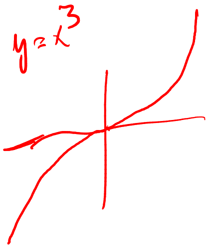
6.5. Řešení diofantických rovnic metodou rozkladu. Tato metoda spočívá v úpravě dané rovnice do tvaru

známe rozklad na prvočísla

$$A_1 \cdot A_2 \cdot \dots \cdot A_n = B, \tag{37}$$

91, nebo třeba p^3



kde $A_1, \dots, A_n$ jsou výrazy obsahující neznámé, které pro celočíselné hodnoty neznámých nabývají celočíselných hodnot, a B je číslo (případně výraz), jehož rozklad na prvočísla známe. Pak totiž existuje pouze konečně mnoho rozkladů čísla B na n celočíselných činitelů $a_1, \dots, a_n$. Vyšetříme-li pak pro každý z těchto rozkladů soustavu rovnic

$$A_1 = a_1, \quad A_2 = a_2, \quad \dots, \quad A_n = a_n,$$

získáme všechna řešení rovnice (37). Ukažme si to na příkladech.

$x, y \in \mathbb{Z}$

Příklad. Řešte diofantickou rovnici $y^3 - x^3 = 91$.

$y^3 - x^3 > 0$

$y^3 > x^3 \Leftrightarrow y > x$

$\Downarrow$

$y^2 + xy + x^2 > 0$

$91 = 7 \cdot 13$

Řešení. Rozložme levou stranu rovnice:

$$\underbrace{(y - x)}_{>0}\underbrace{(y^2 + xy + x^2)}_{>0} = 91.$$

Nemusíme uvažovat rozklady $(-1)(-91) = (-7)(-13) = \dots$

Protože

$$y^2 + xy + x^2 = \left(y + \frac{x}{2}\right)^2 + \frac{3}{4}x^2 \geq 0,$$

musí být také $y - x > 0$. Číslo 91 můžeme rozložit na součin dvou přirozených čísel čtyřmi způsoby: $91 = 1 \cdot 91 = 7 \cdot 13 = 13 \cdot 7 = 91 \cdot 1$. Budeme proto odděleně řešit čtyři systémy rovnic:

(1) $y - x = 1$, $y^2 + xy + x^2 = 91$. Dosazením $y = x + 1$ z první do druhé rovnice dostaneme $x^2 + x - 30 = 0$, odkud $x = 5$ nebo $x = -6$. Příslušné hodnoty druhé neznámé jsou pak $y = 6$, $y = -5$. [5,6] [-6,-5]

(2) $y - x = 7$, $y^2 + xy + x^2 = 13$. Pak $x^2 + 7x + 12 = 0$, tedy $x = -3$ a $y = 4$ nebo $x = -4$ a $y = 3$. $(x+3)(x+4) = 0$ [-3,4] [-4,3]

(3) $y - x = 13$, $y^2 + xy + x^2 = 7$. Nyní $x^2 + 13x + 54 = 0$. Tato rovnice však nemá řešení v oboru reálných čísel, a proto ani v oboru čísel celých.

(4) $y - x = 91$, $y^2 + xy + x^2 = 1$. V tomto případě $x^2 + 91x + 2760 = 0$. Ani tato rovnice nemá řešení v oboru reálných čísel.

Daná rovnice má tedy čtyři řešení:

$$(x; y) \in \{(5; 6), (-6; -5), (-3; 4), (-4; 3)\}.$$

□

Příklad. Řešte diofantickou rovnici $x^4 + 2x^7y - x^{14} - y^2 = 7$.

Řešení. Upravme nejprve levou stranu rovnice:

$$x^4 + 2x^7y - x^{14} - y^2 = x^4 - (x^7 - y)^2 = (x^2 - x^7 + y)(x^2 + x^7 - y)$$

a uvažme, že číslo 7 můžeme rozložit čtyřmi způsoby na součin dvou celých čísel: $7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)$. Budeme proto řešit čtyři soustavy rovnic.

(1) $x^2 - x^7 + y = 1$, $\quad x^2 + x^7 - y = 7$. Sečtením obou rovnic dostaneme $x^2 = 4$, odkud $x = 2$ a $y = 125$, nebo $x = -2$ a $y = -131$.
(2) $x^2 - x^7 + y = 7$, $\quad x^2 + x^7 - y = 1$. Nyní $x^2 = 4$, a tedy $x = 2$, $y = 131$ nebo $x = -2$, $y = -125$.
(3) $x^2 - x^7 + y = -1$, $\quad x^2 + x^7 - y = -7$. Sečtením $x^2 = -4$, což je spor.
(4) $x^2 - x^7 + y = -7$, $\quad x^2 + x^7 - y = -1$. Opět spor $x^2 = -4$.

Rovnice má tedy čtyři řešení:

$$(x; y) \in \{(-2; -131), (-2; -125), (2; 125), (2; 131)\}.$$

□

$x, y \in \mathbb{Z}$

symetrické vzhledem k x, y

Jinak (pomocí dělitelnosti)

Příklad. Řešte diofantickou rovnici

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p},$$

$x, y \neq 0$

kde p je libovolné prvočíslo.

určitě $p \mid xy \Rightarrow$

BÚNO předp. $p \mid x$,

položme $x = p \cdot x_1$, $x_1 \in \mathbb{Z}$

$x_1 y - p \cdot x_1 - y = 0$

$\Rightarrow x_1 \mid y$, $y = k \cdot x_1$, $k \in \mathbb{Z}$

$\cdot\; k \cdot x_1 - p - k = 0$

$\Rightarrow k \mid p \Rightarrow k \in \{\pm 1, \pm p\}$

Řešení. Vynásobením číslem xyp a další úpravou dostaneme

$$xy - px - py = 0.$$

$x(y-p) - py = 0$

$\cancel{x(y-p) - y(p-y) = y^2}$

$\cancel{(x+y)(y-p) = y^2}$

$x(y-p) - p(y-p) = p^2$

$(x-p)(y-p) = p^2$

Úprava do tvaru (37) vyžaduje nyní umělý obrat: přičteme k oběma stranám rovnice p^2, aby bylo možno její levou stranu zapsat jako součin:

$$(x-p)(y-p) = p^2.$$

Protože p je prvočíslo, lze p^2 rozložit na součin dvou celých čísel jen těmito šesti způsoby: $p^2 = 1 \cdot p^2 = p \cdot p = p^2 \cdot 1 = (-1) \cdot (-p^2) = (-p) \cdot (-p) = (-p^2) \cdot (-1)$. Budeme proto řešit šest systémů rovnic:

sym.
(1) $x - p = 1$, $y - p = p^2$, a tedy $x = p + 1$, $y = p^2 + p$;
(2) $x - p = p$, $y - p = p$, a tedy $x = 2p$, $y = 2p$;
(3) $x - p = p^2$, $y - p = 1$, a tedy $x = p^2 + p$, $y = p + 1$;

sym.
(4) $x - p = -1$, $y - p = -p^2$, a tedy $x = p - 1$, $y = p - p^2$;
(5) $x - p = -p$, $y - p = -p$, a tedy $x = y = 0$, což nevyhovuje;
(6) $x - p = -p^2$, $y - p = -1$, a tedy $x = p - p^2$, $y = p - 1$.

Daná rovnice má tedy pět řešení, popsaných v případech (1)-(4) a (6).

□

1) $k = 1$, $x_1 - p - 1 = 0$
$x_1 = p + 1$
$y = 1 \cdot x_1 = p + 1$
$x = p \cdot x_1 = p(p+1)$
ad (3)

2) $k = -1$, $-x_1 - p + 1 = 0$
$x_1 = -p + 1$
$y = -1 \cdot x_1 = p - 1$
$x = p \cdot x_1 = p(1-p)$
ad (6)

3) $k = p$, $p \cdot x_1 - p - p = 0$
$x_1 = 2$
$y = k \cdot x_1 = 2p$ ad (2)
$x = p \cdot x_1 = 2p$

4) $k = -p$ $\quad -px_1 - p + p = 0$
$-px_1 = 0$
$x_1 = 0$ ad 5)
$y = k \cdot x_1 = 0$, $x = p \cdot x_1 = 0$ NEVYHOVUJE

+ symetrická řešení

6.5.1. *Pythagorova rovnice.* Pythagorova rovnice se zabývá otázkou hledání všech pravoúhlých trojúhelníků s celočíselnými délkami stran.

Příklad. V oboru přirozených čísel řešte rovnici

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

$x, y, z \in \mathbb{N}$

Řešení. Označme $t = (x, y, z)$, $x_1 = \frac{x}{t}$, $y_1 = \frac{y}{t}$, $z_1 = \frac{z}{t}$. Pak platí

$$t^2 x_1^2 + t^2 y_1^2 = t^2 z_1^2,$$

odkud po vydělení číslem $t^2 \neq 0$ vychází

$$x_1^2 + y_1^2 = z_1^2 \tag{38}$$

$p | x_1, p | y_1 \Rightarrow p | x_1^2 + y_1^2 = z_1^2 \Rightarrow p | z_1$ ↯

a navíc $(x_1, y_1, z_1) = 1$. Ukážeme nyní, že čísla x_1, y_1, z_1 jsou dokonce po dvou nesoudělná: kdyby nějaké prvočíslo p dělilo dvě z čísel x_1, y_1, z_1, vyšlo by z (38), že dělí i třetí, což vzhledem k $(x_1, y_1, z_1) = 1$ není možné. Z čísel x_1, y_1 je tedy nejvýše jedno sudé. Připusťme, že jsou obě lichá. Pak z kongruence

x	± 1	± 3
$x^2 (8)$	1	1

x	0	2	4	6
$x^2 (8)$	0	4	0	4

$$z_1^2 \equiv x_1^2 + y_1^2 \equiv 1 + 1 \pmod 8$$

plyne, že z_1^2 je sudé číslo, které není dělitelné 4, což není možné. Je tedy z čísel x_1, y_1 právě jedno sudé. Protože v rovnici (38) vystupují x_1 a y_1 symetricky, můžeme pro určitost předpokládat, že sudé je $x_1 = 2r$, $r \in \mathbb{N}$. Z (38) pak plyne

$x_1 = 2r$, $r \in \mathbb{N}$

z_1, y_1 liché $\Rightarrow z_1 + y_1$ sudé, $z_1 - y_1$

$$4r^2 = z_1^2 - y_1^2$$

a tedy

$$r^2 = \frac{z_1 + y_1}{2_{\in \mathbb{N}}} \cdot \frac{z_1 - y_1}{2_{\in \mathbb{N}}}.$$

$u = \frac{z_1 + y_1}{2} \in \mathbb{N}$

$v = \frac{z_1 - y_1}{2} \in \mathbb{N}$

Označme $u = \frac{1}{2}(z_1 + y_1)$, $v = \frac{1}{2}(z_1 - y_1)$. Pak $z_1 = u + v$, $y_1 = u - v$. Protože jsou y_1, z_1 nesoudělná čísla, jsou i u, v nesoudělná čísla. Z rovnice

$(u, v) = 1$, $u > v$

$p | u, p | v \Rightarrow p | u + v = z_1$

$\Rightarrow p | u - v = y_1$

$(y_1, z_1) > 1$ ↯

$$r^2 = u \cdot v$$

pak plyne, že existují nesoudělná přirozená čísla a, b tak, že $u = a^2$, $v = b^2$, navíc vzhledem k $u > v$ platí $a > b$. Celkem tedy dostáváme

$u = a^2$, $a \in \mathbb{N}$

$v = b^2$, $b \in \mathbb{N}$

$(a, b) = 1$

$a > b$

$\Rightarrow r = a \cdot b$

$$x = tx_1 = 2tr = 2tab,$$
$$y = ty_1 = t(u - v) = t(a^2 - b^2),$$
$$z = tz_1 = t(u + v) = t(a^2 + b^2),$$

ověření:

$x^2 + y^2 =$

$(2tab)^2 + t^2(a^2 - b^2)^2 =$

$= t^2(4a^2b^2 + a^4 - 2a^2b^2 + b^4) =$

$= t^2(a^4 + 2a^2b^2 + b^4) =$

$= t^2(a^2 + b^2)^2 = z^2$

což skutečně pro libovolné $t \in \mathbb{N}$ a libovolná nesoudělná $a, b \in \mathbb{N}$ taková, že $a > b$, vyhovuje dané rovnici. Zbylá řešení bychom dostali záměnou x a y (v průběhu řešení jsme předpokládali, že právě x_1 je sudé):

Př: $a = 2, b = 1$

$x = 4, y = 2^2 - 1^2 = 3, z = 2^2 + 1^2 = 5$

$[4, 3, 5]$

$$x = t(a^2 - b^2), \quad y = 2tab, \quad z = t(a^2 + b^2),$$

kde opět $t, a, b \in \mathbb{N}$ jsou libovolná taková, že $a > b$, $(a, b) = 1$. □

$a = 3, b = 1$

$x = 6, y = 8, z = 3^2 + 1^2 = 10$

$2 \cdot [3, 4, 5]$

$a = 3, b = 2$

$x = 12, y = 3^2 - 2^2 = 5$

$z = 3^2 + 2^2 = 13$

$[12, 5, 13]$

6.6. Řešitelnost diofantických rovnic. V předchozí čáasti jsme viděli, že řešení většiny diofantických rovnic není snadné, a ačkoli jsme se naučili několik metod, v mnoha konkrétních případech se nám nepodaří diofantickou rovnici vyřešit ani jednou z nich. Přesto se nám v těchto případech může podařit něco o řešení zjistit. Například nalézt nekonečnou množinu řešení a tím dokázat, že množina všech řešení, i když ji celou neumíme popsat, je nekonečná. Nebo naopak ukázat, že množina všech řešení je prázdná (a tím vlastně danou rovnici vyřešit), popřípadě konečná.

Ukážeme neřešitelnost rovnice $x^4+y^4=z^4$ v $\mathbb{N}$
(tj. Velké Fermatovy věty pro $n=4$)

Konkrétně ukážeme dokonce neřešitelnost $x^4+y^4=z^2$
(metodou tzv. nekonečného sestupu, neboli zmenšování ad absurdum)
infinite descent

sporem: předpokládáme existenci řešení s nějakou „kladnou charakteristikou"
(např. $|z|$, $x^2+y^2+z^2$ atd.), z nich vybereme to nejmenší;
z něj odvodíme existenci řešení menšího

Předpokládejme, že ex. řešení $x^4+y^4=z^2$, kde $x,y,z\in\mathbb{N}$ a z je nejmenší možné.
Nutně $(x,y,z)=1$, dokonce (stejně jako u Pythagorovy rovnice) po 2 nesoud.

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

Podle popisu množiny řešení Pyth. rovnice je

x sudé, y liché

$$x^2=2rs,\ y^2=r^2-s^2,\ z=r^2+s^2,\ \text{kde } r,s\in\mathbb{N},\ (r,s)=1,\ r>s$$

$$\Rightarrow\ y^2+s^2=r^2,\ (y,s)=1$$

(kdyby $p|y \wedge p|s \Rightarrow p|y^2+s^2=r^2 \Rightarrow p|r$ ↯)

Podle popisu ... Pyth. r-ce:

$$s=2ab,\ y=a^2-b^2,\ r=a^2+b^2,\ \text{kde } a,b\in\mathbb{N},\ (a,b)=1,\ a>b$$

Dosadíme zpětně: $x^2=2rs=2(a^2+b^2)\cdot 2ab=4ab(a^2+b^2)$

$$\left(\frac{x}{2}\right)^2=a\cdot b\cdot(a^2+b^2),\ \text{kde } a,b,a^2+b^2 \text{ jsou po 2 nesoudél.}$$

(např. $p|a,\ p|a^2+b^2 \Rightarrow p|a^2+b^2-(a)^2=b^2\Rightarrow p|b$ ↯)

Odkud jsou a,b,a^2+b^2 druhé mocniny, tedy $\exists c,d,e\in\mathbb{N}$:

$$a=c^2,\ b=d^2,\ a^2+b^2=e^2$$

$$\Rightarrow\ c^4+d^4=e^2$$

Toto řešení je ale menší než původní, neboť

$$e\le e^2=a^2+b^2=r<r^2+s^2=z$$

To je spor s minimalitou z.

6.6.1. *Neexistence řešení.* Při důkazu, že nějaká diofantická rovnice nemá žádné řešení, je často možné s úspěchem využít kongruencí. Má-li totiž řešení diofantická rovnice $L = P$ (kde L, P jsou výrazy obsahující neznámé, nabývající celočíselných hodnot pro libovolné celočíselné hodnoty neznámých), musí mít řešení i kongruence $L \equiv P \pmod{m}$ pro libovolné $m \in \mathbb{N}$, protože řešením této kongruence je například zmíněné řešení rovnice. Odtud plyne, že nalezneme-li nějaké přirozené číslo m tak, že kongruence $L \equiv P \pmod{m}$ nemá řešení, nemůže mít řešení ani původní diofantická rovnice $L = P$. Je nutno si však uvědomit, že obrácení předchozí úvahy obecně neplatí: má-li kongruence $L \equiv P \pmod{m}$ pro každé přirozené číslo m řešení, neznamená to ještě, že má řešení též diofantická rovnice $L = P$ (ukážeme to v Příkladu na str. 84).

např. $6x^2+5x+1=0$ nemá řešení v $\mathbb{Z}$, ale je řešitelná $6x^2+5x+1\equiv 0 \pmod{m}$ $\forall m\in\mathbb{N}$.

Příklad. Řešte diofantickou rovnici

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 = 15999.$$

Řešení. Ukážeme, že kongruence

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv 15999 \pmod{16}$$

pro $2\nmid x$: $x^2\equiv 1\ (2^3)$ $\Downarrow$ $(x^2)^2\equiv 1^2\ (2^4)$

pro $2\mid x$: $x^2\equiv 0,4\ (2^3)$ $\Downarrow$ $(x^2)^2\equiv 0,4^2\ (2^4)$, $4^2 \equiv 0$

nemá řešení, odkud vyplyne, že řešení nemá ani daná diofantická rovnice. Je-li totiž celé číslo n sudé, je $n = 2k$ pro $k \in \mathbb{Z}$ a tedy $n^4 = 16k^4 \equiv 0 \pmod{16}$. Jestliže je celé číslo n liché, platí $n^4 - 1 = (n-1)(n+1)(n^2+1) \equiv 0 \pmod{16}$, neboť čísla $n-1$, $n+1$ a n^2+1 jsou sudá a jedno z čísel $n-1$, $n+1$ musí být dokonce dělitelné čtyřmi. Znamená to tedy, že podle modulu 16 je n^4 kongruentní s 0 pro sudá n a s 1 pro lichá čísla n. Je-li proto mezi čísly $x_1, x_2, \ldots, x_{14}$ právě r lichých, je

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv \overset{\in\{0,1,2,\dots,14\}}{r} \pmod{16}.$$

Platí $15999 = 16000 - 1 \equiv 15 \pmod{16}$ a protože $0 \le r \le 14$, nemůže mít kongruence

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 \equiv 15 \pmod{16}$$

řešení, a nemá ho tedy ani daná rovnice. □

Příklad. V oboru celých čísel řešte soustavu rovnic

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

Řešení. Snadno ověříme, že z $x = y = 0$ plyne také $z = u = 0$, což je řešení dané soustavy. Ukážeme, že další řešení soustava nemá. Předpokládejme, že x, y, z, u je řešení a že $x \neq 0$ nebo $y \neq 0$, a označme $d = (x, y) > 0$ největší společný dělitel čísel x, y. Z první rovnice plyne $d \mid z$, ze druhé $d \mid u$. Označíme-li $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$, $z_1 = \frac{z}{d}$, $u_1 =$

$\frac{u}{d}$, dostáváme, že $(x_1, y_1) = 1$, a po zkrácení obou rovnic číslem d^2 dostaneme

$$x_1^2 + 2y_1^2 = z_1^2,$$
$$2x_1^2 + y_1^2 = u_1^2.$$

Odtud plyne sečtením $3x_1^2 + 3y_1^2 = z_1^2 + u_1^2$ a tedy $3 \mid z_1^2 + u_1^2$. Podle Tvrzení 3.1 platí $3 \mid z_1$, $3 \mid u_1$ a tedy $9 \mid z_1^2 + u_1^2$. Pak ale $9 \mid 3(x_1^2 + y_1^2)$, a tedy $3 \mid x_1^2 + y_1^2$. Opět podle Tvrzení 3.1 platí $3 \mid x_1$, $3 \mid y_1$, což je spor s $(x_1, y_1) = 1$. Soustava má tedy jediné řešení $x = y = z = u = 0$. □

Příklad. V oboru přirozených čísel řešte rovnici

$$1! + 2! + 3! + \cdots + x! = y^2.$$

Řešení. Přímým výpočtem se přesvědčíme, že pro $x < 5$ vyhovují rovnici pouze $x = y = 1$ a $x = y = 3$. Ukážeme, že pro $x \geq 5$ rovnice řešení nemá. Protože pro libovolné $n \geq 5$ je $n!$ dělitelné pěti, platí

$$1! + 2! + 3! + \cdots + x! \equiv 1! + 2! + 3! + 4! = 33 \equiv 3 \pmod 5.$$

Ovšem druhá mocnina přirozeného čísla je podle modulu 5 kongruentní s 0 nebo 1 nebo 4. Kongruence $1! + 2! + \cdots + x! \equiv y^2 \pmod 5$ pro $x \geq 5$ tedy nemá řešení, a proto nemá pro $x \geq 5$ řešení ani daná rovnice. □

Příklad. V oboru přirozených čísel řešte rovnici

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

Řešení. Ukážeme, že daná rovnice nemá řešení. Předpokládejme naopak, že pro vhodná $x, y \in \mathbb{Z}$ platí $x^2 - y^3 = 7$. Kdyby y bylo sudé, platilo by $x^2 \equiv 7 \pmod 8$, což není možné. Je tedy y liché, $y = 2k + 1$ pro $k \in \mathbb{Z}$. Pak platí

$$x^2 + 1 = y^3 + 2^3 = (y + 2)(y^2 - 2y + 4) = \tag{39}$$
$$= (y + 2)((y - 1)^2 + 3) = (2k + 3)(4k^2 + 3). \tag{40}$$

Číslo $4k^2 + 3$ musí být dělitelné nějakým prvočíslem $p \equiv 3 \pmod 4$. V opačném případě vzhledem k tomu, že $4k^2 + 3$ je liché, by totiž v rozkladu čísla $4k^2 + 3$ na prvočísla vystupovala pouze prvočísla kongruentní s 1 podle modulu 4 a tedy by i jejich součin $4k^2 + 3$ musel být kongruentní s 1 podle modulu 4, což jistě není. Je tedy $4k^2 + 3$ dělitelné prvočíslem $p \equiv 3 \pmod 4$, a tedy platí

$$x^2 + 1 \equiv 0 \pmod p.$$

Podle Tvrzení 3.1 odtud plyne $x \equiv 1 \equiv 0 \pmod p$, a to je spor. □

Nyní uvedeme slibovaný příklad toho, že diofantická rovnice nemusí být řešitelná ani v případě, že je kongruence $L \equiv P \pmod m$ řešitelná pro libovolný modul $m \in \mathbb{N}$.

Příklad. Dokažte, že kongruence

$$6x^2 + 5x + 1 \equiv 0 \pmod{m}$$

má řešení pro každé přirozené číslo m, a přitom diofantická rovnice

$$6x^2 + 5x + 1 = 0$$

řešení nemá.

Řešení. Platí $6x^2 + 5x + 1 = (3x + 1)(2x + 1)$, a tedy rovnice $6x^2+5x+1 = 0$ nemá celočíselné řešení. Nechť m je libovolné přirozené číslo a platí $m = 2^n \cdot k$, kde $n \in \mathbb{N}_0$ a k je liché číslo. Protože $(3, 2^n) = (2, k) = 1$, mají obě kongruence soustavy

$$3x \equiv -1 \pmod{2^n}$$
$$2x \equiv -1 \pmod{k}$$

podle Věty 21 řešení, a protože $(2^n, k) = 1$, má podle Věty 23 řešení i celá soustava. Pro libovolné x vyhovující této soustavě je pak $3x + 1$ dělitelné číslem 2^n a $2x + 1$ číslem k a proto součin $(3x + 1)(2x + 1)$ je dělitelný číslem $2^n \cdot k = m$. Je tedy x řešením kongruence

$$6x^2 + 5x + 1 \equiv 0 \pmod{m}.$$

□

6.6.2. *Zmenšování ad absurdum.* Je to metoda důkazu neexistence řešení diofantické rovnice. Při důkazu touto metodou libovolné řešení dané diofantické rovnice charakterizujeme nějakým přirozeným číslem (například největším společným dělitelem hodnot některých neznámých nebo druhou mocninou hodnoty některé neznámé a podobně) a ukážeme, že existuje-li řešení charakterizované přirozeným číslem d, musí existovat jiné řešení, charakterizované přirozeným číslem $d' < d$. Pak totiž žádné takové řešení existovat nemůže, o čemž se snadno můžeme přesvědčit sporem: kdyby existovalo, mohli bychom zvolit to řešení, které je ze všech řešení charakterizováno co nejmenším přirozeným číslem d; pak by ovšem muselo existovat i jiné řešení, charakterizované přirozeným číslem $d' < d$, což však by byl spor s volbou d.

Příklad. Řešte diofantickou rovnici $x^3 + 2y^3 + 4z^3 - 6xyz = 0$. $x, y, z \in \mathbb{Z}$

Řešení. Rovnici jistě vyhovuje $x = y = z = 0$. Ukážeme, že jiné řešení rovnice nemá. Označme $d = x^2 + y^2 + z^2$ a předpokládejme, že pro nějaké řešení x, y, z dané rovnice platí $d > 0$. Z původní rovnice plyne, že x^3 je sudé číslo, a proto je $x = 2x_1$ pro vhodné $x_1 \in \mathbb{Z}$. Dosazením do rovnice dostaneme

$$8x_1^3 + 2y^3 + 4z^3 - 12x_1yz = 0,$$

po vydělení dvěma

$$4x_1^3 + y^3 + 2z^3 - 6x_1yz = 0,$$

je to skutečně menší řešení?

(y, z, x_1) (x, y, z)

$y^2 + z^2 + x_1^2 < x^2 + y^2 + z^2$

ano, pokud ověřím $x \neq 0$

a proto i y^3 je sudé číslo, tedy $y = 2y_1$ pro vhodné $y_1 \in \mathbb{Z}$. Dosazením a vydělením dvěma dostaneme

(z, x_1, y_1)

$$2x_1^3 + 4y_1^3 + z^3 - 6x_1y_1z = 0,$$

odkud plyne, že z^3 je také sudé číslo, a proto $z = 2z_1$ pro vhodné $z_1 \in \mathbb{Z}$. Dosazením a vydělením dvěma dostaneme

$$x_1^3 + 2y_1^3 + 4z_1^3 - 6x_1y_1z_1 = 0,$$

(x_1, y_1, z_1)

a tedy x_1, y_1, z_1 je řešení původní diofantické rovnice, přičemž platí

$d > 0$

$$x_1^2 + y_1^2 + z_1^2 = \frac{x^2}{4} + \frac{y^2}{4} + \frac{z^2}{4} = \frac{d}{4} < d.$$

Podle metody popsané v 6.4 daná diofantická rovnice nemá řešení s vlastností $d > 0$, a tedy $x = y = z = 0$ je jejím jediným řešením. $\square$

Příklad. V oboru přirozených čísel řešte rovnici $x^2 + y^2 = 4^z$.

Řešení. Užijeme metodu 6.6.2 pro $d = z$. Předpokládejme nejprve, že x, y, z je řešením dané rovnice. Pak jistě platí $z \neq 1$, protože je-li $x = y = 1$, platí $x^2 + y^2 = 2 < 4$, a je-li alespoň jedno z čísel x, y větší než jedna, je $x^2 + y^2 > 4$. Je tedy $z > 1$ a platí $x^2 + y^2 = 4^z \equiv 0 \pmod 8$. Protože druhá mocnina lichého čísla je kongruentní s 1 podle modulu 8 a druhá mocnina sudého čísla je kongruentní s 0 nebo 4 podle modulu 8, plyne z této kongruence, že x i y jsou sudá, a tedy $x = 2x_1$, $y = 2y_1$ pro vhodná $x_1, y_1 \in \mathbb{N}$. Pak ovšem

$$x_1^2 + y_1^2 = \frac{x^2}{4} + \frac{y^2}{4} = 4^{z-1},$$

a tedy, označíme-li $z_1 = z - 1 \in \mathbb{N}$, čísla x_1, y_1, z_1 splňují danou rovnici, přičemž $z_1 < z$. Proto daná rovnice nemá řešení.

Příklad. Řešte diofantickou rovnici $x^4 + y^4 + z^4 = 9u^4$.

Řešení. Je-li $u = 0$, musí být rovněž $x = y = z = 0$, což je řešení dané rovnice. Ukážeme, že jiné řešení rovnice nemá. Předpokládejme, že celá čísla x, y, z, u vyhovují dané rovnici, přičemž $u \neq 0$, a označme $d = u^4$. Kdyby číslo u nebylo dělitelné pěti, bylo by $u^4 \equiv 1 \pmod 5$ podle Fermatovy věty, a tedy by platilo

$$x^4 + y^4 + z^4 \equiv 4 \pmod 5,$$

což však není možné, neboť podle Fermatovy věty každé z čísel x^4, y^4, z^4 může být podle modulu 5 kongruentní pouze s 0 nebo 1. Je tedy u dělitelné pěti, $u = 5u_1$ pro vhodné $u_1 \in \mathbb{Z}$, a platí

$$x^4 + y^4 + z^4 \equiv 0 \pmod 5,$$

odkud plyne, že čísla x, y, z jsou dělitelné pěti, tj. $x = 5x_1$, $y = 5y_1$, $z = 5z_1$ pro vhodná $x_1, y_1, z_1 \in \mathbb{Z}$. Dosazením do rovnice a vydělením 5^4 dostaneme

$$x_1^4 + y_1^4 + z_1^4 = 9u_1^4,$$

a tedy x_1, y_1, x_1, u_1 vyhovují dané rovnici. Přitom platí

$$u_1^4 = \frac{u^4}{5^4} < u^4 = d.$$

□

Příklad. Řešte diofantickou rovnici $x^2 + y^2 + z^2 = 2xyz$.

Řešení. Rovnice jistě splňuje $x = y = z = 0$. Ukážeme, že další řešení tato rovnice nemá. Dokážeme dokonce silnější tvrzení: žádná rovnice

$$x^2 + y^2 + z^2 = 2^u xyz, \tag{41}$$

kde $x, y, z \in \mathbb{Z}$ a $u \in \mathbb{N}$ nemá jiné řešení než $x = y = z = 0$, $u \in \mathbb{N}$ libovolné. Předpokládejme, že $x, y, z \in \mathbb{Z}$, $u \in \mathbb{N}$ vyhovují rovnici (41) a že $d = x^2 + y^2 + z^2 > 0$. Protože $u \geq 1$, je $2^u xyz$ sudé číslo, a proto i $x^2 + y^2 + z^2$ je sudé číslo. To ale znamená, že právě jedno z čísel x, y, z, nebo všechna tři jsou sudá. V prvním případě je však

$$x^2 + y^2 + z^2 \equiv 1 + 1 + 0 = 2 \pmod 4,$$

kdežto

$$2^u xyz \equiv 0 \pmod 4,$$

neboť $u \geq 1$ a jedno z čísel x, y, z je sudé. Nastane tedy druhý případ a čísla $x_1 = \frac{x}{2}$, $y_1 = \frac{y}{2}$, $z_1 = \frac{z}{2}$ jsou celá. Položme $u_1 = u + 1$ a dosaďme do (41):

$$4x_1^2 + 4y_1^2 + 4z_1^2 = 2^{u_1 - 1} \cdot 2x_1 \cdot 2y_1 \cdot 2z_1,$$

po vydělení čtyřmi

$$x_1^2 + y_1^2 + z_1^2 = 2^{u_1} \cdot x_1 y_1 z_1,$$

a tedy x_1, y_1, z_1, u_1 vyhovují rovnici (41). Přitom platí $0 < x_1^2 + y_1^2 + z_1^2 = \frac{d}{4} < d$, neboť $d > 0$. Podle 6.6.2 tedy rovnice (41) může mít jen řešení s vlastností $d = 0$, což jsou výše uvedená řešení $x = y = z = 0$, $u \in \mathbb{N}$ libovolné. Speciálně, zadaná rovnice má jediné řešení $x = y = z = 0$. □

6.6.3. *Početnost množiny řešení.* V mnoha případech, kdy neumíme najít všechna řešení diofantické rovnice, se nám může alespoň podařit rozhodnout, zda řešení je konečně či nekonečně mnoho. Konečnost je například zaručena zjištěním, že hodnoty neznámých jsou v absolutní hodnotě menší než nějaké číslo. Pokud toto číslo nalezneme a je „rozumně“ malé, můžeme pak najít všechna řešení metodou popsanou v 6.4

To, že daná diofantická rovnice má řešení nekonečně mnoho, můžeme dokázat například tak, že nalezneme pro každou neznámou nějaký výraz s parametrem, a to takový, že po dosazení do rovnice dostaneme rovnost, přitom pro nekonečně mnoho hodnot parametru dostaneme navzájem různé hodnoty neznámých (jde tedy o jakousi zkoušku nekonečně mnoha řešení). Nebo můžeme nalézt jedno řešení rovnice a