Diofantické rovnice

Pozorování. Lineární diofantická rovnice

$$a_1x_1 + \cdots + a_nx_n$$

má řešení právě tehdy, když $\mathrm{NSD}(a_1, \ldots, a_n)$ dělí b.

Věta. Celá čísla x, y, z splňují $x^2 + y^2 = z^2$, právě když (až na případnou záměnu x a y) platí $x = (a^2 - b^2)c$, $y = 2abc$ a $z = (a^2 + b^2)c$, kde a, b a c jsou libovolná celá čísla.

Důkaz. Je snadné ověřit, že pro libovolnou trojici čísel a, b, c rovnost platí. Dokažme opačnou implikaci.

Číslo c volme jako největšího společného dělitele čísel x, y a z, kterého vytkneme, a můžeme dále předpokládat, že x, y a z jsou nesoudělná.

Zkoumejme vztah

$$(x + yi)(x - yi) = z^2.$$

Nechť α je nějaké Gaussovo prvočíslo dělící z. Pokud by α dělilo jak $x + yi$, tak $x - yi$, dělilo by obě čísla také $\bar{\alpha}$ a tedy i $\mathbf{N}(\alpha)$, v rozporu s nesoudělností x a y. Tedy α^2 dělí buď $x + yi$ nebo $x - yi$ pro každé Gaussovo prvočíslo v rozkladu z. (Speciálně není žádný prvočinitel ze $\mathbb{Z}$.)

Je tedy $x + yi = u(a + bi)^2$, $x - yi = \bar{u}(a - bi)^2$ a $z = a^2 + b^2$, kde $a, b \in \mathbb{Z}$ a u je invertibilní, tedy $u \in \{\pm i, \pm 1\}$. Protože $i = (-1)^2$, $-i = (-i)^2$, $-1 = i^2$ a $1 = 1^2$, máme $x + yi = (va + vbi)^2$, kde v je invertibilní a $u = v^2$. Dostáváme dvě různé možnosti:

$$\begin{cases} x = a^2 - b^2, y = 2ab & \text{pro } v = \pm 1 \\ x = -2ab, y = b^2 - a^2 & \text{pro } v = \pm i. \end{cases}$$

Uvedené možnosti odpovídají symetrii proměnných x a y, v jednom případě je y sudé a x (díky předpokladu nesoudělnosti) liché, ve druhém případě je tomu naopak. □

Věta. Třetí mocnina z^3, $z \in \mathbb{Z}$, je součtem čtverců, právě když je z nezáporné a $\mathrm{val}_p(z)$ je sudé pro každé prvočíslo $p = 4k + 3$.

Důkaz. Nechť je $x^2 + y^2 = z^3$, tedy $(x+iy)(x-iy) = z^3$. Je zřejmé, že součet čtverců nemůže být záporný. Uvažujme nějaký Gaussův prvočinitel $p \in \mathbb{Z}$, tedy $p = 4k + 3$. Pak p^j dělí $x+iy$, právě když dělí $x-iy$, a tedy $3\mathrm{val}_p(z) = \mathrm{val}_p(x+iy)+\mathrm{val}_p(x-iy) = 2\mathrm{val}_p(x + iy)$, kde valuaci chápeme v $\mathbb{Z}[i]$. Zřejmě je tedy $\mathrm{val}_p(z)$ sudé.

Pro z splňující podmínky věty stačí zvolit x a y tak, aby rozklad $x + iy$ na Gaussovy prvočinitele měl tvar

$$(x + iy) = \prod_{p=4k+3} p^{\frac{3}{2}\cdot \mathrm{val}_p(z)} \cdot \prod_{p=\alpha\bar{\alpha}=4k+1} \alpha^{3\mathrm{val}_p(z)}.$$

□

Jako speciální případ dostáváme následující větu.

Věta. Diofantická rovnice $x^2 + 1 = z^3$ má jediné řešení $(x, z) = (0, 1)$.

Důkaz. Z předchozí věty víme, že $x + i$ je tvaru $(a + bi)^3$. Tedy $1 = 3a^2b - b^3 = b(3a^2 - b^2)$. Z toho plyne $b = \pm 1$ a snadno dostaneme jedinou možnost $a = 0$, $b = -1$. □