Pokroky matematiky, fyziky a astronomie

Zdeněk Pezlar

Řešení diofantických rovnic rozkladem nad číselnými tělesy

Pokroky matematiky, fyziky a astronomie, Vol. 66 (2021), No. 2, 103–117

Persistent URL: http://dml.cz/dmlcz/148980

Řešení diofantických rovnic rozkladem nad číselnými tělesy

Zdeněk Pezlar

Abstrakt. Článek představuje zjednodušené základy teorie kvadratických zbytků a algebraické teorie čísel a jejich užití při řešení diofantických rovnic. Obsahuje i několik příkladů pro čtenáře.

Pod termínem *diofantická rovnice* rozumíme rovnici nad celými čísly ve více proměnných. Mezi nejstudovanější problémy tohoto typu patří hledání pythagorejských trojic, či známá rovnice $x^n + y^n = z^n$ pro $n \geqslant 3$ figurující ve Velké Fermatově větě.

Při řešení diofantických rovnic máme hned několik cest, kterými se můžeme vydat. Můžeme se pokusit neznámé ohraničit pomocí nerovností, využít modulární aritmetiku, či rozložit rovnici na součin. Práci s mocninami v modulární aritmetice usnadňují mocninné zbytky, z nichž nejstudovanější jsou ty kvadratické. S jejich pomocí u mnoha úloh ukážeme, že nemají řešení, a zformulujeme několik důležitých tvrzení.

1. Kvadratické zbytky

Definice 1.1. O celém čísle d nesoudělném s n řekneme, že je *kvadratický zbytek* modulo n, pokud existuje celé x takové, že $x^2 \equiv d \pmod{n}$. V opačném případě d nazveme *kvadratickým nezbytkem* modulo n.

Pokud neznáme prvočíselný rozklad n, těžko popíšeme, jak vypadá jeho příslušná množina kvadratických zbytků, nicméně pro prvočísla a prvočíselné mocniny je to jednodušší. K tomu potřebujeme pro lichá prvočísla p definovat Legendrův symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{pokud } a \text{ je kvadratický zbytek modulo } p, \\ 0, & \text{pokud } p \mid a, \\ -1, & \text{pokud } a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Legendrův symbol se dá vypočítat ze vztahu $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Skutečně, pokud je a dělitelné p, pak $\left(\frac{a}{p}\right) = 0$. Pro zbylá a máme za pomoci Malé Fermatovy věty $0 \equiv a^{p-1} - 1 = (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \pmod{p}$, tudíž $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Pokud $a \equiv x^2 \not\equiv 0 \pmod{p}$, platí $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$. Dá se ukázat, že polynom stupně n má v $\mathbb{Z}_p$ nejvýše n kořenů, tedy $a^{\frac{p-1}{2}} - 1$ má v $\mathbb{Z}_p$ nejvýše $\frac{p-1}{2}$ kořenů. Každý prvek má v $\mathbb{Z}_p$ nejvýše dvě odmocniny, protože $x^2 \equiv y^2 \pmod{p}$ znamená $x \equiv \pm y \pmod{p}$. Nenulových druhých mocnin a je tak v $\mathbb{Z}_p$ právě $\frac{p-1}{2}$, přičemž všechny splňují $a^{\frac{p-1}{2}} \equiv 1$

Zdeněk Pezlar, Gymnázium Brno, třída Kapitána Jaroše 14, 602 00 Brno, e-mail: zdendapezlar@seznam.cz

(mod p); žádná jiná řešení proto kongruence nemá. Všechny kvadratické nezbytky tak musí splňovat $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Ze znalosti kvadratických zbytků pro prvočísla dokážeme poměrně snadno popsat kvadratické zbytky pro prvočíselné mocniny a následně i pro libovolné celé číslo, známe-li jeho prvočíselný rozklad.

Kvadratické zbytky mají mnoho dalších důležitých a zajímavých vlastností, platí například tzv. zákon kvadratické reciprocity a jeho doplňky. Jako obsáhlejší text zabývající se kvadratickými zbytky vřele doporučuji [4], kapitola 1 a pro důkladnější seznámení s touto teorií [1], kapitola 2. Nyní si ukážeme kvadratické zbytky v praxi.

Než se pustíme do řešení příkladů, připomeňme, že ke každému nenulovému $a \in \mathbb{Z}_p$ existuje inverzní prvek vzhledem k násobení. Čísla $a, 2a, \ldots, (p-1)a$ jsou totiž v $\mathbb{Z}_p$ navzájem různá, protože $ka \equiv \ell a$ znamená $p \mid (k-\ell)a$, tedy $k = \ell$. Speciálně existuje číslo $\frac{1}{a} \in \mathbb{Z}_p$ splňující $\frac{1}{a} \cdot a = 1$ v $\mathbb{Z}_p$. Můžeme tak pro každé celé číslo y nedělitelné p chápat podíl $\frac{x}{y} = x \cdot \frac{1}{y}$ jako prvek $\mathbb{Z}_p$.

Příklad 1.2. Mějme prvočíslo $p \equiv 3 \pmod 4$ a celá čísla a, b taková, že $p \mid a^2 + b^2$. Ukažte, že $p \mid a$ a $p \mid b$.

Řešení. Předpokládejme, že p nedělí jedno z čísel a a b, pak nedělí ani druhé. Máme dáno $a^2 \equiv -b^2 \pmod p$. Protože $p \nmid b$, můžeme celou kongruenci vynásobit $\frac{1}{b^2}$:

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p}.$$

Pak -1 je kvadratický zbytek modulo p, tj. $1 = \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Nicméně $\frac{p-1}{2}$ je liché, tedy $(-1)^{\frac{p-1}{2}} = -1$, spor. Náš předpoklad byl mylný, tudíž p dělí jedno z čísel a, b a tím pádem dělí obě. □

Příklad 1.3. Řešte v $\mathbb{Z}$ rovnici $x^2 + 4 = y^5$.

Řešení. Chtěli bychom použít kvadratické zbytky. Proto si všimneme, že prvočíslo $p = 11$ splňuje $5 = \frac{p-1}{2}$, tj. $y^5 \equiv \left(\frac{y}{11}\right) \in \{\pm 1, 0\} \pmod{11}$. Pro každou ze tří možných hodnot y^5 dopočteme $x^2 \in \{6, 7, 8\} \pmod{11}$.

Nyní ukážeme, že rovnice nemá řešení. K tomu by například stačilo, aby žádná z kongruencí $x^2 \equiv 6, 7, 8 \pmod{11}$ neměla řešení. Počítejme

$$\left(\frac{6}{11}\right) \equiv 6^5 \equiv -1 \pmod{11},$$
$$\left(\frac{7}{11}\right) \equiv 7^5 \equiv -1 \pmod{11},$$
$$\left(\frac{8}{11}\right) \equiv 8^5 \equiv -1 \pmod{11},$$

takže daná rovnice nemůže mít řešení. □

Nyní můžete zkusit využít kvadratické zbytky k řešení následující úlohy.

Cvičení 1.4. Dokažte, že rovnice $x^2 + 2 = y^9$ nemá celočíselné řešení.

Pomocí Legendrova symbolu dokážeme elegantně vyřešit mnohé úlohy, které bychom jinak řešit nemohli buď vůbec, či s obtížemi. Třeba u příkladu 1.3 jsme mohli vypsat zbytky, které dávají čísla 0^2, 1^2, 2^2, ... , 10^2, a poté zjistit, že se mezi nimi nenachází 6, 7 ani 8, nicméně při práci s většími prvočísly by to bylo příliš pracné. Místo toho nám stačilo vypočítat tři čísla a byli jsme hotovi.

Ne vždy však vystačíme s modulární aritmetikou. Pokud bychom při řešení rovnice $x^2 + 13 = y^3$ zkoušeli podobné metody, nikam bychom se nedostali, protože rovnice má řešení pro $x = 70$. Rovnice má tedy i řešení modulo každé přirozené číslo, tj. pouze zkoumáním dělitelnosti nedokážeme úlohu vyřešit. Existují však rovnice, které mají více řešení, např. rovnice $x^2 + 26 = y^3$ má řešení pro $x = 1$ i $x = 207$. Nemůžeme tak s jistotou říci, zda rovnice nemá nějaká další řešení, jehož absolutní hodnota je moc velká i na servery Wolfram Alpha. Předmětem podobných úvah byla i dlouho otevřená *Catalanova domněnka*. Chtěli bychom se tak ubírat například směrem rozkladu na součin, kdy dokážeme spolehlivě najít všechna řešení.

Vzpomeňme si na vzorec $a^2 - b^2 = (a - b)(a + b)$. Díky komplexním číslům můžeme analogicky rozložit součet druhých mocnin $a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i})$. Snadno tak rozložíme i $x^2 + 13 = (x + \sqrt{-13})(x - \sqrt{-13})$. V klasické elementární teorii čísel nepracujeme s iracionálními ani s komplexními čísly, zatímco při užití tohoto rozkladu potřebujeme oboje. Ve zbytku článku vybudujeme teorii, která nám umožní s těmito rozklady pracovat, a poté budeme schopni výše uvedenou rovnici vyřešit tímto netradičním rozkladem.

2. Číselná tělesa

Nápad, že bychom mohli s iracionálními i imaginárními čísly pracovat při řešení rovnic, sahá až ke Carlu Friedrichu Gaussovi, který byl i jedním z prvních, kdo podrobně studoval kvadratické zbytky. První větší pokroky v této takzvané *algebraické teorii čísel* přišly ve snaze dokázat Velkou Fermatovu větu, a přesto, že první správný důkaz byl veden cestou eliptických křivek, algebraický pohled přinesl mnoho nových pozorování.

Budeme studovat *algebraická čísla*, což jsou komplexní čísla, která jsou kořeny polynomů s celočíselnými koeficienty. Speciálně nás budou zajímat *celá algebraická čísla*, tedy algebraická čísla, která jsou kořeny polynomů s vedoucím koeficientem 1. Celočíselný polynom s nejnižším možným stupněm, jehož kořenem je dané algebraické číslo, nazveme *minimálním polynomem* tohoto čísla.

Definice 2.1. Množinu K obsahující algebraická čísla takovou, že $\mathbb{Q} \subseteq K$, nazveme *algebraickým číselným tělesem*, pokud:

- pro $a, b \in K$ je $a + b \in K$, $a \cdot b \in K$,
- pro $a \in K$ nenulové je $\frac{1}{a} \in K$,
- existují čísla $x_1, \ldots, x_n \in K$ taková, že $K = \{c_1x_1 + \ldots + c_nx_n : c_i \in \mathbb{Q}\}$.

Definice 2.2. Buď K algebraické číselné těleso a $\alpha_1, \ldots, \alpha_n$ komplexní čísla. Čísla $\alpha_1, \ldots, \alpha_n$ nazveme *lineárně nezávislá nad* K, pokud jediná $c_i \in K$ taková, že

$$c_1\alpha_1 + \ldots + c_n\alpha_n = 0,$$

splňují $c_1 = c_2 = \ldots = c_n = 0$.

Definice 2.3. Nejmenší (vzhledem k inkluzi) těleso, které obsahuje iracionální čísla $\alpha_1, \ldots, \alpha_n$ lineárně nezávislá nad $\mathbb{Q}$, budeme značit $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Triviálním případem takového číselného tělesa je množina racionálních čísel. Pokud bychom rozšířili racionální čísla o $\sqrt{2}$, pak by všechny prvky $\mathbb{Q}(\sqrt{2})$ byly tvaru $a+b\sqrt{2}$ pro racionální a, b. Pokud bychom však uvážili rozšíření $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, pak by všechny prvky byly tvaru $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, nikoliv $a+b\sqrt{2}+c\sqrt{3}$, neboť $\sqrt{2}\cdot\sqrt{3}$ se také nachází v $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Snadno ale ověříme, že všechny prvky $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ jsou tohoto tvaru.

V tělese algebraických čísel můžeme též uvážit množinu všech celých algebraických čísel, kterou budeme značit $\mathcal{O}_K$. Množina $\mathcal{O}_K$ tvoří *okruh*, tedy splňuje všechny podmínky kladené na algebraické číselné těleso až na existenci multiplikativních inverzí. Například v tělese $\mathbb{Q}$ je tímto okruhem množina celých čísel a multiplikativní inverzi v něm mají pouze čísla ± 1. Vhodným úvodem ke studiu těchto algebraických struktur je [7]. Ve zbytku textu budeme zkoumat vlastnosti okruhu $\mathcal{O}_K$. Nejprve nás bude zajímat, jak vlastně $\mathcal{O}_K$ vypadá.

Budeme se zabývat tělesy racionálních čísel rozšířených o čísla, jejichž minimální polynom nad $\mathbb{Z}$ je kvadratický. Tato tělesa budeme nazývat *kvadratická*. Při práci nad tělesy vyšších řádů bychom museli pracovat i s polynomy vyšších řádů, což je obecně obtížné. S kvadratickými tělesy dokážeme rozumně manipulovat a využijeme znalosti kvadratických zbytků. Speciálně dokážeme přesně popsat množinu celých algebraických čísel.

Okruh celých algebraických čísel v tělese $\mathbb{Q}(\mathrm{i})$ je $\mathbb{Z}[\mathrm{i}] = \{a+b\mathrm{i} \colon a, b \in \mathbb{Z}\}$, tedy Gaussova celá čísla. Bylo by krásné, pokud by pro m *bezčtvercové*, tj. nedělitelné čtvercem celého čísla, byl okruh celých algebraických čísel kvadratického tělesa $\mathbb{Q}(\sqrt{m})$ roven $\mathbb{Z}[\sqrt{m}]$. Bohužel tomu tak vždy není.

Věta 2.4. *Nechť $m \neq 0, 1$ je bezčtvercové celé číslo a $K = \mathbb{Q}(\sqrt{m})$ je algebraické číselné těleso. Pak platí*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{m}\right] & = \{a+b\sqrt{m} \colon a, b \in \mathbb{Z}\}, \ \textit{pokud } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & = \left\{a+b\frac{1+\sqrt{m}}{2} \colon a, b \in \mathbb{Z}\right\}, \ \textit{pokud } m \equiv 1 \pmod 4. \end{cases}$$

Důkaz plyne z tvaru řešení kvadratické rovnice, neboť všechny prvky okruhu $\mathcal{O}_K$ kvadratického tělesa mají stupeň nejvýše 2. Plný důkaz je k nalezení v [2, věta 3.1.1]. Dále si přiblížíme práci v těchto okruzích.

Při řešení rovnic v celých číslech mnohdy pracujeme s dělitelností a rozkladem na prvočísla. Jediná celá čísla, která mají v $\mathbb{Z}$ multiplikativní inverzi, jsou pouze ± 1. Analogicky můžeme v okruzích definovat *jednotky* jako prvky, které mají multiplikativní inverzi. Ne vždy jsou jednotky pouze ± 1, v $\mathbb{Z}[\mathrm{i}]$ jsou jednotkami též $\pm\mathrm{i}$. Obdobně můžeme za zobecnění prvočísel považovat *ireducibilní prvky*, tedy prvky okruhu R, které nelze vyjádřit jako součin dvou prvků R, které oba nejsou jednotkami. V $\mathbb{Z}[\mathrm{i}]$ nejsou obecně prvočísla ireducibilní, neboť např. 5 můžeme rozložit na součin dvou ireducibilních Gaussových čísel $(2+\mathrm{i})(2-\mathrm{i})$, i když brzy odůvodníme, že např. 7 ireducibilní je.

V číselných okruzích neplatí nutně ani jednoznačnost rozkladu, za chvíli totiž ukážeme, že číslo 6 můžeme rozložit na součin iredubilních prvků v $\mathbb{Z}[\sqrt{-5}]$ dvěma různými

způsoby. Chtěli bychom pracovat s objekty, ve kterých jednoznačnost rozkladu platí. V některých okruzích jsou tímto objektem *ideály*.

Ideál si můžeme představit jako zobecnění násobků celých čísel v číselných okruzích. Uveďme formální definici.

Definice 2.5. Ideálem okruhu R nazveme neprázdnou množinu $\mathcal{I} \subseteq R$ takovou, že pokud $a, b \in \mathcal{I}$, $r \in R$, pak $a + b \in \mathcal{I}$, $r \cdot a \in \mathcal{I}$.

V okruhu celých čísel tělesa $\mathbb{Q}$ jsou ideálem např. sudá čísla či násobky tří. V tomto článku se budeme zabývat pouze okruhy, jejichž ideály jsou konečně generované, tuto vlastnost totiž nemají všechny okruhy. Podstatným faktem pro nás bude, že každý ideál okruhu $\mathcal{O}_K$ je konečně generovaný.

Pro naše účely je ideál $\mathcal{I}$ okruhu R množinou $\{r_1a_1 + \cdots + r_na_n : a_i \in R\}$ pro nějaká $n \in \mathbb{N}$ a $r_1, \ldots, r_n \in R$. Řekneme, že r_i *generují* $\mathcal{I}$, a tento ideál budeme značit $(r_1, \ldots, r_n)$. Pokud máme ideál (a) generovaný jediným prvkem a, řekneme, že je ideálem *hlavním*. Sudá čísla i násobky tří jsou v $\mathbb{Z}$ hlavními ideály, protože jsou generované čísly 2, resp. 3.

U ideálů můžeme definovat násobení, přičemž součinem dvou ideálů je ideál

$$\mathcal{I} \cdot \mathcal{J} = \left\{ \sum_{i=1}^{n} a_i b_i \colon a_i \in \mathcal{I},\, b_i \in \mathcal{J},\, n \in \mathbb{N} \right\}.$$

Násobení ideálů je komutativní a asociativní, tj.

$$(\mathcal{I} \cdot \mathcal{J}) \cdot \mathcal{K} = \left\{ \sum_{i=1}^{n} a_i b_i c_i \colon a_i \in \mathcal{I},\, b_i \in \mathcal{J},\, c_i \in \mathcal{K},\, n \in \mathbb{N} \right\} = \mathcal{I} \cdot (\mathcal{J} \cdot \mathcal{K}).$$

Též definujme mocninu ideálu $\mathcal{I}^k$ pro přirozené k:

$$\mathcal{I}^k = \underbrace{\mathcal{I} \cdot \mathcal{I} \cdot \ldots \cdot \mathcal{I}}_{k}.$$

Pro nás bude podstatné, jak funguje násobení hlavních ideálů, protože při řešení úloh budeme chtít pracovat s hlavními ideály. Pro součin dvou hlavních ideálů platí následující tvrzení.

Věta 2.6. *Pro $a, b \in R$ platí $(a)(b) = (ab)$.*

Důkaz. Zjevně $ab \in (a)(b)$, a protože ab je obsažen v ideálu $(a)(b)$, jsou v něm obsaženy i všechny jeho násobky, tedy platí $(ab) \subseteq (a)(b)$. Na druhé straně, v každém součtu $\sum_{i=1}^{n} a_i b_i$, kde $a_i \in (a)$, $b_i \in (b)$, je každý sčítanec dělitelný ab, takže $(a)(b) \subseteq (ab)$. □

Stejně jako v celých číslech můžeme definovat dělitelnost ideálů, konkrétně píšeme $\mathcal{I} \mid \mathcal{J}$, pokud existuje ideál $\mathcal{K}$ takový, že $\mathcal{J} = \mathcal{I} \cdot \mathcal{K}$.

Důsledek 2.7. *Pro nenulová $a, b \in R$ platí $(a) \mid (b)$, právě když $b \in (a)$.*

Důkaz. Pokud platí $b \in (a)$, pak je b rovno ak pro $k \in R$, tedy dle předchozí věty $(a) \mid (a)(k) = (ak) = (b)$. Naopak pokud platí $(a) \mid (b)$, je $(b) = (a) \cdot \mathcal{I}$ pro nenulový

ideál $\mathcal{I} \subseteq R$. Dle definice násobení ideálů je každý prvek $(a) \cdot \mathcal{I}$ konečným součtem součinů prvku z (a) a prvku z $\mathcal{I}$. Každý takový součin náleží do (a), tedy $(a) \cdot \mathcal{I} \subseteq (a)$. Tudíž $b \in (b) = (a) \cdot \mathcal{I} \subseteq (a)$. □

Ideály okruhu R obsaženého v tělese K můžeme rozšířit do K na tzv. *lomené ideály* tělesa K.

Definice 2.8. Buď K těleso. Pokud je $\mathcal{I}$ ideálem okruhu $R \subseteq K$, pak pro nenulové $m \in R$ nazveme množinu $\frac{\mathcal{I}}{m} = \left\{ \frac{a}{m} | a \in \mathcal{I} \right\}$ *lomeným ideálem* $\mathcal{O}_K$.

Například lomený ideál $\frac{(3)}{2}$ v $\mathbb{Z}$ je množinou obsahující právě všechna čísla $\frac{3m}{2}$ pro celá m. Násobení lomených ideálů definujeme pomocí násobení ideálů okruhu R.

Dále budeme studovat dělitelnost čísel a ideálů v okruhu $\mathcal{O}_K$ a k tomu nám pomohou známé pojmy z oboru komplexních čísel.

3. Normy a prvoideály

Pro komplexní číslo $z = a + b\mathrm{i}$ definujeme komplexně sdružené číslo $\overline{z} = a - b\mathrm{i}$ a absolutní hodnotu $|z| = \sqrt{a^2 + b^2}$ splňující $|z|^2 = z\overline{z} = a^2 + b^2$.

Sdružená čísla v tělese K definujeme trochu jinak, značení nicméně zachováme. Pro $\alpha \in \mathbb{Z}$ definujeme $\overline{\alpha} = \alpha$. Pro každé $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$, kde $K = \mathbb{Q}(\sqrt{m})$ je kvadratické těleso, je minimální polynom α nad $\mathbb{Z}$ kvadratický. Pokud jsou α a α_2 jeho kořeny, definujeme $\overline{\alpha} = \alpha_2$. Platí

$$\overline{\left(a + b\sqrt{m}\right)} = a - b\sqrt{m},$$
$$\overline{\left(a + b\frac{1+\sqrt{m}}{2}\right)} = a + b\frac{1-\sqrt{m}}{2},$$

neboť minimální polynom prvního prvku je $(x-a)^2 - b^2 m$ a minimální polynom druhého je $(x-a)^2 - bx + ab + b^2\frac{1-m}{4}$. Pro $m = -1$ definice splývá s klasickou definicí komplexně sdruženého čísla.

Na rozdíl od komplexních čísel se nám bude hodit místo absolutní hodnoty $|z|^2 = z\overline{z}$ definovat *normu* čísla jako $N(z) = z\overline{z}$, nechceme přece pracovat s výrazy pod odmocninou. Pro celá čísla t, jejichž minimální polynom v $\mathcal{O}_K$ je $x - t$, pak máme $N(t) = t^2$, v $\mathbb{Z}[\sqrt{2}]$ má zase například $1 + 2\sqrt{2}$ minimální polynom $x^2 - 2x - 7$ a normu -7. Ze znalosti minimálních polynomů prvků kvadratického tělesa pak snadno charakterizujeme normu.

Věta 3.1. *Nechť $m \neq 0, 1$ je celé bezčtvercové číslo. Norma prvku $a + b\sqrt{m} \in \mathcal{O}_K$ tělesa $K = \mathbb{Q}(\sqrt{m})$ vypadá následovně:*

- $N\left(a + b\sqrt{m}\right) = a^2 - mb^2$, *pokud* $m \not\equiv 1 \pmod 4$,
- $N\left(a + b\frac{1+\sqrt{m}}{2}\right) = a^2 + ab + \frac{1-m}{4}b^2$, *pokud* $m \equiv 1 \pmod 4$.

V obecném číselném tělese stupně n pro číslo α s minimálním polynomem stupně k a jeho kořeny $\alpha, \alpha_2, \ldots, \alpha_k$ nazveme čísla α_i sdružená s α a definujeme normu α vztahem

$$N(\alpha) = (\alpha \cdot \alpha_2 \cdot \ldots \cdot \alpha_k)^{n/k},$$

což je vždy celé číslo. Norma nám pomůže při práci s dělitelností v okruhu $\mathcal{O}_K$. Norma je totiž multiplikativní, pro $m \not\equiv 1 \pmod 4$ a $a + b\sqrt{m}$, $c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ platí

$$\begin{aligned} N(a + b\sqrt{m})N(c + d\sqrt{m}) &= (a^2 - mb^2)(c^2 - md^2) = \\ &= a^2c^2 + m^2b^2d^2 - m\left(a^2d^2 + b^2c^2\right) = \\ &= a^2c^2 + 2acmbd + m^2b^2d^2 - m\big(a^2d^2 + b^2c^2\big) - 2acmbd = \\ &= (ac + mbd)^2 - m(ad + bc)^2 = \\ &= N\Big(ac + mbd + \sqrt{m}(ad + bc)\Big) = \\ &= N\Big((a + b\sqrt{m})(c + d\sqrt{m})\Big). \end{aligned}$$

Analogický výpočet je možno provést i v okruzích s $m \equiv 1 \pmod 4$. Pokud tedy v $\mathcal{O}_K$ dělí a číslo b, tj. existuje $c \in \mathcal{O}_K$ tak, že $b = a \cdot c$, pak $N(b) = N(a)N(c)$, a tedy $N(a) \mid N(b)$. Nicméně $N(a) \mid N(b)$ nutně neznamená $a \mid b$, například v $\mathbb{Z}[\mathrm{i}]$ máme čísla $2 + \mathrm{i}$ a $1 + 2\mathrm{i}$ se stejnou normou, i když $\frac{2+\mathrm{i}}{1+2\mathrm{i}} = \frac{(2+\mathrm{i})(1-2\mathrm{i})}{5} = \frac{4-3\mathrm{i}}{5}$ neleží v $\mathbb{Z}[\mathrm{i}]$.

Pomocí normy můžeme odůvodnit ireducibilitu 7 v $\mathbb{Z}[\mathrm{i}]$. Pokud by šla rozložit na součin dvou nejednotek, nutně by obě měly normu 7, jelikož norma 7 je 49. Poté ale $7 = N(a + b\mathrm{i}) = a^2 + b^2$, což nemá celočíselné řešení, protože kvadráty dávají pouze zbytky 0, 1 při dělení čtyřmi. Pomocí kvadratických zbytků tak například můžeme ukázat ireducibilitu 7 a 11 v $\mathbb{Z}[\sqrt{-13}]$. Pokud máme obecněji těleso $\mathbb{Q}(\sqrt{\pm p})$ pro prvočíslo p takové, že jeho okruh celých algebraických čísel je $\mathbb{Z}[\sqrt{\pm p}]$, pak je libovolné prvočíslo, které je kvadratickým nezbytkem modulo p, ireducibilní.

Budeme chtít pracovat s dělitelností i v množině ideálů okruhu $\mathcal{O}_K$ a k tomu definujeme normu ideálů. Norma obecného ideálu je definována jako počet prvků jisté množiny, jejíž přesná definice pro nás není důležitá. Podstatné však je, že normu hlavních ideálů snadno určíme.

Věta 3.2. *Pro $m \in \mathcal{O}_K$ platí $N((m)) = |N(m)|$.*

Důkaz i přesná definice normy je k nalezení v [3], Theorem 22. Norma se zde v absolutní hodnotě nachází proto, že norma prvků může být obecně záporná, ale normu ideálu definujeme jako počet prvků, tedy nezáporné číslo. Z tohoto tvrzení speciálně plyne, že na hlavních ideálech je norma též multiplikativní. Obecně je norma multiplikativní vždy, tj. platí

$$N(\mathcal{I})N(\mathcal{J}) = N(\mathcal{I} \cdot \mathcal{J})$$

pro ideály $\mathcal{I}$, $\mathcal{J}$ okruhu $\mathcal{O}_K$, kde $\cdot$ je součin ideálů. Toto elegantní tvrzení je bohužel netriviální a jeho důkaz užívá pokročilejších prostředků algebraické teorie čísel. Postup důkazu je k nalezení v [3], Chapter 3, Exercise 14.

Když už jsme obeznámeni s normami, můžeme diskutovat normy speciálních prvků, konkrétně jednotek a prvoideálů.

Mějme jednotku $\beta \in \mathcal{O}_K$, pak platí $\alpha \cdot \beta = 1$ pro nějaké $\alpha \in \mathcal{O}_K$. Z multiplikativity normy plyne

$$N(\alpha)N(\beta) = N(\alpha \cdot \beta) = N(1) = 1.$$

Protože norma prvků $\mathcal{O}_K$ je celé číslo, je nutně $N(\alpha) = \pm 1 = N(\beta)$, jednotky $\mathcal{O}_K$ jsou proto prvky s normou ± 1. Navíc z definice normy jakožto součinu sdružených čísel

dostaneme, že každý prvek $\mathcal{O}_K$ normy ± 1 je skutečně jednotkou. Pro okruhy $\mathbb{Z}[\sqrt{m}]$, kde $m \not\equiv 1 \pmod 4$, jsou jednotky dány vztahem

$$\pm 1 = N\big(a + b\sqrt{m}\big) = a^2 - mb^2,$$

jde tedy o řešení rozšířené Pellovy rovnice. V případě $m < 0$ máme jen konečně mnoho řešení, v $\mathbb{Z}[\mathrm{i}]$ máme jednotky ± 1, $\pm \mathrm{i}$ a v ostatních okruzích celých algebraických čísel pouze ± 1. Pro kladné m existuje jednotek nekonečně mnoho a tvoří multiplikativní grupu.

V případě $0 > m \equiv 1 \pmod 4$ analogicky máme pouze konečně mnoho řešení, pro $m > 0$ opět jednotky vykazují grupovou strukturu. Jednotky v kvadratických tělesech tak dokážeme většinou poměrně snadno najít.

Pomocí jednotek dokážeme trochu obratněji pracovat s hlavními ideály, konkrétně určit, kdy se dva hlavní ideály rovnají. K tomu se však ještě musíme na chvíli pozastavit u dělitelů nuly v okruhu $\mathcal{O}_K$.

Pokud okruh nemá netriviální dělitele nuly, neboli součin dvou jeho nenulových prvků je nenulový, nazveme jej *oborem integrity*. Například okruh zbytků při dělení 6 není oborem integrity, neboť 2, 3 jsou dělitelé 0. Naopak si snadno rozmyslíme, že okruh $\mathcal{O}_K$ pro číselné těleso K již oborem integrity je. Můžeme tedy vyslovit následující tvrzení.

Věta 3.3. *Mějme a, $b \in \mathcal{O}_K$. Pak platí $(a) = (b)$, právě když existuje jednotka $u \in \mathcal{O}_K$ taková, že $a = ub$.*

Důkaz. Pokud platí $(a) \mid (b)$, pak $b \in (a)$ díky důsledku 2.7, tudíž $b = ax$ pro $x \in \mathcal{O}_K$. Analogicky $a \in (b)$, tedy $a = by$, $y \in \mathcal{O}_K$. Pak $a = axy$, tedy $a(1 - xy) = 0$, a protože je $\mathcal{O}_K$ oborem integrity, je alespoň jeden z činitelů 0. Případ $a = 0$ je triviální, jinak $xy = 1$, tedy x, y jsou jednotky. Naopak pokud $a = ub$ pro jednotku u okruhu $\mathcal{O}_K$, je $a = ub \in (b)$, tedy $(a) \subseteq (b)$. Obdobně $b = \frac{1}{u}a \in (a)$, tedy $(b) \subseteq (a)$. Platí tak $(a) = (b)$. □

Definice 3.4. O prvcích a, $b \in \mathcal{O}_K$ splňujících $a = ub$ pro jednotku u okruhu $\mathcal{O}_K$ řekneme, že jsou *asociované*.

Nyní se pojďme podívat na prvoideály, ekvivalenty prvočísel v ideálech okruhu $\mathcal{O}_K$.

Definice 3.5. Mějme ideál $\mathcal{P} \subset \mathcal{O}_K$ takový, že pokud pro a, $b \in \mathcal{O}_K$ platí $ab \in \mathcal{P}$, tak buď $a \in \mathcal{P}$, či $b \in \mathcal{P}$. Pak $\mathcal{P}$ nazveme *prvoideálem*.

Nejjednodušší příklad prvoideálů se opět nachází v celých číslech, jsou to totiž přesně násobky prvočísel.

Víme, že v číselném tělese mohou mít prvočíselné normy pouze ireducibilní prvky. Podobně pro prvoideály platí následující tvrzení.

Věta 3.6. *Je-li $\mathcal{P}$ prvoideál, pak existují $j \in \mathbb{N}$ a prvočíslo p takové, že $N(\mathcal{P}) = p^j$ a $p \in \mathcal{P}$.*

Existence příslušného prvočísla se dá vyvodit z definice normy ideálu, nástin důkazu se nachází v [3], Theorem 22. Prvoideály tak mají normy rovné mocninám prvočísel a naopak, pokud ideál má normu rovnou prvočíslu, je prvoideálem.

Z naší zatím omezené znalosti prvoideálů opravdu vidíme, že jsou úzce spojené s prvočísly, jejichž jednou z nejzákladnějších vlastností je jednoznačnost rozkladu.

Již jsme zmínili, že v číselných okruzích obecně jednoznačnost rozkladu neplatí. Např. v okruhu $\mathbb{Z}[\sqrt{-5}]$ můžeme rozložit $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Čísla $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ jsou v $\mathbb{Z}[\sqrt{-5}]$ všechna ireducibilní, protože jejich normy jsou po řadě 4, 9, 6, 6 a existence prvků s normou 2 či 3 v $\mathbb{Z}[\sqrt{-5}]$ znamená, že rovnice $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$, resp. 3 má celočíselná řešení. Pro nějaké a tedy platí $a^2 \equiv 2 \pmod 5$, resp. $a^2 \equiv 3 \pmod 5$, což je spor, neboť 2 ani 3 nejsou kvadratické zbytky modulo 5.

Obecně v okruzích nemusí platit ani jednoznačnost rozkladu na prvoideály. Ty, ve kterých platí, nazveme *Dedekindovy*. Dá se ukázat, že okruh celých algebraických čísel $\mathcal{O}_K$ je Dedekindovým okruhem. V $\mathbb{Z}[\sqrt{-5}]$ se tedy ideál (6) jednoznačně rozkládá na prvoideály. Pro zajímavost uveďme rozklad

$$(6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

s tím, že ideály, jejichž generátory jsou výše uvedení dělitelé 6, se v $\mathbb{Z}[\sqrt{-5}]$ se rozkládají následovně:

- $(2) = (2, 1 + \sqrt{-5})^2$,
- $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$,
- $(1 + \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})$,
- $(1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$.

S následujícím tvrzením jsme se již setkali v případě hlavních ideálů.

Věta 3.7. *Mějme ideály $\mathcal{A}, \mathcal{B}$ v $\mathcal{O}_K$. Pak platí $\mathcal{B} \mid \mathcal{A}$, právě když $\mathcal{A} \subseteq \mathcal{B}$.*

Důkaz užívající jednoznačnosti rozkladu ideálů okruhu $\mathcal{O}_K$ je podán v [6], věta 4.3.3. Následující fakta lze odůvodnit podobně jako v oboru celých čísel.

Věta 3.8. *Mějme nenulové ideály $\mathcal{A}, \mathcal{B}, \mathcal{C}$ okruhu $\mathcal{O}_K$. Pokud pro nějaké $k \in \mathbb{N}$ platí $\mathcal{A} \cdot \mathcal{B} = \mathcal{C}^k$ a navíc jsou $\mathcal{A}, \mathcal{B}$ nesoudělné, pak existují ideály $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}_K$ takové, že*

$$\mathcal{A} = \mathcal{I}^k, \qquad \mathcal{B} = \mathcal{J}^k.$$

Důkaz. Nechť $\mathcal{A} = \mathcal{P}_1^{a_1} \cdot \ldots \cdot \mathcal{P}_p^{a_p}$, $\mathcal{B} = \mathcal{Q}_1^{b_1} \cdot \ldots \cdot \mathcal{Q}_q^{b_q}$ jsou jednoznačně určené rozklady $\mathcal{A}, \mathcal{B}$ na prvoideály. Pokud jsou $\mathcal{A}, \mathcal{B}$ nesoudělné, pak $\mathcal{P}_i$ a $\mathcal{Q}_i$ jsou disjunktní posloupnosti prvoideálů. Libovolný ideál dělící $\mathcal{C}^k$ ho dělí v k-té mocnině (případně násobku k), z nesoudělnosti ideálů tak plyne, že každý prvoideál dělící jeden z $\mathcal{A}, \mathcal{B}$ jej dělí v mocnině dělitelné k. Oba ideály jsou proto k-té mocniny. □

Pokud platí $\mathcal{A} \cdot \mathcal{B} = \mathcal{P} \cdot \mathcal{I}^k$ pro nesoudělné ideály $\mathcal{A}, \mathcal{B}$ a prvoideál $\mathcal{P}$, pak tento prvoideál dělí právě jeden z $\mathcal{A}, \mathcal{B}$. Díky jednoznačnosti rozkladu můžeme postupovat analogicky jako výše a ukázat, že jeden z $\mathcal{A}, \mathcal{B}$ musí být k-tou mocninou ideálu.

Součet dvou násobků celého čísla d je opět násobkem d. U ideálů můžeme formulovat podobné tvrzení, tentokrát se však zaměříme pouze na hlavní ideály.

Věta 3.9. *Pokud pro $a, b \in \mathcal{O}_K$ a $\mathcal{I} \subseteq \mathcal{O}_K$ platí $\mathcal{I} \mid (a), (b)$, pak $\mathcal{I} \mid (a \pm b)$.*

Důkaz. Pokud $\mathcal{I} \mid (a)$, (b), pak díky větě 3.7 je a, $b \in \mathcal{I}$, tudíž z definice ideálu $a \pm b \in \mathcal{I}$. Proto $\mathcal{I} \mid (a \pm b)$. □

V Dedekindových okruzích, speciálně v $\mathcal{O}_K$, platí jednoznačnost rozkladu na prvoideály, nicméně v okruzích $\mathbb{Z}$ a $\mathbb{Z}[\mathrm{i}]$ platí i jednoznačný rozklad čísel na ireducibilní prvky. Pro imaginární tělesa, tj. $K = \mathbb{Q}(\sqrt{d})$ pro $d < 0$, se Carl Friedrich Gauss domníval, že jediná d, pro která v $\mathcal{O}_K$ platí jednoznačnost rozkladu, jsou

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

První důkaz této domněnky byl podán až ve 20. století Kurtem Heegnerem, po němž nesou tato čísla pojmenování *Heegnerova*. Pro reálná tělesa toho mnoho nevíme, dokonce ani zda je reálných těles s jednoznačným rozkladem nekonečně mnoho.

Obecně bychom chtěli zavést strukturu, která bude měřit, do jaké míry selhává v daném okruhu jednoznačnost rozkladu. A takový účel splňuje grupa tříd ideálů.

4. Třídy ideálů

Uvažme množinu všech lomených ideálů okruhu $\mathcal{O}_K$. Řekneme, že dva ideály $\mathcal{I}$, $\mathcal{J}$ okruhu $\mathcal{O}_K$ jsou *ekvivalentní*, což značíme $\mathcal{I} \sim \mathcal{J}$, pokud existují a, $b \in \mathcal{O}_K$ takové, že $\mathcal{I} \cdot (a) = \mathcal{J} \cdot (b)$. Dostáváme pak třídy ekvivalence na $\mathcal{O}_K$, kde dva ideály leží ve stejné třídě, právě když $\mathcal{I} \sim \mathcal{J}$.

Díky tomu, že součinem dvou hlavních ideálů je hlavní ideál, platí, že když vynásobíme prvky nějaké z tříd hlavním ideálem, získáme prvek téže třídy. Množina všech tříd ideálů tedy tvoří grupu s operací násobení ideálů a třída hlavních ideálů okruhu $\mathcal{O}_K$ je jejím neutrálním prvkem. Ukázali jsme totiž, že násobení ideálů je asociativní, a v Dedekindových okruzích existuje inverzní prvek pro nenulové ideály, viz [6], věta 4.1.7, kde je dokázána existence inverze prvoideálů. Vzhledem k jednoznačnému rozkladu ideálů na prvoideály tak existuje inverzní prvek k libovolnému nenulovému ideálu okruhu $\mathcal{O}_K$.

Právě popsaná grupa se nazývá *grupa tříd ideálů* okruhu $\mathcal{O}_K$.

Věta 4.1. *Grupa tříd ideálů okruhu $\mathcal{O}_K$ je konečná.*

Důkaz tohoto tvrzení je k nalezení v [6], důsledek 5.2.5. Poznamenejme, že v libovolném okruhu není grupa tříd ideálů obecně konečná, dokonce ani když se omezíme na Dedekindovy okruhy.

Počet prvků grupy tříd ideálů okruhu $\mathcal{O}_K$ nazveme *třídovým číslem* $\mathcal{O}_K$ a budeme jej značit h_K. Víme, že libovolný prvek grupy dá po umocnění na její řád neutrální prvek. Můžeme proto zformulovat následující výsledek.

Věta 4.2. *Buď $\mathcal{I}$ lomený ideál okruhu $\mathcal{O}_K$. Pak $\mathcal{I}^{h_K}$ je hlavním ideálem.*

Tato věta je jedním z nejdůležitějších stavebních bloků, díky kterému budeme moci řešit rovnice. Dále propojíme grupu tříd ideálů s jednoznačností rozkladu prvků v okruhu $\mathcal{O}_K$.

Věta 4.3. *Pokud algebraické číselné těleso K splňuje $h_K = 1$, pak $p \in \mathcal{O}_K$ je ireducibilní, právě když (p) je prvoideál.*

Důkaz. Mějme prvoideál (p) a řekněme, že $p = ab$ pro $a, b \in \mathcal{O}_K$. Díky větě 2.6 platí $(p) = (ab) = (a)(b)$, tedy vzhledem k jednoznačnému rozkladu ideálů na prvoideály je jedno z a, b jednotkou a p je ireducibilní. Naopak mějme p ireducibilní a (p) součin dvou ideálů okruhu $\mathcal{O}_K$. Protože každý ideál tohoto okruhu je hlavní, je $(p) = (a)(b) = (ab)$, tedy z věty 3.3 plyne $p = uab$ pro jednotku u okruhu $\mathcal{O}_K$. Protože je p ireducibilní, je jedno z a, b jednotkou, a (p) se nedá vyjádřit jako součin dvou ideálů, které oba nejsou generované jednotkou. Je proto prvoideálem. □

Důsledek 4.4. *Pokud třídové číslo algebraického číselného tělesa K je rovno* 1*, pak v okruhu $\mathcal{O}_K$ platí jednoznačný rozklad čísel na ireducibilní prvky.*

Důkaz. Uvažme těleso K, kde $h_K = 1$, a pro nějaké $n \in \mathcal{O}_K$ uvažme dva rozklady na ireducibilní prvky $u_1 p_1 p_2 \cdots p_k = n = u_2 q_1 q_2 \cdots q_\ell$, kde u_i jsou jednotky okruhu $\mathcal{O}_K$. Z věty 2.6 máme rovnost ideálů

$$(p_1) \cdot (p_2) \cdot \ldots \cdot (p_k) = (p_1 p_2 \ldots p_k) = (q_1 q_2 \ldots q_\ell) = (q_1) \cdot (q_2) \cdots (q_\ell).$$

Podle předchozí věty jsou ideály (p_i) a (q_i) prvoideály. Rozklad obou stran na prvoideály musí být shodný, tedy podle věty 3.3 se množiny příslušných ireducibilních prvků musí až na násobení jednotkou rovnat. □

Analogicky se dá ukázat, že pokud platí jednoznačný rozklad čísel $\mathcal{O}_K$ na ireducibilní prvky, pak $h_K = 1$. Podrobnosti o rozkladu prvků i ideálů okruhu $\mathcal{O}_K$ lze najít v [4], kapitoly 4 a 5.

Víme, že součinem dvou hlavních ideálů je hlavní ideál, můžeme proto vyslovit následující tvrzení.

Věta 4.5. *Buď $\mathcal{I}$ lomený ideál okruhu $\mathcal{O}_K$ a k celé číslo. Pokud $\mathcal{I}^k$ je hlavním ideálem a k je nesoudělné s h_K, pak $\mathcal{I}$ je hlavním ideálem.*

Důkaz. Pokud jsou k, h_K nesoudělná, podle Bezoutovy věty existují celá čísla a, b splňující $ak + bh_K = 1$. Pak $\mathcal{I} = \mathcal{I}^{ak+bh_K} = (\mathcal{I}^k)^a \cdot (\mathcal{I}^{h_K})^b$ je součinem dvou hlavních ideálů, neboť mocnina hlavního ideálu $(x)^y$ je díky větě 2.6 hlavní ideál (x^y). Tedy $\mathcal{I}$ je hlavní ideál okruhu $\mathcal{O}_K$. □

Např. okruh $\mathbb{Z}[\sqrt{-5}]$ má grupu tříd ideálů dvouprvkovou, tedy pokud lichá mocnina ideálu $\mathcal{I}$ je hlavní, pak je $\mathcal{I}$ hlavní. V tomto okruhu neplatí jednoznačnost rozkladu (například čísla 6).

Protože ani neznáme všechny reálné okruhy s třídovým číslem 1, nepřekvapí nás, že obecně nejsme schopni říci, která všechna tělesa mají dané třídové číslo, dokonce ani, zda jich je nekonečně mnoho. Tento problém je znám jako *Class number problem*. Existují nicméně rozsáhlé tabulky třídových čísel $\mathbb{Q}(\sqrt{n})$ pro malá n, například v knihovně posloupností OEIS, a proto můžeme pomocí programů jako Wolfram Alpha či Wolfram Mathematica třídová čísla zjistit.

Povedlo se nám popsat dělitelnost ideálů v okruhu $\mathcal{O}_K$ a jisté vlastnosti grupy tříd ideálů. Nyní se s touto teorií konečně můžeme pustit do řešení rovnic.

5. Příklady

Nejprve vyřešíme rovnici v okruhu Gaussových čísel, neboť s nimi jsme nejvíce obeznámeni.

Příklad 5.1. Řešte v $\mathbb{Z}$ rovnici

$$x^2 + 4 = y^5. \tag{1}$$

Řešení. Předpokládejme, že (x, y) je řešením dané rovnice. Pak x, y zjevně mají stejnou paritu. Pokud jsou x, y soudělná, tj. obě dělitelná prvočíslem p, pak z rovnice plyne $p^2 \mid 4$, neboli $p = 2$. Pak máme $x = 2x_1$, $y = 2y_1$ a pro celá x_1, y_1 platí

$$x_1^2 + 1 = 8y_1^5,$$

tedy $x_1^2 \equiv -1 \pmod 4$, což je nemožné, neboť -1 je kvadratický nezbytek modulo 4. Nutně jsou tak x, y nesoudělná, a tedy obě lichá. Tyto vlastnosti x, y použijeme při důkazu nesoudělnosti ideálů.

Nyní rozložme rovnici (1) v $\mathbb{Z}[\mathrm{i}]$:

$$(x + 2\mathrm{i})(x - 2\mathrm{i}) = y^5.$$

Z této rovnosti speciálně plyne, že ideály generované jednotlivými stranami jsou též shodné. Díky větě 2.6 můžeme chápat

$$(x + 2\mathrm{i})(x - 2\mathrm{i}) = \Big((x + 2\mathrm{i})(x - 2\mathrm{i})\Big) = \big(y^5\big) = (y)^5$$

jako rovnost ideálů. Nyní bychom chtěli ukázat, že ideály generované $x + 2\mathrm{i}$ a $x - 2\mathrm{i}$ jsou nesoudělné. Předpokládejme naopak, že existuje prvoideál $\mathcal{P}$ dělící $(x + 2\mathrm{i})$ i $(x - 2\mathrm{i})$. Podle vět 3.2, 3.9 a multiplikativity normy máme

$$\mathcal{P} \mid (4\mathrm{i}) \Rightarrow N(\mathcal{P}) \mid N((4\mathrm{i})) = |N(4\mathrm{i})| = 16.$$

Pak pro prvočíslo $p \in \mathcal{P}$ je $p^j = N(\mathcal{P}) \mid 16$, tedy $p = 2$. Platí ale $\mathcal{P} \mid (x + 2\mathrm{i})$, a tak $2 \mid N(\mathcal{P}) \mid N(x + 2\mathrm{i}) = x^2 + 4$, tedy x je sudé číslo, spor. Ideály $(x + 2\mathrm{i})$ a $(x - 2\mathrm{i})$ jsou nesoudělné.

Součin dvou nesoudělných ideálů $(x + 2\mathrm{i})$, $(x - 2\mathrm{i})$ je pátou mocninou ideálu (y), tedy díky větě 3.8 jsou oba tyto ideály pátou mocninou ideálu. Existuje tak ideál $\mathcal{I} \subseteq \mathcal{O}_K$ takový, že $(x + 2\mathrm{i}) = \mathcal{I}^5$.

Pomocí příkazu

```
NumberFieldClassNumber[Sqrt[-1]]
```

v programu Wolfram Mathematica zjistíme, že $h_{\mathbb{Q}(\mathrm{i})} = 1$, v $\mathbb{Z}[\mathrm{i}]$ tudíž platí jednoznačnost rozkladu na ireducibilní prvky. Každý ideál okruhu $\mathbb{Z}[\mathrm{i}]$ je hlavní, existuje proto $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ takové, že $\mathcal{I} = (a + b\mathrm{i})$:

$$(x + 2\mathrm{i}) = \mathcal{I}^5 = (a + b\mathrm{i})^5 = \Big((a + b\mathrm{i})^5\Big),$$

což opět platí díky větě 2.6. $\mathbb{Z}[i]$ je oborem integrity, tedy podle věty 3.3 jsou $x + 2\mathrm{i}$ a $(a + b\mathrm{i})^5$ asociované, jejich podílem je jednotka v $\mathbb{Z}[i]$.

Jednotky $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ jsou Gaussova celá čísla splňující

$$\pm 1 = N(a + b\mathrm{i}) = a^2 + b^2,$$

tedy $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$ a jednotkami jsou pouze $1, -1, \mathrm{i}, -\mathrm{i}$. Máme tak

$$x + 2\mathrm{i} = u(a + b\mathrm{i})^5$$

pro $u \in \{\pm 1, \pm \mathrm{i}\}$. Samozřejmě bychom mohli rozebrat všechny čtyři případy, nicméně si můžeme práci usnadnit. Všimneme si, že pokud pro nějaké x máme pro $u = -1, \mathrm{i}, -\mathrm{i}$ řešení (a, b), pak z něj získáme řešení pro $u = 1$ s dvojicemi po řadě $(-a, -b)$, $(-b, a)$ a $(b, -a)$. Stačí tedy uvažovat pouze případ $u = 1$. Máme

$$x + 2\mathrm{i} = (a + b\mathrm{i})^5 = a^5 - 10a^3b^2 + 5ab^4 + \mathrm{i}(5a^4b - 10a^2b^3 + b^5).$$

Čísla 1 a i jsou lineárně nezávislá nad racionálními čísly, dokonce i nad $\mathbb{R}$, proto se musí rovnat reálné i imaginární složky obou stran. Porovnáním imaginárních složek získáme

$$2 = 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4).$$

Máme $b \mid 2$, tedy $b \in \{\pm 1, \pm 2\}$. Pro každý z těchto případů nám zbyde kvadratická rovnice v a^2 a snadno ověříme, že nezískáme celočíselná řešení pro a.

Neexistuje x takové, že $x + 2\mathrm{i}$ je pátou mocninou Gaussova celého čísla, tedy rovnice (1) nemá celočíselná řešení. □

Viděli jsme, jak dokázat, že rovnice nemá celočíselná řešení, a jak pracovat v okruhu $\mathbb{Z}[\sqrt{d}]$. Pokud by rovnice řešení měla, tak bychom postupovali stejně, jen bychom v posledním kroku našli vyhovující a, b. Nyní již do práce zapojíme i grupu tříd ideálů.

Příklad 5.2. Řešte v $\mathbb{Z}$ rovnici

$$x^2 + 13 = y^3. \tag{2}$$

Řešení. Nechť (x, y) je řešení rovnice. Vidíme, že x, y jsou nesoudělná a různých parit. Pokud by bylo y sudé, je $x^2 \equiv -1 \pmod 4$, což je nemožné, proto je x sudé a y liché. Nyní se již můžeme pustit do rozkladu v $\mathbb{Z}[\sqrt{-13}]$:

$$(x + \sqrt{-13})(x - \sqrt{-13}) = y^3,$$

což můžeme díky větě 2.6 vyjádřit jako rovnost ideálů $\mathbb{Z}[\sqrt{-13}]$:

$$(x + \sqrt{-13})(x - \sqrt{-13}) = (y)^3.$$

Součin ideálů na levé straně je tedy třetí mocninou ideálu. Chtěli bychom ukázat, že tyto ideály jsou nesoudělné. Předpokládejme naopak, že jsou oba dělitelné prvoideálem $\mathcal{P}$. Pomocí multiplikativity normy a věty 3.2 máme

$$\mathcal{P} \mid (x \pm \sqrt{-13}) \Rightarrow N(\mathcal{P}) \mid x^2 + 13 = y^3,$$

avšak díky větě 3.9 platí

$$\mathcal{P} \mid (2\sqrt{-13}) \Rightarrow N(\mathcal{P}) \mid N((2\sqrt{-13})) = 4 \cdot 13.$$

Víme, že y je liché, a pokud $13 \mid y$, tak $13 \mid x$, což je spor s nesoudělností x a y. Oba ideály jsou nesoudělné a jejich součinem je třetí mocnina ideálu. Dle věty 3.8 jsou oba třetí mocninou ideálu, existuje tedy ideál $\mathcal{I} \subseteq \mathbb{Z}[\sqrt{-13}]$ takový, že $\mathcal{I}^3 = (x + \sqrt{-13})$, speciálně třetí mocninou ideálu $\mathcal{I}$ je hlavní ideál.

Teď se do řešení zapojí grupa tříd ideálů. Příkaz

```
NumberFieldClassNumber[Sqrt[-13]]
```

prozradí, že grupa tříd ideálů okruhu $\mathbb{Z}[\sqrt{-13}]$ je dvouprvková, neplatí v něm jednoznačnost rozkladu. Podle věty 4.2 je tak druhá mocnina libovolného ideálu $\mathbb{Z}[\sqrt{-13}]$ hlavní. Protože 3 je nesoudělné se 2 a součinem dvou hlavních ideálů je hlavní ideál, je nutně ideál $\mathcal{I}$ hlavní ideál generovaný nějakým prvkem okruhu $\mathbb{Z}[\sqrt{-13}]$, což je $a + b\sqrt{-13}$ pro a, b celá. Opět podle věty 2.6 platí

$$(x + \sqrt{-13}) = (a + b\sqrt{-13})^3 = \left((a + b\sqrt{-13})^3\right),$$

což je rovnost hlavních ideálů našeho okruhu. Podle věty 3.3 je podílem $x + \sqrt{-13}$ a $(a + b\sqrt{-13})^3$ jednotka $\mathbb{Z}[\sqrt{-13}]$, tj. ± 1. Navíc pro vyhovující (x, a, b) a jednotku -1 vyhovují $(x, -a, -b)$ pro jednotku 1, a proto můžeme předpokládat, že

$$x + \sqrt{-13} = (a + b\sqrt{-13})^3. \tag{3}$$

Čísla 1 a $\sqrt{-13}$ jsou lineárně nezávislá nad $\mathbb{Q}$, dokonce i nad $\mathbb{R}$, takže se v předchozí rovnosti shodují reálné a imaginární části. Porovnáním koeficientů u $\sqrt{-13}$ získáme

$$b(3a^2 - 13b^2) = 1,$$

takže $b \mid 1$, a tedy $b \in \{\pm 1\}$. Snadno pak nalezneme jediná možná řešení $(a, b) = (\pm 2, -1)$ a z racionální části (3) dopočteme $x \in \{\pm 70\}$. Z naší původní rovnice dopočteme jediná možná řešení $(\pm 70, 17)$. Žádné jiné x nemůže řešit naši původní rovnici, jsme tedy hotovi. □

Poslední dvě rovnice jsme řešili pouze rozkladem v okruzích $\mathbb{Z}[\sqrt{d}]$, nicméně práce v okruzích $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ není příliš odlišná a všechny podstatné rozdíly jsme v článku zmínili. Jak se v těchto okruzích pracuje, si můžete vyzkoušet v následující úloze.

Cvičení 5.3. Vyřešte v celých číslech rovnici

$$x^2 + 11 = y^3,$$

pokud víte, že $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ je Dedekindův obor.

Přeji hezké počítání!

6. Závěr

Díky studiu rozšíření racionálních čísel o algebraická čísla a grupám tříd ideálů dokážeme vyřešit rovnice, které bychom pomocí elementárních metod řešili jen těžko. Doufáme, že jsme čtenáři poskytli alespoň malé okénko za oponu, byť jsme samozřejmě museli vynechat četné podrobnosti. Metodami uvedenými v tomto článku jsme schopni vyřešit i složitější rovnice, jak se může čtenář dočíst v [2] a [5].

Studiem algebraické teorie čísel však můžeme dojít k mnoha důležitějším výsledkům, než je vyřešení diofantické rovnice. Pomocí poznatků z této oblasti matematiky můžeme studovat podrobněji například právě kvadratické zbytky, dokázat tzv. zákon

kvadratické reciprocity a zobecnit jej do vyšších řádů na tzv. *Artinův zákon reciprocity*. Můžeme též studovat například Dedekindovy zeta funkce, které jsou zobecněním Riemannovy zeta funkce, a jsou tedy úzce spjaty s rozložením prvočísel.

Poděkování. Rád bych poděkoval Tomáši Perutkovi za uvedení do této krásné oblasti matematiky a pomoc při psaní tohoto článku i práce SOČ, na které je článek založen.

L i t e r a t u r a

[1] Beneš, P.: *Zákony reciprocity*. Diplomová práce. Masarykova univerzita, Brno, 2010.

[2] Hrnčiar, M.: *Řešení diofantických rovnic rozkladem v číselných tělesech*. Diplomová práce. Univerzita Karlova, Praha, 2015.

[3] Marcus, D. A.: *Number fields*. Springer-Verlag, New York, 1977.

[4] Perutka, T.: *Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity*. Středoškolská odborná činnost. Masarykova univerzita, Brno, 2018.

[5] Pezlar, Z.: *Zajímavá využití algebraické teorie čísel*. Středoškolská odborná činnost. Masarykova univerzita, Brno, 2020.

[6] Pupík, P.: *Užití grupy tříd ideálů při řešení některých diofantických rovnic*. Diplomová práce. Masarykova univerzita, Brno, 2009.

[7] Rosický, J.: *Algebra*. Masarykova univerzita, Brno, 2002.