

Příklad. Řešte v $\mathbb{Z}$

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

Řešení. • Uvažme řešení x, y, z zadané rovnice a označme $d = (x, y, z)$, pak jistě $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ je také řešením zadané rovnice. Můžeme tedy dále předpokládat, že máme řešení x, y, z , kde jsou tato čísla po dvou nesoudělná, vždyť společný dělitel libovolných dvou čísel bude dělit i to třetí.

- Z předchozího víme, že nejvýše jedno číslo bude sudé. Předpokládejme, že $2 \nmid x$ a $2 \nmid y$, pak $x^2 \equiv y^2 \equiv 1 \pmod{8}$. Zejména $z^2 \equiv 2 \pmod{8}$, což je ale spor. Proto bude právě jedno z čísel x, y sudé. Úloha symetrická, nechť je to x , tedy $x = 2r$.
- Přepíšeme původní rovnici jako $4r^2 = z^2 - y^2 = (z + y)(z - y)$. Položme

$$u = \frac{z + y}{2}, \quad v = \frac{z - y}{2}.$$

- Buď p prvočíslo takové, že $p \mid u, p \mid v$, pak $p \mid u + v = z$ a $p \mid u - v = y$, což je spor s nesoudělností y, z . Proto jsou nutně u, v nesoudělná.
- Víme $r^2 = \frac{z+y}{2} \cdot \frac{z-y}{2} = uv$. Z nesoudělnosti u, v vidíme, že u i v jsou druhými mocninami, tj. $u = a^2, v = b^2$, kde $(a, b) = 1$.
- Dosadíme do vztahů: $x = 2r, y = u - v, z = u + v$ a dostáváme

$$\begin{aligned} x &= 2ab, \\ y &= a^2 - b^2, \\ z &= a^2 + b^2, \end{aligned}$$

přičemž $(a, b) = 1, a, b \in \mathbb{N}$.

- Ověříme nalezená řešení tím, že dosadíme do původní rovnice:

$$x^2 + y^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = z^2.$$