celá čísla pro všechna $i = 1, 2, \ldots, k$. Nechť konečně je $m = lcm(m_1, m_2, \ldots, m_k)$. Pak kongruence $u \equiv v \pmod{m}$ je splněna právě tehdy, když jsou splněny kongruence*

$$u \equiv v \pmod{m_i}$$

pro všechna $i = 1, 2, \ldots, k$.

Důkaz.

Protože věta je vyslovená ve tvaru ekvivalence, musíme dokázat dvě věci:

(I) Jestliže $u \equiv v \pmod{m}$, pak $u \equiv v \pmod{m_i}$, pro všechna $i = 1, 2, \ldots, k$.

(II) Jestliže pro všechna $i = 1, 2, \ldots, k$ platí $u \equiv v \pmod{m_i}$, pak $u \equiv v \pmod{m}$.

ad(I) Jestliže $u \equiv v \pmod{m}$, musí $m \mid (u - v)$. Buď $i = 1, 2, \ldots, k$. Protože m je nejmenší společný násobek čísel m_i, musí $m_i \mid m$ a důsledkem tranzitivnosti relace dělí, tj. lemmatu 3.2, musí také $m_i \mid (u - v)$, což ovšem znamená, že $u \equiv v \pmod{m_i}$.

ad(II) Jestliže pro všechna $i = 1, 2, \ldots, k$ je $u \equiv v \pmod{m_i}$, musí $m_i \mid (u - v)$. Tedy číslo $u - v$ musí být společným násobkem čísel m_i, $i = 1, 2, \ldots, k$, a tudíž musí být dělitelné jejich nejmenším společným násobkem, tj. číslem m. Protože $m \mid (u - v)$, musí být $u \equiv v \pmod{m}$.

□

Například kongruence $7x = 2 \pmod{15}$ je podle této věty ekvivalentní se soustavou kongruencí

$$\begin{aligned} 7x &\equiv 2 \pmod{5} \\ 7x &\equiv 2 \pmod{3}. \end{aligned}$$

Došlo tedy ke snížení modulu, ale nárůstu rovnic. Musíme se naučit vyřešit tyto obržené soustavy.

Uvažujme řešitelnou kongruenci $ax \equiv b \pmod{n}$ a proveďme prvočíselný rozklad čísla n:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k},$$

kde p_i jsou navzájem různá prvočísla, α_i jsou kladná celá čísla, pro všechna $i = 1, 2, \dots, k$. Protože $lcm({p_1}^{\alpha_1}, {p_2}^{\alpha_2}, \dots, {p_k}^{\alpha_k}) = n$, je tato kongruence podle věty 3.15 ekvivalentní se soustavou kongruencí

$$\begin{aligned} ax &\equiv b \pmod{{p_1}^{\alpha_1}} \\ ax &\equiv b \pmod{{p_2}^{\alpha_2}} \\ &\vdots \\ ax &\equiv b \pmod{{p_k}^{\alpha_k}}. \end{aligned}$$

Protože původní kongruence je řešitelná a je ekvivalentní s obdrženou soustavou, je řešitelná každá z těchto kongruencí. Potom ovšem můžeme pomocí povolených úprav soustavu převést na tvar

$$\begin{aligned} x &\equiv c_1 \pmod{{p_1}^{\alpha_1}} \\ x &\equiv c_2 \pmod{{p_2}^{\alpha_2}} \\ &\vdots \\ x &\equiv c_k \pmod{{p_k}^{\alpha_k}}, \end{aligned}$$

kde c_i jsou vhodná celá čísla, $i = 1, 2, \dots, k$.

Uvažujme nejprve $k = 2$, hledáme tedy řešení následující soustavy

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2}. \end{aligned} \tag{3.27}$$

O tom jak vypadá řešení soustavy kongruencí (3.27) hovoří následující věta, známá jako Čínská zbytková věta.

Věta 3.16 (Čínská zbytková věta)**.** *Nechť m je kladné celé číslo, navíc takové, že $m = m_1 \cdot m_2$, kde m_1, m_2 jsou kladná celá čísla, $m_1 \geq 2$, $m_2 \geq 2$, $gcd(m_1, m_2) = 1$. Soustava lineárních kongruencí*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

má vždy řešení a toto řešení je jednoznačně určeno v modulo m.

Důkaz.
Řešením první kongruence jsou čísla tvaru

$$x = c_1 + m_1 t, \tag{3.28}$$

kde t je celé číslo. Dosadíme toto řešení do druhé kongruence, máme

$$\begin{aligned} c_1 + m_1 t &\equiv c_2 \pmod{m_2} \\ m_1 t &\equiv c_2 - c_1 \pmod{m_2} \end{aligned}$$

Obdrželi jsme lineární kongruenci pro t, ta má podle věty 3.13 řešení, neboť podle předpokladu je $gcd(m_1, m_2) = 1$ a $1 \mid (c_2 - c_1)$. Proto dokážeme tuto kongruenci upravit na tvar $t \equiv c_3 \pmod{m_2}$, kde c_3 je nějaké celé číslo, odtud $t = c_3 + sm_2$. Dosazením do (3.28)

$$\begin{aligned} x &= c_1 + m_1 \cdot (c_3 + sm_2) \\ x &= c_1 + m_1 c_3 + sm_1 m_2 \\ x &= c + sm_1 m_2 \\ x &\equiv c \pmod{m_1 m_2} \\ x &\equiv c \pmod{m}, \end{aligned} \tag{3.29}$$

kde jsme označili $c = c_1 + m_1 c_3$. □

Všimněmě si, že získaná kongruence, která je řešením soustavy (3.27) je stejného tvaru jako původní kongruence. Důkaz Čínské zbytkové věty je současně návodem, jak řešit soustavu lineárních kongruencí o jedné neznámé. Pokud tedy bude mít soustava více než dvě kongruence, pak první dvě nahradíme jedinou kongruencí

podle věty 3.16 a k ní si vezmeme třetí kongruenci atd. Budeme-li řešit soustavu k kongruencí, tak po $k-1$ krocích nalezneme řešení celé soustavy.

Vše si ukážeme na následujícím příkladu.

Příklad 3.13. $238x - 171y = 23$

Vidíme, že koeficienty jsou relativně velká čísla, což by vedlo k nepohodlnému počítací podle velkého modulu. Proto využijeme věty 3.15. Řešení musí splňovat

$$\begin{aligned} 238x - 171y &\equiv 23 \pmod{171} \\ 67x &\equiv 23 \pmod{171}. \end{aligned}$$

Potože $171 = 9 \cdot 19$, můžeme poslední kongruenci nahradit soustavou

$$\begin{aligned} 67x &\equiv 23 \pmod{9} \\ 67x &\equiv 23 \pmod{19}. \end{aligned}$$

Najdeme řešení první z nich

$$\begin{aligned} 67x &\equiv 23 \pmod{9} \\ 4x &\equiv -4 \pmod{9} \\ x &\equiv -1 \pmod{9} \\ x &= -1 + 9s, \end{aligned}$$

kde s je celé číslo. Toto řešení dosadíme do druhé kongruence.

$$\begin{aligned} 67(-1 + 9s) &\equiv 23 \pmod{19} \\ -67 + 603s &\equiv 23 \pmod{19} \\ 603s &\equiv 90 \pmod{19} \\ 14s &\equiv 14 \pmod{19} \\ s &\equiv 1 \pmod{19} \\ s &= 1 + 19t, \end{aligned}$$

kde t je celé číslo. Dosazením za s máme $x = 8 + 171t$. Nyní zbývá dopočítat y, to opět uděláme dosazením řešení pro x do zadání, získáme $y = 11 + 238t$.

Cvičení 3.3. Pomocí kongruencí vyřešte následující diofantické rovnice.

(a) $41x + 12y = 5$

(b) $9x + 4y = 12$

(c) $72x - 27y = 18$

(d) $826x - 1074y = 2808$

3.4 Školské řešení a geometrická interpretace

V této podkapitole bych rád stručně ukázal, jak bychom mohli se středoškolskými studenty řešit lineární diofantické rovnice o dvou neznámých, aniž bychom museli zavádět složitý matematický aparát, který by nejspíše byl nad rámec matematických schopností většiny studentů. Budu postupovat jako v [8, kapitola 7], jen využiji vlastní příklady. Pro jednoduchost budeme nejprve uvažovat rovnice v základním tvaru.

Příklad 3.14. $3x - 5y = 4$

Ze zadání můžeme vyjádřit jednu proměnnou, například y, tím dostáváme

$$y = \frac{1}{5} \cdot (3x - 4),$$

nyní postupným dosazováním celých čísel za x, tj. systematickým experimentováním, budeme sledovat, kdy hodnota y bude také celočíselná. Dosazujme postupně čísla 0, 1, 2, 3,..., výsledky zaznamenáme tabulkou.

x	0	1	2	3	4	5	6	7	8
y	-0,8	-0,2	0,4	1	1,6	2,2	2,8	3,4	4

Vidíme, že y nabývá celočíselné hodnoty pro $x = 3$ a $x = 8$. Zkusme ještě dosadit několik prvních záporných celých čísel.

x	-1	-2	-3	-4	-5	-6	-7	-8	-9
y	-1,4	-2	-2,6	-3,2	-3,8	-4,4	-5	-5,6	-6,2

Nyní dostáváme celočíselné y volbou $x = -2$ a $x = -7$. Vypišme si pro přehlednost posloupnosti celých čísel x a y, která jsme objevili systematickým experimentováním a dávají nám řešení v celých číslech.

$$x : -7,\ -2,\ 3,\ 8$$
$$y : -5,\ -2,\ 1,\ 4$$

Vidíme, že celočíselná x, která jsou řešením rovnice, se od sebe vždy liší o číslo 5, v případě y je to číslo 3. Je důležité si uvědomit, že v rozsahu našeho experimentování jsme objevili všechna celočíselná řešení, tedy žádné řešení nám nevypadlo,

neboť jsme postupovali systematicky. Na základě těchto úvah by se mohla vyslovit hypotéza: *Rovnice má nekonečně mnoho řešení. Jedním řešením je například* $x = 3$, $y = 1$, *ostatní řešení získáme tak, že k číslu* x *budeme přičítat všechny celočíselné násobky čísla* 5, *v případě* y *celočíselné násobky čísla* 3.

Matematicky vyjádřeno

$$x = 3 + 5t \qquad y = 1 + 3t,$$

kde t je celé číslo. Tuto hypotézu můžeme ověřit dosazením do zadání.

$$3 \cdot (3 + 5t) - 5 \cdot (1 + 3t) = 9 + 15t - 5 - 15t = 4$$

Nyní by bylo na místě sdělit studentům větu 3.3, z které plyne, že řešení, která jsme našli jsou skutečně všechna a neexistuje žádné jiné. Případně by se mohl udělat důkaz, který by pro středoškolské studenty neměl být příliš složitý, nebo můžeme postupovat následujícím způsobem.

Jedno z řešení, které jsme našli je $x = 3$, $y = 1$, platí tedy $3 \cdot 3 - 5 \cdot 1 = 4$. Takto vyjádřené číslo 4 dosadíme do zadané rovnice a dostaneme

$$\begin{aligned} 3x - 5y &= 3 \cdot 3 - 5 \cdot 1 \\ 3x - 3 \cdot 3 &= 5y - 5 \cdot 1 \\ 3(x - 3) &= 5(y - 1) \end{aligned} \tag{3.30}$$

Využijeme následující fakt: Jsou-li p, c, d celá čísla, p je prvočíslo a platí $p \mid c \cdot d$, pak $p \mid c$ nebo $p \mid d$.[7)]

Z (3.30) máme $3 \mid 5(y - 1)$, takže $3 \mid 5$ nebo $3 \mid (y - 1)$, protože $3 \nmid 5$ musí $3 \mid (y - 1)$. Tedy $y - 1 = 3t$, $y = 1 + 3t$, kde t je celé číslo. Nyní dosadíme za y do původní rovnice a máme

$$\begin{aligned} 3x - 5(1 + 3t) &= 4 \\ 3x - 5 - 15t &= 4 \\ 3x &= 9 + 15t \\ x &= 3 + 5t. \end{aligned}$$

[7)] Jedná se o jednu z nejzákladnějších vlastností prvočísel, kterou by středoškolský student měl znát ze základů teorie čísel.

Nyní vidíme, že všechna řešení mají tvar

$$x = 3 + 5t \qquad y = 1 + 3t,$$

kde t je celé číslo.

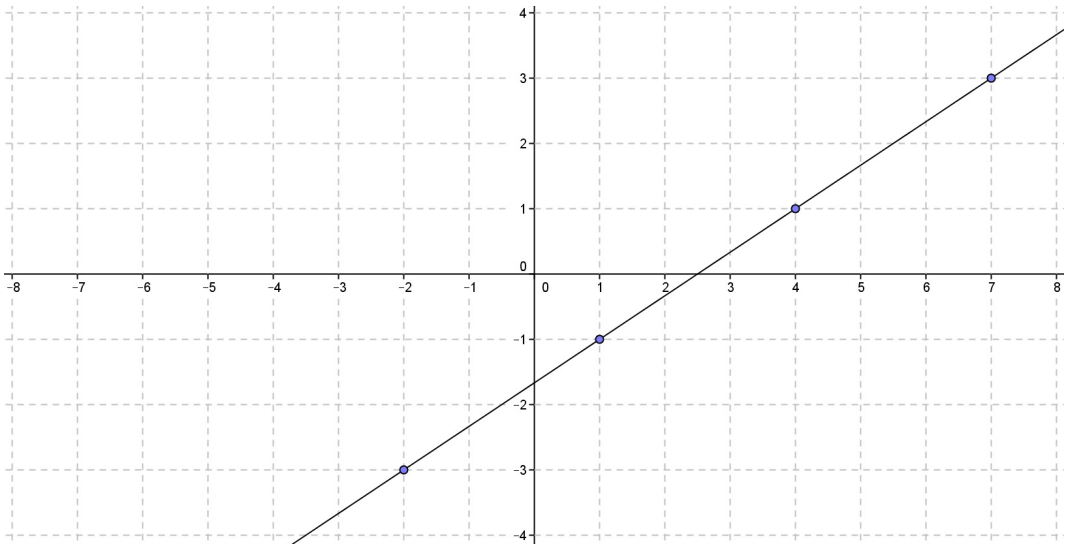
Středoškolským studentům, kteří by měli za sebou kurz analytické geometrie, bychom mohli nastínit geometrickou interpretaci lineární diofantické rovnice. Na rovnici (3.1) se můžeme podívat jako na obecné vyjádření přímky v rovině nebo jako na funkci vyjádříme-li

$$y = -\frac{a}{b}x - \frac{c}{b}.$$

Necháme-li si vykreslit graf této funkce v celočíselné síti na počítači, tak celočíselné řešení rovnice (3.1) pak odpovídá mřížovým bodům[8)], ležícím na dané přímce. Důsledkem věty 3.3 je skutečnost, že protne-li graf funkce jeden mřížový bod, pak už jich protne nekonečně mnoho a to jsou právě všechna celočíselná řešení dané rovnice.

Příklad 3.15. $2x - 3y - 5 = 0$

Rovnici upravíme, $y = \frac{2}{3}x - \frac{5}{3}$ a necháme si graf této funkce vykreslit, můžeme například využít program GeoGebra.



Obrázek 3.1: Graf funkce $y = \frac{2}{3}x - \frac{5}{3}$ v celočíselné síti.

[8)] Mřížovými body rozumíme průsečíky přímek rovnoběžných s osou x a s osou y, které navíc prochází celočíselnými hodnotami os x, y.

Na základě obrázku 3.1 by studenti měli dokázat napsat obecný tvar řešení

$$x = 4 + 3t \qquad y = 1 + 2t,$$

kde t je celé číslo a následně toto řešení dosadit do zadané rovnice a provést tak zkoušku.

Nyní bychom mohli začít uvažovat rovnice, které nejsou v základním tvaru a uvést větu 3.1. Tato věta by se také mohla dokázat. V textu jsme k důkazu použili rozšířený Euklidův algoritmus, ten ovšem studenti na střední škole neznají. Klíčem k důkazu je hlavně Bezoutova rovnost. O platnosti této rovnosti můžeme studenty přesvědčit následující větou, v jejímž důkazu využijeme dělení se zbytkem, které studenti znají. Pro jednoduchost větu uvádím pouze pro kladná celá čísla, což nám stačí, neboť vždy snadno dokážeme rovnici (3.1) převést na tvar, kde budou koeficienty u neznámých kladná celá čísla.

Věta 3.17. *Nechť a, b jsou kladná celá čísla, $d = gcd(a, b)$. Pak existují celá čísla α, β tak, že $a\alpha + b\beta = d$.*

Důkaz.
Položme

$$\mathbb{M} = \{ak + lb; k, l \in \mathbb{Z} \text{ a } ak + bl > 0\}.$$

Buď $e = \min \mathbb{M}$. Je $e > 0$, $e = a\alpha + b\beta$, kde α, β jsou celá čísla. Dokážeme, že $e = d$. Musíme dokázat dvě věci:

(I) $e \mid a$ a $e \mid b$,

(II) Jestliže f je kladné celé číslo, $f \mid a$, $f \mid b$, pak $f \mid e$.

ad(I) Provedeme dělení se zbytkem: $a = eq + r$, kde q, r jsou celá čísla, $0 \leq r < e$. Předpokládejme, že $0 < r$.

$$a = eq + r$$
$$a = (a\alpha + b\beta)q + r$$
$$a = a\alpha q + b\beta q + r$$
$$r = a - a\alpha q - b\beta q$$
$$r = a(1 - \alpha q) + b(-\beta q)$$

Odtud vidíme, že $r \in \mathbb{M}$. Avšak $r < e = \min \mathbb{M}$, což je spor. Nutně tedy musí být $r = 0$, pak $a = eq$, tj. $e \mid a$. Stejně se dokáže $e \mid b$.

ad(II) Nechť f je kladné celé číslo, $f \mid a$, $f \mid b$. Chceme: $f \mid e$. Podle předpokladu je $a = fa'$, $b = fb'$, kde a', b' jsou kladná celá čísla. Počítejme:

$$\begin{aligned} e &= a\alpha + b\beta \\ &= fa'\alpha + fb'\beta \\ &= f(a'\alpha + b'\beta), \end{aligned}$$

odtud $f \mid e$. Dokázali jsme, že $e = d$. Platí tedy $d = a\alpha + b\beta$, kde α, β jsou celá čísla.

□

Díky této větě jsme schopni provést krok (II) v důkazu věty 3.1 bez použití rozšířeného Euklidova algoritmu. Zbytek důkazu by neměl být pro středoškolského studenta problém.

Kapitola 4

Lineární diofantické rovnice o n neznámých

V této kapitole vycházím z [4, str. 200 – 203].

Definice 4.1. *Lineární diofantickou rovnici o n neznámých nazveme každou rovnici ve tvaru*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{4.1}$$

kde $a_1, a_2, \ldots, a_n, b$ jsou celá čísla, $a_i \neq 0$ pro všechna $i = 1, 2, \ldots, n$ a $x_1, x_2, \ldots, x_n$ jsou neznámé, n je kladné celé číslo.

Označme $d = gcd(a_1, a_2, \ldots, a_n)$, potom můžeme psát $a_i = d \cdot a_i'$, a_i' je celé číslo, pro všechna $i = 1, 2, \ldots, n$. Pak lze číslo d v rovnici (4.1) vytknout a dostáváme

$$d \cdot (a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n) = b,$$

odkud vidíme, že pro libovolná celá $x_1, x_2, \ldots, x_n$ je levá strana rovnice dělitelná číslem d, proto aby tato rovnice měla celočíselné řešení, musí $d \mid b$. Potom lze psát

$$a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n = b', \tag{4.2}$$

kde $b' = d \cdot b$ a navíc už je $gcd(a_1', a_2', \ldots, a_n') = 1$. Pokud tedy má rovnice (4.1) celočíselné řešení, lze vždy převést na rovnici (4.2).

Definice 4.2. *Jestliže je v rovnici* (4.1) $gcd(a_1, a_2, \ldots, a_n) = 1$*, pak budeme říkat, že je tato rovnice v základním tvaru.*

Věta 4.1. *Nechť n je kladné celé číslo, $n \geq 2$. Rovnice* (4.1) *má v základním tvaru vždy celočíselné řešení..*

Důkaz.

Provedeme ho indukcí vzhledem k n. Musíme tedy dokázat následující:

(I) Dokážeme tvrzení pro $n = 2$.

(II) Budeme předpokládat, že věta platí pro $n - 1$ a ukážeme, že platí také pro n.

ad(I) Řešíme rovnici

$$a_1x_1 + a_2x_2 = b,$$

což je lineární diofantická rovnice, které jsme věnovali předešlou kapitolu, ze které podle věty 3.1 víme, že tato rovnice bude mít vždy celočíselné řešení, neboť máme $gcd(a_1, a_2) = 1$.

ad(II) Nyní nechť je $n > 2$. Předpokládáme, že věta platí pro rovnice o $n - 1$ neznámých a dokážeme ji pro rovnici (4.1) o n neznámých. Označme $d = gcd(a_1, a_2, \ldots, a_{n-1})$. Nechť celá čísla $x_1, x_2, \ldots, x_n$ jsou řešením, pak musí splňovat kongruenci

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{d}.$$

Protože $d \mid a_i$, pro všechna $i = 1, 2, \ldots, n - 1$ dostáváme

$$a_nx_n \equiv b \pmod{d}. \tag{4.3}$$

Neboť je $gcd(d, a_n) = gcd(a_1, a_2, \ldots, a_{n-1}, a_n) = 1$, má kongruence (4.3) podle věty 3.13 řešení a dokážeme jí upravit na tvar

$$x_n \equiv c \pmod{d},$$

kde c je nějaké celé číslo, neboli $x_n = c + dt$, kde t je celé číslo. Dosazením do rovnice (4.1) obdržíme

$$\begin{aligned} a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + a_n(c + dt) &= b \\ a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} &= b - a_nc - a_ndt \\ d \cdot (a'_1x_1 + a'_2x_2 + \cdots + a'_{n-1}x_{n-1}) &= b - a_nc - a_ndt. \end{aligned}$$

Rovnici můžeme vydělit číslem d neboť je $a_n c \equiv b \pmod{d}$, tj. $d \mid (b - a_n c)$. Získáváme tak

$$a'_1 x_1 + a'_2 x_2 + \cdots + a'_{n-1} x_{n-1} = b',$$

kde $b' = (b - a_n c)/d - a_n t$. V této rovnici už je $gcd(a'_1, a'_2, \ldots, a'_{n-1}) = 1$ a podle předpokladů, má tato rovnice celočíselné řešení.

□

Budeme věnovat pozornost už pouze diofantickým rovnicím o n neznámých pro $n \geq 3$, případem $n = 2$ jsme se dosti podrobně zabývali v přechozí kapitole, navíc budeme uvažovat rovnici (4.1) tak, že je $a_i \neq 1$ pro všechna $i = 1, 2, \ldots, n$. Kdyby bylo pro nějaké $k \in \{1, 2, \ldots, n\}$ $a_k = 1$, pak řešením této rovnice jsou čísla tvaru

$$\begin{aligned}
x_1 &= t_1 \\
x_2 &= t_2 \\
&\vdots \\
x_k &= b - a_1 t_1 - a_2 t_2 - \ldots - a_n t_n \\
&\vdots \\
x_n &= t_n,
\end{aligned}$$

kde $t_1, t_2, \ldots, t_{k-1}, t_{k+1}, \ldots, t_n$ jsou celá čísla.

4.1 Metoda řešení kongruencí

Při výpočtech konkrétních příkladů budeme postupovat obdobně jako v předchozím důkazu, to znamená, že budeme řešit kongruenci podle modulu, který je největším společným dělitelem $n-1$ koeficientů, za předpokladu, že bude různý od 1, pak budeme řešit kongruenci o jedné neznámé a následně postupně dopočítáme zbývající proměnné.

Pro přehlednost výpočtu budeme v případě malého počtu neznámých užívat značení pro neznámé x, y, z, u atd. místo $x_1, x_2, \ldots, x_n$.

Příklad 4.1. $12x - 9y + 5z = 13$

Libovolné celočíselné řešení musí nutně splňovat následující kongruenci, kterou hned začneme upravovat

$$\begin{aligned} 12x - 9y + 5z &\equiv 13 \pmod 3 \\ 2z &\equiv 4 \pmod 3 \\ z &\equiv 2 \pmod 3 \\ z &= 2 + 3t, \end{aligned}$$

kde t je celé číslo. Dosadíme řešení pro z do zadané rovnice.

$$\begin{aligned} 12x - 9y + 5 \cdot (2 + 3t) &= 13 \\ 12x - 9y + 10 + 15t &= 13 \\ 12x - 9y &= 3 - 15t \\ 4x - 3y &= 1 - 5t \end{aligned} \tag{4.4}$$

Tím jsme dostali lineární diofantickou rovnici o dvou neznámých, kterou umíme řešit z předešlé kapitoly.

$$\begin{aligned} 4x - 3y &\equiv 1 - 5t \pmod 4 \\ y &\equiv 1 + 3t \pmod 4 \\ y &= 1 + 3t + 4s, \end{aligned}$$

kde s je celé číslo. Dosazením za y do rovnice (4.4) dostaneme rovnici pouze pro x,

kterou vyřešíme.

$$\begin{aligned} 4x - 3(1 + 3t + 4s) &= 1 - 5t \\ 4x - 3 - 9t - 12s &= 1 - 5t \\ 4x &= 4 + 4t + 12s \\ x &= 1 + t + 3s \end{aligned}$$

Řešením jsou tedy všechna čísla x, y, z, která jsou tvaru

$$\begin{aligned} x &= 1 + t + 3s \\ y &= 1 + 3t + 4s \\ z &= 2 + 3t, \end{aligned}$$

kde t, s jsou celá čísla.

Příklad 4.2. $17x + 5y - 3z = 4$

Tento příklad se od předchozího liší v tom, že pro libovolnou dvojici koeficientů je nějvetší společný dělitel těchto koeficientů roven jedné. Proto budeme postupovat tak, že jako modul zvolíme jeden z koeficientů, tím se zbavíme jedné neznámé, přebytečné neznámé pak následně volíme jako celočíselné parametry s jejichž pomocí příklad dořešíme.

$$\begin{aligned} 17x + 5y - 3z &\equiv 4 \pmod 3 \\ 2x + 2y &\equiv 4 \pmod 3 \\ x + y &\equiv 2 \pmod 3 \end{aligned}$$

Nechť $y = t$, kde t je celé číslo, pak

$$\begin{aligned} x + t &\equiv 2 \pmod 3 \\ x &\equiv 2 - t \pmod 3 \\ x &= 2 - t + 3s, \end{aligned}$$

kde s je celé číslo. Dosazením do zadání dostaneme řešení pro z.

$$\begin{aligned} 17 \cdot (2 - t + 3s) + 5t - 3z &= 4 \\ 3z &= 34 - 17t + 51s + 5t - 4 \\ 3z &= 30 - 12t + 51s \\ z &= 10 - 4t + 17s \end{aligned}$$

Celkem

$$\begin{aligned} x &= 2 - t + 3s \\ y &= t \\ z &= 10 - 4t + 17s, \end{aligned}$$

kde t, s jsou celá čísla.

Příklad 4.3. $-14x - 2y + 5z + 3u = 2$

Budeme postupovat podobně jako v předchozím příkladě.

$$\begin{aligned} -14x - 2y + 5z + 3u &\equiv 2 \pmod 5 \\ x - 2y + 3u &\equiv 2 \pmod 5 \end{aligned}$$

Nechť $y = t$ a $u = s$, kde t, s jsou celá čísla, pak

$$\begin{aligned} x - 2t + 3s &\equiv 2 \pmod 5 \\ x &\equiv 2 + 2t - 3s \pmod 5 \\ x &= 2 + 2t - 3s + 5r, \end{aligned}$$

kde r je celé číslo. Dosazením dopočítáme poslední neznámou.

$$\begin{aligned} -14 \cdot (2 + 2t - 3s + 5r) - 2t + 5z + 3s &= 2 \\ -28 - 28t + 42s - 70r - 2t + 5z + 3s &= 2 \\ 5z &= 30 + 30t - 45s + 70r \\ z &= 6 + 6t - 9s + 14r \end{aligned}$$

Dohromady

$$\begin{aligned} x &= 2 + 2t - 3s + 5r \\ y &= t \\ z &= 6 + 6t - 9s + 14r \\ u &= s, \end{aligned}$$

kde t, s, r jsou celá čísla.

4.2 Metoda redukce na menší počet neznámých

Následující postup navrhnul vedoucí práce. Výhoda této metody spočívá v tom, že nebudeme potřebovat kongruence, vystačíme si jen s rozšířeným Euklidovým algoritmem.

Omezíme se na případ, kdy je rovnice (4.1) v základním tvaru, neboť pokud není a má celočíselné řešení, můžeme jí na tento tvar převést. Připomínám, že uvažujeme $n \geq 3$.

Určíme $d = gcd(a_1, a_2, \ldots, a_{n-1})$ a položme $a'_i = \dfrac{a_i}{d}$ pro $i = 1, 2, \ldots, n-1$.

$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + a_nx_n = b$$
$$a'_1dx_1 + a'_2dx_2 + \cdots + a'_{n-1}dx_{n-1} + a_nx_n = b$$
$$d(a'_1x_1 + a'_2x_2 + \cdots + a'_{n-1}x_{n-1}) + a_nx_n = b$$

Provedeme-li substituci $y = a'_1x_1 + a'_2x_2 + \cdots + a'_{n-1}x_{n-1}$, obdržíme lineární diofantickou rovnici o dvou neznámých[1)]

$$dy + a_nx_n = b,$$

tím je problém převeden na případ, který umíme řešit. Po nalezení řešení y, x_n budeme řešit rovnici

$$a'_1x_1 + a'_2x_2 + \cdots + a'_{n-1}x_{n-1} = y,$$

kde máme o jednu neznámou meně než na počátku a bude mít celočíselné řešení, neboť je $gcd(a'_1, a'_2, \ldots, a'_{n-1}) = 1$. Celý postup můžeme opakovat, dokud rovnici (4.1) nezredukujeme na lineární diofantickou rovnici o dvou neznámých, kterou umíme řešit. Tím získáme všechna řešení rovnice (4.1).

Ukažme si uvedený postup pro $n = 3$. Řešíme rovnici v základním tvaru

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

kde a, b, c, d jsou celá čísla, $a > 1$, $b > 1$, $c > 1$.

[1)] Tato rovnice samozřejmě bude mít celočíselné řešení, neboť platí:
$gcd(d, a_n) = gcd(a_1, a_2, \ldots, a_{n-1}, a_n) = 1$.

Označme $D = gcd(a, b)$, potom $a = Da'$, $b = Db'$, kde a', b' jsou kladná celá čísla a platí $gcd(a', b') = 1$, $gcd(D, c) = 1$.

$$\begin{aligned} ax + by + cz &= d \\ Da'x + Db'y + cz &= d \\ D(a'x + b'y) + cz &= d \\ Du + cz &= d \end{aligned}$$

Označili jsme $a'x + b'y = u$. Pomocí rozšířeného Euklidova algoritmu najdeme čísla u_0, c_0 splňující $Du_0 + cz_0 = 1$. Pak $u = du_0 - pc$, $z = dz_0 + pD$, kde p je celé číslo. Nyní vyřešíme rovnici $a'x + b'y = du_0 - pc$. Opět pomocí rozšířeného Euklidova algoritmu nalezneme celá čísla x_0, y_0 splňující $a'x_0 + b'y_0 = 1$. Pak $x = x_0(du_0 - pc) - b'q$, $y = y_0(du_0 - pc) + a'q$, kde q je celé číslo.

Celá čísla x, y, z řeší rovnici $ax + by + cz = d$ právě tehdy, když

$$\begin{aligned} x &= x_0 du_0 - x_0 cp - b'q \\ y &= y_0 du_0 - y_0 cp + a'q \\ z &= z_0 d + pD, \end{aligned}$$

kde p, q jsou celá čísla.

Příklad 4.4. $12x + 9y + 5z = 4$

Je $gcd(12, 9) = 3$, potom

$$\begin{aligned} 12x + 9y + 5z &= 4 \\ 3(4x + 3y) + 5z &= 4 \\ 3u + 5z &= 4, \end{aligned}$$

kde jsme zavedli substituci $4x + 3y = u$. Vyřešíme rovnici $3u + 5z = 4$. Pomocí rozšířeného Euklidova algoritmu získáme následující Bezoutovu rovnost, kterou budeme dále upravovat

$$\begin{aligned} 3(2) + 5(-1) &= 1 \\ 3(8) + 5(-4) &= 4, \end{aligned}$$

řešením rovnice $3u + 5z = 4$ jsou pak čísla tvaru

$$u = 8 + 5p \qquad z = -4 - 3p,$$

kde p je celé číslo. Vrátíme se k substituci, musíme vyřešit rovnici $4x + 3y = 8 + 5p$. Opět pomocí rozšířeného Euklidova algoritmu získáme Bezoutovu rovnost

$$4(1) + 3(-1) = 1$$
$$4(8 + 5p) + 3(-8 - 5p) = 8 + 5p,$$

řešením jsou pak čísla tvaru

$$x = 8 + 5p - 3q \qquad y = -8 - 5p + 4q,$$

kde q je celé číslo. Řešením rovnice $12x + 9y + 5z = 4$ jsou celá čísla tvaru

$$x = 8 + 5p - 3q$$
$$y = -8 - 5p + 4q$$
$$z = -4 - 3p,$$

kde p, q jsou celá čísla.

Cvičení 4.1. Vyřešte diofantické rovnice:

(a) $12x + 16y - 7z = 26$

(b) $8x - 32y + 48z - 3u = 12$

(c) $12x + 13y - 4z + 2u = 25$

(d) $5x + 15y - 25z = 4$

Kapitola 5

Lineární diofantické rovnice vzhledem k alespoň jedné neznámé

V této kapitole vycházím z [4, kapitola 3].

Neprve si povíme, jak řešit nelineární kongruenci s jednou neznámou, tj. kongruenci, ve které se na obou stranách nachází polynom proměnné x s celočíselnými koeficienty. Je jasné, že tuto kongruenci můžeme převést na tvar

$$F(x) \equiv 0 \pmod{m}, \tag{5.1}$$

kde m je kladné celé číslo.

Věta 5.1. *Nechť $F(x)$ je polynom s celočíselnými koeficienty, m je kladné celé číslo. Nechť jsou dána celá čísla a, b, navíc taková, že $a \equiv b \pmod{m}$. Pak platí $F(a) \equiv F(b) \pmod{m}$.*

Důkaz.

Nechť $F(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, kde c_n, $c_{n-1}, \ldots, c_1$, c_0 jsou celá čísla. Protože podle předpokladů je $a \equiv b \pmod{m}$, můžeme pro všechna $i = 0, 1, \ldots, n$ podle věty 3.10 psát

$$a^i \equiv b^i \pmod{m}$$

a navíc podle (III) ve větě 3.9

$$c_i a^i \equiv c_i b^i \pmod{m}.$$

Díky (I) z věty 3.9 můžeme všechny tyto kongruence sečíst.

$$\sum_{0 \le i \le n} c_i a^i \equiv \sum_{0 \le i \le n} c_i b^i \pmod{m}$$

Tím dostáváme

$$F(a) \equiv F(b) \pmod{m},$$

což jsme měli dokázat. □

Věta 5.2. *Nechť existuje přesně k celých čísel a splňujících*

$$0 \leq a < m \quad \wedge \quad F(a) \equiv 0 \pmod{m}.$$

Označme tato čísla $a_1, \ldots, a_k$. Buď x celé číslo. Pak platí: x řeší kongruenci (5.1) *právě tehdy, když $x \equiv a_i \pmod{m}$, pro nějaké $i \in \{1, \ldots, k\}$.*

Důkaz.
Je potřeba dokázat dvě věci.

(I) Jestliže x řeší kongruenci (5.1), pak $x \equiv a_i \pmod{m}$ pro nějaké $i \in \{1, \ldots, k\}$.

(II) Jestliže $x \equiv a_i \pmod{m}$ pro nějaké $i \in \{1, \ldots, k\}$, pak x řeší kongruenci (5.1).

ad(I) Platí $F(x) \equiv 0 \pmod{m}$. Vydělíme celé číslo x se zbytkem číslem m. Je tedy $x = qm + a$, kde q, a jsou celá čísla, $0 \leq a < m$. Je tedy $x \equiv a \pmod{m}$. Podle věty 5.1 platí: $F(x) \equiv F(a) \pmod{m}$. Pak $F(a) \equiv 0 \pmod{m}$ a tedy $a = a_i$ pro nějaké $i \in \{1, \ldots, k\}$. Takže $x \equiv a_i \pmod{m}$ pro nějaké $i \in \{1, \ldots, k\}$.

ad(II) Nechť $i \in \{1, \ldots, k\}$, $x \equiv a_i \pmod{m}$. Podle věty 5.1 platí $F(x) \equiv F(a_i) \pmod{m}$, takže $F(x) \equiv 0 \pmod{m}$, tedy x řeší kongruenci (5.1).

□

Věta 5.2 nám dává jasný návod jak řešit kongruenci (5.1).

(I) Všech m celých čísel a splňujících $0 \leq a < m$ dosadíme postupně do kongruence (5.1). Zjistíme, která z nich této kongruenci vyhovují, označme je $a_1, a_2, \ldots, a_k$. V případě, že žádné takové číslo a neexistuje, nemá kongruence (5.1) řešení a již dále nepostupujeme.

(II) Pro $i = 1, 2, \ldots, k$ označme $\mathbb{M}_i$ množinu celých čísel x, která řeší kongruenci $x \equiv a_i \pmod{m}$.

(III) Označme $\mathbb{M}$ množinu všech celých čísel x, která řeší kongruenci (5.1). Je

$$\mathbb{M} = \bigcup_{i \in \{1,\, 2,\ldots,\, k\}} \mathbb{M}_i.$$

Toto je univerzální metoda, která se ovšem s rostoucím m stává pracnější, neboť m udává počet čísel, která musíme dosadit do (5.1).

Při výpočtech se nám často bude hodit následující věta, známá jako Malá Fermatova věta. Nejprve několik pomocných vět.

Lemma 5.1. *Nechť p je prvočíslo. Nechť a, b jsou celá čísla. Jestliže $p \mid ab$, pak musí $p \mid a$ nebo $p \mid b$.*

Důkaz.
Číslo $gcd(p,\, a)$ je kladný dělitel čísla p. Protože p je prvočíslo, musí být $gcd(p,\, a) = p$, nebo $gcd(p,\, a) = 1$. V prvním případě dostáváme, že $p \mid a$, ve druhém případě podle lemmatu 3.1 musí $p \mid b$. □

Obměnou lemma 5.1 dostáváme další lemma.

Lemma 5.2. *Nechť p je prvočíslo. Nechť a, b jsou celá čísla. Jestliže $p \nmid a$ a zároveň $p \nmid b$, pak $p \nmid ab$.*

Lemma 5.3. *Nechť p je prvočíslo. Nechť k je celé číslo, $1 \leq k < p-1$. Pak $p \mid \binom{p}{k}$.*

Důkaz.

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1}$$

$$\binom{p}{k} k(k-1)\ldots 1 = p(p-1)\ldots(p-k+1)$$

Z poslední rovnosti vidíme, že $p \mid \binom{p}{k} k(k-1)\ldots 1$. Pro i celé, $0 < i < p$, zřejmě $p \nmid i$. Takže $p \nmid 1$, $p \nmid 2, \ldots, p \nmid k$. Podle lemmatu 5.2 $p \nmid k(k-1)\ldots 1$. Konečně podle lemmatu 5.1 musí $p \mid \binom{p}{k}$. □

Věta 5.3 (Malá Fermatova věta)**.** *Nechť p je prvočíslo. Nechť a je libovolné celé číslo. Pak platí*

$$a^p \equiv a \pmod{p}, \tag{5.2}$$

specielně pokud je $gcd(a,\, p) = 1$, tj. pokud $p \nmid a$, platí

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.3}$$

Důkaz.

Nejprve dokážeme první část, tj. platnost kongruence (5.2). Specielně uvažujme $p = 2$. Jedno z celých čísel a, $a - 1$ je sudé. Proto $2 \mid a(a-1)$, $2 \mid a^2 - a$, tj. $a^2 \equiv a \pmod 2$.

Nyní uvažujme lichá prvočísla p a důkaz věty rozdělíme na dvě části.

(I) Větu dokážeme pro $a \geq 0$.

(II) Větu dokážeme pro $a < 0$.

ad(I) Použijeme matematickou indukci vzhledem k a:

(i) Dokážeme, že kongruence (5.2) platí pro $a = 0$.

(ii) Budeme předpokládat, že kongruence (5.2) platí pro $a - 1$, kde $a > 0$ a dokážeme, že platí pro a.

ad(i) To je jednoduché, $0^p = 0 \equiv 0 \pmod p$.

ad(ii) Nechť je $a > 0$. Předpokládáme, že platí $(a-1)^p \equiv a - 1 \pmod p$. Chceme dokázat $a^p \equiv a \pmod p$. Počítejme:

$$a^p = ((a-1)+1)^p = \sum_{0 \leq i \leq p} \binom{p}{i} (a-1)^i = 1 + (a-1)^p + \sum_{1 \leq i \leq p-1} \binom{p}{i} (a-1)^i$$

Použili jsme binomickou větu. Podle lemmatu 5.3 je každé z čísel $\binom{p}{i}$ dělitelné číslem p, pro všechna celá i, $1 \leq i \leq p-1$, proto $p \mid \sum_{1 \leq i \leq p-1} \binom{p}{i} (a-1)^i$, tedy $\sum_{1 \leq i \leq p-1} \binom{p}{i} (a-1)^i \equiv 0 \pmod p$. Navíc s využitím indukčního předpokladu dostáváme

$$a^p = 1 + (a-1)^p + \sum_{1 \leq i \leq p-1} \binom{p}{i} (a-1)^i \equiv 1 + (a-1) + 0 = a \pmod p,$$

což jsme chtěli dokázat.

ad(II) Nechť $a < 0$. Pak $-a > 0$ a dle již dokázané části (I) máme:

$$(-a)^p \equiv -a \pmod p.$$

Protože p je liché prvočíslo dostáváme:

$$(-a)^p = ((-1) \cdot (a))^p = (-1)^p \cdot a^p = -a^p,$$

takže $-a^p \equiv -a \pmod p$, $a^p \equiv a \pmod p$.

Zbývá dokázat druhou část tvrzení. Platí

$$a^p \equiv a \pmod{p}$$
$$a \cdot a^{p-1} \equiv a \pmod{p}$$

a s použitím věty 3.11 dostáváme $a^{p-1} \equiv 1 \pmod{p}$. □

Jak nám tato věta pomůže si ukážeme na příkladech.

Příklad 5.1. $x^{2015} + 2 \equiv 0 \pmod{3}$

Podle návodu popsaného výše je třeba spočítat $F(0)$, $F(1)$, $F(2)$. Počítejme:

$$F(0) = 0^{2015} + 2 = 0 + 2 \equiv 2 \pmod{3}$$
$$F(1) = 1^{2015} + 2 = 1 + 2 = 3 \equiv 0 \pmod{3}$$
$$F(2) = 2^{2015} + 2 \equiv 2 + 2 = 4 \equiv 1 \pmod{3}$$

V posledním výpočtu jsme použili Malou Fermatovu větu, tj. větu 5.3, neboť je $gcd(2, 3) = 1$, pak platí, že $2^2 \equiv 1 \pmod{3}$. S využitím (III) z věty 3.9 a věty 3.10 je

$$2^2 \equiv 1 \pmod{3}$$
$$\left(2^2\right)^{1007} \equiv 1^{1007} \pmod{3}$$
$$\left(2^2\right)^{1007} \cdot 2 \equiv 1^{1007} \cdot 2 \pmod{3}$$
$$2^{2014+1} \equiv 1^{1007} \cdot 2 \pmod{3}$$
$$2^{2015} \equiv 2 \pmod{3}.$$

Řešením jsou všechna x vyhovující kongruenci $x \equiv 1 \pmod{3}$, tj. čísla tvaru $x = 1 + 3t$, kde t je celé číslo.

Malou Fermatovu větu můžeme využít jinak. Zadanou kongruenci $x^{2015} + 2 \equiv 0 \pmod{3}$ nahradíme kongruencí, která je s ní ekvivalentní.

Uvažujme nejprve x takové, že platí $3 \mid x$, pak $x \equiv 0 \pmod{3}$ a podle (III) z věty 3.9 je $x^{2015} \equiv 0 \pmod{3}$. Je tedy

$$x^{2015} + 2 \equiv 0 + 2 = 2 \pmod{3}$$

a žádné řešení pro tento případ nedostáváme.

Nyní nechť $3 \nmid x$, pak platí $x^2 \equiv 1 \pmod 3$.

$$x^{2015} = x^{2\cdot 1007+1} = \left(x^2\right)^{1007} \cdot x \equiv 1^{1007} \cdot x = x \pmod p$$

Takže

$$x^{2015} + 2 \equiv x + 2 \pmod 3.$$

Stačí tedy vyřešit $x + 2 \equiv 0 \pmod 3$.

$$\begin{aligned} x + 2 &\equiv 0 \pmod 3 \\ x &\equiv -2 \pmod 3 \\ x &\equiv 1 \pmod 3 \\ x &= 1 + 3t, \end{aligned}$$

kde t je celé číslo.

Příklad 5.2. $x^7 - 4x - 2 \equiv 0 \pmod 5$

Tuto kongruenci bude výhodné nahradit kongruencí s ní ekvivalentní.

$$x^7 - 4x - 2 = x^5 \cdot x^2 - 4x - 2 \equiv x \cdot x^2 + x + 3 = x^3 + x + 3 \pmod 5$$

Stačí nám vyřešit $x^3 + x + 3 \equiv 0 \pmod 5$.

$$\begin{aligned} F(0) &= 0 + 0 + 3 \equiv 3 \pmod 5 \\ F(1) &= 1 + 1 + 3 = 5 \equiv 0 \pmod 5 \\ F(2) &= 8 + 2 + 3 = 13 \equiv 3 \pmod 5 \\ F(3) &= 27 + 3 + 3 = 33 \equiv 3 \pmod 5 \\ F(4) &= 64 + 4 + 3 = 71 \equiv 1 \pmod 5 \end{aligned}$$

Řešením jsou čísla tvaru $x = 1 + 5t$, kde t je celé číslo.

Ikdyž jsme nikde v textu nevyslovili přesnou definici polynomu jedné proměnné, často jsme s tímto pojmem pracovali a předpokládali, že čtenář alespoň intuitivně ví, o co se jedná. Nyní ovšem budeme pracovat s polynomy k proměnných, kde k je kladné celé číslo, $k > 1$. Ty je potřeba přesně definovat, pro jednoduchost a přehlednost začneme s $k = 2$, následně vše zobecníme.

Definice 5.1. *Polynomem dvou proměnných $F(x, y)$ s celočíselnými koeficienty budeme rozumět výraz ve tvaru*

$$F(x, y) = \sum_{0 \leq i \leq n} f_i(x) y^i,$$

kde pro $i = 1, 2, \ldots, n$ je $f_i(x)$ polynom jedné proměnné s celočíselnými koeficienty, tj.

$$f_i(x) = \sum_{0 \leq j \leq n_i} c_{ij} x^j.$$

Věta 5.4. *Nechť $F(x, y)$ je polynom dvou proměnných s celočíselnými koeficienty, m je kladné celé číslo. Nechť jsou dána celá čísla a_1, a_2, b_1, b_2, navíc taková, že $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$. Pak platí $F(a_1, a_2) \equiv F(b_1, b_2) \pmod{m}$.*

Důkaz.

Protože platí $a_1 \equiv b_1 \pmod{m}$, je splněn předpoklad věty 5.1 a proto pro $i = 1, 2, \ldots, n$ je $f_i(a_1) \equiv f_i(b_1) \pmod{m}$. Podle věty 3.10 je ${a_2}^i \equiv {b_2}^i \pmod{m}$, pro $i = 1, 2, \ldots, n$. Podle (III) z věty 3.9 pro $i = 1, 2, \ldots, n$ je $f_i(a_1){a_2}^i \equiv f_i(a_1){b_2}^i \pmod{m}$. A konečně podle (I) z věty 3.9 je

$$\sum_{0 \leq i \leq n} f_i(a_1){a_2}^i \equiv \sum_{0 \leq i \leq n} f_i(a_1){b_2}^i \pmod{m},$$

což je

$$F(a_1, a_2) \equiv F(b_1, b_2) \pmod{m}.$$

□

Je zřejmé, že bychom mohli analogicky definovat polynom tří proměnných a následně vyslovit a dokázat větu 5.4 pro polynom tří proměnných. A takto bychom mohli stále pokračovat. Výsledkem je následující zobecnění.

Definice 5.2. *Polynomem k proměnných $F(x_1, x_2, \ldots, x_k)$ s celočíselnými koeficienty budeme rozumět výraz ve tvaru*

$$F(x_1, x_2, \ldots, x_k) = \sum_{0 \leq i \leq n} f_i(x_1, x_2, \ldots, x_{k-1}){x_k}^i,$$

kde pro $i = 1, 2, \ldots, n$ je $f_i(x_1, x_2, \ldots, x_{k-1})$ polynom $k - 1$ proměnných s celočíselnými koeficienty.

Věta 5.5. *Nechť $F(x_1, x_2, \ldots, x_k)$ je polynom k proměnných s celočíselnými koeficienty, m je kladné celé číslo. Nechť jsou dána celá čísla a_1, $a_2, \ldots, a_k$, b_1, $b_2, \ldots, b_k$, navíc taková, že $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}, \ldots, a_k \equiv b_k \pmod{m}$. Pak platí $F(a_1, a_2, \ldots, a_k) \equiv F(b_1, b_2, \ldots, b_k) \pmod{m}$.*

Definice 5.3. *Lineární diofantickou rovnicí vzhledem k alespoň jedné neznámé budeme rozumět každou rovnici ve tvaru*

$$F(x_1, x_2, \ldots, x_{s-1}, x_s) = 0, \tag{5.4}$$

kde $F(x_1, x_2, \ldots, x_{s-1}, x_s)$ je polynom s celočíselnými koeficienty a alespoň jedna z neznámých, označme jí x_s, se v (5.4) vyskytuje pouze v první mocnině.

Je jasné, že (5.4) lze upravit na tvar

$$P(x_1, x_2, \ldots, x_{s-1}) = mx_s, \tag{5.5}$$

kde m je kladné celé číslo a $P(x_1, x_2, \ldots, x_{s-1})$ je polynom $s-1$ proměnných s celočíselnými koeficienty.

Bude-li $m = 1$, je řešení jasné:

$$\begin{aligned} x_1 &= t_1 \\ x_2 &= t_2 \\ &\vdots \\ x_{s-1} &= t_{s-1} \\ x_s &= P(t_1, t_2, \ldots, t_{s-1}), \end{aligned}$$

kde t_1, $t_2, \ldots, t_{s-1}$ jsou celá čísla. Od této chvíle uvažujeme $m \neq 1$.

Nechť x_1, $x_2, \ldots, x_{s-1}$, x_s je celočíselné řešení rovnice (5.5), pak toto řešení musí vyhovovat kongruenci

$$P(x_1, x_2, \ldots, x_{s-1}) \equiv 0 \pmod{m}. \tag{5.6}$$

Obdrželi jsme nelineární kongruenci $s-1$ proměnných. Tu dokážeme vyřešit díky větě 5.5, postup bude analogický postupu při řešení kongruence (5.1).

Abychom nalezli řešení kongruence (5.6) musíme do polynomu $P(x_1, x_2, \ldots, x_{s-1})$ za $(x_1, x_2, \ldots, x_{s-1})$ volit všechny prvky $(a_1, a_2, \ldots, a_{s-1}) \in \{0, 1, \ldots, m-1\}^{s-1}$. A právě tehdy, když je pro čísla a_1, $a_2, \ldots, a_{s-1}$ splněna podmínka

$$P(a_1, a_2, \ldots, a_{s-1}) \equiv 0 \pmod{m},$$

dostáváme řešení kongruence (5.6) ve tvaru

$$\begin{aligned} x_1 &= a_1 + t_1 m \\ x_2 &= a_2 + t_2 m \\ &\vdots \\ x_{s-1} &= a_{s-1} + t_{s-1} m, \end{aligned}$$

kde $t_1, t_2, \ldots, t_{s-1}$ jsou celá čísla. Řešení rovnice (5.5) je potom

$$\begin{aligned} x_1 &= a_1 + t_1 m \\ x_2 &= a_2 + t_2 m \\ &\vdots \\ x_{s-1} &= a_{s-1} + t_{s-1} m \\ x_s &= \frac{1}{m} P(a_1 + t_1 m,\, a_2 + t_2 m, \ldots,\, a_{s-1} + t_{s-1} m). \end{aligned}$$

Číslo m^{s-1} vyjadřuje počet dosazení[1)], která musíme provést, abychom ověřili podmínku $P(a_1, a_2, \ldots, a_{s-1}) \equiv 0 \pmod{m}$. Vidíme, že tento počet je mocninnou funkcí vzhledem ke koeficientu stojícím u neznámé x_s, tj. m, která je v rovnici (5.5) zastoupena lineárně, a dále tento počet roste exponenciálně vzhledem k počtu neznámých v rovnici (5.5). S rostoucím m a s se řešení rovnice (5.4) stává velmi zdlouhavým pro ruční počítání, nicméně uvedená metoda je univerzální a po konečném počtu kroků vždy nalezne všechna řešení. K urychlení a usnadnění práce by jistě šel využít počítač. V následujících řešených příkladech a cvičeních se proto vyhneme zbytečně komplikovaným a zdlouhavým výpočtům tím, že počet neznámých nebude vyšší než 3 a koeficient m nebudeme volit příliš velký.

Příklad 5.3. $13x^3 - 6y + 5 = 0$

Rovnice je lineární vzhledem k neznámé y, aplikujme výše uvedený postup.

$$\begin{aligned} 13x^3 - 6y + 5 &= 0 \\ 13x^3 + 5 &= 6y \end{aligned}$$

Označme $P(x) = 13x^3 + 5$.

$$\begin{aligned} P(x) &= 6y \\ P(x) &\equiv 0 \pmod{6} \end{aligned}$$

[1)] Jedná se o počet prvků množiny $\{0, 1, \ldots, m-1\}^{s-1}$.

Podle návodu bychom do polynomu $P(x)$ měli dosazovat čísla $a \in \{0, 1, 2, 3, 4, 5\}$ a zkoumat, pro která a nastane $P(a) \equiv 0 \pmod 6$. Jednodušeji se nám ovšem bude dosazovat do polynomu $Q(x) = x^3 + 5$, neboť platí, že

$$P(x) = 13x^3 + 5 \equiv x^2 + 5 \pmod 6,$$

je tedy $Q(x) \equiv P(x) \pmod 6$.

$$\begin{aligned} Q(0) &= 0 + 5 = 5 \equiv 5 \pmod 6 \\ Q(1) &= 1 + 5 = 6 \equiv 0 \pmod 6 \\ Q(2) &= 8 + 5 = 13 \equiv 1 \pmod 6 \\ Q(3) &= 27 + 5 = 32 \equiv 2 \pmod 6 \\ Q(4) &= 64 + 5 = 69 \equiv 3 \pmod 6 \\ Q(5) &= 125 + 5 = 130 \equiv 4 \pmod 6 \end{aligned}$$

Pouze pro $x = 1$ jsme obdrželi $Q(1) \equiv 0 \pmod 6$, proto jsou řešením všechna čísla ve tvaru $x = 1 + 6t$, kde t je celé číslo. Zbývá dopočítat y.

$$6y = P(1 + 6t) = 13 \cdot (1 + 6t)^3 + 5 = 13 + 234t + 1404t^2 + 2808t^3 + 5$$

Dohromady

$$x = 1 + 3t \qquad y = 3 + 39t + 234t^2 + 468t^3,$$

kde t je celé číslo.

Příklad 5.4. $x^3 + 5y^2 - 2z = 0$

Postupovat budeme úplně stejným způsobem jako v předchozím příkladu.

$$\begin{aligned} x^3 + 5y^2 - 2z + 3 &= 0 \\ x^3 + 5y^2 + 3 &= 2z \\ x^3 + 5y^2 + 3 &\equiv 0 \pmod 2 \end{aligned}$$

Označme $P(x, y) = x^3 + 5y^2 + 3$. Platí $P(x, y) \equiv Q(x, y) = x^2 + y + 1 \pmod 2$. Počet potřebných dosazení je $2^2 = 4$.

$$\begin{aligned} Q(0, 0) &= 0 + 0 + 1 = 1 \\ Q(0, 1) &= 0 + 1 + 1 = 2 \equiv 0 \pmod 2 \\ Q(1, 0) &= 1 + 0 + 1 = 2 \equiv 0 \pmod 2 \\ Q(1, 1) &= 1 + 1 + 1 = 3 \equiv 1 \pmod 2 \end{aligned}$$

Vyhovují nám dvě různé dvojice čísel x, y. Označme $x_1 = 2t_1$, $y_1 = 1+2s_1$, kde t_1, s_1 jsou celá čísla a dopočítáme k nim příslušné z_1.

$$z_1 = \frac{1}{2}\left[P(x_1, y_1)\right] = \frac{1}{2}\left[(2t_1)^3 + 5(1+2s_1)^2 + 3\right] = 4 + 4{t_1}^3 + 10s_1 + 10{s_1}^2$$

V druhém případě označme $x_2 = 1 + 2t_2$, $y_2 = 2s_2$, kde t_2, s_2 jsou celá čísla.

$$z_2 = \frac{1}{2}\left[P(x_2, y_2)\right] = \frac{1}{2}\left[(1+2t_2)^3 + 5(2s_2)^2 + 3\right] = 2 + 10{s_2}^2 + 3t_2 + 6{t_2}^2 + 4{t_2}^3$$

Řešením jsou dvě následující různé trojice celých čísel, první trojice je

$$\begin{aligned} x_1 &= 2t_1 \\ y_1 &= 1 + 2s_1 \\ z_1 &= 4 + 4{t_1}^3 + 10s_1 + 10{s_1}^2, \end{aligned}$$

kde t_1, s_1 jsou celá čísla, druhá trojice je

$$\begin{aligned} x_2 &= 1 + 2t_2 \\ y_2 &= 2s_2 \\ z_2 &= 2 + 10{s_2}^2 + 3t_2 + 6{t_2}^2 + 4{t_2}^3, \end{aligned}$$

kde t_2, s_2 jsou celá čísla.

Příklad 5.5. $2x^2 - 3y^2 + 4z + 2 = 0$

Tento příklad již bude pracnější, neboť musíme provést $4^2 = 16$ dosazení.

$$\begin{aligned} 2x^2 - 3y^2 + 4z + 2 &= 0 \\ -2x^2 + 3y^2 - 2 &= 4z \\ -2x^2 + 3y^2 - 2 &\equiv 0 \pmod 4 \end{aligned}$$

Bude výhodné dosazovat systematicky. Označme $P(x, y) = -2x^2 + 3y^2 - 2$ a počítejme.

$$\begin{aligned} P(0,0) &= 0 + 0 - 2 = -2 \equiv 2 \pmod 4 \\ P(0,1) &= 0 + 3 - 2 = 1 \equiv 1 \pmod 4 \\ P(0,2) &= 0 + 12 - 2 = 10 \equiv 2 \pmod 4 \\ P(0,3) &= 0 + 27 - 2 = 25 \equiv 1 \pmod 4 \\ P(1,0) &= -2 + 0 - 2 = -4 \equiv 0 \pmod 4 \\ P(2,0) &= -8 + 0 - 2 = -10 \equiv 2 \pmod 4 \end{aligned}$$

$$P(3,0) = -18 + 0 - 2 = -20 \equiv 0 \pmod 4$$

$$P(1,1) = -2 + 3 - 2 = -1 \equiv 3 \pmod 4$$

$$P(1,2) = -2 + 12 - 2 = 8 \equiv 0 \pmod 4$$

$$P(1,3) = -2 + 27 - 2 = 23 \equiv 3 \pmod 4$$

$$P(2,1) = -8 + 3 - 2 = -7 \equiv 1 \pmod 4$$

$$P(3,1) = -18 + 3 - 2 = -17 \equiv 3 \pmod 4$$

$$P(2,2) = -8 + 12 - 2 = 2 \equiv 2 \pmod 4$$

$$P(2,3) = -8 + 27 - 2 = 17 \equiv 1 \pmod 4$$

$$P(3,2) = -18 + 12 - 2 = -8 \equiv 0 \pmod 4$$

$$P(3,3) = -18 + 27 - 2 = 7 \equiv 3 \pmod 4$$

Vyhovují celkem čtyři různé dvojice x, y, postupně ke každé dvojici dopočítáme příslušné z.

Pro dvojici $x_1 = 1 + 4t_1$, $y_1 = 4s_1$, kde t_1, s_1 jsou celá čísla, dostáváme

$$\begin{aligned} z_1 &= \frac{1}{4}\left[P(1 + 4t_1, 4s_1)\right] \\ &= \frac{1}{4}\left[-2(1 + 8t_1 + 16{t_1}^2) + 3(16{s_1}^2) - 2\right] \\ &= \frac{1}{4}\left[-4 - 16t_1 - 32{t_1}^2 + 48{s_1}^2\right] \\ &= -1 - 4t_1 - 8{t_1}^2 + 12{s_1}^2. \end{aligned}$$

Pro dvojici $x_2 = 3 + 4t_2$, $y_2 = 4s_2$, kde t_2, s_2 jsou celá čísla, dostáváme

$$\begin{aligned} z_2 &= \frac{1}{4}\left[P(3 + 4t_2, 4s_2)\right] \\ &= \frac{1}{4}\left[-2(9 + 24t_2 + 16{t_2}^2) + 3(16{s_2}^2) - 2\right] \\ &= \frac{1}{4}\left[-20 - 48t_2 - 32{t_2}^2 + 48{s_2}^2\right] \\ &= -5 - 12t_2 - 8{t_2}^2 + 12{s_2}^2. \end{aligned}$$

Pro dvojici $x_3 = 1 + 4t_3$, $y_3 = 2 + 4s_3$, kde t_3, s_3 jsou celá čísla, dostáváme

$$\begin{aligned} z_3 &= \frac{1}{4}\left[P(1 + 4t_3, 2 + 4s_3)\right] \\ &= \frac{1}{4}\left[-2(1 + 8t_3 + 16{t_3}^2) + 3(4 + 16s_3 + 16{s_3}^2) - 2\right] \\ &= \frac{1}{4}\left[8 - 16t_3 - 32{t_3}^2 + 48s_3 + 48{s_3}^2\right] \\ &= 2 - 4t_3 - 8{t_3}^2 + 12s_3 + 12{s_3}^2. \end{aligned}$$

Pro dvojici $x_4 = 3 + 4t_4$, $y_4 = 2 + 4s_4$, kde t_4, s_4 jsou celá čísla, dostáváme

$$\begin{aligned} z_4 &= \frac{1}{4}\left[P(3 + 4t_4, 2 + 4s_4)\right] \\ &= \frac{1}{4}\left[-2(9 + 24t_4 + 16{t_4}^2) + 3(4 + 16s_4 + 16{s_4}^2) - 2\right] \\ &= \frac{1}{4}\left[-8 - 48t_4 - 32{t_4}^2 + 48s_4 + 48{s_4}^2\right] \\ &= -2 - 12t_3 - 8{t_4}^2 + 12s_4 + 12{s_4}^2. \end{aligned}$$

Cvičení 5.1. Vyřešte následující diofantické rovnice.

(a) $3x^3 + 5y - 2z + 3 = 0$

(b) $5x^2 - 3y + 2 = 0$

(c) $4x^2 + 7y - 2 = 0$

(d) $12x^5 + 24y^6 + 3z - 12 = 0$

Kapitola 6

Pythagorejské trojice

Pythagorejskou trojicí nazveme kladná celá čísla x, y, z pokud vyhovují rovnici

$$x^2 + y^2 = z^2. \tag{6.1}$$

Rovnice (6.1) je speciální případ rovnice

$$x^n + y^n = z^n, \tag{6.2}$$

kde n je kladné celé číslo. Této rovnici se říká Fermatova rovnice a patří k jedné z nejznámějších diofantických rovnic, neboť má velmi zajímavou historii.

Touto rovnicí pro $n = 2$ se zabývali již ve starověkém Řecku a vědělo se, že bude mít nekonečně mnoho řešení. Francouzský matematik Pierre Fermat, který žil v 17. století, se domníval, že neexistují kladná celá čísla, která by vyhovovala rovnici (6.2) pro $n \geq 3$. Tato hypotéza je známa jako Velká Fermatova věta. Fermat měl na okraji jedné ze svých knih poznámku, že nalezl důkaz této věty, ale údajně je příliš dlouhý na to, aby ho zde napsal. Jeho důkaz však nebyl nikdy nalezen, nicméně víme, že se mu toto tvrzení podařilo dokázat pro $n = 4$. Konečný obecný důkaz ovšem přinesl až britský matematik Andrew Wiles v roce 1994, jedná se o nejdelší důkaz v historii matematiky. V dodatku tohoto textu si ukážeme neexistenci řešení rovnice (6.2) pro $n = 4$.

My si nyní vyřešíme rovnici (6.1). Postupovat budeme stejně, jako je tomu v [9, str. 35 – 36]. Využijeme známé identity

$$1 + 2a + a^2 = (1 + a)^2, \tag{6.3}$$

kterou bychom mohli porovnat se zkoumanou rovnicí (6.1). Potřebovali bychom, aby $1 + 2a$ bylo čtvercem nějakého kladného celého čísla t, tedy požadujeme

$$t^2 = 1 + 2a,$$

odsud vyjádříme $a = \frac{1}{2} \cdot (t^2 - 1)$ a dosadíme do (6.3).

$$t^2 + \frac{1}{4}\left(t^2 - 1\right)^2 = \frac{1}{4}\left(t^2 + 1\right)^2$$
$$(2t)^2 + \left(t^2 - 1\right)^2 = \left(t^2 + 1\right)^2$$

Dalším porovnáním dostáváme

$$x = 2t$$
$$y = t^2 - 1$$
$$z = t^2 + 1,$$

kde t je kladné celé číslo, $t \geq 2$, neboť volbou $t = 1$ bychom dostali $y = 0$, my ovšem hledáme pouze kladná řešení. Tyto rovnice můžeme nazývat generátor pythagorejských trojic.

Ukažme si, jak bude vypadat prvních pět trojic, získáme je volbou $t = 2, 3, 4, 5, 6$.

t	x	y	z
2	4	3	5
3	6	8	10
4	8	15	17
5	10	24	26
6	12	35	37

Našli jsme sice nekonečně mnoho trojic vyhovující rovnici (6.1), ale bohužel to nejsou všechna řešení. To dokážeme tak, že se nám podaří najít nějakou trojici, která je řešením dané rovnice, ale nedostaneme ji žádnou volbou paramatru t, tak například

$$5^2 + 12^2 = 13^2.$$

Vidíme, že tuto trojici nám generátor nevygeneroval a už ani nemůže, neboť čísla hledaných trojic tvoří rostoucí posloupnosti a již na řádku volby $t = 3$ jsou hodnoty vysoké. Budeme hledat tedy generátor, který nám najde všechny pythagorejské trojice. Toto odvození přebírám z [3, kapitola 3], ovšem doplním ho o několik pomocných vět, které jsou nezbytné.

Lemma 6.1. *Nechť c je liché, resp. sudé, číslo. Pak c^2 je také liché, resp. sudé, číslo.*

Důkaz.

Bude-li c liché, lze zapsat ve tvaru $c = 2k - 1$, kde k je celé číslo. Potom ovšem

$$c^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 4(k^2 - k) + 1,$$

což je opět liché číslo.

Bude-li c sudé, lze zapsat ve tvaru $c = 2l$, kde l je celé číslo. Potom ovšem

$$c^2 = (2l)^2 = 4l^2,$$

což je opět sudé číslo. □

Lemma 6.2. *Nechť a, b jsou kladná celá čísla taková, že* $\gcd(a, b) = 1$. *Má-li být $a \cdot b = n^2$, kde n je kladné celé číslo, pak musí*

$$a = u^2 \qquad b = v^2,$$

kde u, v jsou kladná celá čísla.

Důkaz.

Proveďme prvočíselný rozklad čísel a, b, n:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \dots < p_k$ jsou prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k$ jsou kladná celá čísla,

$$b = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l},$$

kde $q_1 < q_2 < \dots < q_l$ jsou prvočísla a $\beta_1, \beta_2, \dots, \beta_l$ jsou kladná celá čísla,

$$n = r_1^{\gamma_1} r_2^{\gamma_2} \dots r_m^{\gamma_m},$$

kde $r_1 < r_2 < \dots < r_m$ jsou prvočísla a $\gamma_1, \gamma_2, \dots, \gamma_m$ jsou kladná celá čísla.

Navíc je

$$n^2 = r_1^{2\gamma_1} r_2^{2\gamma_2} \dots r_m^{2\gamma_m}.$$

Protože $gcd(a, b) = 1$ musí být prvočísla p_h různá od prvočísel q_i, pro všechna $h = 1, 2, \dots, k$ a $i = 1, 2, \dots, l$.

$$n^2 = a \cdot b$$

$$r_1^{2\gamma_1} r_2^{2\gamma_2} \dots r_m^{2\gamma_m} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

Přeznačíme si pravou stranu poslední rovnosti

$$r_1^{2\gamma_1} r_2^{2\gamma_2} \dots r_m^{2\gamma_m} = s_1^{\delta_1} s_2^{\delta_2} \dots {s_{k+l}}^{\delta_{k+l}}, \tag{6.4}$$

kde $s_1 < s_2 < \cdots < s_{k+l}$ jsou prvočísla a $\delta_1, \delta_2, \dots, \delta_{k+l}$ jsou kladná celá čísla. Odtud musí $r_j \mid s_1^{\delta_1} s_2^{\delta_2} \dots {s_{k+l}}^{\delta_{k+l}}$ pro všechna $j = 1, 2, \dots, m$, protože r_j je prvočíslo, pak podle lemma 5.1 existuje $s_e^{\delta_e}$, pro nějaké $e = 1, 2, \dots, k+l$ tak, že $r_j \mid s_e^{\delta_e}$. Opětovným využitím, že r_j je prvočíslo, získáváme $r_j \mid s_e$, to je možné ovšem pouze tehdy, pokud $r_j = s_e$. To znamená, že na pravé straně rovnosti (6.4) je alespoň tolik prvočísel, jako na levé, tedy $k + l \geq m$. Zcela podobnou úvahou se dokáže, že $m \geq k + l$, což nám dohromady dává $m = k + l$. Protože v (6.4) máme prvočísla uspořádána podle velikosti platí

$$r_1 = s_1,\ r_2 = s_2, \dots,\ r_m = s_m.$$

Důsledkem těchto rovností je rovnost exponentů prvočísel

$$\delta_j = 2\gamma_j,$$

pro všechna $j = 1, 2, \dots, m$. Protože exponenty δ_j jsou sudá čísla, jsou také α_j, β_j sudá čísla, tudíž a, b jsou druhými mocninami nějakých kladných celých čísel u, v.

□

Lemma 6.3. *Nechť a, b jsou kladná celá čísla. Jestliže $b^2 \mid a^2$, pak $b \mid a$.*

Důkaz.
Z předpokladů je $a^2 = u \cdot b^2$. Pokud se nám podaří dokázat, že $u = v^2$, kde v je kladné celé číslo, pak

$$a^2 = v^2 \cdot b^2$$
$$a^2 = (v \cdot b)^2,$$

odtud pak $a = v \cdot b$, neboť $v \cdot b$ je kladné celé číslo, a tedy $b \mid a$.

Ukážeme, že $u = v^2$, kde v je kladné celé číslo. Proveďme prvočíselný rozklad čísel a, b, u:

$$a = r_1^{\gamma_1} r_2^{\gamma_2} \dots r_m^{\gamma_m},$$

kde $r_1 < r_2 < \cdots < r_m$ jsou prvočísla a $\gamma_1, \gamma_2, \dots, \gamma_m$ jsou kladná celá čísla,

$$b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_k$ jsou kladná celá čísla,

$$u = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l},$$

kde $q_1 < q_2 < \cdots < q_l$ jsou prvočísla a $\beta_1, \beta_2, \ldots, \beta_l$ jsou kladná celá čísla.

Navíc je

$$b^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_k^{2\alpha_k}$$
$$a^2 = r_1^{2\gamma_1} r_2^{2\gamma_2} \ldots r_l^{2\gamma_l}.$$

Počítejme:

$$a^2 = u \cdot b^2$$
$$r_1^{2\gamma_1} r_2^{2\gamma_2} \ldots r_l^{2\gamma_l} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l} p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_k^{2\alpha_k}$$

Přeznačme pravou stranu poslední rovnosti.

$$r_1^{2\gamma_1} r_2^{2\gamma_2} \ldots r_m^{2\gamma_m} = s_1^{\delta_1} s_2^{\delta_2} \ldots {s_{k+l}}^{\delta_{k+l}},$$

kde $s_1 < s_2 < \cdots < s_{k+l}$ jsou prvočísla a $\delta_1, \delta_2, \ldots, \delta_{k+l}$ jsou kladná celá čísla. Nyní by se naprosto analogicky, jako v důkazu předchozího lemma, dokáže, že exponenty δ_j jsou sudá čísla, pro všechna $j = 1, 2, \ldots, m$. Z toho plyne, že u je druhou mocninou nějakého kladného celého čísla v. □

Označme d největšího společného dělitele čísel x, y z rovnice (6.1). Můžeme potom psát $x = x_1 d$, $y = y_1 d$, kde x_1, y_1 jsou nesoudělná kladná celá čísla a dosazením do rovnice máme

$$d^2 x_1^2 + d^2 y_1^2 = z^2$$
$$d^2 \cdot (x_1^2 + y_1^2) = z^2,$$

odtud $d^2 \mid z^2$, tedy podle lemma 6.3 $d \mid z$, potom ale $z = z_1 d$, kde z_1 je kladné celé číslo.

$$d^2 \cdot (x_1^2 + y_1^2) = d^2 \cdot z_1^2$$
$$x_1^2 + y_1^2 = z_1^2$$

Dostali jsme tu samou rovnici, ovšem zkrácenou, tedy každá rovnice (6.1) lze převést na tvar, kde bude největší společný dělitel čísel x, y roven 1. Uvažujme proto od této

chvíle rovnici (6.1), kde je $gcd(x, y) = 1$. Potom ovšem alespoň jedno z čísel x, y musí být liché. Bez újmy na obecnosti můžeme předpokládat, že x je liché číslo.

$$x^2 = z^2 - y^2 = (z + y)(z - y) \tag{6.5}$$

Označme $d_1 = gcd(z + y, z - y)$. Potom

$$z + y = ad_1 \qquad z - y = bd_1, \tag{6.6}$$

kde a, b jsou kladná celá čísla a samozřejmě $gcd(a, b) = 1$. Dosazením do rovnice (6.5)

$$x^2 = abd_1{}^2. \tag{6.7}$$

Dokážeme sporem, že $gcd(ab, d_1{}^2) = 1$. Předpokládejme, že $gcd(ab, d_1{}^2) \neq 1$, pak existuje prvočíslo p tak, že $p \mid ab$, $p \mid d_1{}^2$. Protože $p \mid ab$ a $x^2 = abd_1{}^2$, $p \mid x^2$, jelikož p je prvočíslo, pak podle lemma 5.1 musí $p \mid x$, navíc víme, že x je liché, proto $p \neq 2$. Protože $p \mid d_1{}^2$, musí $p \mid d_1$ a tedy z (6.6) plyne, $p \mid (z + y)$, $p \mid (z - y)$, odtud $p \mid 2y$ a protože již víme, že $p \neq 2$, musí $p \mid y$, to je ovšem spor s nesoudělností čísel x, y.

Protože v (6.7) je $gcd(ab, d_1{}^2) = 1$, musí podle lemmatu 6.2 být $ab = q^2$, kde q je kladné celé číslo. Odtud opětovným použitím lemma 6.2 je

$$a = u^2 \qquad b = v^2,$$

kde u, v jsou kladná celá čísla. Pak

$$x^2 = u^2 v^2 d_1{}^2$$
$$x^2 = (uvd_1)^2$$
$$x = uvd_1$$

Odtud musí být čísla u, v, d_1 také lichá, neboť kdyby alespoň jedno z nich bylo sudé, pak by bylo sudé i číslo x, což je spor s naším předpokladem. Sečtením rovnic (6.6) dostáváme

$$2z = ad_1 + bd_1$$
$$2z = u^2 d_1 + v^2 d_1$$
$$z = \frac{u^2 + v^2}{2} d_1.$$

Analogicky odečtením rovnic (6.6) získáme

$$2y = ad_1 - bd_1$$
$$2y = u^2 d_1 - v^2 d_1$$
$$y = \frac{u^2 - v^2}{2} d_1.$$

Odtud plyne, že $d_1 = 1$, jinak by čísla x a y byla soudělná, což by opět bylo v rozporu s předpokladem jejich nesoudělnosti. Ještě si uvědomme, že rozdíl $u^2 - v^2$ je vždy kladné číslo, neboť z rovností (6.6) plyne $a > b$ a proto také $u > v$. Z nesoudělnosti čísel a, b plyne nesoudělnost čísel u, v. Rovnosti

$$x = uv, \qquad y = \frac{u^2 - v^2}{2}, \qquad z = \frac{u^2 + v^2}{2}, \tag{6.8}$$

nám pro kladná celá, lichá u, v, $u > v$ dávají všechny nesoudělné trojice x, y, z, které vyhovují rovnici (6.1). Všechna ostatní řešení získáme násobením řešení, která obdržíme ze vzorců (6.8), libovolným kladným celým číslem.

Pro představu si vypišme několik pythagorejských trojic získaných generátorem (6.8).

v	u	x	y	z
1	3	3	4	5
1	5	5	12	13
1	7	7	24	25
3	5	15	8	17
3	7	21	20	29

Dejme generátoru pythagorejských trojic (6.8) ještě jiný tvar, který se nám bude později hodit. Položme

$$r = \frac{u + v}{2} \qquad s = \frac{u - v}{2}.$$

Vypočítáme u , v.

$$2r = u + v$$
$$2s = u - v$$

Odtud dostaneme součtem ,resp. rozdílem, rovností

$$u = r + s \qquad v = r - s,$$

z těchto rovností plyne, že r, s musí být nesoudělná, jinak by byla porušena nesoudělnost čísel u, v, navíc, aby rozdíl, resp. součet, čísel r, s byl liché číslo, musí jedno z nich být liché a druhé sudé. Dosazením do (6.8) získáme jiný tvar generátorů pythagorejských trojic

$$x = r^2 - s^2, \qquad y = 2rs, \qquad z = r^2 + s^2, \tag{6.9}$$

kde r, s jsou kladná celá čísla, $r > s$, nesoudělná a jedno z nich musí být liché a jedno sudé. Odtud je také vidět, že y je sudé.

Dodatek

7.1 Důkaz Velké Fermatovy věty pro n=4

Při důkazu se budu nejvíce držet postupu z [3, kapitola 7], trochu odlišný důkaz lze nalézt také v [5, str. 271–272], kde navíc je proveden důkaz také pro $n = 3$.

Věta 7.1. *Rovnice*

$$x^4 + y^4 = z^4 \tag{7.1}$$

nemá řešení pro kladná celá čísla x, y, z.

Víme, že tuto větu dokázal už Pierre Fermat. Větu 7.1 dokážeme tak, že dokážeme následující silnější tvrzení.[1)]

Věta 7.2. *Rovnice*

$$x^4 + y^4 = f^2 \tag{7.2}$$

nemá řešení pro kladná celá čísla x, y, f.

K důkazu budeme potřebovat několik pomocných tvrzení.

Lemma 7.1. *Nechť c je liché číslo. Pak $c^2 \equiv 1 \pmod 4$.*

Důkaz.

Je $c = 2k + 1$, kde k je celé číslo. Pak $c^2 = 4k^2 + 4k + 1$, odtud tvrzení věty. □

Lemma 7.2. *Nechť c je sudé číslo. Pak $c^2 \equiv 0 \pmod 4$.*

Důkaz.

Je $c = 2k$, kde k je celé číslo. Pak $c^2 = 4k^2$, odtud tvrzení věty. □

[1)] Jestliže rovnice (7.1) má řešení $x = a$, $y = b$, $z = c$, kde a, b, c jsou kladná celá čísla, pak rovnice (7.2) má řešení $x = a$, $y = b$, $f = c^2$.

Lemma 7.3. *Nechť n je racionální číslo a n^2 je celé číslo. Pak n je celé číslo.*

Důkaz.

Protože n je racionální číslo, lze vyjádřit ve tvaru $n = \frac{p}{q}$, kde p, q jsou celá čísla, $q > 0$, $gcd(p, q) = 1$. Postupujme sporem, nechť $q > 1$. Číslo

$$n^2 = \left(\frac{p}{q}\right)^2,$$

je dle předpokladů celé, musí tedy $\left(\frac{p}{q}\right)^2 = c$, kde c je celé číslo. Odtud máme $p^2 = cq^2$, tedy $q \mid p \cdot p$. Protože $gcd(p, q) = 1$, musí podle lemmatu 3.1 $q \mid p$, což je spor. Musí tedy nutně být $q = 1$ a tedy n je celé číslo. □

Lemma 7.4. *Nechť kladná celá čísla x, y, f jsou řešením rovnice (7.2). Pak existují další kladná celá čísla, která tuto rovnici řeší a jsou po dvou nesoudělná.*

Důkaz.

Nechť $gcd(x, y) = d$, potom je $x = \alpha d$, $y = \beta d$, kde α, β jsou kladná celá čísla a již nesoudělná. Dosazením do (7.2) máme

$$\begin{aligned}(\alpha d)^4 + (\beta d)^4 &= f^2\\ \alpha^4 d^4 + \beta^4 d^4 &= f^2\\ \alpha^4 + \beta^4 &= \left(\frac{f}{d^2}\right)^2 = \gamma^2 \qquad (7.3)\end{aligned}$$

Protože v poslední rovnosti jsou α, β kladná celá čísla, musí být i na druhé straně této rovnosti kladné celé číslo, tedy kvadrát racionálního čísla $\frac{f}{d^2}$ je celé číslo, podle lemmatu 7.3 musí být číslo $\frac{f}{d^2}$ celé, lze tedy psát $\frac{f}{d^2} = \gamma$, kde γ je kladné celé číslo. Rovnost (7.3) je stejného tvaru jako (7.2), kde ovšem čísla α, β, γ jsou po dvou nesoudělaná, neboť kdyby $gcd(\beta, \gamma) \neq 1$, pak by muselo existovat nějaké prvočíslo p tak, že $\beta = \beta_1 p$, $\gamma = \gamma_1 p$, kde β_1, γ_1 jsou kladná celá čísla a dosazením do (7.3) obdržíme:

$$\begin{aligned}\alpha^4 + {\beta_1}^4 p^4 &= {\gamma_1}^2 p^2\\ \alpha^4 &= p(p{\gamma_1}^2 - {\beta_1}^4 p^3)\end{aligned}$$

Odtud $p \mid \alpha^4$, to ale podle lemmatu 5.1 znamená, že $p \mid \alpha$. To je ovšem spor s nesoudělností čísel α, β. Úplně stejným postupem by se dostal spor kdybychom uvažovali $gcd(\alpha, \gamma) \neq 1$. □

Přejděme už k vlastnímu důkazu věty 7.2.

Důkaz.
Postupujme sporem. Nechť rovnice (7.2) má řešení v oboru kladných celých čísel. Dle lemmatu (7.4) pak existují kladná celá čísla, která řeší rovnici (7.2) a která jsou po dvou nesoudělná. Mezi všemi těmito trojicemi vybereme tu, která má nejmenší třetí složku a označme ji (x_0, y_0, f_0)[2)].

Nechť tedy trojice kladných celých čísel (x_0, y_0, f_0), která jsou po dvou nesoudělaná, splňuje rovnici (7.2), tedy platí

$$x_0{}^4 + y_0{}^4 = f_0{}^2. \tag{7.4}$$

Protože $gcd(x_0, y_0) = 1$, musí být alespoň jedno z těchto čísel liché. Nechť x_0 je liché číslo. Ukážeme, že y_0 nemůže být liché číslo. Kdyby také y_0 bylo liché číslo, pak podle lemmatu 6.1 je $y_0{}^2$ liché, stějně tak pro x_0 dostáváme, že $x_0{}^2$ je liché. Rovnost (7.4) lze také zapsat

$$(x_0{}^2)^2 + (y_0{}^2)^2 = f_0{}^2.$$

Protože $x_0{}^2$, $y_0{}^2$ jsou lichá čísla, je podle lemmatu 7.1

$$(x_0{}^2)^2 \equiv 1 \pmod 4 \qquad (y_0{}^2)^2 \equiv 1 \pmod 4,$$

součtem těchto kongruencí dostáváme

$$(x_0{}^2)^2 + (y_0{}^2)^2 \equiv 2 \pmod 4,$$

pak by ovšem muselo být

$$2 \equiv f_0{}^2 \pmod 4.$$

Ukážeme, že tato kongruence není možná. Kdyby f_0 bylo liché číslo, tak opět podle lemmatu 7.1 je $f_0{}^2 \equiv 1 \pmod 4$ a dostali bychom $2 \equiv 1 \pmod 4$, tj. $4 \mid 1$. Kdyby f_0 bylo sudé číslo, tak podle lemmatu 7.2 je $f_0{}^2 \equiv 0 \pmod 4$ a dostali bychom $2 \equiv 0 \pmod 4$, tj. $4 \mid 2$. Musí tedy nutně být y_0 sudé číslo.

[2)] Taková trojice s minimální třetí složkou musí existovat, protože všechna uvažovaná čísla jsou kladná celá.

Na trojici čísel (x_0, y_0, f_0), která řeší (7.2) se lze podívat jako na trojici čísel $({x_0}^2, {y_0}^2, f_0)$ která řeší (6.1). Toto řešení lze podle (6.9) zapsat pomocí dvou kladných celých čísel a, b, $a > b$, která jsou nesoudělná, jedno z nich je liché, druhé sudé.

$$ {x_0}^2 = a^2 - b^2 \qquad {y_0}^2 = 2ab \qquad f_0 = a^2 + b^2 $$

Z rovnosti

$$ {x_0}^2 = a^2 - b^2 \tag{7.5} $$

získáme, že liché musí být číslo a. Kdyby b bylo liché a a sudé, pak by podle lemmatu 7.1 a lemmatu 7.2 platilo

$$ a^2 \equiv 0 \pmod 4 \qquad b^2 \equiv 1 \pmod 4, $$

rozdílem těchto kongruencí

$$ a^2 - b^2 \equiv 0 - 1 \pmod 4 $$
$$ a^2 - b^2 \equiv -1 \pmod 4, $$

ovšem ${x_0}^2 \equiv 1 \pmod 4$, neboť je liché. Celkem tak z (7.5) máme

$$ 1 \equiv -1 \pmod 4, $$

což je spor. Pro opačný případ, kdy a je liché a b sudé obdržíme $1 \equiv 1 \pmod 4$.

Protože a je liché a $gcd(a, b) = 1$, je také $gcd(a, 2b) = 1$. Důsledkem toho z rovnosti

$$ {y_0}^2 = a(2b) $$

a lemmatu 6.2 plyne, že čísla a, $2b$ jsou druhými mocninami nějakých kladných celých čísel t, s.

$$ a = t^2 \qquad 2b = s^2 $$

Z (7.5) máme

$$ {x_0}^2 + b^2 = a^2, $$

tedy trojice čísel (x_0, b, a), která je nesoudělaná, jinak by byla porušena nesoudělnost čísel x_0, y_0, je řešením rovnice (6.1). Potom existují kladná celá nesoudělná čísla m, n, $m > n$ tak, že platí

$$ x_0 = m^2 - n^2 \qquad b = 2mn \qquad a = m^2 + n^2. $$

Dosazením za b do $2b = s^2$ dostaneme[3)]

$$mn = \left(\frac{s}{2}\right)^2,$$

odkud díky lemma 6.2 máme

$$m = p^2 \qquad n = q^2,$$

kde p, q jsou kladná celá čísla. Dosazením do $a = m^2 + n^2$ s tím, že $a = t^2$ obdržíme

$$p^4 + q^4 = t^2,$$

což je rovnost stejného tvaru jako (7.4). V této rovnosti je trojice čísel (p, q, t) nesoudělná, jinak bychom dostali spor s nesoudělností čísel m, n. Označíme-li nyní $x_1 = p$, $y_1 = q$, $f_1 = t$, našli jsme další řešení rovnice (7.2). Uvědomíme-li si platnost následujících nerovností

$$f_0 > \sqrt[4]{f_0} = \sqrt[4]{a^2 + b^2} > \sqrt[4]{a^2} = \sqrt[4]{t^4} = t = f_1$$

dostáváme spor, neboť jsme našli další řešení, kde $f_0 > f_1$. □

[3)] Protože $2b = s^2$, musí $2 \mid s^2$, pak podle lemmatu 5.1 musí $2 \mid s$, s je sudé číslo.

7.2 Ekvivalence metody řešení rozšířeným Euklidovým algoritmem a řetězovým zlomkem

Na podnět vedoucího práce jsem vyřešil několik diofantických rovnic o dvou neznámých v základním tvaru nejprve pomocí rozšířeného Euklidova algoritmu a následně pomocí řetězového zlomku. Na těchto příkladech se ukázalo, že výstupy těchto postupů, tj. čísla x_0, y_0, jsou stejné. Ukažme si to na jednom konkrétním příkladě.

Příklad 7.1. $127x + 58y + 4 = 0$

Vyřešme jej nejprve pomocí rozšířeného Euklidova algoritmu. Výpočet zaznamenáme tabulkou.

α'	α	β'	β	γ	d	q	r
1	0	0	1	127	58	2	11
0	1	1	−2	58	11	5	3
1	−5	−2	11	11	3	3	2
−5	16	11	−35	3	2	1	1
16	−21	−35	46	2	1	2	0

$$127 \cdot (-21) + 58 \cdot 46 - 1 = 0$$

$$127 \cdot 84 + 58 \cdot (-184) + 4 = 0$$

$$x_0 = 84 \qquad y_0 = -184$$

Nyní nalezněme řešení pomocí řetězového zlomku.

$$\frac{127}{58} = //2, 5, 3, 1, 2//$$

$$n = 5,\ q_1 = 2,\ q_2 = 5,\ q_3 = 3,\ q_4 = 1,\ q_5 = 2$$

$$x_0' = (-1)^6 \cdot 4 \cdot K_3(5, 3, 1) = 84$$

$$y_0' = (-1)^5 \cdot 4 \cdot K_4(2, 5, 3, 1) = -184$$

Vidíme, že

$$x_0 = x_0'$$

$$y_0 = y_0'.$$

Vyvstává otázka, zda to platí zcela obecně.

Nejprve ještě několik poznámek o rozšířeném Euklidově algoritmu. Algoritmus je vždy konečný, což plyne z konečnosti obyčejného Euklidova algoritmu. Nechť skončí po n krocích. Průběh algoritmu lze zapsat tabulkou, kde na i-tém řádku jsou zachyceny hodnoty čísel α', α, β', β, γ, d, q, r, po i-tém provedení kroku E2, $i = 1, 2, \ldots, n$:

$$\begin{array}{cccccccc} \alpha' & \alpha & \beta' & \beta & \gamma & d & q & r \\ \alpha'_1 & \alpha_1 & \beta'_1 & \beta_1 & \gamma_1 & d_1 & q_1 & r_1 \\ \alpha'_2 & \alpha_2 & \beta'_2 & \beta_2 & \gamma_2 & d_2 & q_2 & r_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha'_n & \alpha_n & \beta'_n & \beta_n & \gamma_n & d_n & q_n & r_n \end{array}$$

Podle kroků tohoto algoritmu, které jsou popsány v kapitole 3, můžeme pro celé k, $2 \leq k \leq n$ psát následující rekurentní vzorce[4)]

$$\begin{aligned} \alpha_k &= \alpha'_{k-1} - q_{k-1}\alpha_{k-1} \qquad & \alpha'_k &= \alpha_{k-1} \\ \beta_k &= \beta'_{k-1} - q_{k-1}\beta_{k-1} \qquad & \beta'_k &= \beta_{k-1}, \end{aligned} \tag{7.6}$$

kde $\alpha'_1 = \beta_1 = 1$, $\alpha_1 = \beta'_1 = 0$, dále

$$\gamma_k = d_{k-1} = r_{k-2}, \tag{7.7}$$

$r_0 = b$, $r_{-1} = a$, kde a, b jsou kladné celé koeficienty řešené rovnice v základním tvaru.

Vypišme obecné vzorce pro x_0, y_0, x'_0, y'_0, které jsme odvodili v kapitole 3:

$$\begin{aligned} x_0 &= -c \cdot \alpha_n \\ y_0 &= -c \cdot \beta_n \\ x'_0 &= (-1)^{n+1} \cdot c \cdot K_{n-2}(q_2, q_3, \ldots, q_{n-1}) \\ y'_0 &= (-1)^{n} \cdot c \cdot K_{n-1}(q_1, q_2, q_3, \ldots, q_{n-1}) \end{aligned}$$

Ptáme se, zda je obecně $x_0 = x'_0$ a $y_0 = y'_0$, dosazení dle vzorců výše

$$\begin{aligned} -c \cdot \alpha_n &= (-1)^{n+1} \cdot c \cdot K_{n-2}(q_2, q_3, \ldots, q_{n-1}) \\ -c \cdot \beta_n &= (-1)^{n} \cdot c \cdot K_{n-1}(q_1, q_2, q_3, \ldots, q_{n-1}), \end{aligned}$$

[4)] Pro $n = 1$ by muselo být $b = 1$, tento případ jsme si ovšem vyřešili zvlášť, proto jej nyní neuvažujeme.

což po úpravě dává (uvažujeme $c \neq 0$, pro $c = 0$ jsou rovnosti jasné)

$$\alpha_n = (-1)^n \cdot K_{n-2}(q_2, q_3, \ldots, q_{n-1})$$
$$\beta_n = (-1)^{n-1} \cdot K_{n-1}(q_1, q_2, q_3, \ldots, q_{n-1}).$$

Z (3.16) a (7.7) plyne, že pro $i = 1, 2, \ldots, n$ jsou čísla q_i, ve výše uvedených kontinuantech shodná s čísly q_i vystupují ve vzorcích (7.6).

Věta 7.3. *Nechť n je kladné celé číslo, $n \geq 2$. Potom platí pro všechna celá čísla k, $2 \leq k \leq n$*

$$\begin{aligned} \alpha_k &= (-1)^k \cdot K_{k-2}(q_2, q_3, \ldots, q_{k-1}) \\ \beta_k &= (-1)^{k-1} \cdot K_{k-1}(q_1, q_2, q_3, \ldots, q_{k-1}), \end{aligned} \tag{7.8}$$

kde α_k, β_k jsou koeficienty z rozšířeného Euklidova algoritmu, pro které platí vzorce (7.6) *a $K_{k-2}(q_2, q_3, \ldots, q_{k-1})$, $K_{k-1}(q_1, q_2, q_3, \ldots, q_{k-1})$ jsou kontinuanty, které jsou dány definicí* 3.8 *a q_1, $q_2, \ldots,$ q_{k-1}, q_k jsou kladná celá čísla.*

Důkaz.
Opět jej provedeme indukcí.

(I) Dokážeme, že rovnosti platí pro $k = 2$, ale také pro $k = 3$ (pokud $n \geq 3$).

(II) Budeme předpokládat, že rovnosti platí pro $k - 1$, ale také pro k a ukážeme, že platí pro $k + 1$ (pokud $3 \leq k < n$).

ad(I) Uvažujme nejprve $\alpha_k = (-1)^k \cdot K_{k-2}(q_2, q_3, \ldots, q_{k-1})$. Pro $k = 2$ spočteme zvlášť obě strany rovnosti. Budeme při tom používat rekurentních vzorců (7.6) a rozepisování kontinuantů podle definice 3.8.

$$\alpha_2 = \alpha_1' - q_1\alpha_1 = 1 - q_1 \cdot 0 = 1$$
$$(-1)^2 \cdot K_0 = 1 \cdot 1 = 1$$

Vidíme, že obě strany se rovnají číslu 1. Spočtěme nyní totéž pro $k = 3$.

$$\alpha_3 = \alpha_2' - q_2\alpha_2 = \alpha_1 - q_2\alpha_2 = 0 - q_2 \cdot 1 = -q_2$$
$$(-1)^3 \cdot K_1(q_2) = (-1) \cdot q_2 = -q_2.$$

Nyní ověříme platnost $\beta_k = (-1)^{k-1} \cdot K_{n-1}(q_1, q_2, q_3, \ldots, q_{n-1})$ pro $k = 2$, 3.

$$\beta_2 = \beta_1' - q_1\beta_1 = 0 - q_1 \cdot 1 = -q_1$$
$$(-1)^1 \cdot K_1(q_1) = -q_1$$
$$\beta_3 = \beta_2' - q_2\beta_2 = \beta_1 - q_2 \cdot (-q_1) = 1 + q_1q_2$$
$$(-1)^2 K_2(q_1, q_2) = 1 \cdot q_2 K_1(q_1) + K_0 = q_2q_1 + 1$$

Tím jsou rovnosti dokázány pro $k = 2$ a $k = 3$.

ad(II) Předpokládáme, že rovnosti platí pro $k-1$ a k, kde $3 \leq k < n$, tzn.

$$\alpha_{k-1} = (-1)^{k-1} \cdot K_{k-3}(q_2, q_3, \ldots, q_{k-2})$$
$$\beta_{k-1} = (-1)^{k-2} \cdot K_{k-2}(q_1, q_2, q_3, \ldots, q_{k-2})$$
$$\alpha_k = (-1)^k \cdot K_{k-2}(q_2, q_3, \ldots, q_{k-1})$$
$$\beta_k = (-1)^{k-1} \cdot K_{k-1}(q_1, q_2, q_3, \ldots, q_{k-1}).$$

Nyní dokážeme platnost pro $k+1$, tj. aby platilo

$$\alpha_{k+1} = (-1)^{k+1} \cdot K_{k-1}(q_2, q_3, \ldots, q_k)$$
$$\beta_{k+1} = (-1)^k \cdot K_k(q_1, q_2, q_3, \ldots, q_k).$$

Počítejme opět každou stranu rovnosti zvlášť. Nejprve uvažujme rovnost

$$\alpha_{k+1} = (-1)^{k+1} \cdot K_{k-1}(q_2, q_3, \ldots, q_k).$$

Rozepíšeme-li kontinuant na pravé straně podle definice, dostaneme

$$(-1)^{k+1}[q_k \cdot K_{k-2}(q_2, q_3, \ldots, q_{k-1}) + K_{k-3}(q_2, q_3, \ldots, q_{k-2})],$$

což nám po roznásobení a použití indukčního předpokladu dává

$$-q_k\alpha_k + \alpha_{k-1}.$$

Rozepíšeme-li nyní výraz na levé staně rovnice, tj.

$$\alpha_{k+1} = \alpha_k' - q_k\alpha_k = \alpha_{k-1} - q_k\alpha_k,$$

dostáváme totéž. Nyní postupujme naprosto analogicky pro rovnost

$$\beta_{k+1} = (-1)^k \cdot K_k(q_1, q_2, q_3, \ldots, q_k).$$

Tedy rozepsáním kontinuantu dostáneme

$$(-1)^k[q_k \cdot K_{k-1}(q_1, q_2, \ldots, q_{k-1}) + K_{k-2}(q_1, q_2, \ldots, q_{k-2})]$$

a díky indukčnímu předpokladu obdržíme

$$-q_k\beta_k + \beta_{k-1}$$

a konečně $\beta_{k+1} = \beta'_k - q_k\beta_k = \beta_{k-1} - q_k\beta_k$. Tím je celý důkaz proveden.

□

Výsledky cvičení

Nechť t, s, r, t_1, s_1, t_2, s_2 jsou celá čísla.

Cvičení 2.1.

(a) $x = 1$

(b) $x \in \{-1,\ -3\}$

(c) $x \in \{1,\, 2\}$

(d) Nemá řešení v celých číslech.

Cvičení 3.1.

(a) $x = -25 + 34t$
$y = -20 + 27t$

(b) $x = 20 - 13t$
$y = -5 + 3t$

(c) $x = -195 - 237t$
$y = 2001 + 2432t$

(d) Nemá řešení v celých číslech, neboť $gcd(156,\, 65) = 13$ a $13 \nmid 11$.

Cvičení 3.2.

(a) $x = -4 - 5t$
$y = 16 + 19t$

(b) $x = 72 + 23t$
$y = 564 + 180t$

(c) Nemá řešení v celých číslech, neboť čísla 182, 104 jsou sudá a $2 \nmid 29$.

(d) $x = 48 - 11t$
$y = -16 + 4t$

Cvičení 3.3.

(a) $x = 1 + 12t$
$y = -3 - 41t$

(b) $x = 4t$
$y = 3 - 9t$

(c) $x = 1 + 3t$
$y = 2 + 8t$

(d) $x = 6 + 537t$
$y = 2 + 413t$

Cvičení 4.1.

(a) $x = 2 + t - 4s$
$y = 1 + t + 3s$
$z = 2 + 4t$

(b) $x = 3 + 4t + 4s - 6r$
$y = s$
$z = r$
$u = 4 + 8t$

(c) $x = s$
$y = 1 + 2t$
$z = r$
$u = 6 - 13t - 6s + 2r$

(d) Nemá řešení v celých číslech, neboť $gcd(5,\ 15,\ 25) = 5$ a $5 \nmid 4$.

Cvičení 5.1.

(a) $x_1 = 2t_1$
$y_1 = 1 + 2s_1$
$z_1 = 4 + 12{t_1}^3 + 5s_1$
$x_2 = 1 + 2t_2$
$y_2 = 2s_2$
$z_2 = 3 + 9t_2 + 18{t_2}^2 + 12{t_2}^3 + 5s_2$

(b) Nemá řešení v celých číslech.

(c) $x_1 = 2 + 7t_1$
$y_1 = -2 - 16t_1 - 28{t_1}^2$
$x_2 = 5 + 7t_2$
$y_2 = -14 - 40t_2 - 28{t_2}^2$

(d) $x = t_1$
$y = t_2$
$z = 14 - 4{t_1}^5 - 8{t_2}^8$

Seznam použité literatury

[1] Adamowicz, Zofia, Zbierski, Pawel. *Logic of mathematics: A Modern Course of Classical Logic*. New York: John Wiley, 1997. ISBN 0-471-06026-7

[2] Apfelbeck, Alois. *Kongruence*. Praha: Mladá fronta, 1968. Škola mladých matematiků, 21.

[3] Gelfond, Alexander Osipovich. *Neurčité rovnice*. 1. vydání. Praha: Státní nakladatelství technické literatury, 1954.

[4] Herman, Jiří, Kučera, Radan a Šimša, Jaromír. *Metody řešení matematických úloh I*. 3. vydání. Brno: Masarykova univerzita, 2011. ISBN 978-80-210-5636-7

[5] Ireland, Kenneth a Rosen, Michael. *A Classical Introduction to Modern Number Theory*. 2nd edition. New York: Springer, 1990. ISBN 03-879-7329-X.

[6] Knuth, Donald Ervin. *Umění programování 1. díl: Základní algoritmy*. 1. vydání. Brno: Computer Press, 2008. ISBN 978-80-251-2025-5.

[7] Knuth, Donald Ervin. *Umění programování 2. díl: Seminumerické algoritmy*. 1. vydání. Brno: Computer Press, 2010. ISBN 978-80-251-2898-5.

[8] Kopka, Jan. *Kapitoly o celých číslech*. 1. vydání. Ústí nad Labem: Univerzita J. E. Purkyně, 2004. ISBN 80-7044-562-9.

[9] Kopka, Jan. *Umění řešit matematické problémy*. 1. vydání. Praha: HAV, 2013. ISBN 978-80-903625-5-0.

[10] Mareš, Milan. *Příběhy matematiky*. 1. vydání. Příbram: Pistorius, 2008. ISBN 978-808-7053-164.

[11] Ondráčková, Zdena. *Diofantovské rovnice.* Ústí nad Labem, 1979. Diplomová práce. Pedagogická fakulta v Ústí nad Labem.