čísla. Není se čemu divit, vždyť v mnoha praktických úlohách, vedoucích k rovnicím, nemusí mít neceločíselná řešení rozumnou interpretaci. (Jde například o úlohu, jak pomocí pětilitrové a sedmilitrové nádoby odměřit do třetí nádoby osm litrů vody, která vede na rovnici $5x + 7y = 8$.) Na Diofantovu počest se rovnice, ve kterých hledáme jen celočíselná řešení, nazývají diofantické.

Pro řešení těchto rovnic bohužel neexistuje žádná univerzální metoda. Dokonce neexistuje ani metoda (jinými slovy algoritmus), která by určila, jestli má obecná polynomiální diofantická rovnice řešení. Tato otázka je známá pod názvem *10. Hilbertův problém* a důkaz neexistence algoritmu podal Юрий Матиясевич (Yuri Matiasevič) v roce 1970 (viz elementárně psaný text [**1**]).

Přesto však uvedeme několik nejobvyklejších metod, které v řadě konkrétních případů povedou k výsledku.

6.1. Lineární diofantické rovnice.

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{30}$$

kde $x_1, \ldots, x_n$ jsou neznámé, $a_1, \ldots, a_n, b$ daná celá čísla. Budeme předpokládat, že $a_i \neq 0$ pro každé $i = 1, \ldots, n$ (je-li $a_i = 0$, pak neznámá x_i z rovnice „zmizí“). K řešení těchto rovnic je možné užít kongruencí. Nejprve si všimněme, kdy má rovnice (30) řešení. Jestliže číslo b není dělitelné číslem $d = (a_1, \ldots, a_n)$, nemůže mít (30) žádné řešení, protože pro libovolná celá čísla $x_1, \ldots, x_n$ je levá strana (30) dělitelná číslem d. Jestliže naopak $d \mid b$, můžeme celou rovnici (30) vydělit číslem d. Dostaneme tak ekvivalentní rovnici

$$a'_1x_1 + a'_2x_2 + \cdots + a'_nx_n = b',$$

kde $a'_i = a_i/d$ pro $i = 1, \ldots, n$ a $b' = b/d$. Přitom platí

$$d \cdot (a'_1, \ldots, a'_n) = (da'_1, \ldots, da'_n) = (a_1, \ldots, a_n) = d,$$

a tedy $(a'_1, \ldots, a'_n) = 1$. V následující větě ukážeme, že taková rovnice má vždy řešení, a proto naše úvahy můžeme shrnout takto: rovnice (30) má celočíselné řešení, právě když číslo b je dělitelné největším společným dělitelem čísel $a_1, a_2, \ldots, a_n$.

$(a_1, \ldots, a_n) \mid b$

Platí i pro $n=1$, v tom případě $(a_1) = |a_1| = 1$, tj. $a_1 = \pm 1$.

Věta 39. *Nechť $n \geq 2$. Rovnice*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{31}$$

kde $a_1, a_2, \ldots, a_n, b$ jsou celá čísla taková, že $(a_1, \ldots, a_n) = 1$, má vždy celočíselné řešení. Všechna celočíselná řešení této rovnice je možné popsat pomocí $n - 1$ celočíselných parametrů.

Důkaz. Provedeme indukcí vzhledem k počtu n neznámých x_i v rovnici (31).

Je výhodné formálně začít s případem $n = 1$, kdy podmínka $(a_1) = 1$ znamená, že $a_1 = \pm 1$. Tehdy rovnice (31) má tvar buď $x_1 = b$,

nebo $-x_1 = b$, a tedy jediné řešení, které zřejmě nezávisí na žádném parametru, což odpovídá tomu, že $n - 1 = 0$.

IK: Předpokládejme, že $n \geq 2$ a že věta platí pro rovnice o $n-1$ neznámých; dokážeme ji pro rovnici (31) o n neznámých. Označme $d = (a_1, \ldots, a_{n-1})$. Pak libovolné řešení $x_1, \ldots, x_n$ rovnice (31) triviálně splňuje kongruenci

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv b \pmod{d}.$$

Vzhledem k tomu, že d je společný dělitel čísel $a_1, \ldots, a_{n-1}$, je tato kongruence tvaru

$$a_n x_n \equiv b \pmod{d}.$$

Protože platí, že $(d, a_n) = (a_1, \ldots, a_{n-1}, a_n) = 1$, má podle věty 21 tato kongruence řešení

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

kde c je vhodné celé číslo, neboli $x_n = c + d \cdot t$, kde $t \in \mathbb{Z}$ je libovolné. Dosazením do (31) a úpravou dostaneme

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} = b - a_n c - a_n d t.$$

Protože $a_n c \equiv b \pmod{d}$, je číslo $(b - a_n c)/d$ celé a poslední rovnici můžeme vydělit číslem d. Dostaneme pak rovnici

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

kde $a'_i = a_i/d$ pro $i = 1, \ldots, n-1$ a $b' = ((b - a_n c)/d) - a_n t$. Protože

$$(a'_1, \ldots, a'_{n-1}) = (d a'_1, \ldots, d a'_{n-1}) \cdot \tfrac{1}{d} = (a_1, \ldots, a_{n-1}) \cdot \tfrac{1}{d} = 1,$$

podle indukčního předpokladu má tato rovnice pro libovolné $t \in \mathbb{Z}$ řešení popsatelné pomocí $n-2$ celočíselných parametrů. Přidáme-li k tomuto řešení podmínku $x_n = c + dt$, dostaneme řešení rovnice (31) popsané pomocí $n-2$ původních parametrů a nového parametru t. Důkaz indukcí je hotov. □

Metodu z důkazu věty 39 použijeme na řešení následujících diofantických rovnic, v nichž z důvodů přehlednosti zápisu budeme neznámé značit $x, y, z, \ldots$ místo $x_1, x_2, x_3, \ldots$.

PŘÍKLAD. $5x + 7y = 8$.

ŘEŠENÍ. Libovolné řešení této rovnice musí splňovat kongruenci

$$5x + 7y \equiv 8 \pmod{5},$$

tedy $2y \equiv -2 \pmod{5}$), odkud $y \equiv -1 \pmod{5}$), tj. $y = -1 + 5t$ pro $t \in \mathbb{Z}$. Dosazením do dané rovnice dostaneme

$$5x + 7(-1 + 5t) = 8,$$

odkud vypočítáme $x = 3 - 7t$. Řešením naší rovnice je tedy

$$x = 3 - 7t, \quad y = -1 + 5t,$$

kde t je libovolné celé číslo. □

PŘÍKLAD. $91x - 28y = 35$.

ŘEŠENÍ. Protože $(91, 28) = 7$ a $7 \mid 35$, má rovnice celočíselné řešení. Vydělme ji sedmi:

$$13x - 4y = 5.$$

Libovolné řešení této rovnice musí splňovat kongruenci

$$13x - 4y \equiv 5 \pmod{13},$$

tj. $-4y \equiv -8 \pmod{13}$, odkud $y \equiv 2 \pmod{13}$ a $y = 2 + 13t$ pro $t \in \mathbb{Z}$. Dosazením

$$13x - 4(2 + 13t) = 5,$$

odkud vypočteme $x = 1+4t$. Řešením je tedy $x = 1+4t$, $y = 2+13t$, kde t je libovolné celé číslo. Tentýž výsledek bychom samozřejmě dostali, i kdybychom uvažovali kongruenci podle modulu 4 místo 13. Protože řešit kongruenci podle menšího modulu bývá snadnější, je vhodné na to pamatovat a uspořádat si výpočet tak, aby nebylo nutné pracovat s kongruencemi podle velkých modulů. □

PŘÍKLAD. $18x + 20y + 15z = 1$. $x, y, z \in \mathbb{Z}$

ŘEŠENÍ. Protože $(18, 20, 15) = 1$, má rovnice celočíselné řešení. Libovolné řešení musí splňovat kongruenci (za modul volíme největší společný dělitel čísel 18, 20)

$$18x + 20y + 15z \equiv 1 \pmod{2},$$

tedy $z \equiv 1 \pmod{2}$, odkud $z = 1 + 2s$, kde $s \in \mathbb{Z}$. Dosazením

$$18x + 20y + 15(1 + 2s) = 1$$

odkud po vydělení dvěma a úpravě dostaneme rovnici,

$$9x + 10y = -7 - 15s$$

kterou budeme řešit pro libovolné $s \in \mathbb{Z}$. Je-li tato rovnice splněna, musí platit

$$9x + 10y \equiv -7 - 15s \pmod{9},$$

odkud $y \equiv 2+3s \pmod{9}$, a proto $y = 2+3s+9t$, kde $t \in \mathbb{Z}$. Dosazením

$$9x + 10(2 + 3s + 9t) = -7 - 15s,$$

odkud po úpravě $x = -3 - 5s - 10t$. Řešení dané rovnice jsou tedy trojice

$$\begin{aligned} x &= -3 - 5s - 10t \\ y &= 2 + 3s + 9t \\ z &= 1 + 2s \end{aligned}$$

kde s, t jsou libovolná celá čísla. □

PŘÍKLAD. $15x - 12y + 48z - 51u = 1$.

ŘEŠENÍ. Protože $(15, 12, 48, 51) = 3$ není dělitel čísla 1, nemá rovnice celočíselné řešení. □

6.2. Diofantické rovnice lineární vzhledem k některé neznámé. Jde o rovnice, které můžeme upravit do tvaru

$$mx_n = F(x_1, \dots, x_{n-1}), \tag{32}$$

kde m je přirozené číslo a $F(x_1, \dots, x_{n-1})$ mnohočlen s celočíselnými koeficienty. Je zřejmé, že má-li být $x_1, x_2, \dots, x_n$ celočíselným řešením rovnice (32), musí platit

$$F(x_1, \dots, x_{n-1}) \equiv 0 \pmod{m}. \tag{33}$$

Naopak, je-li $x_1, \dots, x_{n-1}$ řešení kongruence (33), pak pro $x_n = F(x_1, \dots, x_{n-1})/m$ dostaneme celočíselné řešení $x_1, \dots, x_{n-1}, x_n$ rovnice (32). Proto pro řešení rovnice (32) postačí vyřešit kongruenci (33). V případě $n = 2$, tj. v případě, kdy je mnohočlen $F(x_1)$ mnohočlenem jedné proměnné, jde o úlohu, kterou jsme se zabývali v části 4. Případ $n > 2$ je však možné řešit zcela analogicky pomocí následující věty.

VĚTA 40. *Pro libovolný mnohočlen $F(x_1, \dots, x_s)$ s celočíselnými koeficienty, přirozené číslo m a celá čísla $a_1, \dots, a_s$, $b_1, \dots, b_s$ taková, že $a_1 \equiv b_1 \pmod{m}$, $\dots$, $a_s \equiv b_s \pmod{m}$, platí $F(a_1, \dots, a_s) \equiv F(b_1, \dots, b_s) \pmod{m}$.*

DŮKAZ. Snadný. □

Pro nalezení všech řešení kongruence (33) tedy postačí dosazovat do mnohočlenu $F(x_1, \dots, x_{n-1})$ za $x_1, \dots, x_{n-1}$ nezávisle na sobě postupně čísla $0, 1, 2, \dots, m-1$ (tj. celkem m^{n-1}-krát). A právě tehdy, když pro čísla $a_1, \dots, a_{n-1}$ je splněna podmínka $F(a_1, \dots, a_{n-1}) \equiv 0 \pmod{m}$, dostáváme řešení kongruence (33) ve tvaru

$$x_1 = a_1 + mt_1, \ \dots, \ x_{n-1} = a_{n-1} + mt_{n-1},$$

kde $t_1, \dots, t_{n-1}$ mohou nabývat libovolných celočíselných hodnot. Tak dostaneme i řešení rovnice (32):

$$\begin{aligned} x_1 &= a_1 + mt_1, \\ &\vdots \\ x_{n-1} &= a_{n-1} + mt_{n-1}, \\ x_n &= \frac{1}{m} F(a_1 + mt_1, \dots, a_{n-1} + mt_{n-1}). \end{aligned}$$

PŘÍKLAD. Řešte diofantickou rovnici $7x^2 + 5y + 13 = 0$.

ŘEŠENÍ. Rovnici upravíme na tvar $5y = -7x^2 - 13$ a budeme řešit kongruenci

$$-7x^2 - 13 \equiv 0 \pmod{5},$$

tj. $3x^2 \equiv 3 \pmod{5}$, odkud $x^2 \equiv 1 \pmod{5}$. Dosadíme-li za x čísla 0, 1, 2, 3, 4, zjistíme, že kongruence je splněna pro čísla 1 a 4. Řešením této kongruence jsou tedy podle 4.11 právě čísla

$$x = 1 + 5t \quad \text{nebo} \quad x = 4 + 5t,$$

kde $t \in \mathbb{Z}$. Dosazením dostaneme v prvním případě

$$5y = -7(1+5t)^2 - 13 = -7 - 70t - 175t^2 - 13$$

a tedy

$$y = -4 - 14t - 35t^2,$$

ve druhém případě

$$5y = -7(4+5t)^2 - 13 = -112 - 280t - 175t^2 - 13,$$

a proto

$$y = -25 - 56t - 35t^2.$$

Řešením dané rovnice jsou tedy právě všechny dvojice čísel x, y tvaru

$x = 1+5t, y = -4-14t-35t^2$ nebo $x = 4+5t, y = -25-56t-35t^2$,

kde t je libovolné celé číslo. □

PŘÍKLAD. Řešte diofantickou rovnici $x(x+3) = 4y - 1$.

ŘEŠENÍ. Rovnici upravíme na tvar $4y = x^2 + 3x + 1$ a budeme řešit kongruenci

$$x^2 + 3x + 1 \equiv 0 \pmod 4.$$

Dosazením čísel 0, 1, 2, 3 zjistíme, že kongruenci nesplňuje žádné z nich, a tedy tato kongruence nemá řešení. Řešení proto nemá ani daná rovnice. □

PŘÍKLAD. Řešte diofantickou rovnici $x^2 + 4z^2 + 6x + 7y + 8z = 1$.

ŘEŠENÍ. Rovnici upravíme na tvar

$$7y = -x^2 - 6x - 4z^2 - 8z + 1$$

a doplníme na čtverce

$$7y = -(x+3)^2 - (2z+2)^2 + 14.$$

Proto budeme řešit kongruenci

$$(x+3)^2 + (2z+2)^2 \equiv 0 \pmod 7 \qquad (34)$$

Nyní bychom mohli za uspořádanou dvojici $(x; z)$ postupně dosazovat uspořádané dvojice $(0;0), (0;1), \ldots, (0;6), (1;0), (1;1), \ldots, (6;5), (6;6)$ a spočítat pro všech 49 hodnot výraz stojící na levé straně kongruence (34). Výhodnější ale bude využít tvaru kongruence (34) a odvolat se na tvrzení 3.1, odkud pro $p = 7$, $a = x+3$, $b = 2z+2$ dostaneme, že z kongruence (34) plyne

$$x + 3 \equiv 2z + 2 \equiv 0 \pmod 7,$$

a tedy všechna řešení kongruence (34) jsou tvaru

$$x = -3 + 7t, \quad z = -1 + 7s,$$

kde t, s jsou celá čísla. Dosazením do rovnice dostaneme

$$7y = -(x+3)^2 - (2z+2)^2 + 14 = -49t^2 - 196s^2 + 14,$$

odkud

$$y = -7t^2 - 28s^2 + 2.$$

Řešením dané rovnice jsou tedy právě všechny trojice čísel x, y, z tvaru

$$x = -3 + 7t, \quad y = -7t^2 - 28s^2 + 2, \quad z = -1 + 7s,$$

kde s, t jsou libovolná celá čísla. □

6.3. Rovnice jiného tvaru. Metodu, kterou jsme řešili předchozí příklady, je možno popsat také takto: „vyjádři některou z neznámých pomocí ostatních a zkoumej, kdy je celočíselná“. Skutečně, vyjádříme-li z rovnice (32) neznámou x_n, dostaneme

$$x_n = \frac{F(x_1, \ldots, x_{n-1})}{m},$$

což je celé číslo, právě když $m \mid F(x_1, \ldots, x_{n-1})$, tj. právě když je splněna kongruence (33). Ukážeme si na příkladech, že tento postup je použitelný i na rovnice, které nejsou tvaru (32). V příkladech uvedeme i případ, kdy je vhodné vyjádřit namísto některé neznámé nějaký jiný vhodný výraz a zkoumat, za jakých okolností bude celočíselný.

Příklad. Řešte diofantickou rovnici $3^x = 4y + 5$.

Řešení. Vyjádřeme z této rovnice neznámou y:

$$y = \frac{1}{4}(3^x - 5).$$

Je-li $x < 0$, je $0 < 3^x < 1$, a tedy $\frac{1}{4}(3^x - 5) \notin \mathbb{Z}$. Pro $x \geq 0$ platí

$$3^x - 5 \equiv (-1)^x - 1 \pmod 4;$$

číslo $(-1)^x - 1$ je kongruentní s nulou podle modulu 4 právě tehdy, když x je sudé, tj. $x = 2k$, kde $k \in \mathbb{N}_0$. Řešením této diofantické rovnice jsou tedy právě všechny dvojice

$$x = 2k, \qquad y = \frac{9^k - 5}{4},$$

kde $k \in \mathbb{N}_0$ je libovolné. □

Příklad. Řešte v $\mathbb{Z}$ rovnici $x(y+1)^2 = 243y$.

Řešení. Vyjádřeme neznámou x:

$$x = \frac{243y}{(y+1)^2}.$$

Aby $x \in \mathbb{Z}$, musí $(y+1)^2$ být dělitelem čísla $243y$. Protože y a $y+1$ jsou nesoudělná čísla pro libovolné $y \in \mathbb{Z}$, musí být $(y+1)^2$ dělitelem čísla $243 = 3^5$. Toto číslo má však jen tři dělitele, kteří jsou druhou mocninou celého čísla: 1,9 a 81. Proto musí nastat některá z těchto

možností: $y+1=\pm1$, $y+1=\pm3$ nebo $y+1=\pm9$. Dostáváme tedy šest řešení dané rovnice:

$$\begin{aligned} y&=0, & x&=0,\\ y&=-2, & x&=-2\cdot 243=-486,\\ y&=2, & x&=2\cdot 27=54,\\ y&=-4, & x&=-4\cdot 27=-108,\\ y&=8, & x&=8\cdot 3=24,\\ y&=-10, & x&=-10\cdot 3=-30. \end{aligned}$$

Jiná řešení daná diofantická rovnice nemá. □

PŘÍKLAD. Řešte v $\mathbb{Z}$ rovnici $\sqrt{x}+\sqrt{y}=\sqrt{1988}$.

ŘEŠENÍ. Odečteme-li od obou stran rovnice $\sqrt{y}$ a umocníme-li na druhou, dostaneme

$$x=1988-4\sqrt{7\cdot 71\cdot y}+y.$$

Jsou-li x, y celá čísla, je i $4\sqrt{7\cdot 71y}$ celé číslo, a tedy $\sqrt{7\cdot 71y}$ je racionální číslo. Pak je $\sqrt{7\cdot 71y}=k$ nezáporné celé číslo. Platí tedy $7\cdot 71y=k^2$, odkud plyne, že k^2 a tedy i k je dělitelné prvočísly 7, 71. Je tedy $k=7\cdot 71t$ pro vhodné $t\in\mathbb{N}_0$ a tedy

$$y=\frac{k^2}{7\cdot 71}=497t^2.$$

Zcela analogicky je možné odvodit, že existuje $s\in\mathbb{N}_0$ tak, že

$$x=497s^2.$$

Dosazením do původní rovnice dostáváme

$$\sqrt{497}s+\sqrt{497}t=\sqrt{1988},$$

odkud po vydělení plyne $s+t=2$. Jsou tedy tři možnosti: $s=0$, $t=2$ nebo $s=t=1$ nebo $s=2$, $t=0$, takže daná diofantická rovnice má tři řešení:

$x=0,\quad y=1988$ nebo $x=y=497$ nebo $x=1988,\quad y=0.$

□

6.4. Řešení diofantických rovnic pomocí nerovností. Tato metoda je založena na tom, že pro libovolná reálná čísla a, b existuje jen konečně mnoho celých čísel x tak, že $a<x<b$. Proto při řešení dané rovnice hledáme taková čísla a, b, aby nerovnosti $a<x<b$ pro některou neznámou x byly důsledkem této rovnice. Konečně mnoho celých čísel ležících mezi čísly a, b pak můžeme jedno po druhém dosadit do rovnice za x a tím ji zjednodušit. Ukažme si to na následujících příkladech.

PŘÍKLAD. Řešte diofantickou rovnici $6x^2+5y^2=74$.

ŘEŠENÍ. Protože pro libovolné $y \in \mathbb{Z}$ platí $5y^2 \geq 0$, musí libovolné řešení x, y dané rovnice splňovat

$$74 = 6x^2 + 5y^2 \geq 6x^2,$$

odkud $x^2 < \frac{37}{3}$, tedy $-3 \leq x \leq 3$, proto x^2 je některé z čísel 0, 1, 4, 9. Dosazením do rovnice postupně dostáváme $5y^2 = 74$, $5y^2 = 68$, $5y^2 = 50$, $5y^2 = 20$. První tři případy jsou ve sporu s $y \in \mathbb{Z}$, z posledního dostáváme $y^2 = 4$, tj. $y = \pm 2$. Rovnice má tedy čtyři řešení: $x = 3$, $y = 2$; $x = 3$, $y = -2$; $x = -3$, $y = 2$; $x = -3$, $y = -2$. □

PŘÍKLAD. Řešte v $\mathbb{Z}$ rovnici $x^2 + xy + y^2 = x^2y^2$.

ŘEŠENÍ. Protože jsou v dané rovnici neznámé x, y zastoupeny symetricky, můžeme předpokládat, že $x^2 \leq y^2$, odkud plyne $xy \leq y^2$, a tedy

$$x^2y^2 = x^2 + xy + y^2 \leq y^2 + y^2 + y^2 = 3y^2.$$

Platí tedy $y = 0$ nebo $x^2 \leq 3$. Dosazením do rovnice dostáváme v prvním případě $x = 0$, ve druhém pro $x = 0$ opět $y = 0$, pro $x = 1$ je $y = -1$ a pro $x = -1$ je $y = 1$. Rovnice má tedy tři řešení:

$$x = 0, \quad y = 0; \qquad x = 1, \quad y = -1; \qquad x = -1, \quad y = 1.$$

□

PŘÍKLAD. Řešte v $\mathbb{Z}$ rovnici $2^x = 1 + 3^y$.

ŘEŠENÍ. Je-li $y < 0$, platí $1 < 1 + 3^y < 2$, odkud $0 < x < 1$, což je spor. Je tedy $y \geq 0$ a proto $2^x = 1 + 3^y \geq 2$, odkud $x \geq 1$. Ukážeme, že také platí $x \leq 2$. Kdyby totiž bylo $x \geq 3$, platilo by

$$1 + 3^y = 2^x \equiv 0 \pmod 8,$$

odkud bychom dostali

$$3^y \equiv -1 \pmod 8,$$

což však není možné, neboť pro sudá čísla y je $3^y \equiv 1 \pmod 8$ a pro lichá čísla y platí $3^y \equiv 3 \pmod 8$. Zbývá tedy vyřešit případ $1 \leq x \leq 2$. Pro $x = 1$ dostáváme

$$3^y = 2^1 - 1 = 1,$$

a tedy $y = 0$. Z $x = 2$ plyne

$$3^y = 2^2 - 1 = 3,$$

takže $y = 1$. Rovnice má tedy dvě řešení: $x = 1$, $y = 0$ a $x = 2$, $y = 1$. □

PŘÍKLAD. Řešte rovnici $x + y + z = xyz$ v oboru přirozených čísel.

ŘEŠENÍ. Protože jsou v dané rovnici neznámé zastoupeny symetricky, můžeme předpokládat $x \leq y \leq z$. Pak ale

$$xyz = x + y + z \leq z + z + z = 3z,$$

odkud $xy \leq 3$. Je tedy $xy = 1$, nebo $xy = 2$, nebo $xy = 3$.

Je-li $xy = 1$, platí $x = 1$, $y = 1$, odkud dostaneme dosazením do rovnice $2 + z = z$, což není možné.

Je-li $xy = 2$, platí $x = 1$, $y = 2$ (předpokládáme $x \leq y$), odkud $3 + z = 2z$, a tedy $z = 3$.

Je-li $xy = 3$, platí $x = 1$, $y = 3$, odkud $4 + z = 3z$, tedy $z = 2$, což je ve sporu s předpokladem $y \leq z$.

Rovnice má tedy jediné řešení $x = 1$, $y = 2$, $z = 3$ splňující $x \leq y \leq z$. Všechna řešení v oboru přirozených čísel dostaneme všemi záměnami pořadí čísel 1, 2, 3:

$$(x; y; z) \in \{(1; 2; 3), (1; 3; 2), (2; 1; 3), (2; 3; 1), (3; 1; 2), (3; 2; 1)\}.$$

□

Často je možné s výhodou ukázat sporem, že množina hodnot neznámé x je konečná a omezená nerovnostmi $a < x < b$; přitom z předpokladu $x \leq a$ (resp. $x \geq b$) odvodíme nepravdivé tvrzení. V následujících příkladech bude takovým nepravdivým tvrzením dvojice nerovností

$$c^n < d^n < (c + 1)^n,$$

kde c, d jsou celá a n přirozené číslo.

Příklad. Řešte diofantickou rovnici $x(x + 1)(x + 7)(x + 8) = y^2$.

Řešení. Úpravou

$$y^2 = (x^2 + 8x)(x^2 + 8x + 7).$$

Označíme-li $x^2 + 8x = z$, je naše rovnice tvaru

$$y^2 = z^2 + 7z.$$

Ukážeme, že $z \leq 9$. Předpokládejme naopak $z > 9$. Pak platí

$$(z + 3)^2 = z^2 + 6z + 9 < z^2 + 7z = y^2 < z^2 + 8z + 16 = (z + 4)^2,$$

což je spor, neboť $z + 3$, y, $z + 4$ jsou celá čísla a z těchto nerovností by plynulo

$$|z + 3| < |y| < |z + 4|.$$

Je tedy $z \leq 9$, tj. $x^2 + 8x \leq 9$, odkud

$$(x + 4)^2 = x^2 + 8x + 16 \leq 25,$$

a proto $-5 \leq x + 4 \leq 5$, neboli $-9 \leq x \leq 1$. Dosazením těchto hodnot do rovnice dostaneme všechna řešení: $(x; y) \in \{(-9; 12), (-9; -12), (-8; 0), (-7; 0), (-4; 12), (-4; -12), (-1; 0), (0; 0), (1; 12), (1; -12)\}$.

□

Příklad. Řešte diofantickou rovnici $(x + 2)^4 - x^4 = y^3$.

Řešení. Úpravou získáme

$$y^3 = 8x^3 + 24x^2 + 32x + 16 = 8(x^3 + 3x^2 + 4x + 2),$$

odkud plyne, že y je sudé. Položme $y = 2z$, $z \in \mathbb{Z}$. Platí tedy

$$z^3 = x^3 + 3x^2 + 4x + 2.$$

Je-li $x \geq 0$, platí

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 < x^3 + 3x^2 + 4x + 2 = \\ = z^3 < x^3 + 6x^2 + 12x + 8 = (x+2)^3,$$

odkud $x + 1 < z < x + 2$, což není možné. Daná rovnice tedy nemá řešení $x, y \in \mathbb{Z}$ takové, že $x \geq 0$. Předpokládejme, že má nějaké řešení $x_1, y_1 \in \mathbb{Z}$ takové, že $x_1 \leq -2$. Pak platí

$$(x_1 + 2)^4 - x_1^4 = y_1^3$$

a dosadíme-li $x_2 = -x_1 - 2$, $y_2 = -y_1$, dostaneme

$$x_2^4 - (x_2 + 2)^4 = -y_2^3,$$

a proto x_2, y_2 je také řešení dané rovnice. Ovšem $x_2 = -x_1 - 2 \geq 0$ a z předchozích úvah plyne, že tato situace nastat nemůže. Dohromady tedy $-2 < x < 0$, tj. $x = -1$. Pro $x = -1$ vychází z původní rovnice $y = 0$; dvojice $x = -1$, $y = 0$ je jediným řešením úlohy. □

6.4.1. *Některé nerovnosti.* Při řešení diofantických rovnic jsou někdy užitečné i některé složitější postupy a nerovnosti. Uveďme si některé z nejčastěji používaných.

VĚTA 41 (AG-nerovnost). *Pro libovolná čísla $a_1, a_2, \ldots, a_n \in \mathbb{R}_0^+$ platí nerovnost*

$$\sqrt{\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n}} \geq \frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n}, \tag{35}$$

přitom rovnost v (35) nastane, jen když $a_1 = a_2 = \cdots = a_n$.

DŮKAZ. *Prozatím neuveden.* □

VĚTA 42 (Bernoulliova nerovnost). *$\forall x \in \mathbb{R}, x \geq -1, \forall n \in \mathbb{N}$ platí:*

$$(1 + x)^n \geq 1 + n \cdot x.$$

DŮKAZ. Pro $n = 1$ nebo $x = 0$ je tvrzení zřejmé. Pro reálná $A > B \geq 0$ a přirozené číslo $n \geq 2$ platí:

$$n(A - B)B^{n-1} < A^n - B^n < n(A - B)A^{n-1} \quad (A > B \geq 0,\ n \geq 2),$$

z čehož po dosazení $A = 1 + x$ a $B = 1$ (pro $x > 0$), resp. $A = 1$, $B = 1 + x$ (pro $-1 \leq x < 0$) dostaneme požadované tvrzení. □

PŘÍKLAD. V oboru přirozených čísel řešte rovnici

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3.$$

Řešení. Podíl přirozených čísel je číslo kladné, a proto můžeme pro čísla $\frac{x}{y}$, $\frac{y}{z}$ a $\frac{z}{x}$ použít nerovnost mezi aritmetickým a geometrickým průměrem (viz Věta 41). Geometrický průměr těchto tří čísel je 1, a proto pro jejich aritmetický průměr platí

$$\frac{1}{3}\left(\frac{x}{y}+\frac{y}{z}+\frac{z}{x}\right) \geq 1,$$

kde rovnost nastane právě tehdy, když

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

Porovnáme-li získanou nerovnost s danou rovnicí, dostáváme, že rovnice má nekonečně mnoho řešení $x=y=z$, kde z je libovolné přirozené číslo, a žádné jiné řešení nemá. □

Příklad. Dokažte, že pro libovolné přirozené číslo $n>2$ rovnice

$$x^n+(x+1)^n=(x+2)^n$$

nemá řešení v oboru přirozených čísel.

Řešení. Předpokládejme naopak, že pro nějaká přirozená čísla x, n, kde $n>2$, je daná rovnice splněna, a označme $y=x+1\geq 2$. Pak platí

$$(y-1)^n+y^n=(y+1)^n, \tag{36}$$

odkud dostáváme

$$0=(y+1)^n-y^n-(y-1)^n\equiv 1-(-1)^n \pmod{y}.$$

Připusťme, že n je liché, pak $0\equiv 2 \pmod{y}$, tedy $y=2$ a

$$0=3^n-2^n-1,$$

což platí pouze pro $n=1$. Je tedy n sudé a podle binomické věty platí

$$\begin{aligned}(y+1)^n &\equiv \tbinom{n}{2}y^2+\tbinom{n}{1}y+1 \pmod{y^3},\\ (y-1)^n &\equiv \tbinom{n}{2}y^2-\tbinom{n}{1}y+1 \pmod{y^3},\end{aligned}$$

odkud plyne

$$0=(y+1)^n-y^n-(y-1)^n\equiv 2ny \pmod{y^3},$$

tedy $0\equiv 2n \pmod{y^2}$, a proto $2n\geq y^2$. Vydělíme-li (36) číslem y^n, dostaneme

$$\left(1+\frac{1}{y}\right)^n=1+\left(1-\frac{1}{y}\right)^n<2.$$

Naopak podle Bernoulliovy nerovnosti (viz Věta 42) platí

$$\left(1+\frac{1}{y}\right)^n>1+\frac{n}{y}=1+\frac{2n}{2y}\geq 1+\frac{y^2}{2y}=1+\frac{y}{2}\geq 2.$$

Shrneme-li předchozí úvahy, vychází, že pro žádné přirozené číslo $n>2$ nemá daná rovnice řešení v oboru přirozených čísel.