STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Zajímavá využití algebraické teorie čísel

Zdeněk Pezlar
Jihomoravský kraj

Brno 2020

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Zajímavá využití algebraické teorie čísel

Interesting Uses of Algebraic Number Theory

Autor: Zdeněk Pezlar
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultant: Tomáš Perutka

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ..... Podpis: .....

jihomoravský kraj

Poděkování

Zde bych chtěl poděkovat Tomáši Perutkovi za cenné rady a za nekonečnou trpělivost při opravování mých četných chyb. Tato práce byla vypracována za finanční podpory JMK.

Abstrakt

Cílem práce je uvést čtenáře do studia algebraické teorie čísel a aplikovat její metody na řešení jistých obtížných diofantických rovnic. V první kapitole definujeme kvadratické zbytky a ukážeme, co s nimi dokážeme řešit a co ne. V dalších kapitolách pak představíme jisté důležité oblasti algebraické teorie čísel a na konci naše poznatky zužitkujeme řešením několika vybraných rovnic.

Klíčová slova

kvadratický zbytek; číselné těleso; grupa tříd ideálů; jednoznačnost rozkladu; diofantické rovnice.

Abstract

The aim of this thesis is to introduce the reader to algebraic number theory and its applications in solving certain difficult diophantine equations. In the first chapter we define quadratic residues and show what they are capable or incapable of. In the rest of our paper we present select important areas of algebraic theory and at the end we solve a few equations via the theory we present.

Key words

quadratic residue; number field; ideal class group; unique factorization; diophantine equations.

Obsah

Úvod **5**

1 Kvadratické zbytky **7**

2 Algebraická teorie čísel **13**
2.1 Základy 13
2.2 Ideály 14
2.3 Normy 16
2.4 Prvoideály a jednotky 17
2.5 Dedekindovy okruhy 18
2.6 Grupa tříd ideálů 19

3 Diofantické rovnice **21**
3.1 Pellova rovnice 21
3.2 Thueho rovnice 23

4 Číselná tělesa **24**
4.1 Těleso $\mathbb{Q}(i)$ 26
4.2 Těleso $\mathbb{Q}(\sqrt{-13})$ 26
4.3 Těleso $\mathbb{Q}(\sqrt{-7})$ 27
4.4 Těleso $\mathbb{Q}(\sqrt{86})$ 27

5 Příklady **28**

Závěr **48**

Úvod

Nalezení řešení dané diofantické rovnic je častým problémem teorie čísel. Ať už čelíme pouhým lineárním diofantických rovnicím, ku příkladu $2a + 3b = 1$, či rovnicím vyšších řádu, třeba $a^3 - b^3 = 1$, máme hned několik nástrojů na řešení. Můžeme najít nějaké omezení za pomocí modulární aritmetiky, což můžeme využít v první rovnici, či najít nějaký rozklad, což zase užijeme v druhém příkladu. Pokud se začneme dostávat do vyšších řádů a nebo dokonce budeme mít rovnice, které nebudou homogenní v některých proměnných, tak nám tyto základní metody většinou moc nepomohou.

Jedním způsobem, jak můžeme aplikovat modulární aritmetiku na rovnice vyšších řádů, jsou mocninné zbytky. Nejznámější a nejpoužívanější oblastí jsou v tomto ohledu kvadratické zbytky, kterými se zabývá naše první kapitola. Ty nám rozšíří možnosti jak dokazovat, že rovnice nemá řešení, případně určit celočíselná řešení, nicméně ani ty nejsou všemocné.

Uvažme následující úlohu:
Nalezněte všechny dvojice celých čísel (x, y) *splňující*:

$$x^2 + 13 = y^3.$$

Jak si ukážeme na příkladu (1.0.10), u rovnic podobného typu dokážeme mnohdy snadno ukázat, že nemají řešení, na příklad použitím modulární aritmetiky. Pokud nicméně použijeme výpočetní techniky, zjistíme, že existují řešení $(\pm 70, 17)$. Pokud má taková rovnice jedno poměrně netriviální řešení, nedokážeme s jistotou říci, zda nemá nějaká další.

Když nám s řešením nepomůže modulární aritmetika, tak co kdybychom se vrátili k již zmíněnému rozkladání? Známe vzorec $a^2 - b^2 = (a - b)(a + b)$, což dokážeme za pomoci komplexních čísel rozšířit na součet kvadrátů: $a^2 + b^2 = (a + bi)(a - bi)$, s komplexní jednotkou však nyní v klasické teorii čísel pracovat neumíme. Analogicky pokud takto rozložíme naši rovnici, kde uvážíme $13b^2$ jako čtverec, získáme ve výrazech $\sqrt{-13}$, což není reálné číslo a dokonce obsahuje iracionální $\sqrt{-13}$. Nyní nevidíme žádnou souvislost tohoto rozkladu s celočíselnými řešeními naší rovnice. V naší práci se pokusíme onu souvislost čtenáři představit.

Použitá značení

$a \mid b$	a dělí b
$\mathcal{D}(a,b)$	největší společný dělitel a, b
$a \sim b$	a je asociované s b
$\overline{a+b\sqrt{m}}$	konjugát $a+b\sqrt{m}$, neboli $a-b\sqrt{m}$
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	množina přirozených, celých, racionálních, reálných, komplexních čísel
$\mathbb{Z}_d$	okruh zbytků modulo d
$R[x]$	okruh polynomů s koeficienty nad okruhem R
$K(a_1, \ldots, a_n)$	nejmenší podtěleso L, které obsahuje těleso K i prvky $a_1, \ldots, a_n \in L$
$[K : L]$	stupeň rozšíření tělesa K nad L, t.j. dimenze vektorového prostoru $K : L$
$\mathcal{O}_K$	okruh celých algebraických čísel tělesa K
$Cl(\mathcal{O}_K)$	grupa tříd ideálů tělesa K
h_K	řád grupy tříd ideálů tělesa K
$\mathcal{U}(\mathcal{O}_K)$	grupa jednotek tělesa K
(a)	hlavní ideál generovaný prvkem a
$\frac{\mathcal{I}}{m}$	lomený ideál $\frac{\mathcal{I}}{m}$
$\left(\frac{a}{m}\right)$	hlavní lomený ideál $\frac{(a)}{m}$
$N(a)$	norma prvku a
$N((a))$	norma ideálu generovaného a
$\mathcal{I} \mid \mathcal{J}$	ideál $\mathcal{I}$ dělí ideál $\mathcal{J}$
P_α	minimální polynom α nad K
G/H	faktorgrupa G podle H

Kapitola 1

Kvadratické zbytky

V této kapitole si zběžně definujeme kvadratické zbytky a Legendreův symbol a zmíníme několik souvisejících tvrzení. Je předpokládána znalost základů modulární aritmetiky celých a racionálních čísel.

Definice 1.0.1. *Buďte $d \in \mathbb{N}, a \in \mathbb{Z}$. Pokud existuje $0 \not\equiv x \in \mathbb{Z}_d : x^2 \equiv a \pmod{d}$, pak řekneme, že a je kvadratický zbytek modulo d. Pokud takové a neexistuje, tak řekneme, že a je kvadratický nezbytek modulo d.*

Například mějme $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Pokud umocníme tyto hodnoty na druhou, získáme po řadě $0, 1, 4, 4, 1 \pmod 5$, tedy $1, 4$ jsou kvadratické zbytky modulo 5 a $2, 3$ jsou kvadratické nezbytky.

Bez znalosti rozkladu d pouze těžko popíšeme, jak vypadá množina kvadratických zbytků modulo d, nicméně pro prvočísla a jejich mocniny je to jednodušší. Poté pouze stačí zmínit, že číslo a je kvadratickým zbytkem modulo d právě pokud je kvadratickým zbytkem modulo každé prvočíslé mocniny p^k dělící d. Pokud totiž číslo není zbyktem modulo nějakou prvočíselnou mocninu dělící d, tak zjevně není zbytkem modulo d, s opačnou implikací nám pomůže Čínská zbytková věta. Než se ale pustíme na prvočísla, připomeňme si Malou Fermatovu větu.

Věta 1.0.2. *Nechť p je prvočíslo, $p \in \mathbb{Z}$. Pak:*

$$a^p \equiv a \pmod{p}.$$

Navíc pokud $p \nmid a$, tak můžeme psát $a^{p-1} \equiv 1 \pmod{p}$.

Definice 1.0.3. *Buď p prvočíslo, $a \in \mathbb{Z}$. Pak Legendrův symbol $\left(\frac{a}{p}\right)$ definujeme jako:*

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

Dalším známým tvrzením ohledně kvadratických zbytků je Lagrangeova věta.

Věta 1.0.4. *V $\mathbb{Z}_p \setminus \{0\}$ existuje právě $\frac{p-1}{2}$ kvadratických zbytků a $\frac{p-1}{2}$ kvadratických nezbytků modulo p.*

Legendreův symbol $\left(\frac{a}{p}\right)$ dokážeme přímo vyčíslit díky takzvanému Eulerovu kritériu, které plyne z předchozích uvedených vět:

Věta 1.0.5. *Buď p liché prvočíslo, $a \in \mathbb{Z}$. Pak:*

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

Důkaz: Pokud $p \mid a$, je tvrzení zřejmé. Pro zbylá a máme z (1.0.2): $0 \equiv a^{p-1} - 1 = (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \pmod{p}$, takže $a^{\frac{p-1}{2}} \in \{\pm 1\} \pmod{p}$. Předpokládejme nejprve, že a je kvadratický zbytek modulo p. Pak pro nějaké $x \in \mathbb{Z}$:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1,$$

kde poslední rovnost plyne z (1.0.2). Kvadratických zbytků je právě $\frac{p-1}{2}$ a pro $\frac{p-1}{2}$ zbytků tvrzení platí. Rovnice $x^{\frac{p-1}{2}} = 1$ má v $\mathbb{Z}_p$ nejvýše $\frac{p-1}{2}$ kořenů, kterými jsou právě zbytky, tedy pro nezbytky je $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Za pomocí těchto nástrojů dokážeme určit kvadratické zbytky modulo prvočíslo. Kvadratické zbytky pro mocniny lichého prvočísla p dokážeme ze znalosti zbytků modulo p s trochou práce spočítat, nicméně tím se zabývat nebudeme.

Další důležitou vlastností Legendrova symbolu je multiplikativita.

Věta 1.0.6. *Buď p prvočíslo, $a, b \in \mathbb{Z}$. Pak:*

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Důkaz: Můžeme použít Eulerovo kritérium. Máme:

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

□

Nyní si představíme takzvaný Zákon kvadratické reciprocity. Tuto větu poprvé dokázal Gauss a dokonce ji nazval „zlatou větou“. Sám našel přes 6 důkazů.

Věta 1.0.7. *Buďte p, q různá lichá prvočísla. Pak:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

V této práci žádný důkaz neuvedeme, nicméně vyzdvihněme důkaz pomocí takzvané dekompoziční grupy, podán v [10]. Další známý důkaz je veden přes počítání mřížových bodů v obdélníku za pomocí takzvaného Eisensteinova lemmatu, které tvrdí:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{2|i}^{\frac{p-1}{2}} \lfloor \frac{qi}{p} \rfloor}.$$

Za pomocí tohoto faktu je již důkaz nasnadě. Plný důkaz touto metodou jak pro Zákon kvadratické reciprocity tak i pro Eisensteinovo lemma je k nalezení v [1].

Na konec této sekce si ještě ukážeme jedno hezké lemma o součtech kvadrátů:

Lemma 1.0.8. *Buď $p \equiv -1 \mod 4$ a $a, b \in \mathbb{Z}$, že $p \mid a^2 + b^2$. Pak $p \mid a, b$.*

Důkaz : Předpokládejme, že $p \nmid a, b$. Máme $a^2 \equiv -b^2 \mod p \Rightarrow (\frac{a}{b})^2 \equiv -1 \mod p$, protože $p \nmid b$. Protože $p \equiv -1 \mod 4$, tak $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = -1$. To je spor, s tím, že $(\frac{a}{b})^2 \equiv -1 \mod p$, takže $p \mid a, b$. □

Kvadratické zbytky jsou velmi mocným nástrojem, jejich sílu si ukážeme na pár příkladech:

Příklad 1.0.9. *Nalezněte všechna prvočísla p, pro která má kongruence $x^2 \equiv 15 \mod p$ řešení.*

Řešení: Zřejmě vyhovují $p \in \{2, 3, 5\}$. Pokud jiná prvočísla vyhovují, tak $\left(\frac{15}{p}\right) = 1$. Máme:

$$1 = \left(\frac{15}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot 1}\left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}\cdot 2} = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)(-1)^{\frac{3(p-1)}{2}} = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}},$$

protože p je liché.

Nejprve pro $p \equiv 1 \pmod 4$ máme $1 = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$. Pokud máme $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = 1$, tak $p \equiv 1 \mod 3$ a $p^2 \equiv 1 \mod 5 \Rightarrow p \equiv -1, 1 \mod 5$. Díky Čínské zbytkové větě existuje pro kongruence $p \equiv 1 \pmod 4, p \equiv 1 \pmod 3$ a $p \equiv 1 \pmod 5$ respektive $p \equiv -1 \pmod 5$ právě jedno řešení modulo 60, dohromady budou dvě. Pak již snadno dopočteme $p \equiv 1, 49 \pmod{60}$. Pokud je $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = -1$, tak $p \equiv 1 \pmod 4, p \equiv -1 \pmod 3$ a $p^2 \equiv -1 \pmod 5 \Rightarrow p \equiv 2, 3 \pmod 5$. Spočteme $p \equiv 17, 53 \pmod{60}$.

Nyní mějme $p \equiv -1 \pmod 4$, pak $-1 = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$. Pokud $\left(\frac{p}{3}\right) = 1$ a $\left(\frac{p}{5}\right) = -1$, tak $p \equiv 1 \pmod 3$ a $p \equiv 2, 3 \pmod 5$. Pak dopočteme $p \equiv 7$, resp. $43 \pmod{60}$. Pokud by $\left(\frac{p}{3}\right) = -1$ a $\left(\frac{p}{5}\right) = 1$, tak je $p \equiv -1 \pmod 3$ a $p \equiv 1, -1 \pmod 5$. Pak $p \equiv 11, 59 \pmod{60}$.

Dohromady tedy kongruence má řešení, právě když $p = 2, 3, 5$ a nebo $p \equiv 1, 7, 11, 17, 49, 53, 59 \pmod{60}$. □

Příklad 1.0.10. *(Balkán 1998)*
Řešte v $\mathbb{Z}$ rovnici:

$$x^2 + 4 = y^5.$$

Řešení: Všimneme si, že $5 = \frac{11-1}{2}$. Je tak $y^5 \equiv \left(\frac{y}{11}\right) \in \{\pm 1, 0\} \pmod{11}$. Z původní rovnice pak dopočteme $x^2 \equiv -3, -4, -5$.

Nicméně:

$$\left(\frac{-3}{11}\right) \equiv (-3)^5 \equiv -1 \pmod{11},$$
$$\left(\frac{-4}{11}\right) \equiv (-4)^5 \equiv -1 \pmod{11},$$
$$\left(\frac{-5}{11}\right) \equiv (-5)^5 \equiv -1 \pmod{11},$$

tedy rovnice nemůže mít řešení. □

Příklad 1.0.11. *(iKS, 7. ročník, N5)*
Řešte v prvočíslech p, q rovnici:

$$p^3 + 107 = 2q(17q + 24).$$

Řešení : Pokud je $p = 2$, tak pravá strana je sudá a levá lichá, spor. Dále buď p liché. Pokud je $q = 2$, dopočteme $p = 5$, dále je i q liché. Zřejmě pak 4 nedělí $2q(17q + 34)$, takže pravá strana dává zbytek 2 (mod 4). Musí ho tedy dávat i strana levá a dopočteme $p \equiv -1 \pmod{4}$. Hlavním trikem této úlohy je nyní přičíst k oběma stranám 18, na levé straně budeme mít součet třetích mocnin a na pravé zase součet kvadrátů:

$$(p + 5)(p^2 - 5p + 25) = (5q + 3)^2 + (3q + 3)^2.$$

Protože je $p \equiv -1 \pmod{4}$, tak $p^2 - 5p + 25 \equiv -1 \pmod{4}$. Zřejmě číslo dávající zbytek $-1 \pmod{4}$ má prvočíselného dělitele, který je též $-1 \pmod{4}$, protože $1 \cdot 1 \equiv 1 \pmod{4}$. Existuje proto prvočíslo $r \equiv -1 \pmod{4}$, které dělí levou stranu a proto dělí i pravou:

$$r \mid (5q + 3)^2 + (3q + 3)^2.$$

Nyní dle (1.0.8) platí i:

$$r \mid 5q + 3, 3q + 3 \Rightarrow r \mid (5q + 3) - (3q + 3) = 2q.$$

Je buď $r = 2$, což je spor s $r \equiv -1 \pmod{4}$, nebo $r = q$. Protože $q \mid 5q + 3$, tak $q = 3$, dopočteme $p = 7$. Jedinými řešeními jsou proto $(p, q) = (5, 2), (7, 3)$. □

Tento příklad byl zadán na korespondenčním semináři iKS, který řeší středoškolští studenti, musel proto mít nějaké elementární řešení. Dá se ukázat, že naše nalezená řešení

jsou dokonce jediná celočíselná, to však běžnými metodami zjistíme těžko. Příklad přívádí na světlo otázku: „Co kdybychom daný polynom v q nahradili libovolným polynomem druhého stupně?“ Naprostá většina podobných rovnic nebude mít takové trikové řešení, proto bychom se chtěli nějak obecněji podívat na rovnice podobného typu:

$$ax^2 + bx + c = y^3$$

pro daná a, b, c. Víme, že polynom na levé straně můžeme rozložit, pokud však diskriminant není čtvercem, tak se v rozkladu vyskytne iracionální číslo a s nimi se v klasické teorii čísel těžko manipuluje. Pokud bychom však přesto chtěli pracovat s tímto rozkladem, museli bychom pracovat s číslem $\sqrt{b^2 - 4ac}$, které není nutně celé a někdy ani nemusí být reálné. V dalších kapitolách si zavedeme důležité pojmy z algebraické teorie čísel, díky kterým dokážeme rozšířit racionální čísla o $\sqrt{b^2 - 4ac}$ a získáme těleso $\mathbb{Q}(\sqrt{b^2 - 4ac})$, což si můžeme představit jako množinu, která obsahuje všechna racionální čísla, číslo $\sqrt{b^2 - 4ac}$ a je uzavřená na sčítání a násobení. Nebudeme příliš zabíhat do detailů, budeme spíše uvádět pouze věty důležité při manipulaci s takovými tělesy.

Uvažme již zmíněný příklad:

Příklad 1.0.12. *Řešte v $\mathbb{Z}$ rovnici:*

$$x^2 + 13 = y^3.$$

Známe řešení $(\pm 70, 17)$, nicméně nevíme, zda nemá rovnice řešení, kde absolutní velikost proměnných je moc velká na to, abychom ji v rozumném čase našli. Pomocí znalostí v následujících kapitolách dokážeme rozložit rovnici v tělese $\mathbb{Q}(\sqrt{-13})$ na:

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

a dokážeme s takovými výrazy pracovat. Ukážeme, že v jistém smyslu jsou čísla $x + \sqrt{-13}, x - \sqrt{-13}$ nesoudělná, proto množiny všech násobků $x + \sqrt{-13}$ a $x - \sqrt{-13}$, takzvané ideály $(x + \sqrt{-13}), (x - \sqrt{-13})$ jsou nesoudělné a proto jsou oba třetí mocninou jiného ideálu, kde pak poměrně jednoduchým výpočtem ukážeme, že $(\pm 70, 17)$ je skutečně jediné řešení dané rovnice.

Zmiňme ještě, že křivku $x^2 + a = y^3$ pro $a \in \mathbb{Z} \setminus \{0\}$ nazveme Mordellovu, pojmenovanou po Lousi Mordellu, který studoval jejich celočíselné body. Obecně Mordellovy křivky patří pod eliptické křivky, které mají tvar:

$$x^3 + ax + b = y^2$$

pro $a, b \in \mathbb{Z}$, že křivka není singulární, neboli že sama sebe neprotíná a nemá žádný „hrot“. Tato rovnice se též nazývá Weiestrassovou a Siegel ukazál, že má pouze konečně mnoho celočíselných řešení, konkrétně dokázal horní (exponenciální) hranici pro velikost proměnných x, y, jsou tedy všechna řešení dané Weierstrassovy rovnice teoreticky spočitatelná. Navíc

pouze rok před Siegelovým výsledkem byla dokázáno, že všechny racionální body na eliptické křivce tvoří konečně generovanou grupu (se sčítáním na eliptické křivce). Kromě toho jich dokážeme mnoho spočíst. Lutz a Nagell ukázali, že pokud je racionální bod (x, y) na eliptické křivce konečného řádu, tak je mřížový a buď je $y = 0$ (tedy má řád 2, t.j. je 2-torsní), nebo $y^2 \mid 4a^3 + 27b^2$, což je diskriminant daného kubického polynomu. Pokud diskriminant není nulový, což je podmínka nesingularity, tak existuje pouze konečně mnoho bodů konečného řádu. Ku příkladu $(70, 13)$ je bod nekonečného řádu na $x^2 + 13 = y^3$ a tato křivka nemá žádný bod konečného řádu. Za pomocí sčítání bodů na křivce dokážeme spočíst několik racionálních bodů, pokud „zdvojnásobíme“ bod $(70, 13)$ naší křivce, tak získáme racionální bod $(\frac{22858837}{2744000}, \frac{85289}{19600})$ a můžeme takto najít hned několik netriviálních racionálních bodů.

Zjevně u většiny křivek budou existovat mřížové a racionální body nekonečného řádu. Nalezení všech těchto bodů je řádově obtížnější problém a vyžaduje již hlubší poznatky o eliptických křivkách. K uvedení do studia eliptických křivek může posloužit [12] či [14], přičemž v druhé publikaci je i uveden důkaz Lutz-Nagellovy věty.

Kapitola 2

Algebraická teorie čísel

V této kapitole se seznámíme se základy algebraické teorie čísel a v dalších kapitolách se zaměříme na rozklady ideálů v číselným tělesech. Po vybudování této teorie budeme mít nástroje na řešení jistých obtížných diofantických rovnic.

Stručně uvedem uvedeme potřebné definice a tvrzení, důkazy spíše nebudou uvedeny. Pro podrobnější úvod to algebraické teorie čísel a i důkazy zmíněných tvrzení se odkazujeme na [8]. Předpokládáme základní znalosti z algebry, například z teorie grup, okruhů a rozšíření těles.

2.1 Základy

Definice 2.1.1. *Buď $\alpha \in \mathbb{C}$ kořenem polynomu $P(x) \in \mathbb{Z}[x]$, pak řekneme, že α je algebraické číslo.*

Definice 2.1.2. *Pokud je navíc $P(x)$ normovaný, řekneme, že α je algebraické celé číslo.*

Definice 2.1.3. *Algebraickým číselným tělesem nazveme libovolné konečné rozšíření racionálních čísel, neboli těleso tvaru $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, kde $\alpha_1, \ldots, \alpha_n$ jsou algebraická čísla.*

Navíc pro libovolné algebraické číselné těleso platí:

Věta 2.1.4. *Buď K algebraické číselné těleso. Pak existuje algebraické celé číslo α takové, že $K = \mathbb{Q}(\alpha)$.*

Definice 2.1.5. *Nechť K je algebraické číselné těleso takové, že $[K : \mathbb{Q}] = n$. Pak řekneme, že K je těleso stupně n.*

Definice 2.1.6. *Buď K těleso stupně 2 nad $\mathbb{Q}$. Pak řekneme, že K je kvadratické těleso.*

Věta 2.1.7. *Buď K kvadratické těleso. Pak $K = \mathbb{Q}(\sqrt{m})$ pro nějaké $m \in \mathbb{Z} \setminus \{0, 1\}$ bezčtvercové, t.j. neexistuje prvočíslo, jehož čtverec dělí m.*

Triviálně je těleso $\mathbb{Q}$ algebraické číselné těleso. Další příklady algebraických číselných těles jsou $\mathbb{Q}(\sqrt{7})$ či $\mathbb{Q}(1+\sqrt[3]{2})$, neboť $\sqrt{7}$ a $1+\sqrt[3]{2}$ jsou kořeny po řadě normovaných polynomů x^2-7 a x^3-3x^2+3x-3. Z těchto tří těles je pouze $\mathbb{Q}(\sqrt{7})$ těleso kvadratické.

V racionálních číslech jsou algebraická celá čísla právě čísla celá, neboť racionální kořeny normovaného polynomu nad $\mathbb{Z}[x]$ jsou vždy celé. V algebraických číselných tělesech můžeme o trochu obecněji říci následující:

Věta 2.1.8. *Buď K algebraické číselné těleso. Pak algebraická celá čísla v tělese K tvoří se sčítáním a násobením okruh $\mathcal{O}_K$.*

Věta 2.1.9. *Buď K číselné těleso, $[K:\mathbb{Q}]=n$. Pak existují $\alpha_1,\ldots,\alpha_n \in K$, že $\mathcal{O}_K = \{a_1\alpha_1+\cdots+a_n\alpha_n | a_1,\ldots,a_n \in \mathbb{Z}\}$.*

Definice 2.1.10. *Čísla $\alpha_1,\ldots\alpha_n$ z předchozí věty nazýváme celočíselnou bází $\mathcal{O}_K$.*

Vraťme se k tělesům $\mathbb{Q}, \mathbb{Q}(\sqrt{7})$ a $\mathbb{Q}(1+\sqrt[3]{2})$. Z našich tří těles je pouze druhé zmíněné těleso je kvadratické. Celočísenou bází tělesa $\mathbb{Q}$ je pouze $\{1\}$, protože $\mathcal{O}_K=\mathbb{Z}$. Celočíselnou bází $\mathbb{Q}(\sqrt{7})$ je $\{1,\sqrt{7}\}$. Dá se ukázat, že celočíselná báze tělesa $\mathbb{Q}(1+\sqrt[3]{2})$ je $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$.

Definice 2.1.11. *Buď R oborem integrity a K těleso, že $R \subseteq K$. Prvek $a \in K$ označíme jako celý nad R, pokud existuje normovaný polynom nad R, jehož kořenem je a.*

Věta 2.1.12. *Buď R oborem integrity a K těleso, že $R \subseteq K$. Množina všech prvků $a \in K$ celých nad R tvoří podokruh K. Tento okruh nazveme celým uzávěrem R v tělese K.*

Definice 2.1.13. *Buď R obor integrity a K těleso, že $R \subseteq K$. Pokud je K podílovým tělesem R a R je svým celým uzávěrem v K tak řekneme, že R je celouzavřený obor.*

Okruh celých čísel je celouzavřený, neboť jak už jsme zmínili, jeho celým uzávěrem v tělese racionálních čísel je právě $\mathbb{Z}$.

2.2 Ideály

V elementární teorii číslech často klademe důraz na množinu násobku nějakého prvočísla, jako jsou například sudá čísla. Víme, že pro dvě sudá čísla a,b je i $a-b$ sudé číslo a pro libovolné celé číslo x a sudé číslo a je $x\cdot a$ sudým číslem. Analogické vlastností mají množiny všech násobků daného čísla. V číselných okruzích si můžeme zavést množiny s podobnými vlastnosti, jen násobky nemusí být celočíselné a nemusí být násobky celých čísel.

Definice 2.2.1. *Buď $(\mathcal{I},+)$ neprázdná podgrupa aditivní podgrupy okruhu R, že pro každé $a \in \mathcal{I}$, $r \in R$ je $r\cdot a$, resp. $a\cdot r \in \mathcal{I}$. Pak $\mathcal{I}$ nazveme ideálem R.*

Ideál nazveme pravým resp. levým, pokud $r\cdot a \in \mathcal{I}$ resp. $a\cdot r \in \mathcal{I}$. Pokud platí $r\cdot a \in \mathcal{I}$ a zároveň $a\cdot r \in \mathcal{I}$ pro každá vyhovující a,r, nazveme ideál oboustranným. V této práci

však pracujeme pouze nad komutativními okruhy, tedy pravé a levé ideály rozlišovat nebudeme.

Jak jsme již nastínili, množina násobků libovolného celého k, značena (k), tvoří ideál v $\mathbb{Z}$. V okruhu $\mathbb{Z}[i] = \{a+bi|a,b \in \mathbb{Z}\}$ tělesa $\mathbb{Q}(i)$ obsahuje ideál $(2+i)$ všechna čísla tvaru $k(2+i)$ pro celé k, ale také například číslo 5, neboť $(2+i)(2-i) = 5$.

Definice 2.2.2. *Mějme ideál $\mathcal{I}$ okruhu R. Pokud je generovaný jediným prvkem v R řekneme, že je hlavní.*

Abychom mohli dále pokračovat, potřebujeme si zadefinovat, jak se sčítají a násobí ideály:

Definice 2.2.3. *Buďte $\mathcal{I}, \mathcal{J}$ ideály okruhu R. Pak jejich součet a součin definujeme následovně:*

- $\mathcal{I} + \mathcal{J} = \{a + b|a \in \mathcal{I}, b \in \mathcal{J}\}$,
- $\mathcal{I} \cdot \mathcal{J} = \{\sum_{i=1}^{n} a_i b_i | a_i \in \mathcal{I}, b_i \in \mathcal{J}, n \in \mathbb{N}\}$.

Důležitou vlastností součtu a součinu ideálů je, že výsledkem je též ideál. Pro sčítání je to poměrně jednoduché, pokud $a, b \in \mathcal{I}, c \in \mathcal{J}$, tak $a + c, b + c \in \mathcal{I} + \mathcal{J}$, ale též $a + b \in \mathcal{I}, 2c \in \mathcal{J}$, protože jsou to ideály, takže $(a+c)+(b+c) = a+b+2c = (a+b)+2c \in \mathcal{I}+\mathcal{J}$. Též pro vyhovující $k : ka, kb \in \mathcal{I}, kc \in \mathcal{J} \Rightarrow k(a + b + 2c) \in \mathcal{I} + \mathcal{J}$, je tak součet našich ideálů též ideálem. Analogicky se ukáže, že součinem dvou ideálů je taktéž ideál.

Poznamenejme, že ideály okruhu R tvoří se sčítáním i s násobením monoid (operace uvažujeme dle definice výše). Pro sčítání je to celkem zřejmé, asociativita $(\mathcal{I} + \mathcal{J}) + \mathcal{K} = \{a + b + c|a \in \mathcal{I}, b \in \mathcal{J}, c \in \mathcal{K}\} = \mathcal{I} + (\mathcal{J} + \mathcal{K})$ jistě platí a neutrální prvek je $(0) = \{0\}$. Násobení ideálů je taktéž asociativní, neboť $(\mathcal{I} \cdot \mathcal{J}) \cdot \mathcal{K} = \{\sum_{i=1}^{n} a_i b_i c_i | a_i \in \mathcal{I}, b_i \in \mathcal{J}, c_i \in \mathcal{K}, n \in \mathbb{N}\} = \mathcal{I} \cdot (\mathcal{J} \cdot \mathcal{K})$ a neutrální prvek je vždy celý okruh R.

Součin dvou hlavních ideálů okruhu $\mathcal{O}_K$ dokážeme snadno přímo určit a ukážeme si to ve čtvrté kapitole. V tento moment nás přesný výsledek nicméně tolik nezajímá, bude nám stačit pouze následující tvrzení:

Věta 2.2.4. *Součinem dvou hlavních ideálů je též hlavní ideál.*

Když pracujeme s násobením ideálů, tak jistě čtenáře může napadnout idea mocnění ideálu, tudíž následující definice nepřekvapí:

Definice 2.2.5. *Nechť je K algebraické číselné těleso a $\mathcal{I}$ je ideál $\mathcal{O}_K$, $k \in \mathbb{N}$. Potom definujeme mocninu ideálu $\mathcal{I}^k$ následovně:*

$$\mathcal{I}^k = \underbrace{\mathcal{I} \cdot \mathcal{I} \cdots \mathcal{I}}_{k},$$

kde násobení ideálů bereme v souladu s (2.2.3).

Na konec si ještě definujme lomené ideály:

Definice 2.2.6. *Nechť je K algebraické číselné těleso a $\mathcal{I}$ je podgrupa K se sčítáním. Pokud existuje $m \in \mathcal{O}_K$, že $m\mathcal{I}$ je ideál $\mathcal{O}_K$, řekneme, že $\mathcal{I}$ je lomený ideál K. Tento ideál budeme značit $\frac{\mathcal{I}}{m}$.*

Ku příkladu ideál $\left(\frac{3}{2}\right)$ je lomený ideál $\mathbb{Q}$, neboť $2\left(\frac{3}{2}\right) = (3)$.

2.3 Normy

V řešení příkladů budeme rozkládat ideály na prvoideály. Jak za chvíli uvidíme, znalost normy ideálu nám v tomto hodně pomůže.

Definice 2.3.1. *Ať α je algebraické číslo a $P_\alpha(x)$ jeho minimální polynom nad $\mathbb{Q}$. Označme $\alpha, \alpha_2, \ldots, \alpha_n$ všechny komplexní kořeny P_α. Pak řekneme, že $\alpha, \alpha_2, \ldots, \alpha_n$ jsou konjugáty α.*

Definice 2.3.2. *Ať K je algebraické číselné těleso stupně n a $\alpha \in K$, jehož minimální polynom je stupně k. Pak normou nenulového čísla α rozumíme:*

$$N(\alpha) = (\alpha\alpha_2 \cdots \alpha_k)^{n/k}$$

a navíc $N(0) = 0$.

Z přechozí definice též plyne, že normu prvku α dokážeme poměrně snadno spočíst ze znalosti minimálního polynomu nad daným tělesem. Dá se navíc ukázat, že vždy k dělí n, neboli je norma racionálním číslem, případně celým, je-li číslo celé algebraické. Nikdy nebudeme pracovat s více tělesy zaráz, tedy vždy budeme vědět, v kterém tělese normu bereme a budeme psát pouze $N(\alpha)$.

Pro příklad mějme $\mathbb{Q}(\sqrt{2})$. Čísla $2, \sqrt{2}, 1 + 2\sqrt{2}$ mají normy $N(2) = 4, N(\sqrt{2}) = -2, N(1+2\sqrt{2}) = -7$, neboť jejich minimální polynomy jsou po řadě $x-2, x^2-2, x^2-2x-7$. V kapitole (4) si ukážeme, jak zjistit normu čísla $a + b\sqrt{m}$ v tělese $\mathbb{Q}(\sqrt{m})$ bez potřeby znalosti minimálního polynomu, tato znalost pro nás nyní není podstatná.

Dá se ukázat, že norma v číselné tělese je multiplikativní, neboli:

Věta 2.3.3. *Pro $x, y \in K$ platí $N(x)N(y) = N(xy)$.*

Nyní si definujme normu ideálu:

Definice 2.3.4. *Nechť je $\mathcal{I}$ nenulový ideál okruhu $\mathcal{O}_K$. Pak normou ideálu $N(\mathcal{I})$ rozumíme počet prvků faktorokruhu $\mathcal{O}_K/\mathcal{I}$. Definujeme $N((0)) = 0$.*

Toto číslo je tak celé a až na nulový ideál dokonce přirozené. Pro hlavní ideály platí:

Věta 2.3.5. *Buď K algebraické číselné těleso stupně n a (m) je hlavní ideál K. Pak:*

$$N((m)) = |N(m)|.$$

Pro celá čísla díky této větě dokážeme určit normu snadno:

Důsledek 2.3.6. *Buď K číselné těleso stupně n a m celé číslo. Pak*

$$N((m)) = |m|^n.$$

Nyní si definujme normu lomeného ideálu:

Definice 2.3.7. *Ať jsou $\mathcal{I}, m \in \mathcal{O}_K$, že $\frac{\mathcal{I}}{m}$ je lomený ideál. Pak normu lomeného ideálu definujeme následovně:*

$$N\Big(\frac{\mathcal{I}}{m}\Big) = \frac{N(\mathcal{I})}{N((m))}.$$

Definice 2.3.8. *Pokud pro lomené ideály $\mathcal{A}, \mathcal{B}$ okruhu $\mathcal{O}_K$ existuje ideál $\mathcal{C}$, že $\mathcal{A} = \mathcal{B} \cdot \mathcal{C}$, pak řekneme, že ideál $\mathcal{B}$ dělí $\mathcal{A}$ a značíme $\mathcal{B} \mid \mathcal{A}$.*

Důležitým výsledkem je, že norma ideálů je multiplikativní, neboli:

Věta 2.3.9. *Nechť K je číselné těleso a $\mathcal{A}, \mathcal{B}$ jsou lomené ideály $\mathcal{O}_K$. Pak:*

$$N(\mathcal{A}\mathcal{B}) = N(\mathcal{A})N(\mathcal{B}).$$

Důsledek 2.3.10. *Mějme $\mathcal{A}, \mathcal{B}$ ideály $\mathcal{O}_K$. Pak $\mathcal{A} \mid \mathcal{B} \Rightarrow N(\mathcal{A}) \mid N(\mathcal{B})$.*

2.4 Prvoideály a jednotky

V celých číslech mají speciální význam prvočísla a číslo 1. V číselných tělesech mají podobný význam prvoideály a jednotky.

Definice 2.4.1. *Neprázdný nenulový ideál $\mathcal{P} \subset \mathcal{O}_K$ nazveme prvoideálem, pokud pro $a, b \in \mathcal{O}_K$ platí $a \cdot b \in \mathcal{P} \Rightarrow a \in \mathcal{P} \vee b \in \mathcal{P}$.*

Nadále prvoideály uvažujeme nenulové, neprázdné a negenerující celý okruh.

Věta 2.4.2. *Buď $\mathcal{P}$ prvoideál okruhu $\mathcal{O}_K$. Pak $N(\mathcal{P}) = p^j$ pro nějaké prvočíslo p, $j \in \mathbb{N}$.*

Důsledek 2.4.3. *Buď $\mathcal{P}$ prvoideál, p prvočíslo a $j \in \mathbb{N}$. Pak $N(\mathcal{P}) = p^j \iff \mathcal{P} \mid (p)$.*

V okruhu celých čísel jsou prvoideály právě ideály generované prvočísly, jak napovídá jméno.

Nyní se podívejme, co se stane, když má prvek nebo ideál $\mathcal{O}_K$ prvočíselnou normu:

Věta 2.4.4. *Buď $\alpha \in \mathcal{O}_K$, že pro nějaké prvočíslo p je $N(\alpha) = \pm p$. Pak je α ireducibilní nad K.*

Věta 2.4.5. *Buď $\mathcal{I}$ nenulový ideál $\mathcal{O}_K$, že pro nějaké prvočíslo $p, j \in \mathbb{N}$, je $N(\mathcal{I}) = p^j$. Pak je $\mathcal{I}$ mocnina prvoideálu K.*

Dále si definujeme jednotky.

Definice 2.4.6. *Buď K algebraické číselné těleso. Pak $\alpha \in \mathcal{O}_K$ nazveme jednotkou, pokud má multiplikativní inverzi.*

Důsledek 2.4.7. *Buď K algebraické číselné těleso. Pak $\alpha \in \mathcal{O}_K$ je jednotkou právě pokud $N(\alpha) = \pm 1$.*

Jednotkami v celých číslech jsou právě ta celá a, splňující $a = \pm 1$, neboli ± 1.

2.5 Dedekindovy okruhy

V řešení diofantických rovnic budeme většinou chtít hledat nějaký rozklad. V celých číslech existuje jednoznačný rozklad na prvočísla, to již dávno víme. V Dedekindových okruzích toto obecně neplatí, ku příkladu v okruhu celých algebraických čísel tělesa $\mathbb{Q}(\sqrt{-5})$, se dá vyjádřit $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ dvakrát jako součin různých ireducibilních prvků. Každý ideál Dedekindových okruhů ale jednoznačný rozklad na prvoideály má, což v této práci budeme potřebovat. Pro přesnou definici Dedekindových okruhů potřebujeme ještě definovat Noetherovské okruhy:

Definice 2.5.1. *Okruh R nazveme Noetherovským, jestliže je každý ideál R konečně generovaný.*

Dedekindovy okruhy pak definujeme následovně:

Definice 2.5.2. *Obor integrity R nazveme Dedekindův okruh, jestliže platí:*

- *R je Noetherovský,*
- *Každý prvoideál R je maximální,*
- *R je celouzavřený.*

Jak jsme již zmínili, důležitost Dedekindových okruhů leží v následující větě:

Věta 2.5.3. *Buď R Dedekindův okruh. Pak každý vlastní ideál okruhu R se dá jednoznačně vyjádřit jako součin prvoideálů.*

Pak již nutně platí následující tvrzení:

Důsledek 2.5.4. *Buď R Dedekindův okruh a $\mathcal{A}, \mathcal{B}$ jeho ideály. Pak $\mathcal{B} \mid \mathcal{A}$ právě pokud $\mathcal{B} \subseteq \mathcal{A}$.*

Při řešení příkladů budeme pracovat pouze nad okruhem celých algebraických čísel daného tělesa. Důvod, proč zmiňujeme Dedekindovy okruhy, je pak zřejmý:

Věta 2.5.5. *Buď K číselné těleso a $\mathcal{O}_K$ okruh algebraických celých čísel. Pak $\mathcal{O}_K$ je Dedekindův.*

2.6 Grupa tříd ideálů

Definice 2.6.1. *Nechť K je algebraické číselné těleso a $0 \neq \alpha \in K$. Pak ideál $(\alpha) = \alpha\mathcal{O}_K$ nazveme hlavním lomeným ideálem K.*

Věta 2.6.2. *Množina G_K všech lomených ideálů tělesa K tvoří grupu a množina H_K všech hlavních lomených ideálů K tvoří její podgrupu.*

Definice 2.6.3. *Faktorgrupu $\mathsf{G}_K/\mathsf{H}_K$ nazýváme grupou tříd ideálů tělesa K a značíme ji $Cl(\mathcal{O}_K)$.*

Definice 2.6.4. *Označme $h_K = |Cl(\mathcal{O}_K)|$ řád grupy tříd ideálů tělesa K. Říkáme, že h_K je třídové číslo tělesa K.*

Věta 2.6.5. *Označme $h_K = |Cl(\mathcal{O}_K)|$ řád grupy tříd ideálů tělesa K. Pak h_K je konečné číslo.*

Krom toho, že třídové číslo je konečné, ho dokážeme i shora ohraničit a tak ho pro každé těleso teoreticky spočíst. Třídové číslo je totiž ohraničeno shora takzvanou Hurwitzovou konstantou nebo o trochu silnější Minkowského hranicí. Podrobnosti jeho určení však přesahují tuto práci a jeho konkrétní vyčíslení je obecně obtížné i pro moderní matematiku, proto na zjištění třídového čísla užijeme Wolfram Mathematica. Postup výpočtu třídového čísla je s četnými příklady uveden například v [4] či [11].

Neutrálním prvkem této grupy jsou právě hlavní ideály okruhu $\mathcal{O}_K$, tedy můžeme psát následující výsledek.

Věta 2.6.6. *Ať K je algebraické číselné těleso a h_K jeho třídové číslo a $\mathcal{I}$ je ideál $\mathcal{O}_K$. Pak je $\mathcal{I}^{h_K}$ hlavní ideál.*

Pokud je $h_K = 1$, tak řekneme, že je třídové číslo K triviální. V takovém případě je každý ideál okruhu $\mathcal{O}_K$ hlavní a každý prvek lze jednoznačně rozložit na ireducibilní prvky. Pokud je h_K vyšší, tak každý prvek již nemá jednoznačný rozklad a některé ideály nemusí být hlavní.

Například v tělese $K = \mathbb{Q}(\sqrt{-5})$, kde je $h_K = 2$, jsme si ukázali rozklad 6 dvakrát jako součin různých ireducibilních prvků. Každý ideál $\mathcal{O}_K$ sice není hlavní, nicméně součin každých dvou nehlavních ideálů již hlavním ideálem je. Sice platí rovnost ideálů $(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$, ale žádný z těchto ideálů není prvoideálem. Rozklad na prvoideály jednotlivých ideálů je následující:

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

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

takže ideál (6) má jednoznačný rozklad na prvoideály, což je $(2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.

Důsledkem předchozí věty a (2.2.4) je:

Věta 2.6.7. *Ať K je algebraické číselné těleso a h_K jeho třídové číslo. Pokud $\mathcal{I} \in \mathcal{O}_K$ je ideál, že pro $k \in \mathbb{N}, \mathcal{D}(k, h_K) = 1$ je $\mathcal{I}^k$ hlavní ideál, pak je $\mathcal{I}$ hlavní ideál.*

V kapitole (5) se budeme zabývat pouze příklady, kde je exponent u $\mathcal{I}^k$ nesoudělný s h_K. Případ, kdy je exponent ideálu soudělný s třídovým číslem je podrobně rozebírán v [4] v sekci 4.6.3 při řešení příkladu $x^2 - 79 = y^3$.

Kapitola 3

Diofantické rovnice

Určení jednotek kvadratického tělesa nebo nalezení celočíselných řešení jistých obtížných diofantických rovnic, jakou je například:

$$7 = 5a^3 + 138a^2b + 1290ab^2 + 3956b^3,$$

je pro nás v tento moment prakticky nemožné. Vybaveni arsenálem, který obsahuje tato kapitola, však již podobným úkolům budeme schopni čelit.

3.1 Pellova rovnice

Jednou z nejznámějších diofantických rovnic je právě Pellova. Známe ji již přes tisíc let, studoval ji už indický matematik Brahmagupta. V 17. století ji podrobně studovali matematici jako Pierre Fermat a William Brouncker, nicméně jméno nosí po anglickému matematikovi Johnu Pellovi, když si Leonhard Euler Brounckera a Pella mylně zaměnil a nazval rovnici Pellovou.

Definice 3.1.1. *Buď $m \in \mathbb{N}$ bezčtvercové číslo. Pak rovnici:*

$$x^2 - my^2 = 1$$

nazveme Pellovou.

Definice 3.1.2. *Pellova rovnice má řešení $(\pm 1, 0)$, toto řešení nazýváme triviálním řešením.*

Věta 3.1.3. *Pellova rovnice má netriviální řešení v $\mathbb{N}$.*

Všechna řešení Pellovy rovnice jsou parametrizovatelné na základě je tzv. fundamentálnáho řešení:

Definice 3.1.4. *O řešení $(a, b) \in \mathbb{N}^2$ Pellovy rovnice řekneme, že je fundamentální, pokud $a + b\sqrt{m}$ je nejmenší přes všechna netriviální řešení.*

Věta 3.1.5. *Buď (a, b) fundamentální řešení Pellovy rovnice $x^2 - my^2 = 1$. Pak všechna jiná netriviální řešení $(\pm x, \pm y)$ splňují:*

$$x + y\sqrt{m} = (a + b\sqrt{m})^n$$

pro nějaké $n \in \mathbb{N}$, kde $\pm$ se mohou lišit.

Příklad 3.1.6. *Řešme v $\mathbb{Z}$ rovnici:*

$$x^2 - 2y^2 = 1.$$

Řešení: Rovnice je Pellova, takže má triviální řešení $(\pm 1, 0)$. Vidíme, že rovnici splňují čísla $(3, 2)$. Všechny dvojice přirozených čísel (x, y), že $x+y\sqrt{2} < 3+2\sqrt{2}$ jsou $(1, 1), (2, 1), (3, 1), (4, 1), (1, 2), (2, 2), (1, 3)$. Snadno ověříme, že ani jedna z uvedených dvojic rovnici neřeší, takže $(3, 2)$ je fundamentální řešení rovnice $x^2 - 2y^2 = 1$. Všechna $(\pm x, \pm y)$ splňující naši rovnici proto splňují:

$$x + y\sqrt{2} = (3 + 2\sqrt{2})^n.$$

□

Kromě „klasické“ Pellovy rovnice byly podrobně studovány i rovnice Pellova typu, kde 1 je nahrazena nenulovou konstantou. Nejvíce nás bude zajímat tzv. rozšířená Pellova rovnice

Definice 3.1.7. *Buď $m \in \mathbb{N}$ bezčtvercové číslo. Pak rovnici:*

$$x^2 - my^2 = \pm 1$$

nazveme rozšířenou Pellovou.

Věta 3.1.8. *Rozšířená Pellova rovnice má netriviální řešení.*

I rozšířená Pellova rovnice má fundamentální řešení:

Definice 3.1.9. *O řešení $(a, b) \in \mathbb{N}^2$ rozšířené Pellovy rovnice řekneme, že je fundamentální, pokud $a + b\sqrt{m}$ je nejnižší přes všechna netriviální řešení.*

Věta 3.1.10. *Buď (a, b) fundamentální řešení rozšířené Pellovy rovnice $x^2 - my^2 = \pm 1$. Pak všechna jiná řešení $(\pm x, \pm y)$ splňují pro nějaké $n \in \mathbb{N}_0$:*

$$x + y\sqrt{m} = (a + b\sqrt{m})^n,$$

kde se $\pm$ mohou u x, y lišit.

Poznámka 3.1.11. *Záporná Pellova rovnice, tedy $x^2 - my^2 = -1$, nemusí vždy mít řešení. To si ukážeme na následujícím příkladu:*

Příklad 3.1.12. *Buď $p \equiv -1 \pmod 4$ prvočíslo. Ukážeme, že následující záporná rovnice nemá řešení:*

$$x^2 - py^2 = -1.$$

Důkaz: Uvažme rovnici modulo p. Máme pak $x^2 \equiv -1 \pmod{p}$. Nicméně z příkladu (1.0.5) je $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = -1$, což je spor. □

Pokud nalezneme fundamentální řešení dané Pellovy rovnice, tak ji máme vyřešenou. Ta však mohou být velká, příkladem je rovnice $x^2 - 313y^2 = 1$, která má fundamentální řešení:

$$32188120829134849 + 1819380158564160\sqrt{313}.$$

Jistě se proto nedají všechny Pellovy rovnice řešit bez pomoci počítače. Za pomocí strojů však nalezneme řešení poměrně rychle. Bylo dokázáno, že pokud je $a+b\sqrt{m}$ fundamentální řešení příslušné Pellovy rovnice, tak $(a, b) = (c_i, j_i)$, kde c_i, resp. j_i, jsou čitatel, resp. jmenovatel, i-tého parciálního řetězového zlomku čísla $\sqrt{m}$ pro nějaké přirozené i, viz [7]. Existují algoritmy na rychlé násobení velkých čísel, za pomocí kterých dokážeme počítat tyto řetězové zlomky a tak najít fundamentální řešení.

Na řešení netriviálních Pellových rovnic budeme používat Wolfram Mathematica.

3.2 Thueho rovnice

V této práci budeme též hojně využívat takzvané Thueho rovnice.

Definice 3.2.1. *Buď $P(x, y) \in \mathbb{Z}[x]$ homogenní ireducibilní polynom stupně $n \geqslant 3$, $k \in \mathbb{Z} \setminus \{0\}$. Pak rovnici:*

$$P(x, y) = k$$

nazveme Thueho.

Věta 3.2.2. *Thueho rovnice má konečně mnoho celočíselných řešení.*

Tuto větu dokázal jako první právě Axel Thue roku 1909, až o pár desítek let později byla dokázána horní hranice velikosti řešení a vznikly poměrně efektivní algoritmy na řešení těchto rovnic. Horní hranice na $\max(|x|, |y|)$ je totiž polynomiální vzhledem k $|k|$.

Na řešení Thueho rovnic budeme používát Wolfram Mathematica.

Kapitola 4

Číselná tělesa

Při řešení příkladů budeme potřebovat podrobněji prozkoumat tělesa, nad kterými budeme pracovat. Nejprve si představíme několik obecných faktů, která budeme potřebovat při řešení rovnice, v následujících sekcích budeme popisovat jednotlivá tělesa. V této sekci si proto například ukážeme, jak vypadají grupy jednotek příslušných těles, či kolik prvků má grupa tříd ideálů.

V kapitole (5) budeme řešit pouze rozkladem nad tělesy kvadratickými. Jak v nich vypadá okruh algebraických celých čísel popisuje následující věta:

Věta 4.0.1. *Nechť $m \neq 0, 1$ je bezčtvercové celé číslo a $K = \mathbb{Q}(\sqrt{m})$ je algebraické číselné těleso. Pak platí:*

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

Neboť minimální polynom prvku nad kvadratickým tělesem je nejvýše kvadratický, dokážeme snadno díky (2.3.2) popsat normu prvku.

Věta 4.0.2. *Norma prvku $a + b\sqrt{m} \in \mathcal{O}_K$ tělesa $\mathbb{Q}(\sqrt{m})$ vypadá následovně:*

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

Lemma 4.0.3. *Mějme $a, b \in \mathcal{O}_K$, že $(a) = (b)$. Pak $a = ub$, kde u je jednotka $\mathcal{O}_K$.*

Důkaz: Protože $a \in (b)$, je $a \mid b$, analogicky $b \in (a) \Rightarrow b \mid a$, tedy $a \sim b$, takže $a = ub$ pro nějakou jednotku $\mathcal{O}_K$, jelikož je $\mathcal{O}_K$ obor integrity. □

Lemma 4.0.4. *Buďte $a, b \in K$, $\mathcal{I}$ ideál okruhu $\mathcal{O}_K$. Pokud $\mathcal{I} \mid (a), \mathcal{I} \mid (b)$, tak $\mathcal{I} \mid (a \pm b)$.*

Důkaz: Pokud $\mathcal{I} \mid (a), \mathcal{I} \mid (b)$ tak jsou $a, b \in \mathcal{I}$. Pak i $a \pm b \in \mathcal{I}$, takže $\mathcal{I} \mid (a \pm b)$. □

Definice 4.0.5. *Pokud pro dva ideály $\mathcal{I}, \mathcal{J}$ okruhu $\mathcal{O}_K$ existuje prvoideál $\mathcal{P}$, že $\mathcal{P} \mid \mathcal{I}, \mathcal{P} \mid \mathcal{J}$, tak řekneme, že je $\mathcal{P}$ společným dělitelem $\mathcal{I}, \mathcal{J}$. Pokud takový prvoideál neexistuje, tak řekneme, že jsou ideály nesoudělné.*

Pokud máme v $\mathbb{Z}$ dva ideály $(a), (b)$, kde a, b jsou nesoudělná, tak dle Bezoutovy věty existují celá čísla x, y, že $ax + by = 1$. To znamená, že $1 = ax + by \in (a) + (b)$. Pokud se v ideálů nachází 1, tak zřejmě generuje celý okruh, tedy pro nesoudělná a, b je $(a) + (b) = \mathbb{Z}$. Analogicky můžeme formulovat:

Věta 4.0.6. *Ať jsou $\mathcal{I}, \mathcal{J} \in \mathcal{O}_K$ a $\mathcal{C}$ je jejich největší společný dělitel, pak $\mathcal{I} + \mathcal{J} = \mathcal{C}$. Speciálně pokud jsou ideály nesoudělné, tak $\mathcal{I} + \mathcal{J} = \mathcal{O}_K$. Zde bereme největší společný dělitel jako ideál dělící $\mathcal{I}, \mathcal{J}$, který je vzhledem k inkluzi největší.*

Důkaz: Pokud máme $\mathcal{C} \mid \mathcal{I}, \mathcal{J}$, tak neboť je $\mathcal{O}_K$ Dedekindův, tak dle věty (2.5.4) je $\mathcal{I}, \mathcal{J} \subseteq \mathcal{C}$. Pak i $\mathcal{I} + \mathcal{J} \subseteq \mathcal{C}$. Snadno ale nahlédneme, že $\mathcal{I} \mid \mathcal{I} + \mathcal{J}$ a též $\mathcal{J} \mid \mathcal{I} + \mathcal{J}$. Proto $\mathcal{C} \mid \mathcal{I} + \mathcal{J} \Rightarrow \mathcal{C} \subseteq \mathcal{I} + \mathcal{J}$. Pak už $\mathcal{C} = \mathcal{I} + \mathcal{J}$. □

Tento výsledek nebudeme při řešení příkladů využívat, nicméně by byla škoda ho neuvést. Nesoudělná čísla nesdílí žádné prvočinitele, tudíž pokud součin nesoudělných čísel a, b je n-tá mocnina, tak jsou obě $\pm n$-tá mocnina. Analogicky pro nesoudělné ideály platí:

Věta 4.0.7. *Mějme $\mathcal{A}, \mathcal{B}, \mathcal{C}$ nenulové ideály 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, tak existují ideály $\mathcal{I}, \mathcal{J} \in \mathcal{O}_K$, že:

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

Při řešení příkladu budeme muset manipulovat s ideálem generovaným součinem více prvků. Jak jsme slíbili v druhé kapitole, tento výsledek je poměrne jednoduchý, nicméně mocný.

Věta 4.0.8. *Buďte $a, b \in \mathcal{O}_K$. Pak $(ab) = (a)(b)$.*

Důkaz: Jistě $ab \in (a)(b) \Rightarrow (a)(b) \mid (ab)$. Též v libovolném konečném součtu $\sum_{i=1}^{n} a_i b_i$, kde $a_i \in (a), b_i \in (b), n \in \mathbb{N}$ je každý sčítanec dělitelný ab, takže $(ab) \mid (a)(b)$. □

Důsledek 4.0.9. *Buď $a \in \mathcal{O}_K, k \in \mathbb{N}$. pak $(a^k) = (a)^k$.*

Nyní popíšeme, jak vypadá grupa jednotek kvadratického tělesa.

Věta 4.0.10. *Ať je pro bezčtvercové $m > 0, m \not\equiv 1 \pmod 4$: $K = \mathbb{Q}(\sqrt{m})$ těleso a $\mathcal{U}(\mathcal{O}_K)$ je grupa jeho jednotek. Pak je $\mathcal{U}(\mathcal{O}_K) = \{a + b\sqrt{m}\}$, kde (a, b) jsou všechna řešení rozšířené Pellovy rovnice $a^2 - mb^2 = \pm 1$.*

Věta 4.0.11. *Ať je pro bezčtvercové $m < 0 : K = \mathbb{Q}(\sqrt{m})$ těleso a $\mathcal{U}(\mathcal{O}_K)$ je grupa jeho jednotek. Pak je $\mathcal{U}(\mathcal{O}_K)$ dána:*

- $\mathcal{U}(\mathcal{O}_K) = \{\pm 1, \pm i\}$, *pokud* $K = \mathbb{Q}(i)$,
- $\mathcal{U}(\mathcal{O}_K) = \{\pm 1, \pm\omega, \pm(\omega - 1)\}$, *pokud* $K = \mathbb{Q}(\sqrt{3})$ *a* $\omega = \frac{1+\sqrt{-3}}{2}$,
- $\mathcal{U}(\mathcal{O}_K) = \{\pm 1\}$ *jinak.*

4.1 Těleso $\mathbb{Q}(i)$

Prvky tělesa $K = \mathbb{Q}(i)$ jsou ve tvaru $a + bi$, kde $a, b \in \mathbb{Q}$. Dle (4.0.1) je okruh celých algebraických čísel $\mathbb{Z}[i]$. Norma prvku $a + bi, a, b \in \mathbb{Z}$ je podle (4.0.2):

$$N(a + bi) = a^2 + b^2.$$

Grupa jednotek $\mathcal{U}(\mathbb{Z}[i])$ je množina $\{a+bi | a^2+b^2 = \pm 1, a, b \in \mathbb{Z}\}$. Jediná celá čísla splňující:

$$a^2 + b^2 = \pm 1$$

jsou zřejmě $(\pm 1, 0), (0, \pm 1)$, tedy je $\mathcal{U}(\mathbb{Z}[i])$ čtyřprková a je rovna $\{\pm 1, \pm i\}$, což koresponduje s (4.0.11).

Příkazem `NumberFieldClassNumber[Sqrt[-1]]` v programu Wolfram Mathematica získáme že grupa tříd ideálu Cl_K je jednoprvková, což koresponduje s tím, že každý ideál $\mathbb{Z}[i]$ je hlavní.

4.2 Těleso $\mathbb{Q}(\sqrt{-13})$

Prvky tělesa $K = \mathbb{Q}(\sqrt{-13})$ jsou ve tvaru $a + b\sqrt{-13}$, kde $a, b \in \mathbb{Q}$. Dle (4.0.1) je okruh celých algebraických čísel $\mathbb{Z}[\sqrt{-13}]$. Normou prvku $a + b\sqrt{-13}$ je podle (4.0.2):

$$N(a + b\sqrt{-13}) = a^2 + 13b^2.$$

Grupa jednotek $\mathcal{U}(\mathbb{Z}[\sqrt{-13}])$ je množina $\{a+b\sqrt{-13} | a^2+13b^2 = \pm 1, a, b \in \mathbb{Z}\}$. Jediná celá čísla splňující:

$$a^2 + 13b^2 = \pm 1$$

jsou zřejmě $(\pm 1, 0)$, pak je $\mathcal{U}(\mathbb{Z}[\sqrt{-13}]) = \{\pm 1\}$, což koresponduje s (4.0.11).

Příkazem `NumberFieldClassNumber[Sqrt[-13]]` v programu Wolfram Mathematica získáme že grupa tříd ideálu Cl_K je dvojprvková, což znamená, že druhá mocnina libovolného ideálu je hlavní ideál.

4.3 Těleso $\mathbb{Q}(\sqrt{-7})$

Prvky tělesa $K = \mathbb{Q}(\sqrt{-7})$ jsou ve tvaru $a + b\sqrt{-7}$, kde $a, b \in \mathbb{Q}$. Dle (4.0.1) je okruh celých algebraických čísel $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Normou prvku $a + b\frac{1+\sqrt{-7}}{2}$ je podle (4.0.2):

$$N\Big(a + b\frac{1+\sqrt{-7}}{2}\Big) = a^2 + ab + 2b^2.$$

Grupa jednotek $\mathcal{U}(\mathbb{Z}[\frac{1+\sqrt{-7}}{2}])$ je množina $\{a+b\frac{1+\sqrt{-7}}{2}]|a^2+ab+2b^2 = \pm 1, a, b \in \mathbb{Z}\}$. Jediná celá čísla splňující:

$$a^2 + ab + 2b^2 = \pm 1$$

jsou zřejmě pouze $(\pm 1, 0)$, pak je $\mathcal{U}(\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]) = \{\pm 1\}$, což koresponduje s (4.0.11).

Příkazem `NumberFieldClassNumber[Sqrt[-7]]` v programu Wolfram Mathematica získáme že grupa tříd ideálu Cl_K je jednoprvková, což koresponduje s tím, že každý ideál $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ je hlavní.

4.4 Těleso $\mathbb{Q}(\sqrt{86})$

Prvky tělesa $K = \mathbb{Q}(\sqrt{86})$ jsou ve tvaru $a+b\sqrt{86}$, kde $a, b \in \mathbb{Q}$. Dle (4.0.1) je okruh celých algebraických čísel $\mathbb{Z}[\sqrt{86}]$. Normou prvku $a + b\sqrt{86}$ je podle (4.0.2):

$$N(a + b\sqrt{86}) = a^2 - 86b^2.$$

Grupa jednotek $\mathcal{U}(\mathbb{Z}[\sqrt{86}])$ je množina $\{a + b\sqrt{86}|a^2 - 86b^2 = \pm 1, a, b \in \mathbb{Z}\}$. Nejprve si všimněme, že rovnice

$$a^2 - 86b^2 = -1$$

nemá podle příkladu (3.1.12) řešení modulo 43.

Rovnice:

$$a^2 - 86b^2 = 1$$

je Pellova, proto má triviální řešení $(\pm 1, 0)$. Všechna ostatní řešení $(\pm a, \pm b)$ jsou dle (3.1.5) dána:

$$a + b\sqrt{86} = (a_0 + b_0\sqrt{86})^k,$$

kde $k \in \mathbb{N}$ a (a_0, b_0) je fundamentální řešení naší Pellovy rovnice. Toto fundatmentální řešení získáme v Mathematice příkazem `NumberFieldFundamentalUnits[Sqrt[86]]` a jest jím $(10405, 1122)$. Všechna ostatní řešení $(\pm a, \pm b)$ jsou proto ve tvaru:

$$a + b\sqrt{86} = (10405 + 1122\sqrt{86})^k,$$

pro $k \in \mathbb{N}$.

Příkazem `NumberFieldClassNumber[Sqrt[86]]` získáme, že grupa tříd ideálu Cl_K je jednoprvková, což koresponduje s tím, že každý ideál $\mathbb{Z}[\sqrt{86}]$ je hlavní.

Kapitola 5

Příklady

V této kapitole použijeme námi vybudovanou teorii k řešení vybraných diofantických rovnic. Při řešení rovnice (5.1) si ukážeme metodu řešení rovnic rozkladem nad číselnými tělesy a jak ukázat, že rovnice nemá celočíslená řešení. V příkladech (5.2),(5.4) určíme všechna řešení dané rovnice a naučíme se pracovat jak s netriviálním tělesem, tak s tělesem s neobvyklým okruhem celých algebraických čísel.

V příkladu (5.6) se pokusíme zobecnit naše poznatky z přechozích tří rovnic a za omezených podmínek bude zkoumat, kdy nějaký daný normovaný kvadratický trojčlen může být třetí mocninou.

Konečně v příkladu (5.9) budeme znovu řešit rovnici (1.0.11), tentokrát rozkladem v tělese $\mathbb{Q}(\sqrt{86})$ a pro všechna celá čísla. Zatímco naše prvé řešení bylo relativně jednoduché a elegantní, teď už to tak krásné nebude. Budeme muset čelit jak netriviálním společným dělitelům tak faktu, že grupa jednotek $\mathbb{Q}(\sqrt{86})$ je nekonečná.

Příklad 5.0.1. *(Balkán 1998)*
Řešte v $\mathbb{Z}$ rovnici:

$$x^2 + 4 = y^5. \tag{5.1}$$

Řešení: Předpokládejme, že (x, y) je řešením rovnice. Jistě jsou x, y stejné parity. Nejprve předpokládejme, že jsou x, y soudělná, t.j. že je oba dělí prvočíslo p. Pak $p^2 \mid 4 \Rightarrow p = 2$. Máme pak $x = 2x_1, y = 2y_1$ pro $x_1, y_1 \in \mathbb{Z}$, dosazením získáme:

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

Uvažme rovnici modulo 4:

$$x_1^2 \equiv -1 \pmod 4,$$

což je zřejmě spor. Jsou proto čísla nesoudělná, a tak nutně lichá.

Rozložme nyní rovnici (5.1) v okruhu $\mathbb{Z}[i]$ tělesa $\mathbb{Q}(i)$:

$$(x+2i)(x-2i) = y^5.$$

Tuto rovnost můžeme též brát jako rovnost ideálů $\mathbb{Z}[i]$:

$$\Big((x+2i)(x-2i)\Big) = (y^5),$$
$$(x+2i)(x-2i) = (y)^5.$$

Kde jsme využili $(ab) = (a)(b)$ a $(y^5) = (y)^5$ viz věty (4.0.8) a (4.0.9). Nyní ukážeme, že ideály $(x+2i), (x-2i)$ jsou nesoudělné. Předpokládejme naopak, že je oba dělí nějaký prvoideál $\mathcal{P}$. Máme z (4.0.4):

$$\mathcal{P} \mid (4i),$$
$$p \mid N(\mathcal{P}) \mid 16,$$

kde $p \in \mathcal{P}$ je prvočíslo. Nutně je tedy $p = 2$. Nicméně je:

$$N(\mathcal{P}) \mid N((x+2i)) = x^2 + 4,$$

což je liché. Žádný takový prvoideál proto neexistuje a ideály jsou nesoudělné.

Dle (4.0.7) je $(x+2i) = \mathcal{I}^5$, kde $\mathcal{I}$ je ideál $\mathbb{Z}[i]$. Dle sekce (4.1) je $Cl(\mathbb{Z}[i]) = 1$, takže je $\mathcal{I}$ hlavní, $\mathcal{I} = (a+bi)$ pro $a, b \in \mathbb{Z}$. Dle (4.0.3) máme pak:

$$x + 2i = u(a+bi)^5,$$

kde $u \in \{\pm 1, \pm i\}$ jednotka $\mathbb{Z}[i]$.

Ukážeme, že žádná x, y nesplňují (5.1) a to tak, že neexistuje hlavní ideál $\mathcal{I} = (a+bi)$ který by splňoval $(x+2i) = \mathcal{I}^5$, tedy že neexistuje vyhovující celá a, b.

Pokud by pro $u = -1, i$ nebo $-i$ splňovala rovnici $x+2i = u(a+bi)^5$ nějaká $a, b \in \mathbb{Z}$, tak můžeme místo (a, b) uvážit $(-a, -b), (-b, a)$ resp. $(b, -a)$ a získáme řešení $x+2i = (a+bi)^5$. Abychom ukázali, že neexistují vyhovující $a, b \in \mathbb{Z}$ bez újmy na obecnosti stačí uvážit pouze $u = 1$.

Máme pak:

$$x + 2i = (a+bi)^5.$$

Protože $x \in \mathbb{Z}$ a i jsou lineárně nezávislé nad $\mathbb{Q}$, je:

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

tedy $b \mid 2 \Rightarrow b \in \{\pm 1, \pm 2\}$. Pro žádnou z těchto hodnot nevyhovuje žádné celé a.

Zjistili jsme, že $x + 2i$ nemůže být pátou mocninou hlavního ideálu a tedy nemohou rovnici (5.1) vyhovovat žádná celá x, y. ■

Příklad 5.0.2. *Řešte v $\mathbb{Z}$ rovnici:*

$$x^2 + 13 = y^3. \tag{5.2}$$

Řešení: Předpokládejme, že existují vyhovující x, y. Zřejmě jsou čísla různé parity. Pokud by y bylo sudé, tak $x^2 \equiv -1 \pmod 4$, což je spor. Je proto x sudé a y liché. Pokud by je dělilo nějaké prvočíslo p, tak $p^2 \mid 13$, což je spor. Jsou proto čísla nesoudělná.

Rozložme nyní rovnici (5.2) v okruhu $\mathbb{Z}[\sqrt{-13}]$ tělesa $\mathbb{Q}[\sqrt{-13}]$:

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

To můžeme brát i jako rovnost ideálů v $\mathbb{Z}[\sqrt{13}]$:

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

kde opět užíváme větu (4.0.8). Nyní ukážeme, že ideály $(x + \sqrt{-13}), (x - \sqrt{-13})$ jsou nesoudělné. Pokud by existoval prvoideál $\mathcal{P}$, který by dělil oba ideály, tak podle lemmatu (4.0.4) platí:

$$\begin{aligned} \mathcal{P} &\mid (2\sqrt{-13}), \\ \mathcal{P} &\mid (x + \sqrt{-13}), \\ N(\mathcal{P}) &\mid 4 \cdot 13, \\ N(\mathcal{P}) &\mid x^2 + 13 = y^3, \end{aligned}$$

kde y je liché. Proto $N(\mathcal{P}) = \pm 13 \Rightarrow 13 \mid y$. Z (5.2) by však muselo $13 \mid x$, což je spor s nesoudělností x, y. Jsou proto nutně ideály nesoudělné. Z (4.0.7) existuje ideál $\mathcal{I}$ okruhu $\mathbb{Z}[\sqrt{-13}]$, že:

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

Z (4.2) máme $Cl_K = 2$, protože je $\mathcal{I}^3$ hlavní, je i $\mathcal{I}$ hlavní, $\mathcal{I} = (a + b\sqrt{-13})$. Dle (4.0.3) pak:

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

pro jednotku u, kde podle věty (4.0.11) je $u \in \{\pm 1\}$. Vidíme, že pokud (a, b) je řešení pro $u = 1$, tak $(-a, -b)$ je řešení pro $u = -1$.

Mějme proto $u = 1$. Pak:

$$x + \sqrt{-13} = (a + b\sqrt{-13})^3, \tag{5.3}$$

z čehož získáme:

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

takže $b \in \{\pm 1\}$. Dopočteme jediné možné řešení $(\pm 2, -1)$. Dosazením těchto dvojic do (5.3) získáme $x \in \{\pm 70\}$. Pokud tyto hodnotu dosadíme do (5.2), získáme $y = 17$.

Rovnice (5.2) má proto pouze dvě celočíselná řešení, $(\pm 70, 17)$. ■

Příklad 5.0.3. *Řešte v $\mathbb{Z}$ rovnici:*

$$x^2 - x + 2 = y^3. \tag{5.4}$$

Předpokládejme, že existují vyhovující x, y. Nejprve ukážeme, že $x \not\equiv 4 \pmod 7$. Předpokládejme opak, pak $y^3 = x^2 - x + 2 \equiv 0 \pmod 7$, mějme tedy $x = 7k + 4, y = 7l$, pak:

$$\begin{aligned}(7k+4)^2 - (7k+4) + 2 &= (7l)^3,\\ 7k^2 + 7k + 2 &= 49l^3,\end{aligned}$$

což je nemožné.

Rozložme nyní rovnici (5.4) v okruhu celých algebraických čísel $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ tělesa $\mathbb{Q}(\sqrt{-7})$:

$$\Big(x - \frac{1-\sqrt{-7}}{2}\Big)\Big(x - \frac{1+\sqrt{-7}}{2}\Big) = y^3.$$

To můžeme brát i jako rovnost ideálů v $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$:

$$\Big(x - \frac{1-\sqrt{-7}}{2}\Big)\Big(x - \frac{1+\sqrt{-7}}{2}\Big) = (y)^3,$$

kde opět užíváme (4.0.8). Nyní ukážeme, že ideály $\big(x - \frac{1-\sqrt{-7}}{2}\big), \big(x - \frac{1+\sqrt{-7}}{2}\big)$ jsou nesoudělné. Předpokládejme naopak, že existuje prvoideál $\mathcal{P}$, který by dělil oba ideály. Pak dle (4.0.4) platí:

$$\begin{aligned}\mathcal{P} \mid (\sqrt{-7}),\\ N(\mathcal{P}) \mid 7,\end{aligned}$$

ale též:

$$\begin{aligned}\mathcal{P} \mid (2x-1),\\ N(\mathcal{P}) \mid (2x-1)^2.\end{aligned}$$

Pak $2x \equiv 1 \equiv 8 \mod 7 \Rightarrow x \equiv 4 \mod 7$, což není možné. Ideály jsou proto nesoudělné.

Dle (4.0.7) pak máme:

$$\Big(x - \frac{1-\sqrt{-7}}{2}\Big) = \mathcal{I}^3$$

pro ideál $\mathcal{I} \in \mathcal{O}_K$. Dle (4.3) je $Cl_K = 1$, takže $\mathcal{I}$ je hlavní ideál $\mathcal{I} = (a + b\frac{1+\sqrt{-7}}{2})$ pro $a, b \in \mathbb{Z}$.

Z lemmatu (4.0.3) je:

$$x - \frac{1-\sqrt{-7}}{2} = u\Big(a + b\frac{1+\sqrt{-7}}{2}\Big)^3.$$

Pro jednotku u. Podle (4.0.11) je $u \in \{\pm 1\}$. Vidíme, že pokud (a, b) je řešení pro $u = 1$, tak $(-a, -b)$ je řešení pro $u = -1$.

Uvažme proto BÚNO $u = 1$:

$$x - \frac{1 - \sqrt{-7}}{2} = \left(a + b\frac{1 + \sqrt{-7}}{2}\right)^3, \tag{5.5}$$

neboli:

$$\begin{aligned} \frac{1}{2} &= \frac{3}{2}a^2b + \frac{3}{2}ab^2 - \frac{1}{2}b^3, \\ 1 &= b(3a^2 + 3ab - b^2), \end{aligned}$$

takže $b \in \{\pm 1\}$ a dopočteme $(a, b) = (0, -1), (1, -1)$. Z (5.5) máme:

$$x - \frac{1}{2} = a^3 + \frac{3}{2}a^2b - \frac{9}{2}ab^2 - \frac{5}{2}b^3,$$

tedy $x \in \{3, -2\}$ a dopočteme $(x, y) = (3, 2), (-2, 2)$.

Rovnice (5.4) má dvě celočíselná řešení, $(-2, 2), (3, 2)$. ■

Příklad 5.0.4. *Buďte a, b celá čísla, že a je liché a $a^2 < 4b-3$. Pokud je a^2-4b bezčtvercové a počet prvků grupy tříd ideálů tělesa $\mathbb{Q}(\sqrt{a^2 - 4b})$ není dělitelný třemi, tak má rovnice:*

$$x^2 + ax + b = y^3 \tag{5.6}$$

nejvýše dvě celočíselná řešení a pokud $-3a^2 + 12b + 12$ ani $-3a^2 + 12b - 12$ nejsou čtverce, tak nemá žádné. Dokažte a určete všechna řešení.

Řešení: Předpokládejme, že (x, y) pro daná a, b řeší rovnici výše. Nejprve ukážeme, že $2x + a$ a $a^2 - 4b$ jsou nesoudělná čísla. Předpokládejme naopak, že je dělí nějaké prvočíslo p a upravme rovnici (5.6) násobením čtyřmi na:

$$(2x + a)^2 + 4b - a^2 = 4y^3.$$

Máme $p \mid 2x + a, 4b - a^2 \Rightarrow p \mid 4y^3$. Protože je a liché, tak je $4b - a^2$ liché, tudíž je i p liché a tak $p \mid y^3 \Rightarrow p \mid y$. Dle předpokladu pak $p^2 \mid (2x + a)^2$ a $p^3 \mid 4y^3$, což znamená, že $p^2 \mid 4b - a^2$, což je spor s tím, že je $a^2 - 4b$ bezčtvercové. Jsou proto čísla $2x + a$ a $a^2 - 4b$ nesoudělná.

Neboť je a liché, tak $a^2 - 4b \equiv 1 \mod 4$, tudíž okruh celých algebraických prvků tělesa $\mathbb{Q}(\sqrt{a^2 - 4b})$ je dle (4.0.1) $\mathbb{Z}[\frac{1+\sqrt{a^2-4b}}{2}]$. Rozložme v tomto okruhu rovnici (5.6):

$$\left(x - \frac{-a + \sqrt{a^2 - 4b}}{2}\right)\left(x - \frac{-a - \sqrt{a^2 - 4b}}{2}\right) = y^3,$$

což můžeme též brát jako rovnost ideálů v $\mathbb{Z}[\frac{1+\sqrt{a^2-4b}}{2}]$:

$$\Big(x - \frac{-a+\sqrt{a^2-4b}}{2}\Big)\Big(x - \frac{-a-\sqrt{a^2-4b}}{2}\Big) = (y)^3, \tag{5.7}$$

kde užíváme (4.0.9). Ukážeme, že ideály $(x - \frac{-a+\sqrt{a^2-4b}}{2}), (x - \frac{-a-\sqrt{a^2-4b}}{2})$ jsou nesoudělné. Předpokládejme naopak, že existuje prvoideál $\mathcal{P}$, který by dělil oba dva. Dle (4.0.4) je:

$$\begin{aligned} \mathcal{P} \mid (2x+a),\\ \mathcal{P} \mid \sqrt{a^2-4b},\\ N(\mathcal{P}) \mid (2x+a)^2,\\ N(\mathcal{P}) \mid a^2-4b. \end{aligned}$$

Nicméně jsme ukázali, že $2x+a$ a a^2-4b jsou nesoudělné, tudíž žádný takový prvoideál neexistuje a ideály jsou vskutku nesoudělné.

Podle (4.0.9) existuje ideál $\mathcal{I} \in \mathbb{Z}[\frac{1+\sqrt{a^2-4b}}{2}]$, že:

$$\Big(x - \frac{-a+\sqrt{a^2-4b}}{2}\Big) = \mathcal{I}^3.$$

Ideál $\mathcal{I}^3$ je tedy hlavní. Dle předpokladu je mohutnost grupy tříd ideálů nesoudělná se 3, tudíž díky (2.6.7) je $\mathcal{I}$ hlavní ideál, neboli existují $s,t \in \mathbb{Z}$, že $\mathcal{I} = \Big(s + t\frac{1+\sqrt{a^2-4b}}{2}\Big)$, máme proto:

$$\Big(x - \frac{-a+\sqrt{a^2-4b}}{2}\Big) = \Big(s + t\frac{1+\sqrt{a^2-4b}}{2}\Big)^3,$$

takže:

$$x - \frac{-a+\sqrt{a^2-4b}}{2} = u\Big(s + t\frac{1+\sqrt{a^2-4b}}{2}\Big)^3$$

pro nějakou jednotku $u \in \mathbb{Z}[\frac{1+\sqrt{a^2-4b}}{2}]$.

Předpokládali jsme, že $a^2-4b < -3$, tudíž je těleso imaginární a podle (4.0.11) je $u \in \{\pm 1\}$. Pokud (s,t) je řešení pro $u=1$, tak $(-s,-t)$ je řešení pro $u=-1$. Uvažme proto $u=1$:

$$x - \frac{-a+\sqrt{a^2-4b}}{2} = \Big(s + t\frac{1+\sqrt{a^2-4b}}{2}\Big)^3, \tag{5.8}$$

kde porovnáním koeficientů získáme:

$$\begin{aligned} -\frac{1}{2} &= \frac{3}{2}s^2t + \frac{3}{2}st^2 + \frac{a^2-4b}{8}t^3 + \frac{3}{8}t^3,\\ -4 &= t(12s^2 + 12st + (a^2-4b)t^2 + 3t^2), \end{aligned}$$

takže $t \mid 4$.

- $t = 1$:
  Pak $12s^2+12s+a^2-4b+7 = 0$. Toto je kvadratická rovnice v s, tedy máme maximálně dvě řešení pro s a můžeme dopočíst až dvě řešení pro x. Aby měla rovnice celočíselné kořeny, tak má celočíselný diskriminant, tedy:

  $$-3a^2 + 12b - 12$$

  je čtvercem. Spočteme:

  $$s = \frac{-3 \pm \sqrt{-3a^2 + 12b - 12}}{6},$$

  což je celé číslo, neboť $\sqrt{-3a^2 + 12b - 12}$ je liché celé číslo dělitelné třemi. Z (5.8) dopočteme:

  $$x = s^3 + \frac{3}{2}s^2t + \frac{3(a^2-4b)}{4}st^2 + \frac{3(a^2-4b)}{8}t^3 + \frac{3}{4}st^2 + \frac{1}{8}t^3 - \frac{a}{2},$$
  $$x = \frac{\pm(2a^2 - 8b - 1)\sqrt{-3a^2 + 12b - 12} - 9a}{18}.$$

  Pokud je $\sqrt{-3a^2 + 12b - 12}$ celým číslem, tak je dělitelné třemi. Dále je z lichosti a odmocnina lichá, $9a$ a $(2a^2 - 8b - 1)$ taktéž, tudíž 18 dělí čitatel zlomku a x je celé číslo.

- $t = -1$:
  Pak $12s^2 - 12s + a^2 - 4b - 1 = 0$, což má nejvýše dvě řešení. Diskriminantem rovnice je:

  $$-3a^2 + 12b + 12,$$

  což musí být čtvercem. Pokud není, tak nemůžeme najít celočíselné s. Spočteme:

  $$s = \frac{3 \pm \sqrt{-3a^2 + 12b + 12}}{6}.$$

  Z (5.8) dopočteme:

  $$x = s^3 + \frac{3}{2}s^2t + \frac{3(a^2-4b)}{4}st^2 + \frac{3(a^2-4b)}{8}t^3 + \frac{3}{4}st^2 + \frac{1}{8}t^3 - \frac{a}{2},$$
  $$x = \frac{\pm(2a^2 - 8b + 1)\sqrt{-3a^2 + 12b + 12} - 9a}{18},$$

  kde opět snadno ověříme, že x vyjde celé.

- zbylá t:
  t je nutně sudé, tedy každý sčítanec výrazu $t(12s^2+12st+(a^2-4b)t^2+3t^2)$ je dělitelný alespoň 8, což je spor.

Dopočteme, že jediná možná řešení (5.6) jsou:

$$\begin{aligned}
x &= \frac{(2a^2-8b-1)\sqrt{-3a^2+12b-12}-9a}{18}, & y &= \frac{-a^2+4b-1}{3},\\
x &= \frac{-(2a^2-8b-1)\sqrt{-3a^2+12b-12}-9a}{18}, & y &= \frac{-a^2+4b-1}{3},\\
x &= \frac{(2a^2-8b+1)\sqrt{-3a^2+12b+12}-9a}{18}, & y &= \frac{-a^2+4b+1}{3},\\
x &= \frac{-(2a^2-8b+1)\sqrt{-3a^2+12b+12}-9a}{18}, & y &= \frac{-a^2+4b+1}{3},
\end{aligned}$$

takže má rovnice 0,2 či 4 řešení, přičemž čtyři řešení má jen pokud $-3a^2+12b+12$ i $-3a^2+12b-12$ jsou celými čtverci. To znamená, že se dva čtverce liší o 24 a jediná taková čísla jsou $7^2-5^2, 5^2-1$, což je však nemožné, neboť ani jeden ze čtverců není dělitelný 3. Až jeden z výrazů tedy může být čtvercem, tudíž má rovnice nejvýše dvě řešení pro každá dvě vyhovující a, b. ■

Poznámka 5.0.5. *Pokud by bylo a sudé, $a := 2c$, tak můžeme rovnici* (5.6) *upravit na:*

$$(x+c)^2 + b - c^2 = y^3,$$

což je rovnice, která je podrobně řešena v [11].

Příklad 5.0.6. *(iKS, 7. ročník, N5, rozšíření)*
Řešte v celých číslech p, q rovnici:

$$p^3 + 107 = 2q(17q+24). \tag{5.9}$$

Řešení: Předpokládejme, že (p, q) je řešením naší rovnice. Nejprve vidíme, že p je liché číslo. Uvažme rovnici (5.9) jako kvadratickou v q, jejíž diskriminant musí být kvadrát celého čísla a:

$$48^2 + 4 \cdot 34 \cdot (p^3+107) = a^2.$$

Vidíme, že a je sudé, proto mějme $2x = a$ a rovnici upravíme na:

$$x^2 - 4214 = 34p^3. \tag{5.10}$$

Všimněme si, že $43 \nmid p$, neboť jinak $43 \mid x$ a tudíž $43^2 \mid 4214 = 2 \cdot 7^2 \cdot 43$, což je nemožné. Rovnici (5.10) nyní rozložme v okruhu $\mathbb{Z}[\sqrt{86}]$ tělesa $\mathbb{Q}[\sqrt{86}]$:

$$(x+7\sqrt{86})(x-7\sqrt{86}) = (102+11\sqrt{86})(-102+11\sqrt{86})(19+2\sqrt{86})(19-2\sqrt{86})p^3,$$

kde $2 = (102+11\sqrt{86})(-102+11\sqrt{86}), 17 = (19+2\sqrt{86})(19-2\sqrt{86})$ je rozklad na prvočinitele v $\mathbb{Z}[\sqrt{86}]$.

Tuto rovnost můžeme uvážit i jako rovnost ideálů v $\mathbb{Z}[\sqrt{86}]$:

$$(x+7\sqrt{86})(x-7\sqrt{86}) = (102+11\sqrt{86})(-102+11\sqrt{86})(19+2\sqrt{86})(19-2\sqrt{86})(p)^3,$$

což platí díky (4.0.8). Nyní prošetřeme možné prvoideály $\mathcal{P}$, které jsou společnými děliteli ideálů $(x+7\sqrt{86}), (x-7\sqrt{86})$. Dle (4.0.4) a (4.0.2) platí:

$$\begin{aligned} \mathcal{P} &\mid (2x), \\ \mathcal{P} &\mid (14\sqrt{86}), \\ N(\mathcal{P}) &\mid 4x^2, \\ N(\mathcal{P}) &\mid 14^2 \cdot 86, \end{aligned}$$

ale též:

$$N(\mathcal{P}) \mid N((x+7\sqrt{86})) = |x^2 - 4214| = |34p^3|,$$

protože $N((x+7\sqrt{86})) = |x^2-4214|$. Protože je p liché, tak $N(\mathcal{P}) \nmid 4$. Pokud nějaký prvoideál $\mathcal{P}$ dělí oba ideály, tak $N(\mathcal{P}) \mid 2 \cdot 7 \cdot 43$. Víme však, že $43 \nmid p$, takže je buď $N(\mathcal{P}) = 2$ nebo $N(\mathcal{P}) = 7$. Neboť je dle (4.4) grupa tříd prvků našeho tělesa triviální, je $\mathcal{P}$ hlavní. Platí rozklady $2 = (102+11\sqrt{86})(-102+11\sqrt{86}), 7 = (37+4\sqrt{86})(37-4\sqrt{86})$, takže existují až čtyři prvoideály, které mohou dělit oba ideály.

Nejprve předpokládejme, že nějaký jejich společný dělitel je normy 7. Pak $7 \mid 34p^3$, neboli $7 \mid p, p = 7k$ pro $k \in \mathbb{N}$. Pak i $7 \mid x, x = 7l$. Rovnici (5.10) upravíme na:

$$l^2 - 86 = 238k^3.$$

Víme, že $43 \nmid p \Rightarrow 43 \nmid k$ a tedy $43 \nmid l$. Díky $17 = (19+2\sqrt{86})(19-2\sqrt{86})$ rozložíme v $\mathbb{Z}[\sqrt{86}]$ na:

$$(l+\sqrt{86})(l-\sqrt{86}) = (102+11\sqrt{86})(-102+11\sqrt{86})(19+2\sqrt{86})(19-2\sqrt{86})(37+4\sqrt{86})(37-4\sqrt{86})k^3,$$

což též můžeme díky (4.0.9) uvážit jako rovnost ideálů v $\mathbb{Z}[\sqrt{86}]$:

$$(l+\sqrt{86})(l-\sqrt{86}) = (102+11\sqrt{86})(-102+11\sqrt{86})(19+2\sqrt{86})(19-2\sqrt{86})(37+4\sqrt{86})(37-4\sqrt{86})(k)^3. \tag{5.11}$$

Předpokládejme, že ideály $(l+\sqrt{86}), (l-\sqrt{86})$ jsou soudělné, tedy že je dělí prvoideál $\mathcal{Q}$. Pak dle (4.0.4):

$$\begin{aligned} \mathcal{Q} &\mid (2l), \\ \mathcal{Q} &\mid (2\sqrt{86}), \\ N(\mathcal{Q}) &\mid 4l^2, \\ N(\mathcal{Q}) &\mid 4 \cdot 86. \end{aligned}$$

Protože $43 \nmid k$, tak $43 \nmid l$ a $N(\mathcal{Q}) \mid 8$. Pokud by bylo k sudé, tak $16 \mid N((l+\sqrt{86})) = |l^2 - 86| = |238k^3|$ a tak je l sudé a 43 je rozdílem dvou sudých čísel, to je spor. Je proto

k liché a $4 \nmid 238k^3$. Je proto nemožné $N(\mathcal{Q}) = 4, 8$, tedy $N(\mathcal{Q}) = 2$.

Takový prvoideál je až na násobení jednotkou generovaný prvkem konjugovaným s $102 + 11\sqrt{86}$. Dokonce $(102 + 11\sqrt{86}) = (-10405 + 11\sqrt{86})(102 - 11\sqrt{86})$, takže $(102 + 11\sqrt{86}) = (102 - 11\sqrt{86})$, neboli $(2) = (102 + 11\sqrt{86})^2$. Pak upravíme (5.11) na:

$$\Big(\frac{l + \sqrt{86}}{102 + 11\sqrt{86}}\Big)\Big(\frac{l - \sqrt{86}}{102 + 11\sqrt{86}}\Big) = (19 + 2\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})(37 - 4\sqrt{86})(k)^3.$$

Ideály $\left(\frac{l+\sqrt{86}}{102+11\sqrt{86}}\right), \left(\frac{l-\sqrt{86}}{102+11\sqrt{86}}\right)$ jsou pak již nesoudělné. 7 ani 17 nedělí $4 \cdot 86$, takže z každé dvojice ideálů generovaných asociovanými prvky na pravé straně nedělí oba stejný lomený ideál. Máme tak čtyři možnosti:

- $(19 + 2\sqrt{86})(37 + 4\sqrt{86}) \mid \left(\frac{l+\sqrt{86}}{102+11\sqrt{86}}\right)$.

  Pak $(19-2\sqrt{86})(37-4\sqrt{86}) \mid \left(\frac{l-\sqrt{86}}{102+11\sqrt{86}}\right)$. Lomené ideály $\left(\frac{l+\sqrt{86}}{(102+11\sqrt{86})(19+2\sqrt{86})(37+4\sqrt{86})}\right)$, $\left(\frac{l-\sqrt{86}}{(102+11\sqrt{86})(19-2\sqrt{86})(37-4\sqrt{86})}\right)$ jsou pak nesoudělné a jejich součin je třetí mocnina nějakého ideálu, dle (4.0.7) je každý z nich třetí mocninou ideálu. Je nutně:

  $$\left(\frac{l + \sqrt{86}}{(102 + 11\sqrt{86})(19 + 2\sqrt{86})(37 + 4\sqrt{86})}\right) = \mathcal{I}^3$$

  pro nějaký ideál $\mathcal{I}$. Každý ideál okruhu $\mathbb{Z}[\sqrt{86}]$ je podle (4.4) hlavní, $\mathcal{I} = (a+b\sqrt{86})$, a dle (4.0.3) je:

  $$l + \sqrt{86} = u(102 + 11\sqrt{86})(19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3$$

  pro jednotku $u \in \mathbb{Z}[\sqrt{86}]$, které jsou dle (4.4) ve tvaru $\pm s \pm t\sqrt{86} = (10405 + 1122\sqrt{86})^n$ pro nějaké $n \in \mathbb{Z}$. Pokud by $|n| > 1$, tak můžeme napsat u ve tvaru $(10405+1122\sqrt{86})^i v^3$, kde $i \in \{\pm 1, 0\}$. Člen v^3 se započte do třetí mocniny všeobecného prvku, nemusíme jej tedy uvažovat. Protože $(-1)^3 = -1$ a $(10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$, stačí nám uvážit $u = (10405 + 1122\sqrt{86})^i$ pro $i \in \{\pm 1, 0\}$.

  - $u = 1$:
    pak máme:

    $$l + \sqrt{86} = (102 + 11\sqrt{86})(19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

    neboli:

    $$1 = 30601a^3 + 851346a^2b + 7895058ab^2 + 24405252b^3,$$

    což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:
pak máme:

$$l+\sqrt{86} = (10405+1122\sqrt{86})(102+11\sqrt{86})(19+2\sqrt{86})(37+4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = 636806809a^3 + 17716510206a^2b + 164296156722ab^2 + 507873292572b^3,$$

což nemá řešení modulo 7.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:
pak máme:

$$l+\sqrt{86} = (10405-1122\sqrt{86})(102+11\sqrt{86})(19+2\sqrt{86})(37+4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = a^3 + 54a^2b + 258ab^2 + 1548b^3,$$

což je Thueho rovnice, která má řešení $(1, 0)$, z čehož pak dopočteme $l = 18$, neboli $x = 126$, $p = 7$ a řešení naší původní rovnice $(7, 3)$.

- $(19 + 2\sqrt{86})(37 - 4\sqrt{86}) \mid \left(\frac{l+\sqrt{86}}{102+11\sqrt{86}}\right)$.

pak $(19-2\sqrt{86})(37+4\sqrt{86}) \mid \left(\frac{l-\sqrt{86}}{102+11\sqrt{86}}\right)$. Lomené ideály $\left(\frac{l+\sqrt{86}}{(102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})}\right)$, $\left(\frac{l-\sqrt{86}}{(102+11\sqrt{86})(19-2\sqrt{86})(37+4\sqrt{86})}\right)$ jsou pak nesoudělné a jejich součin je třetí mocnina nějakého ideálu, dle (4.0.7) je každý z nich třetí mocninou ideálu. Je nutně:

$$\left(\frac{l+\sqrt{86}}{(102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})}\right) = \mathcal{I}^3$$

pro nějaký ideál $\mathcal{I}$. Každý ideál okruhu $\mathbb{Z}[\sqrt{86}]$ je podle (4.4) hlavní, $\mathcal{I} = (a+b\sqrt{86})$, a dle (4.0.3) je:

$$l+\sqrt{86} = u(102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3,$$

kde u je jednotka. Analogicky k předchozímu případu stačí uvážit $u = (10405 + 1122\sqrt{86})^i$ pro $i \in \{\pm 1, 0\}$.

– $u = 1$:
pak máme:

$$l+\sqrt{86} = (102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = -39a^3 - 1086a^2b - 10062ab^2 - 31132b^3,$$

což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:
pak máme:

$$l+\sqrt{86} = (10405+1122\sqrt{86})(102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = -811959a^3 - 22589394a^2b - 209485422ab^2 - 647562628b^3,$$

což je Thueho rovnice, která nemá řešení.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:
pak máme:

$$l+\sqrt{86} = (10405-1122\sqrt{86})(102+11\sqrt{86})(19+2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = 369a^3 - 10266a^2b + 95202ab^2 - 294292b^3,$$

což nemá řešení modulo 7.

- $(19 - 2\sqrt{86})(37 + 4\sqrt{86}) \mid \left(\frac{l+\sqrt{86}}{102+11\sqrt{86}}\right)$.
Nyní již netřeba opět vše do detailu vysvětlovat, je nutně:

$$\left(\frac{l + \sqrt{86}}{(102 + 11\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})}\right) = \mathcal{I}^3$$

pro nějaký ideál $\mathcal{I}$. Každý ideál okruhu $\mathbb{Z}[\sqrt{86}]$ je podle (4.4) hlavní, $\mathcal{I} = (a+b\sqrt{86})$, a dle (4.0.3) je:

$$l + \sqrt{86} = u(102 + 11\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

kde u je jednotka. Analogicky k předchozímu případu stačí uvážit $u = (10405 + 1122\sqrt{86})^i$ pro $i \in \{\pm 1, 0\}$.

– $u = 1$:
Pak máme:

$$l + \sqrt{86} = (102 + 11\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = 369a^3 + 10266a^2b + 95202ab^2 + 294292b^3,$$

což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:
Pak máme:

$$l+\sqrt{86} = (10405+1122\sqrt{86})(102+11\sqrt{86})(19-2\sqrt{86})(37+4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = 7678929a^3 + 213634374a^2b + 1981163682ab^2 + 6124185388b^3,$$

což je Thueho rovnice, která nemá řešení.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:
Pak máme:

$$l+\sqrt{86} = (10405-1122\sqrt{86})(102+11\sqrt{86})(19-2\sqrt{86})(37+4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = -39a^3 + 1086a^2b - 10062ab^2 + 31132b^3,$$

což nemá řešení modulo 7.

- $(19 - 2\sqrt{86})(37 - 4\sqrt{86}) \mid \left(\frac{l+\sqrt{86}}{102+11\sqrt{86}}\right)$.
Máme:

$$\left(\frac{l+\sqrt{86}}{(102+11\sqrt{86})(19-2\sqrt{86})(37-4\sqrt{86})}\right) = \mathcal{I}^3$$

pro nějaký ideál $\mathcal{I}$. Každý ideál okruhu $\mathbb{Z}[\sqrt{86}]$ je podle (4.4) hlavní, $\mathcal{I} = (a+b\sqrt{86})$, a dle (4.0.3) je:

$$l + \sqrt{86} = u(102 + 11\sqrt{86})(19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

kde u je jednotka. Analogicky k předchozímu případu stačí uvážit $u = (10405 + 1122\sqrt{86})^i$ pro $i \in \{\pm 1, 0\}$.

– $u = 1$:
Pak máme:

$$l + \sqrt{86} = (102 + 11\sqrt{86})(19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = a^3 - 54a^2b + 258ab^2 - 1548b^3,$$

což je Thueho rovnice, která má řešení $(1, 0)$, z čehož dopočteme $l = -18$, takže $k = 1 \Rightarrow p = 7$. Z (5.9) máme řešení $(7, 3)$.

– $u = 10405 + 1122\sqrt{86}$:
Pak máme:

$$l+\sqrt{86} = (10405+1122\sqrt{86})(102+11\sqrt{86})(19-2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3$$

neboli:

$$1 = -9791a^3 - 272394a^2b - 2526078ab^2 - 7808628b^3$$

což nemá řešení modulo 7.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:
Pak máme:

$$l+\sqrt{86} = (10405-1122\sqrt{86})(102+11\sqrt{86})(19-2\sqrt{86})(37-4\sqrt{86})(a+b\sqrt{86})^3,$$

neboli:

$$1 = 30601a^3 - 851346a^2b + 7895058ab^2 - 24405252b^3,$$

což nemá řešení modulo 7.

Nyní již mějme ideály $(l + \sqrt{86})(l - \sqrt{86})$ nesoudělné. Jistě nemůže $2, 7$ ani 17 dělit dělit 1, ze dvojic $(19 + 2\sqrt{86}), (19 - 2\sqrt{86})$ a $(37 + 4\sqrt{86}), (37 - 4\sqrt{86})$ proto nedělí oba ideály ten stejný lomený ideál. Pro součin S ideálů z těchto čtyřech, které dělí $(l + \sqrt{86})$, jsou čtyři možnosti, a lomené ideály $\left(\frac{l+\sqrt{86}}{S}\right), \left(\frac{l+\sqrt{86}}{(14)/S}\right)$ jsou nesoudělné, jejich součin je třetí mocninou ideálu. Díky (4.0.7) je:

$$\left(\frac{l+\sqrt{86}}{S}\right) = \mathcal{I}^3$$

pro nějaký ideál. Dle sekce (4.4) je každý ideál $\mathbb{Z}[\sqrt{86}]$ hlavní, takže $\mathcal{I} = (a + b\sqrt{86})$ pro celá a, b. Je tak dle (4.0.7):

$$\left(\frac{l+\sqrt{86}}{S}\right) = u(a+b\sqrt{86})^3$$

pro jednotku $u = (10405 + 1122\sqrt{86})^i$. Jako předtím můžeme uvažovat $i \in \{\pm 1, 0\}$.

- $S = (19 + 2\sqrt{86})(37 + 4\sqrt{86})$.

$$l + \sqrt{86} = u(19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3.$$

Máme proto tři možnosti:

– $u = 1$:
Pak:
$$l + \sqrt{86} = (19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$
neboli porovnáním koeficientů:
$$1 = 150a^3 + 4173a^2b + 38700ab^2 + 119626b^3,$$
což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:
Pak:
$$l + \sqrt{86} = (10405 + 1122\sqrt{86})(19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$
neboli:
$$1 = 3121452a^3 + 86841465a^2b + 805334616ab^2 + 2489455330b^3,$$
což nemá řešení modulo 7.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:
Pak:
$$l + \sqrt{86} = (10405 - 1122\sqrt{86})(19 + 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$
neboli:
$$1 = 48a^3 - 1335a^2b + 12384ab^2 - 38270b^3,$$
což je Thueho rovnice, která nemá celočíselná řešení.

- $S = (19 + 2\sqrt{86})(37 - 4\sqrt{86})$.
$$l + \sqrt{86} = u(19 + 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3.$$
Stačí prošetřit tři možnosti:

– $u = 1$:
$$l + \sqrt{86} = (19 + 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$
neboli:
$$1 = -2a^3 + 45a^2b - 516ab^2 + 1290b^3,$$
což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 + 1122\sqrt{86})(19 + 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = -3980a^3 - 110727a^2b - 1026840ab^2 - 3174174b^3,$$

což nemá řešení modulo 7.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 - 1122\sqrt{86})(19 + 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = -37640a^3 + 1047177a^2b - 9711120ab^2 + 30019074b^3,$$

což je Thueho rovnice, která nemá celočíselná řešení.

- $S = (19 - 2\sqrt{86})(37 + 4\sqrt{86})$.

$$l + \sqrt{86} = u(19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3.$$

– $u = 1$:

$$l + \sqrt{86} = (19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = 2a^3 + 45a^2b + 516ab^2 + 1290b^3,$$

což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 + 1122\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = 37640a^3 + 1047177a^2b + 9711120ab^2 + 30019074b^3,$$

což je Thueho rovnice, která nemá celočíselná řešení.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 - 1122\sqrt{86})(19 - 2\sqrt{86})(37 + 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = 3980a^3 - 110727a^2b + 1026840ab^2 - 3174174b^3,$$

což nemá řešení modulo 7.

- $S = (19 - 2\sqrt{86})(37 - 4\sqrt{86})$.

$$l + \sqrt{86} = u(19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3.$$

opět stačí prošetřit tři možnosti pro u:

– $u = 1$:

$$l + \sqrt{86} = (19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = -150a^3 + 4173a^2b - 38700ab^2 + 119626b^3.$$

což nemá řešení modulo 7.

– $u = 10405 + 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 + 1122\sqrt{86})(19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = -48a^3 - 1335a^2b - 12384ab^2 - 38720b^3,$$

což je Thueho rovnice, která nemá celočíselná řešení.

– $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$:

$$l + \sqrt{86} = (10405 - 1122\sqrt{86})(19 - 2\sqrt{86})(37 - 4\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$1 = -3121452a^3 + 86841465a^2b - 805334616ab^2 + 2489455330b^3,$$

což nemá řešení modulo 7.

Nyní již předpokládejme, že společný dělitel ideálů $(x+7\sqrt{86}), (x-7\sqrt{86})$ nemá normu 7. Pak jsou buď ideály nesoudělné, nebo má jejich společný dělitel normu 2, tedy je buď $(102 + 11\sqrt{86})$ či $(102 - 11\sqrt{86})$, což je však ten stejný ideál.

Mějme proto $(102 + 11\sqrt{86}) \mid (x + 7\sqrt{86}), (x - 7\sqrt{86})$. Máme pak:

$$\left(\frac{x + 7\sqrt{86}}{102 + 11\sqrt{86}}\right)\left(\frac{x - 7\sqrt{86}}{102 + 11\sqrt{86}}\right) = (10405 - 1122\sqrt{86})(19 + 2\sqrt{86})(19 - 2\sqrt{86})(p)^3,$$

kde $\left(\frac{x+7\sqrt{86}}{102+11\sqrt{86}}\right), \left(\frac{x-7\sqrt{86}}{102+11\sqrt{86}}\right)$ už jsou v $\mathbb{Z}[\sqrt{86}]$ nesoudělné a můžeme zanedbat ideál $(10405 - 1122\sqrt{86})$. Jistě $17 = (19 + 2\sqrt{86})(19 - 2\sqrt{86})$ nedělí jeden z činitelů, neboť by pak $17 \mid 7$,

což je nemožné. Proto $\left(\frac{x+7\sqrt{86}}{102+11\sqrt{86}}\right)$ je dělitelný buď $(19+2\sqrt{86})$ nebo $(19-2\sqrt{86})$. Pokud by $(19+2\sqrt{86}) \mid \left(\frac{x+7\sqrt{86}}{102+11\sqrt{86}}\right)$, tak máme součin dvou nesoudělných lomených ideálů $\left(\frac{x+7\sqrt{86}}{(102+11\sqrt{86})(19+2\sqrt{86})}\right), \left(\frac{x-7\sqrt{86}}{(102+11\sqrt{86})(19-2\sqrt{86})}\right)$ roven třetí mocnině ideálu, každý je proto třetí mocninou.

Poté:

$$(x+7\sqrt{86}) = (102+11\sqrt{86})(19+2\sqrt{86})\mathcal{I}^3$$

pro nějaký ideál $\mathcal{I}$ okruhu $\mathbb{Z}[\sqrt{86}]$. Dle sekce (4.4) je každý ideál $\mathbb{Z}[\sqrt{86}]$ hlavní, existují proto $a, b \in \mathbb{Z}$, že $\mathcal{I} = (a+b\sqrt{86})$. Pak již za pomoci (4.0.3) máme:

$$x+7\sqrt{86} = u(102+11\sqrt{86})(19+2\sqrt{86})(a+b\sqrt{86})^3$$

pro nějakou jednotku $u \in \mathbb{Z}[\sqrt{86}]$, které jsou dle (4.4) ve tvaru $\pm s \pm t\sqrt{86} = (10405+1122\sqrt{86})^n$ pro nějaké $n \in \mathbb{Z}$. Pokud by $|n| > 1$, tak můžeme napsat u ve tvaru $(10405+1122\sqrt{86})^i v^3$, kde $i \in \{\pm 1, 0\}$. Člen v^3 se započte do třetí mocniny všeobecného prvku, nemusíme jej tedy uvažovat. Protože $(-1)^3 = -1$ a $(10405+1122\sqrt{86})^{-1} = 10405-1122\sqrt{86}$, stačí nám uvážit $u = (10405+1122\sqrt{86})^i$ pro $i \in \{\pm 1, 0\}$.

- $u = 1$.
  Pak:
  $$x+7\sqrt{86} = (102+11\sqrt{86})(19+2\sqrt{86})(a+b\sqrt{86})^3,$$
  což po roznásobení a porovnání koeficientů u $\sqrt{86}$ dá:
  $$7 = 413a^3 + 11490a^2b + 106554ab^2 + 329380b^3,$$
  což je Thueho rovnice, jejíž jediné celočíselné řešení je $(-9, 1)$, z čehož dopočteme $x = 92$. Z rovnice $x^2 - 4214 = 34p^3$ máme $p = 5$ a řešení $(5, 2)$ naší původní rovnice.

- $u = 10405+1122\sqrt{86}$.
  Pak:
  $$x+7\sqrt{86} = (10405+1122\sqrt{86})(102+11\sqrt{86})(19+2\sqrt{86})(a+b\sqrt{86})^3,$$
  neboli:
  $$7 = 8594525a^3 + 239107038a^2b + 2217387450ab^2 + 6854401756b^3,$$
  což má řešení modulo 7 jen pokud $7 \mid a, b$, což je však zřejmě nemožné.

- $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$.
  Pak:

  $$x + 7\sqrt{86} = (10405 - 1122\sqrt{86})(102 + 11\sqrt{86})(19 + 2\sqrt{86})(a + b\sqrt{86})^3,$$

  neboli:

  $$7 = 5a^3 - 138a^2b + 1290ab^2 - 3956b^3,$$

  což je analogicky nemožné modulo 7.

Nyní budiž $(19-2\sqrt{86}) \mid \left(\frac{x+7\sqrt{86}}{102+11\sqrt{86}}\right)$, pak $(19+2\sqrt{86}) \mid \left(\frac{x-7\sqrt{86}}{102+11\sqrt{86}}\right)$. Ideály $\left(\frac{x+7\sqrt{86}}{(102+11\sqrt{86})(19-2\sqrt{86})}\right)$, $\left(\frac{x-7\sqrt{86}}{(102+11\sqrt{86})(19+2\sqrt{86})}\right)$ jsou už nesoudělné. Jejich součin je třetí mocninou ideálu, je proto dle (4.0.7):

$$\left(\frac{x + 7\sqrt{86}}{(102 + 11\sqrt{86})(19 - 2\sqrt{86})}\right) = \mathcal{I}^3$$

pro nějaký ideál $\mathcal{I}$. Protože grupa tříd ideálů tělesa $\mathbb{Q}(\sqrt{86})$ je triviální, je $\mathcal{I}$ hlavní, $\mathcal{I} = (a + b\sqrt{86})$. Máme tak:

$$\left(\frac{x + 7\sqrt{86}}{(102 + 11\sqrt{86})(19 - 2\sqrt{86})}\right) = u(a + b\sqrt{86})^3,$$

kde $u = (10405 + 1122\sqrt{86})^i$ je jednotka, stačí uvážit $i \in \{-1, 0, 1\}$.

Pro $u = 1$ máme:

$$x + 7\sqrt{86} = (102 + 11\sqrt{86})(19 - 2\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$7 = 5a^3 + 138a^2b + 1290ab^2 + 3956b^3,$$

což má řešení modulo 7 jen pokud $7 \mid a, b$, což je nemožné.

Pro $u = 10405 + 1122\sqrt{86}$ máme:

$$x + 7\sqrt{86} = (10405 + 1122\sqrt{86})(102 + 11\sqrt{86})(19 - 2\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$7 = 103637a^3 + 2883270a^2b + 26738346ab^2 + 82653740b^3,$$

což má řešení modulo 7 jen pokud $7 \mid a, b$, což je nemožné.

Pro $u = (10405 + 1122\sqrt{86})^{-1} = 10405 - 1122\sqrt{86}$ máme:

$$x + 7\sqrt{86} = (10405 - 1122\sqrt{86})(102 + 11\sqrt{86})(19 - 2\sqrt{86})(a + b\sqrt{86})^3,$$

neboli:

$$7 = 413a^3 - 11490a^2b + 106554ab^2 - 329380b^3,$$

což je Thueho rovnice, která má řešení $(-9, -1)$ a $x = -92$, dopočteme opět $p = 5$ a řešení původní rovnice $(5, 2)$.

Nyní již můžeme předpokládat, že $(x+7\sqrt{86}), (x-7\sqrt{86})$ jsou nesoudělné. Proto $(102+11\sqrt{86})(-102+11\sqrt{86}) = (102+11\sqrt{86})^2 = (2)$ dělí právě jeden z ideálů. Pokud ale $(2) \mid (x \pm 7\sqrt{86})$, tak:

$$4 = N((2)) \mid N((x \pm 7\sqrt{86})) = |x^2 - 4214| = |34p^3|,$$

takže p je sudé. To je nicméně spor, neboť pak je v (5.9) levá strana rovnice lichá a prává sudá.

Rovnice (5.9) má tedy pouze dvě celočíselná řešení, $(5, 2)$ a $(7, 3)$. ■

Závěr

Než se rozloučíme, pojďme se podívat na to, co vlastně dokážeme metodami, které jsme v této práci popsali. Dokážeme řešit jisté rovnice rovnice tvaru $P(x) = y^m$ pro kvadratický polynom P ireducibilní nad $\mathbb{Q}$ a pro m nesoudělná s třídovým číslem okruhu tělesa racionálnách čísel rozšířeného o diskriminant P. Pokud se zamyslíme, jistě nás napadne hned několik rozšíření našich metod. Pokud bychom v (5.6) nahradili 3 obecným celým číslem, mohli bychom s obtížemi studovat rovnice podobného typu, nicméně by byl problém s rozkladem obecného binomického rozvoje. Též bychom se nemuseli omezovat pouze na kvadratická tělesa, v [4] je řešení rovnice vedeno rozkladem nad kubickým tělesem, nicméně z rozkladů nad tělesy vyšších stupňů získáme netriviální soustavy diofantických rovnic, které nedokážeme obecně řešit.

Jediná tělesa vyšších stupňů, nad kterými můžeme smysluplně pracovat, jsou kruhová tělesa, tedy rozšíření racionálních čísel o primitivní odmocniny z jedné. Podrobnějším studiem těchto oborů můžeme mimo jiné dojít k důkazu hlavního i vedlejších Zákonů kvadratické reciprocity, jak bylo provedeno v práci [10]. Tyto obory též můžeme občas využít při řešení těžších olympiádních úloh, viz. [5]. Pokud bychom hledali příspěvěk více zaměřený na řešení Pellovy rovnice rozkladem a teorii okolo, opět s mnoha příklady na procvičení, poté můžeme čtenáře zase odkázat na [3].

Pokud bychom chtěli ještě obtížnější výzvu, můžeme nechat y konstantou a exponent neznámou. Neznámější rovnicí tohoto typu je Ramanujan-Nagellova, která vypadá následovně:

$$x^2 + 7 = 2^n.$$

V $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ můžeme tuto rovnici rozložit na $(x+\sqrt{-7})(x-\sqrt{-7}) = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2}$. Na vyřešení podobných úloh však potřebujeme obratněji pracovat s algebraickými čísly, například modulární aritmetiku a p-valuace algebraických celých čísel, pro zvídavého čtenáře se odkazujeme na [2]. Úlohy podobného typu, kde jsou neznámé i v exponentu, budou mít všechny analogický postup řešení až na nějaké detaily, například jednotky či společné dělitele, s čímž dokážeme pracovat.

Doufám, že čtenář po dokončení této práce pochopil sílu algebraické teorie čísel a možná i popřemýšlel o jejím dalším studiu, neboť tato oblast matematiky je více než zajímavá.

Literatura

[1] BENEŠ, Petr: *Zákony Reciprocity.* Diplomová práce. Brno: Masarykova univerzita, 2010.

[2] DECHENNE, Spencer. The Ramanujan-Nagell Theorem: Understanding the Proof. Dostupné z: http://buzzard.ups.edu/courses/2013spring/projects/spencer-ant-ups-434-2013.pdf

[3] DOLEŽÁLEK, Matěj. Pellova rovnice a kvadratické okruhy. In: PraSe, Organizátoři. PraSe Sborníček 2019 [online]. Sklené, 2019. Dostupné z: `https://prase.cz/soustredeni/sbornik.php?sous=47`.

[4] HRNČIAR, Maroš: *Řešení diofantických rovnic rozkladem v číselných tělesech.* Diplomová práce. Praha: 2015.

[5] HUDEC, Pavel. Odmocniny z jedničky. In: *i*KS, Organizátoři. *i*KS Sborníček 2019 [online]. Kunžak, 2019. Dostupné z: `http://iksko.org/files/sbornik8.pdf`.

[6] KUŘIL, Martin: *Základy teorie grup.*

[7] LENSTRA JR, Hendrik W.: *Solving the Pell Equation.* 2002.

[8] MARCUS, Daniel A.: *Number fields.* New York: Springer-Verlag, 1977.

[9] PERUTKA, Tomáš: *Vyjadřování prvočísel kvadratickými formami.* Středoškolská odborná činnost. Brno: Masarykova univerzita, 2017.

[10] PERUTKA, Tomáš: *Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity.* Středoškolská odborná činnost. Brno: Masarykova univerzita, 2018.

[11] PUPÍK, Petr: *Užití grupy tříd ideálů při řešení některých diofantických rovnic.* Diplomová práce. Brno: Masarykova univerzita, 2009.

[12] RACLAVSKÝ, Marek. *Racionální body na eliptických křivkách.* Diplomová práce. Praha, 2014.

[13] ROSICKÝ, Jiří: *Algebra.* Brno: Masarykova univerzita, 2002.

[14] WASHINGTON, Lawrence C.: *Elliptic Curves: Number theory and cryptography*. Maryland, 2008.

[15] *i*KS - mezinárodní korespondenční seminář [online]. Dostupné z: `iksko.org`.