UNIVERZITA PALACKÉHO V OLOMOUCI
Přírodovědecká fakulta
Katedra algebry a geometrie

DIPLOMOVÁ PRÁCE

Diofantovské rovnice a jejich soustavy

Vedoucí diplomové práce:
RNDr. Jaroslav Švrček, CSc.
Rok odevzdání: 2017

Vypracoval:
Bc. Tomáš Riemel
F-M, 2. ročník

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně pod vedením pana RNDr. Jaroslava Švrčka, CSc., s použitím uvedené literatury.

V Olomouci 12. května 2017 .....

Poděkování

Rád bych poděkoval vedoucímu diplomové práce panu RNDr. Jaroslavu Švrčkovi, CSc., za spolupráci i za čas, který mi věnoval při konzultacích a v neposlední řadě mé rodině za podporu při celém studiu.

Obsah

Seznam použitých symbolů

$\mathbb{N} = \{1, 2, 3, \dots\}$ ..... množina všech přirozených čísel

$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ ..... množina všech nezáporných celých čísel

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ ..... množina všech celých čísel

$a \in T$ ..... prvek a náleží množině T

$a \,|\, b$ ..... číslo a dělí číslo b

$a \nmid b$ ..... číslo a nedělí číslo b

$D(a, b)$ ..... největší společný dělitel čísel a, b

$\square$ ..... konec řešení příkladu (důkazu)

$\deg P(x)$ ..... stupeň polynomu $P(x)$

$\min\{a, b\}$ ..... minimum z čísel a, b

MO ..... Matematická olympiáda

MD ..... Matematický duel

Úvod

Cílem diplomové práce *Diofantovské rovnice a jejich soustavy* byla sumarizace základních metod řešení diofantovských rovnic a také jejich soustav s ohledem na kompetence žáka střední školy. Téma diofantovské rovnice není obsaženo v rámcových vzdělávacích programech (RVP), představuje tedy nadstandardní část školské matematiky. Často se přitom využívá v mnoha matematických soutěžích pro žáky středních škol. Tato práce může sloužit mj. jako učební pomůcka ve výběrových seminářích na gymnáziích a jiných středních školách či může poskytovat návrh přípravy žáků řešících Matematickou olympiádu (MO) a jiné matematické soutěže. Diplomová práce představuje volné pokračování mé bakalářské práce *Dělitelnost v oboru celých čísel na středních školách*. Jsou zde uvedeny řešené příklady, které jsou modifikací úloh z uvedené literatury, popřípadně jsou původní – autorské.

Diplomová práce je rozčleněna do šesti kapitol. První kapitola obsahuje (kromě jiného) také základní historické informace o řeckém matematikovi Diofantovi z Alexandrie, podle něhož byly pojmenovány diofantovské rovnice.

Druhá kapitola je stěžejní částí práce. Je zde popsáno 11 základních metod pro řešení diofantovských rovnic a jejich soustav. Každá metoda je teoreticky objasněna a prezentována na několika řešených příkladech.

Ve třetí kapitole, která je pojmenována „Soustavy diofantovských rovnic“, jsou shrnuty poznatky z předchozí kapitoly a navíc je zde uveden univerzální postup, jak řešit soustavy diofantovských rovnic na základě znalosti řešení jednotlivých rovnic dané soustavy.

Čtvrtá kapitola představuje výběr řešených příkladů z MO týkajících se diofantovských rovnic. Tyto příklady mohou sloužit jako pomůcka při přípravě nadaných žáků pro uvedené středoškolské matematické soutěže.

V následující, páté kapitole jsou uvedeny některé vybrané neřešené úlohy, které lze řešit užitím metod řešení uvedených v 2. kapitole. U každé z těchto úloh je uveden návod, jak ji řešit, včetně správného výsledku.

V závěrečné kapitole diplomové práce jsou pak prezentovány dva speciální

typy diofantovských rovnic a také tzv. desátý Hilbertův problém, který je úzce spjat s diofantovskými rovnicemi.

Celá práce je vysázená systémem LaTeX.

1 Diofantovské rovnice

V této kapitole diplomové práce uvedeme některé definice a základní pojmy, které jsou pro diplomovou práci nezbytné. Uvedeme zde také historické informace o antickém (řeckém) učenci Diofantovi, podle něhož je pojmenován typ rovnic, o nichž práce pojednává.

Řecký matematik *Diofantos*, který žil v 3. století (našeho letopočtu) v Alexandrii, se zabýval řešením rovnic, v nichž připouštěl řešení pouze v oboru celých čísel (či v některé speciální podmnožině množiny celých čísel). Zajímavostí je, že není přesně znám rok narození, či úmrtí Diofanta, avšak díky textu na jeho náhrobku známe délku jeho života. Diofantův epitaf zní:

„*Jeho mládí trvalo* $\frac{1}{6}$ *jeho života,*
ženat byl $\frac{1}{7}$ *života,*
vousy mu rostly další $\frac{1}{12}$ *života,*
o pět let později se mu narodil syn,
syn žil přesně $\frac{1}{2}$ *délky života svého otce,*
otec skonal po čtyřech letech od smrti syna.“[1]

Diofantovskými rovnicemi se zabývali i jiní významní matematici před i po Diofantovi. Například Pythagoras, Euler či Fermat. Přes veškeré snahy těchto matematiků neexistuje obecný algoritmus, který by řešil univerzálně všechny typy diofantovských rovnic. V současnosti umí matematika řešit spolehlivě diofantovské rovnice nejvýše druhého stupně o dvou neznámých. U dalších typů diofantovských rovnic není vždy zcela jednoduché najít řešení v oboru celých čísel. Přesto se vyplatí zabývat se těmito rovnicemi, neboť využití diofantovských rovnic lze nalézt například v řadě praktických úloh vedoucích k rovnicím, v nichž pouze celočíselná řešení mají konkrétní interpretaci.

[1] Jestliže věk označíme jako x, pak Diofantův epitaf lze přepsat do tvaru rovnice:

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

Úpravami zjistíme, že $x = 84$. Diofantos tedy zemřel v 84 letech.

1.1 Lineární diofantovské rovnice

Definice 1.1.1

Rovnice ve tvaru

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

kde $a_1, \ldots, a_n, b \in \mathbb{Z}$ ($a_i \neq 0$ pro všechna $i = 1, 2, \ldots, n$), se nazývá *lineární diofantovská rovnice* o celočíselných neznámých $x_1, \ldots, x_n$.

Definice 1.1.2

Řešením diofantovské rovnice $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ nazveme každou uspořádanou n-tici $(c_1, c_2, \ldots, c_n) \in \mathbb{Z}^n$, která splňuje identitu

$$a_1c_1 + a_2c_2 + \ldots + a_nc_n = b.$$

Úmluva. Kvůli přehlednosti budeme často značit v některých konkrétních úlohách neznámé ve tvaru $x, y, z, \ldots$ namísto $x_1, x_2, x_3, \ldots$

Definice 1.1.3

Nechť $a, b \in \mathbb{Z}$. Řekneme, že *číslo* b *dělí číslo* a, právě když existuje číslo $t \in \mathbb{Z}$, pro něž platí $a = tb$. Symbolicky značíme $b \mid a$. Pokud neexistuje žádné číslo $t \in \mathbb{Z}$, pro něž platí $a = tb$, říkáme, že *číslo* b *nedělí číslo* a, což symbolicky zapisujeme $b \nmid a$.

Definice 1.1.4

Nechť $n \in \mathbb{N}$, $(n \geq 2)$, a dále $a, b \in \mathbb{Z}$. Řekneme, že číslo a je *kongruentní* s číslem b podle modulu n (modulo n), právě když $n \mid (a - b)$ a píšeme symbolicky

$$a \equiv b \pmod{n}. \tag{1}$$

Vztah (1) se nazývá *číselná kongruence*. Čísla a, b budeme nazývat *levou a pravou stranou číselné kongruence* (1).

Poznámka. Číselné kongruence zavádíme především z důvodu jejich možné aplikace při řešení diofantovských rovnic. Jak uvidíme, již při důkazu následující věty bude potřeba znalosti tohoto pojmu. Vzájemný vztah číselných kongruencí

a diofantovských rovnic je následující: Libovolnou lineární diofantovskou rovnici lze ekvivalentně přepsat do tvaru tzv. *kongruenční rovnice 1. stupně* popsané v mé bakalářské práci [15]. Příkladem může být lineární diofantovská rovnice o dvou neznámých $3x + 8y = 7$, kterou lze přepsat např. do tvaru kongruenční rovnice $3x \equiv 7 \pmod 8$ nebo $8y \equiv 7 \pmod 3$.

Věta 1.1.5

Lineární diofantovská rovnice $a_1x_1 + \ldots + a_nx_n = b$ je řešitelná, právě když $D(a_1, \ldots, a_n) \,|\, b$. Navíc řešení závisí na $n - 1$ nezávislých celočíselných parametrech.

Důkaz.

a) Nechť je diofantovská rovnice $a_1x_1 + \ldots + a_nx_n = b$ řešitelná. Potom existují čísla $c_1, c_2, \ldots, c_n \in \mathbb{Z}$, která dle definice 1.1.2 splňují identitu

$$a_1c_1 + a_2c_2 + \ldots + a_nc_n = b.$$

Z řešitelnosti dané diofantovské rovnice plyne existence $D(a_1, \ldots, a_n) = d$ a tudíž $d \,|\, a_1, \ldots, d \,|\, a_n$. To znamená, že d dělí levou stranu původní diofantovské rovnice a tedy musí platit $d \,|\, b$.

b) V druhé části důkazu se snažíme dokázat, že z předpokladu $D(a_1, \ldots, a_n) \,|\, b$ plyne řešitelnost dané diofantovské rovnice. Tuto část důkazu vedeme pomocí principu matematické indukce vzhledem k n.[2]

(i) Dokážeme platnost implikace pro $n = 2$, lineární diofantovskou rovnici dostaneme ve tvaru

$$a_1x_1 + a_2x_2 = b. \tag{2}$$

Podle definice 1.1.4 a poznámky na předešlé straně můžeme přepsat rovnici (2) ve tvaru kongruenční rovnice 1. stupně

$$a_1x_1 \equiv b \pmod{a_2}. \tag{3}$$

[2]Princip matematické indukce rozebereme v kapitole 2.9.

Z předpokladu implikace víme, že $d = D(a_1, a_2) \,|\, b$. Proto lze rovnici (2) dělit číslem d. Na základě znalostí o řešení tohoto typu rovnic (uvedených např. v [9] nebo [15]) víme, že rovnice (3) má právě jedno řešení ve tvaru

$$x_1 \equiv c_1 \pmod{a_2}, \quad \text{tj.} \quad x_1 = c_1 + a_2 k,\ k \in \mathbb{Z}.$$

Dosazením x_1 do rovnice (2) dostaneme

$$x_2 = \frac{b - a_1 c_1}{a_2} - a_1 k = c_2 - a_1 k.$$

Jelikož x_2 musí být celé číslo, je tudíž i c_2 číslo celé. Řešení rovnice (2) zde závisí na $2 - 1 = 1$ parametru.

(ii) Předpokládejme, že tvrzení platí pro určité $l \geq 2$. Dokážeme, že platí i pro $l + 1$. Mějme rovnici

$$a_1 x_1 + \ldots + a_l x_l + a_{l+1} x_{l+1} = b \tag{4}$$

a nechť $p = D(a_1, \ldots, a_l, a_{l+1}) \,|\, b$. Pokud si označíme $q = D(a_1, \ldots, a_l)$, pak evidentně $q \,|\, b$, $p \,|\, q$ a $q \,|\, (a_1 x_1 + \ldots + a_l x_l)$. Proto platí

$$a_1 x_1 + \ldots + a_l x_l \equiv 0 \pmod{q}, \tag{5}$$

a tedy

$$a_{l+1} x_{l+1} \equiv b \pmod{q}. \tag{6}$$

Zjevně $p = D(a_{l+1}, q) \,|\, b$, z čehož plyne, že rovnice (6) má řešení ve tvaru

$$a_{l+1} x_{l+1} = b + qh, \quad h \in \mathbb{Z}. \tag{7}$$

Dosazením rovnice (7) do rovnice (4) získáme

$$a_1 x_1 + \ldots + a_l x_l = b - b - qh = -qh.$$

Jelikož $q \,|\, qh$ má výše uvedená rovnice řešení a její řešení závisí (dle indukčního předpokladu) na $l - 1$ parametrech. Přidáním parametru h k již existujícím parametrům zjistíme, že rovnice (4) je řešitelná a její řešení závisí na l parametrech.

Spojením kroků (i) a (ii) máme dokázánu platnost tvrzení, že z $D(a_1, \ldots, a_n) \mid b$ plyne řešitelnost diofantovské rovnice $a_1x_1 + \ldots + a_nx_n = b$ pro každé přirozené číslo $n \geq 2$. □

V následujících kapitolách jsou zkoumány diofantovské rovnice nejen lineární, ale i vyšších řádů. S nimi se můžeme setkat především při řešení úloh v matematických soutěžích pro žáky středních škol. Právě z tohoto důvodu proto definujeme v této kapitole uvedený typ diofantovských rovnic.

Definice 1.1.6

Rovnice ve tvaru

$$a_1x^2 + a_2x + a_3xy + a_4y + a_5y^2 = b,$$

kde x, y jsou neznámé, $a_1, \ldots, a_5, b \in \mathbb{Z}$ a zároveň koeficienty $a_1, a_3, a_5 \neq 0$, se nazývá *kvadratická diofantovská rovnice o dvou neznámých.*

Definice 1.1.7

Nechť $P(x_1, x_2, \ldots, x_m)$ je nenulový polynom s celočíselnými koeficienty o m $(m \geq 2)$ neznámých $x_1, x_2, \ldots, x_m$, kde $\deg P(x_1, x_2, \ldots, x_m) = n \geq 1$.
Pak rovnice

$$P(x_1, x_2, \ldots, x_m) = b$$

kde $b \in \mathbb{Z}$, se nazývá *diofantovská rovnice řádu n.*

2 Metody řešení diofantovských rovnic a jejich soustav

V předchozí kapitole bylo již zmíněno, že obecný algoritmus pro řešení obecných typů diofantovských rovnic neexistuje. Přesto k některým typům diofantovských rovnic o jistém počtu neznámých existuje řada metod, jak nalézt řešení dané rovnice. V této kapitole lze nalézt několik základních metod pro řešení diofantovských rovnic a rovněž zde najdeme objasnění jednotlivých principů uvedených metod řešení. Ve 4. kapitole pak aplikujeme zde popsané metody na některých příkladech z MO.

2.1 Metoda řešení pomocí Eukleidova algoritmu

Dříve než popíšeme metodu řešení diofantovských rovnic pomocí Eukleidova algoritmu, uvedeme několik matematických vět, které jsou zásadní pro tuto metodu.

Věta 2.1.1 (O dělení celých čísel se zbytkem)

Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$ jsou libovolně zvolená čísla, pak existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, b-1\}$, která splňují vztah

$$a = qb + r.$$

Číslo r nazýváme zbytek při dělení čísla a číslem b.

Důkaz této věty lze nalézt např. v [6].

Věta 2.1.2 (Eukleidův algoritmus)

Nechť $a_1, a_2 \in \mathbb{Z}$. Pro každé $n \geq 3$, pro něž $a_{n-1} \neq 0$, označíme a_n zbytek při dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků $a_k = 0$ a platí $a_{k-1} = D(a_1, a_2)$.

Důkaz. Podle věty 2.1.1 platí, že $a_2 > a_3 > \ldots$ Jelikož jde o nezáporná čísla, musí být každé následující číslo aspoň o 1 menší než předchozí. Proto po určitém

počtu kroků $a_k = 0$ a $a_{k-1} \neq 0$. Podle toho, jak bylo definováno číslo a_n, plyne existence čísel $b_1, b_2, \ldots, b_{k-2}$, která splňují postupně rovnosti

$$\begin{aligned} a_1 &= b_1 \cdot a_2 + a_3, \\ a_2 &= b_2 \cdot a_3 + a_4, \\ &\vdots \\ a_{k-3} &= b_{k-3} \cdot a_{k-2} + a_{k-1}, \\ a_{k-2} &= b_{k-2} \cdot a_{k-1}. \end{aligned}$$

Z poslední rovnosti plyne, že $a_{k-1} \,|\, a_{k-2}$, z předposlední $a_{k-1} \,|\, a_{k-3}$ až postupně $a_{k-1} \,|\, a_2$ a $a_{k-1} \,|\, a_1$. Společný dělitel čísel a_1, a_2 je tedy a_{k-1}. Libovolný dělitel těchto dvou čísel dělí i a_3 a tedy i a_4 až postupně i a_{k-1}. Proto $a_{k-1} = D(a_1, a_2)$. □

Věta 2.1.3 (Bézoutova)

Nechť a, b jsou libovolná celá čísla, pak existuje jejich největší společný dělitel $D(a, b)$ a zároveň existují čísla $k, l \in \mathbb{Z}$ taková, že $D(a, b) = ka + lb$.

Důkaz. Bézoutovu větu stačí dokázat pro $a_1, a_2 \in \mathbb{N}$. Pokud je možné vyjádřit nějaká čísla $t, s \in \mathbb{Z}$ ve tvaru $t = t_1 a_1 + t_2 a_2$ a $s = s_1 a_1 + s_2 a_2$, kde $t_1, t_2, s_1, s_2 \in \mathbb{Z}$, pak lze vyjádřit i jejich součet a celočíselný násobek ve tvaru

$$\begin{aligned} t + s &= (t_1 + s_1) \cdot a_1 + (t_2 + s_2) \cdot a_2, \\ n \cdot s &= (n \cdot s_1) \cdot a_1 + (n \cdot s_2) \cdot a_2, \end{aligned}$$

kde $n \in \mathbb{Z}$. Jelikož $a_1 = 1 \cdot a_1 + 0 \cdot a_2$, $a_2 = 0 \cdot a_1 + 1 \cdot a_2$, pak vyplývá z důkazu předchozí věty, že $a_3 = a_1 - b_1 a_2, \ldots, a_{k-1} = a_{k-3} - b_{k-3} a_{k-2}$. Z věty 2.1.2 plyne $a_{k-1} = D(a_1, a_2)$. □

Věta 2.1.4

Nechť (x_0, y_0) je řešení diofantovské rovnice $ax + by = c$, pak všechna řešení této diofantovské rovnice lze zapsat ve tvaru

$$x = x_0 - \frac{b}{D(a,b)}p,$$
$$y = y_0 + \frac{a}{D(a,b)}p, \quad \text{kde } p \in \mathbb{Z}.$$

Eukleidův algoritmus lze využít při řešení lineární diofantovských rovnic o dvou neznámých ve tvaru $ax + by = c$. Podle věty 2.1.2 najdeme největší společný násobek $D(a, b)$. Z věty 2.1.3 pak určíme jedno řešení rovnice $au + bv = D(a, b)$, kde u, v jsou neznámé. Pokud $D(a, b) \nmid c$, pak nemá rovnice $ax + by = c$ podle věty 1.1.5 řešení. V opačném případě stačí celou rovnici násobit číslem $e \in \mathbb{Z}$, takovým, že $c = e \cdot D(a, b)$, a dostaneme hledané řešení původní diofantovské rovnice. Obecné řešení lze pak vyjádřit za pomocí jednoho celočíselného parametru. Tato metoda je univerzální, a proto jsme díky této metodě schopni vždy najít řešení lineární diofantovské rovnice.
Celý postup řešení ilustrujeme při řešení dvou níže uvedených příkladů.

Příklad 1

V oboru celých čísel řešte diofantovskou rovnici

$$13x - 25y = 7.$$

Řešení. Pomocí Eukleidova algoritmu (věta 2.1.2) zjistíme $D(13, 25)$:

$$25 = 13 \cdot 1 + 12,$$
$$13 = 12 \cdot 1 + 1,$$
$$12 = 12 \cdot 1.$$

Největší společný dělitel čísel 25 a 13 je tedy číslo 1. Nyní nalezneme řešení rovnice $13x - 25y = 1$ podle Bézoutovy věty 2.1.3:

$$12 = 25 - 13 \cdot 1,$$
$$1 = 13 - 12 \cdot 1 = 13 - (25 - 13) \cdot 1 = (-1) \cdot 25 + 2 \cdot 13.$$

Jedním řešením rovnice $13x - 25y = 1$ je uspořádaná dvojice čísel $(2, 1)$. Jelikož $1 = D(13, 25) \mid 7$, stačí vynásobit identitu $1 = (-1) \cdot 25 + 2 \cdot 13$ číslem 7 a získáme řešení původní rovnice.

Závěr. Obecné řešení dané rovnice je tedy ve tvaru

$$\begin{aligned} x &= 14 + 25k, \\ y &= \ \ 7 + 13k, \ \text{ kde } \ k \in \mathbb{Z}. \end{aligned}$$

□

Příklad 2

V oboru celých čísel řešte diofantovskou rovnici

$$82x + 58y = 16.$$

Řešení. Užitím např. Eukleidova algoritmu (věta 2.1.2) určíme $D(82, 58)$:

$$\begin{aligned} 82 &= 58 \cdot 1 + 24, \\ 58 &= 24 \cdot 2 + 10, \\ 24 &= 10 \cdot 2 + \ \ 4, \\ 10 &= \ \ 4 \cdot 2 + \ \ 2, \\ 4 &= \ \ 2 \cdot 2. \end{aligned}$$

Je tedy $D(82, 58) = 2$. Nyní najdeme řešení rovnice $82x+58y = 2$ podle algoritmu věty 2.1.3. Platí:

$$\begin{aligned} 24 &= 82 - 58 \cdot 1, \\ 10 &= 58 - 24 \cdot 2 = 58 - (82 - 58) \cdot 2 = (-2) \cdot 82 + 3 \cdot 58, \\ 4 &= 24 - 10 \cdot 2 = 82 - 58 - (3 \cdot 58 - 2 \cdot 82) \cdot 2 = 5 \cdot 82 - 7 \cdot 58, \\ 2 &= 10 - 4 \cdot 2 = 3 \cdot 58 - 2 \cdot 82 - (5 \cdot 82 - 7 \cdot 58) \cdot 2 = (-12) \cdot 82 + 17 \cdot 58. \end{aligned}$$

Jedním řešením rovnice $82x+58y = 2$ je uspořádaná dvojice celých čísel $(-12, 17)$. Jelikož $2 = D(82, 58) \mid 16$, stačí vynásobit identitu $2 = 17 \cdot 58 - 12 \cdot 82$ číslem 8 a získáme řešení původní rovnice.

Závěr. Obecné řešení je tedy ve tvaru

$$\begin{aligned} x &= -96 - 29m, \\ y &= \ 136 + 41m, \ \text{ kde } \ m \in \mathbb{Z}. \end{aligned}$$

□

2.2 Eulerova metoda

Eulerova metoda (někdy taktéž zvaná metoda vyjádření nejmenšího koeficientu) je metodou zejména pro lineární diofantické rovnice o dvou neznámých. Jedná se tedy o jednu ze základních metod pro řešení diofantovských rovnic. Mějme rovnici ve tvaru $ax + by = c$, kde x, y jsou neznámé a $a, b, c \in \mathbb{Z}$. Z této rovnice si vyjádříme koeficient, který má v absolutní hodnotě nejmenší hodnotu. Bez újmy na obecnosti předpokládejme, že nejmenší hodnotu v absolutní hodnotě má koeficient a. Danou rovnici si upravíme do tvaru:

$$x = \frac{c - by}{a}$$

Jelikož jsme předpokládali, že a je nejmenší koeficient v absolutní hodnotě, pak podíl $\frac{c - by}{a}$ lze přepsat do tvaru

$$\frac{c - by}{a} = ky + \frac{c - dy}{a}, \text{ kde } k \in \mathbb{Z}, \ |d| < |a|.$$

Řešení diofantovských rovnic hledáme v oboru celých čísel, proto čísla $x, y \in \mathbb{Z}$. A tedy i číslo $\frac{c - dy}{a}$ musí být celé, tj.

$$c - dy = al, \ \ l \in \mathbb{Z}.$$

Po úpravě dostaneme (za předpokladu $d \neq 0$):

$$y = \frac{c - al}{d}$$

Jelikož číslo $y \in \mathbb{Z}$, lze vyjádřit $c - al$ ve tvaru násobku čísla d. A takto analogicky postupujeme dále. Tato metoda se opírá o princip Eukleidova algoritmu. Jelikož koeficienty u neznámých tvoří neúplné podíly a zbytky při postupném dělení v Eukleidově algoritmu, vede tudíž tento proces po konečně mnoho krocích k řešení.

Pro objasnění celého procesu uvedeme několik řešených příkladů.

Příklad 3

V oboru celých čísel řešte diofantovskou rovnici

$$58x - 67y = 23.$$

Řešení. Na počátku řešení každé lineární diofantovské rovnice ověříme, zda je daná diofantovská rovnice řešitelná podle věty 1.1.5. Jelikož $1 = D(58, 67) \mid 23$, je rovnice řešitelná a její řešení bude záviset na jednom celočíselném parametru. Dále si vyjádříme neznámou x, jelikož $58 < |-67|$:

$$x = \frac{23 + 67y}{58} = y + \frac{23 + 9y}{58}.$$

Jelikož $x, y \in \mathbb{Z}$, musí rovněž $\dfrac{23 + 9y}{58} \in \mathbb{Z}$, tj.

$$23 + 9y = 58a, \quad a \in \mathbb{Z}.$$

Úpravou získáme vztah pro y

$$y = \frac{58a - 23}{9} = 6a - 2 + \frac{4a - 5}{9}.$$

Opět tedy musí být $\dfrac{4a - 5}{9} \in \mathbb{Z}$, odtud plyne

$$4a - 5 = 9b, \quad b \in \mathbb{Z}.$$

V dalším kroku si vyjádříme parametr a v závislosti na parametru b

$$a = \frac{9b + 5}{4} = 2b + 1 + \frac{b + 1}{4}.$$

Hodnota $\dfrac{b + 1}{4}$ musí být opět celé číslo, a proto ji můžeme zapsat ve tvaru

$$b + 1 = 4c, \quad c \in \mathbb{Z}.$$

Vyjádřením parametru b v závislosti na parametru c a zpětným dosazením získáme postupně následující vztahy:

$$\begin{aligned}
b &= 4c - 1 \\
a &= 2b + 1 + c = 8c - 2 + 1 + c = 9c - 1 \\
y &= 6a - 2 + b = 6 \cdot (9c - 1) - 2 + 4c - 1 = 58c - 9 \\
x &= y + a = 58c - 9 + 9c - 1 = 67c - 10
\end{aligned}$$

Závěr. Řešením dané diofantovské rovnice jsou všechny dvojice ve tvaru $(67c - 10, 58c - 9)$, kde $c \in \mathbb{Z}$. □

Příklad 4

V oboru celých čísel řešte diofantovskou rovnici

$$21x + 6y = 15.$$

Řešení. Stejně jako v předešlém příkladě ověříme, zda je daná diofantovská rovnice řešitelná podle věty 1.1.5. Jelikož $3 = D(21, 6) \mid 15$, je rovnice řešitelná a její řešení bude záviset na jednom celočíselném parametru.
Dále si vyjádříme neznámou y, jelikož $6 < 21$.

$$y = \frac{15 - 21x}{6} = 2 - 3x + \frac{1 - x}{2}$$

Jelikož $x, y \in \mathbb{Z}$, musí rovněž $\dfrac{1 - x}{2} \in \mathbb{Z}$, tzn.

$$1 - x = 2d, \quad d \in \mathbb{Z}.$$

Úpravou získáme vztah pro x:

$$x = 1 - 2d$$

Zpětným dosazením za x získáme závislost y na parametru d.

$$y = 2 - 3x + d = 2 - 3 \cdot (1 - 2d) + d = -1 + 7d$$

Závěr. Řešením dané diofantovské rovnice jsou všechny uspořádané dvojice $(1 - 2d, -1 + 7d)$, kde $d \in \mathbb{Z}$. □

Příklad 5

Řešte v $\mathbb{Z}$ rovnici

$$24x + 8y = 5.$$

Řešení. V prvním kroku ověříme, zda je daná rovnice řešitelná. Jelikož $8 = D(24, 8) \nmid 5$, nemá daná rovnice řešení v oboru celých čísel. □

2.3 Substituční metoda

Při řešení mnoha matematický úloh, v nichž se vyskytují rovnice či algebraické výrazy, se hojně využívají substituce. Substituční metodu lze použít i při řešení diofantovských rovnic. Mnohdy se tato metoda využívá v kombinaci s jinými metodami řešení a tvoří určitý mezikrok v celkovém řešení, viz následující dva příklady.

Příklad 6

Dokažte, že existuje nekonečně mnoho celých čísel x, y, z, která splňují rovnici

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2.$$

Řešení. Položíme–li $z = -y$, přejde daná rovnice do tvaru $x^3 = x^2 + 2y^2$. Opětovnou substitucí $y = kx$, kde $k \in \mathbb{Z}$, dostaneme jako jednu z možností $x = 1 + 2k^2$.

Závěr. Našli jsme tak jeden typ uspořádané trojice čísel vyhovující zadání úlohy, a to:

$$\begin{aligned} x &= \quad 1 + 2k^2, \\ y &= \quad k(1 + 2k^2), \\ z &= -k(1 + 2k^2). \end{aligned}$$

Řešení je tudíž nekonečně mnoho. □

Příklad 7

Najděte všechny trojice (x, y, z) přirozených čísel, které splňují rovnici

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$$

Řešení. Jelikož x, y, z jsou přirozená čísla, lze celou rovnici přepsat do tvaru

$$z = \frac{xy}{x + y}.$$

Označme $p = D(x, y)$. Pak $x = pk$ a $y = pl$, kde $k, l \in \mathbb{N}$ a zároveň $D(k, l) = 1$. Jelikož $D(k, l) = 1$, pak $D(kl, k + l) = 1$. To dokážeme sporem.
Nechť platí $D(k, l) = 1$ a zároveň $D(kl, k + l) = d \geq 2$. Přirozená čísla $kl, k + l$ lze zapsat ve tvaru

$$\begin{aligned} kl &= da, \\ k + l &= db, \end{aligned}$$

kde $a, b \in \mathbb{N}$. Odtud plyne $l = db - k$. Dosazením za l do vztahu pro kl dostaneme

$$k^2 = d(kb - a).$$

Z výše uvedené rovnosti plyne $d \mid k^2$, a tedy $d \mid k$, tj. $k = dc$, kde $c \in \mathbb{N}$. Dosazením za k do $l = db - k$ dostaneme

$$l = d(b - c),$$

z čehož plyne $d \mid l$, což je ale spor s $D(k, l) = 1$, tudíž platí dokazované tvrzení. Je tedy $D(kl, k + l) = 1$. Neznámou z lze zapsat ve tvaru

$$z = \frac{pkl}{k + l}.$$

Z této rovnice plyne, že $(k + l) \mid p$, čili $p = t(k + l)$, kde $t \in \mathbb{N}$.

Závěr. Řešením dané rovnice je každá uspořadaná trojice přirozených čísel, kterou lze zapsat ve tvaru $(tk(k + l), tl(k + l), tkl)$, kde k, l, t jsou libovolná přirozená čísla. □

2.4 Metoda číselných kongruencí

Metoda řešení diofantovských rovnic užitím číselných kongruencí je poněkud sofistikovanější metodou než předchozí dvě metody, jelikož ji lze obecně použít na všechny typy diofantovských rovnic a nejen na lineární diofantovské rovnice. Pojem číselná kongruence je definován v kapitole 1. Číselné kongruence mají řadu pozoruhodných vlastností. Mají rovněž velké uplatnění v teorii čísel. V této části práce se omezíme pouze na používání číselných kongruencí při řešení diofantovských rovnic, viz např. v [9] či [15].

Příklad 8

V množině $\mathbb{Z}$ řešte rovnici

$$3x + 12y - 7z + 11u - 5v = 9.$$

Řešení. Jelikož se jedná o lineární diofantovskou rovnici, ověříme nejprve řešitelnost dané rovnice. Protože $1 = D(3, 12, 7, 11, 5) \mid 9$, je daná diofantovská rovnice řešitelná.

Podle poznámky v kapitole 1 lze přepsat diofantovskou rovnici do tvaru kongruenční rovnice, neboť $D(3, 12) = 3$

$$-7z + 11u - 5v \equiv 9 \pmod 3.$$

Nyní řešíme kongruenční rovnici a upravíme ji následujícím způsobem, neboť jsou splněny kongruence $11 \equiv 2$, $-7 \equiv -1$, $-5 \equiv 1$, $9 \equiv 0$ (všechny modulo 3), tj.

$$-z + 2u + v \equiv 0 \pmod 3.$$

Tedy $v = z - 2u + 3k$, kde $k \in \mathbb{Z}$. Dosazením za v do původní rovnice dostaneme rovnici

$$x + 4y - 4z + 7u = 3 + 5k.$$

Tuto rovnici přepíšeme do tvaru následující kongruenční rovnice (jsou splněny kongruence $4 \equiv 0$, $7 \equiv 3$, $5 \equiv 1$, všechny modulo 4)

$$x + 3u \equiv 3 + k \pmod 4.$$

Z posledního vztahu plyne, že $x = 3 + k - 3u + 4l$, kde $l \in \mathbb{Z}$. Dosazením za x do původní rovnice dostaneme

$$y - z + u = k - l.$$

Pokud označíme $z = m$, $u = n$, kde $m, n \in \mathbb{Z}$, dostaneme řešení původní diofantovské rovnice.

Závěr. Řešením dané diofantovské rovnice jsou všechny uspořádané pětice ve tvaru $(3 + k + 4l - 3n, k - l + m - n, m, n, 3k + m - 2n)$, kde $k, l, m, n \in \mathbb{Z}$. □

Příklad 9

Dokažte, že diofantovská rovnice

$$(x+1)^2 + (x+2)^2 + \ldots + (x+201)^2 = y^2$$

nemá řešení v oboru celých čísel.

Řešení. Označme $x = k - 101$. Potom původní rovnici lze přepsat do tvaru

$$(k-100)^2 + \ldots + (k-1)^2 + k^2 + (k+1)^2 + \ldots + (k+100)^2 = y^2.$$

Úpravou dostaneme rovnici

$$201k^2 + 2(1^2 + 2^2 + \ldots + 100^2) = y^2.$$

Jelikož pro každé $n \in \mathbb{N}$ platí $1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1)$,[3] dostáváme rovnici ve tvaru

$$201k^2 + \frac{1}{3} \cdot 100 \cdot 101 \cdot 201 = y^2.$$

Díky platnosti kongruencí $201 \equiv 0 \pmod 3$, $100 \cdot 101 \cdot 67 \equiv 2 \pmod 3$ lze uvedenou rovnici přepsat ve tvaru kongruenční rovnice

$$y^2 \equiv 2 \pmod 3.$$

Poslední vztah představuje kongruenční rovnici 2. stupně. Pokud by byla daná kongruenční rovnice řešitelná, pak by $y^2 \equiv 1 \pmod 3$ (viz např. [9], str. 55), což však neplatí.

Závěr. Daná diofantovská rovnice nemá řešení v oboru celých čísel. □

2.5 Metoda řetězových zlomků

Metoda řešení diofantovských rovnic užitím řetězových zlomků je kombinovanou metodou řešení pomocí Eukleidova algoritmu (kapitola 2.1) a metody číselných kongruencí (kapitola 2.4). Tato metoda je velmi užitečná při hledání řešení lineárních diofantovských rovnic či při hledání (alespoň) přibližného řešení. Dříve než popíšeme tuto metodu řešení, zavedeme několik potřebných pojmů.

Definice 2.5.1

Nechť a/b je libovolné racionální číslo (zlomek), kde $a \in \mathbb{Z}$, $b \in \mathbb{N}$, které lze pomocí známého Eukleidova algoritmu vyjádřit následovně:

$$\begin{aligned}
\frac{a}{b} &= c_1 + \frac{q_2}{b}, \quad 0 < q_2 < b, \\
\frac{b}{q_2} &= c_2 + \frac{q_3}{q_2}, \quad 0 < q_3 < q_2, \\
&\vdots \\
\frac{q_{n-2}}{q_{n-1}} &= c_{n-1} + \frac{q_n}{q_{n-1}}, \quad 0 < q_n < q_{n-1}, \\
\frac{q_{n-1}}{q_n} &= c_n.
\end{aligned}$$

[3] Důkaz tohoto tvrzení lze provést pomocí principu matematické indukce.

Pak výraz

$$\frac{a}{b} = c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \ldots + \cfrac{1}{c_{n-1} + \cfrac{1}{c_n}}}}$$

nazveme *řetězový zlomek* příslušný zlomku a/b, kde $c_1 \in \mathbb{Z}$, $c_2, \ldots, c_n \in \mathbb{N}$. Tento řetězový zlomek pak zapisujeme ve tvaru

$$\frac{a}{b} = (c_1, \ldots, c_n).$$

Poznámka. Skutečnost, že výraz napravo obsahuje konečný počet členů, je zaručena konečným počtem kroků v Eukleidově algoritmu.

Definice 2.5.2

Nechť $(c_1, \ldots, c_n)$ je řetězový zlomek příslušící zlomku a/b. Pak výrazy

$$\delta_1 = (c_1), \delta_2 = (c_1, c_2), \delta_3 = (c_1, c_2, c_3), \ldots, \delta_n = (c_1, \ldots, c_n),$$

nazýváme *parciální zlomky* příslušící řetězovému zlomku $(c_1, \ldots, c_n)$, přičemž δ_k, kde $1 \leq k \leq n$, nazýváme *parciální zlomek řádu k*.

Poznámka. Pro výpočet parciálních zlomků lze využít rekurentní vztah

$$\delta_k = \frac{P_k}{Q_k} = \frac{c_k P_{k-1} + P_{k-2}}{c_k Q_{k-1} + Q_{k-2}},$$

kde $P_0 = 1, P_1 = c_1, Q_0 = 0, Q_1 = 1$.[4]

Nyní již máme vše potřebné k vysvětlení metody řešení diofantovských rovnic pomocí řetězových zlomků. Mějme lineární diofantovskou rovnici ve tvaru $ax + by = d$, kde $D(a, b) = 1$, kterou lze ekvivalentně přepsat do tvaru kongruenční rovnice $ax \equiv d \pmod{b}$. V dalším kroku rozložíme číslo b/a v řetězový zlomek $(c_1, \ldots, c_n)$, kde $\delta_k = \frac{P_k}{Q_k}$ jsou jeho parciální zlomky. Jelikož $D(a, b) = 1$, pak $P_n = b$ a $Q_n = a$. Řešení uvedené kongruenční rovnice lze nalézt ve tvaru (viz např. [9], str. 45)

$$x \equiv (-1)^{n-1} P_{n-1} d \pmod{b}.$$

[4] Ověření tohoto rekurentního vztahu lze provést pomocí principu matematické indukce viz kapitola 2.9.

Příklad 10

V oboru celých čísel řešte rovnici $57x + 82y = 13$.

Řešení. Uvedenou diofantovskou rovnici nejprve převedeme do tvaru kongruenční rovnice $57x \equiv 13 \pmod{82}$, kde $D(57, 82) = 1$. Dále rozložíme číslo $82/57$ v řetězový zlomek:

$$\begin{aligned}
\frac{82}{57} &= 1 + \frac{25}{57} \\
\frac{57}{25} &= 2 + \frac{7}{25} \\
\frac{25}{7} &= 3 + \frac{4}{7} \\
\frac{7}{4} &= 1 + \frac{3}{4} \\
\frac{4}{3} &= 1 + \frac{1}{3}
\end{aligned}$$

Tedy $82/57 = (1, 2, 3, 1, 1, 3)$, přičemž $n = 6$ a dle rekurentního vztahu vypočteme P_5.

c_k		1	2	3	1	1	3
P_k	1	1	3	10	13	$\underline{23}$	82

Je tedy $P_5 = 23$, a tudíž řešení kongruenční rovnice je ve tvaru

$$x \equiv (-1)^5 \cdot 23 \cdot 13 \equiv 29 \pmod{82},$$

což znamená, že $x = 29 + 82k$, kde $k \in \mathbb{Z}$. Dosazením za x do původní rovnice dostaneme $y = -20 - 57k$.

Závěr. Řešením dané rovnice jsou všechny dvojice $(29 + 82k, -20 - 57k)$, kde $k \in \mathbb{Z}$. □

Příklad 11

V oboru celých čísel řešte diofantovskou rovnici

$$268x + 141y = 58.$$

Řešení. Uvedenou diofantovskou rovnici nejprve převedeme do tvaru kongruenční rovnice $141y \equiv 58 \pmod{268}$, kde $D(141, 268) = 1$. Dále rozložíme číslo $268/141$ v řetězový zlomek:

$$\frac{268}{141} = 1 + \frac{127}{141}$$
$$\frac{141}{127} = 1 + \frac{14}{127}$$
$$\frac{127}{14} = 9 + \frac{1}{14}$$

Platí tedy $268/141 = (1, 1, 9, 14)$, přičemž $n = 4$ a dle rekurentního vztahu vypočteme P_3.

c_k		1	1	9	14
P_k	1	1	2	$\underline{19}$	268

Dostáváme tedy $P_3 = 19$, a tudíž řešení kongruenční rovnice lze zapsat ve tvaru

$$y \equiv (-1)^3 \cdot 19 \cdot 58 \equiv 238 \pmod{268},$$

což znamená, že $y = 238 + 268u$, kde $u \in \mathbb{Z}$. Dosazením za y do původní rovnice dostaneme $x = -125 - 141u$.

Závěr. Řešením dané diofantovské rovnice jsou všechny dvojice ve tvaru $(-125 - 141u, 238 + 268u)$, kde $u \in \mathbb{Z}$. □

2.6 Metoda nerovností a odhadů

Při řešení některých typů diofantovských rovnic či nerovnic si lze povšimnout určitých symetrií, které lze využít pro určitý odhad nějaké neznámé uvedené v diofantovské rovnici. Metoda nerovností a odhadů je velmi efektivní při řešení diofantovských rovnic vyšších řádů. Pro vysvětlení užití nerovností a odhadů uvádíme několik níže uvedených příkladů. Další příklady na metodu řešení diofantovských rovnic pomocí nerovností a odhadů lze najít např. v mé předešlé práci viz [15].

Příklad 12 (T. Riemel)

V oboru celých čísel řešte rovnici

$$5x^2 + 2xy + 5y^2 = 8x^2y^2.$$

Řešení. Ze zadání diofantovské rovnice lze vidět, že neznámé x, y jsou rozloženy v dané rovnici symetricky. Tudíž bez újmy na obecnosti můžeme předpokládat, že $x \leq y$. V opačném případě pouze přehodíme neznámé a celý následující postup zůstane zachován. Z uvedené nerovnosti plyne, že $x^2 \leq y^2$ a $xy \leq y^2$. Celou rovnici lze odhadnout

$$8x^2y^2 = 5x^2 + 2xy + 5y^2 \leq 12y^2.$$

Tudíž pro splnění uvedené nerovnosti musí buď $y = 0$, nebo $x^2 \leq \frac{3}{2}$. Po dosazení $y = 0$ do původní rovnice plyne, že $x = 0$. Pokud $x^2 \leq \frac{3}{2}$, může x nabývat celočíselných hodnot v rozmezí $-1 \leq x \leq 1$. Dosazením za x do původní rovnice zjistíme, že

$$\begin{aligned} y &= 0 \quad \text{pro} \quad x = 0, \\ y &\notin \mathbb{Z} \quad \text{pro} \quad x = \pm 1. \end{aligned}$$

Závěr. Daná rovnice má právě jedno řešení, kterým je dvojice $(x, y) = (0, 0)$. □

Příklad 13

Najděte všechny uspořádané čtveřice přirozených čísel x, y, z a v, pro které platí

$$x^2 + y^2 + z^2 + 2xy + 2x(z-1) + 2y(z+1) = v^2.$$

Řešení. Předně si uvědomme, že platí

$$(x + y + z \pm 1)^2 = x^2 + y^2 + z^2 + 2xy + 2x(z \pm 1) + 2y(z \pm 1) + 2z + 1.$$

Z toho plyne, že musí platit následující nerovnost

$$(x + y + z - 1)^2 < v^2 < (x + y + z + 1)^2.$$

Tedy $x^2+y^2+z^2+2xy+2x(z-1)+2y(z+1)$ může být rovno pouze $(x+y+z)^2$. To ovšem implikuje $x = y$. Pokud si vyjádříme $x = k$, $z = l$, kde $k, l \in \mathbb{N}$, pak dosazením do původní rovnice získáme $v = 2k + l$.

Závěr. Řešením původní rovnice jsou uspořádané čtveřice $(k, k, l, 2k + l)$, kde $k, l \in \mathbb{N}$. □

Příklad 14 (T. Riemel)

V oboru celých čísel řešte rovnici

$$8x^2 + 6y^2 = 31.$$

Řešení. Předně si uvědomme, že pro libovolné $x \in \mathbb{Z}$ platí $x^2 \geq 0$, proto musí platit nerovnost

$$31 = 8x^2 + 6y^2 \geq 6y^2.$$

Z nerovnosti ovšem plyne, že $y^2 \leq \frac{31}{6}$. Jelikož $y \in \mathbb{Z}$, může y^2 nabývat pouze hodnot $0, 1, 4$. Dosazením přípustných hodnot za y^2 do původní rovnice dostáváme

$$\begin{aligned} 8x^2 &= 31 \quad \text{pro} \quad y^2 = 0, \\ 8x^2 &= 25 \quad \text{pro} \quad y^2 = 1, \\ 8x^2 &= \ 7 \quad \text{pro} \quad y^2 = 4. \end{aligned}$$

Závěr. Jelikož ani v jednom případě nedostaneme celočíselnou hodnotu pro x, nemá daná úloha řešení v oboru celých čísel. □

2.7 Metoda faktorizace

Metoda faktorizace je velmi užívanou metodou v mnoha oblastech matematiky. Už žáci na základní škole (mnohdy nevědomky) tuto metodu využívají například při řešení kvadratických rovnic, když přepíší kvadratickou rovnici do součinového (faktorizovaného) tvaru. Rozklad na součin nebo–li faktorizace je jednou ze základních metod řešení diofantovských rovnic.

Nechť $f(x_1, x_2, \ldots, x_n)$ je polynom o n neznámých a $f(x_1, x_2, \ldots, x_n) = 0$ je rovnice, kterou lze ekvivalentně přepsat ve tvaru

$$f_1(x_1, x_2, \ldots, x_n) \cdot f_2(x_1, x_2, \ldots, x_n) \cdot \ldots \cdot f_k(x_1, x_2, \ldots, x_n) = c,$$

kde $f_1, f_2, \ldots, f_k$ jsou celočíselné polynomy a $c \in \mathbb{Z}$. Pokud rozložíme číslo c na čísla $c_1, c_2, \ldots, c_k$, pak dostáváme soustavy rovnic ve tvaru

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= c_1, \\ f_2(x_1, x_2, \ldots, x_n) &= c_2, \\ &\vdots \\ f_k(x_1, x_2, \ldots, x_n) &= c_k. \end{aligned}$$

Vyřešením všech soustav dostaneme všechna řešení původní rovnice. Pro lepší pochopení dané metody faktorizace uvádíme několik příkladů.

Příklad 15

V oboru celých čísel řešte rovnici

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{9}.$$

Řešení. Nejprve si uvědomme podmínku řešitelnosti, tj. $x, y \neq 0$. Úpravami lze danou rovnici přepsat do tvaru

$$(x - 9) \cdot (y - 9) = 81.$$

Tato rovnice je již v součinovém tvaru. Číslo 81 lze rozložit na prvočísla 1 a 9, proto dostáváme následující možnosti rozkladu

$$81 = 1 \cdot 81 = (-1) \cdot (-81) = 9 \cdot 9 = (-9) \cdot (-9),$$

ze kterých dostáváme soustavy rovnic

$$\begin{aligned} x - 9 &= 1, & x - 9 &= -1, \\ y - 9 &= 81, & y - 9 &= -81, \end{aligned}$$

$$\begin{aligned} x - 9 &= 9, & x - 9 &= -9, \\ y - 9 &= 9, & y - 9 &= -9, \end{aligned}$$

$$\begin{aligned} x - 9 &= 81, & x - 9 &= -81, \\ y - 9 &= 1, & y - 9 &= -1. \end{aligned}$$

Řešením uvedených soustav rovnic jsou uspořádané dvojice $(x, y) \in \{(10, 90), (8, -72), (18, 18), (0, 0), (90, 10), (-72, 8)\}$.

Závěr. Zkouškou zjistíme, že řešením dané diofantovské rovnice jsou uspořádané dvojice $(x, y) \in \{(10, 90), (8, -72), (18, 18), (90, 10), (-72, 8)\}$. □

Příklad 16 (T. Riemel)

Najděte všechna celočíselná řešení rovnice

$$x^2y^2 + 9x^2 + 4y^2 - 6x^2y + 4xy^2 - 24xy + 36x - 24y + 27 = 0.$$

Řešení. Danou rovnici přepíšeme do tvaru

$$(xy - 6)^2 + (3x - 2y)^2 - 2(xy - 6)(3x - 2y) = 9.$$

Tento tvar rovnice můžeme dále upravit na rovnici

$$(xy - 6 - (3x - 2y))^2 = 9.$$

Odmocněním a následnou úpravou dostaneme rovnici v součinovém tvaru

$$(x + 2)(y - 3) = \pm 3.$$

Z této rovnice vytvoříme následující soustavy rovnic, neboť $3 = 1 \cdot 3 = (-1) \cdot (-3)$.

$$\begin{aligned} x + 2 &= 1, & x + 2 &= -1, \\ y - 3 &= 3, & y - 3 &= -3, \end{aligned}$$

$$\begin{aligned} x + 2 &= -1, & x + 2 &= 1, \\ y - 3 &= 3, & y - 3 &= -3. \end{aligned}$$

Závěr. Řešením uvedených soustav jsou uspořádané dvojice $(x, y) \in \{(-1, 6), (-3, 0), (-3, 6), (-1, 0)\}$. Zkouškou ověříme, že nalezená řešení soustav lineárních rovnic jsou i řešením dané rovnice. □

2.8 Metoda nekonečného klesání

Metoda nekonečného klesání (Fermat's Method of Infinite Descent, viz [1]) byla formulována Fermatem[5] v 17. století. Metoda nekonečného klesání je založena na neexistenci nekonečné klesající posloupnosti v množině celých nezáporných čísel (či v její podmnožině). Tato metoda se využívá v existenčních důkazových úlohách, kde se má rozhodnout, zda existuje či neexistuje řešení pro danou

[5] Pierre de Fermat (17. srpen 1601 - 12. leden 1665) - francouzský matematik

úlohu. V literatuře (např. [1] nebo [5]) lze najít dvě varianty této metody, které lze obě využít při řešení diofantovských rovnic.

Varianta 1. Nechť $V(n)$ je výroková forma, která je definovaná na množině nezáporných celých čísel. Předpokládejme, že existuje celé nezáporné číslo n_1 takové, že $V(n_1)$ platí. Pokud ovšem existuje další nezáporné celé číslo n_2 ($n_2 < n_1$), pro které tvrzení $V(n_2)$ platí, a pokud takto můžeme pokračovat libovolněkrát, pak existuje posloupnost celých nezáporných čísel

$$n_1 > n_2 > \ldots > n_k > \ldots$$

taková, že $V(n_k)$ platí pro všechna n_k, kde $k \in \mathbb{N}$. Jelikož je množina celých nezáporných čísel zdola omezená, proto posloupnost daných vlastností nemůže existovat. Pomocí důkazu sporem jsme tedy dokázali, že daný předpoklad je chybný, a tudíž neexistuje žádné celé nezáporné číslo n_1, pro které by tvrzení $V(n_1)$ bylo pravdivé.

Varianta 2. Nechť $V(n)$ je výroková forma definovaná na množině nezáporných celých čísel. Předpokládejme, že existuje alespoň jedno číslo $n_1 \in R$, kde R je neprázdná podmnožina nezáporných celých čísel, pro něž tvrzení $V(n_1)$ neplatí. Pokud si označíme Q podmnožinu množiny R, ve které se vyskytují prvky $q \in R$, pro něž tvrzení $V(q)$ neplatí, pak musí vzhledem k neprázdnosti množiny Q existovat její nejmenší prvek. Budeme jej značit $q_{\min}$. Jestliže najdeme číslo $p \in R$ ($p < q_{\min}$), pro něž tvrzení $V(p)$ neplatí, dostame spor s minimalitou prvku $q_{\min}$. Pomocí důkazu sporem musí tedy tvrzení $V(n)$ platit pro všechna $n \in R$.

K ilustraci této metody uvádíme následující příklady, ve kterých použijeme obě varianty řešení.

Příklad 17

V oboru nezáporných celých čísel řešte rovnici

$$x^5 + 4y^5 = 8z^5.$$

Řešení. Povšimněme si, že řešením rovnice je určitě uspořádaná trojice $(0, 0, 0)$. Předpokládejme, že existuje i jiné nenulové řešení (x, y, z). Pokud by byla jedna

z neznámých x, y, z nulová, pak i další neznámé by musely být nulové a dostaneme opět uspořádanou trojici $(0, 0, 0)$. Dále předpokládejme, že x, y, z jsou přirozená čísla. Z původní rovnice plyne, že $4 \mid x^5$, a tedy $2 \mid x$, tj. $x = 2x_1$, kde $x_1 \in \mathbb{N}$. Úpravou získáme rovnici ve tvaru

$$8x_1^5 + y^5 = 2z^5.$$

Z této rovnice plyne, že $2 \mid y^5$, a tedy $2 \mid y$, tj. $y = 2y_1$, kde $y_1 \in \mathbb{N}$. Opětovným dosazením za $y = 2y_1$ získáme rovnici ve tvaru

$$4x_1^5 + 16y_1^5 = z^5.$$

Z výše uvedené rovnice plyne, že $4 \mid z^5$, a tedy $2 \mid z$, tj. $z = 2z_1$, kde $z_1 \in \mathbb{N}$. Konečně tak dostaneme rovnici

$$x_1^5 + 4y_1^5 = 8z_1^5,$$

kde $x_1 < x$, $y_1 < y$, $z_1 < z$. Jelikož tento postup můžeme opakovat libovolněkrát, dostáváme tak nekonečnou klesající posloupnost uspořádáných trojic

$$(x, y, z) > (x_1, y_1, z_1) > \ldots > (x_k, y_k, z_k) > \ldots$$

Podle varianty 1 ovšem taková posloupnost neexistuje.

Závěr. Jediným řešením původní rovnice je tudíž uspořádaná trojice $(0, 0, 0)$. □

Příklad 18

Dokažte, že neexistují přirozená čísla x, y, z splňující rovnici

$$x^7 + 8y^7 + 16z^7 = 16xyz.$$

Řešení. Předpokládejme sporem, že existují přirozená čísla x, y, z splňující danou rovnici. Tedy uspořádaná trojice $(x, y, z) \in Q$ (podle varianty 2). Jestliže je množina Q neprázdná, musí obsahovat nejmenší prvek, značíme jej $(x_{\min}, y_{\min}, z_{\min})$. Původní rovnici dostaneme ve tvaru

$$x_{\min}^7 + 8y_{\min}^7 + 16z_{\min}^7 = 16x_{\min}y_{\min}z_{\min}.$$

Z této rovnice plyne, že $8 \mid x_{\min}^7$, a tedy $2 \mid x_{\min}$, tj. $x_{\min} = 2x_1$, kde $x_1 \in \mathbb{N}$. Úpravou dostaneme rovnici ve tvaru

$$16x_1^7 + y_{\min}^7 + 2z_{\min}^7 = 4x_1 y_{\min} z_{\min}.$$

Z uvedené rovnice plyne, že $2 \mid y_{\min}^7$, a rovněž $2 \mid y_{\min}$, tj. $y_{\min} = 2y_1$, kde $y_1 \in \mathbb{N}$. Opět úpravou dostaneme rovnici

$$8x_1^7 + 64y_1^7 + z_{\min}^7 = 4x_1 y_1 z_{\min}.$$

Z poslední rovnice plyne, že $4 \mid z_{\min}^7$, a rovněž $2 \mid z_{\min}$, tj. $z_{\min} = 2z_1$, kde $z_1 \in \mathbb{N}$. V konečném kroku dostáváme rovnici ve tvaru

$$x_1^7 + 8y_1^7 + 16z_1^7 = 16x_1 y_1 z_1.$$

Jelikož $x_{\min} > x_1$, $y_{\min} > y_1$, $z_{\min} > z_1$, pak $(x_1, y_1, z_1) < (x_{\min}, y_{\min}, z_{\min})$. To je ovšem spor s minimalitou $(x_{\min}, y_{\min}, z_{\min})$.

Závěr. Podle varianty 2 neexistuje žádná uspořádaná trojice přirozených čísel (x, y, z) vyhovující původní rovnici. □

2.9 Metoda řešení užitím principu matematické indukce

Princip matematické indukce je důkazová metoda pro výrokové formy $V(n)$, kde $n \in \mathbb{N}$, která se používá na tvrzeních, jež jsou definované na množině přirozených čísel (nebo na množině s ní ekvivalentní). S touto metodou dokazování matematických tvrzení se setkávají žáci obvykle již na střední škole. Uvedená metoda je velmi užitečná při dokazování mnoha rovností či při řešení mnoha algebraických příkladů. Princip matematické indukce lze využít při řešení rovnic, a to i diofantovských rovnic.

Princip matematické indukce se skládá vždy ze dvou kroků:
1. *krok*: Dokážeme, že dokazované tvrzení platí pro nejmenší přirozené číslo n, kterým obecně nemusí být vždy $n = 1$.

Indukční krok: Předpokládejme, že tvrzení platí pro nějaké $k \in \mathbb{N}$ (indukční předpoklad). Dále se snažíme dokázat, že z platnosti tvrzení pro k plyne i platnost tvrzení pro $k + 1$.
Spojením obou kroků je tak ověřeno, že dané tvrzení platí pro libovolné $n \in \mathbb{N}$. K lepšímu objasnění celého procesu uvádíme příklad.

Příklad 19

Dokažte, že pro všechna $n \in \mathbb{N}$ je rovnice

$$x^2 + y^2 + z^2 = 41^n$$

řešitelná v oboru přirozených čísel.

Řešení. K důkazu použijeme princip matematické indukce vzhledem k n.
(i) Ověříme, zda daná rovnice má řešení pro $n = 1$ a $n = 2$.[6] Pro $n = 1$ existuje uspořádaná trojice přirozených čísel $(1, 2, 6)$, která po dosazení splňuje původní rovnici. Platí

$$1^2 + 2^2 + 6^2 = 41, \text{ tj.}$$

$$41 = 41.$$

Pro $n = 2$ existuje uspořádaná trojice přirozených čísel $(23, 24, 24)$, která po dosazení splňuje původní rovnici. Platí

$$23^2 + 24^2 + 24^2 = 41^2, \text{ tj.}$$

$$1681 = 1681.$$

(ii) Předpokládejme, že rovnice platí pro $n \geq 3$ a řešením je uspořádaná trojice (x_n, y_n, z_n). Definujme nyní $x_{k+2} = 41x_k$, $y_{k+2} = 41y_k$, $z_{k+2} = 41z_k$, pro každé $k \geq 1$. Pak

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 41^2(x_k^2 + y_k^2 + z_k^2).$$

Podle indukčního předpokladu platí $x_n^2 + y_n^2 + z_n^2 = 41^n$. Z indukčního předpokladu a výše uvedené rovnice plyne i platnost rovnice

$$x_{n+2}^2 + y_{n+2}^2 + z_{n+2}^2 = 41^2(x_n^2 + y_n^2 + z_n^2) = 41^{n+2}.$$

Jelikož jsme dokázali, že z tvrzení pro n plyne tvrzení pro $n+2$, potřebovali jsme v prvním kroku dokázat platnost tvrzení pro jedno číslo liché a druhé sudé.

Závěr. Spojením obou kroků je ověřena platnost tvrzení pro všechna $n \in \mathbb{N}$. Všechna řešení původní rovnice jsou uspořádané trojice přirozených čísel, protože uspořádané trojice v 1. kroku řešení byly rovněž trojice přirozených čísel. □

[6] Nalezení uspořádaných trojic přirozených čísel pro $n = 1$ a $n = 2$ lze provést např. pomocí metody nerovností a odhadů.

2.10 Eliminační metoda

Eliminační metoda je metodou řešení soustav rovnic. Tuto metodu znají žáci již na základní škole, kde patří mezi základní metody. V 3. kapitole rozebereme podrobněji problematiku soustav diofantovských rovnic. V této kapitole se omezíme pouze na popsaní eliminační metody při řešení soustav diofantovských rovnic. Eliminační metoda je založena na jednoduché myšlence, že z vhodné rovnice dané soustavy diofantovských rovnic vyloučíme vztah pro určitou neznámou. Tento vztah dosadíme do dalších rovnic soustavy, které následně upravíme a tím eliminujeme určité neznámé. Tímto způsobem pokračujeme do té doby, dokud nezískáme již jednu diofantovskou rovnici, kterou můžeme řešit např. metodami již dříve popsanými v této práci. Získáme tak řešení, které vyhovuje všem rovnicím dané soustavy.

Příklad 20 (T. Riemel)

V oboru celých čísel řešte soustavu diofantovských rovnic:

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

Řešení. Daná soustava diofantovských rovnic se skládá pouze z lineárních diofantovských rovnic. Tudíž, aby mohla být uvedená soustava řešitelná, musí být řešitelná každá rovnice soustavy. Pro ověření řešitelnosti použijeme větu 1.1.5. Jelikož $D(1,3) \mid 4$, je první rovnice soustavy řešitelná. Druhá rovnice je taktéž řešitelná, protože $D(3,2,5) \mid 7$. V dalším kroku si vyjádříme z první rovnice neznámou x

$$x = 4 - 3y.$$

Dosazením x do druhé rovnice získáme rovnici ve tvaru

$$-11y + 5z = -5.$$

Tato rovnice je lineární diofantovská rovnice o dvou neznámých a lze ji řešit pomocí metod popsaných ve výše uvedených kapitolách. V tomto příkladu využijeme metodu řešení pomocí číselných kongruencí (viz kapitola 2.4). Podle této

metody můžeme přepsat rovnici $-11y + 5z = -5$ na kongruenční rovnici, kterou následně upravíme

$$\begin{aligned} -11y &\equiv 0 \pmod 5, \\ 4y &\equiv 0 \pmod 5, \\ y &\equiv 0 \pmod 5. \end{aligned}$$

Je tedy $y = 5k$, kde $k \in \mathbb{Z}$. Dosazením za y do rovnice $-11y+5z = -5$ dostaneme

$$z = -1 + 11k.$$

Jelikož $y = 5k$, pak $x = 4 - 15k$.

Závěr. Řešením dané soustavy diofantovských rovnic jsou všechny uspořádané trojice $(4 - 15k, 5k, -1 + 11k)$, kde $k \in \mathbb{Z}$. □

2.11 Aditivní metoda

Mezi základní metody řešení soustav rovnic patří aditivní metoda. Tuto metodu znají žáci již ze základních škol. Žáci mnohdy používají při řešení soustav rovnic buď tuto metodu či metodu eliminační (viz kapitola 2.10). Hlavní myšlenkou této metody je skutečnost, že vhodným sečtením určitých násobků některých rovnic soustavy vznikne nová rovnice s menším počtem neznámých. Tuto novou rovnici můžeme záměnou vložit do původní soustavy diofantovských rovnic a opakovat celý postup několikrát, dokud nezbyde jediná diofantovská rovnice, kterou už můžeme řešit např. pomocí metod popsaných v předchozích kapitolách.

Příklad 21 (T. Riemel)

V oboru celých čísel řešte soustavu diofantovských rovnic:

$$\begin{aligned} x + 11z &= 2, \\ 3x - 7y + 31z &= 12. \end{aligned}$$

Řešení. Daná soustava diofantovských rovnic se skládá pouze z lineárních diofantovských rovnic. Tudíž, aby mohla být uvedená soustava řešitelná, musí být řešitelná každá rovnice soustavy. Pro ověření řešitelnosti použijeme větu 1.1.5.

Jelikož $D(1, 11) \mid 2$, je první rovnice soustavy řešitelná. Druhá rovnice je taktéž řešitelná, protože $D(3, 7, 31) \mid 12$. V dalším kroku vynásobíme první rovnici soustavy číslem -3. Dostaneme soustavu ve tvaru:

$$\begin{aligned} -3x - 33z &= -6, \\ 3x - 7y + 31z &= \ 12. \end{aligned}$$

Sečtením obou rovnic této upravené soustavy, která je ekvivalentní s původní soustavou, získáme diofantovskou rovnici

$$7y + 2z = -6.$$

Tuto rovnici lze řešit pomocí metod uvedených dříve v této práci. V tomto příkladu použijeme Eulerovu metodu (kapitola 2.2). Jelikož menší koeficient je u neznámé z, vyjádříme si neznámou z ve tvaru

$$z = -\frac{6 + 7y}{2} = -3 - 3y - \frac{y}{2}.$$

Zlomek $y/2$ musí být celým číslem, neboť $z \in \mathbb{Z}$. Je tedy

$$y = 2l,$$

kde $l \in \mathbb{Z}$. Dosazením za y do rovnice $7y + 2z = -6$ získáme vztah

$$z = -3 - 7l.$$

Dosazením za y a z do libovolné rovnice původní soustavy diofantovských rovnic dostaneme vztah

$$x = 35 + 77l.$$

Závěr. Řešením dané soustavy jsou uspořádané trojice $(35 + 77l, 2l, -3 - 7l)$, kde $l \in \mathbb{Z}$. □

3 Soustavy diofantovských rovnic

Na základní, resp. na střední škole se žáci mohou setkat s řešením soustav rovnic, v nichž se hledají celočíselná řešení, která jsou řešením každé rovnice soustavy. Jinými slovy hledáme průnik všech řešení rovnic dané soustavy. V předchozích kapitolách 2.10 a 2.11 jsme představili metody řešení soustav diofantovských rovnic (eliminační a aditivní metodu), které lze využít. V této kapitole se pokusíme shrnout řešení soustav diofantovských rovnic pomocí již zmíněných dvou metod a na základě řešení jednotlivých rovnic soustavy tak najít průnik těchto řešení, který je tedy zároveň řešením dané soustavy.

3.1 Soustavy lineárních diofantovských rovnic

Při řešení soustav lineárních diofantovských rovnic lze využít poznatků z kapitoly 1 a to konkrétně větu 1.1.5. Pokud se nám podaří ukázat, že alespoň jedna z lineárních diofantovských rovnic dané soustavy nemá řešení, pak celá soustava nemá řešení. Proto bude zmínka na začátku každého příkladu, abychom zjistili, zda daná soustava může být řešitelná. V dalším kroku použijeme aditivní, eliminační metodu nebo na základě znalosti řešení jednotlivých rovnic soustavy budeme hledat průnik těchto řešení.

Příklad 1 (T. Riemel)

V oboru celých čísel řešte soustavu diofantovských rovnic:

$$\begin{aligned} x - 7y + 6z &= \ \ 3, \\ 5x + 12y - 8z &= 11. \end{aligned}$$

Řešení 1. Nejprve ověříme, zda jsou obě rovnice dané soustavy řešitelné. Jelikož $D(1,7,6) \mid 3$ a $D(5,12,8) \mid 11$, jsou obě rovnice řešitelné. V tomto řešení použijeme eliminační metodu (viz kapitola 2.10). Z první rovnice soustavy získáme vztah $x = 3+7y-6z$. Po dosazení tohoto vztahu do druhé rovnice získáme diofantovskou rovnici ve tvaru

$$47y - 38z = -4.$$

Tuto rovnici budeme řešit Eulerovou metodou (kapitola 2.2). Nejprve si vyjádříme vztah pro z

$$z = \frac{4 + 47y}{38} = y + \frac{4 + 9y}{38}.$$

Jelikož $z \in \mathbb{Z}$, musí být celým číslem $(4 + 9y)/38$, tzn.

$$4 + 9y = 38k,$$

kde $k \in \mathbb{Z}$. Úpravou získáme vztah

$$y = \frac{38k - 4}{9} = 4k + \frac{2k - 4}{9}.$$

Jelikož $y \in \mathbb{Z}$, musí být celým číslem $(2k - 4)/9$, tzn.

$$2k - 4 = 9l,$$

kde $l \in \mathbb{Z}$. Opětovnou úpravou získáme vztah

$$k = \frac{9l + 4}{2} = 4l + 2 + \frac{l}{2}.$$

Z poslední rovnice plyne, že musí platit vztah $l = 2m$, kde $m \in \mathbb{Z}$. Dosazením získáme

$$\begin{aligned} y &= 38m + 8, \\ z &= 47m + 10, \\ x &= -16m - 1. \end{aligned}$$

Závěr. Řešením dané soustavy jsou všechny uspořádané trojice ve tvaru $(-16m - 1, 38m + 8, 47m + 10)$, kde $m \in \mathbb{Z}$. □

Řešení 2. Jelikož v řešení 1 jsme již ověřili, že jsou obě rovnice soustavy řešitelné, proto tento krok přeskočíme a řešíme dále danou soustavu aditivní metodou (kapitola 2.11). První rovnici soustavy vynásobíme číslem -5 a získáme tak novou soustavu ve tvaru

$$\begin{aligned} -5x + 35y - 30z &= -15, \\ 5x + 12y - 8z &= 11. \end{aligned}$$

Sečtením obou rovnic získáme diofantovskou rovnici

$$47y - 38z = -4,$$

v níž došlo k eliminaci neznámé x. Dále můžeme postupovat analogicky jako v 1. řešení a dostaneme stejné (analogické) řešení. □

Řešení 3. Třetí způsob řešení vychází ze znalosti řešení jednotlivých rovnic soustavy. Jelikož jsme v 1. řešení ověřovali řešitelnost obou rovnic, proto tento krok přeskočíme. V dalším kroku řešme první rovnici soustavy $x-7y+6z = 3$. Pro získání řešení této rovnice použijeme metodu číselných kongruencí (viz kapitola 2.4), díky níž lze přepsat rovnici do tvaru

$$x \equiv y \pmod 3.$$

Pokud položíme $y = k$, kde $k \in \mathbb{Z}$, pak $x = k + 3l$, kde $l \in \mathbb{Z}$. Dosazením za x, y do původní rovnice získáme

$$z = \frac{1 + 2k - l}{2}.$$

Jelikož $z \in \mathbb{Z}$, musí být výraz $1 + 2k - l = 2m$, kde $m \in \mathbb{Z}$. Úpravou dostaneme vztah $l = 1+2k-2m$. Dosazením získáme uspořádané trojice $(3+7k-6m, k, m)$, které jsou řešením rovnice $x - 7y + 6z = 3$.
Nyní řešme rovnici $5x + 12y - 8z = 11$. Opět použijeme metodu číselných kongruencí a rovnici přepíšeme do tvaru

$$x \equiv 1 \pmod 2.$$

Je tedy $x = 1 + 2a$, kde $a \in \mathbb{Z}$. Dosazením za x do rovnice $5x + 12y - 8z = 11$ získáme diofantovskou rovnici

$$6y - 4z = 3 - 5a.$$

Levá strana této rovnice je sudé číslo, z čehož plyne, že $a = 2b - 1$, kde $b \in \mathbb{Z}$. Úpravou dostaneme

$$3y - 2z = 4 - 5b,$$

kterou lze přepsat do tvaru kongrueční rovnice $y \equiv b \pmod 2$, tzn. $y = b + 2c$, kde $c \in \mathbb{Z}$. Dosazením vztahu $y = b + 2c$ do $3y - 2z = 4 - 5b$ dostaneme

$z = 4b + 3c - 2$. Řešením druhé rovnice soustavy jsou tedy uspořádané trojice $(-1 + 4b, b + 2c, -2 + 4b + 3c)$.

Porovnáním nalezených uspořádaných trojic vznikne soustava

$$\begin{aligned} -1 + 4b &= 3 + 7k - 6m, \\ b + 2c &= k, \\ -2 + 4b + 3c &= m. \end{aligned}$$

Dosazením za k, m do první rovnice této soustavy získáme

$$c = \frac{16 - 21b}{4} = 4 - 5b - \frac{b}{4}.$$

Jelikož $c \in \mathbb{Z}$, pak $b = 4d$, kde $d \in \mathbb{Z}$. Zpětným dosazením dostaneme řešení příkladu

$$\begin{aligned} x &= -1 + 4b &&= -1 + 16d, \\ y &= b + 2c &&= 8 - 38d, \\ z &= -2 + 4b + 3c = &&10 - 47d. \end{aligned}$$

Závěr. Řešením dané soustavy rovnic jsou všechny uspořádané trojice ve tvaru $(-1 + 16d, 8 - 38d, 10 - 47d)$, kde $d \in \mathbb{Z}$. □

Příklad 2 (T. Riemel)

V oboru celých čísel řešte soustavu diofantovských rovnic:

$$\begin{aligned} 2x - y + 3z &= 5, \\ 5x + 6y - 2z + v &= 7, \\ 3x - 5y + 11z + 3v &= 9. \end{aligned}$$

Řešení. Každá rovnice soustavy řešitelná, neboť $D(2, 1, 3) \mid 5$, $D(5, 6, 2, 1) \mid 7$ a $D(3, 5, 11, 3) \mid 9$. Tuto soustavu rovnic budeme řešit eliminační metodou (viz kapitola 2.10). Z první rovnice soustavy získáme vztah $y = 2x + 3z - 5$, který aplikujeme do zbylých rovnic soustavy a získáme soustavu

$$\begin{aligned} 17x + 16z + v &= 37, \\ 7x + 4z - 3v &= 16. \end{aligned}$$

Znovu použijeme eleminační metodu a vztah $v = 37 - 17x - 16z$ získaný z první rovnice této soustavy aplikujeme na rovnici druhou. Dostaneme diofantovskou rovnici ve tvaru

$$58x + 52z = 127.$$

Jelikož levá strana této diofantovské rovnice je sudé číslo a pravá strana číslo liché, pak nemá tato rovnice řešení v oboru celých čísel, a tudíž nemá řešení ani původní soustava rovnic.

Závěr. Daná soustava nemá řešení v oboru celých čísel, ačkoliv každá rovnice dané soustavy diofantovských rovnic je řešitelná. □

3.2 Soustavy diofantovských rovnic vyšších řádů

Mnohdy je potřeba řešit nejen soustavy lineárních rovnic, ale i soustavy rovnic vyšších řádů. Proto je v této práci věnována její část právě této problematice. Soustavou diofantovských rovnic vyšších řádů máme na mysli soustavu diofantovských rovnic, v níž alespoň jedna z rovnic soustavy je vyššího řádu než lineární. V předchozí kapitole jsme ukázali 3 způsoby řešení soustav lineárních diofantovských rovnic. U soustav rovnic vyšších řádů první dvě metody (aditivní a eliminační) nemusí být vždy efektivní, a proto je většinou vhodnější využít třetí možnost řešení založenou na hledání společného řešení vycházejícího ze znalosti řešení jednotlivých rovnic soustavy.

Příklad 3 (T. Riemel)

V oboru celých čísel řešte soustavu:

$$\begin{aligned} x^2y^2 + 9x^2 + 4y^2 - 6x^2y + 4xy^2 - 24xy + 36x - 24y + 27 &= 0, \\ 21x + 6y &= 15. \end{aligned}$$

Řešení. První rovnice soustavy je řešenou rovnicí z příkladu 16 v kapitole 2.7. Řešením dané rovnice jsou uspořádané dvojice $(x, y) \in \{(-1, 6), (-3, 0), (-3, 6), (-1, 0)\}$. Druhá rovnice soustavy je řešenou rovnicí v příkladu 4 v kapitole 2.2. Řešením dané diofantovské rovnice jsou uspořádané dvojice $(1 - 2d, -1 + 7d)$, kde $d \in \mathbb{Z}$. Ze znalosti řešení obou rovnic soustavy hledáme společné řešení soustavy, jenž musí splňovat alespoň jednu z následujících čtyř soustav rovnic:

$$\begin{aligned} \text{a)}\ -1 &= \quad 1 - 2d, \\ 6 &= -1 + 7d, \end{aligned} \qquad \begin{aligned} \text{b)}\ -3 &= \quad 1 - 2d, \\ 0 &= -1 + 7d, \end{aligned}$$

$$\begin{aligned} \text{c)}\ -3 &= \quad 1 - 2d, \\ 6 &= -1 + 7d, \end{aligned} \qquad \begin{aligned} \text{d)}\ -1 &= \quad 1 - 2d, \\ 0 &= -1 + 7d. \end{aligned}$$

Nyní budeme řešit jednotlivě výše uvedené soustavy rovnic.

a) Nechť

$$\begin{aligned} -1 &= \quad 1 - 2d, \\ 6 &= -1 + 7d. \end{aligned}$$

Z první rovnice plyne $d = 1$. Dosazením tohoto vztahu do druhé rovnice získáme rovnost $6 = 6$. Tedy $(-1, 6)$ je řešením dané soustavy diofantovských rovnic.

b) Nechť

$$\begin{aligned} -3 &= \quad 1 - 2d, \\ 0 &= -1 + 7d. \end{aligned}$$

Z první rovnice plyne $d = 2$. Dosazením tohoto vztahu do druhé rovnice získáme rovnost $1 = 14$, která neplatí. Tudíž $(-3, 0)$ není řešením dané soustavy diofantovských rovnic.

c) Nechť

$$\begin{aligned} -3 &= \quad 1 - 2d, \\ 6 &= -1 + 7d. \end{aligned}$$

Z první rovnice plyne $d = 2$. Dosazením tohoto vztahu do druhé rovnice získáme rovnost $7 = 14$, která neplatí. Tudíž $(-3, 6)$ není řešením dané soustavy diofantovských rovnic.

d) Nechť

$$\begin{aligned} -1 &= \quad 1 - 2d, \\ 0 &= -1 + 7d. \end{aligned}$$

Z první rovnice plyne $d = 1$. Dosazením tohoto vztahu do druhé rovnice získáme rovnost $1 = 6$, která neplatí. Tudíž $(-1, 0)$ není řešením dané soustavy diofantovských rovnic.

Závěr. Jediným řešením dané soustavy diofantovských rovnic je uspořádaná dvojice $(x, y) = (-1, 6)$. □

Příklad 4 (T. Riemel)

V oboru celých čísel řešte soustavu:

$$\begin{aligned} 5x^2 + 2xy + 5y^2 &= 8x^2y^2, \\ x^5 + 4y^5 &= 8z^5. \end{aligned}$$

Řešení. První rovnice soustavy je řešenou rovnicí z příkladu 12 v kapitole 2.6. Řešením dané rovnice je uspořádaná dvojice $(0, 0)$. Druhá rovnice soustavy je řešenou rovnicí v příkladu 17 v kapitole 2.8. Řešením dané diofantovské rovnice je uspořádaná trojice $(0, 0, 0)$. Řešením druhé rovnice je uspořádaná trojice, z čehož plyne, že řešením první rovnice jsou uspořádané trojice $(x, y, z) = (0, 0, k)$, kde k je libovolné celé číslo.

Závěr. Řešením dané soustavy je uspořádaná trojice $(x, y, z) = (0, 0, 0)$, jelikož musí být splněny obě rovnice dané soustavy zároveň. □

Příklad 5 (MD A–I–3–05)

V oboru celých čísel řešte soustavu:

$$\begin{aligned} x^2z + y^2z + 4xy &= 40, \\ x^2 + \quad y^2 + xyz &= 20. \end{aligned}$$

Řešení. Při řešení této úlohy použijeme aditivní metodu. Nejprve vynásobíme druhou rovnici soustavy číslem 2 a získáme ekvivalentní soustavu rovnic ve tvaru

$$x^2z + y^2z + \ 4xy = 40,$$
$$2x^2 + 2y^2 + 2xyz = 40.$$

Sečtením obou rovnic takto upravené soustavy dostaneme

$$x^2y + y^2z + 4xy + 2x^2 + 2y^2 + 2xyz = 80.$$

Tuto rovnici lze zapsat v součinovém tvaru

$$(x + y)^2(z + 2) = 80.$$

Z poslední rovnice plyne metoda faktorizace. Jelikož $80 = 2^4 \cdot 5$, dostáváme tři možnosti:

a) $x+y = \pm 1$. Dostáváme $(\pm 1)^2(z+2) = 80$, z čehož plyne $z = 78$. Dosazením za z do původní soustavy rovnic získáme soustavu rovnic

$$39(x^2 + y^2) + 2xy = 20,$$
$$x^2 + \ y^2 = 20 - 78xy.$$

Tuto soustavu řešíme eliminační metodou a dostaneme rovnici

$$76xy = 19,$$

která však nemá žádné řešení pro x, y celá.

b) $x+y = \pm 2$. Dostáváme $(\pm 2)^2(z+2) = 80$, z čehož plyne $z = 18$. Dosazením za z do původní soustavy rovnic získáme soustavu rovnic

$$9(x^2 + y^2) + 2xy = 20,$$
$$x^2 + \ y^2 = 20 - 18xy.$$

Tuto soustavu řešíme eliminační metodou a dostaneme rovnici

$$xy = 1,$$

ze které plynou 2 řešení $x_1 = y_1 = 1$ a $x_2 = y_2 = -1$. Řešením dané soustavy jsou uspořádané trojice $(x, y, z) \in \{(1, 1, 18), (-1, -1, 18)\}$.

c) $x+y=\pm 4$. Dostáváme $(\pm 4)^2(z+2)=80$, z čehož plyne $z=3$. Dosazením za z do původní soustavy rovnic získáme soustavu rovnic

$$\begin{aligned} 3(x^2+y^2)+4xy &= 40, \\ x^2+\ \ y^2 &= 20-3xy. \end{aligned}$$

Tuto soustavu řešíme eliminační metodou a dostaneme rovnici

$$xy=4.$$

Z druhé rovnice upravené soustavy plyne $x^2+y^2=8$. Získáváme tak 2 řešení $x_3=y_3=2$ a $x_4=y_4=-2$. Řešením dané soustavy jsou zde uspořádané trojice $(x,y,z)\in\{(2,2,3),(-2,-2,3)\}$.

Závěr. Řešením dané soustavy rovnic jsou následující uspořádané trojice celých čísel $(x,y,z)\in\{(1,1,18),\ (-1,-1,18),(2,2,3),(-2,-2,3)\}$. □

4 Řešené úlohy z MO

Na většině středních škol studují žáci, kteří řeší MO. Jelikož v mnoha uplynulých ročnících MO se vyskytovaly diofantovské rovnice, uvádíme zde některé řešené příklady z MO z oblasti diofantovských rovnic.

Příklad 1 (MO 57–C–II–2)

Klárka udělala chybu při písemném násobení dvou dvoumístných čísel, a tak jí vyšlo číslo o 400 menší, než byl správný výsledek. Pro kontrolu vydělila číslo, které dostala, menším z násobených čísel. Tentokrát počítala správně a vyšel jí neúplný podíl 67 a zbytek 56. Která čísla Klárka násobila?

Řešení. Pokud označíme x menší a y větší z násobených čísel, pak ze zadání úlohy plyne

$$xy - 400 = 67x + 56.$$

Tuto rovnici lze zapsat ve tvaru $x(y - 67) = 456$. Číslo x musí být dvoumístný dělitel čísla $456 = 2^3 \cdot 3 \cdot 19$, kde jsme využili metody faktorizace (kapitola 2.7). Ze zadání rovněž plyne, že číslo x je větší než příslušný zbytek 56. Nejmenší možnou hodnotou x, které splňuje zadání úlohy je $x = 3 \cdot 19 = 57$. Další možná hodnota x musí splňovat nerovnost $x \geq 4 \cdot 19 = 76$. Pro y dostáváme nerovnost $y - 67 \leq 2 \cdot 3 = 6$. Z těchto dvou nerovností plyne, že

$$y \leq 73 < x.$$

Poslední vztah ovšem odporuje zvolenému označení, kdy $x < y$. Jediným možným řešením dané úlohy je tedy uspořádaná dvojice $(x, y) = (57, 75)$.

Závěr. Klárka násobila čísla 57 a 75. □

Příklad 2 (MO 57–C–II–4)

Najděte všechny trojice celých čísel x, y, z pro něž platí

$$x + y\sqrt{3} + z\sqrt{7} = y + z\sqrt{3} + x\sqrt{7}.$$

Řešení. Danou rovnici lze přepsat ve tvaru

$$x - y = (z - y)\sqrt{3} + (x - z)\sqrt{7}.$$

Po umocnění a následné úpravě získáme rovnici

$$(x-y)^2 - 3(z-y)^2 - 7(x-z)^2 = 2(x-z)(z-y)\sqrt{21}.$$

Povšimněme si, že pro $x \neq z$ a $y \neq z$ nemůže výše uvedená rovnice platit, neboť na levé straně rovnice by bylo číslo celé a na pravé straně číslo iracionální. Rovnost může nastat, právě když $x = z$ nebo $y = z$. Po dosazení za $x = z$ do původní rovnice dostaneme

$$z - y = \sqrt{3}(z - y).$$

Tato rovnost platí jen, když $x = y = z$. V druhém případě po dosazení $y = z$ do původní rovnice dospějeme ke stejnému výsledku.

Závěr. Řešením dané rovnice jsou uspořádané trojice $(x, y, z) = (m, m, m)$, kde $m \in \mathbb{Z}$. □

Příklad 3 (MO 57–C–I–3)

Máme určitý počet krabiček a určitý počet kuliček. Dáme–li do každé krabičky právě jednu kuličku, zbyde nám n kuliček. Když však dáme právě n krabiček stranou, můžeme všechny kuličky rozmístit tak, aby jich v každé zbývající krabičce bylo právě n. Kolik máme krabiček a kolik kuliček?

Řešení. Označme neznámou x počet krabiček a neznámou y počet kuliček. Toto označení umožňuje zapsat zadání úlohy ve tvaru soustavy rovnic

$$x + n = y,$$
$$(x - n) \cdot n = y,$$

s neznámými $x, y, n \in \mathbb{N}$. Tuto soustavu diofantovských rovnic lze řešit např. pomocí eliminační či aditivní metody (kapitoly 2.10 a 2.11). Vyjádřením $y = x + n$ a následným přepsáním druhé rovnice soustavy získáme rovnici ve tvaru $x + n = (x - n) \cdot n$, která nemá řešení pro $n = 1$. Pro $n \geq 2$ dostaneme rovnici

$$x = \frac{n^2 + n}{n - 1} = n + 2 + \frac{2}{n - 1}.$$

Jelikož $x \in \mathbb{N}$, musí být číslo $n - 1$ dělitelem čísla 2, tj. $n \in \{2, 3\}$. Dosazením $n = 2$ do původní soustavy rovnic získáme řešení $(x, y) = (6, 8)$. Dosazením $n = 3$ do původní soustavy rovnic získáme řešení $(x, y) = (6, 9)$.

Závěr. Daná úloha má 2 řešení. Buď máme šest krabiček a osm kuliček, nebo máme šest krabiček a devět kuliček. □

Příklad 4 (MO 57–C–I–6)

Klárka měla na papíru napsáno trojmístné číslo. Když ho správně vynásobila devíti, dostala čtyřmístné číslo, jež začínalo touž číslicí jako číslo původní, prostřední dvě číslice se rovnaly a poslední číslice byla součtem číslic původního čísla. Které čtyřmístné číslo mohla Klárka dostat?

Řešení. Neznámou x označme původní číslo $x = 100a + 10b + c$, kde a, b, c jsou jeho číslice. Neznámou d označme číslici, která se vyskytuje na prostředních dvou místech výsledného součinu. Zadání úlohy lze pak zapsat ve tvaru

$$9 \cdot (100a + 10b + c) = 1000a + 100d + 10d + (a + b + c).$$

Úpravou lze rovnici zapsat ve tvaru

$$100 \cdot (b - a - d) = 10d + a + 11b - 8c.$$

Využitím metody nerovností a odhadů (kapitola 2.6) můžeme bez újmy na obecnosti předpokládat, že platí $b \geq a$. Pomocí dosazování jednotlivých přípustných hodnot za neznámé a, b, c v níže uvedené tabulce hledáme řešení dané úlohy.

a	1	1	1	1	2	2	2	3	3	4
b	7	5	3	1	6	4	2	5	3	4
c	1	2	3	4	1	2	3	1	2	1
$9x$	1539	1368	1197	1026	2349	2178	2007	3159	2988	3969

Závěr. Řešením úlohy je právě jedno čtyřmístné číslo vyhovující zadání, a to číslo 2007. □

Příklad 5 (MO 56–C–I–1)

Určete všechny dvojice (a, b) přirozených čísel, pro něž platí

$$a + b\sqrt{5} = b + a\sqrt{5}.$$

Řešení. Pomocí substitucí (viz kapitola 2.3) $m = \sqrt{a}$, $n = \sqrt{b}$ dostaneme danou rovnici ve tvaru

$$m^2 - n^2 - 5(m - n) = 0.$$

Úpravou lze převést předchozí rovnici do součinového tvaru

$$(m-n)(m+n-5)=0,$$

kterou řešíme pomocí metody faktorizace (kapitola 2.7). Tedy $m=n$ nebo $m+n=5$. V prvním případě po zpětné substituci zjistíme, že zadání úlohy vyhovují všechny uspořádané dvojice ve tvaru $(a,b)=(k,k)$, kde $k\in\mathbb{Z}$. V druhém případě dostáváme rovnici $\sqrt{a}+\sqrt{b}=5$, kterou řešíme metodou nerovností a odhadů (kapitola 2.6). Jelikož $a,b\in\mathbb{N}$, platí $1\leq\sqrt{a},\sqrt{b}\leq 4$. Všimněme si, že rovnice $\sqrt{a}+\sqrt{b}=5$ se nezmění záměnou neznámých a,b. Proto můžeme předpokládat, že $a\leq b$. Z předpokladu plyne $\sqrt{a}\leq 2,5$, a tedy $a\leq 6,25$. Dosazením hodnot $a=1,2,\ldots,6$ do vztahu

$$b=(5-\sqrt{a})^2,$$

získáme konkrétní řešení rovnice, přičemž zbylá řešení získáme záměnou nalezených hodnot pro a,b.

Závěr. Dané rovnici vyhovují uspořádané dvojice $(a,b)\in\{(1,16),\,(4,9),\,(9,4),\,(16,1),\,(k,k)\}$, kde $k\in\mathbb{Z}$. □

Příklad 6 (MO 53–C–II–4)

Žáci měli vypočítat příklad $x+y\cdot z$ pro trojmístné číslo x a dvojmístná čísla y,z. Martin umí násobit a sčítat čísla zapsaná v desítkové soustavě, ale zapomněl na pravidlo přednosti násobení před sčítáním. Proto mu vyšlo sice zajímavé číslo, které se čte stejně zleva doprava jako zprava doleva, správný výsledek byl ale o 2 004 menší. Určete čísla x,y,z.

Řešení. Martin spočítal hodnotu $(x+y)z$ místo $x+yz$, takže podle zadání platí

$$(x+y)z-(x+yz)=2\,004\quad\text{čili}\quad x(z-1)=2\,004=12\cdot 167,$$

přičemž číslo 167 je prvočíslem. V dalším kroku řešení využijeme metodu faktorizace a metodu nerovností a odhadů (viz kapitoly 2.7 a 2.6). Číslo z je dvojmístné, tudíž musí platit nerovnost

$$9\leq z-1\leq 98.$$

Z rovnice $x(z-1) = 2\,004 = 12 \cdot 167$ plyne $x = 167$, $z = 13$. Martin tedy vypočítal číslo $C = (167 + y) \cdot 13$. Číslo C je čtyřmístné, a jelikož se čte zepředu stejně jako zezadu, pak lze zapsat ve tvaru $C = 1\,001a + 110b$, kde $a \in \{1, 2, \ldots, 9\}$, $b \in \{0, 1, \ldots, 9\}$. Protože $1\,001 = 13 \cdot 77$, musí platit rovnost

$$(167 + y) \cdot 13 = 13 \cdot 77a + 110b.$$

Z této rovnosti plyne, že $13 \mid b$, což splňuje pouze $b = 0$. Po dosazení b dostaneme rovnost

$$167 + y = 77a.$$

Jelikož číslo y je dvojmístné, tudíž musí splňovat i nerovnost $10 \leq y \leq 99$. Z čehož plyne, že $a = 3$ a tedy $y = 64$.

Závěr. Žáci měli počítat příklad $167 + 64 \cdot 13$, tedy $x = 167$, $y = 64$, $z = 13$. □

Příklad 7 (MO 51–C–I–3)

Určete všechny dvojice (x, y) celých čísel, které jsou řešením nerovnice

$$\frac{x}{\sqrt{x}} + \frac{6}{y\sqrt{x}} < \frac{5\sqrt{y}}{y}.$$

Řešení. V zadání úlohy se vyskytuje diofantovská nerovnice. Ačkoliv je tato práce věnovaná diofantovským rovnicím, přesto uvádíme jeden příklad diofantovské nerovnice, kterou lze řešit pomocí metod používaných pro řešení diofantovských rovnic.

Ze zadání úlohy plyne, že x, y musí být přirozená čísla. Vynásobením obou stran nerovnice kladným číslem $y\sqrt{x}$ získáme ekvivalentní nerovnici

$$xy + 6 < 5\sqrt{5}.$$

Úpravou dostaneme nerovnici v součinovém tvaru

$$(\sqrt{xy} - 3)(\sqrt{xy} - 2) < 0,$$

která platí, právě když $2 < \sqrt{xy} < 3$. Jelikož $x, y \in \mathbb{N}$, z poslední nerovnice plyne, že stačí uvažovat jen $xy < 9$. Dosazením přípustných hodnot za x, y získáme uspořádané dvojice přirozených čísel, jenž jsou řešením poslední nerovnice a dané nerovnice, která je s ní ekvivalentní.

Závěr. Řešením dané nerovnice jsou uspořádané dvojice $(x, y) \in \{(1,5),\ (1,6),\ (1,7),\ (1,8),\ (2,3),\ (2,4),\ (3,2),\ (4,2),\ (5,1),\ (6,1),\ (7,1),\ (8,1)\}$. □

Příklad 8 (MO 51–C–I–4)

Josef se vracel z výletu. Nejdříve jel vlakem a pak pokračoval ze zastávky na kole. Celá cesta mu trvala přesně 1 hodinu 30 minut a urazil při ní vzdálenost 60 km. Vlak jel průměrnou rychlostí 50 km/h. Určete, jak dlouho jel Josef na kole, když jeho rychlost v km/h je vyjádřena přirozeným číslem stejně jako vzdálenost měřená v km, kterou na kole ujel.

Řešení. Označme x vzdálenost, kterou Josef ujel na kole a v jeho rychlost v km/h. Podle zadání $x, v \in \mathbb{N}$, přičemž $x < 60$. Na kole jel Josef po dobu x/v h. Vlakem ujel vzdálenost $(60 - x)$ km a tuto vzdálenost ujel za $(60 - x)/50$ h. Ze zadání plyne platnost rovnice

$$\frac{60 - x}{50} + \frac{x}{v} = \frac{3}{2},$$

kterou lze upravit do tvaru

$$50x - 15v - xv = 0.$$

Poslední rovnici lze přepsat v součinovém tvaru

$$(50 - v)(x + 15) = 15 \cdot 50 = 2 \cdot 3 \cdot 5^3,$$

jenž řešíme metodou faktorizace (kapitola 2.7). Z této rovnice plyne, že $50 - v$ je přirozené číslo menší než 50 a $x + 15$ je přirozené číslo větší než 15, které nepřevyšuje 75, a navíc součin $(50 - v)(x + 15)$ je dělitelný číslem 5^3. Dostáváme čtyři případy.

a) $5^3 \mid (50 - v)$. To není ovšem možné, neboť $1 \leq 50 - v < 50$.

b) $5^2 \mid (50 - v)$ a $5 \mid (x + 15)$. Číslo $50 - v$ je rovno 25, odtud $v = 25$ a $x = 15$.

c) $5 \mid (50 - v)$ a $5^2 \mid (x + 15)$. Číslo $x + 15 \in \{25, 50\}$, z čehož plynou dvě možnosti $v = 20$, $x = 10$ a $v = 35$, $x = 35$.

d) $5^3 \mid (x + 15)$. To není ovšem možné, neboť $15 < x + 15 < 75$.

Možné časy Josefovy jízdy na kole (v minutách) proto jsou $15 \cdot 60/25 = 36$, $10 \cdot 60/20 = 30$ a $35 \cdot 60/35 = 60$.

Závěr. Podle zadání úlohy ujel Josef na kole 30, 36 nebo 60 minut. □

Příklad 9 (MO 65–C–I–1)

Najděte všechny možné hodnoty součinu prvočísel p, q, r, pro která platí

$$p^2 - (q + r)^2 = 637.$$

Řešení. Podle vzorce $a^2 - b^2$ lze přepsat rovnici ve tvaru

$$(p + q + r)(p - q - r) = 637.$$

Tato rovnice je v součinovém tvaru, a proto použijeme metodu faktorizace (kapitola 2.7). Jelikož p, q, r jsou prvočísla, pak první činitel v uvedené rovnici je větší a kladný, a tudíž i druhý je kladný. Číslo 637 lze rozložit

$$637 = 637 \cdot 1 = 91 \cdot 7 = 49 \cdot 13,$$

proto hodnoty činitelů v uvedené rovnici musí být číselně rovny alespoň jedné dvojici čísel $(637, 1)$, $(91, 7)$, $(49, 13)$. Povšimněme si, že prvočíslo p je aritmetickým průměrem obou činitelů, tudíž se musí rovnat jednomu z čísel $(637 + 1)/2 = 319$, $(91 + 7)/2 = 49$, $(49 + 13)/2 = 31$. Jelikož první dvě čísla nejsou prvočísla a třetí ano ($319 = 11 \cdot 29$, $49 = 7^2$), pak $p = 31$. Z toho plynou rovnosti $31 + q + r = 49$, $31 - p - q = 13$, které jsou splněny, právě když $q + r = 18$. Takové dvojice $\{q, r\}$ jsou jedině $\{5, 13\}$ a $\{7, 11\}$.

Závěr. Zkoumaný součin pqr má dvě možné hodnoty, tj. $31 \cdot 5 \cdot 13 = 2\,015$ a $31 \cdot 7 \cdot 11 = 2\,387$. □

Příklad 10 (MO 65–C–II–1)

Najděte nejmenší možnou hodnotu výrazu

$$3x^2 - 12xy + y^4,$$

ve kterém x a y jsou libovolná nezáporná celá čísla.

Řešení. Označme daný výraz M a upravme jej pomocí dvojího užití tzv. doplnění na druhou mocninu

$$M = 3x^2 - 12xy + y^4 = 3(x-2y)^2 - 12y^2 + y^4 = 3(x-2y)^2 + (y^2-6)^2 - 36.$$

Zřejmě platí $(x-2y)^2 \geq 0$, takže nejmenší možnou hodnotu výrazu M dostaneme, právě když $x = 2y$. Nyní zbývá vyřešit nejmenší možnou hodnotu výrazu $(y^2-6)^2$. Jelikož $y^2 \in \{0, 1, 4, 9, \ldots\}$ a číslo 6 leží mezi čísly 4 a 9, platí pro každé celé číslo y nerovnost

$$(y^2-6)^2 \geq \min\{(4-6)^2, (9-6)^2\} = \min\{4, 9\} = 4.$$

Dostáváme odhad výrazu M pro libovolná celá čísla x a y

$$M \geq 3 \cdot 0 + 4 - 36 = -32.$$

Závěr. Rovnost $M = -32$ (což je nejmenší hodnota daného výrazu) nastane v poslední nerovnosti, právě když $y = 2$ a $x = 2y = 4$. □

5 Soubor neřešených úloh

Pro potřeby matematických seminářů na středních školách je možné využít i níže uvedené neřěšené příklady. U každého příkladu se nalézá návod k řešení a správný výsledek dané úlohy. Každou úlohu z kapitoly 5 lze řešit metodami již dříve popsanými v této práci.

Příklad 1 (T. Riemel)

V oboru celých čísel řešte diofantovskou rovnici

$$83x - 53y = 12.$$

[*Návod*: Úlohu lze řešit např. pomocí Eulerovy metody, metody řešení pomocí Eukleidova algoritmu, číselných kongruencí, řetězových zlomků.
Řešení: $(x, y) = (11 + 53k, 17 + 83k)$, kde $k \in \mathbb{Z}$.]

Příklad 2 (T. Riemel)

V oboru celých čísel řešte diofantovskou rovnici

$$28x + 13y = 8.$$

[*Návod*: Úlohu lze řešit např. pomocí Eulerovy metody, metody řešení pomocí Eukleidova algoritmu, číselných kongruencí, řetězových zlomků.
Řešení: $(x, y) = (4 - 13m, -8 + 28m)$, kde $m \in \mathbb{Z}$.]

Příklad 3 (MD B–T–2–13)

Najděte všechny dvojice celých čísel x a y splňující rovnici

$$\frac{2}{x} + \frac{3}{y} = 1.$$

[*Návod*: Danou rovnici lze upravit do tvaru $(x-2)(y-3) = 6$ a dále postupovat pomocí metody faktorizace.
Řešení: $(x, y) \in \{(3, 9), (8, 4), (4, 6), (5, 5), (1, -3), (-4, 2), (-1, 1)\}$.]

Příklad 4 (MD B–T–1–96)

Najděte všechna celočíselná řešení rovnice

$$xyz + xy + yz + xz + x + y + z = 1996.$$

[*Návod*: Po přičtení čísla 1 k oběma stranám dané rovnice lze upravenou rovnici zapsat ve tvaru $(x+1)(y+1)(z+1) = 1997$ a dále postupovat pomocí metody faktorizace.
Řešení: $(x, y, z) \in \{(1996, 0, 0), (0, 1996, 0), (0, 0, 1996), (1996, -2, -2), (-2, 1996, -2), (-2, -2, 1996), (1998, -2, 0), (-2, 1998, 0), (-2, 0, 1998), (1998, 0, -2), (0, 1998, -2), (0, -2, 1998)\}$.]

Příklad 5 (T. Riemel)

Řešte rovnici

$$2x + 4y - 5z + 12u = 17,$$

kde $x, y, z, u \in \mathbb{Z}$.

[*Návod*: Danou rovnici lze řešit např. metodou číselných kongruencí. Rovnici lze přepsat do tvaru kongruenční rovnice $z \equiv 1 \pmod 2$.
Řešení: $(x, y, z, u) = (1 + k + 2l, 5 + 2k - l - 3m, 1 + 2k, m)$, kde $k, l, m \in \mathbb{Z}$.]

Příklad 6 (T. Riemel)

V oboru celých čísel řešte diofantovskou rovnici

$$68x + 71y = 11.$$

[*Návod*: Úlohu lze řešit např. pomocí Eulerovy metody, metody řešení pomocí Eukleidova algoritmu, číselných kongruencí, řetězových zlomků.
Řešení: $(x, y) = (20 - 71a, -19 + 68a)$, kde $a \in \mathbb{Z}$.]

Příklad 7 (T. Riemel)

V oboru nezáporných celých čísel řešte diofantovskou rovnici

$$3x^2 - 2xy + 3y^2 = 7x^2y^2.$$

[*Návod*: Úlohu lze řešit např. pomocí metody nerovností a odhadů. Předpokládejme, že platí $x \geq y$, pak získáváme nerovnost $4x^2 \geq 7x^2y^2$.
Řešení: $(x, y) = (0, 0)$.]

Příklad 8 (T. Riemel)

V oboru nezáporných celých čísel řešte rovnici

$$x^7 + 3y^7 = 9z^7.$$

[*Návod*: Úlohu lze řešit pomocí metody nekonečného klesání, kde $x_1 = 3x$. *Řešení*: $(x, y, z) = (0, 0, 0)$.]

Příklad 9 (T. Riemel)

Nalezněte všechna celočíselná řešení soustavy rovnic

$$\begin{aligned} 3x + \ \ y \ \ \ \ &= 2, \\ 5x - 3y + z &= 7. \end{aligned}$$

[*Návod*: Danou soustavu lze řešit např. pomocí aditivní nebo eliminační metody. *Řešení*: $(x, y, z) = (k, 2 - 3k, 13 - 14k)$, kde $k \in \mathbb{Z}$.]

Příklad 10 (T. Riemel)

V oboru celých čísel řešte soustavu rovnic

$$\begin{aligned} 5x + \ \ y + 3z \ \ \ \ &= 6, \\ 9x - 3y + 4z - 8u &= 7, \\ 2x - 4y - 3z + 4u &= 9. \end{aligned}$$

[*Návod*: Danou soustavu lze řešit např. pomocí aditivní nebo eliminační metody. *Řešení*: $(x, y, z, u) = (10 - 62t, 13 - 98t, -19 + 136t, -4 + 35t)$, kde $t \in \mathbb{Z}$.]

6 Dodatek k diofantovským rovnicím

V závěru diplomové práce uvádíme dva speciální typy diofantovských rovnic a tzv. 10. Hilbertův problém. Tato kapitola má informativní charakter, a proto případní zájemci o danou problematiku mohou čerpat i z jiných zdrojů.

6.1 Pellova rovnice

Prvním speciálním typem diofantovských rovnic je tzv. Pellova rovnice. Pro níže uvedený popis řešení Pellovy rovnice se opíráme o znalosti z kapitoly 2.5.

Definice 6.1.1

Kvadratickou iracionalitou nazveme každý iracionální kořen kvadratické rovnice s celočíselnými koeficienty. Obecný tvar kvadratické iracionality lze zapsat ve tvaru

$$\frac{a+\sqrt{b}}{c},$$

kde $a, b, c \in \mathbb{Z}$, $b > 0$, kde b není druhou mocninou žádného přirozeného čísla.

Věta 6.1.2 (Lagrangeova)

Řetězový zlomek každé kvadratické iracionality je periodický.

Definice 6.1.3

Diofantovská rovnice ve tvaru

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

kde $a > 0$, $\sqrt{a}$ je kvadratická iracionalita, s neznámými $x, y \in \mathbb{Z}$, se nazývá *Pellova rovnice*.

Pellova rovnice má vždy triviální řešení $(x, y) = (1, 0)$. Pokud hledáme kladné řešení, tj. $(x, y) \in \mathbb{N}^2$, pak jej lze hledat ve tvaru $\frac{P_k}{Q_k}$, kde k je sudé a $\frac{P_k}{Q_k}$ je parciálním zlomkem čísla $\sqrt{a}$. Dá se dokázat, že (P_k, Q_k) je řešením Pellovy rovnice, je–li $\sqrt{a}$ periodický řetězový zlomek s periodou od 2. členu ve tvaru

$$\sqrt{a} = (c_1, (c_2, \ldots, c_{k+1})),$$

s délkou periody k (viz [9], str. 97). Jelikož jsme předpokládali, že k je sudé číslo, pak řešením Pellovy rovnice jsou dvojice (P_k, Q_k), (P_{2k}, Q_{2k}), atd. Pokud je k liché číslo, pak řešením Pellovy rovnice jsou dvojice (P_{2k}, Q_{2k}), (P_{4k}, Q_{4k}), atd.

Příklad 1

Najděte nejmenší kladné řešení rovnice $x^2 - 8y^2 = 1$.

Řešení. Platí $\sqrt{8} = (2, (1, 4))$, kde $k = 2$. Nejmenší kladné řešení dané rovnice je tedy $(x, y) = (P_2, Q_2) = (3, 1)$. □

Příklad 2

Určete nejmenší kladné řešení rovnice $x^2 - 13y^2 = 1$.

Řešení. Platí $\sqrt{13} = (3, (1, 1, 1, 1, 6))$, kde $k = 5$. Nejmenší kladné řešení dané rovnice je tedy $(x, y) = (P_{10}, Q_{10}) = (649, 180)$. □

6.2 Pythagorejská rovnice

Definice 6.2.1

Diofantovská rovnice ve tvaru

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

kde $x, y, z \in \mathbb{Z}$, se nazývá *pythagorejská rovnice*.

Definice 6.2.2

Uspořádaná trojice čísel (a, b, c), kde $a, b, c \in \mathbb{N}$, která splňuje pythagorejskou rovnici, se nazývá *pythagorejská trojice*.

Geometricky lze čísla a, b chápat jako velikosti odvěsen u pravoúhlého trojúhelníku a číslo c jako velikost přepony (viz Pythagorova věta). Mnozí žáci ze základních škol znají pythagorejské trojice $(3, 4, 5)$ a $(5, 12, 13)$, ovšem obecně je těchto čísel nekonečně mnoho.

Další zajímavostí v oblasti diofantovských rovnic je tzv. *Fermatův problém*. Fermatovým problémem se nazývá úloha řešit rovnici

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

kde $x, y, z \in \mathbb{Z}$, $n \in \mathbb{N}$. Triviálním řešením se nazývají uspořádané trojice $(x, y, z) \in \{(0, \pm k, k), (\pm k, 0, k)\}$ pro n sudé a $(x, y, z) \in \{(0, k, k), (k, 0, k), (k, -k, 0)\}$ pro n liché, kde k je libovolné celé číslo. Pierre de Fermat v 17. století při četbě Diofantovy Aritmetiky poznamenal na okraj knihy tvrzení:

Věta 6.2.3 (Velká Fermatova)

Pro přirozené číslo $n \geq 3$ neexistují netriviální celočíselná řešení rovnice

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

Zajímavostí je, že Fermat napsal, že údajně objevil jednoduchý důkaz tohoto tvrzení, ale jelikož se už na okraj knihy nevejde, proto ho neuvádí. Velkou Fermatovu větu dokázal anglický matematik *Andrew Wiles* roku 1994, který za důkaz této věty obdržel roku 2016 Abelovu cenu.

6.3 10. Hilbertův problém

Už v úvodní kapitole uvádíme, že neexistuje obecný algoritmus, který by vyřešil každou diofantovskou rovnici v konečném čase v oboru celých čísel. Tato znalost neexistence algoritmu nebyla však dlouhou dobu zřejmá. David Hilbert roku 1900 formuloval seznam nevyřešených otázek pro 20. století, ve kterém pod číslem 10 vystupuje následující problém:
„*Mějme diofantickou rovnici s celočíselnými koeficienty s libovolným počtem neznámých. Určete předpis, podle něhož lze po konečném počtu kroků rozhodnout, zda je tato rovnice řešitelná v oboru celých čísel.*“
Důkaz neexistence algoritmu dokončil roku 1970 *Jurij Matijasevič*, který vycházel z prací z 50. let. Více o tomto zajímavém problému lze nalézt např. v [7].

Závěr

V diplomové práci jsou soustředěny základní poznatky o metodách řešení diofantovských rovnic a jejich soustav. Práce je rozčleněna do šesti kapitol. V každé z nich (kromě 4. kapitoly) jsou uvedeny řešené příklady, které jsou modifikací úloh z uvedené literatury, nebo jsou úlohami vytvořenými autorem práce. Dalším vlastním přínosem práce je vlastní popis univerzálního postupu k řešení soustav diofantovských rovnic vyšších řádů na základě znalosti řešení jednotlivých rovnic dané soustavy.

Problematika diofantovských rovnic a jejich soustav je součást oblasti matematiky s názvem teorie čísel, která se neustále rozvíjí a přichází s novými poznatky v této oblasti.

Celá práce je koncipována tak, aby jejímu obsahu porozuměli mj. i žáci středních škol a mohli využít získané znalosti z této oblasti při řešení typových úloh v nadstandardních partiích školské matematiky, popř. v různých středoškolských matematických soutěžích.

Literatura

[1] Andreescu, T., Andrica, D.: *An Introduction to Diophantine Equations*. USA, 2002.

[2] Andreescu, T., Andrica, D.: *Number Theory* (*Structures, Examples and Problems*). USA, 2009.

[3] Apfelbeck, A.: *Kongruence*. ÚV MO v nakladatelství Mladá fronta, Praha, 1968.

[4] Botur, M.: *Úvod do aritmetiky*. VUP, Olomouc, 2011.

[5] Botková, P.: *Metoda nekonečného klesání při řešení diofantických rovnic*. Diplomová práce, Olomouc, 2009.

[6] Bulant, M.: *Algebra 2 - Teorie čísel* [online], [cit. 2017-04-11]. Dostupné na http://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-screen.pdf.

[7] Dodova, B.: *Desátý Hilbertův problém*. Bakalářská práce, Praha, 2009.

[8] Erban, R.: *Velká Fermatova věta* [online], [cit. 2017-04-11]. Dostupné na https://mks.mff.cuni.cz/library/VelkaFermatovaVetaRE/VelkaFermatovaVetaRE.pdf.

[9] Halaš, R.: *Teorie čísel*. VUP, Olomouc, 2014, 2.vydání.

[10] Kučera, R., Herman, J., Šimša, J.: *Metody řešení matematických úloh* I. Masarykova univerzita, Brno, 2011, 3.vydání.

[11] Kučera, R., Herman, J., Šimša, J.: *Metody řešení matematických úloh* II. Masarykova univerzita, Brno, 1991.

[12] Laurichová, I.: *Elementární teorie čísel v matematické olympiádě*. Diplomová práce, Hradec Králové, 2015.

[13] Marshall, D. C., Odell, E., Starbird, M.: *Number Theory Through Inquiry*. The Mathematical Association of America, USA, 2007.

[14] Matematická olympiáda [online], [cit. 2017-04-11]. Dostupné na http://www.matematickaolympiada.cz/.

[15] Riemel, T.: *Dělitelnost v oboru celých čísel na středních školách*. Bakalářská práce, Olomouc, 2015.

[16] Švrček, J.: *Gradované řetězce úloh v práci s matematickými talenty*. VUP, Olomouc, 2014.

[17] Švrček, J.: *Soustavy rovnic a metody jejich řešení*. Olomouc, 2016.

[18] Švrček, J., et. al: 4! *Years of Problems from Mathematical Duel*. World Scientific, Singapore – New York, v tisku.

[19] Veselý, F.: *O dělitelnosti čísel celých*. ÚV MO v nakladatelství Mladá fronta, Praha, 1966.