Celočíselné okruhy

Kondr

5. září 2008

Obsah

Příklad č.1

$$a^2 - 4b^2 = 1$$

- umíme řešit rozkladem
- $(a - 2b)(a + 2b) = 1$
- Obě závorky ± 1, proto $a = \pm 1, b = 0$

Příklad č.2

$$a^2 - 3b^2 = 1$$

- je to případ tzv. Pellovy rovnice
- lze uhodnout některá řešení: (2,1),(7,4),(26,15),...
- metodu rozkladu nad $\mathbb{Z}$ nelze použít
- rozklad nad $\mathbb{R}$ dává $(a - \sqrt{3}b)(a + \sqrt{3}b) = 1$
- budeme zkoumat nejmenší množinu čísel, nad nimiž lze rozklad provést

Kvadratické pole

- Nechť k je celé bezčtvercové číslo. Množinu $\mathbb{Q}[\sqrt{k}] = \{p + q\sqrt{k} | p, q \in \mathbb{Q}\}$ nazveme kvadratickým polem.
- Grupa vzhledem ke sčítání i násobení.
- Distributivita násobení.
- Definující rovnicí čísla $\frac{a+b\sqrt{k}}{c}$ je rovnice

$$c^2x^2 - 2acx + a^2 - b^2a^2k = 0.$$

- Pokud $p_1 + q_1\sqrt{k} = p_2 + q_2\sqrt{k}$, pak $p_1 = p_2$ a $q_1 = q_2$.

Celočíselný okruh I

- Kvadratickým celým číslem nazveme takový prvek $\mathbb{Q}[\sqrt{k}]$
- Pro $k \equiv 2, 3 \pmod 4$ je $\mathbb{Z}[\sqrt{k}] = \{a + b\sqrt{k} | a, b, k \in \mathbb{Z}\}$ množina kvadratických celých čísel.
- Pro $k = -1$ se jedná o Gaussova čísla.
- Pro $k \equiv 1 \pmod 4$ je $\mathbb{Z}[\frac{\sqrt{k}-1}{2}] = \{a + b\frac{\sqrt{k}-1}{2} | a, b \in \mathbb{Z}\}$, značíme
- Pro $k = -3$ se jedná o Eisensteinova čísla.
- Grupové vlastnosti vzhledem ke sčítání.
- Monoid vzhledem k násobení.
- Distributivita násobení vzhledem ke sčítání.
- Pro $k > 0$ hustá množina v $\mathbb{R}$
- Pro $k < 0$ obdélníková/trojúhelníková síť v $\mathbb{C}$

Celočíselný okruh II

- *Číslem sdruženým k* $z = a + b\sqrt{k}$ *nazveme číslo* $\bar{z} = a - b\sqrt{k}$
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$
- $\overline{z_1^n} = \overline{z_1}^n$

Celočíselný okruh III

- *Normou čísla* $z = a + b\sqrt{k}$ *nazveme číslo*

$$\|z\| = z \cdot \overline{z} = (a + b\sqrt{k})(a - b\sqrt{k}) = a^2 - kb^2$$

- $\|z_1 \cdot z_2\| = \|z_1\| \cdot \|z_2\|$
- $\|z_1^n\| = \|z_1\|^n$

Dělitelnost

- Řekneme, že z_1 *dělí* z_2, pokud existuje z takové, že $z \cdot z_1 = z_2$.
- Pokud $p \in \mathbb{Z}, p|z = a + b\sqrt{k}$, pak $p|a, p|b$.
- Pokud $p \in \mathbb{Z}, z|p, z = a + b\sqrt{k}, \gcd(a, b) = 1$, pak $\|z\| \mid p$.
- Pokud $z_1 \mid z_2$ a $z_2 \mid z_1$, řekneme, že jsou z_1 a z_2 asociované $(z_1 \approx z_2)$.
- Pokud $z_1 \mid z_2$, pak $\|z_1\| \mid \|z_2|$

Jednotky

- *Jednotkou* nazveme takové číslo z_1, že $z_1 | 1$.
- Pro jednotky platí $z_1 \overline{z_1} = \pm 1$.
- Pokud je z_1 jednotkou, je i z_1^n dělitelem jedničky pro všechna n.
- Pro $k = -1$ jednotkami čísla $1, -1, i, -i$.
- Pro $k = -3$ jednotkami čísla $1, -1, \frac{\pm 1 \pm \sqrt{-3}}{2}$.
- Pro $k < -3$ jednotkami čísla $1, -1$.
- Pro $k > 1$ existuje jednotek nekonečně mnoho.

Dirichletova věta

V kvadratickém poli existuje jedna fundamentální jednotka a všechny ostatní jednotky jsou jejími mocninami (až na sdružení).

Důkaz.

- Omezme se na jednotky, pro které $z\overline{z} = 1$ a $|z| > 1$
- Nejmenší z nich (ve smyslu uspořádání $\mathbb{R}$) označme z_1
- Pokud $|z_1|^k < |z_i| < |z_1|^{k+1}$ pro nějaké i, najdeme menší i s touto vlastností, spor.
- Jednotky splňující $z\overline{z} = 1$ a $\|z\| > 1$ jsou tvaru z_1^k
- Jednotky splňující $z\overline{z} = 1$ a $\|z\| < 1$ jsou tvaru z_1^{-k}
- Nechť $z_m\overline{z_m} = -1$. Pak $z_m^2 = z_1^k$ pro nějaké k.

Pellova rovnice

Pellovou rovnicí rozumíme diofantickou rovnici tvaru

$$x^2 - ky^2 = 1,$$

kde k není čtverec.

- $z = (x - y\sqrt{k})$ a $\overline{z} = (x - y\sqrt{k})$ musí být jednotky v $\mathbb{Z}[\sqrt{k}]$ splňující $z\overline{z} = 1$.
- Dle Dirichletovy věty existuje jednotka $z_1 = a + b\sqrt{k}$ taková, že
$$x + y\sqrt{k} = \pm(a + b\sqrt{k})^n$$
- $x = \frac{z_1^n + \overline{z_1}^n}{2}$, $x = \frac{z_1^n - \overline{z_1}^n}{2\sqrt{k}}$
- Takto nalezneme všechna řešení, můžeme je vyjádřit rekurentně

Zobecněná Pellova rovnice

Zobecněnou Pellovou rovnicí rozumíme diofantickou rovnici tvaru

$$x^2 - ky^2 = n,$$

kde k není čtverec.

- Výše popsanou metodou umíme ke každému fundamentálnímu řešení nalézt ∞ dalších
- Aby řešení existovalo, musí být rovnice řešitelná $\pmod{k}$.

Rozklady na prvočísla

- Prvočíslo je číslo p, které dělí jen čísla asociovaná s 1 a s p.
- V okruzích s $k < 0$,
  $k \notin \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ nelze čísla rozložit na prvočísla jednoznačně.
- Pro $k \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ to jde.
- Platí $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.
- Jako $\gcd(z_1, z_2)$ označme $\{z_3\}$ splňující $z_3|z_1$, $z_3|z_2$ a $z|z_1 \wedge z|z_2 \Rightarrow z|z_3$
- Platí $\gcd(z_1, z_2) = \gcd(z_1 + kz_2, z_2)$.
- V okruzích s $k = -1, -2, -3$ lze použít Euklidův algoritmus.

Základní věta aritmetiky

Tuto větu uvažujme v $Z[\sqrt{k}]$, $k \in -1, -2, -3$: **Věta.** Pokud $z_1|z_2 \cdot z_3$ a $1 \in \gcd(z_1, z_2)$, pak $z_1|z_3$. **Důkaz.**

- $z_1 z_4 = z_2 z_3$
- $z_1 z_5 - z_2 z_6 = 1$vynásobíme z_3 a dosadíme z předchozího:
- $z_1 z_3 z_5 - z_1 z_4 z_6 = z_3$
- $z_1(z_3 z_5 - z_4 z_6) = z_3$

Tuto větu lze formulovat také tak, že rozklad na prvočísla je jednoznačný.

Prvočísla II

Věta.
Každé přirozené prvočíslo je buď prvočíslem, nebo součinem dvou sdružených prvočísel.

Důkaz
Pokud $z_1 z_2 | p$, pak $\|z_1 z_2\| | p$. Proto je jedno z čísel z_1, z_2 jednotka a druhé prvočíslo.

Prvočísla III

Věta.
Pokud je $k \in \{-1, -2, -3\}$ kvadratický zbytek $\pmod p$, lze p v $\mathbb{Z}[\sqrt{k}]$ (resp. $\mathbb{Z}[\frac{\sqrt{k}+1}{2}]$) rozložit, v opačném případě je p v $\mathbb{Z}[\sqrt{k}]$ prvočíslo.

Aplikace

- Řešení rovnic typu $x^2 + 2 = y^3$
- Hledání rozkladu čísla na součet dvou čtverců