Cvičení 26. 4. 2013

Dnes si ukážeme, jak vyzrát na vypečené diofantické rovnice pomocí algebry.

Množina Gaussových celých čísel $\mathbb{Z}[i]$ je tvořená čísly $a + bi, a, b \in \mathbb{Z}$. Je to euklidovský obor, takže máme velmi pěknou dělitelnost (existují NSD, každé číslo lze rozložit na součin prvočinitelů, platí Bézoutova věta a tak podobně).

Věta 1. Číslo $z = a + bi$ je v $\mathbb{Z}[i]$ prvočinitel, právě když je $a^2 + b^2$ prvočíslo, nebo pokud $z = \pm p, \pm ip$ pro $p \in \mathbb{N}$ prvočíslo tvaru $4k + 3$.

Příklad 1. Najděte všechny invertibilní prvky v $\mathbb{Z}[i]$.

Příklad 2. Rozhodněte, zda je prvočinitel v $\mathbb{Z}[i]$:

1. 2,
2. 3,
3. $9 + 3i$,
4. $4 + i$,
5. $5 + 3i$.

Příklad 3. Buď $x, y \in \mathbb{Z}$ řešení rovnice $x^2 + 1 = y^3$. Dokažte, že:

1. Čísla $x + i$ a $x - i$ jsou v $\mathbb{Z}[i]$ nesoudělná.
2. Výraz $x - i$ je v $\mathbb{Z}[i]$ třetí mocnina nějakého prvku.
3. Jediné x splňující, že $x + i$ je třetí mocnina v $\mathbb{Z}[i]$, je $x = 0$.

Příklad 4 (Obecná Pellova rovnice)**.** Buď $d > 0$ nečtvercové celé číslo. Označme G množinu všech kladných čísel $a + \sqrt{d}b$, že $a, b \in \mathbb{Z}$ a platí $a^2 - db^2 = 1$. Předpokládejme, že G obsahuje aspoň jeden prvek různý od 1 (tak tomu vždy je). Dokažte:

1. G s násobením zděděným z $\mathbb{R}$ tvoří grupu
2. G je nekonečná cyklická grupa