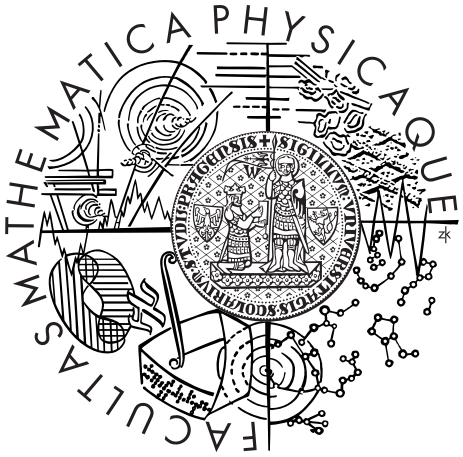
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Bc. Maroš Hrnčiar

Řešení diofantických rovnic rozkladem v číselných tělesech

Katedra algebry

Vedoucí diplomové práce:	Mgr. Vítězslav Kala, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2015

Ďakujem vedúcemu tejto diplomovej práce Víťovi za príkladné vedenie, cenné pripomienky a ochotne poskytovanú pomoc po celý čas pri jej vypracovaní. Osobitné poďakovanie patrí aj priateľke Terezke za odbornú i jazykovú kontrolu.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Řešení diofantických rovnic rozkladem v číselných tělesech

Autor: Bc. Maroš Hrnčiar

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Vítězslav Kala, Ph.D., Mathematisches Institut, Georg-August Universität Göttingen

Abstrakt: Problém řešitelnosti diofantických rovnic je jedním z nejstarších matematických problémů v historii. Postupně se vyvinuly různé přístupy k řešení určitých typů rovnic, z nichž se v práci zabýváme převážně metodou využívající faktorizaci v algebraickém číselném tělese. Myšlenkou této metody je vyjádřit rovnici ve tvaru $L = y^n$, kde levá strana L je součin typicky lineárních faktorů s koeficienty v daném číselném tělese. Při splnění několika předpokladů potom můžeme každý z faktorů napsat jako n–tou mocninu. Klíčovou roli při aplikaci metody hraje struktura číselných těles, proto neoddělitelnou součást práce tvoří přehled algebraické teorie čísel. Kromě výkladu obecné teorie jsou zde uvedené i výpočty v jednotlivých kvadratických a kubických tělesech popisující jejich vlastnosti. Hlavním předmětem práce je však řešení konkrétních úloh. Například v rovnici $x^2 + y^2 = z^3$ se potýkáme s netriviálními společnými děliteli faktorů v okruhu celistvých prvků, v rovnici $x^3 + 2x + 1 = y^2$ zase dělá problém samotný rozklad v kubickém tělese. Rovnici $x^2 - 2 = y^3$ rozkládáme v tělese $\mathbb{Q}(\sqrt{2})$, kde je náročnější najít grupu jednotek úzce spojenou s řešením Pellovy rovnice. Při zkoumání rovnice $x^2 - 79 = y^3$ má důležitou úlohu třídová grupa číselného tělesa, na jejíž určení je potřebná rozsáhlá výpočetní příprava. Pomocí uvažované metody obvykle převedeme zmíněné diofantické rovnice na Thueho rovnice, které sice často nelze vyřešit elementárně, ale dá se použít známý efektivní algoritmus. Na závěr práce dokážeme několik obecných výsledků souvisejících s řešitelností rovnic tvaru $x^2 - dc^2 = y^n$ v p–adických číslech.

Klíčová slova: diofantická rovnice, faktorizace, číselné těleso, třídová grupa, grupa jednotek

Title: Solving diophantine equations by factorization in number fields

Author: Bc. Maroš Hrnčiar

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Mathematical Institute, University of Göttingen

Abstract: The question of solvability of diophantine equations is one of the oldest mathematical problems in the history of mankind. While different approaches have been developed for solving certain types of equations, this thesis predominantly deals with the method of factorization over algebraic number fields. The idea behind this method is to express the equation in the form $L = y^n$ where L equals a product of typically linear factors with coefficients in a particular number field. Provided that several assumptions are met, it follows that each of the factors must be the n–th power of an element of the field. The structure of number fields plays a key role in the application of this method, hence a crucial part of the thesis presents an overview of algebraic number theory. In addition to the general theoretical part, the thesis contains all the necessary computations in specific quadratic and cubic number fields describing their basic characteristics. However, the main objective of this thesis is solving specific examples of equations. For instance, in the case of equation $x^2 + y^2 = z^3$ we focus on dealing with common factors in the ring of integers, while in the equation $x^3 + 2x + 1 = y^2$ problems occur with factorization over the cubic field itself. When considering the equation $x^2 - 2 = y^3$ and the field $\mathbb{Q}(\sqrt{2})$ it is more complicated to determine a unit group which relies on solutions of Pell's equation. Extensive calculations are needed to describe the class group of the field related to the equation $x^2 - 79 = y^3$. Using the method of factorization over number fields we are usually able to reduce the given diophantine equation to several Thue equations and despite the fact that the latter are often not elementarily solvable, the generally known effective algorithm may be applied. Finally we prove number of statements regarding the equation $x^2 - dc^2 = y^n$ in p–adic numbers.

Keywords: diophantine equation, factorization, number field, class group, unit group

Názov práce: Riešenie diofantických rovníc rozkladom v číselných telesách

Autor: Bc. Maroš Hrnčiar

Katedra: Katedra algebry

Vedúci diplomovej práce: Mgr. Vítězslav Kala, Ph.D., Mathematisches Institut, Georg-August Universität Göttingen

Abstrakt: Problém riešiteľnosti diofantických rovníc je jedným z najstarších matematických problémov v histórii. Postupne sa vyvinulo viacero rôznych prístupov na riešenie určitých typov rovníc, no v práci sa zaoberáme prevažne jednou metódou využívajúcou faktorizáciu v algebraickom číselnom telese. Myšlienkou tejto metódy je vyjadriť rovnicu v tvare $L = y^n$, kde ľavá strana L je súčin typicky lineárnych faktorov s koeficientami v danom číselnom telese. Pri splnení niekoľkých predpokladov potom môžeme každý z faktorov napísať ako n–tú mocninu. Kľúčovú rolu pri aplikácii metódy hrá štruktúra číselných telies, preto neoddeliteľnú súčasť práce tvorí prehľad algebraickej teórie čísel. Okrem výkladu všeobecnej teórie sú tu uvedené aj výpočty v jednotlivých kvadratických a kubických telesách popisujúce ich vlastnosti. Hlavným predmetom práce je však riešenie konkrétnych úloh. Napríklad v rovnici $x^2 + y^2 = z^3$ sa potýkame s netriviálnymi spoločnými deliteľmi faktorov v okruhu celistvých prvkov, v rovnici $x^3 + 2x + 1 = y^2$ zasa robí problém samotný rozklad v kubickom telese. Rovnicu $x^2 - 2 = y^3$ rozkladáme v telese $\mathbb{Q}(\sqrt{2})$, kde je náročnejšie nájsť grupu jednotiek úzko spojenú s riešeniami Pellovej rovnice. Pri skúmaní rovnice $x^2 - 79 = y^3$ má dôležitú úlohu triedová grupa číselného telesa, pričom na jej určenie je potrebná rozsiahla výpočetná príprava. Pomocou uvažovanej metódy obvykle prevedieme zmienené diofantické rovnice na Thueho rovnice, ktoré síce často nejde vyriešiť elementárne, ale možno použiť známy efektívny algoritmus. Na záver práce dokážeme niekoľko všeobecných výsledkov súvisiacich s riešiteľnosťou rovníc tvaru $x^2 - dc^2 = y^n$ v p–adických číslach.

Kľúčové slová: diofantická rovnica, faktorizácia, číselné teleso, triedová grupa, grupa jednotiek

Obsah

Úvod

Diofantické rovnice sú polynomiálne rovnice, ktorých premenné môžu nadobúdať iba celočíselné hodnoty. Výraz *Diofantické* je odvodený od helénskeho matematika Diofanta z Alexandrie, ktorý v 3. storočí takéto rovnice študoval. Naviac bol jedným z prvých matematikov vôbec, ktorý zaviedol v algebre symbolizmus, čím si vyslúžil označenie otec algebry. Matematické štúdium rovníc, prípadne sústav rovníc, ktoré načrtol už Diofantos, sa v súčasnosti označuje ako Diofantovská analýza.

Typickými otázkami v Diofantovskej analýze sú:

- dokázanie (ne)existencie riešenia,
- overenie (ne)konečného počtu riešení alebo
- určenie kompletnej množiny riešení danej rovnice či sústavy rovníc.

Problém nájdenia algoritmu na overenie existencie riešenia Diofantickej rovnice je desiatym zo slávnych Hilbertových problémov predložených v r. 1900. Dnes je známe, že hľadaný algoritmus všeobecne neexistuje, no Diofantické rovnice sú predmetom záujmu aj naďalej a je vyvinutých niekoľko metód na aspoň čiastočné riešenie istých typov rovníc.

V práci sa budeme venovať najmä štúdiu metódy riešenia Diofantických rovníc rozkladom v algebraických číselných telesách. Myšlienka rozkladu bola historicky základnou myšlienkou pre dôkaz Veľkej Fermatovej vety a tá v prípade, keď exponentom je regulárne prvočíslo, je dokonca prostredníctvom tejto metódy aj dokázaná. Andrew Wiles a Richard Taylor ju následne dokázali pomocou eliptických kriviek a modulárnych foriem v plnej verzii.

Hlavným cieľom práce je podrobne popísať metódu faktorizácie v číselných telesách ako užitočný nástroj na riešenie niektorých Diofantických rovníc a ilustrovať ju na vzorke príkladov odlišného druhu a náročnosti. Napriek rôznym komplikáciam, ktoré sa pri riešení jednotlivých úloh môžu naskytnúť, vo veľkej väčšine prípadov budeme schopní získať kompletnú množinu riešení zadaných rovníc, eventuálne aj spolu s ďalšími súvislosťami. Všetky netriviálne výsledky použité pri riešení budú podložené teóriou algebraických číselných telies (viz [AW03], [IR98], [ME05]) predstavenej na začiatku práce.

Práca môže slúžiť k zoznámeniu sa s priamou aplikáciou algebraickej teórie čísel na riešenie Diofantických rovníc, prevažne eliptických kriviek, no vzhľadom na rozsiahlu praktickú časť je vhodná aj ako zbierka riešených príkladov. Keďže však súčasne poukazuje na vzťahy k známym výsledkom z algebry a matematiky všeobecne, čiastočne sa dotýka aj iných odvetví.

Samotný obsah práce je rozdelený do piatich ucelených kapitol, pričom obsah jednotlivých kapitol je vždy podrobnejšie uvedený na ich začiatku. Na úplnom

konci práce nájdeme zoznam citovanej literatúry a stručný prehľad použitého značenia.

Teoretickú časť predstavuje hlavne Kapitola 1, v ktorej sa zozačiatku venujeme číselným telesám, konečným rozšíreniam racionálnych čísel. V tých následne definujeme okruh celistvých prvkov ako určité zovšeobecnenie celých čísel a prototyp Dedekindovho oboru. Ďalej sa v týchto okruhoch zaoberáme faktorizáciou na súčin prvočiniteľov, kde stanovíme triedové číslo ako metriku, ktorá hovorí ako ďaleko od jednoznačnosti faktorizácie sa v danom okruhu zrovna nachádzame. Na záver sformulujeme podporné tvrdenia pre určenie grupy jednotiek tohto okruhu, nakoľko rozklad bude vždy daný až na násobky jednotkami. Popri tom vyložíme potrebné pojmy a v podobe tvrdení zhrnieme ich kľúčové vlastnosti, na ktoré sa budeme priebežne v práci odkazovať. K prevzatým tvrdeniam však nebudeme uvádzať dôkazy.

V Kapitole 2 najprv popíšeme metódu na riešenie rovníc pomocou modulárnej aritmetiky a následne ju demonštrujeme na jednoduchých príkladoch. Potom prejdeme k historicky významným rodinám Diofantických rovníc (viz [Coh07]), pričom sa budeme venovať jednej z najdôležitejších rovníc v celej teórii čísel, tzv. Pellovej rovnici, ktorej špeciálne prípady vyriešili už v 4. storočí p.n.l. niektorí grécki a indickí matematici. Pierre Fermat a John Pell následne v 17. storočí prišli na všeobecnú metódu riešenia tejto rovnice. Postupne sa dostaneme aj k ďalšiemu známemu príkladu Diofantických rovníc, tzv. Thueho rovniciam, pomenovaných podľa nórskeho matematika Axela Thueho, ktorý v r. 1909 dokázal, že rovnice tohoto typu majú len konečne veľa riešení. V súčasnosti ich už takisto vieme efektívne určiť, čo využijeme v neskorších aplikáciach. Zvyšok kapitoly je venovaný metóde riešenia rovníc rozkladom v číselných telesách, ktorá tvorí gro celej práce. Spoločne s jej teoretickým popisom ukážeme príklad riešenia rovnice rozkladom v triviálnom číselnom telese $\mathbb{Q}$ a tvrdenia užitočné pri prechode do telies komplikovanejších.

Kapitola 3 pozostáva z detailnej charakteristiky číselných telies. Pozornosť bude venovaná kvadratickým a kubickým číselným telesám, nakoľko v nich budú následne v Kapitole 4 riešené jednotlivé Diofantické rovnice. Niektoré vlastnosti budeme skúmať spoločne pre celú triedu telies, niektoré jednotlivo pre vybrané telesá, ale v uvažovaných číselných telesách finálne vždy vyriešime kľúčové otázky týkajúce sa okruhu celistvých prvkov, triedovej grupy či grupy jednotiek. Cennou pomôckou budú funkcie programu Wolfram Mathematica 10.1 spojené práve s číselnými telesami, ktorých príkazy budeme explicitne uvádzať.

V Kapitole 4, ako už bolo zmienené, sa pozrieme na konkrétne príklady Diofantických rovníc, ktoré riešime metódou faktorizácie v príslušnom číselnom telese. Väčšinu rovníc budeme riešiť v kvadratických telesách, kde ukážeme spektrum úloh od jednoduchých po zložitejšie. Každá bude poukazovať na určité špecifické vlastnosti, ktoré danej úlohe pridávajú na náročnosti – typicky to môže byť spoločný deliteľ v okruhu celistvých prvkov, netriviálna triedová grupa alebo nekonečná grupa jednotiek. Tieto úlohy budú zároveň slúžiť ako návod na riešenie iných rovníc v kvadratických číselných telesách zväčša podobného typu, na ktoré je následne možné uplatniť jeden či kombináciu viacerých tu uvedených postupov. Špeciálne sa zameriame na teleso $\mathbb{Q}(i)$, ktorého okruhom celistvých prvkov sú známe Gaussove celé čísla. Počas riešení sa často dostaneme späť k Thueho rovniciam, z ktorých niektoré vyriešime elementárne a na niektoré použijeme výsledok

Vety 2.3.3. V závere ukážeme príklad rovnice riešenej v kubickom telese, kde zistíme, že jej obtiažnosť je značne vyššia aj za pomoci teórie z predchádzajúcich kapitol. Aby výsledné Thueho rovnice boli čo najjednoduchšie a kvôli prehľadnosti vykladaných postupov významnú časť riešených úloh tvoria eliptické krivky, ale použitie metódy je možné analogicky aj na rovnice vyšších stupňov.

Pri riešení Diofantických rovníc nami zvolenou metódou hrá dôležitú úlohu modulárna aritmetika. Elegantný nástroj ako študovať modulá prvočísel a ich mocnín poskytujú p–adické čísla, preto v Kapitole 5 skúsime aplikovať metódu faktorizácie v číselnom telese na overovanie existencie riešenia rovníc v okruhoch p–adických celých čísel. Prechod medzi kongruenciami a prácou v p–adických celých číslach je daný Henselovým lemmatom, ktoré sformulujeme v niekoľkých verziách v Sekcii 5.2. Konkrétne sa zameriame na rovnicu $x^2 - dc^2 = y^n$, kde d je bezštvorcové celé číslo. S nadobudnutými vedomosťami zároveň na príklade tejto rovnice dokážeme tvrdenia o neexistencii riešenia celých tried Thueho rovníc.

V jednotlivých kapitolách práce využívame znalosti základného kurzu lineárnej algebry (vektorové priestory, sústavy linárnych rovníc, determinanty), všeobecnej a komutatívnej algebry (grupy, okruhy, obory integrity, telesá, ideály, moduly, celistvosť) a elementárnej teórie čísel (kongruencie, kvadratická reciprocita). Naopak vysvetlené sú všetky použité poznatky z algebraickej teórie čísel.

Kapitola 1

Úvod do algebraickej teórie čísel

Algebraická teória čísel je významnou časťou teórie čísel zaoberajúca sa algebraickými štruktúrami spojenými s algebraickými číslami a štúdiom ich vlastností. Historicky bola vyvinutá ako nástroj na riešenie problémov v elementárnej teórii čísel užitočný hlavne pri riešení Diofantických rovníc, na čo bude primárne slúžiť aj v tejto práci.

Cieľom prvej kapitoly bude prehľadne definovať pojmy a spolu s tým formulovať výsledky z algebraickej teórie čísel, ktoré neskôr použijeme pri riešení jednotlivých rovníc. Tým zhrnieme teóriu a základné princípy potrebné k riešeniu Diofantických rovníc rozkladom v číselných telesách, čo obnáša hlavne znalosť okruhu celistvých prvkov daného číselného telesa, triedovej grupy, či grupy jednotiek.

V tejto časti budeme postupovať predovšetkým v zhode s [AW03] a [Mil14], kde je možné nájsť aj dôkazy k použitým tvrdeniam.

1.1 Algebraické číselné teleso

Definícia 1.1.1. (Algebraické číselné teleso)
Algebraickým číselným telesom je každé podteleso $\mathbb{C}$ tvaru $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, kde $\alpha_1, \alpha_2, \ldots, \alpha_n$ sú algebraické čísla.

Definícia 1.1.2. (Algebraické celé číslo)
Algebraické celé číslo je komplexné číslo, ktoré je koreňom nejakého monického polynómu s celočíselnými koeficientami.

Nasledujúce dve tvrdenia hovoria o tom, že číselné telesá a jejich prvky možno uvažovať v zjednodušenom tvare.

Veta 1.1.3. *Ak K je algebraické číselné teleso, potom existuje algebraické celé číslo θ, že $K = \mathbb{Q}(\theta)$.*

Tvrdenie 1.1.4. *Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso a nech n je stupeň minimálneho polynómu $m_{\theta,K}(x)$. Potom ľubovolný prvok K je možné jednoznačne vyjadriť v tvare $c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$, kde $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$.*

Zrejme K je n–dimenzionálny vektorový priestor nad $\mathbb{Q}$ a stupeň K nad Q je n. Ak $n = 2$, hovoríme o K ako o kvadratickom telese, ak $n = 3$, K je kubické teleso, a pod.

1.2 Okruh celistvých prvkov

Algebraické celé čísla tvoria v číselnom telese okruh, celistvý uzáver $\mathbb{Z}$.

Veta 1.2.1. *Nech K je algebraické číselné teleso. Množina všetkých algebraických celých čísel, ktoré patria do K, tvorí okruh (dokonca obor integrity).*

Definícia 1.2.2. (Okruh celistvých prvkov)
Okruh algebraických celých čísel v K nazývame okruhom celistvých prvkov algebraického číselného telesa K a značíme ho $\mathcal{O}_K$.

Ďalej pozorujme nejaké charakteristiky okruhu celistvých prvkov.

Veta 1.2.3. *Ak K je algebraické číselné teleso, potom K je podielové teleso $\mathcal{O}_K$.*

Veta 1.2.4. *Ak K je algebraické číselné teleso, potom $\mathcal{O}_K$ je celistvo uzavretý obor.*

1.3 Diskriminant

Definícia 1.3.1. (Konjugácie α nad K)
Nech $\alpha \in \mathbb{C}$ je algebraické nad K, kde K je podtelesom $\mathbb{C}$. Konjugácie α nad K sú korene minimálneho polynómu $m_{\alpha,K}(x)$.

K nájdeniu okruhu celistvých prvkov v konkrétnych prípadoch potrebujeme zaviesť pojem diskriminantu spolu s jeho základnými vlastnosťami.

Definícia 1.3.2. (Diskriminant n prvkov v algebraickom číselnom telese stupňa n)
Nech K je algebraické číselné teleso stupňa n. Nech $\omega_1, \omega_2, \ldots, \omega_n$ je n prvkov telesa K a nech σ_k ($k = 1,2,\ldots,n$) označujú n rôznych monomorfizmov $K \to \mathbb{C}$. Pre $i = 1,\ldots,n$ nech

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), \ldots, \omega_i^{(n)} = \sigma_n(\omega_i)$$

značia konjugácie ω_i nad K. Potom diskriminant $\{\omega_1, \omega_2, \ldots, \omega_n\}$ je

$$D(\omega_1, \omega_2, \ldots, \omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \ldots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \ldots & \omega_n^{(2)} \\ \vdots & \vdots & \ldots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}^2 .$$

Definícia 1.3.3. (Diskriminant prvku α)
Nech K je algebraické číselné teleso stupňa n, $\alpha \in K$. Definujme diskriminant $D(\alpha)$ ako

$$D(\alpha) = D(1,\alpha,\alpha^2,\ldots,\alpha^{n-1}).$$

Veta 1.3.4. *Nech K je algebraické číselné teleso stupňa n, $\alpha \in K$. Potom*

$$D(\alpha) = \prod_{1 \le i < j \le n} (\alpha^{(i)} - \alpha^{(j)})^2,$$

kde $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(n)}$ sú konjugácie α nad K.

Veta 1.3.5. *Nech K je algebraické číselné teleso stupňa n, $\alpha \in K$. Potom*

$$K = \mathbb{Q}(\alpha) \text{ práve vtedy, keď } D(\alpha) \neq 0.$$

Tvrdenie 1.3.6. *Nech K je algebraické číselné teleso stupňa n.*

- *Ak $\omega_1, \omega_2, \ldots, \omega_n \in K$, potom $D(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{Q}$.*
- *Ak $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$, potom $D(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{Z}$.*
- *Ak $\omega_1, \omega_2, \ldots, \omega_n \in K$, potom $D(\omega_1, \omega_2, \ldots, \omega_n) \neq 0$ práve vtedy, keď $\omega_1, \omega_2, \ldots, \omega_n$ sú lineárne nezávislé nad $\mathbb{Q}$.*

Na záver sekcie ukážme ako diskriminant algebraického čísla čo najefektívnejšie spočítať a jeho súvislosť s diskriminantom minimálneho polynómu.

Veta 1.3.7. *Nech θ je algebraické číslo a $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ sú konjugácie θ nad $\mathbb{Q}$, t.j. korene $f(x) := m_{\theta,\mathbb{Q}}(x)$. Potom*

$$D(\theta) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\theta_i).$$

Definícia 1.3.8. (Diskriminant polynómu)
Nech

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x],$$

kde $n \in \mathbb{Z}_{>0}$ a $a_n \neq 0$. Nech $x_1, x_2, \ldots, x_n \in \mathbb{C}$ sú korene $f(x)$. Diskriminant $f(x)$ definujeme ako

$$\operatorname{disc}(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{C}.$$

Dôsledok 1.3.9. *Nech θ je algebraické číslo a $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ sú konjugácie θ nad $\mathbb{Q}$, t.j. korene $f(x) := m_{\theta,\mathbb{Q}}(x)$. Potom*

$$D(\theta) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\theta_i) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2 =$$

$$= \operatorname{disc}(\prod_{i=1}^{n} (x - \theta_i)) = \operatorname{disc}(m_{\theta,\mathbb{Q}}(x)).$$

1.4 Celistvá báza

Veta 1.4.1. *Okruh celistvých prvkov $\mathcal{O}_K$ algebraického číselného telesa K je najväčší podokruh, ktorý je konečne generovaný ako $\mathbb{Z}$-modul.*

Keďže okruh celistvých prvkov je konečne generovaný ako $\mathbb{Z}$-modul, môžme uvažovať jeho bázu.

Definícia 1.4.2. (Celistvá báza K)
Nech K je algebraické číselné teleso. Bázu $\mathcal{O}_K$ ako $\mathbb{Z}$-modulu nazývame celistvou bázou K.

Síce celistvá báza číselného telesa nie je jednoznačne určená, ale všetky báze jedného telesa majú zhodný diskriminant a zároveň každá ďalšia množina prvkov s rovnakým diskriminantom tvorí takisto bázu. Preto diskriminant ľubovolnej celistvej báze nazveme diskriminantom celého telesa a táto definícia bude korektná.

Tvrdenie 1.4.3. *Nech K je algebraické číselné teleso.*

- *Ak $\{\eta_1, \eta_2, \ldots, \eta_n\}$ a $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ sú dve celistvé báze K, potom platí $D(\eta_1, \eta_2, \ldots, \eta_n) = D(\lambda_1, \lambda_2, \ldots, \lambda_n)$.*
- *Pokiaľ $\{\eta_1, \eta_2, \ldots, \eta_n\}$ je celistvá báza K a $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathcal{O}_K$ tak, že $D(\eta_1, \eta_2, \ldots, \eta_n) = D(\lambda_1, \lambda_2, \ldots, \lambda_n)$, potom $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ je takisto celistvá báza K.*

Definícia 1.4.4. (Diskriminant číselného telesa)
Nech K je algebraické číselné teleso stupňa n a nech $\{\eta_1, \eta_2, \ldots, \eta_n\}$ je celistvá báza K. Potom $D(\eta_1, \eta_2, \ldots, \eta_n)$ nazveme diskriminant K a značíme $d(K)$.

Ďalšie tvrdenie sa nám bude hodiť pri hľadaní okruhu celistvých prvkov v konkrétnych prípadoch, nakoľko pri väčšine nám bude stačiť spočítať diskriminant prvku θ generujúceho číselné teleso a overiť, že to je bezštvorcové celé číslo.

Veta 1.4.5. *Nech K je algebraické číselné teleso a nech $\theta \in \mathcal{O}_K$ tak, že $K = \mathbb{Q}(\theta)$. Potom*

$$D(\theta) = d(K)(\mathcal{O}_K : \mathbb{Z}[\theta])^2,$$

pričom $(\mathcal{O}_K : \mathbb{Z}[\theta]) = |\mathcal{O}_K / \mathbb{Z}[\theta]|$.

Dôsledok 1.4.6. *Nech K je algebraické číselné teleso stupňa n a nech $\theta \in \mathcal{O}_K$ tak, že $K = \mathbb{Q}(\theta)$. Ak $D(\theta)$ je bezštvorcové, potom $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ je celistvá báza K.*

Ak by diskriminant θ bezštvorcový nevyšiel, môžme sa pri hľadaní okruhu celistvých prvkov skúsiť obrátiť na Stickelbergerovu vetu.

Veta 1.4.7. *(Stickelberger)*
Nech K je algebraické číselné teleso. Potom

$$d(K) \equiv 0 \text{ alebo } 1 \pmod 4.$$

1.5 Dedekindov obor

Okruhy celistvých prvkov nie sú vždy Gaussovými obormi, teda nie je v nich zaručená existencia a jednoznačnosť rozkladu prvkov na prvočinitele. Nakoľko by sme ale túto vlastnosť pri riešení rovníc potrebovali, pripomeňme v tejto sekcii pojem Dedekindovho oboru a uvažujme okruh celistvých prvkov ako Dedekindov obor, kde sa ideály na súčin prvoideálov rozkladajú.

Definícia 1.5.1. (Dedekindov obor)
Obor integrity D, ktorý spĺňa nasledujúce tri vlastnosti:

- D je Noetherovský,

- D je celistvo uzavretý a
- každý prvoideál D je maximálnym ideálom,

sa nazýva Dedekindov obor.

Veta 1.5.2. *Ak D je Dedekindov obor, potom každý vlastný ideál oboru D je súčinom prvoideálov a táto faktorizácia je jednoznačná (až na usporiadanie).*

Veta 1.5.3. *Nech K je algebraické číselné teleso a $\mathcal{O}_K$ príslušný okruh celistvých prvkov. Potom $\mathcal{O}_K$ je Dedekindov obor a každý vlastný ideál $\mathcal{O}_K$ môžeme jednoznačne (až na usporiadanie) vyjadriť ako súčin prvoideálov.*

Sekciu ešte doplňme o definíciu lomeného ideálu Dedekindovho oboru a aj na ideáloch zaveďme pre prehľadnosť reláciu deliteľnosti.

Definícia 1.5.4. (Lomený ideál)
Nech D je Dedekindov obor a K jeho podielové teleso. Lomený ideál D je každý nenulový D-podmodul A telesa K, pre ktorý existuje nenulový prvok $r \in D$, že $rA \subseteq D$.

Poznámka. Lomený ideál Dedekindovho oboru D je každý nenulový D-podmodul K, ktorého prvky majú spoločného menovateľa. Možno ho vždy vyjadriť v tvare $A = \frac{1}{r}I$ kde $r \in D \setminus \{0\}$ a I je ideál D.

Definícia 1.5.5. (Deliteľnosť ideálov)
Nech D je Dedekindov obor a A, B sú dva nenulové (lomené) ideály D. Hovoríme, že A delí B (zn. $A \mid B$), ak existuje ideál C taký, že $B = AC$.

Poznámka. Ak $A = \prod_{i=1}^{n} P_i^{a_i}$ a $B = \prod_{i=1}^{n} P_i^{b_i}$, kde $P_1, \ldots, P_n$ sú rôzne prvoideály a $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in \mathbb{Z}$, potom

$$A \mid B \Leftrightarrow a_i \leq b_i,\ i = 1,2,\ldots,n.$$

Veta 1.5.6. *Nech D je Dedekindov obor a A, B sú dva nenulové (lomené) ideály D. Potom*

$$A \mid B \Leftrightarrow B \subseteq A.$$

Definícia 1.5.7. (Komaximálne ideály)
Nech D je Dedekindov obor a I, J sú dva ideály D. Hovoríme, že I a J sú komaximálne, ak

$$I + J = D.$$

Komaximálnym ideálom niekedy hovoríme aj nesúdeliteľné, pretože nemajú žiadne spoločné prvoideály v rozkladoch.

1.6 Normy

Ďalším aspoň čiastočným cieľom bude rozklady niektorých ideálov nájsť. Pre rozpoznávanie prvoideálov budeme potrebovať počítať ich normu, ktorá je veľmi úzko spojená s bežnou normou prvkov.

Definícia 1.6.1. (Norma prvku)

Nech K je algebraické číselné teleso stupňa n, nech $\alpha \in K$ a $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ sú K-konjugácie α. Potom norma α je definovaná ako

$$N(\alpha) = \alpha_1 \alpha_2 \ldots \alpha_n.$$

Veta 1.6.2. *Nech K je algebraické číselné teleso stupňa n a $\alpha, \beta \in K$. Potom*

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

Definícia 1.6.3. (Norma ideálu)

Nech K je algebraické číselné teleso stupňa n a nech $0 \neq I$ je ideál $\mathcal{O}_K$ s generátormi $\{\eta_1, \eta_2, \ldots, \eta_n\}$. Potom norma ideálu I je definovaná ako

$$N(I) = \sqrt{\frac{D(I)}{d(K)}},$$

kde $D(I) = D(\eta_1, \eta_2, \ldots, \eta_n)$.

Tvrdenie 1.6.4. *Nech K je algebraické číselné teleso stupňa n a nech $0 \neq I$ je ideál $\mathcal{O}_K$. Potom $N(I)$ je kladné celé číslo.*

Tvrdenie 1.6.5. *Nech K je algebraické číselné teleso stupňa n a nech $0 \neq c \in \mathbb{Z}$. Potom norma hlavného ideálu $N((c))$ je*

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

Veta 1.6.6. *Nech K je algebraické číselné teleso stupňa n a nech $0 \neq I$ je ideál $\mathcal{O}_K$. Potom*

$$N(I) = (\mathcal{O}_K : I).$$

Definícia 1.6.7. (Norma lomeného ideálu)

Ak $A = \frac{1}{r}I$ je lomený ideál, potom jeho normu definujeme ako

$$N(A) = \frac{N(I)}{N((r))}.$$

Veta 1.6.8. *Nech K je algebraické číselné teleso a nech A, B sú dva nenulové (lomené) ideály v $\mathcal{O}_K$. Potom*

$$N(AB) = N(A)N(B).$$

Veta 1.6.9. *Nech K je algebraické číselné teleso stupňa n a $\mathcal{O}_K$ príslušný okruh celistvých prvkov. Ďalej nech $\alpha \in \mathcal{O}_K$. Potom*

$$N((\alpha)) = |N(\alpha)|.$$

1.7 Prvoideály

Každý prvoideál okruhu celistvých prvkov súvisí s práve jedným prvočíslom.

Veta 1.7.1. *Nech K je algebraické číselné teleso a P prvoideál $\mathcal{O}_K$. Potom existuje práve jedno prvočíslo p také, že*

$$P \mid (p).$$

Veta 1.7.2. *Nech K je algebraické číselné teleso stupňa n, P prvoideál $\mathcal{O}_K$ a p prvočíslo, pre ktoré $P \mid (p)$. Potom*

$$N(P) = p^f,$$

kde $f \in \mathbb{Z}_{>0}$.

Definícia 1.7.3. (Stupeň inercie)
Nech K je algebraické číselné teleso stupňa n, P prvoideál $\mathcal{O}_K$ a p prvočíslo, pre ktoré $P \mid (p)$. Potom $f \in \mathbb{Z}_{>0}$, pre ktoré platí

$$N(P) = p^f,$$

sa nazýva stupeň inercie P v $\mathcal{O}_K$, zn. $f_K(P)$.

Definícia 1.7.4. (Index vetvenia)
Nech K je algebraické číselné teleso stupňa n, P prvoideál $\mathcal{O}_K$ a p prvočíslo, pre ktoré $P \mid (p)$. Potom $e \in \mathbb{Z}_{>0}$, pre ktoré platí

$$P^e \mid (p),\ P^{e+1} \nmid (p),$$

sa nazýva index vetvenia P v K (alebo aj ramifikačný index), zn. $e_K(P)$.

Veta 1.7.5. *Nech K je algebraické číselné teleso stupňa n a p je prvočíslo. Predpokladajme, že*

$$(p) = P_1^{e_1} \dots P_g^{e_g}$$

je rozklad na súčin rôznych prvoideálov v $\mathcal{O}_K$ a $f_i = f_K(P_i)$ je stupeň inercie P_i v $\mathcal{O}_K$ pre všetky $i = 1,2,\dots,g$. Potom

$$e_1 f_1 + e_2 f_2 + \dots + e_g f_g = n.$$

Predchádzajúce tvrdenie jednak ukazuje vzťah stupňa inercie a indexu vetvenia, ale zároveň hovorí, že v číselnom telese stupňa n sa hlavný ideál generovaný prvočíslom nikdy nerozkladá na viac ako n rôznych prvoideálov.

Ďalej ozrejmime aké všetky prvky, respektíve ideály, majú prvočíselnú normu.

Veta 1.7.6. *Nech K je algebraické číselné teleso. Ak $\alpha \in \mathcal{O}_K$ tak, že*

$$N(\alpha) = \pm p,$$

kde p je prvočíslo, potom α je ireducibilný prvok.

Veta 1.7.7. *Nech K je algebraické číselné teleso a $0 \neq I$ ideál $\mathcal{O}_K$. Ak $N(I) = p$, kde p je prvočíslo, potom I je prvoideál.*

Na záver sekcie si ešte ukážme tvrdenie, ktoré nám priamo dáva algoritmus ako rozkladať hlavné ideály generované prvočíslami na súčiny prvoideálov v číselnom telese.

Veta 1.7.8. *Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso také, že $\mathcal{O}_K = \mathbb{Z}[\theta]$. Ďalej nech p je prvočíslo a*

$$f(x) = m_{\theta,\mathbb{Q}}(x) \in \mathbb{Z}[x].$$

Zvoľme monické polynómy $g_1(x), \ldots, g_r(x) \in \mathbb{Z}[x]$ tak, že sú navzájom rôzne, ireducibilné modulo p a zároveň

$$f(x) \equiv \prod_{i=1}^{r} g_i(x)^{e_i} \pmod{p},$$

kde $e_1, e_2, \ldots, e_n \in \mathbb{Z}_{>0}$. Ak položíme

$$P_i = (p,\ g_i(\theta)),\ \ i = 1,2,\ldots,r,$$

potom $P_1, P_2, \ldots, P_r$ sú navzájom rôzne prvoideály $\mathcal{O}_K$ a

$$(p) = P_1^{e_1} P_2^{e_2} \ldots P_r^{e_r},$$

$$N(P_i) = p^{\deg f_i},\ \ i = 1,2,\ldots,r.$$

1.8 Triedová grupa

Vedieť faktorizovať ideály bude dôležité najmä pre zistenie triedovej grupy číselného telesa.

Veta 1.8.1. *Nech K je algebraické číselné teleso a $\mathcal{O}_K$ príslušný okruh celistvých prvkov. Potom množina všetkých nenulových ideálov a lomených ideálov $\mathcal{O}_K$ tvorí spolu s operáciou násobenia Abelovskú grupu $I(K)$.*

Dôsledok 1.8.2. *Hlavné ideály v $I(K)$ sú tvaru $(\alpha) = \{r\alpha,\ r \in \mathcal{O}_K\}$ pre nejaké $\alpha \in K \setminus \{0\}$ a tvoria normálnu podgrupu $P(K)$ grupy $I(K)$.*

Faktorgrupa $I(K)/P(K)$ je dobre definovaná a Abelovská.

Definícia 1.8.3. (Triedová grupa)
Nech K je algebraické číselné teleso, $I(K)$ grupa nenulových ideálov a lomených ideálov $\mathcal{O}_K$ a $P(K)$ jej podgrupa hlavných ideálov. Potom faktorgrupa $I(K)/P(K)$ sa nazýva triedová grupa K, zn. $H(K)$, príp. $Cl(\mathcal{O}_K)$.

Definícia 1.8.4. (Triedové číslo)
Nech K je algebraické číselné teleso. Rádu grupy $H(K)$ hovoríme triedové číslo K, zn. $h(K)$.

Najjednoduchší prípad nastáva, ak okruh celistvých prvkov je Gaussov. To je ekvivalentné triedovému číslu 1 a vtedy všetky ideály okruhu sú hlavné.

Veta 1.8.5. *Nech K je algebraické číselné teleso. Potom*

$$h(K) = 1 \Leftrightarrow \mathcal{O}_K \text{ je obor integrity hlavných ideálov} \Leftrightarrow \mathcal{O}_K \text{ je Gaussov obor.}$$

Nasledujúce tvrdenia smerujú k hlavnému výsledku tejto sekcie o konečnosti triedovej grupy číselného telesa.

Veta 1.8.6. *Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso stupňa $n = r + 2s$, kde θ má r reálnych konjugácii a s dvojíc rýdzo komplexných konjugácii. Ďalej nech $C \in H(K)$. Potom C obsahuje ideál $B \neq 0$, pre ktorý platí*

$$N(B) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d(K)|}.$$

Definícia 1.8.7. (Minkowského hranica)
Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso stupňa $n = r + 2s$, kde θ má r reálnych konjugácii a s dvojíc rýdzo komplexných konjugácii. Minkowského hranicu M_K definuje predpis

$$M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d(K)|}.$$

Veta 1.8.8. *Nech K je algebraické číselné teleso a $k \in \mathbb{Z}_{>0}$. Potom existuje len konečný počet ideálov A okruhu celistvých prvkov $\mathcal{O}_K$ s normou $N(A) = k$.*

Dôsledok 1.8.9. *Nech K je algebraické číselné teleso. Potom jeho triedová grupa $H(K)$ je konečná (triedové číslo $h(K)$ je konečné).*

Všimnime si, že tvrdenia zároveň čiastočne ukazujú možnosť, ako triedovú grupu určiť, a to nájdením množiny jej reprezentantov zostavenej z ideálov normy menšej ako Minkowského hranica a súvislostí medzi nimi.

1.9 Jednotky

V záverečnej časti úvodnej kapitoly ukážeme spôsob, akým budeme overovať či daný prvok je jednotkou (invertibilným prvkom), ba dokonca hľadať celú grupu jednotiek v jednotlivých okruhoch celistvých prvkov.

Vo väčšine prípadov, napríklad keď bude grupa jednotiek konečná, alebo budeme vedieť vzniknutú rovnicu riešiť, nám bude stačiť použiť nasledujúci vzťah k norme.

Veta 1.9.1. *Nech K je algebraické číselné teleso.*

- *Ak α je jednotkou $\mathcal{O}_K$, potom $N(\alpha) = \pm 1$.*
- *Ak $\alpha \in \mathcal{O}_K$ a $N(\alpha) = \pm 1$, potom α je jednotkou $\mathcal{O}_K$.*

V zložitejších prípadoch nekonečnej grupy jednotiek použijeme silnú Dirichletovu vetu o jednotkách, ktorá hovorí, že jednotky v okruhu celistvých prvkov sú navzájom závislé a pre nájdenie celej grupy bude stačiť nájsť generátory (fundamentálne jednotky), ktorých je vždy len konečne veľa.

Veta 1.9.2. *(Dirichletova veta o jednotkách)*

Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso stupňa $n = r + 2s$, kde θ má r reálnych konjugácii a s dvojíc rýdzo komplexných konjugácii. Potom $\mathcal{O}_K$ obsahuje $r + s - 1$ jednotiek u_1,$u_2, \ldots, u_{r+s-1}$ takých, že každá jednotka $u \in \mathcal{O}_K$ sa dá jednoznačne vyjadriť v tvare

$$u = \rho u_1^{n_1} u_2^{n_2} \ldots u_{r+s-1}^{n_{r+s-1}},$$

kde ρ je odmocnina z jednej v $\mathcal{O}_K$ a $n_1, n_2, \ldots, n_{r+s-1} \in \mathbb{Z}$.

Definícia 1.9.3. (Fundamentálny systém jednotiek)

Nech $K = \mathbb{Q}(\theta)$ je algebraické číselné teleso stupňa $n = r + 2s$, kde θ má r reálnych konjugácii a s dvojíc rýdzo komplexných konjugácii. Ak $u_1, u_2, \ldots, u_{r+s-1}$ je $r + s - 1$ jednotiek $\mathcal{O}_K$ takých, že $u_1, u_2, \ldots, u_{r+s-1}$ sú vzájomne nezávislé a každá jednotka $u \in \mathcal{O}_K$ sa dá jednoznačne vyjadriť v tvare

$$u = \rho u_1^{n_1} u_2^{n_2} \ldots u_{r+s-1}^{n_{r+s-1}},$$

kde ρ je odmocnina z jednej v $\mathcal{O}_K$ a $n_1, n_2, \ldots, n_{r+s-1} \in \mathbb{Z}$, potom množinu

$$\{u_1, u_2, \ldots, u_{r+s-1}\}$$

nazývame fundamentálny systém jednotiek $\mathcal{O}_K$.

Kapitola 2

Diofantické rovnice

Uvažujme nasledovný problém: nech je daný polynóm $f(x_1, x_2, \ldots, x_n)$, $f \in \mathbb{Z}[x_1,x_2, \ldots, x_n]$. Má rovnica $f(x_1, x_2, \ldots, x_n) = 0$ celočíselné riešenie? Ak áno, nájdime ich všetky, pokiaľ nie, dokážme to.

Síce v súčasnosti je dokázané, že algoritmus na overenie existencie riešenia rovnice takéhoto typu neexistuje, no sú vyvinuté isté metódy a techniky, ktorými sa určité Diofantické rovnice riešiť dajú.

Jednou z najzákladnejších takých metód je využitie kongruencií, t.j. modulárnej aritmetiky, ktorej sa budeme venovať v Sekcii 2.1. Samostatné metódy boli vyvinuté na riešenie niektorých historicky významných rovníc, preto sa v Sekcii 2.2 zameriame na Pellovu rovnicu a jej riešiteľnosť, v Sekcii 2.3 zasa na Thueho rovnicu. Následne sa konečne dostaneme k metóde riešenia rovníc rozkladom v číselnom telese, ktorú na ilustratívnom príklade popíšeme v Sekcii 2.4 spolu so súvisiacimi tvrdeniami.

2.1 Modulárna aritmetika

Definícia 2.1.1. (Diofantická rovnica)
Diofantická rovnica je polynomiálna rovnica, obvykle o dvoch alebo viacerých premenných, pri ktorej uvažujeme iba jej celočíselné riešenia.

Veta 2.1.2. *Nech $f(x_1, x_2, \ldots, x_n) = 0$ je Diofantická rovnica. Pokiaľ existuje celočíselné riešenie $f(x_1, x_2, \ldots, x_n) = 0$, potom existuje riešenie tejto rovnice aj v $(\mathbb{Z}/a\mathbb{Z})^n$ pre ľubovolné $a \in \mathbb{Z}_{>0}$.*

Celočíselné riešenia budeme v práci ďalej značiť ako $\mathbb{Z}$-riešenia bez ohľadu na počet premenných rovnice (analogicky aj pri iných oboroch).

Príklad 2.1.3. Riešme rovnicu

$$x^2 - 117x + 31 = 0.$$

Pozrime sa teda na danú rovnicu modulo 2. Ak rovnica $\mathbb{Z}$-riešenie má, podľa Vety 2.1.2 má riešenie aj v $\mathbb{Z}/2\mathbb{Z}$. Obrátene, ak neexistuje $\mathbb{Z}/2\mathbb{Z}$-riešenie, neexistuje ani $\mathbb{Z}$-riešenie.

Takže pre celočíselné riešenie (x,y) pokiaľ $x \equiv 0 \pmod 2$, dostávame $0^2 - 0 + 1 \equiv 0 \pmod 2$, čo je spor, naopak ak $x \equiv 1 \pmod 2$, máme $1^2 - 1 + 1 \equiv 0 \pmod 2$, čo je opäť spor. Riešenie modulo 2 teda neexistuje, spolu s čím sme súčasne dokázali aj neexistenciu celočíselného riešenia.

Táto metóda môže byť užitočná aj v prípade zdanlivo menej triviálnych Diofantických rovníc.

Príklad 2.1.4. Riešme rovnicu

$$x^2 + y^2 = 4z^2 + 3.$$

Pozrime sa tento raz na rovnicu modulo 4. Pravá strana rovnice je zrejme vždy kongruentná 3 (mod 4).

Ak x,$y \equiv 0$ alebo 2 modulo 4, potom $x^2 \equiv y^2 \equiv 0 \pmod 4$. V prípade, že x,$y \equiv 1$ alebo 3 modulo 4, dostávame $x^2 \equiv y^2 \equiv 1 \pmod 4$. To však znamená, že pre ľubovolné možné riešenia rovnice x,y,$z \in \mathbb{Z}$ vždy $x^2 + y^2 \equiv 0$, 1, alebo 2 (mod 4), t.j. ľavá strana nie je modulo 4 kongruentná pravej.

Preto ani táto rovnica nemá celočíselné riešenie.

Ďalej sa pozrieme na špeciálne typy Diofantických rovníc, ktoré budeme často využívať. Vzhľadom na fakt, že boli dlhodobo analyzované, sú známe aj tvrdenia vhodné na ich riešenie.

2.2 Pellova rovnica

Najskôr sa budeme venovať jednej z najpreskúmanejších rovníc vôbec, tzv. Pellovej rovnici, na ktorej riešenie máme všeobecne známy postup.

Definícia 2.2.1. (Pellova rovnica)
Diofantická rovnica v tvare

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

kde $m > 0$ je bezštvorcové celé číslo, sa nazýva Pellova rovnica.

Zjavne $(x,y) = (\pm 1, 0)$ sú triviálnymi riešeniami Pellovej rovnice, ktorými sa ďalej v tejto sekcii už nebudeme zaoberať.

Veta 2.2.2. *Nech $m > 0$ je bezštvorcové celé číslo. Potom existujú x_1,$y_1 \in \mathbb{Z}_{>0}$, ktoré riešia Pellovu rovnicu $x^2 - my^2 = 1$.*

Definícia 2.2.3. (Fundamentálne riešenie)
Nech $m > 0$ je bezštvorcové celé číslo a x_1,$y_1 \in \mathbb{Z}_{>0}$ sú také, že (x_1,y_1) je riešením Pellovej rovnice $x^2 - my^2 = 1$ a zároveň $x_1 + \sqrt{m}y_1$ je najmenšie možné. Potom riešeniu (x_1,y_1) hovoríme fundamentálne riešenie Pellovej rovnice.

Poznámka. Definícia je korektná, nakoľko Veta 2.2.2 garantuje existenciu minimálneho kladného riešenia.

Veta 2.2.4. *Nech $m > 0$ je bezštvorcové celé číslo a (x_1,y_1) je fundamentálne riešenie Pellovej rovnice $x^2 - my^2 = 1$. Potom*

- *každé ďalšie riešenie tejto rovnice je v tvare $\pm(x_n,y_n)$, kde*

$$x_n + \sqrt{m}y_n = (x_1 + \sqrt{m}y_1)^n$$

  pre nejaké $n \in \mathbb{Z}$.

- *Ak x,$y \in \mathbb{Z}_{>0}$ sú také, že (x,y) je riešením danej rovnice a všetky ostatné riešenia tejto rovnice sú v tvare $\pm(x_n,y_n)$, kde*

$$x_n + \sqrt{m}y_n = (x + \sqrt{m}y)^n,$$

  potom nutne $(x,y) = (x_1,y_1)$.

Dôsledok 2.2.5. *Ak $m > 0$ je bezštvorcové celé číslo, potom Pellova rovnica $x^2 - my^2 = 1$ má nekonečne veľa celočíselných riešení.*

Príklad 2.2.6. Riešme rovnicu

$$x^2 - 3y^2 = 1.$$

Zjavne sa jedná o Pellovu rovnicu, t.j. $(\pm 1, 0)$ sú jej triviálnymi riešeniami. Ďalej pozorujme, že (2,1) je takisto riešenie danej rovnice. Aby sme overili, že sa jedná o fundamentálne riešenie, potrebujeme zistiť, či neexistuje iné kladné netriviálne riešenie (x_i,y_i), že $x_i + \sqrt{3}y_i < 2 + 1\sqrt{3} < 4$.

Jedinými takými kandidátmi na fundamentálne riešenia sú (1,1), (1,2), no ani jedno z nich nie je v skutočnosti riešením. Preto (2,1) je fundamentálne riešenie a podľa Vety 2.2.4 ostatné riešenia rovnice sú v tvare $\pm(x_n,y_n)$, kde

$$x_n + \sqrt{3}y_n = (2 + 1\sqrt{3})^n$$

pre všetky $n \in \mathbb{Z}$.

Vedieť riešiť Pellove rovnice bude užitočné v práci aj ďalej pri hľadaní jednotiek v niektorých kvadratických číselných telesách. Z rovnakého dôvodu do skupiny Pellových rovníc zahrnieme aj tzv. rozšírenú Pellovu rovnicu, ktorá bola taktiež historicky rozsiahlo skúmaná.

Definícia 2.2.7. (Rozšírená Pellova rovnica)
Diofantická rovnica v tvare

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

kde $m > 0$ je bezštvorcové celé číslo, sa nazýva rozšírená Pellova rovnica.

Analogické tvrdenie o existencii a jednoznačnosti fundamentálneho riešenia platí aj pri rozšírenej Pellovej rovnici.

Veta 2.2.8. *Nech $m > 0$ je bezštvorcové celé číslo. Potom existuje jednoznačne určené riešenie (x_1,y_1) rozšírenej Pellovej rovnice $x^2 - my^2 = \pm 1$, pre ktoré platí:*

- *$x_1,y_1 \in \mathbb{Z}_{>0}$,*
- *$x_1 + \sqrt{m}y_1$ je najmenšie možné a*
- *každé ďalšie riešenie tejto rovnice je v tvare $\pm(x_n,y_n)$, kde $x_n + \sqrt{m}y_n = (x_1 + \sqrt{m}y_1)^n$ pre ľubovolné $n \in \mathbb{Z}$.*

Podobne ako pri základnej Pellovej rovnici, riešenie z predchádzajúceho tvrdenia budeme nazývať fundamentálne riešenie rozšírenej Pellovej rovnice.

2.3 Thueho rovnica

Ďalšou historicky významnou a dôležitou rodinou Diofantických rovníc sú Thueho rovnice.

Veta 2.3.1. *(Thue)*
Ak

$$T(x,y) = a_0x^n + a_1x^{n-1}y + ... + a_{n-1}xy^{n-1} + a_ny^n,$$

kde $a_i \in \mathbb{Z}$ *pre všetky* $i \in \{0,1,\ldots,n\}$*, je homogénny ireducibilný polynóm celkového stupňa* $n \geq 3$*,* $0 \neq k \in \mathbb{Z}$*, potom diofantická rovnica*

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

má konečne veľa celočíselných riešení.

Ako prvý toto tvrdenie dokázal Axel Thue, po ktorom sú rovnice tohoto typu pomenované.

Definícia 2.3.2. (Thueho rovnica)
Nech $0 \neq k \in \mathbb{Z}$ a $T(x,y)$ je homogénny ireducibilný polynóm celkového stupňa $n \geq 3$. Každá diofantická rovnica tvaru $T(x,y) = k$ sa nazýva Thueho rovnica.

Thueho pôvodný dôkaz neviedol k algoritmu na samotné vyriešenie rovníc. Ten vznikol o pár desaťročí neskôr objavením hornej hranice na veľkosť riešenia Thueho rovníc.

Veta 2.3.3. *Nech* $T(x,y) = k$ *je Thueho rovnica. Všetky riešenia* $T(x,y) = k$ *sú efektívne algoritmicky spočítateľné a hranica pre* $max(|x|,|y|)$ *je polynomiálna vzhľadom ku* $|k|$*.*

Samotnú hranicu však nie je jednoduché explicitne vyjadriť, detaily k tomuto problému vieme nájsť v [Coh93], kap. 12.10.

Na netriviálne Thueho rovnice budeme ďalej využívať implementáciu algoritmu na ich riešenie v programe Wolfram Mathematica 10.1.

2.4 Faktorizácia v číselnom telese

Touto sekciou sa dostávame k metóde riešenia Diofantických rovníc rozkladom v príslušnom číselnom telese, ktorou sa budeme zaoberať prakticky po celý zvyšok práce.

Najskôr pri riešení elementárneho príkladu v telese racionálnych čísel popíšeme jednotlivé kroky, čím predstavíme metódu ako takú, pričom upozorníme na možné problémy, ktoré vzniknú prechodom do zložitejších číselných telies a ktorými sa budeme hlbšie zaoberať v práci ďalej.

Zároveň sformulujeme tvrdenia súvisiace s touto metódou použiteľné pri riešení konkrétnych úloh.

2.4.1 Rovnica $x^2 - 1 = y^3$ a popis metódy

Príklad 2.4.1. Riešme rovnicu

$$x^2 - 1 = y^3.$$

Predpokladajme, že (x,y) je nejaké celočíselné riešenie danej rovnice.

Parita

Ako prvú rozmyslime paritu x,y, čím na tieto čísla vytvoríme isté základné obmedzenia. Ak by x, y boli rovnakej parity, potom x^2 a y^3 by boli tiež rovnakej parity a $x^2 - 1 \neq y^3$, čo je spor. Takže môžme predpokladať, že ich parita je opačná.

Číselné teleso

Ďalším dôležitým krokom je popis číselného telesa, čo vždy obnáša určenie okruhu celistvých prvkov a jeho vlastností, triedovej grupy a grupy jednotiek. Nakoľko našu rovnicu budeme rozkladať v triviálnom číselnom telese $\mathbb{Q}$, jeho popis je ihneď z príslušných definícií zrejmý. Okruh celistvých prvkov tvorí okruh celých čísel $\mathbb{Z}$, čo je Euklidov obor a teda v ňom existujú jednoznačne určené rozklady na prvočísla. Preto podľa Vety 1.8.5 je triedová grupa jednoprvková a grupu jednotiek zjavne tvoria prvky ± 1.

V netriviálnych číselných telesách však môže byť jednak zložitejšie okruh celistvých prvkov nájsť, ďalej nemusí sa v ňom intuitívne pracovať a takisto nemusia v ňom existovať jednoznačne určené rozklady na prvočinitele. V takých prípadoch budeme musieť prechádzať do sveta ideálov pomocou tvrdení formulovaných v prvej kapitole a hľadať triedovú grupu. Rovnako môže byť v niektorých telesách náročnejšie určiť grupu jednotiek, ktorá naviac môže byť nekonečná.

Rozklad a spoločné delitele

Nasleduje samotný rozklad členov rovnice v príslušnom okruhu, čím našu rovnicu dostávame do tvaru

$$(x + 1)(x - 1) = y^3.$$

Ďalej pri riešení postupujeme určením možných spoločných deliteľov faktorov $x + 1$, $x - 1$.

Ak $d \in \mathbb{Z}$ delí $x + 1$ a zároveň $x - 1$, potom

$$d \mid ((x + 1) - (x - 1)) = 2,$$

teda $d \in \{1,2\}$ (až na znamienko). Zostáva rozdeliť úlohu na 2 prípady podľa parity a previesť diofantickú rovnicu do podoby, v ktorej ju budeme vedieť riešiť.

Riešenie pre párne x

Ak x je párne, potom zrejme $d = 1$ a čísla $x + 1$, $x - 1$ sú nesúdeliteľné. Nakoľko ale vieme, že ich súčin je treťou mocninou nejakého čísla, z existencie

a jednoznačnosti rozkladov na prvočísla musí aj každé z nich samostatne byť treťou mocninou nejakého celého čísla až na násobok jednotkou. Keďže každú z jednotiek vieme vyjadriť ako tretiu mocninu samej seba, nie je nutné ich brať do úvahy separátne a môžme ich zahrnúť do všeobecných prvkov. Preto uvažujme

$$x + 1 = a^3,$$

$$x - 1 = b^3$$

pre nejaké a,$b \in \mathbb{Z}$, z čoho ďalej plynie rovnosť

$$a^3 - 1 = b^3 + 1.$$

Jedinou možnosťou ako rozdiel dvoch tretích mocnín celých čísel môže byť 2 je zjavne prípad $a = 1$, $b = -1$, t.j. dostávame

$$x = a^3 - 1 = 1^3 - 1 = 0$$

a následne z pôvodnej rovnice

$$y^3 = x^2 - 1 = -1,$$

čo znamená $y = -1$.

Ak by celistvá báza okruhu celistvých prvkov nebola triviálna, čo nastane pri prechode na zaujímavejšie číselné telesá, namiesto jednej výslednej rovnice by sme dostali na riešenie sústavu rovníc.

Riešenie pre nepárne x

Naopak pokiaľ x je nepárne, potom zrejme $d = 2$ a $2 \mid x^2 - 1 = y^3$. Vieme, že y je párne, aplikujme teda na rovnicu substitúciu

$$y := 2y_1$$

a prepíšme ju do tvaru

$$(x + 1)(x - 1) = (2y_1)^3,$$

následne

$$\left(\frac{x+1}{2}\right)\left(\frac{x-1}{2}\right) = 2y_1^3,$$

kde už členy $\frac{x+1}{2}$, $\frac{x-1}{2}$ musia byť nesúdeliteľné. Preto môžme použiť obdobný postup ako vyššie a rozdeliť úlohu na ďalšie dva prípady, ktoré mohli nastať.

- Ak platí

$$\frac{x+1}{2} = a^3,$$

$$\frac{x-1}{2} = 2b^3$$

pre nejaké a,$b \in \mathbb{Z}$, potom určite máme rovnosť

$$x = 2a^3 - 1 = 4b^3 + 1,$$

čo z dôvodu rôznych koeficientov pri a,b zrejme nemá riešenie pre dostatočne veľké $|a|$,$|b|$. Overením niekoľkých možností na a,b dostávame dve riešenia

$$(a,b) = (-1,1),\ (a,b) = (1,0),$$

následne

$$(x,y) = (-3,2) \text{ a } (x,y) = (1,0).$$

- Pokiaľ

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

pre a,$b \in \mathbb{Z}$, analogicky

$$x = 4a^3 - 1 = 2b^3 + 1,$$

$$(a,b) = (0,-1),\ (a,b) = (1,1),$$

z čoho plynú ďalšie riešenia pôvodnej rovnice

$$(x,y) = (-1,0) \text{ a } (x,y) = (3,2).$$

Pri niektorých ďalších úlohách budeme nútení uvažovať viacero kandidátov na spoločných deliteľov jednotlivých faktorov, čím sa riešenie diofantickej rovnice viac–menej vždy rozdelí do niekoľkých častí, ktoré budeme musieť rozobrať samostatne.

Zhrnutie

Všetky riešenia rovnice $x^2 - 1 = y^3$ sú

$$(x,y) = (0,-1),\ (\pm 1,0),\ (\pm 3,2).$$

2.4.2 Práca s ideálmi

Pri telesách s vyšším triedovým číslom budeme musieť aj niektoré elementárne úvahy použité v príklade preniesť na ideály. Jeden zo základných princípov metódy, a to vyjadrenie každého z nesúdeliteľných faktorov ako mocniny všeobecného prvku, možno preložiť do jazyka ideálov pomocou nasledujúceho tvrdenia.

Tvrdenie 2.4.2. *Nech K je algebraické číselné teleso a nech A,B sú dva komaximálne ideály $\mathcal{O}_K$ také, že*

$$AB = C^k$$

pre nejaký ideál C a $k \in \mathbb{Z}_{>0}$. Potom

$$A = I^k,$$

$$B = J^k$$

pre nejaké ideály I,J.

Dôkaz. Z Vety 1.5.3 vieme, že $\mathcal{O}_K$ je Dedekindov obor a existuje v ňom jednoznačne určený rozklad každého vlastného ideálu na prvoideály. Keďže A,B sú komaximálne, môžme (pri vhodnom usporiadaní) uvažovať rozklady ideálov A,B na prvoideály v podobe

$$A = \prod_{i=1}^{m} P_i^{k_i},$$

$$B = \prod_{i=m+1}^{n} P_i^{k_i},$$

pričom $m < n \in \mathbb{Z}_{>0}$ a $P_i \neq P_j$ pre všetky $i \neq j$.

Predpokladáme $AB = C^k$, teda

$$AB = \prod_{i=1}^{n} P_i^{k_i} = C^k,$$

z čoho vyplýva

$$k \mid k_i \ \ \forall i \in \{1,2,\ldots,n\}.$$

Položme

$$I := \prod_{i=1}^{m} P_i^{k_i/k},$$

$$J := \prod_{i=m+1}^{n} P_i^{k_i/k}$$

a ihneď dostávame $A = I^k$, $B = J^k$.

❑

Kapitolu ukončíme tvrdením, ktoré nám za určitých predpokladov zaručí počítanie iba s hlavnými ideálmi aj v telesách s netriviálnou triedovou grupou, čím nám pri riešení niektorých náročnejších rovníc aspoň čiastočne umožní používať postup zo vzorového príkladu.

Veta 2.4.3. *Nech K je algebraické číselné teleso a h je triedové číslo K. Ďalej nech A je ideál $\mathcal{O}_K$ taký, že A^k je hlavný ideál pre $k \in \mathbb{Z}_{>0}$ spĺňajúce NSD(h,k) = 1. Potom A je takisto hlavný ideál.*

Dôkaz. Keďže rád triedovej grupy $H(K)$ je h, ideál A^h je určite hlavný. Nakoľko predpokladáme NSD(h,k)= 1, existujú r,$s \in \mathbb{Z}$ také, že $rh + sk = 1$. Naviac vieme, že ideál A^k je hlavný tiež, takže máme

$$A = A^{rh+sk} = (A^h)^r (A^k)^s,$$

čo je postačujúce, pretože súčin dvoch hlavných ideálov je hlavný ideál.

❑

Kapitola 3

Výpočty v číselných telesách

V tejto kapitole spravíme časť výpočetnej prípravy na riešenie konkrétnych rovníc a dokážeme tvrdenia týkajúce sa najmä okruhov celistvých prvkov, triedovej grupy či grupy jednotiek, ktoré v úlohách následne aplikujeme.

Sekciu 3.1 zameriame na kvadratické číselné telesá, pričom sa najskôr pozrieme na všeobecné vlastnosti tejto skupiny, no vzápätí detailnejšie rozoberieme príklady telies, v ktorých budeme pri riešení úloh pracovať.

Pozornosť v Sekcii 3.2 budeme venovať kubickým telesám, kde rozdiely v porovnaní s kvadratickými telesami zaznamenáme hlavne na príklade telesa určeného reálnym koreňom polynómu $x^2 + 2x + 1$.

3.1 Kvadratické číselné telesá

Pri kvadratických telesách vieme všeobecne vyjadriť okruh celistvých prvkov, celistvú bázu a diskriminant.

Veta 3.1.1. *Nech K je algebraické číselné teleso a m bezštvorcové celé číslo také, že $K = \mathbb{Q}(\sqrt{m})$. Potom okruh celistvých prvkov $\mathcal{O}_K$ je daný ako*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{ak } m \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right], & \text{ak } m \equiv 1 \pmod 4. \end{cases}$$

Dôkaz. Je ľahko overiteľné, že prvky okruhu $\mathbb{Z}[\sqrt{m}]$ pre $m \not\equiv 1 \pmod 4$ a prvky $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ pre $m \equiv 1 \pmod 4$ sú algebraické celé čísla v $K = \mathbb{Q}(\sqrt{m})$. Preto

$$\mathcal{O}_K \supseteq \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{ak } m \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right], & \text{ak } m \equiv 1 \pmod 4. \end{cases}$$

Pre dokončenie dôkazu potrebujeme ukázať i opačnú inklúziu. Buď $\alpha \in \mathcal{O}_K$. Potom $\alpha = a + b\sqrt{m}$ pre $a,b \in \mathbb{Q}$, teda α je koreňom monického polynómu $x^2 - 2ax + (a^2 - mb^2) \in \mathbb{Q}[x]$. Diskriminant tohto polynómu je

$$(2a)^2 - 4(a^2 - mb^2) = 4mb^2,$$

takže náš polynóm je rozložiteľný v $\mathbb{Q}[x]$ práve vtedy, keď $b = 0$. Preto

$$m_{\alpha,\mathbb{Q}}(x) = \begin{cases} x - a, & \text{ak } b = 0, \\ x^2 - 2ax + (a^2 - mb^2), & \text{ak } b \neq 0. \end{cases}$$

Keďže α je algebraické celé číslo, nutne $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ a

$$\begin{cases} \alpha \in \mathbb{Z}, & \text{ak } b = 0, \\ 2a,\ a^2 - mb^2 \in \mathbb{Z}, & \text{ak } b \neq 0. \end{cases}$$

Ak $b = 0$, máme $\alpha = a \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{m}]$. Ďalej predpokladajme $b \neq 0$.

Ak $2a$ je párne, potom $a \in \mathbb{Z}$ a teda $mb^2 \in \mathbb{Z}$. Keďže m je bezštvorcové, vidíme, že $b \in \mathbb{Z}$. V takom prípade $\alpha \in \mathbb{Z}[\sqrt{m}]$.

Ak $2a$ je nepárne, potom nakoľko $4(a^2 - mb^2) \in \mathbb{Z}$, máme $4mb^2 \in \mathbb{Z}$. A keďže m je bezštvorcové, $2b \in \mathbb{Z}$. Ak by $2b$ bolo párne, potom $b \in \mathbb{Z}$ a teda

$$a^2 = (a^2 - mb^2) + mb^2 \in \mathbb{Z},$$

čo je v spore s $2a$ nepárne. Takže $2b$ je nepárne, teda $a = (2u+1)/2$ a $b = (2v+1)/2$ pre nejaké u,$v \in \mathbb{Z}$. Potom však

$$a^2 - mb^2 = \frac{1}{4}((2u+1)^2 - m(2v+1)^2),$$

takže

$$\frac{m-1}{4} = u^2 + u - m(v^2 + v) - (a^2 - mb^2) \in \mathbb{Z}.$$

Z toho dostávame $m \equiv 1 \pmod 4$ a

$$\alpha = a + b\sqrt{m} = \frac{2u+1}{2} + \frac{2v+1}{2}\sqrt{m} =$$

$$= (u - v) + (2v+1)\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right],$$

čím je dôkaz opačnej inklúzie dokončený.

❑

Dôsledok 3.1.2. *Nech K je algebraické číselné teleso a m bezštvorcové celé číslo také, že $K = \mathbb{Q}(\sqrt{m})$. Ak $m \not\equiv 1 \pmod 4$, potom celistvú bázu K tvorí množina $\{1,\sqrt{m}\}$. V opačnom prípade, teda ak $m \equiv 1 \pmod 4$, celistvou bázou K je $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$.*

Veta 3.1.3. *Nech K je kvadratické číselné teleso a m bezštvorcové celé číslo také, že $K = \mathbb{Q}(\sqrt{m})$. Potom diskriminant $d(K)$ telesa K je*

$$d(K) = \begin{cases} 4m, & \text{ak } m \not\equiv 1 \pmod 4, \\ m, & \text{ak } m \equiv 1 \pmod 4. \end{cases}$$

Dôkaz. Najprv riešme prípad $m \not\equiv 1 \pmod 4$. Z Dôsledku 3.1.2 vieme, že $\{1, \sqrt{m}\}$ je celistvá báza K, preto

$$d(K) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = (-2\sqrt{m})^2 = 4m.$$

Ak naopak $m \equiv 1 \pmod 4$, celistvá báza K je $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$, takže

$$d(K) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = (-\sqrt{m})^2 = m.$$

❑

Ďalej sa pozrime ako v okruhoch celistvých prvkov kvadratických telies vyzerá norma.

Veta 3.1.4. *Nech m je bezštvorcové celé číslo a $K = \mathbb{Q}(\sqrt{m})$ je kvadratické číselné teleso. Potom norma všeobecného prvku $\mathcal{O}_K$ je daná ako*

$$\begin{cases} N(a + b\sqrt{m}) = a^2 - mb^2, & \text{ak } m \not\equiv 1 \pmod 4, \\ N(a + b\frac{1+\sqrt{m}}{2}) = a^2 + ab + \left(\frac{1-m}{4}\right) b^2, & \text{ak } m \equiv 1 \pmod 4. \end{cases}$$

Dôkaz. Ak $K = \mathbb{Q}(\sqrt{m})$ je kvadratické teleso také, že $m \not\equiv 1 \pmod 4$, potom podľa Vety 3.1.1 máme $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ a všeobecný prvok $\mathcal{O}_K$ je tvaru $a + b\sqrt{m}$. Jeho normu spočítame z definície ako

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

Naopak pokiaľ $m \not\equiv 1 \pmod 4$, máme $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. V takomto prípade je všeobecný prvok tvaru $a + b\left(\frac{1+\sqrt{m}}{2}\right)$ a jeho norma je

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

$$= a^2 + ab + \left(\frac{1-m}{4}\right) b^2,$$

čo je pre $m \equiv 1 \pmod 4$ vždy celé číslo.

❑

S výpočtom normy je spojená otázka určenia grupy jednotiek, ktorú vo väčšine prípadov kvadratických telies vieme jednoducho popísať. V imaginárnych telesách je jednotková grupa vždy konečná a pri reálnych narazíme na historicky významnú Pellovu rovnicu, ktorú z predchádzajúcej kapitoly vieme riešiť.

Veta 3.1.5. *Nech K je imaginárne kvadratické číselné teleso, t.j. $K = \mathbb{Q}(\sqrt{m})$ pre nejaké $m < 0$ bezštvorcové. Potom grupa jednotiek telesa K je daná ako*

$$\mathcal{U}(\mathcal{O}_K) = \begin{cases} \{\pm 1, \pm i\}, & \text{ak } K = \mathbb{Q}(i) \text{ a } i = \sqrt{-1}, \\ \{\pm 1, \pm\omega, \pm(\omega - 1)\}, & \text{ak } K = \mathbb{Q}(\sqrt{-3}) \text{ a } \omega = \frac{1+\sqrt{-3}}{2}, \\ \{\pm 1\}, & \text{inak}. \end{cases}$$

Dôkaz. Ak $K = \mathbb{Q}(i)$, potom podľa Vety 3.1.1 $\mathcal{O}_K = \mathbb{Z}[i]$. Z Vety 1.9.1 sú jednotkami $\mathcal{O}_K$ prvky s normou ± 1, t.j. prvky tvaru $a + bi$, že

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 = \pm 1.$$

Túto rovnicu zrejme spĺňajú len prvky $(a,b) = (0, \pm 1)$ a $(a,b) = (\pm 1,0)$, teda grupa jednotiek je

$$\mathcal{U}(\mathcal{O}_K) = \{\pm 1, \pm i\}.$$

Ak $K = \mathbb{Q}(\sqrt{-3})$, potom $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\omega]$. Jednotkami sú prvky tvaru $a + b\omega$, pre ktoré

$$N(a + b\omega) = \left(a + b\frac{1+\sqrt{-3}}{2}\right)\left(a + b\frac{1-\sqrt{-3}}{2}\right) = a^2 + ab + b^2 = \pm 1,$$

čo zjavne spĺňajú prvky $\pm 1, \pm\omega$ a $\pm(\omega - 1)$.

Ak $K = \mathbb{Q}(\sqrt{m})$ je iné imaginárne kvadratické teleso také, že $m \not\equiv 1 \pmod 4$, potom sú jednotkami $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ práve prvky tvaru $a + b\sqrt{m}$ spĺňajúce

$$N(a + b\sqrt{m}) = \pm 1,$$

pričom normu vieme podľa Vety 3.1.4 vyjadriť ako

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

Keďže $m < 0$ a $m \neq -1$, túto rovnicu zjavne riešia iba $(a,b) = (\pm 1,0)$, t.j. grupa jednotiek je tvorená prvkami ± 1.

Ak $K = \mathbb{Q}(\sqrt{m})$ je iné imaginárne kvadratické teleso také, že $m \equiv 1 \pmod 4$, potom analogicky sú jednotkami prvky tvaru $a + b\left(\frac{1+\sqrt{m}}{2}\right)$ spĺňajúce rovnosť

$$N\left(a + b\left(\frac{1+\sqrt{m}}{2}\right)\right) = a^2 + ab + \left(\frac{1-m}{4}\right)b^2 = \pm 1.$$

Nakoľko $m < 0$ a $m \neq -3$, opäť zjavne rovnicu riešia iba $(a,b) = (\pm 1, 0)$, teda $\mathcal{U}(\mathcal{O}_K) = \{\pm 1\}$.

❑

Veta 3.1.6. *Nech K je reálne kvadratické číselné teleso také, že $K = \mathbb{Q}(\sqrt{m})$ pre nejaké $m \not\equiv 1 \pmod 4$ bezštvorcové. Potom grupa jednotiek $\mathcal{U}(\mathcal{O}_K)$ je nekonečná a tvorená prvkami $a + b\sqrt{m}$, kde (a,b) je ľubovolné riešenie Pellovej rovnice $x^2 - my^2 = \pm 1$.*

Dôkaz. Keďže sa jedná o reálne kvadratické teleso, nutne $m > 0$. Ďalej nakoľko $m \not\equiv 1 \pmod 4$ je bezštvorcové, okruh celistvých prvkov je podľa Vety 3.1.1 $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Z Vety 1.9.1 sú jednotkami $\mathcal{O}_K$ prvky s normou ± 1, t.j. prvky tvaru $a + b\sqrt{m}$, že

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

čím sme úlohu previedli na nájdenie všetkých riešení Pellovej rovnice $x^2 - my^2 = \pm 1$. Finálne podľa Dôsledku 2.2.5 je množina všetkých týchto riešení nekonečná.

❑

Poznámka. Ak predpoklad $m \not\equiv 1 \pmod 4$ splnený nie je, nekonečnú grupu jednotiek väčšinou vieme nájsť odhadnutím fundamentálnej jednotky a použitím Dirichletovej vety o jednotkách, viz Veta 1.9.2.

Na záver sekcie o kvadratických telesách odvoďme vzorec pre konjugácie v okruhoch celistvých prvkov.

Veta 3.1.7. *Nech K je kvadratické číselné teleso a m bezštvorcové celé číslo také, že $K = \mathbb{Q}(\sqrt{m})$. Neidentický konjugovaný prvok k všeobecnému prvku okruhu $\mathcal{O}_K$ je daný ako*

$$\begin{cases} \overline{a + b\sqrt{m}} = a - b\sqrt{m}, & \text{ak } m \not\equiv 1 \pmod 4, \\ \overline{(a + b\frac{1+\sqrt{m}}{2})} = (a+b) - b\left(\frac{1+\sqrt{m}}{2}\right), & \text{ak } m \equiv 1 \pmod 4. \end{cases}$$

Dôkaz. Ak $m \not\equiv 1 \pmod 4$, potom máme $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ a konjugácie prvku $a + b\sqrt{m}$ sú z definície identita a prvok $a - b\sqrt{m}$.

Pokiaľ $m \not\equiv 1 \pmod 4$, okruh celistvých prvkov je $\mathcal{O}_K = \mathbb{Z}[\omega]$, kde $\omega = \frac{1+\sqrt{m}}{2}$. Neidentickú konjugáciu $a + b\omega$ vieme vyjadriť ako

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

❑

3.1.1 Teleso $\mathbb{Q}(\sqrt{-3})$

Okruh celistvých prvkov a diskriminant

Nech $K = \mathbb{Q}(\sqrt{-3})$ je číselné teleso, $\omega = \frac{1+\sqrt{-3}}{2}$ celistvý prvok a $f(z) := m_{w,\mathbb{Q}}(z) = z^2 - z + 1$ jeho minimálny polynóm nad $\mathbb{Q}$. Potom z Vety 1.4.5 a Dôsledku 1.3.9 platí

$$\begin{aligned} D(1,\omega) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\omega])^2 = \\ &= \operatorname{disc}(f(z)) = \operatorname{disc}(z^2 - z + 1) = -4 + 1^2 = -3, \end{aligned}$$

teda $d(K) = -3$ je bezštvorcové. Z Dôsledku 1.4.6 je $\{1,\omega\}$ celistvá báza $\mathcal{O}_K$ a $\mathcal{O}_K = \mathbb{Z}[\omega]$, čo korešponduje s výsledkom Vety 3.1.1.

Euklidovskosť $\mathbb{Z}[\omega]$

Na ukázanie, že $\mathbb{Z}[\omega]$ je Euklidov (a teda aj Gaussov) obor, stačí overiť, že

$$N(a + b\omega) = (a + b\frac{1+\sqrt{-3}}{2})(a + b\frac{1-\sqrt{-3}}{2}) = a^2 + ab + b^2,$$

kde $a,b \in \mathbb{Z}$, je Euklidovská norma, t.j.

$$N(0) = 0,$$

$$s \mid t,\ t \neq 0 \Rightarrow |N(s)| \leq |N(t)|,$$

$$\forall\, s,t \neq 0\ \exists\, q,r \text{ také, že } s = tq + r,\ |N(r)| < |N(t)|,$$

pričom $s,t,q,r \in \mathbb{Z}[\omega]$.

Najprv pozorujme, že ak $\rho \in \mathbb{Z}[\omega]$, potom z tvaru konjugácii vo Vete 3.1.7 dostávame

$$N(\rho) = \rho\bar{\rho} = |\rho|^2,$$

kde $|\rho|$ je absolútna hodnota ρ ako komplexného čísla.

$N(0) = 0$ je zrejmé.

Ak $s \mid t$, teda $t = sc$ pre nejaké nenulové c, potom

$$|N(t)| = |N(sc)| = |sc|^2 = |s|^2|c|^2 = |N(s)||N(c)|,$$

preto $|N(s)| \leq |N(t)|$.

Z toho zároveň plynie aj fakt, že pokiaľ $\rho \in \mathbb{Z}[\omega]$ je invertibilný prvok, $N(\rho) = \pm 1$. Opačnú implikáciu dostávame z $\pm 1 = N(\rho) = \rho\bar{\rho}$, nakoľko $\bar{\rho} \in \mathbb{Z}[\omega]$.

Pre $s,t \in \mathbb{Z}[\omega]$ uvažujme podiel $\frac{s}{t} \in \mathbb{C}$ a q nech je prvok $\mathbb{Z}[\omega]$ taký, že vzdialenosť $\left|\frac{s}{t} - q\right|$ je minimálna. Položme $r := s - tq$, teda $s = tq + r$ a zostáva ukázať $|N(r)| < |N(t)|$.

Zakreslením $\frac{s}{t}$ do Gaussovej roviny dostávame $\frac{s}{t}$ ako prvok obdĺžnika (vnútra alebo hrán) s hranami dlhými $\frac{1}{2}$ a $\frac{\sqrt{3}}{2}$, kde $q \in \mathbb{Z}[\omega]$ je jeden z jeho vrcholov (podľa definície vzdialenostne najbližší alebo ľubovolný z najbližších k $\frac{s}{t}$). Uhlopriečka obdĺžnika má podľa Pythagorovej vety dĺžku $\sqrt{\frac{3}{4} + \frac{1}{4}} = 1$, teda vzdialenosť priesečníka uhlopriečok k vrcholom je $\frac{1}{2}$, čím dostávame $\left|\frac{s}{t} - q\right| \leq \frac{1}{2} < 1$, čiže

$$|N(r)| = |r|^2 = |s - tq|^2 = |t|^2 \left|\frac{s}{t} - q\right|^2 < |t|^2 = |N(t)|.$$

Jednotková grupa

Rovnosť $N(a + b\omega) = a^2 + ab + b^2 = \pm 1$ spĺňajú práve prvky $\pm u \in \{1,\omega,\omega^2 = \omega - 1\}$, čím dostávame 6–prvkovú grupu jednotiek $\mathcal{U}(\mathbb{Z}[\omega])$, viz Veta 3.1.5.

3.1.2 Teleso $\mathbb{Q}(\sqrt{-7})$

Okruh celistvých prvkov a diskriminant

Uvažujme $K = \mathbb{Q}(\sqrt{-7})$, $\omega = \frac{1+\sqrt{-7}}{2}$, $f(z) := m_{w,\mathbb{Q}}(z) = z^2 - z + 2$. Analogicky ako v predchádzajúcom telese z Vety 3.1.1 máme $\mathcal{O}_K = \mathbb{Z}[\omega]$ a pre diskriminanty platí vzťah

$$\begin{aligned} D(1,\omega) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\omega])^2 = \\ &= \operatorname{disc}(f(z)) = \operatorname{disc}(z^2 - z + 2) = -7, \end{aligned}$$

teda $d(K) = -7$.

Euklidovskosť $\mathbb{Z}[\omega]$

Ďalej ukážme, že $\mathbb{Z}[\omega]$ je Euklidov obor. Opäť potrebujeme overiť, že

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

je pre a,$b \in \mathbb{Z}$ Euklidovská norma, t.j.

$$N(0) = 0,$$

$$s \mid t \neq 0 \Rightarrow |N(s)| \leq |N(t)|,$$

$$\forall\, s,t \neq 0\ \exists\, q,r \text{ také, že } s = tq + r,\ |N(r)| < |N(t)|,$$

kde s,t,q,$r \in \mathbb{Z}[\omega]$.

Znovu pokiaľ $\rho \in \mathbb{Z}[\omega]$, z tvaru konjugácii vo Vete 3.1.7 dostávame

$$N(\rho) = \rho\bar{\rho} = |\rho|^2,$$

kde $|\rho|$ je absolútna hodnota ρ ako komplexného čísla.

$N(0) = 0$ je zrejmé.

Ak $s \mid t$, teda $s = tc$ pre nejaké nenulové c, potom

$$|N(t)| = |N(sc)| = |sc|^2 = |s|^2\,|c|^2 = |N(s)||N(c)|$$

a $|N(s)| \leq |N(t)|$.

Preto pokiaľ $\rho \in \mathbb{Z}[\omega]$ je invertibilný prvok, $N(\rho) = \pm 1$. Z $\pm 1 = N(\rho) = \rho\bar{\rho}$ zasa plynie opačná implikácia, keďže $\bar{\rho} \in \mathbb{Z}[\omega]$.

Pre s,$t \in \mathbb{Z}[\omega]$ majme podiel $\frac{s}{t} \in \mathbb{C}$ a súčasne q nech je prvok $\mathbb{Z}[\omega]$ taký, že vzdialenosť $\left|\frac{s}{t} - q\right|$ je minimálna možná. Položme $r := s - tq$, teda $s = tq + r$ a zostáva ukázať $|N(r)| < |N(t)|$.

Zakreslením $\frac{s}{t}$ do Gaussovej roviny dostávame $\frac{s}{t}$ ako prvok obdĺžnika (vnútra alebo hrán) s hranami dlhými $\frac{1}{2}$ a $\frac{\sqrt{7}}{2}$, kde $q \in \mathbb{Z}[\omega]$ je jeden z jeho vrcholov (podľa definície vzdialenostne najbližší alebo ľubovolný z najbližších k $\frac{s}{t}$). Uhlopriečka obdĺžnika má podľa Pythagorovej vety dĺžku $\sqrt{\frac{7}{4} + \frac{1}{4}} = \sqrt{2}$, teda vzdialenosť priesečníka uhlopriečok k vrcholom je $\frac{\sqrt{2}}{2}$, čím dostávame $\left|\frac{s}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1$, čiže

$$|N(r)| = |r|^2 = |s - tq|^2 = |t|^2 \left|\frac{s}{t} - q\right|^2 < |t|^2 = |N(t)|.$$

Jednotková grupa

Z Vety 3.1.5 priamo dostávame 2–prvkovú grupu jednotiek $\mathcal{U}(\mathbb{Z}[\omega])$, teda $N(a + bw) = a^2 + ab + 2b^2 = \pm 1$ len pre prvky $u \in \{\pm 1\}$.

3.1.3 Teleso $\mathbb{Q}(\sqrt{2})$

Celistvá báza a diskriminant

Nech $K = \mathbb{Q}(\sqrt{2})$, $f(z) := m_{\sqrt{2},\mathbb{Q}}(z) = x^2 - 2$. Z Vety 3.1.1 plynie $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ a naviac z Vety 1.4.5 a Dôsledku 1.3.9

$$\begin{aligned} D(1,\sqrt{2}) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\sqrt{2}])^2 = \\ &= \operatorname{disc}(f(z)) = \operatorname{disc}(z^2 - 2) = 8. \end{aligned}$$

Následne zo Stickelbergerovej vety $d(K) = 8$ a $\{1,\sqrt{2}\}$ je celistvá báza $\mathcal{O}_K$.

Triedová grupa

Znovu by bolo možné overiť euklidovskosť $\mathcal{O}_K$, no pre naše účely bude stačiť ukázať, že tento obor je Gaussov, preto volíme rýchlejšiu cestu pomocou Minkowského hranice.

Vieme, že $m := [K : \mathbb{Q}] = 2$. Označme r počet reálnych koreňov $f(z)$, $2s$ počet rýdzo komplexných koreňov $f(z)$, t.j. v našom prípade $r = 2$ a $s = 0$.

Potom Minkowského hranica

$$M_K = \frac{m!}{m^m}\left(\frac{4}{\pi}\right)^s \sqrt{|d(K)|} = \frac{2}{4}\sqrt{8} < 2,$$

takže existuje množina reprezentantov triedovej grupy $H(K)$ zostavená z ideálov normy menšej ako 2, z čoho nutne plynie, že $H(K)$ je jednoprvková a podľa Vety 1.8.5 je $\mathcal{O}_K$ Gaussov obor.

Norma a jednotky

Uvažujme

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

a,$b \in \mathbb{Z}$, teda grupu jednotiek dostaneme podľa Vety 3.1.6 riešením Pellovej rovnice. Fundamentálne riešenie je zjavne $(a,b) = (1,1)$, preto jednotková grupa je tvorená prvkami

$$\pm(1 + \sqrt{2})^n,$$

kde $n \in \mathbb{Z}$.

3.1.4 Teleso $\mathbb{Q}(\sqrt{-5})$

Celistvá báza a diskriminant

Nech $\beta = \sqrt{-5}$, $K = \mathbb{Q}(\beta)$, $f(z) := m_{\beta,\mathbb{Q}}(z) = z^2 + 5$ a

$$\begin{aligned} D(1,\beta) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\beta])^2 = \\ &= \operatorname{disc}(f(z)) = \operatorname{disc}(z^2 + 5) = 4(-5) = -20. \end{aligned}$$

Ak by $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 2$, potom $d(K) = -5 \equiv 3 \pmod 4$, čo je v rozpore so Stickelbergerovou vetou. Teda $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 1$ a $d(K) = -20$, čiže $\{1, \sqrt{-5}\}$ je celistvá báza $\mathcal{O}_K$ ako $\mathbb{Z}$-modulu a $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ v súlade s Vetou 3.1.1.

Triedová grupa

Vieme, že $m := [K : \mathbb{Q}] = 2$. Označme r počet reálnych koreňov $f(z)$, $2s$ počet rýdzo komplexných koreňov $f(z)$, t.j. v našom prípade $r = 0$ a $s = 1$.

Potom Minkowského hranica

$$M_K = \frac{m!}{m^m}\left(\frac{4}{\pi}\right)^s \sqrt{|d(K)|} = \frac{2}{4}\frac{4}{\pi}\sqrt{20} = \frac{2\sqrt{20}}{\pi} < 3,$$

takže existuje množina reprezentantov triedovej grupy $H(K)$ zostavená z ideálov λ, kde $N(\lambda) < 3$.

Jediné prvočíslo menšie ako 3 je 2. Keďže

$$x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \,(\mathrm{mod}\, 2),$$

podľa Vety 1.7.8 rozklad (2) na prvoideály v $\mathbb{Z}[\sqrt{-5}]$ je daný ako

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

a teda

$$4 = N(2) = N(P^2) = N(P)^2,$$

z čoho plynie

$$N(P) = 2.$$

Kandidátom na množinu reprezentantov grupy $H(K) = Cl(\mathbb{Z}[\sqrt{-5}])$ je

$$\{\mathbb{Z}[\sqrt{-5}], P\},$$

pričom $\mathbb{Z}[\sqrt{-5}]$ je určite hlavný ideál, v grupe prvok rádu 1.

Ideál P hlavný nie je, pretože neexistuje žiadny prvok $c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, ktorého norma $N(c + d\sqrt{-5}) = c^2 + 5d^2$ je rovná ± 2. Preto P je v triedovej grupe prvkom rádu 2 a $Cl(\mathbb{Z}[\sqrt{-5}])$ je grupa veľkosti 2, t.j. $\simeq \mathbb{Z}_2$.

Triedové číslo číselného telesa $\mathbb{Q}(\sqrt{-5})$ vieme nájsť aj prostredníctvom programu Wolfram Mathematica 10.1 príkazom

```
NumberFieldClassNumber[Sqrt[5]*I].
```

Jednotková grupa

Grupa jednotiek $\mathcal{U}(\mathbb{Z}[\sqrt{-5}])$ je podľa Vety 3.1.5 rovnako dvojprvková, teda $u \in \{\pm 1\}$ sú jedinými jednotkami.

3.1.5 Teleso $\mathbb{Q}(\sqrt{58})$

Okruh celistvých prvkov a diskriminant

Nech $\beta = \sqrt{58}$, $K = \mathbb{Q}(\beta)$, $f(z) := m_{\beta,\mathbb{Q}}(z)$ a

$$\begin{aligned} D(1,\beta) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\beta])^2 = \\ &= \mathrm{disc}(f(z)) = \mathrm{disc}(z^2 - 58) = 232 = 2^3 29. \end{aligned}$$

Ak by $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 2$, potom $d(K) = 58 \equiv 2 \,(\mathrm{mod}\, 4)$, čo však zo Stickelbergerovej vety nemôže nastať. Teda $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 1$ a $d(K) = 232$. Z toho alebo z Vety 3.1.1 zároveň plynie okruh celistvých prvkov $\mathcal{O}_K = \mathbb{Z}[\sqrt{58}]$.

Triedová grupa

Zrejme $m := [K : \mathbb{Q}] = 2$, teda keď označíme r počet reálnych koreňov $f(z)$, $2s$ počet rýdzo komplexných koreňov $f(z)$ (v našom prípade $r = 2$ a $s = 0$), vieme spočítať Minkowského hranicu M_K ako

$$M_K = \frac{m!}{m^m} \left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{d}(K)|} = \frac{2!}{2^2}\sqrt{232} < 8.$$

Takže existuje množina reprezentantov triedovej grupy $H(K)$ zostavená z ideálov λ, kde $N(\lambda) < 8$.

Vezmime preto prvočísla menšie ako 8 a postupne nájdime rozklady ideálov, ktoré sú nimi generované.

- Keďže
$$f(z) = z^2 - 58 \equiv z^2 \pmod 2,$$
rozklad (2) na prvoideály v $\mathbb{Z}[\sqrt{58}]$ podľa Vety 1.7.8 je daný ako
$$(2) = P^2,$$
kde
$$P = (2,\sqrt{58}),\ N(P) = 2.$$

- Obdobne
$$f(z) = z^2 - 58 \equiv (z+1)(z+2) \pmod 3,$$
teda
$$(3) = P_1P_2,$$
$$P_1 = (3,1+\sqrt{58}),$$
$$P_2 = (3,2+\sqrt{58}),$$
$$N(P_1) = N(P_2) = 3.$$

- Ďalej
$$f(z) = z^2 - 58 \equiv (z^2+2) \pmod 5,$$
$$(5) = Q \text{ je prvoideál.}$$

- Na záver
$$f(z) = z^2 - 58 \equiv (z+3)(z+4) \pmod 7,$$
$$(7) = Q_1Q_2,$$
$$Q_1 = (7,3+\sqrt{58}),$$
$$Q_2 = (7,4+\sqrt{58}),$$
$$N(Q_1) = N(Q_2) = 7.$$

Teraz uvažujme vybrané prvky $\mathbb{Z}[\sqrt{58}]$ tvaru $k+\sqrt{58}$, $k \in \mathbb{Z}$, ktoré zrejme patria do niektorých z prvoideálov P,P_1,P_2,Q_1,Q_2 a ktorých normy obsahujú v prvočíselných rozkladoch len prvočísla 2,3,7:

- $2+\sqrt{58} \in P, P_2;\ N(2+\sqrt{58}) = -2^1 3^3$
- $3+\sqrt{58} \in Q_1;\ N(3+\sqrt{58}) = -7^2$
- $4+\sqrt{58} \in P, P_1;\ N(4+\sqrt{58}) = -2^1 3^1 7^1$
- $7+\sqrt{58} \in P_1;\ N(7+\sqrt{58}) = -3^2$
- $8+\sqrt{58} \in P;\ N(8+\sqrt{58}) = 2^1 3^1$
- $10+\sqrt{58} \in P, Q_1;\ N(10+\sqrt{58}) = 2^1 3^1 7^1$

- $11 + \sqrt{58} \in Q_2$; $N(11 + \sqrt{58}) = 3^2 7^1$.

S pomocou týchto vzťahov a vyčíslených noriem nájdime súvislosti medzi triedami ideálov okruhu $\mathbb{Z}[\sqrt{58}]$. Označme triedu obsahujúcu ideál I ako $[I]$ a triedu hlavných ideálov jednoducho ako 1.

- Keďže $3 + \sqrt{58} \in Q_1$, $Q_1 \mid (3 + \sqrt{58})$. Ak by $Q_2 \mid (3 + \sqrt{58})$, $(7) = Q_1 Q_2 \mid (3 + \sqrt{58})$, čo zjavne neplatí.

  Nech r je maximálne možné, že $Q_1^r \mid (3 + \sqrt{58})$. Potom $(3 + \sqrt{58}) = Q_1^r B$, kde $Q_1 \nmid B$, $Q_2 \nmid B$ a $N(B)$ neobsahuje 7 v prvočíselnom rozklade.

  Porovnaním noriem dostávame

  $$7^2 = N((3 + \sqrt{58})) = N(Q_1)^r N(B) = 7^r N(B),$$

  teda $r = 2$, $N(B) = 1$, $B = (1)$ a $(3 + \sqrt{58}) = Q_1^2$, čiže Q_1^2 je hlavný ideál.

  Máme $[Q_1 Q_2] = [Q_1]^2 = 1$.

- Analogicky zoberme vzťah $7 + \sqrt{58} \in P_1$, t.j. $P_1 \mid (7 + \sqrt{58})$. Ak by $P_2 \mid (7 + \sqrt{58})$, $(3) = P_1 P_2 \mid (7 + \sqrt{58})$, čo neplatí.

  Nech teraz r je maximálne možné, že $P_1^r \mid (7 + \sqrt{58})$. Potom $(7 + \sqrt{58}) = P_1^r B$, kde $P_1 \nmid B$, $P_2 \nmid B$, a $N(B)$ neobsahuje v rozklade prvočíslo 3.

  Opäť porovnaním noriem dostávame

  $$3^2 = N((7 + \sqrt{58})) = N(P_1)^r N(B) = 3^r N(B),$$

  teda $r = 2$, $N(B) = 1$, $B = (1)$ a $(7 + \sqrt{58}) = P_1^2$, čiže aj P_1^2 je hlavný ideál.

  Takže $[P_1 P_2] = [P_1]^2 = 1$.

- Ďalej $2 + \sqrt{58} \in P$,P_2, t.j. $P \mid (2 + \sqrt{58})$, $P_2 \mid (2 + \sqrt{58})$, a preto aj $PP_2 \mid (2 + \sqrt{58})$. Potom existuje ideál B, že $(2 + \sqrt{58}) = PP_2 B$.

  Vieme, že

  $$2^1 3^3 = N(2 + \sqrt{58}) = N(P) N(P_2) N(B) = 2^1 3^1 N(B),$$

  teda $N(B) = 3^2$ a B sa musí rovnať buď P_1^2, P_2^2 alebo $P_1 P_2$.

  Ak $B = P_1 P_2$, potom

  $$(2 + \sqrt{58}) = PP_2 P_1 P_2 = PP_2(3),$$

  t.j. $(3) \mid (2 + \sqrt{58})$, čo neplatí.

  Ak $B = P_1^2$, potom

  $$(2 + \sqrt{58}) = PP_2 P_1^2 = PP_1(3)$$

  a znova sa dostávame do sporu, pretože by muselo platiť $(3) \mid (2 + \sqrt{58})$.

  Takže $B = P_2^2$,

  $$(2 + \sqrt{58}) = PP_2^3,$$

z čoho plynie

$$[P][P_2]^3 = [P][P_2^3] = [P][P_2] = 1$$

a teda

$$[P] = [P^2P_2] = [P_2].$$

Týmto dostávame ďalší vzťah $[P] = [P_2] = [P_1]$.

- Ešte sa pozrime na prípad $10 + \sqrt{58} \in P, Q_1$, t.j. $P \mid (10 + \sqrt{58})$, $Q_1 \mid (10 + \sqrt{58})$, a preto aj $PQ_1 \mid (10 + \sqrt{58})$. Podobne ako vyššie napíšme $(10 + \sqrt{58}) = P^r Q_1^s B$, kde P,$Q_1 \nmid B$.

  Máme

  $$2^1 3^1 7^1 = N(P)^r N(Q_1)^s N(B) = 2^1 7^1 N(B),$$

  teda $N(B) = 3$ a $B = P_1$ alebo $B = P_2$.

  Pokiaľ $B = P_1$, potom $[PQ_1P_1] = 1$ a následne $[Q_1] = 1$, ak $B = P_2$, potom $[PQ_1P_2] = 1$ a $[Q_1] = 1$ tiež.

  Dostávame vzťah $[Q_1] = 1 = [Q_2]$.

Zosumarizujme si, že už máme

$$[P] = [P_1] = [P_2],$$

$$[Q] = [Q_1] = [Q_2] = 1,$$

t.j. nakoľko máme dve triedy ideálov 1,$[P]$, je zrejmé, že triedová grupa bude mať 1 alebo 2 prvky.

Skúsme predpokladať, že triedová grupa je jednoprvková a teda ideál P je hlavný (spolu s ním aj všetky ostatné). Potom nakoľko $N(P) = 2$, z Vety 1.6.9 musí existovať prvok $a+b\sqrt{58} \in P$, ktorého norma $N(a+b\sqrt{58}) = a^2-58b^2 = \pm 2$.

Keď sa na rovnosť $a^2 - 58b^2 = \pm 2$ pozrieme modulo 29, dostávame $a^2 \equiv \pm 2 \pmod{29}$, no $(\frac{\pm 2}{29}) = -1$, teda ± 2 nie je štvorcom modulo 29 a $a^2 - 58b^2 = \pm 2$ nemá modulo 29 riešenie. V takom prípade ale rovnosť nemá riešenie ani v $\mathbb{Z}$ a to je spor, čím dostávame, že triedová grupa $\mathbb{Z}[\sqrt{58}]$ je nutne dvojprvková.

Grupa jednotiek

Všetky jednotky okruhu celistvých prvkov $\mathbb{Z}[\sqrt{58}]$ nájdeme vyriešením Pellovej rovnice

$$N(a + \sqrt{58}b) = a^2 - 58b^2 = \pm 1,$$

kde fundamentálne riešenie získané príkazom

```
NumberFieldFundamentalUnits[Sqrt[58]]
```

je $(a,b) = (99,13)$. Ostatné jednotky sú následne z Vety 3.1.6 tvaru $\pm(99 + 13\sqrt{58})^k$, $k \in \mathbb{Z}$.

3.1.6 Teleso $\mathbb{Q}(\sqrt{79})$

Celistvá báza a diskriminant

Nech $\beta = \sqrt{79}$, $K = \mathbb{Q}(\beta)$, $f(z) := m_{\beta,\mathbb{Q}}(z)$, potom

$$\begin{aligned} D(1,\beta) &= d(K)(\mathcal{O}_K : \mathbb{Z}[\beta])^2 = \\ &= \operatorname{disc}(f(z)) = \operatorname{disc}(z^2 - 79) = 316 = 2^2 79. \end{aligned}$$

Ak by $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 2$, potom $d(K) = 79 \equiv 3 \pmod 4$, čo zo Stickelbergerovej vety nemôže nastať. Teda $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 1$, $d(K) = 316$, čiže ako hovorí Veta 3.1.1, $\{1, \sqrt{79}\}$ je celistvá báza $\mathcal{O}_K$ ako $\mathbb{Z}$-modulu a $\mathcal{O}_K = \mathbb{Z}[\sqrt{79}]$.

Norma a grupa jednotiek

Jednotky okruhu $\mathbb{Z}[\sqrt{79}]$ vieme zistiť podľa Vety 3.1.6 riešením Pellovej rovnice

$$N(a + b\sqrt{79}) = a^2 - 79b^2 = \pm 1.$$

Fundamentálne riešenie je $(a,b) = (80,9)$, preto grupu jednotiek $\mathcal{U}(\mathbb{Z}[\sqrt{79}])$ tvorí množina

$$\{\pm(80 + 9\sqrt{79})^k, k \in \mathbb{Z}\}.$$

Triedová grupa

Opäť označme r počet reálnych koreňov $f(z)$, $2s$ počet rýdzo komplexných koreňov $f(z)$, teda $r = 2$ a $s = 0$ a položme $m := [K : \mathbb{Q}] = 2$.

Minkowského hranica

$$M_K = \frac{m!}{m^m} \left(\frac{4}{\pi}\right)^s \sqrt{|d(K)|} = \frac{2!}{2^2}\sqrt{316} < 9,$$

takže existuje množina reprezentantov triedovej grupy $H(K)$ zostavená z ideálov λ, kde $N(\lambda) < 9$.

Uvažujme prvočísla menšie ako 9 a nájdime rozklady ideálov, ktoré generujú.

- Máme
$$f(z) = z^2 - 79 \equiv (z+1)^2 \pmod 2,$$
takže rozklad (2) na prvoideály v $\mathbb{Z}[\sqrt{79}]$ je podľa Vety 1.7.8
$$(2) = P^2,$$
pričom
$$P = (2,1 + \sqrt{79}),\ N(P) = 2.$$

- Podobne
$$f(z) = z^2 - 79 \equiv (z+1)(z+2) \pmod 3,$$
teda
$$\begin{aligned} (3) &= P_1 P_2, \\ P_1 &= (3,1 + \sqrt{79}), \\ P_2 &= (3,2 + \sqrt{79}), \\ N(P_1) &= N(P_2) = 3. \end{aligned}$$

- Ďalej
$$f(z) = z^2 - 79 \equiv (z+2)(z+3) \pmod 5,$$
$$(5) = Q_1 Q_2,$$
$$Q_1 = (5,2+\sqrt{79}),$$
$$Q_2 = (5,3+\sqrt{79}),$$
$$N(Q_1) = N(Q_2) = 5.$$

- Na záver
$$f(z) = z^2 - 79 \equiv (z+3)(z+4) \pmod 7,$$
$$(7) = R_1 R_2,$$
$$R_1 = (7,3+\sqrt{79}),$$
$$R_2 = (7,4+\sqrt{79}),$$
$$N(R_1) = N(R_2) = 7.$$

Vezmime niektoré prvky $\mathbb{Z}[\sqrt{79}]$ tvaru $k+\sqrt{79}$, $k \in \mathbb{Z}$, ktoré patria do prvoideálov P,P_1,P_2,Q_1,Q_2,R_1,R_2 a ktorých normy obsahujú v rozkladoch iba prvočísla 2,3,5,7:

- $5+\sqrt{79} \in P, P_2$; $N(5+\sqrt{79}) = -2^1 3^3$
- $8+\sqrt{79} \in P_2, Q_2$; $N(8+\sqrt{79}) = -3^1 5^1$
- $9+\sqrt{79} \in P$; $N(9+\sqrt{79}) = 2^1$
- $10+\sqrt{79} \in P_1, R_1$; $N(10+\sqrt{79}) = 3^1 7^1$.

Ďalej nájdime vzťahy medzi triedami ideálov okruhu $\mathbb{Z}[\sqrt{79}]$.

- Keďže $9+\sqrt{79} \in P$ a $|N(9+\sqrt{79})| = 2 = N(P)$, $P = (9+\sqrt{79})$ je nutne hlavný, teda $[P] = 1$.
- Keďže $8+\sqrt{79} \in P_2$,Q_2 a $|N(8+\sqrt{79}| = 15 = N(P_2)N(Q_2)$, $P_2Q_2 = (8+\sqrt{79})$.

  Analogicky $10+\sqrt{79} \in P_1$,R_1 a $|N(10+\sqrt{79}| = 21 = N(P_1)N(R_1)$, z čoho plynie $P_1R_1 = (10+\sqrt{79})$.

  Tým dostávame vzťahy $[P_2Q_2] = 1$, respektíve $[P_1R_1] = 1$, a následne
$$[P_1P_2Q_2] = [P_1] = [Q_2] = [P_1R_1R_2] = [R_2],$$
$$[P_1P_2R_1] = [P_2] = [R_1] = [P_2Q_1Q_2] = [Q_1].$$
- Zoberme ešte $5+\sqrt{79} \in P, P_2$, teda $P \mid (5+\sqrt{79})$, $P_2 \mid (5+\sqrt{79})$, a preto aj $PP_2 \mid (5+\sqrt{79})$.

  Napíšme $(5+\sqrt{79}) = PP_2B$ pre nejaký ideál B, porovnaním noriem dostaneme $2^1 3^3 = 2^1 3^1 N(B)$, z čoho jasne $N(B) = 3^2$.

  Ak by $B = P_1P_2 = (3)$, potom $(3) \mid (5+\sqrt{79})$, čo zrejme neplatí. Rovnako pokiaľ $B = P_1^2$, $B = PP_1^2P_2 = PP_1(3)$ a znovu by muselo platiť $(3) \mid (5+\sqrt{79})$. Takže $B = P_2^2$ a $(5+\sqrt{79}) = PP_2^3$, preto $[PP_2^3] = 1$ a nakoľko už vieme, že P je hlavný ideál, nutne $[P_2]^3 = 1$ a potom $[P_1] = [P_1P_2^3] = [P_2^2] = [P_2]^2$.

Máme vzťahy

$$[P] = 1,$$
$$[P_1] = [Q_2] = [R_2],$$
$$[P_2] = [Q_1] = [R_1],$$
$$[P_2]^2 = [P_1],$$
$$[P_2]^3 = 1,$$

teda triedová grupa bude zjavne mať najviac 3 prvky.

Keby $H(K)$ bola dvojprvková, tak $[P_2]^2 = 1$. Nakoľko však platí $[P_2]^3 = 1$, nutne by potom aj $[P_2] = 1$ a to je spor, pretože by všetky ideály boli hlavné.

Skúsme ďalej predpokladať, že triedová grupa je jednoprvková a ideál $P_2 = (\alpha)$ hlavný (spolu s ním aj všetky ostatné). Nakoľko rovnica $a^2 - 79b^2 = -3$ má racionálne riešenia, overenie neexistencie prvku normy 3 použitím kongruencií analogicky ako pri telese $\mathbb{Q}(\sqrt{58})$ tentokrát nezafunguje, preto si ukážeme alternatívny postup ako doviesť tento predpoklad k sporu. Keďže $P_2 = (\alpha)$, potom

$$(\alpha^3) = P_2^3 = (5 + \sqrt{79})P^{-1} = (5 + \sqrt{79})(9 + \sqrt{79})^{-1},$$

a nakoľko $\frac{1}{9+\sqrt{79}} = \frac{9-\sqrt{79}}{2}$ a $\frac{(5+\sqrt{79})(9-\sqrt{79})}{2} = -17 + 2\sqrt{79}$, dostávame

$$(\alpha^3) = P_2^3 = (-17 + 2\sqrt{79}).$$

Z toho plynie, že

$$\alpha^3 = (a + b\sqrt{79})^3 = u(-17 + 2\sqrt{79})$$

pre a,$b \in \mathbb{Z}$ a $u \in \mathcal{U}(\mathbb{Z}[\sqrt{79}])$ jednotku okruhu celistvých prvkov.

K nájdeniu triedovej grupy už zostáva vyriešiť len sústavy rovníc, ktoré vzniknú roznásobením výrazov v rovnosti

$$\alpha^3 = (a + b\sqrt{79})^3 = (80 + 9\sqrt{79})^k(-17 + 2\sqrt{79}),$$

kde sa môžme obmedziť na $k \in \{0, \pm 1\}$ vzhľadom na fakt, že ostatné jednotky sú zahrnuté v tretej mocnine všeobecného prvku okruhu.

- Ak $k = 0$, máme
$$-17 + 2\sqrt{79} = (a + b\sqrt{79})^3,$$
z čoho dostávame sústavu
$$-17 = a^3 + 237ab^2,$$
$$2 = 3a^2b + 79b^3,$$
ktorá celočíselné riešenie nemá.

- Ak $k = 1$, sme v situácii
$$(-17 + 2\sqrt{79})(80 + 9\sqrt{79}) = 62 + 7\sqrt{79} = (a + b\sqrt{79})^3,$$
teda
$$62 = a^3 + 237ab^2,$$
$$7 = 3a^2b + 79b^3,$$
čo opäť nemá celočíselné riešenie.

- Ak $k = -1$, dostávame

$$(-17 + 2\sqrt{79})(80 - 9\sqrt{79}) = -2782 + 313\sqrt{79} = (a + b\sqrt{79})^3,$$

teda

$$-2782 = a^3 + 237ab^2,$$
$$313 = 3a^2b + 79b^3$$

a ani teraz celočíselné riešenie nemáme.

Neexistenciou riešenia ani jednej z rovníc dostávame spor s predpokladom, že ideál P_2 je hlavný a triedová grupa triviálna, teda musí platiť, že táto grupa obsahuje práve 3 prvky (iné možnosti sme vylúčili vyššie).

3.2 Kubické číselné telesá

Ďalej uvažujme kubické telesá definované koreňom ireducibilného polynómu stupňa 3 tvaru $x^3 + ax + b \in \mathbb{Z}[x]$. V takých prípadoch vieme spočítať všeobecný vzorec na diskriminant generujúceho prvku, z čoho následne vo väčšine prípadov len pomocou tvrdení z úvodnej kapitoly dostaneme okruh celistvých prvkov.

Veta 3.2.1. *Nech a,$b \in \mathbb{Z}$ sú také, že $x^3 + ax + b \in \mathbb{Z}[x]$ je ireducibilný polynóm. Ďalej nech $\theta \in \mathbb{C}$ je koreň $x^3 + ax + b$ a $K = \mathbb{Q}(\theta)$ je kubické teleso definované θ, pričom $\theta \in \mathcal{O}_K$. Potom*

$$D(\theta) = -4a^3 - 27b^2.$$

Dôkaz. Nech $f(x) := m_{\theta,\mathbb{Q}}(x) = x^3 + ax + b$ a $\theta_1 = \theta, \theta_2, \theta_3$ sú konjugácie θ nad $\mathbb{Q}$, že

$$(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 + ax + b.$$

Porovnaním koeficientov dostávame

$$\theta_1 + \theta_2 + \theta_3 = 0,$$

$$\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = a,$$
$$\theta_1\theta_2\theta_3 = -b.$$

Derivácia $f(x)$ je

$$f'(x) = 3x^2 + a,$$

teda

$$f'(\theta_1)f'(\theta_2)f'(\theta_3) = (3\theta_1^2 + a)(3\theta_2^2 + a)(3\theta_3^2 + a) =$$
$$= a^3 + 3a^2(\theta_1^2 + \theta_2^2 + \theta_3^2) + 9a(\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2) + 27\theta_1^2\theta_2^2\theta_3^2.$$

Ďalej pozorujme, že

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) = -2a,$$

$$\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2 = (\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) = a^2,$$
$$\theta_1^2\theta_2^2\theta_3^2 = (\theta_1\theta_2\theta_3)^2 = b^2,$$

čiže

$$f^{'}(\theta_1)f^{'}(\theta_2)f^{'}(\theta_3) = a^3 + 3a^2(-2a) + 9a(a^2) + 27b^2 = 4a^3 + 27b^2.$$

Z Vety 1.3.7 nakoniec dostávame

$$D(\theta) = (-1)^{\frac{6}{2}} f^{'}(\theta_1)f^{'}(\theta_2)f^{'}(\theta_3) = -4a^3 - 27b^2.$$

❑

K nájdeniu grupy jednotiek nám analogicky ako v prípade kvadratických telies zväčša pomôže Dirichletova veta 1.9.2, no najskôr potrebujeme vedieť ako vyzerá norma, nájsť predpis pre overovanie jednotiek a následne vyjadriť všetky odmocniny z jednej.

Veta 3.2.2. *Nech a,b* $\in \mathbb{Z}$ *sú také, že* $x^3 + ax + b \in \mathbb{Z}[x]$ *je ireducibilný polynóm a ďalej nech* $K = \mathbb{Q}(\theta)$ *je kubické teleso, kde* $\theta^3 + a\theta + b = 0$. *Ak* $\mathcal{O}_K = \mathbb{Z}[\theta]$, *potom norma všeobecného prvku tohto okruhu je daná predpisom*

$$N(r + s\theta + t\theta^2) = r^3 - bs^3 + b^2t^3 + ars^2 + a^2rt^2 - 2ar^2t - abst^2 + 3brst.$$

Dôkaz. Nech $\theta = \theta_1, \theta_2, \theta_3$ sú konjugácie θ nad $\mathbb{Q}$, že

$$(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 + ax + b.$$

Z dôkazu Vety 3.2.1 už vieme, že

$$\theta_1 + \theta_2 + \theta_3 = 0,$$
$$\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = a,$$
$$\theta_1\theta_2\theta_3 = -b,$$

a zároveň

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = -2a,$$
$$\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2 = a^2.$$

Naviac platí

$$\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3 =$$
$$= (\theta_1 + \theta_2)\theta_1\theta_2 + (\theta_1 + \theta_3)\theta_1\theta_3 + (\theta_2 + \theta_3)\theta_2\theta_3 =$$
$$= -\theta_1\theta_2\theta_3 - \theta_1\theta_2\theta_3 - \theta_1\theta_2\theta_3 = -3\theta_1\theta_2\theta_3 = 3b,$$

takže

$$N(r + s\theta + t\theta^2) = (r + s\theta_1 + t\theta_1^2)(r + s\theta_2 + t\theta_2^2)(r + s\theta_3 + t\theta_3^2) =$$
$$= r^3 + s^3\theta_1\theta_2\theta_3 + t^3(\theta_1\theta_2\theta_3)^2 + rs^2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) +$$
$$+rt^2(\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2) + r^2s(\theta_1 + \theta_2 + \theta_3) + r^2t(\theta_1^2 + \theta_2^2 + \theta_3^2) +$$
$$+s^2t\theta_1\theta_2\theta_3(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) +$$
$$+rst(\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_1\theta_3^2 + \theta_1^2\theta_3 + \theta_2\theta_3^2 + \theta_2^2\theta_3) =$$
$$= r^3 - bs^3 + b^2t^3 + ars^2 + a^2rt^2 - 2ar^2t - abst^2 + 3brst.$$

❑

Dôsledok 3.2.3. *Nech a,$b \in \mathbb{Z}$ sú také, že $x^3 + ax + b \in \mathbb{Z}[x]$ je ireducibilný polynóm. Ďalej nech $K = \mathbb{Q}(\theta)$ je kubické teleso, kde $\theta^3 + a\theta + b = 0$, a zároveň $\mathcal{O}_K = \mathbb{Z}[\theta]$. Ak r,s,$t \in \mathbb{Z}$ spĺňajú*

$$r^3 - bs^3 + b^2t^3 + ars^2 + a^2rt^2 - 2ar^2t - abst^2 + 3brst = \pm 1,$$

potom $r + s\theta + t\theta^2$ je jednotkou $\mathcal{O}_K$.

Dôkaz. Tvrdenie vyplýva priamo z Vety 3.2.2 a Vety 1.9.1. ❑

Veta 3.2.4. *Prvky ± 1 sú všetky odmocniny z jednej v okruhu celistvých prvkov ľubovolného kubického číselného telesa.*

Dôkaz. Nech K je kubické teleso a ζ primitívna k-tá odmocnina z jednej v $\mathcal{O}_K$. Potom $\mathbb{Q}(\zeta) \subseteq K$ a teda $[\mathbb{Q}(\zeta) : \mathbb{Q}] \mid [K : \mathbb{Q}]$, kde $[K : \mathbb{Q}] = 3$ z definície. Veľkosť rozšírenia

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg m_{\zeta,\mathbb{Q}}(x) = \phi(k),$$

kde ϕ je Eulerova funkcia, takže dostávame $\phi(k) \mid 3$. Z vlastností a predpisu Eulerovej funkcie neexistuje k, že $\phi(k) = 3$, t.j. nutne $k \leq 2$. Keďže zjavne $\pm 1 \in \mathcal{O}_K$ odmocniny z jednej sú, žiadna ďalšia nemôže existovať. ❑

Na záver ešte uveďme jeden vzťah medzi diskriminantom telesa a fundamentálnou jednotkou.

Tvrdenie 3.2.5. *Nech K je kubické teleso s diskriminantom $d(K) < 0$ a nech $u \in \mathcal{U}(\mathcal{O}_K)$ je fundamentálna jednotka taká, že $u > 1$. Potom*

$$|d(K)| < 4u^3 + 24.$$

Dôkaz. Dôkaz je čisto technický a je možné ho nájsť ako Lemma 5.13 v [Mil14]. ❑

3.2.1 Reálne teleso dané koreňom $x^3 + 2x + 1$

Okruh celistvých prvkov a diskriminant

Nech $f(z) := z^3 + 2z + 1$. Diskriminant $\mathrm{disc}(f(z))$ je podľa Vety 3.2.1 rovný

$$\mathrm{disc}(f(z)) = -4 \cdot 2^3 - 27 \cdot 1^2 = -59$$

a keďže je záporný, priamo z definície má $f(z)$ nutne jeden reálny koreň a 2 čisto komplexné korene, t.j. $r = 1$ a $2s = 2$. Označme teda θ reálny koreň $f(z)$, θ' a $\bar{\theta'}$ zostávajúce dva a uvažujme teleso $K = \mathbb{Q}(\theta)$.

Keďže polynóm $f(z)$ je v $\mathbb{Z}[x]$ ireducibilný, $m := [K : \mathbb{Q}] = 3$.

Potom

$$D(1,\theta,\theta^2) = d(K)(\mathcal{O}_K : \mathbb{Z}[\theta])^2 = \mathrm{disc}(f(z)) = -59$$

a nakoľko tento diskriminant je bezštvorcový, $d(k) = -59$ a následne $\{1,\theta,\theta^2\}$ je celistvá báza $\mathcal{O}_K$. Preto okruh celistvých prvkov $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Diskriminant aj celistvú bázu telesa K vieme zistiť i príkazmi

```
NumberFieldDiscriminant[Root[1 + 2 # 1 + # 1^3 &, 1]],
```

respektíve

```
NumberFieldIntegralBasis[Root[1 + 2 # 1 + # 1^3 &, 1]].
```

Triedová grupa

Minkowského hranica

$$M_K = \frac{m!}{m^m}\left(\frac{4}{\pi}\right)^s \sqrt{|d(K)|} = \frac{3!}{3^3}\frac{4}{\pi}\sqrt{59} < 3,$$

takže existuje množina reprezentantov triedovej grupy $H(K)$ zostavená z ideálov λ, kde $N(\lambda) < 3$.

Vezmime 2 ako jediné prvočíslo menšie ako 3 a polynóm $f(z)$ rozložme modulo 2. Keďže

$$z^3 + 2z + 1 \equiv (z+1)(z^2+z+1) \,(\mathrm{mod}\, 2),$$

rozklad (2) na prvoideály v $\mathbb{Z}[\theta]$ podľa Vety 1.7.8 je daný ako

$$(2) = PQ,$$

kde

$$P = (2,\theta+1),$$

$$Q = (2,\theta^2+\theta+1),$$

$$N(P) = 2^1,\ N(Q) = 2^2.$$

Úpravou výrazu

$$(\theta+1)^3 - 3(\theta+1)^2 + 5(\theta+1) = \theta^3 + 3\theta^2 + 3\theta + 1 - 3\theta^2 - 6\theta - 3 + 5\theta + 5 =$$

$$= -1 + \theta + 3\theta^2 + 3\theta + 1 - 3\theta^2 - 6\theta - 3 + 5\theta + 5 = 2$$

dostávame, že $(\theta+1) \mid 2$ a teda $P = (\theta+1)$ je hlavný ideál.

Následne

$$(\theta+1)((\theta+1)^2 - 3(\theta+1) + 5) = 2,$$

preto

$$\frac{2}{\theta+1} = (\theta+1)^2 - 3(\theta+1) + 5 = \theta^2 + 2\theta + 1 - 3\theta - 3 + 5 = \theta^2 - \theta + 3$$

a $Q = (2)P^{-1} = \left(\frac{2}{\theta+1}\right) = (\theta^2 - \theta + 3)$ je tiež hlavný.

Tým sme dokázali, že rád triedovej grupy $h(K) = 1$ a $Z[\theta]$ je tiež oborom hlavných ideálov.

Norma a jednotková grupa

Vzhľadom na to, že K je reálne kubické teleso a $r + s - 1 = 1$, z Vety 1.9.2 existuje práve jedna fundamentálna jednotka $u > 1$ okruhu $\mathbb{Z}[\theta]$ a grupu jednotiek následne tvorí množina $\{\pm u^k,\ k \in \mathbb{Z}\}$.

Z Tvrdenia 3.2.5 vieme, že $59 = |d(K)| < 4u^3 + 24$, teda v našom prípade $u > 2$. Jednotkami sú podľa Dôsledku 3.2.3 práve tie prvky $a+b\theta+c\theta^2$, a,b,$c \in \mathbb{Z}$, ktoré spĺňajú

$$N(a + b\theta + c\theta^2) = a^3 - b^3 + c^3 + 2ab^2 + 4ac^2 - 4ca^2 - 2bc^2 + 3abc = \pm 1,$$

z čoho je zrejmé, že θ je jednotkou. Numericky $\theta \approx -0.4534$, no $-\theta^{-1} = 2 + \theta^2 \approx 2.2 > 2$ musí byť jednotkou tiež. Keďže nutne $1 < 2 + \theta^2 = u^l$ pre nejaké $l \in \mathbb{Z}_{>0}$ a zároveň $\sqrt{2 + \theta^2} \approx 1.485 < 2$, prvok $2 + \theta^2$ je iste hľadaná fundamentálna jednotka u.

Kapitola 4

Aplikácia na príkladoch rovníc

V tejto kapitole budeme metódou faktorizácie v číselnom telese riešiť vybrané Diofantické rovnice. Tie budú vhodne zvolené tak, aby ich riešenia neboli príliš technické, ale zároveň aby reprezentovali možné úskalia, ktoré sa pri riešení rovníc touto metódou môžu vyskytnúť. Tým by mali zároveň tvoriť istý návod na riešenie rovníc podobného typu.

Až po Sekciu 4.3 vrátane budeme pracovať v telese $\mathbb{Q}(i)$, kde celkovo prejdeme 5 rovníc od jednoduchých po poslednú najzložitejšiu o troch premenných. Na náročnosti pridajú rôzne spoločné delitele faktorov v okruhu celistvých prvkov.

V Sekcii 4.4 vyriešime dve rovnice vo výpočetne zložitejších okruhoch celistvých prvkov, v Sekcii 4.5 sa budeme zaoberať nekonečnou grupou jednotiek telesa $\mathbb{Q}(\sqrt{2})$ a Sekcia 4.6 bude patriť trom rovniciam, ktoré budeme rozkladať v telesách s netriviálnou triedovou grupou, opäť zoradených podľa náročnosti riešenia. Pri všetkých úlohách budeme využívať nadobudnuté znalosti z predchádzajúcich častí práce.

Nato sa v Sekcii 4.7 dostaneme k rovnici, ktorú budeme riešiť rozkladom v kubickom číselnom telese a finálne ju dokážeme previesť na problém riešenia sústav rovníc podobných Thueho rovniciam. Na záver doplníme vzťah k teórii eliptických kriviek.

Hoci väčšina rovníc, ktorými sa budeme zaoberať, sú eliptické krivky, podobným spôsobom možno riešiť aj rovnice s vyšším exponentom pri y. Avšak výsledné Thueho rovnice by v takom prípade vyšli komplikovanejšie a riešenie by bolo zbytočne menej priehľadné.

4.1 Pythagorejské trojice

Začneme príkladom všeobecne známej homogénnej rovnice celkového stupňa 2, ktorej riešním je množina všetkých Pythagorejských trojíc, t.j. trojíc prirodzených čísel a,b,$c \in \mathbb{Z}_{>0}$ spĺňajúcich rovnosť $a^2 + b^2 = c^2$, podobne ako v Pythagorovej vete pre dĺžky strán pravouhlého trojuholníka. Na túto úlohu potom v Sekcii 4.3 nadviažeme zdanlivo podobnou úlohou, kde však jedna premenná bude v tretej mocnine a príklad sa tým náležite skomplikuje.

4.1.1 Rovnica $x^2 + y^2 = z^2$

Príklad 4.1.1. Riešme rovnicu

$$x^2 + y^2 = z^2.$$

Poznámka. Pre prehľadnosť počas riešenia uvažujme (x,y,z) ako hľadané riešenie zadanej rovnice (podobne aj pri všetkých nasledujúcich príkladoch).

Elementárne úvahy

Na úvod sa obmedzme len na nezáporné riešenia $x \geq 0$, $y \geq 0$, $z \geq 0$, nakoľko všetky premenné sú v rovnici v druhej mocnine, a preto všetky záporné hodnoty by boli riešením tiež.

Ak $z = 0$, zrejme dostávame len triviálne riešenie rovnice $(x,y,z) = (0,0,0)$. Ak $x = 0$, ďalšie riešenia budú v tvare $(x,y,z) = (0,a,a)$, $a \in \mathbb{Z}_{>0}$. Symetricky v prípade, že $y = 0$, dostávame riešenia $(x,y,z) = (a,0,a)$, $a \in \mathbb{Z}_{>0}$, a po celý zvyšok príkladu môžme uvažovať x,y,z kladné.

Ďalej zjavne pokiaľ $d \mid x,y$, potom aj $d \mid z$, t.j. ak nájdeme nejaké riešenie rovnice pre x,y nesúdeliteľné, ďalšími riešeniami budú aj všetky jeho kladné celočíselné násobky. Teda zároveň predpokladajme, že x,y sú nesúdeliteľné.

Parita

Ak x, y sú obe nepárne, potom $x^2 + y^2 \equiv 2 \pmod 4$, ale $z^2 \not\equiv 2 \pmod 4$ pre ľubovolné z. Preto (keďže x, y nesúdeliteľné) môžme naviac predpokladať, že x, y sú opačnej parity (BÚNO x nepárne, y párne), z bude následne nutne nepárne.

Rozklad v číselnom telese

Ďalej pracujme v algebraickom číselnom telese $\mathbb{Q}(i)$, respektíve v jeho okruhu celistvých prvkov, ktorým je podľa Vety 3.1.1 obor integrity $\mathbb{Z}[i]$, a rovnicu prepíšme do tvaru

$$x^2 + y^2 = (x - iy)(x + iy) = z^2.$$

Vieme, že $\mathbb{Z}[i]$ je Gaussov, t.j. ireducibilné prvky sú nutne prvočinitele a existuje jednoznačný rozklad každého prvku okruhu. Norma všeobecného prvku $a+bi$ je

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

Nesúdeliteľnosť faktorov

Buď $\pi \in \mathbb{Z}[i]$ prvočiniteľ, ktorý delí $x - iy$ a $x + iy$. Potom

$$\pi \mid 2x,$$

$$\pi \mid 2iy,$$

$$N(\pi) \mid 4x^2,$$

$$N(\pi) \mid 4y^2,$$

$$N(\pi) = p^j,\ p \text{ prvočíslo},\ j \leq 2.$$

Z toho nutne plynie, že $N(\pi) = 2$ a teda $\pi \sim 1 + i$. To ale znamená, že $\pi^2 = \pm 2i \mid z^2$, čo je spor s nepárnosťou z. Preto $x - iy$ a $x + iy$ musia byť nesúdeliteľné.

Určenie riešenia

Buď $z = \pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k}$ rozklad z na prvočinitele. Z rovnosti

$$x^2 + y^2 = (x - iy)(x + iy) = z^2 = \pi_1^{2e_1}\pi_2^{2e_2}\ldots\pi_k^{2e_k}$$

a nesúdeliteľnosti $(x - iy)$, $(x + iy)$ dostávame $x + iy = u(a + bi)^2$ pre nejaké $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ a u jednotku.

Uvažujeme kladné riešenia, takže podľa Vety 3.1.5 stačí predpokladať $u \in \{1,i\}$.

Ak $u = 1$, máme

$$x + iy = (a + bi)^2 = a^2 - b^2 + 2abi,$$

teda $x = a^2 - b^2$, $y = 2ab$ a $z = a^2 + b^2$.

Ak $u = i$, máme

$$x + iy = i(a + bi)^2 = i(a^2 - b^2 + 2abi),$$

teda $x = -2ab$, $y = a^2 - b^2$ a $z = a^2 + b^2$, čo je ale v spore s nepárnosťou x.

Overenie podmienok

Pre zistenie podmienok nesúdeliteľnosti x,y nech p je prvočíslo, ktoré delí $a^2 - b^2$, $2ab$. Potom ale nastáva buď $p \mid (a - b)$, alebo $p \mid (a + b)$, a zároveň buď $p \mid 2$, $p \mid a$ alebo $p \mid b$.

Ak $p \mid 2$ a $p \mid (a \pm b)$, potom $a \pm b$ musia byť párne a teda a,b musia byť rovnakej parity. V ostatných prípadoch $p \mid a$ alebo $p \mid b$ a zároveň $p \mid (a-b)$ alebo $p \mid (a + b)$, z čoho nutne plynie, že $p \mid a$ a aj $p \mid b$.

Preto x,y sú nesúdeliteľné len vtedy, keď a,b sú nesúdeteliteľné a naviac opačnej parity.

Jednoznačnosť riešenia

Predpokladáme $x > 0$, $y > 0$, $z > 0$, teda aj $a^2 - b^2 > 0$ a $2ab > 0$. Z $2ab > 0$ plynie, že a,b majú rovnaké znamienko. Prípad a,$b < 0$ ale uvažovať nemusíme, pretože vedie k rovnakému riešeniu pre x,y,z ako prípad a,$b > 0$. Z $a^2 - b^2 > 0$ následne plynie, že $a > b > 0$.

Dostávame riešenia v tvare $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$, kde $a > b > 0$ sú nesúdeliteľné a opačnej parity. Naviac $x + z = (a^2 - b^2) + (a^2 + b^2) = 2a^2$, $z - x = (a^2 + b^2) - (a^2 - b^2) = 2b^2$, teda pre a,b kladné, $a = \sqrt{\frac{x+z}{2}}$, $b = \sqrt{\frac{z-x}{2}}$. Vidíme, že a,b sú určené jednoznačne, teda nájdené riešenia sú vzájomne disjunktné.

Zhrnutie

Týmto sme ukázali, že pre ľubovolné $c > 0$ všetky kladné celočíselné disjunktné riešenia danej rovnice (až na zámenu x,y) sú:

$$x = (a^2 - b^2)c,$$

$$y = 2abc,$$

$$z = (a^2 + b^2)c,$$

kde $a > b > 0$ sú nesúdeliteľné a opačnej parity.

4.2 Súdeliteľnosť faktorov

V tejto sekcii ukážme riešenia rovníc, pri ktorých bude existovať netriviálny spoločný deliteľ faktorov v okruhu celistvých prvkov $\mathbb{Z}[i]$, na ktoré sa vždy jedna strana príslušnej rovnice rozkladá.

4.2.1 Rovnica $x^2 + 4 = y^3$

Príklad 4.2.1. Riešme rovnicu

$$x^2 + 4 = y^3.$$

Elementárne úvahy, parita

Ak by ktorékoľvek z čísel x,y bolo nulové, zjavne nemáme celočíselné riešenie rovnice. Ďalej predpokladajme $x \neq 0$, $y \neq 0$.

Zároveň zrejme x,y sú buď obe párne, alebo obe nepárne. Tieto možnosti postupne rozoberieme separátne.

Rozklad v číselnom telese

Pracujme v číselnom telese $\mathbb{Q}(i)$. Okruh celistvých prvkov tohto telesa tvoria podľa Vety 3.1.1 Gaussove celé čísla, t.j. obor $\mathbb{Z}[i]$, v ktorom existujú jednoznačné rozklady prvkov na prvočinitele a norma všeobecného prvku $a + bi$ je

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

Následne vieme rovnicu prepísať do tvaru

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

Nepárne x,y – nesúdeliteľnosť faktorov

Predpokladajme najskôr, že x,y sú obidve nepárne. Nech π je taký prvočiniteľ, že $\pi \mid (x + 2i)$,$(x - 2i)$. Potom

$$\pi \mid ((x + 2i) + (x - 2i)) = 2x,$$

$$\pi \mid ((x + 2i) - (x - 2i)) = 4i,$$

$$N(\pi) \mid N(2x) = 4x^2,$$
$$N(\pi) \mid N(4i) = 16.$$

Keďže predpokladáme x nepárne, z posledných dvoch rovností nutne

$$N(\pi) \mid 4.$$

Naviac však platí

$$N(\pi) \mid N(x + 2i) = x^2 + 4,$$

čo znamená, že

$$N(\pi) \mid x^2,$$

no v takom prípade $N(\pi) = 1$, čo je spor uvažovaným π ako prvočiniteľom. Preto $x + 2i$, $x - 2i$ sú v $\mathbb{Z}[i]$ nesúdeliteľné a vzápätí

$$x + 2i \sim (a + bi)^3$$

pre nejaké a,$b \in \mathbb{Z}$, nakoľko $(x + 2i)(x - 2i) = y^3$.

Nepárne x,y – riešenie

Podľa Vety 3.1.5 sú jednotkami $\mathbb{Z}[i]$ prvky $u \in \{\pm 1, \pm i\}$. Každý prvok u z tejto množiny sa dá vyjadriť ako tretia mocnina nejakej (nie nutne rôznej) jednotky, t.j. $u = v^3$ pre $v \in \{\pm 1, \pm i\}$. Preto ich v rozklade nemusíme uvažovať a rovno dostávame

$$x + 2i = (a + bi)^3.$$

Roznásobením získavame

$$x + 2i = (a + bi)^3 = a^3 + 3ia^2b - 3ab^2 - ib^3,$$

následne porovnaním koeficientov

$$x = a(a^2 - 3b^2),$$

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

z čoho zrejme $b \in \{\pm 1, \pm 2\}$, nakoľko hľadáme $\mathbb{Z}$-riešenia.

Pre $b \in \{-1,2\}$ celočíselné riešenie druhej z rovníc nemáme.

Pre $b = 1$ dostávame $a = \pm 1$ a ďalej $x = \pm 2$, no to je v spore s predpokladom nepárneho x.

Nakoniec pre $b = -2$ máme takisto $a = \pm 1$, ale z tohto už plynie $x = \pm 11$ a dosadením do pôvodnej rovnice aj $y = 5$.

Zistili sme teda, že $(x,y) = (\pm 11,5)$ je riešením danej rovnice.

Párne x,y – spoločné deliteľe

Zostáva sa venovať prípadu, keď x,y sú párne čísla. Položme $x := 2x_1$, $y := 2y_1$ a pôvodnú rovnicu upravme na tvar

$$(2x_1 + 2i)(2x_1 - 2i) = 8y_1^3,$$

následne

$$x_1^2 + 1 = (x_1 + i)(x_1 - i) = 2y_1^3.$$

Keďže pravá strana rovnice je zjavne párne číslo, x_1 musí byť nutne nepárne. Ľavá strana je potom kongruentná 2 (mod 4), čiže aj y_1 musí byť nepárne.

Ďalej nech π_1 je prvočiniteľ, pre ktorý platí $\pi_1 \mid (x_1 + i)$,$(x_1 - i)$. Potom

$$\pi_1 \mid 2i \text{ a } N(\pi_1) \mid 4.$$

Zároveň $N(\pi_1) \mid (x_1^2 + 1)$, čo však nie je deliteľné štyrmi, teda $N(\pi_1) = 2$.

Jediný prvok $\mathbb{Z}[i]$ normy 2 až na násobok jednotkou je $\pi_1 \sim 1+i$, teda rovnicu vieme upraviť do tvaru

$$\frac{2y_1^3}{(1+i)^2} = -iy_1^3 = \left(\frac{x_1 + i}{1+i}\right)\left(\frac{x_1 - i}{1+i}\right).$$

Potom $\left(\frac{x_1 + i}{1+i}\right), \left(\frac{x_1 - i}{1+i}\right)$ už sú nutne nesúdeliteľné, pretože ak by existoval prvočiniteľ π_2, ktorý by bol ich spoločným deliteľom, muselo by platiť

$$N(\pi_2) \mid N\left(\frac{2i}{1+i}\right) = N(1+i) = 2$$

a $N(\pi_2) \mid N(y_1)^3 = y_1^6$ nepárne, čo je spor s predpokladom π_2 ako prvočiniteľa.

Párne x,y – riešenie

Nakoľko $-i = i^3$ je tretia mocnina jednotky, môžme ju zahrnúť do všeobecného prvku. Potom dostávame

$$\frac{x_1 + i}{1+i} = (a + bi)^3 = a^3 + 3ia^2b - 3ab^2 - ib^3$$

pre nejaké a,$b \in \mathbb{Z}$, teda

$$x_1 + i = (1+i)a^3 - (3 - 3i)a^2b - (3 + 3i)ab^2 + (1 - i)b^3$$

a porovnaním koeficientov získavame

$$x_1 = a^3 - 3a^2b - 3ab^2 + b^3,$$

$$1 = a^3 + 3a^2b - 3ab^2 - b^3 = (a - b)(a^2 + 4ab + b^2).$$

Preto $a - b = \pm 1$ a z uvedených rovníc musí byť $(a,b) = (0, -1)$ alebo $(a,b) = (1,0)$, z čoho plynie $x_1 = \pm 1$, $x = \pm 2$ a $y = 2$.

Zhrnutie

Všetky celočíselné riešenia zadanej rovnice sú

$$(x,y) = (\pm 11,5) \text{ a } (x,y) = (\pm 2,2).$$

4.2.2 Rovnica $x^2 + 4 = 3y^3$

Príklad 4.2.2. Riešme rovnicu

$$x^2 + 4 = 3y^3.$$

V tomto príklade využijeme znalosti z predchádzajúceho výpočtu na riešenie podobnej rovnice.

Elementárne úvahy, parita, rozklad

Analogicky ako v Príklade 4.2.1 predpokladajme nenulové x,$y \in \mathbb{Z}$ rovnakej parity a rovnicu prepíšme do tvaru

$$(x + 2i)(x - 2i) = 3y^3.$$

Nepárne x,y – nesúdeliteľnosť faktorov

Najskôr uvažujme x,y nepárne. Vieme, že jediný možný spoločný deliteľ faktorov $x + 2i$, $x - 2i$ je prvok normy 2, t.j. $1 + i$ a jeho násobky jednotkami, no zrejme $\frac{3y^3}{(1+i)^2} = \frac{3y^3}{2i} \notin \mathbb{Z}[i]$. Čiže $x + 2i$, $x - 2i$ sú nesúdeliteľné a nastáva buď

$$x + 2i = (a + bi)^3$$

alebo

$$x + 2i = 3(a + bi)^3$$

pre nejaké a,$b \in \mathbb{Z}$, nakoľko 3 je v $\mathbb{Z}[i]$ nerozložiteľné.

Nepárne x,y – riešenie

Ak by nastal prípad $x + 2i = (a + bi)^3$, potom z riešenia Príkladu 4.2.1 vieme, že $x = \pm 11$, no potom by muselo platiť $3y^3 = 125$, čo $\mathbb{Z}$-riešenie nemá.

Keď by nastal druhý prípad $x + 2i = 3(a + bi)^3$, nutne musí nastať $x - 2i = (a - bi)^3$ a spor dostávame obdobne.

Párne x,y – spoločné delitele

Teraz uvažujme x,y obe párne, opäť položme $x = 2x_1$, $y = 2y_1$ a pôvodnú rovnicu upravme na

$$4x_1^2 + 4 = 24y_1^3$$

a následne

$$x_1^2 + 1 = 6y_1^3.$$

Číslo x_1 je nepárne, pretože druhá strana rovnice je párna. Zároveň y_1 musí byť takisto nepárne, inak by sa ľavá a pravá strana rovnice nerovnali modulo 4.

Rozložme výraz $x_1^2 + 1$ na

$$x_1^2 + 1 = (x_1 + i)(x_1 - i)$$

a uvažujme rovnicu v tvare

$$(x_1 + i)(x_1 - i) = 6y_1^3.$$

Opäť analogicky ako v Príklade 4.2.1 je prvok $1+i$ spoločným deliteľom (x_1+i),(x_1-i), čo znamená, že rovnicu vieme prepísať do tvaru

$$\left(\frac{x_1+i}{1+i}\right)\left(\frac{x_1-i}{1+i}\right) = -3iy_1^3,$$

kde $\left(\frac{x_1+i}{1+i}\right), \left(\frac{x_1-i}{1+i}\right)$ sú v $\mathbb{Z}[i]$ nesúdeliteľné.

Párne x,y – riešenie

Preto platí buď

$$\frac{x_1+i}{1+i} = 3(a+bi)^3$$

alebo

$$\frac{x_1-i}{1+i} = 3(a+bi)^3$$

pre nejaké a,$b \in \mathbb{Z}$.

Ak by nastala prvá možnosť, potom

$$x_1+i = 3(1+i)(a+bi)^3 = 3((a^3-3ab^2-3a^2b+b^3)+i(a^3-3ab^2+3a^2b-b^3)),$$

z čoho by plynulo

$$1 = 3(a-b)(a^2+4ab+b^2),$$

čo však nemá $\mathbb{Z}$-riešenie.

Rovnako nedostávame riešenie ani pri druhej možnosti a tým sme ukázali, že zadaná rovnica žiadne celočíselné riešenia nemá.

4.2.3 Rovnica $x^2+36=y^3$

Príklad 4.2.3. Riešme rovnicu

$$x^2+36 = y^3.$$

Pri riešení tejto rovnice znovu využijeme výsledky predošlých príkladov.

Elementárne úvahy, parita

Zrejme v prípade nulového x či y rovnica $\mathbb{Z}$-riešenie nemá, takže predpokladajme ďalej $x \neq 0$ a $y \neq 0$.

Opäť môžme predpokladať, že x, y sú rovnakej parity a pracovať v číselnom telese $\mathbb{Q}(i)$, kde rovnicu prepíšeme na

$$(x+6i)(x-6i) = y^3.$$

Nepárne x,y – spoločné delitele

Uvažujme x,y nepárne. Ak $\alpha \in \mathbb{Z}[i]$ je spoločným deliteľom $x + 6i$, $x - 6i$, potom

$$\alpha \mid 12i,$$

$$N(\alpha) \mid 144 = 2^4 3^2,$$

$$N(\alpha) \mid (x^2 + 36) = y^3 \text{ nepárne.}$$

Z toho plynie

$$N(\alpha) \in \{1,9\},$$

nakoľko rovnica $a^2 + b^2 = 3$ nemá celočíselné riešenie a teda prvky normy 3 v $\mathbb{Z}[i]$ neexistujú.

Pokiaľ $N(\alpha) = 9$, potom $\alpha \sim 3$ je spoločný deliteľ $x + 6i$, $x - 6i$. V takom prípade $\alpha \mid x$, $\alpha \mid y$ a môžme použiť substitúciu $x := 3x_1$, $y := 3y_1$, pričom x_1,y_1 zostávajú nepárne.

Rovnicu následne dostávame do tvaru

$$9x_1^2 + 36 = 27y_1^3$$

a teda

$$x_1^2 + 4 = (x_1 + 2i)(x_1 - 2i) = 3y_1^3,$$

no z Príkladu 4.2.2 vieme, že celočíselné riešenie tejto rovnice neexistuje. Preto $\alpha \sim 3$ nemôže byť spoločným deliteľom prvkov $x + 6i$, $x - 6i$ a tie sú v $\mathbb{Z}[i]$ nesúdeliteľné.

Nepárne x,y – riešenie

V takom prípade

$$x + 6i = (a + bi)^3 = a^3 + 3ia^2b - 3ab^2 - ib^3$$

pre nejaké a,$b \in \mathbb{Z}$ a porovnaním koeficientov v imaginárnej zložke získavame rovnosť

$$6 = 3a^2b - b^3 = b(3a^2 - b^2).$$

To však znamená, že $b \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$, no pri žiadnej z možností nedostávame celočíselné riešenie pre a, teda ani pre x,y.

Párne x,y – spoločné delitele

Zostáva predpokladať, že x,y sú párne. Nech $x := 2x_2$, $y := 2y_2$. Rovnicu prepíšme do tvaru

$$4x_2^2 + 36 = 8y_2^3,$$

respektíve

$$x_2^2 + 9 = (x_2 + 3i)(x_2 - 3i) = 2y_2^3,$$

pričom x_2,y_2 už musia byť obidve nepárne, inak rovnica očividne nemá riešenie modulo 4.

Keďže pravá strana rovnice je párna a ani jeden z členov $x_2 \pm 3i$ nie je deliteľný dvomi, prvok $1+i$ musí opäť byť spoločným deliteľom x_2+3i, x_2-3i. Prenásobením celej rovnice výrazom $\dfrac{1}{(1+i)^2}$ ju dostávame do tvaru

$$-iy_2^3 = \left(\frac{x_2+3i}{1+i}\right)\left(\frac{x_2-3i}{1+i}\right).$$

Ak $\beta \in \mathbb{Z}[i]$ delí prvky $\dfrac{x_2+3i}{1+i}$ aj $\dfrac{x_2-3i}{1+i}$, potom

$$\beta \mid \frac{6i}{1+i} = 3(1+i),$$

$$N(\beta) \mid 18 = 3^2 2,$$

$$\beta \mid \frac{x_2^2+9}{2} \in \mathbb{Z} \text{ nepárne.}$$

Z toho plynie buď $\beta \sim 3$ alebo $\beta \sim 1$.

Predpokladajme najskôr

$$\beta \sim 3 \mid \frac{x_2+3i}{1+i}, \frac{x_2-3i}{1+i}.$$

V takom prípade $3 \mid -iy_2^3$, čiže $3 \mid y_2$, a potom aj $3 \mid x_2$. Substitúciou $x_2 = 3x_3$ a $y_2 = 3y_3$ dostávame rovnosti

$$-i(3y_3)^3 = \left(\frac{3(x_3+i)}{1+i}\right)\left(\frac{3(x_3-i)}{1+i}\right),$$

$$-3iy_3^3 = \left(\frac{x_3+i}{1+i}\right)\left(\frac{x_3-i}{1+i}\right),$$

kde $\dfrac{x_3+i}{1+i}, \dfrac{x_3-i}{1+i}$ už musia byť nesúdeliteľné.

No to sme znovu v situácii z Príkladu 4.2.2, čiže ani táto vetva nevedie k celočíselnému riešeniu pôvodnej rovnice. Zostáva uvažovať $\beta \sim 1$, teda že prvky $\dfrac{x_2+3i}{1+i}, \dfrac{x_2-3i}{1+i}$ sú nesúdeliteľné.

Párne x,y – riešenie

Potom máme

$$\frac{x_2+3i}{1+i} = (a+bi)^3 = a^3 + 3ia^2b - 3ab^2 - ib^3$$

pre nejaké a,$b \in \mathbb{Z}$ a dostávame

$$x_2 + 3i = (1+i)a^3 - (3-3i)a^2b - (3+3i)ab^2 + (1-i)b^3.$$

Porovnaním koeficientov získavame rovnosti

$$x_2 = a^3 - 3a^2b - 3ab^2 + b^3,$$

$$3 = a^3 + 3a^2b - 3ab^2 - b^3 = (a-b)(a^2+4ab+b^2),$$

teda $a-b \in \{\pm 1, \pm 2, \pm 3\}$, no ani jedna možnosť nevedie k celočíselnému riešeniu druhej z rovností, a preto ani k riešeniu pôvodnej rovnice.

Zhrnutie

Dokázali sme, že ani rovnica $x^2 + 36 = y^3$ žiadne $\mathbb{Z}$-riešenia nemá.

4.3 Rovnica o troch premenných

V tejto sekcii uveďme príklad rovnice troch premenných, pri ktorej riešení využijeme postupy z predchádzajúcich úloh a problém súdeliteľnosti faktorov ešte viac zovšeobecníme.

Príklad 4.3.1. Riešme rovnicu

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

Elementárne úvahy

Ak $x = 0$, rovnica má očividne riešenia $(x,y,z) = (0,a^3,a^2)$ pre všetky $a \in \mathbb{Z}$. Symetricky v prípade keď $y = 0$, riešenia sú v tvare $(x,y,z) = (a^3,0,a^2)$. Ďalej predpokladajme $x \neq 0$, $y \neq 0$ a následne nutne $z > 0$.

Rovnicu budeme ďalej riešiť postupne v závislosti na spoločnom deliteli x,y.

4.3.1 Rovnica $x^2 + y^2 = z^3$ s nesúdeliteľnými x, y

Najskôr vyriešme rovnicu v prípade, že x,y sú nesúdeliteľné.

Parita

Z nesúdeliteľnosti priamo vyplýva, že x,y nemôžu byť obe párne (mali by spoločného deliteľa 2), zároveň nemôžu byť ani obe nepárne, pretože potom by $x^2 + y^2 \equiv 2 \pmod 4$, čo pre z^3 nemôže nastať. Teda x,y sú opačnej parity, z je nepárne, $z \equiv 1 \pmod 4$.

Rozklad, nesúdeliteľnosť faktorov

Pracujme opäť v okruhu celistvých prvkov $\mathbb{Z}[i]$ a napíšme rovnicu v tvare

$$(x + yi)(x - yi) = z^3.$$

Ak π je prvočiniteľ a $\pi \mid (x + yi),(x - yi)$, potom $\pi \mid 2x,2yi$ a teda buď $\pi \mid 2$, alebo $\pi \mid x,y$. Druhá možnosť avšak nastať nemôže, pretože x,y sú nesúdeliteľné. Keďže $2 \sim (1 + i)^2$, $\pi \sim 1 + i$, no $N(\pi) = \pm 2$, čo nedelí z^3 nepárne. Preto sú $x + yi$, $x - yi$ nesúdeliteľné.

Určenie riešenia

Jednotky $\mathbb{Z}[i]$ sú podľa Vety 3.1.5 $\{\pm 1, \pm i\}$ a každá z nich sa dá napísať v tretej mocnine, t.j. v tvare v^3 pre v nejakú z jednotiek. Preto v rozklade $x + yi$ nemusíme jednotky uvažovať a dostávame

$$x + yi = (a + bi)^3 = a^3 + 3iba^2 - 3ab^2 - ib^3,$$

kde $a,b \in \mathbb{Z}$. Z toho plynie $x = a^3 - 3ab^2 = a(a^2 - 3b^2)$ a $y = 3ba^2 - b^3 = b(3a^2 - b^2)$, následne

$$x^2 + y^2 = z^3 = a^6 + 3a^4b^2 + 3a^2b^4 + b^6 = (a^2 + b^2)^3.$$

Overenie podmienok

Pre zistenie podmienok nesúdeliteľnosti x,y nech q je prvočíslo, pre ktoré $q \mid a(a^2-3b^2)$,$b(3a^2-b^2)$. Potom buď $q \mid a$ alebo $q \mid (a^2-3b^2)$ a súčasne $q \mid b$ alebo $q \mid (3a^2-b^2)$.

Nastáva teda buď $q \mid a$,b alebo $q \mid a$,$(3a^2-b^2)$ (respektíve $q \mid b$,(a^2-3b^2)), čo však vedie opäť k $q \mid a$,b. Poslednou možnosťou je $q \mid (a^2-3b^2)$,$(3a^2-b^2)$, z čoho plynie $q \mid (3a^2-9b^2)$,$(9a^2-3b^2)$ a následne $q \mid 8a^2$,$8b^2$, teda $q=2$ alebo $q \mid a$,b. Prípad $q=2$ vedie k tomu, že a^2-3b^2 je párne, a potom a,b musia byť rovnakej parity.

Dostávame riešenia zadanej rovnice v tvare $x=a(a^2-3b^2)$, $y=b(3a^2-b^2)$ a $z=(a^2+b^2)$, kde a,$b \in \mathbb{Z}$ nesúdeliteľné, opačnej parity.

Jednoznačnosť riešenia

Ak by $(a,b) \neq (a_1,b_1)$ viedli k rovnakému riešeniu, nastalo by

$$x+yi=(a+bi)^3=(a_1+b_1i)^3.$$

Potom $\left(\frac{a+bi}{a_1+b_1i}\right)^3=1$, no taký prvok $\mathbb{Z}[i]$ rôzny od 1 neexistuje, teda $\frac{a+bi}{a_1+b_1i}=1$ a nutne $a=a_1, b=b_1$.

4.3.2 Rovnica $x^2+y^2=z^3$, kde NSD(x,y)= p^k

Ďalej skúsme vyriešiť rovnicu v prípade, že NSD(x,y) je p^k, p prvočíslo, $k>0$.

Zjednodušenie, parita

Ak $k \equiv 0 \pmod 3$, potom rovnicu vieme napísať v tvare

$$p^{2k}(x_1^2+y_1^2)=p^{2k}z_1^3,$$

kde $x=p^kx_1$, $y=p^ky_1$, $z=p^{2k/3}z_1$. Teda dostávame rovnicu $x_1^2+y_1^2=z_1^3$, kde x_1,y_1 nesúdeliteľné, no rovnicu v tomto tvare sme už vyriešili vyššie.

Ak $k \equiv 1 \pmod 3$,

$$p^{2k}(x_1^2+y_1^2)=p^{2k+1}z_1^3,$$

kde $x=p^kx_1$,$y=p^ky_1$,$z=p^{(2k+1)/3}z_1$ a x_1,y_1 nesúdeliteľné.

Ak $k \equiv 2 \pmod 3$,

$$p^{2k}(x_1^2+y_1^2)=p^{2k+2}z_1^3,$$

kde $x=p^kx_1$, $y=p^ky_1$, $z=p^{(2k+2)/3}z_1$ a x_1,y_1 nesúdeliteľné.

Zostáva teda vyriešiť rovnice tvaru

$$x^2+y^2=p^jz^3$$

pre x,y nesúdeliteľné a $j \in \{1,2\}$.

Všimnime si, že z musí v oboch rovniciach zostať nepárne, inak by x, y neboli nesúdeliteľné.

Spoločné delitele

Ak β je spoločný deliteľ $x+iy$, $x-iy$, potom $\beta \mid 2x,2yi$, $N(\beta) \mid 4x^2,4y^2$. Ale x,y sú nesúdeliteľné, teda $N(\beta) \mid 4$.

Ak by $N(\beta) = 4$, potom $4 \mid N(x+yi) = x^2+y^2$, čo je opäť v spore s nesúdeliteľnosťou x,y. Takže $N(\beta) \in \{1,2\}$, t.j. $\beta \sim 1+i$ alebo $\beta = u$ pre nejakú jednotku u.

Spoločný deliteľ normy 2

Máme $N(\beta) = 2$ (t.j. $\beta \sim 1+i$). Nakoľko z je nepárne a $2 = N(\beta) \mid N(p^j z^3)$, p musí byť nutne 2. Rozdeľme teraz túto úlohu na dve vetvy podľa hodnoty $j \in \{1,2\}$.

1. Ako prvú riešme rovnicu $x^2+y^2 = 2z^3$, kde $1+i$ je spoločný deliteľ $x+iy$, $x-iy$. Kvôli predpokladu nesúdeliteľnosti musia byť x,y obe nepárne.

   Určenie riešenia

   Prenásobením rovnice výrazom $\frac{1}{(1+i)^2}$ získavame

   $$\frac{2z^3}{2i} = -iz^3 = \left(\frac{x+yi}{1+i}\right)\left(\frac{x-yi}{1+i}\right),$$

   kde $\frac{x+yi}{1+i}, \frac{x-yi}{1+i}$ musia byť nesúdeliteľné (inak by norma spoločného deliteľa musela byť 2 a 2 nedelí z^3 nepárne).

   Ďalej prvok -1 vieme napísať v tvare v^3, kde $v = -1$ je jednotka, čiže dostávame

   $$\frac{x+yi}{1+i} = (a+bi)^3$$

   pre nejaké $a,b \in \mathbb{Z}$ a teda

   $$x+yi = a^3+3iba^2-3ab^2-ib^3+ia^3-3ba^2-3iab^2+b^3.$$

   Z toho plynie

   $$x = a^3-3ab^2-3ba^2+b^3 = (a+b)(a^2-4ab+b^2),$$
   $$y = 3ba^2-b^3+a^3-3ab^2 = (a-b)(a^2+4ab+b^2),$$
   $$x^2+y^2 = 2a^6+6a^4b^2+6a^2b^4+2b^6 = 2z^3,$$
   $$z = a^2+b^2.$$

   Overenie podmienok

   Pre zistenie podmienok nesúdeliteľnosti x,y nech q je prvočíslo, $q \mid (a+b)(a^2-4ab+b^2)$,$(a-b)(a^2+4ab+b^2)$. Potom $q \mid (a+b)$ alebo $(a^2-4ab+b^2)$ a súčasne $q \mid (a-b)$ alebo $(a^2+4ab+b^2)$.

   Ak $q \mid (a+b)$,$(a-b)$, potom $q \mid 2a,2b$, t.j. $q \mid 2$ alebo $q \mid a,b$. Pokiaľ $q \mid 2$, $a-b$ musí byť párne a a,b sú rovnakej parity.

Ak $q \mid (a+b)$,$(a^2+4ab+b^2)$, potom $q \mid a^2+2ab+b^2$ a teda $q \mid 2ab$. Prípad $q \mid 2$ je rovnaký ako vyššie a pokiaľ $q \mid ab$, q musí deliť a aj b súčasne, nakoľko $q \mid (a+b)$.

Prípady $q \mid (a-b)$,$(a^2-4ab+b^2)$, respektíve $q \mid (a^2-4ab+b^2)$,$(a^2+4ab+b^2)$, vedú k identickému výsledku.

Zistili sme teda, že riešenia zadanej rovnice sú v tvare

$$x = (a+b)(a^2-4ab+b^2),$$

$$y = (a-b)(a^2+4ab+b^2),$$

$$z = a^2+b^2,$$

kde a,$b \in \mathbb{Z}$ nesúdeliteľné, opačnej parity. Z rovnakého dôvodu ako vyššie sú tieto riešenia určené jednoznačne.

2. Keď $j = 2$, t.j. rovnica je v tvare $x^2+y^2 = 4z^3$, dostávame spor, pretože $x^2+y^2 \equiv 0 \pmod 4$ platí len vtedy, ak x,y sú súdeliteľné.

Spoločný deliteľ normy 1

Máme $N(\beta) = 1$ (t.j. $\beta \sim 1$). Rozdeľme úlohu na 3 prípady:

1. p párne prvočíslo, $p = 2$,
2. $p \equiv 3 \pmod 4$, čiže p je prvočiniteľ aj v $\mathbb{Z}[i]$,
3. $p \equiv 1 \pmod 4$, čiže p sa v $\mathbb{Z}[i]$ rozkladá na $(c+di)(c-di)$.

Postupne prejdime jednotlivé prípady zvlášť.

1. p párne prvočíslo, $p = 2$:
   (a) $j = 1$, t.j. $x^2+y^2 = 2z^3$:
   Pokiaľ $x+yi = 2(a+bi)^3$, platí $x = 2(a^3-3ab^2)$, $y = 2(3a^2b-ib^3)$, teda 2 je spoločným deliteľom x,y, čo je spor s ich nesúdeliteľnosťou.
   Ak by $x+yi = (1+i)(a+bi)^3$, musí nastať $x-yi = (1+i)(a+bi)^3$, čo je spor s nesúdeliteľnosťou $x+yi$, $x-yi$.
   Ak nastane posledná možnosť, čiže $x+yi = (a+bi)^3$, potom $x-yi = 2(a+bi)^3$ a sme znova v situácii, že 2 je spoločným deliteľom x,y.
   (b) $j = 2$, t.j. $x^2+y^2 = 4z^3$:
   Rovnakým argumentom ako vyššie, teda $x^2+y^2 \equiv 0 \pmod 4$ len v prípade, ak x,y sú súdeliteľné, dostávame spor.
2. $p \equiv 3 \pmod 4$:
   (a) $j = 1$, t.j. $x^2+y^2 = pz^3$:
   Musí platiť buď $x+iy = p(a+bi)^3$ alebo $x-iy = p(a+bi)^3$. V oboch prípadoch však x,y sú násobkami p, teda súdeliteľné, čo je spor.

(b) $j = 2$, t.j. $x^2 + y^2 = p^2 z^3$:

V prípade, že $x+iy = p^2(a+bi)^3$, x,y sú násobkami p, teda súdeliteľné.

V prípade $x + iy = p(a + bi)^3$ dostávame spor s nesúdeliteľnosťou $(x + iy)$,$(x - iy)$ ihneď.

A pokiaľ $x + iy = (a + bi)^3$, potom $x - iy = p^2(a + bi)^3$, teda opäť x,y sú násobkami p.

3. $p \equiv 1 \pmod 4$, čiže $p = c^2 + d^2 = (c + di)(c - di)$

(a) $j = 1$, t.j. $x^2 + y^2 = pz^3$:

Určenie riešenia

Ak $x+iy = p(a+bi)^3$, respektíve $x+iy = (a+bi)^3$, dostávame obdobne ako vyššie spor s nesúdeliteľnosťou x,y.

Ak $x + iy = (c + di)(a + bi)^3$, potom

$$x = a^3c - 3ab^2c - 3a^2bd + b^3d,$$

$$y = 3a^2bc - b^3c + a^3d - 3ab^2d.$$

Následne

$$x^2 + y^2 = (a^2 + b^2)^3(c^2 + d^2) = (c^2 + d^2)z^3,$$

$$z = a^2 + b^2.$$

Prípad $x + iy = (c - di)(a + bi)^3$ je symetrický.

Overenie podmienok

Pre získanie podmienok na nesúdeliteľnosť x,y predpokladajme, že q je prvočíslo, $q \mid x$,y. Potom $q \mid (x + yi) = (c + di)(a + bi)^3$, kde $c + di$ je prvočiniteľ $\mathbb{Z}[i]$.

Ak $q \equiv 3 \pmod 4$, q je prvočiniteľ v $\mathbb{Z}[i]$, $q \mid (a + bi)^3$. Následne $q \mid (a + bi)$ a $q \mid a$,b.

Ak $q \equiv 1 \pmod 4$, $q = (c_1 + d_1 i)(c_1 - d_1 i) \mid (c + di)(a + bi)$, z čoho plynie buď $q \mid a$,b (prípad $c + di \neq c_1 \pm d_1 i$), alebo $(c - di) \mid (a + bi)$ (inak).

Zostáva uvažovať $q = 2$. Potom $q = 2 = (1 + i)^2 \mid (c + di)(a + bi)^3$, teda $(1 + i) \mid (a + bi)$, čo znamená, že a,b sú rovnakej parity (inak by $\frac{a+bi}{1+i}$ nebol prvok $\mathbb{Z}[i]$).

Teda aby x,y nemali spoločného delieteľa, musí platiť, že a,b sú opačnej parity, nesúdeliteľné a naviac $(c - di) \nmid (a + bi)$.

(b) $j = 2$, t.j. $x^2 + y^2 = p^2 z^3$:

Určenie riešenia

Ak $x + iy = (c + di)^2(a + bi)^3$, potom

$$x = a^3c^2 - 3ab^2c^2 - 6a^2bcd + 2b^3cd - a^3d^2 + 3ab^2d^2,$$

$$y = 3a^2bc^2 - b^3c^2 + 2a^3cd - 6ab^2cd - 3a^2bd^2 + b^3d^2.$$

Dostávame $x^2 + y^2 = (c^2 + d^2)^2(a^2 + b^2)^3$, z čoho $z = a^2 + b^2$.
Prípad $x + iy = (c - di)^2(a + bi)^3$ je opäť analogický.
Všetky ostatné možnosti musia obdobne ako vyššie viesť k súdeliteľným x,y (prípadne $x + iy$, $x - iy$), čo nemôže nastať.

Overenie podmienok

Pre získanie podmienok na nesúdeliteľnosť x,y znovu predpokladajme, že q je prvočíslo, $q \mid x$,y. Potom $q \mid (x + yi) = (c + di)^2(a + bi)^3$, kde $(c + di)$ je prvočiniteľ $\mathbb{Z}[i]$.
Ak $q \equiv 3 \pmod 4$, potom q je prvočiniteľ v $\mathbb{Z}[i]$, $q \mid (a + bi)^3$, a preto $q \mid (a + bi)$ a následne $q \mid a$,b.
Ak $q \equiv 1 \pmod 4$, $q = (c_1 + d_1i)(c_1 - d_1i) \mid (c + di)(a + bi)$, z čoho opäť plynie buď

$$\begin{cases} q \mid a,b, & \text{v prípade, že } c + di \neq c_1 \pm d_1i, \text{ alebo} \\ (c - di) \mid (a + bi), & \text{inak .} \end{cases}$$

Pokiaľ $q = 2$, dostávame $q = (1 + i)^2 \mid (c + di)^2(a + bi)^3$, teda $(1 + i) \mid (a + bi)$ a a,b sú nutne rovnakej parity.
Jednoznačne určené riešenia tejto rovnice sú teda

$$x = a^3c^2 - 3ab^2c^2 - 6a^2bcd + 2b^3cd - a^3d^2 + 3ab^2d^2,$$

$$y = 3a^2bc^2 - b^3c^2 + 2a^3cd - 6ab^2cd - 3a^2bd^2 + b^3d^2,$$

$$z = a^2 + b^2,$$

kde a,b sú nesúdeliteľné, opačnej parity a $(c - di) \nmid (a + bi)$.

4.3.3 Rovnica $x^2 + y^2 = z^3$ vo všeobecnom tvare

Zostáva vyriešiť prípad, kedy spoločný deliteľ x,y je nejaké všeobecné číslo $\prod p_r^{k_r}$. Pri riešení už nebudeme postupovať úplne detailne, ale odvoláme sa na rovnaké postupy použité v úvahách v predchádzajúcich krokoch.

Rovnicu vieme analogicky prepísať do tvaru

$$x^2 + y^2 = (x + yi)(x - yi) = \prod p_r^{k_r} z^3 =: 2^j dz^3,$$

kde x,y sú nesúdeliteľné, $k_r \in \{0,1,2\}$, $j \in \{0,1,2\}$.

Použitím obdobných úvah ako vyššie je zrejmé, že pokiaľ $j = 2$, dostávame spor s nesúdeliteľnosťou x,y. Rovnako dostávame spor v prípade, keď $p_s \equiv 3 \pmod 4$ pre akékoľvek s.

Zaoberajme sa teda už len prípadmi, kedy žiadna z týchto možností nenastane a všetky $p_r \mid d$ sú v tvare $(c_r + d_r i)(c_r - d_r i)$.

Ako prvý rozmyslime prípad $j = 0$. Opäť dostávame jednoznačne určené riešenia v prípade

$$x + iy = \prod (c_r + id_r)^{k_r}(a + bi)^3,$$
$$z = a^2 + b^2,$$

kde a,b sú nesúdeliteľné, opačnej parity, a zároveň pre všetky r platí $(c_r - d_r i) \nmid (a + bi)$.

Druhou možnosťou je $j = 1$. V prípade, že $x - iy$, $x - iy$ sú nesúdeliteľné, dostávame spor rovnako ako vyššie. Ak $1 + i$ je ich spoločným deliteľom, rovnicu vieme prepísať do tvaru

$$-idz^3 = \left(\frac{x + yi}{1 + i}\right)\left(\frac{x - yi}{1 + i}\right)$$

a teda $x + iy = d_1(1 + i)(a + bi)^3$, kde $d_1 \mid d$.

Znovu analogicky dostávame riešenia rovnice, keď

$$x + iy = \prod (c_r + id_r)^{k_r}(1 + i)(a + bi)^3,$$
$$z = a^2 + b^2,$$

kde opäť a,b sú nesúdeliteľné, opačnej parity, a súčasne pre všetky r platí $(c_r - d_r i) \nmid (a + bi)$.

4.4 Netypický okruh celistvých prvkov

Ďalej ukážeme dva príklady rovníc, pri riešení ktorých budeme musieť pracovať vo výpočetne náročnejších okruhoch celistvých prvkov.

4.4.1 Rovnica $x^2 + 3 = y^3$

Príklad 4.4.1. Riešme rovnicu

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

Elementárne úvahy, parita

Ak by jedno z čísel x alebo y bolo nulové, rovnica zjavne nemá celočíslené riešenie, t.j. predpokladajme $x \neq 0$ a $y \neq 0$.

Ak x, y sú rovnakej parity, potom x^2, y^3 sú tiež rovnakej parity a $x^2 + 3 \neq y^3$. Pokiaľ je y párne, $y^3 \equiv 0 \pmod 8$, z čoho plynie, že $x^2 \equiv 5 \pmod 8$, ale 5 nie je kvadratický zvyšok mod 8. Teda môžme ďalej predpokladať, že y je nepárne a x párne.

Rozklad v číselnom telese

Ďalej pracujme v algebraickom číselnom telese $\mathbb{Q}(\sqrt{-3})$, respektíve v jeho okruhu celistvých prvkov, ktorým je podľa Sekcie 3.1.1 Euklidov obor $\mathbb{Z}[\omega]$, kde $\omega = \frac{1+\sqrt{-3}}{2}$, a rovnicu prepíšme do tvaru

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

Nesúdeliteľnosť faktorov

Buď $\pi \in \mathbb{Z}[\omega]$ prvočiniteľ, ktorý delí $x - \sqrt{-3}$ a $x + \sqrt{-3}$. Potom

$$\pi \mid 2x,$$

$$\pi \mid 2\sqrt{-3},$$

teda $\pi \mid 2$ alebo $\pi \mid x, \sqrt{-3}$. Minimálny polynóm $f(z)$ zo Sekcie 3.1.1 je modulo 2 ireducibilný, teda podľa Vety 1.7.8 je 2 prvočiniteľ $\mathbb{Z}[\omega]$. Potom ale prípad $\pi \mid 2$ vedie k sporu, pretože $\pi = 2$ by muselo deliť y^3, ktoré je nepárne.

Máme $\pi \mid \sqrt{-3} = -1 + 2\omega$, teda $N(\pi) \mid N(-1 + 2\omega) = 1 - 2 + 4 = 3$. Nakoľko π je prvočiniteľ, určite $N(\pi) = 3$ a následne $\pi \sim 1 + \omega$, pretože iný prvok normy 3 neexistuje (konjugovaný prvok $\overline{1 + \omega} = 2 - \omega$ je takisto len násobok jednotkou).

Ale keď $(1+\omega) \mid (x - \sqrt{-3}), (x + \sqrt{-3})$, nutne $(1+\omega)^2 = 3w \sim 3 \mid x^3 + 3 = y^3$ a teda $3 \mid x, y$. Substitúciou $x := 3x_1$ a $y := 3y_1$ rovnicu dostávame do tvaru

$$9x_1^2 + 3 = 27y_1^3,$$

ktorá nemá riešenie modulo 9 a následne ani $\mathbb{Z}$-riešenie.

Takže neexistuje predpokladaný prvočiniteľ π s normou rovnou 3, teda $x - \sqrt{-3}$ a $x + \sqrt{-3}$ musia byť nesúdeliteľné.

Určenie riešenia

Z rovnice

$$x^2 + 3 = (x - \sqrt{-3})(x + \sqrt{-3}) = (x - (-1 + 2\omega))(x + (-1 + 2\omega)) = y^3$$

dostávame

$$x + \sqrt{-3} = x + (-1 + 2\omega) = u(a + b\omega)^3 =$$
$$= u(a^3 + 3(-1 + \omega)ab^2 + 3\omega a^2 b - b^3)$$

pre nejaké $a, b \in \mathbb{Z}$ a jednotku $u \in \{1, \omega, \omega^2\}$ (ostatné jednotky z Vety 3.1.5 nemusíme uvažovať samostatne, nakoľko $-1 = (-1)^3$).

Ak $u = 1$, máme

$$x - 1 = a^3 - 3ab^2 - b^3,$$

$$2 = 3ab^2 + 3a^2 b,$$

no pretože $\frac{2}{3}$ nie je celé číslo, tento systém rovníc nemá $\mathbb{Z}$-riešenie.

Ak $u = \omega$, dostávame

$$x + (-1 + 2\omega) = \omega a^3 - 3ab^2 + 3(\omega - 1)a^2 b - \omega b^3,$$

$$x - 1 = -3ab^2 - 3a^2 b,$$

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

pričom druhá rovnica nemá riešenie modulo 9, takže opäť celočíselné riešenie neexistuje. Rozbor modulo 9 overíme príkazom

```
Table[Mod[a^3 + 3ab^3 - b^3, 9], {a,0,8}, {b,0,8}].
```

Ak $u = \omega^2$, rovnica je v tvare

$$x + (-1 + 2\omega) = (\omega - 1)a^3 - 3\omega ab^2 - 3a^2b - (\omega - 1)b^3,$$

čím dostávame

$$x - 1 = -a^3 - 3a^2b + b^3,$$
$$2 = a^3 - 3ab^2 - b^3$$

a ani v tomto prípade druhá rovnica nie je riešiteľná modulo 9, teda nie je riešiteľná ani v $\mathbb{Z}$.

Zhrnutie

Dokázali sme, že rovnica $x^2 + 3 = y^3$ nemá žiadne $\mathbb{Z}$-riešenie.

4.4.2 Rovnica $x^2 + 7 = y^3$

Príklad 4.4.2. Riešme rovnicu

$$x^2 + 7 = y^3.$$

Elementárne úvahy, parita

Ak by jedno z čísel x alebo y bolo nulové, rovnica zjavne nemá celočíslené riešenie, t.j. $x \neq 0$ a $y \neq 0$.

Ak x, y sú rovnakej parity, potom x^2, y^3 sú tiež rovnakej parity a $x^2 + 7 \neq y^3$. Preto môžme predpokladať, že x, y majú paritu opačnú.

Rozklad v číselnom telese

Ďalej pracujme v algebraickom číselnom telese $\mathbb{Q}(\sqrt{-7})$, respektíve v jeho okruhu celistvých prvkov $\mathbb{Z}[\omega]$, kde $\omega = \frac{1+\sqrt{-7}}{2}$ podľa Sekcie 3.1.2. Vieme, že obor $\mathbb{Z}[\omega]$ je Euklidov, preto rovnicu prepíšme do tvaru

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

Spoločné delitele faktorov

Nech $\pi \in \mathbb{Z}[\omega]$ je prvočiniteľ, ktorý delí $x - \sqrt{-7}$ a $x + \sqrt{-7}$. Potom

$$\pi \mid 2x,$$

$$\pi \mid 2\sqrt{-7},$$

z čoho plynie buď $\pi \mid 2$ alebo $\pi \mid x, \sqrt{-7}$. Ak $\pi \mid \sqrt{-7}$, musí platiť

$$N(\pi) = 7 \mid N(x + \sqrt{-7}) = x^2 + 7 = y^3.$$

Tento prípad avšak vedie k sporu, nakoľko $7 \mid y^3$ implikuje $7 \mid y$ a následne $7 \mid x$, z čoho substitúciou $x := 7x_1$ a $y := 7y_1$ rovnicu dostávame do tvaru

$$7x_1^2 + 1 = 49y_1^3,$$

ktorá nemá riešenie modulo 7 a následne ani v $\mathbb{Z}$.

Takže nutne $\pi \mid 2$. Minimálny polynóm zo Sekcie 3.1.2 $f(z) = m_{\omega,\mathbb{Q}}(z)$ sa modulo 2 rozkladá na

$$f(z) = z^2 - z + 2 \equiv z(1+z) \bmod 2,$$

teda podľa Vety 1.7.8

$$(2) = (2,\omega)(2,\omega+1).$$

Zjavne $(2,\omega) = (\omega)$ a Euklidovým algoritmom dostávame $(2,\omega+1) = (1-\omega)$, čiže 2 sa v $\mathbb{Z}[\omega]$ rozkladá na $2 = \omega(1-\omega)$.

Riešenie pre párne x

Najskôr vyriešme prípad, kedy x je párne a y nepárne. Ak $\pi \mid 2$, potom $N(\pi) = 2 \mid y^3$ nepárne, čo je spor, preto $x - \sqrt{-7}$, $x + \sqrt{-7}$ sú nesúdeliteľné.

Nakoľko $\omega^2 = \omega - 2$, $\omega^3 = -2 - \omega$ a pre jednotky platí $\pm 1 = (\pm 1)^3$, dostávame

$$x + \sqrt{-7} = x - 1 + 2\omega = (a + b\omega)^3 = a^3 + 3a^2b\omega + 3ab^2\omega - 6ab^2 - 2b^3 - \omega b^3$$

pre nejaké $a,b \in \mathbb{Z}$.

Následne

$$2 = 3a^2b + 3ab^2 - b^3 = b(3a^2 + 3ab - b^2),$$

teda $b \in \{\pm 1, \pm 2\}$, no pre tieto prípady neexistuje celočíselné a, ktoré rovnicu spĺňa.

Riešenie pre nepárne x

Uvažujme ďalej x nepárne a y párne. Položme $y := 2y_1$ a uvažujme rovnicu v podobe

$$x^2 + 7 = (2y_1)^3 = 8y_1^3.$$

Nakoľko x je nepárne a teda $\frac{x \pm (\sqrt{-7})}{2} = \frac{x \pm (2\omega - 1)}{2} \in \mathbb{Z}[\omega]$, dostávame $2 \mid (x \pm \sqrt{-7})$ a rovnicu môžme prepísať na

$$\left(\frac{x + \sqrt{-7}}{2}\right)\left(\frac{x - \sqrt{-7}}{2}\right) = \frac{8}{4}y_1^3 = 2y_1^3,$$

kde $\frac{x+\sqrt{-7}}{2}, \frac{x-\sqrt{-7}}{2}$ už zjavne musia byť nesúdeliteľné.

Riešme jednotlivé možné prípady samostatne:

1. Ak
$$\frac{x + \sqrt{-7}}{2} = \frac{x - 1 + 2\omega}{2} = (a + b\omega)^3 =$$
$$= a^3 + 3a^2b\omega + 3ab^2\omega - 6ab^2 - 2b^3 - \omega b^3,$$
potom
$$x - 1 = 2a^3 - 12ab^2 - 4b^3,$$
$$1 = 3a^2b + 3ab^2 - b^3 = b(3a^2 + 3ab - b^2),$$
t.j. $b \in \{\pm 1\}$ a následne $(a,b) = (0,-1)$ a $(a,b) = (1,-1)$, z čoho plynie $x = \pm 5$. Dosadením týchto x do pôvodnej rovnice však nedostávame celočíselné riešenie pre y, a preto ani v tomto prípade celočíselné riešenie rovnice nemáme.

2. Ak
$$\frac{x+\sqrt{-7}}{2} = \frac{x-1+2\omega}{2} = 2(a+b\omega)^3,$$
potom
$$\frac{x-\sqrt{-7}}{2} = \frac{x+1-2\omega}{2} = (a+b\omega)^3$$
a
$$x+1 = 2a^3 - 12ab^2 - 4b^3,$$
$$-1 = 3a^2b + 3ab^2 - b^3 = b(3a^2 + 3ab - b^2),$$
z čoho dostávame množinu riešení druhej rovnice
$$(a,b) = (-1,1),(0,1)$$
a následne opäť $x = \pm 5$, teda analogicky riešenia originálnej rovnice nedostávame.

3. Ak
$$\frac{x+\sqrt{-7}}{2} = \frac{x-1+2\omega}{2} = \omega(a+b\omega)^3 =$$
$$= a^3\omega - 6ab^2\omega - 2b^3\omega + \omega(3a^2b + 3ab^2 - b^3) - 2(3a^2b + 3ab^2 - b^3) =$$
$$= -6a^2b - 6ab^2 + 2b^3 + \omega(a^3 - 3ab^2 + 3a^2b - 3b^3),$$
potom
$$1 = a^3 - 3ab^2 + 3a^2b - 3b^3,$$
$$x = 1 + 4b^3 - 12a^2b - 12ab^2.$$
Prvá z výsledných rovníc je Thueho rovnica, ktorej celočíselné riešenia získané príkazom

```
Solve[1 == a^3 - 3ab^2 + 3a^2 b - 3b^3, {a,b}, Integers]
```

sú $(a,b) = (1,0),(-2,3)$. Z druhej rovnice potom dostávame $x \in \{1,181\}$, následne z pôvodnej rovnice $(x,y) = (1,2)$, respektíve $(x,y) = (181,32)$.

4. Ak
$$\frac{x+\sqrt{-7}}{2} = \frac{x-1+2\omega}{2} = (1-\omega)(a+b\omega)^3,$$
potom
$$\frac{x-\sqrt{-7}}{2} = \frac{x+1-2\omega}{2} = \omega(a+b\omega)^3$$
a
$$x = -1 + 4b^3 - 12a^2b - 12ab^2,$$
$$-1 = a^3 - 3ab^2 + 3a^2b - 3b^3.$$
Opäť dostávame Thueho rovnicu a množinu jej riešení
$$(a,b) = (2,-3),(-1,0),$$
z čoho ďalej plynie $x \in \{-181,-1\}$ a finálne $(x,y) = (-181,16)$, respektíve $(x,y) = (-1,2)$.

Zhrnutie

Rovnica $x^2 + 7 = y^3$ má $\mathbb{Z}$-riešenia

$$(x,y) = (\pm 1,2),(\pm 181,32).$$

4.5 Nekonečná grupa jednotiek

Nasleduje príklad rovnice riešenej v reálnom kvadratickom telese s nekonečnou jednotkovou grupou.

4.5.1 Rovnica $x^2 - 2 = y^3$

Príklad 4.5.1. Riešme rovnicu

$$x^2 - 2 = y^3.$$

Elementárne úvahy, parita

Znovu môžme triviálne predpokladať $x \neq 0$, $y \neq 0$.

Ak by x, y boli rôznej parity, potom $x^2 - 2$, y^3 sú tiež rôznej parity a nerovnajú sa. Ak sú obe párne, $y^3 \equiv 0 \pmod 4$, no pre $x^2 - 2$ to nikdy nenastane. Takže máme x, y obe nepárne.

Rozklad v číselnom telese

Rozložme rovnicu v algebraickom číselnom telese $\mathbb{Q}(\sqrt{2})$ a jeho okruhu celistvých prvkov, ktorým je podľa Sekcie 3.1.3 Gaussov obor $\mathbb{Z}[\sqrt{2}]$, čím ju vyjadríme ako

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

Nesúdeliteľnosť faktorov

Nech $\pi \in \mathbb{Z}[\sqrt{2}]$ je prvočiniteľ, ktorý delí $x - \sqrt{2}$ a $x + \sqrt{2}$. Potom

$$\pi \mid 2x,$$

$$\pi \mid 2\sqrt{2}$$

a následne $\pi \mid 2$ alebo $\pi \mid \sqrt{2}$,x. Jediným takým prvočiniteľom môže byť $\pi \sim \sqrt{2}$, no potom $N(\pi) = -2 \mid x^2$, čo je spor, pretože x uvažujeme nepárne.

Takže $x - \sqrt{2}$ a $x + \sqrt{2}$ sú nesúdeliteľné a dostávame

$$x + \sqrt{2} = u(a + b\sqrt{2})^3$$

pre nejaké a,$b \in \mathbb{Z}$ a $u \in \mathcal{U}(\mathbb{Z}[\sqrt{2}]) = \{\pm(1 + \sqrt{2})^n,\ n \in \mathbb{Z}\}$.

Určenie riešenia

Stačí nám vyriešiť len 3 rôzne prípady

$$u \in \{(1+\sqrt{2})^j,\ j \in \{-1,0,1\}\},$$

keďže všetky ostatné jednotky vieme napísať v tvare uv^3, kde u je jedna z troch uvažovaných a v^3 bude súčasťou všeobecného $(a+b\sqrt{2})^3$.

1. Ak
$$x+\sqrt{2} = (a+b\sqrt{2})^3 = a^3+3a^2b\sqrt{2}+6ab^2+2\sqrt{2}b^3,$$
porovnaním koeficientov dostávame rovnosť
$$1 = 3a^2b+2b^3 = b(3a^2+2b^2),$$
ktorá zjavne nemá celočíselné riešenie.

2. Ak
$$x+\sqrt{2} = (1+\sqrt{2})(a+b\sqrt{2})^3,$$
dostávame rovnice
$$1 = a^3+3a^2b+6ab^2+2b^3,$$
$$x = a^3+6a^2b+6ab^2+4b^3$$
a riešením Thueho rovnice
```
Solve[1 == a^3 + 3a^2 b + 6ab^2 + 2b^3, {a,b}, Integers]
```
získavame riešenie $(a,b) = (1,0)$, potom $x = 1$ a následne $y^3 = 1-2 = -1$, čiže $y = -1$.

3. Na záver pokiaľ
$$x+\sqrt{2} = (1+\sqrt{2})^{-1}(a+b\sqrt{2})^3 = (-1+\sqrt{2})(a+b\sqrt{2})^3,$$
získavame
$$1 = a^3-3a^2b+6ab^2-2b^3,$$
$$x = -a^3+6a^2b-6ab^2+4b^3,$$
a analogicky $(a,b) = (1,0)$, $x = -1$ a $y = -1$.

Zhrnutie

Rovnica $x^2-2 = y^3$ má $\mathbb{Z}$-riešenia
$$(x,y) = (\pm 1,-1).$$

4.6 Netriviálna triedová grupa

V príkladoch tejto sekcie budeme klásť dôraz na hľadanie triedovej grupy a následné počítanie s ideálmi príslušných okruhov celistvých prvkov. Začneme rovnicou riešenou v číselnom telese $\mathbb{Q}(\sqrt{-5})$, kde algoritmus pre hľadanie triedovej grupy načrtnutý v úvodných kapitolách použijeme len v zjednodušenej podobe, no na ňu nadviažeme rovnicami v telesách $\mathbb{Q}(\sqrt{58})$ a $\mathbb{Q}(\sqrt{79})$, ktoré už budú vyžadovať využitie vybudovanej teórie spolu s netriválnymi výpočtami v plnej miere.

4.6.1 Rovnica $x^2 + 5 = y^3$

Príklad 4.6.1. Riešme rovnicu

$$x^2 + 5 = y^3.$$

Elementárne úvahy, parita

Ak by jedno z čísel x alebo y bolo nulové, rovnica celočíslené riešenie nemá, teda máme $x \neq 0$ a $y \neq 0$.

Ak x, y sú rovnakej parity, potom x^2, y^3 sú tiež rovnakej parity a $x^2 + 5 \neq y^3$. Pokiaľ je y párne, $y^3 \equiv 0 \pmod 8$, z čoho plynie, že $x^2 \equiv 3 \pmod 8$, ale 3 nie je kvadratický zvyšok mod 8. Takže môžme predpokladať, že y je nepárne a x párne.

Rozklad v číselnom telese

Pracujme v algebraickom číselnom telese $\mathbb{Q}(\sqrt{-5})$, teda podľa Sekcie 3.1.4 v okruhu celistvých prvkov $\mathbb{Z}[\sqrt{-5}]$, kde rovnicu vyjadríme ako

$$x^2 + 5 = (x - \sqrt{-5})(x + \sqrt{-5}) = y^3.$$

Obor $\mathbb{Z}[\sqrt{-5}]$ ale nie je Gaussov, ireducibilné prvky nie sú nutne prvočinitele, teda nemáme zaručenú jednoznačnosť faktorizácie prvkov okruhu. Nakoľko ale je to okruh celistvých prvkov číselného telesa $\mathbb{Q}(\sqrt{-5})$, podľa Vety 1.5.3 ide o Dedekindov obor, a preto rozklad ideálov okruhu na prvoideály už jednoznačný je.

Komaximalita faktorov

Buď $Q \in \mathbb{Z}[\sqrt{-5}]$ prvoideál, ktorý delí $(x - \sqrt{-5})$ a $(x + \sqrt{-5})$. Potom

$$Q \mid (2x),$$

$$Q \mid (2\sqrt{-5}),$$

$$N(Q) \mid N(x + \sqrt{-5}) = x^2 + 5 \text{ nepárne a}$$

$$N(Q) = p^j,\ j \leq [\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2.$$

Z toho plynie, že $N(Q) \mid 4x^2$ a $N(Q) \mid (2^2 5) = 20$, teda $N(Q) = 5$ (ostatné delitele 20 sú párne, alebo je to 1, čo by bol spor s definíciou Q ako prvoideálu).

Predpokladajme preto $N(Q) = 5$. Nakoľko $N(Q) \mid 4x^2$, $N(Q)$ musí deliť aj x^2 a aj x. Potom $y^3 \equiv x^2 + 5 \equiv 0 \pmod 5$, teda $y \equiv 0 \pmod 5$. Ale $5 = y^3 - x^2$ je násobok 25, čím dostávame spor, a preto ideály $(x - \sqrt{-5})$ a $(x + \sqrt{-5})$ sú komaximálne.

Zostavenie sústavy rovníc

Z komaximality ideálov $(x - \sqrt{-5})$ a $(x + \sqrt{-5})$ a rovnosti $(x - \sqrt{-5})(x + \sqrt{-5}) = I^3$ pre nejaký ideál I dostávame, že

$$(x + \sqrt{-5}) = J^3,$$

kde J je takisto nejaký ideál $\mathbb{Z}[\sqrt{-5}]$. Súčasne keďže $|Cl(\mathbb{Z}[\sqrt{-5}])| = 2$, J^2 je hlavný ideál. Nakoľko ale J^2 aj J^3 sú hlavné, potom z Vety 2.4.3 aj J musí byť nutne hlavný ideál.

V takom prípade ale

$$x + \sqrt{-5} = u\delta^3,$$

kde $u \in \{\pm 1\}$ je jednotka $\mathbb{Z}[\sqrt{-5}]$ a $\delta \in \mathbb{Z}[\sqrt{-5}]$. Nakoľko ale $\pm 1 = (\pm 1)^3$, $u\delta^3$ vieme napísať v tvare γ^3, pre nejaké $\gamma = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Roznásobením dostávame

$$x + \sqrt{-5} = (a^3 + 3a^2b\sqrt{-5} - 15ab^2 - 5b^3\sqrt{-5}) =$$

$$= (a^3 - 15ab^2) + \sqrt{-5}(3a^2b - 5b^3),$$

z čoho plynú nutné podmienky na riešenie pôvodnej rovnice:

$$x = a^3 - 15ab^2,$$

$$1 = 3a^2b - 5b^3 = b(3a^2 - 5b^2).$$

Určenie riešenia

Nakoľko $3a^2 - 5 \neq \pm 1$ v $\mathbb{Z}$, vidíme, že druhá podmienka je v $\mathbb{Z}$ nesplniteľná, teda ani pôvodná rovnica $x^2 + 5 = y^3$ žiadne celočíselné riešenie nemá.

4.6.2 Rovnica $x^2 - 58 = y^3$

Príklad 4.6.2. Riešme rovnicu

$$x^2 - 58 = y^3.$$

Elementárne úvahy, parita

Ak by x alebo y bolo nulové, rovnica jasne nemá celočíslené riešenie, čiže $x \neq 0$ a $y \neq 0$.

Ak by x, y boli rôznej parity, aj $x^2 - 58$ a y^3 sú rovnako rôznej parity a daná rovnica nemá riešenie. Ak by x a y boli obe párne, $x^2 - 58 \equiv 2 \pmod 4$, no $y^3 \equiv 0 \pmod 4$, takže ani tento prípad nemôže nastať, a preto môžme predpokladať x,y nepárne.

Rozklad v číselnom telese

Rovnicu prepíšme do tvaru

$$x^2 - 58 = (x - \sqrt{58})(x + \sqrt{58}) = y^3$$

v okruhu celistvých prvkov $\mathbb{Z}[\sqrt{58}]$ číselného telesa $\mathbb{Q}(\sqrt{58})$, ktorý má podľa Sekcie 3.1.5 triedové číslo $h(Q(\sqrt{58})) = 2$.

Komaximalita faktorov

Buď Q prvoideál, ktorý delí $(x+\sqrt{58})$ a $(x-\sqrt{58})$. Potom

$$Q \mid (2x),(2\sqrt{58})$$

a z definície prvoideálu buď $Q \mid (2)$ alebo $Q \mid (x),(\sqrt{58})$.

Po zohľadnení noriem je zrejmé, že $Q \nmid (2)$, nakoľko inak by $N(Q) \mid 4$ a zároveň $N(Q) \mid N((y^3)) = y^6$ nepárne, čo je spor.

Takže $Q \mid (\sqrt{58})$ a $N(Q) \mid N((\sqrt{58})) = 58$.

Opäť zrejme $N(Q) \neq 2$, pretože súčasne $N(Q) \mid y^6$ nepárne, takže zostáva uvažovať $N(Q) = 29$.

Keďže $29 \mid y^6$, $29 \mid y$ a následne aj x. Potom ale rovnicu vieme prepísať do tvaru

$$(29x_1)^2 - 58 = (29y_1)^3$$

pre $x = 29x_1$ a $y = 29y_1$, t.j. ekvivalentne

$$29x_1^2 - 2 = 29^2 y_1^3,$$

čo nemá riešenie modulo 29 a teda ani v $\mathbb{Z}$.

Teda ideály $(x+\sqrt{58})$ a $(x-\sqrt{58})$ musia byť komaximálne a

$$(x+\sqrt{58}) = J^3$$

pre nejaký ideál J.

Zostavenie sústav rovníc a určenie riešenia

Vidíme, že J^3 je hlavný ideál a keďže rád triedovej grupy je 2, J^2 musí byť tiež hlavný ideál. No v takom prípade z Vety 2.4.3 je nutne aj J hlavný a dostávame rovnosť

$$x+\sqrt{58} = u(a+b\sqrt{58})^3,$$

kde $u \in \{\pm(99+13\sqrt{58})^k, k \in \mathbb{Z}\}$ je jednotka $\mathbb{Z}[\sqrt{58}]$ a $a+b\sqrt{58}$ všeobecný prvok tohto okruhu.

Ďalej stačí uvažovať rovnicu

$$x+\sqrt{58} = (99+13\sqrt{58})^k(a+b\sqrt{58})^3$$

pre a,$b \in \mathbb{Z}$ a $k \in \{-1,0,1\}$, nakoľko ostatné prípady sú zahrnuté v tretej mocnine všeobecného prvku $a+b\sqrt{58}$.

Rozdeľme teda úlohu na tri prípady.

1. V prípade $k = 0$ máme rovnosť

$$x+\sqrt{58} = (a+b\sqrt{58})^3 = a^3 + 3a^2b\sqrt{58} + 3ab^2 58 + b^3 58\sqrt{58},$$

teda po úprave

$$x = a^3 + 174ab^2,$$

$$1 = 3a^2b + 58b^3 = b(3a^2 + 58b^2).$$

Z toho plynie, že $b = \pm 1$, no potom $3a^2 = -57$ (alebo -59) nemá celočíselné riešenie.

2. Ak $k = 1$, dostávame

$$x + \sqrt{58} = (99 + 13\sqrt{58})(a + b\sqrt{58})^3 =$$

$$= 99a^3 + 13a^3\sqrt{58} + 2262a^2b + 297a^2b\sqrt{58} +$$

$$+17226ab^2 + 2262ab^2\sqrt{58} + 43732b^3 + 5742b^3\sqrt{58}$$

a následne

$$x = 99a^3 + 2262a^2b + 17226ab^2 + 43732b^3,$$

$$1 = 13a^3 + 297a^2b + 2262ab^2 + 5742b^3.$$

Ked sa na výslednú Thueho rovnicu pozrieme modulo 9, vieme ju prepísať do tvaru

$$1 \equiv 4a^3 + 3ab^2 \equiv a(4a^2 + 3b^2) \pmod 9$$

a tá riešenie nemá. Preto neexistuje jej riešenie ani v $\mathbb{Z}$, a teda ani v prípade $k = 1$ celočíselné riešenie pôvodnej rovnice nedostávame.

3. Finálne prípad $k = -1$ vedie k

$$x + \sqrt{58} = (-99 + 13\sqrt{58})(a + b\sqrt{58})^3,$$

z čoho obdobne ako vyššie dostávame rovnosti

$$x = -99a^3 + 2262a^2b - 17226ab^2 + 43732b^3,$$

$$1 = 13a^3 - 297a^2b + 2262ab^2 - 5742b^3.$$

Výsledná Thueho rovnica je modulo 9 rovnaká ako v predošlom prípade, takže ani teraz existenciu nejakého celočíselného riešenia nezískavame.

Zhrnutie

Dokázali sme, že rovnica $x^2 - 58 = y^3$ nemá celočíselné riešenie.

4.6.3 Rovnica $x^2 - 79 = y^3$

Príklad 4.6.3. Riešme rovnicu

$$x^2 - 79 = y^3.$$

Elementárne úvahy, parita

Ak by niektoré z čísel x alebo y bolo nulové, rovnica celočíslené riešenie nemá, t.j. $x \neq 0$ a $y \neq 0$.

Ak by x, y boli rovnakej parity, $x^2 - 79$ a y^3 sú opačnej parity a rovnica takisto nemá riešenie. Ak by x bolo nepárne, potom $x^2 - 79 \equiv 2 \pmod 4$, no pre y párne platí $y^3 \equiv 0 \pmod 4$, takže ani tento prípad nemôže nastať. Preto môžme predpokladať, že x je párne a y nepárne.

Rozklad v číselnom telese

Číselnému telesu $\mathbb{Q}(\sqrt{79})$ náleží podľa Sekcie 3.1.6 okruh celistvých prvkov $\mathbb{Z}[\sqrt{79}]$, takže v ňom rovnicu prepíšme do podoby

$$x^2 - 79 = (x - \sqrt{79})(x + \sqrt{79}) = y^3.$$

Komaximalita faktorov

Buď Q prvoideál, ktorý delí $(x + \sqrt{79})$ a $(x - \sqrt{79})$. Potom $Q \mid (2x)$,$(2\sqrt{79})$ a z definície prvoideálu buď $Q \mid (2)$ alebo $Q \mid (x)$,$(\sqrt{79})$.

Po zohľadnení noriem je zrejmé, že $Q \nmid (2)$, nakoľko inak by $N(Q) \mid 4$ a zároveň $N(Q) \mid N((y^3)) = y^6$ nepárne, čo je spor.

Takže $Q \mid (\sqrt{79})$ a $N(Q) \mid N((\sqrt{79})) = 79$. Nakoľko 79 je prvočíslo, $N(Q) = 79 \mid y^6$. Potom ale $79 \mid y$ a následne aj $79 \mid x$.

Tým pádom vieme rovnicu prepísať do tvaru

$$(79x_1)^2 - 79 = (79y_1)^3$$

pre $x = 79x_1$ a $y = 79y_1$. Ekvivalentne

$$79x_1^2 - 1 = 79^2 y_1^3,$$

čo očividne nemá riešenie modulo 79 a teda ani v $\mathbb{Z}$, čím dostávame spor.

Teda ideály $(x + \sqrt{79})$ a $(x - \sqrt{79})$ musia byť komaximálne a

$$(x + \sqrt{79}) = J^3$$

pre nejaký ideál J.

Vidíme, že mocnina 3 na ideále J je súdeliteľná s veľkosťou triedovej grupy $h(\mathbb{Q}(\sqrt{79})) = 3$, teda o J nevieme povedať, či je hlavný alebo nie.

Rozbor ideálov

V takom prípade vezmime reprezentantov tried ideálov, konkrétne (1),P_2,P_2^2, pričom $P_2 = (3,2+\sqrt{79})$, uvažujme (α) hlavný ideál generovaný α ako všeobecným prvkom telesa a postupne rozoberme tri prípady, ktoré môžu nastať:

1. $J = (\alpha)$ je hlavný ideál, t.j. $(x + \sqrt{79}) = J^3 = (\alpha^3)$,
2. $J = P_2(\alpha)$, t.j. $(x + \sqrt{79}) = J^3 = P_2^3(\alpha^3)$,
3. $J = P_2^2(\alpha)$, t.j. $(x + \sqrt{79}) = J^3 = (P_2^2)^3(\alpha^3)$.

Ďalej označme $u \in \{\pm(80 + 9\sqrt{79})^k, k \in \mathbb{Z}\}$ jednotku $\mathbb{Z}[\sqrt{79}]$, položme $\alpha = \frac{a+b\sqrt{79}}{c}$ pre a,b,$c \in \mathbb{Z}$ (α nie je nutne celistvý prvok), pričom $c > 0$ a $\mathrm{NSD}(a,b,c) = 1$. Pripomeňme, že $P_2 = (3,2 + \sqrt{79})$, $P_2^3 = (-17 + 2\sqrt{79})$.

Zrejme α je celistvý práve vtedy, keď $c = 1$. V opačnom prípade, nakoľko $x + \sqrt{79}$ je celistvý, rozmyslime, že c môže v jednotlivých prípadoch v skutočnosti nadobúdať len niekoľko hodnôt:

1. $(x+\sqrt{79}) = (\alpha^3) = (\frac{a+b\sqrt{79}}{c})^3 = (\frac{a^3+3a^2b\sqrt{79}+237ab^2+79b^3\sqrt{79}}{c^3})$, teda
$$c^3 \mid a(a^2+237b^2)$$
a súčasne
$$c^3 \mid b(3a^2+79b^2).$$
Buď q ľubovolné prvočíslo, ktoré delí c^3 (nutne $q \mid c$).
   (a) Ak by $q \mid a$,b, potom by q bol spoločný deliteľ a,b,c, čo z definície α nemôže nastať.
   (b) Ak $q \mid b, a^2+237b^2$, potom $q \mid a^2$ a následne $q \mid a$, čo opäť vedie k súdeliteľným a,b,c.
   (c) Ak $q \mid a, 3a^2+79b^2$, potom $q \mid 79b^2$ a buď $q \mid 79$ alebo $q \mid b$. Druhá možnosť by znamenala súdeliteľné a,b,c, takže $q = 79 \nmid b$. Nakoľko $79^3 = q^3 \mid c^3 \mid b(3a^2+79b^2)$, potom $79^2 \mid (3a^2+79b^2)$. Pretože zároveň $79 \mid a$, nutne $79^2 \mid 79b^2$ a teda $79 \mid b$, čo však neplatí.
   (d) Finálne ak $q \mid a^2+237b^2, 3a^2+79b^2$, q delí aj jejich lineárne kombinácie, t.j. $q \mid 3(a^2+237b^2)-(3a^2+79b^2) = 2^3 79b^2$, z čoho plynie $q = 2$ alebo $q = 79$.
   V prípade $q = 2$ je zrejmé, že a,b sú obe nepárne (inak buď $2 = q \mid a$,b,c, alebo $2 \nmid a(a^2+237b^2)$) a následne $a^3+237ab^2$, $3a^b+79b^3$ sú modulo 2^3 nenulové pre ľubovolné a,b, čo je spor. Teda $q = 79$. No keďže $79 \mid 3a^2+79b^2$, rozhodne $79 \mid a$, čím sa dostávame do situácie v predchádzajúcom bode, ktorá viedla k sporu. To znamená, že $c = 1$ a α je nutne celistvý.

   Síce celistvosť prvku α rovnako ako vo všetkých predchádzajúcich úlohách bola v tomto prípade zrejmá (v rozklade sa nevyskytoval člen P_2), no overenie sme uviedli ako ilustráciu toho, čo bude nasledovať v ďalších dvoch prípadoch. Tam uvidíme, že c môže nadobúdať aj iných hodnôt a na tento postup sa niekoľkokrát odvoláme.

2. $(x+\sqrt{79}) = P_2^3(\alpha^3) = (-17+2\sqrt{79})(\frac{a+b\sqrt{79}}{c})^3$, t.j.
$$c^3 \mid r_1 := -17a^3+474a^2b-4029ab^2+12482b^3,$$
$$c^3 \mid s_1 := 2a^3-51a^2b+474ab^2-1343b^3.$$
Potom
$$c^3 \mid 2r_1+17s_1 = 27b(3a^2+79b^2),$$
$$c^3 \mid 17r_1+158s_1 = 27a(a^2+237b^2).$$
To ale znamená, že jediný prvočíselný deliteľ c je $q = 3$, keďže ostatné prípady sú rovnaké ako v predchádzajúcom bode, kde sme ich vylúčili.

   Naviac pokiaľ by $c = 3^k$, $k \geq 2$, dostávame
$$(3^k)^3 \mid 27b(3a^2+79b^2), 27a(a^2+237b^2),$$
z čoho nutne
$$3^k \mid b(3a^2+79b^2), a(a^2+237b^2),$$
no opäť z predchádzajúceho bodu vidíme, že taká situácia nemôže nastať. Takže jedinou možnosťou je $c = 3^1$.

3. $(x+\sqrt{79}) = (P_2^2)^3(\alpha^3) = (605-68\sqrt{79})(\frac{a+b\sqrt{79}}{c})^3$, t.j.

$$c^3 \mid r_2 := 605a^3 - 16116a^2b + 143385ab^2 - 424388b^3,$$

$$c^3 \mid s_2 := -68a^3 + 1815a^2b - 16116ab^2 + 47795b^3.$$

Potom

$$c^3 \mid 68r_2 + 605s_2 = 3^6b(3a^2 + 79b^2),$$
$$c^3 \mid 605r_2 + 5372s_2 = 3^6a(a^2 + 237b^2)$$

a analogicky $c \in \{3^1,3^2\}$.

Zostavenie sústav rovníc a určenie riešenia

Pozorujme, že znovu stačí uvažovať $u \in \{1, 80+9\sqrt{79}, (80+9\sqrt{79})^{-1}\}$, keďže ostatné jednotky budú zahrnuté v tretej mocnine všeobecného prvku. Jednotlivé prípady potom vedú k nasledovným sústavám rovníc:

1. $x+\sqrt{79} = u(a+b\sqrt{79})^3$

   (a) $u = 1$:

   $$x = a^3 + 237ab^2,$$
   $$1 = 3a^2b + 79b^3 = b(3a^2 + 79b^2).$$

   Druhá rovnica zjavne celočíselné riešenie nemá.

   (b) $u = 80+9\sqrt{79}$:

   $$x = 80a^3 + 2133a^2b + 18960ab^2 + 56169b^3,$$

   $$1 = 9a^3 + 240a^2b + 2133ab^2 + 6320b^3.$$

   Thueho rovnica má riešenie $(a,b) = (-19,2)$, t.j. dostávame riešenie pôvodnej rovnice $x = -302$ a $y = 45$.

   (c) $u = 80-9\sqrt{79}$:

   $$x = 80a^3 - 2133a^2b + 18960ab^2 - 56169b^3,$$

   $$1 = -9a^3 + 240a^2b - 2133ab^2 + 6320b^3.$$

   Thueho rovnica má riešenie $(a,b) = (19,2)$, t.j. $x = 302$ a následne $y = 45$.

2. $x+\sqrt{79} = u(-17+2\sqrt{79})(\frac{a+b\sqrt{79}}{c})^3$, $c \in \{1,3\}$

   (a) $u = 1$:

   $$cx = -17a^3 + 474a^2b - 4029ab^2 + 12482b^3,$$
   $$c = 2a^3 - 51a^2b + 474ab^2 - 1343b^3.$$

   (b) $u = 80+9\sqrt{79}$:

   $$cx = 62a^3 + 1659a^2b + 14694ab^2 + 43687b^3,$$

   $$c = 7a^3 + 186a^2b + 1659ab^2 + 4898b^3.$$

(c) $u = 80 - 9\sqrt{79}$:

$$cx = -2782a^3 + 74181a^2b - 659334ab^2 + 1953433b^3,$$

$$c = 313a^3 - 8346a^2b + 74181ab^2 - 219778b^3.$$

Všetky výsledné rovnice sú Thueho rovnice, no modulo 9 nemajú riešenie, a preto nemajú riešenie ani v celých číslach.

3. $x + \sqrt{79} = u(-17 + 2\sqrt{79})^2(\frac{a+b\sqrt{79}}{c})^3$, $c \in \{1,3,9\}$

(a) $u = 1$:

$$cx = 605a^3 - 16116a^2b + 143385ab^2 - 424388b^3,$$

$$c = -68a^3 + 1815a^2b - 16116ab^2 + 47795b^3.$$

(b) $u = 80 + 9\sqrt{79}$:

$$cx = 52a^3 + 1185a^2b + 12324ab^2 + 31205b^3,$$

$$c = 5a^3 + 156a^2b + 1185ab^2 + 4108b^3.$$

(c) $u = 80 - 9\sqrt{79}$:

$$cx = 96748a^3 - 2579745a^2b + 22929276ab^2 - 67933285b^3,$$

$$c = -10885a^3 + 290244a^2b - 2579745ab^2 + 7643092b^3.$$

Tieto rovnice zasa nemajú riešenie modulo 27, t.j. ani teraz celočíselné riešenie neexistuje.

Zhrnutie

Rovnica $x^2 - 79 = y^3$ má dve celočíselné riešenia $(x,y) = (\pm 302,45)$.

4.7 Rozklad v kubickom telese

Na záver sa pozrime na Diofantickú rovnicu trochu iného typu, ktorú budeme riešiť rozkladom v kubickom číselnom telese, čo sa ukáže ako rádovo náročnejší problém.

4.7.1 Rovnica $x^3 + 2x + 1 = y^2$

Príklad 4.7.1. Riešme rovnicu

$$x^3 + 2x + 1 = y^2.$$

Parita

Ak by x, y boli rovnakej parity, aj $x^3 + 2x$ a y^2 sú rovnakej parity a rovnica nemá riešenie. Takže ďalej uvažujme x a y opačnej parity.

Rozklad v číselnom telese

Uvažujme teleso zo Sekcie 3.2.1 dané reálnym koreňom θ polynómu $f(z) = z^3 + 2z + 1$, jeho okruh celistvých prvkov $\mathbb{Z}[\theta]$ a rovnicu prepíšme do tvaru

$$x^3 + 2x + 1 = (x - \theta)(x - \theta')(x - \bar{\theta}') = (x - \theta)(x^2 - (\theta' + \bar{\theta}')x + (\theta'\bar{\theta}')) = y^2,$$

kde θ' a $\bar{\theta}' \in \mathbb{C}$ sú neidentické konjugácie θ.

Porovnaním koeficientov v rovnosti

$$x^3 + 2x + 1 = (x - \theta)(x - \theta')(x - \bar{\theta}') =$$
$$= x^3 - (\theta + \theta' + \bar{\theta}')x^2 + (\theta\theta' + \theta'\bar{\theta}' + \bar{\theta}'\theta)x - (\theta\theta'\bar{\theta}')$$

dostávame

$$\theta' + \bar{\theta}' = -\theta,$$
$$\theta'\bar{\theta}' = 2 - \theta\theta' - \theta\bar{\theta}' = 2 - \theta(\theta' + \bar{\theta}') = 2 + \theta^2$$

a pôvodnú rovnicu vieme vyjadriť v tvare

$$x^3 + 2x + 1 = (x - \theta)(x^2 - (\theta' + \bar{\theta}')x + (\theta'\bar{\theta}')) = (x - \theta)(x^2 + \theta x + (\theta^2 + 2)) = y^2,$$

teda s koeficientami z okruhu celistvých prvkov $\mathbb{Z}[\theta]$.

Spoločný deliteľ faktorov

Vieme, že $h(\mathbb{Q}(\theta)) = 1$, teda podľa Vety 1.8.5 je $\mathbb{Z}[\theta]$ Gaussov obor. Buď $\alpha \in \mathbb{Z}[\theta]$ spoločný deliteľ $x - \theta$ a $x^2 + \theta x + 2 + \theta^2$. Potom

$$\alpha \mid (x - \theta)(-x + \theta) = -x^2 + 2\theta x - \theta^2,$$
$$\alpha \mid ((x^2 + \theta x + \theta^2 + 2) + (-x^2 + 2\theta x - \theta^2)) = 3\theta x + 2,$$

ďalej $\alpha \mid -3\theta(x - \theta)$ a teda $\alpha \mid ((-3\theta x + 3\theta^2) + (3\theta x + 2)) = 3\theta^2 + 2$.

Z toho plynie

$$N(\alpha) \mid N(3\theta^2 + 2) = 2^3 + 3^3 + 72 - 48 = 59,$$

čo je prvočíslo, čiže α je buď jednotka alebo prvočiniteľ $\mathbb{Z}[\theta]$.

Reprezentanti tried prvkov s normou 59 bez ohľadu na násobky jednotkami sú podľa

```
NumberFieldNormRepresentatives[Root[1 + 2 # 1 + # 1^3 &, 1], 59]
```

prvok $3\theta^2 + 2 \sim 3\theta^3 + 2\theta = -3 - 4\theta \sim 3 + 4\theta$ a prvok $3 - 2\theta$.

Zostavenie rovníc

Tým z pôvodnej rovnice, ktorú máme v tvare

$$x^3 + 2x + 1 = (x - \theta)(x^2 + \theta x + (\theta^2 + 2)) = y^2,$$

vieme vyjadriť rovnosti

$$x - \theta = \pm(2 + \theta^2)^k(3 + 4\theta)^l(a + b\theta + c\theta^2)^2$$

alebo

$$x - \theta = \pm(2 + \theta^2)^k(3 - 2\theta)^l(a + b\theta + c\theta^2)^2,$$

kde $\pm(2+\theta^2)^k$ reprezentuje možné jednotky okruhu celistvých prvkov, $(3+4\theta)^l$ či $(3-2\theta)^l$ možného spoločného deliteľa a $(a+b\theta+c\theta^2)^2$ druhú mocninu všeobecného prvku $\mathbb{Z}[\theta]$. Zjavne stačí uvažovať k,$l \in \{0,1\}$, nakoľko ostatné mocniny budú zahrnuté v prvku $(a + b\theta + c\theta^2)^2$.

Určenie riešenia

Postupne rozoberme jednotlivé prípady. Začnime variantom bez spoločného deliteľa, t.j. $l = 0$.

1. $k = 0$:

   Máme

   $$\pm(x - \theta) = (a + b\theta + c\theta^2)^2 =$$
   $$= a^2 + 2ab\theta + b^2\theta^2 + 2ac\theta^2 + 2bc(-1 - 2\theta) + c^2(-\theta - 2\theta^2) =$$
   $$= a^2 - 2bc + \theta(2ab - 4bc - c^2) + \theta^2(b^2 + 2ac - 2c^2),$$

   čo vieme prepísať na

   $$\pm x = a^2 - 2bc,$$
   $$\mp 1 = 2ab - 4bc - c^2,$$
   $$0 = b^2 + 2ac - 2c^2.$$

   Poslednú z rovností upravme tak, že ju prenásobíme b, druhú rovnosť zase c a odčítajme jednu od druhej. Dostávame

   $$\pm c = b^3 + 2bc^2 + c^3,$$

   z čoho vyplýva, že ak akékoľvek prvočíslo q delí c, potom nutne $q \mid b$. To však dáva spor s rovnicou $\mp 1 = 2ab - 4bc - c^2$, a preto $c \in \{\pm 1\}$. Doriešením sústavy získavame

   $$(a,b,c) = (\pm 1, 0, \pm 1),$$

   následne $x = 1$ a $y = \pm 2$.

2. $k = 1$:

   Máme

   $$\pm(x - \theta) = (2 + \theta^2)(a + b\theta + c\theta^2)^2 =$$
   $$= (2 + \theta^2)(a^2 + 2ab\theta + b^2\theta^2 + 2ac\theta^2 + 2bc(-1 - 2\theta) + c^2(-\theta - 2\theta^2) =$$
   $$= (2a^2 - 2ab + c^2) + \theta(-b^2 + 2ac + 2c^2) + \theta^2(a^2 - 2bc),$$

   teda dostávame sústavu rovníc

   $$\pm x = 2a^2 - 2ab + c^2,$$
   $$\mp 1 = -b^2 - 2ac + 2c^2,$$
   $$0 = a^2 - 2bc,$$

   ktorá má určite riešenia

   $$(a,b,c) = (0, \pm 1, 0), (\pm 2, \pm 1, \pm 2),$$

   následne $(x,y) = (0, \pm 1)$ a $(8, \pm 23)$, no štandardnými metódami nevieme posúdiť, či táto množina riešení je kompletná.

Pokračujme prípadom, keď spoločný deliteľ je $(3 + 4\theta)$.

1. $k = 0$:

   Máme

$$\pm(x - \theta) = (3 + 4\theta)(a + b\theta + c\theta^2)^2 =$$

$$= 3a^2 - 4b^2 - 8ac - 6bc + 8c^2 + 4a^2\theta + 6ab\theta - 8b^2\theta - 16ac\theta - 20bc\theta +$$

$$+13c^2\theta + 8ab\theta^2 + 3b^2\theta^2 + 6ac\theta^2 - 16bc\theta^2 - 10c^2\theta^2,$$

   takže

$$\pm x = 3a^2 - 4b^2 - 8ac - 6bc + 8c^2,$$

$$\mp 1 = 4a^2 + 6ab - 8b^2 - 16ac - 20bc + 13c^2,$$

$$0 = 8ab + 3b^2 + 6ac - 16bc - 10c^2.$$

2. $k = 1$:

   Máme

$$\pm(x - \theta) = (2 + \theta^2)(3 + 4\theta)(a + b\theta + c\theta^2)^2 =$$

$$= 2a^2 - 6ab + 8bc + 3c^2 - 8ab\theta - 3b^2\theta - 6ac\theta + 16bc\theta +$$

$$+10c^2\theta + 3a^2\theta^2 - 4b^2\theta^2 - 8ac\theta^2 - 6bc\theta^2 + 8c^2\theta^2,$$

   teda

$$\pm x = 2a^2 - 6ab + 8bc + 3c^2,$$

$$\mp 1 = -8ab - 3b^2 - 6ac + 16bc + 10c^2,$$

$$0 = 3a^2 - 4b^2 - 8ac - 6bc + 8c^2.$$

V týchto dvoch prípadoch riešenia výsledných sústav rovníc nájsť nevieme.

Zostávalo by nám skúmať možnosť, keď spoločný deliteľ je $(3 - 2\theta)$, avšak analogickým postupom by sme získali len sústavy rovníc, na ktorých riešenie nemáme algoritmus.

Zhrnutie

Našli sme celočíselné riešenia zadanej rovnice

$$(x,y) = (1, \pm 2),(0, \pm 1),(8, \pm 23),$$

no nami skúmanou metódou nevieme dokázať prípadnú existenciu alebo neexistenciu nejakých ďalších.

Vidíme, že táto metóda riešenia Diofantických rovníc už pri kubických algebraických číselných telesách vedie k sústavám rovníc, ktoré všeobecne riešiť nevieme, no stále nám môže pomôcť niektoré netriviálne riešenia nájsť a pôvodný problém previesť na iný.

Súvislosť s teóriou eliptických kriviek

Všimnime si však ešte, že naša rovnica je eliptickou krivkou, dokonca vo Weierstrassovom tvare. Tým sa javí zaujímavé prepojenie s teóriou eliptických kriviek a výsledok C. L. Siegela, viz [Sil09], ktorý hovorí, že množina bodov (x,y) na eliptickej krivke, kde x je celočíselné, je konečná.

Toto tvrdenie znamená nie len istotu konečného počtu riešení našej Diofantickej rovnice, ale s pomocou ďalšej analýzy dáva aj hranicu na ich maximálnu možnú veľkosť. Ak Weierstrassova rovnica nejakej krivky má celočíselné koeficienty ohraničené konštantou B, súradnice (x,y) bodu danej krivky pre $x,y \in \mathbb{Z}$ vždy spĺňajú

$$\max(|x|,|y|) < \exp([10^6 B]^{10^6}).$$

Týmto sa zo Siegelovho výsledku stáva algoritmus na riešenie vybraného typu Diofatických rovníc. V našom prípade príkazom

```
Solve[x^3 + 2x + 1 == y^2, {x,y}, Integers]
```

získavame riešenia

$$(x,y) = (1, \pm 2),(0, \pm 1),(8, \pm 23),$$

čím sme overili, že iné riešenia okrem tých, ktoré sme našli štandardným postupom, neexistujú.

Finálne zmieňme, že ako dôsledok dostávame aj fakt, že elementárne neriešiteľné sústavy Thueho rovníc, na ktoré sme v príklade narazili, v skutočnosti nemôžu mať iné riešenia. Toto pozorovanie budeme podrobnejšie skúmať v nasledujúcej kapitole, kde sa ho pokúsime zobecniť a aplikovať na väčšiu množinu rovníc.

Kapitola 5

Použitie p–adických čísel

Ako je z doterajšieho priebehu práce patrné, na čiastočné alebo úplné riešenie Diofantických rovníc je nezriedka využívaná modulárna aritmetika. Nakoľko p–adické čísla dávajú možnosť skúmať modulá mocnín prvočísel súhrnne, aplikácii našej metódy riešenia rovníc na overovanie existencie riešenia práve v okruhoch p–adických celých čísel je venovaná posledná kapitola. Zopár elementárnych vlastností p–adických čísel je zosumarizovaných na úvod v Sekcii 5.1, Sekcia 5.2 zase obsahuje niekoľko verzií Henselovho lemma, ktoré sú užitočné pri skúmaní riešitľnosti rovnice $x^2 - dc^2 = y^n$ za rôznych podmienok. Teoretická časť čerpá najmä z [TMK10].

Ďalej venujeme pozornosť Thueho rovniciam, pričom uvažujeme nasledovný problém. Položme si otázku, či vieme nájsť rovnicu tvaru $x^2 - dc^2 = y^n$, $n \geq 2$, ktorá modulo nejakú mocninu prvočísla p^k zjavne nemá riešenie - a teda nemá ani celočíselné riešenie, ale z nej plynúca Thueho rovnica už riešenia modulo q^l má pre všetky prvočísla q a ľubovolné $l \in \mathbb{Z}_{>0}$. Ak by sme boli úspešní, takýmto spôsobom by sme vedeli posudzovať neriešiteľnosť niektorých netriviálnych Thueho rovníc, pretože tie za stanovených podmienok mať celočíselné riešenie nemôžu. No za určitých predpokladov v Sekcii 5.3 tejto kapitoly ukážeme, že v skutočnosti je nájsť takú rovnicu nemožné. Na záver si v Sekcii 5.4 overíme, že predpoklady dokázaných tvrdení boli nutné.

5.1 Základy práce s p–adickými číslami

Definícia 5.1.1. (p–adické čísla)

Buď p prvočíslo. Množina p–adických čísel $\mathbb{Q}_p$ je množina všetkých formálne nekonečných súčtov $\sum_{i=k}^{\infty} b_i p^i$, kde $k \in \mathbb{Z}$, $b_k \neq 0$ a $b_i \in \{0,1,\ldots,p-1\}$ $\forall i \geq k$. Jednotlivé prvky $\mathbb{Q}_p$ sú p–adické čísla.

Ak p–adické číslo má nulové koeficienty b_i pre všetky záporné i, hovoríme o p–adickom celom čísle. Množinu p–adických celých čísel značíme $\mathbb{Z}_p$.

Nasledujúce tvrdenie hovorí, že $\mathbb{Z}_p$ je okruh, ktorého podokruhom sú celé čísla. Sčítanie a násobenie v okruhu p–adických celých čísel funguje podobne ako pri celých číslach v sústave o základe p. Invertibilné prvky okruhu $\mathbb{Z}_p$ sú všetky také, kde $b_0 \neq 0$.

Veta 5.1.2. *(Vlastnosti p–adických celých čísel)*

1. *Množina p–adických celých čísel $\mathbb{Z}_p$ tvorí okruh.*

2. $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Ďalšie tvrdenie je jedno z kľúčových v zmysle prechodu medzi p–adickými číslami a modulením.

Veta 5.1.3. *Polynóm* $f(x_1,x_2,\ldots,x_n)$ *s celočíselnými koeficientami má koreň v* $\mathbb{Z}_p$ *práve vtedy, keď má koreň modulo* p^j *pre každé* $j \geq 1$.

5.2 Riešiteľnosť $x^2-dc^2 = y^n$ v p–adických číslach

Veta 5.2.1. *(Henselovo lemma – základná verzia)*
Nech $f(x)$ *je polynóm s koeficientami v* $\mathbb{Z}$. *Predpokladajme, že existuje celé číslo* α_j, *že* $f(\alpha_j) \equiv 0 \mod p^j$ *a* $f'(\alpha_j) \not\equiv 0 \mod p$. *Potom existuje celé číslo* $\alpha_{j+1} \equiv \alpha_j \mod p^j$, *ktoré spĺňa* $f(\alpha_{j+1}) \equiv 0 \mod p^{j+1}$.

Veta 5.2.2. *(Henselovo lemma – verzia pre polynóm viacerých premenných)*
Nech $f(x_1,x_2,\ldots,x_m)$ *je polynóm s celočíselnými koeficientami. Ak existuje prvok* $(\alpha_{j,1},\alpha_{j,2},\ldots,\alpha_{j,m}) \in \mathbb{Z}^m$, *že* $f(\alpha_{j,1},\alpha_{j,2},\ldots,\alpha_{j,m}) \equiv 0 \mod p^j$ *a zároveň platí* $\nabla f(\alpha_{j,1},\alpha_{j,2},\ldots,\alpha_{j,m}) \not\equiv (0,0,\ldots,0) \mod p$, *potom* $\exists\ (\alpha_{j+1,1},\alpha_{j+1,2},\ldots,\alpha_{j+1,m}) \equiv (\alpha_{j,1},\alpha_{j,2},\ldots,\alpha_{j,m}) \mod p^j$, *tak, že* $f(\alpha_{j+1,1},\alpha_{j+1,2},\ldots,\alpha_{j+1,m}) \equiv 0 \mod p^{j+1}$.

Dôkaz. Vezmime premennú x_i, pre ktorú platí $\frac{\partial f}{\partial x_i}(\alpha_{j,1},\alpha_{j,2},\ldots,\alpha_{j,m}) \neq 0$ (kvôli nenulovosti celého gradientu $\nabla f = \left(\frac{\partial f}{\partial x_1},\frac{\partial f}{\partial x_2},\ldots,\frac{\partial f}{\partial x_m}\right)$ v danom bode taká musí existovať). Za ostatné premenné $x_{i'}$ dosaďme $\alpha_{j,i'}$ pre všetky $i' \neq i$ a aplikujme základnú verziu Henselovho lemma, z čoho tvrdenie ihneď plynie.

❑

Ďalej uvažujme $0 \neq c \in \mathbb{Z}$ ľubovolné celé číslo, $0 \neq d \in \mathbb{Z}$ ľubovolné bezštvorcové celé číslo a bližšie sa pozrime na rovnicu $x^2-dc^2 = y^n$ pre celočíselné $n > 1$.

Tvrdenie 5.2.3. *Ak* n *je nepárne, rovnica* $x^2 - dc^2 = y^n$ *má riešenie v* $\mathbb{Z}_2$.

Dôkaz. Ak dc^2 je nepárne, (0,1) je riešenie danej rovnice modulo 2. V opačnom prípade máme riešenie (1,1). Keďže $\frac{\partial(x^2-dc^2-y^n)}{\partial y}(a,1) \equiv -n1^{n-1} \equiv 1 \not\equiv 0 \mod 2$ ($a \in \{0,1\}$), použitím Henselovho lemma pre polynóm viacerých premenných dostávame existenciu riešenia modulo 2^2. Naviac toto riešenie je v tvare $(a + 2r,1 + 2r)$, no $\frac{\partial(x^2-dc^2-y^n)}{\partial y}(a + 2r, 1 + 2r) \not\equiv 0 \mod 2$, teda opakovaným použitím Henselovho lemma dostávame existenciu riešení modulo 2^j pre všetky $j \in \mathbb{Z}_{>0}$, následne z Vety 5.1.3 aj v $\mathbb{Z}_2$.

❑

Tvrdenie 5.2.4. *Nech* $p \neq 2$. *Ak* $p \mid c$ *alebo* $p \mid d$, *potom* $x^2 - dc^2 = y^n$ *má riešenie v* $\mathbb{Z}_p$.

Dôkaz. Ak $p \mid d$, $d = pr$ a $x^2 - dc^2 = x^2 - prc^2 = y^n$ má riešenie (1,1) mod p. Gradient $(2x,ny^{n-1})(1,1) = (2,n) \not\equiv (0,0) \mod p$, nakoľko $p \neq 2$. Keďže gradient je

modulo p nenulový aj pre prvky $(1+rp,1+sp)$, opakovaným použitím Henselovho lemma pre polynóm viac premenných získame riešenie modulo p^j pre všetky $j \in \mathbb{Z}_{>0}$. Následne z Vety 5.1.3 máme riešenie v $\mathbb{Z}_p$.

Prípad $p \mid c$ je analogický.

❑

Veta 5.2.5. *(Henselovo lemma – p–adická verzia)*

Nech $f(x)$ je polynóm s koeficientami v $\mathbb{Z}_p$. Predpokladajme, že existuje p–adické celé číslo α_1, že $f(\alpha_1) \equiv 0 \ mod\ p\mathbb{Z}_p$ a $f'(\alpha_1) \not\equiv 0 \ mod\ p\mathbb{Z}_p$. Potom existuje p–adické celé číslo $\alpha \equiv \alpha_1 \ mod\ p\mathbb{Z}_p$, pre ktoré $f(\alpha) = 0$.

Veta 5.2.6. *(Henselovo lemma – p–adická verzia pre polynóm viacerých premenných)*

Nech $f(x_1,x_2,\ldots,x_m)$ je polynóm s koeficientami v $\mathbb{Z}_p$. Ak existujú p–adické celé čísla $\alpha_1,\alpha_2,\ldots,\alpha_m$ také, že $f(\alpha_1,\alpha_2,\ldots,\alpha_m) \equiv 0 \ mod\ p\mathbb{Z}_p$ a súčasne platí $\nabla f(\alpha_1,\alpha_2,\ldots,\alpha_m) \not\equiv (0,0,\ldots,0) \ mod\ p\mathbb{Z}_p$, potom existujú p–adické celé čísla $\alpha'_1,\alpha'_2,\ldots,\alpha'_m$, také, že $(\alpha'_1,\alpha'_2,\ldots,\alpha'_m) \equiv (\alpha_1,\alpha_2,\ldots,\alpha_m) \ mod\ p\mathbb{Z}_p$ a zároveň $f(\alpha'_1,\alpha'_2,\ldots,\alpha'_m) = 0$.

Dôkaz. Dôkaz je analogický ako v prípade Henselovho lemma v $\mathbb{Z}$, viz Veta 5.2.2. ❑

Ak $d \in \mathbb{Z}$, potom prvok $\delta \in \mathbb{Z}_p$ taký, že $\delta^2 = d$ v $\mathbb{Z}_p$, nazývame druhou odmocninou z d v $\mathbb{Z}_p$. Tento prvok nemusí nutne existovať a nie je určený jednoznačne, nakoľko korene polynómu $x^2 - d$ môžu byť dva. Nevieme ich však navzájom rozlíšiť, preto ľubovolný pevne zvolený koreň budeme ďalej značiť $\sqrt{d}$. Naviac ak $\sqrt{d}$ existuje v $\mathbb{Q}_p$, nutne leží v $\mathbb{Z}_p$.

Ak taký prvok neexistuje, potom budeme v ďalších sekciách pracovať s kvadratickým rozšírením $K/\mathbb{Q}_p$, kde

$$K = \mathbb{Q}_p(x)/(x^2 - d) = \mathbb{Q}_p(\delta)$$

pre δ spĺňajúce $\delta^2 = d$. Takýto prvok δ označíme opäť ako $\sqrt{d}$.

Tvrdenie 5.2.7. *Nech p je nepárne prvočíslo a $d \in \mathbb{Z}$ také, že $p \nmid d$. Potom prvok $\sqrt{d} \in \mathbb{Z}_p$ existuje práve vtedy, keď d je kvadratické reziduum modulo p.*

Dôkaz. Majme polynóm

$$P(x) = x^2 - d.$$

Ak d je kvadratické reziduum modulo p, potom existuje $\sqrt{d} \in \mathbb{Z}/p\mathbb{Z}$ tak, že $P(\sqrt{d}) \equiv 0 \bmod p$ a zároveň $P'(\sqrt{d}) = 2\sqrt{d} \not\equiv 0 \bmod p$, keďže $p \neq 2$ a $p \nmid d$. Následne z p–adickej verzie Henselovho lemma plynie existencia $\sqrt{d} \in \mathbb{Z}_p$.

Ak d je kvadratické nereziduum modulo p, $P(x)$ nemá koreň modulo p. No vzhľadom na Vetu 5.1.3 polynóm má koreň v $\mathbb{Z}_p$ práve vtedy, keď má koreň modulo p^j $\forall j \geq 1$. Preto $P(x)$ nemá koreň ani v $\mathbb{Z}_p$.

❑

Veta 5.2.8. *Ak existuje $\sqrt{d}$ v $\mathbb{Z}_p$, $p \neq 2$, potom $x^2 - dc^2 = y^n$ má v $\mathbb{Z}_p$ riešenie.*

Dôkaz. Z Tvrdenia 5.2.4 pokiaľ by $p \mid c$ alebo $p \mid d$, riešenie rovnice $x^2 - dc^2 = y^n$ v $\mathbb{Z}_p$ existuje. Predpokladajme ďalej $p \nmid c,d$ a znovu uvažujme polynóm

$$P(x) = x^2 - d.$$

Nech existuje $\sqrt{d} \in \mathbb{Z}_p$. Potom z Tvrdenia 5.2.7 máme d kvadratické reziduum modulo p, no v takom prípade $x^2 - dc^2 = y^n$ má riešenie $(c\sqrt{d},0)$ modulo p a aplikovaním Henselovho lemma pre viac premenných dostávame riešenia mod p^j $\forall j \geq 1$. Použitím Vety 5.1.3 dostávame koreň aj v $\mathbb{Z}_p$. Nakoľko $p \neq 2$ a $p \nmid c,d$, $2c\sqrt{d} + pr \not\equiv 0 \bmod p$ a teda Henselovo lemma je použité korektne.

❑

5.3 Thueho rovnice v p–adických číslach

Predpokladajme, že sme pri riešení rovnice $x^2 - dc^2 = y^n$ rozkladom v číselnom telese $K = \mathbb{Q}(\sqrt{d})$, respektíve okruhu celistvých prvkov $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ alebo $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, dospeli k rovnosti $x + c\sqrt{d} = ua^n$, kde $u \in \mathcal{U}(\mathcal{O}_K)$ je jednotka. Vzápätí sme získali nejakú Thueho rovnicu

$$T(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n - \delta c = 0,$$

kde $a_i \in \mathbb{Z}$ a $\delta \in \{1,2\}$ v závislosti na okruhu celistvých prvkov.

Veta 5.3.1. *Nech $p \neq 2$ a $p \nmid c$, $p \nmid n$. Ak existuje $l \in \mathbb{Z}_{>0}$, že $T(x,y)$ má riešenie modulo p^l, potom $T(x,y)$ má riešenie aj v $\mathbb{Z}_p$.*

Dôkaz. Nech existuje $l \in \mathbb{Z}_{>0}$ také, že $T(x,y)$ má riešenie (α, β) mod p^l. No potom toto riešenie je určite riešením $T(x,y)$ aj modulo p a aj modulo $p\mathbb{Z}_p$, t.j. $T(\alpha, \beta) \equiv 0 \bmod p\mathbb{Z}_p$. Pre použitie p–adickej verzie Henselovho lemma pre polynóm viacerých premenných treba overiť predpoklad nenulového gradientu modulo p.

Keďže

$$T(x,y) = \sum_{i=0}^{n}(a_ix^{n-i}y^i) - \delta c,$$

potom

$$\frac{\partial T}{\partial x} = a_0nx^{n-1} + (n-1)a_1x^{n-2}y + \cdots + a_{n-1}y^{n-1} =$$

$$= \sum_{i=0}^{n}(n-i)a_ix^{n-i-1}y^i,$$

$$\frac{\partial T}{\partial y} = a_1x^{n-1} + 2a_2x^{n-2}y + \cdots + (n-1)a_{n-1}xy^{n-2} + a_nny^{n-1} =$$

$$= \sum_{i=0}^{n} ia_ix^{n-i}y^{i-1}.$$

Vieme, že $\left(\frac{\partial T}{\partial x}, \frac{\partial T}{\partial y}\right)(\alpha,\beta) \equiv (0,0) \bmod p\mathbb{Z}_p$, no potom aj

$$\alpha\frac{\partial T}{\partial x}(\alpha,\beta) \equiv \alpha\sum_{i=0}^{n}(n-i)a_i\alpha^{n-i-1}\beta^i \equiv \sum_{i=0}^{n}(n-i)a_i\alpha^{n-i}\beta^i \equiv 0,$$

$$\beta\frac{\partial T}{\partial y}(\alpha,\beta) \equiv \beta\sum_{i=0}^{n} ia_i\alpha^{n-i}\beta^{i-1} \equiv \sum_{i=0}^{n} ia_i\alpha^{n-i}\beta^i \equiv 0.$$

To znamená

$$\sum_{i=0}^{n}((n-i)a_i\alpha^{n-i}\beta^i) + \sum_{i=0}^{n}(ia_i\alpha^{n-i}\beta^i) \equiv n\sum_{i=0}^{n} a_i\alpha^{n-i}\beta^i \equiv n\delta c \equiv 0,$$

čiže $p \mid n\delta c$ a následne $p \mid n$, $p \mid c$, alebo $p = 2$, čo z predpokladu nemôže nastať. ❑

Ďalším tvrdením sa dostávame k vzťahu medzi p–adickými riešeniami pôvodnej rovnice $x^2 - dc^2 = y^n$ a z nej plynúcej Thueho rovnice $T(x,y)$.

Veta 5.3.2. *Nech $K = \mathbb{Q}(\sqrt{d})$ je číselné teleso, NSD($h(K)$,n) = 1, kde $h(K)$ je triedové číslo K, $x+c\sqrt{d}$, $x-c\sqrt{d}$ sú nesúdeliteľné v príslušnom okruhu celistvých prvkov $\mathcal{O}_K$ a v prípade, že n je párne, $N(u) = 1$ pre všetky jednotky $u \in \mathcal{U}(\mathcal{O}_K)$. Ak $T(x,y)$ má riešenie v $\mathbb{Z}_p$, potom aj rovnica $x^2 - dc^2 = y^n$ má riešenie v $\mathbb{Z}_p$.*

Dôkaz. Nech $T(x,y)$ má riešenie (α,β) v $\mathbb{Z}_p$. Dosadením tohto riešenia do rovnosti $x + c\sqrt{d} = ua^n$ v $\mathbb{Z}_p[\sqrt{d}]$ (prípadne $\mathbb{Z}_p[\frac{1+\sqrt{d}}{2}]$) dostávame $\alpha^2 - dc^2 = (\alpha + c\sqrt{d})(\alpha - c\sqrt{d}) = u\bar{u}a^n\bar{a}^n = \pm(a\bar{a})^n = \pm\beta^n$, kde $\bar{u}$, $\bar{a}$ sú konjugácie u, respektíve a, v $\mathcal{O}_K$. Prípad $\alpha^2 - dc^2 = -\beta^n$ môže nastať len pokiaľ n je párne a $N(u) = -1$, čo podľa predpokladu nie je možné, čím sme dokázali, že určite existuje riešenie rovnice $x^2 - dc^2 = y^n$ v $\mathbb{Z}_p$.

❑

Spojením doteraz dokázaných tvrdení získame zaujímavý výsledok, ktorý hovorí, že pokiaľ rovnica $x^2 - dc^2 = y^n$ nemá riešenie modulo nejakú mocninu prvočísla, potom ani z nej vyplývajúca Thueho rovnica riešenie nemá. Predpokladom, za ktorých toto tvrdenie platí, sa budeme venovať separátne v Sekcii 5.4.

Dôsledok 5.3.3. *Nech $K = \mathbb{Q}(\sqrt{d})$ je číselné teleso, NSD($h(K)$,n) = 1 a nech existuje prvočíslo p, že rovnica $x^2 - dc^2 = y^n$, $n \geq 2$, nemá riešenie modulo p^k pre nejaké $k \in \mathbb{Z}_{>0}$. Ďalej nech $x + c\sqrt{d}$, $x - c\sqrt{d}$ sú nesúdeliteľné v príslušnom okruhu celistvých prvkov $\mathcal{O}_K$ a v prípade, že n je párne, $N(u) = 1$ pre všetky jednotky $u \in \mathcal{U}(\mathcal{O}_K)$.*

a) Potom existuje $l \in \mathbb{Z}_{>0}$, že vyplývajúca Thueho rovnica $T(x,y)$ nemá riešenie modulo p^l.

b) Pokiaľ $p \nmid n$, potom dokonca pre všetky $l \in \mathbb{Z}_{>0}$ platí, že vyplývajúca Thueho rovnica $T(x,y)$ nemá riešenie modulo p^l.

Dôkaz.

a) Pre spor nech Thueho rovnica $T(x,y)$ má riešenie modulo p^j pre každé $j \in \mathbb{Z}_{>0}$. Potom z Vety 5.1.3 existuje riešenie tejto rovnice aj v $\mathbb{Z}_p$ a priamou aplikáciou Vety 5.3.2 dostávame, že v $\mathbb{Z}_p$ existuje riešenie $x^2 - dc^2 = y^n$. Opätovným použitím Vety 5.1.3 však dostávame riešenia rovnice $x^2 - dc^2 = y^n$ modulo p^j pre každé $j \in \mathbb{Z}_{>0}$ a tým aj spor s jej neriešiteľnosťou mod p^k.

b) Ak by $p = 2$, potom n by bolo nutne nepárne, inak nastáva spor s predpokladom $p \nmid n$. Následne z Tvrdenia 5.2.3 dostávame riešenie $x^2 - dc^2 = y^n$ v $\mathbb{Z}_2$. Z Vety 5.1.3 však existuje riešenie rovnice $x^2 - dc^2 = y^n$ modulo 2^k, čo je opäť spor, a preto $p \neq 2$.

   Analogickým použitím Tvrdenia 5.2.4 dostávame $p \nmid c$ a ďalej postupujme sporom.

   Nech existuje $j \in \mathbb{Z}_{>0}$, pre ktoré Thueho rovnica $T(x,y)$ má riešenie mod p^j. Potom z Vety 5.3.1 $T(x,y)$ má riešenie v $\mathbb{Z}_p$ a rovnakým postupom ako v prípade a) dostávame spor s neriešiteľnosťou rovnice $x^2 - dc^2 = y^n$ modulo p^k.

❑

Záverečný dôsledok sa opiera o Čínsku vetu o zvyškoch a zovšeobecňuje predošlé tvrdenie z mocniny prvočísla na ľubovolné $m \in \mathbb{Z}_{>0}$.

Dôsledok 5.3.4. *Nech $K = \mathbb{Q}(\sqrt{d})$ je číselné teleso, NSD($h(K)$,n) = 1 a nech existuje $m \in \mathbb{Z}_{>0}$, že rovnica $x^2 - dc^2 = y^n$, $n \geq 2$, nemá riešenie modulo m. Ďalej nech $x + c\sqrt{d}$, $x - c\sqrt{d}$ sú nesúdeliteľné v príslušnom okruhu celistvých prvkov $\mathcal{O}_K$ a v prípade, že n je párne, $N(u) = 1$ pre všetky jednotky $u \in \mathcal{U}(\mathcal{O}_K)$.*

a) Potom existuje prvočíslo $p \mid m$ a $l \in \mathbb{Z}_{>0}$, že vyplývajúca Thueho rovnica $T(x,y)$ nemá riešenie modulo p^l.

b) Ak NSD(m,n) = 1, potom existuje prvočíslo $p \mid m$, že vyplývajúca Thueho rovnica $T(x,y)$ nemá riešenie modulo p^l pre všetky $l \in \mathbb{Z}_{>0}$.

Dôkaz. Buď $m = \prod_{i=1}^{s} p_i^{k_i}$ prvočíselný rozklad m. Pre spor predpokladajme, že daná Thueho rovnica $T(x,y)$ má riešenie modulo všetky p_i^l, $i \leq s$, $l \in \mathbb{Z}_{>0}$ (respektíve, že existujú $l_i \in \mathbb{Z}_{>0}$, $i \leq s$, pre ktoré rovnica má riešenie mod $p_i^{l_i}$). Z jednotlivých krokov dôkazu Dôsledku 5.3.3 však vidíme, že nech zoberieme ktorékoľvek p_j, $j \in \{1,\ldots,s\}$, rovnica $x^2 - dc^2 = y^n$ má v $\mathbb{Z}/p_j^{k_j}\mathbb{Z}$ vždy riešenie. Následným použitím Čínskej vety o zvyškoch musí mať $x^2 - dc^2 = y^n$ riešenie aj v $\mathbb{Z}/m\mathbb{Z}$, čím dostávame spor.

❑

5.4 Analýza predpokladov

Nesúdeliteľnosť faktorov

Jedným z predpokladov výsledného Dôsledku 5.3.3 a 5.3.4 je nesúdeliteľnosť prvkov $x+c\sqrt{d}$, $x-c\sqrt{d}$. Teraz ukážme, prečo bol tento predpoklad nevyhnutný a dajme príklad rovnice, ktorá zjavne nemá riešenie modulo 5, no z nej vyplýva viacero Thueho rovníc, z ktorých jedna celočíselné riešenie má.

Uvažujme rovnicu $x^2+3 = y^4$ a chvíľu ignorujme fakt, že nemá riešenie modulo 5 a skúsme aplikovať štandardný postup riešenia.

Zjavne x musí byť nepárne a y párne (inak je dôkaz neriešiteľnosti ešte jednoduchší modulo 2, respektíve 4). Keďže $-3 \equiv 1 \bmod 4$, pracujeme v okruhu celistvých prvkov $Z[\omega]$, kde $\omega = \frac{1+\sqrt{-3}}{2}$.

Podľa Vety 3.1.5 je prvok ω jedna z jednotiek.

Napíšme teda rovnicu v tvare $(x+\sqrt{-3})(x-\sqrt{-3}) = (x-1+2\omega)(x-1-2\omega) = y^4$. Nakoľko x je nepárne, v danom okruhu celistvých prvkov je zrejme 2 spoločným deliteľom $(x-1+2\omega)$,$(x-1-2\omega)$.

Rovnicu teda môžme napísať ako

$$\left(\frac{x-1+2\omega}{2}\right)\left(\frac{x-1-2\omega}{2}\right) = \frac{y^4}{4} = 4y_1^4,$$

kde už prvky $\frac{x-1+2\omega}{2}$, $\frac{x-1-2\omega}{2}$ nesúdeliteľné sú, a preto určite

$$\frac{x-1+2\omega}{2} = \lambda u(a+b\omega)^4,$$

kde za u zvoľme ω a $\lambda \in \{1,2,4\}$.

Z toho následne (bez detailnejšieho skúmania) plynú 3 Thueho rovnice

$$1 = \lambda(a^4+4a^3b-4ab^3-b^4).$$

Napriek neriešiteľnosti pôvodnej rovnice, v prípade, že $\lambda = 1$, Thueho rovnica má celočíselné riešenia $(a,b) = (\pm 1,0)$. Z toho potom plynie $x = 1$, no dosadením do pôvodnej rovnice $1^2+3 = 4 = y^4$ skutočne nedostávame celočíselné riešenie.

Takže všeobecne pri riešení rovníc, kde môže existovať netriviálny spoločný deliteľ $x+c\sqrt{d}$, $x-c\sqrt{d}$, náš postup zvyčajne vedie k viacerým Thueho rovniciam, a preto neplatí ekvivalencia riešiteľnosti pôvodnej rovnice a ľubovolnej z nej plynúcej Thueho rovnice.

Jednotky s kladnou normou

Ďalším predpokladom v tvrdení je použitie jednotky s normou 1 pre získanie Thueho rovnice v prípade, že n je párne. Ukážme príklad, že aj tento predpoklad je pre platnosť tvrdenia nevyhnutný.

Rovnica $x^2 - 32 = y^4$ je zjavne neriešiteľná modulo 5. No skúsme na ňu aplikovať štandardný postup riešenia, ak uvažujeme x,y obe nepárne (v prípade, že x,y sú párne, je 2 spoločným deliteľom $x+4\sqrt{2}$, $x-4\sqrt{2}$ a vtedy tvrdenie platiť nemusí z dôvodu uvedeného vyššie).

Ak by α bol spoločný deliteľ $x+4\sqrt{2}$, $x-4\sqrt{2}$ v $\mathbb{Z}[\sqrt{2}]$, potom $\alpha \mid 2x, 8\sqrt{2}$, t.j. $\alpha \mid 2$ a $2 \mid y^4$ nepárne. To znamená, že $x+4\sqrt{2}$, $x-4\sqrt{2}$ sú nutne nesúdeliteľné

a $x + 4\sqrt{2} = u(a + b\sqrt{2})^4$, kde za u zvoľme jednotku $1 + \sqrt{2}$ s normou -1. Roznásobením dostávame Thueho rovnicu

$$4 = a^4 + 4a^3b + 12a^2b^2 + 8ab^3 + 4b^4,$$

ktorá má riešenia $(a,b) = (0, \pm 1)$, z čoho by následne vyplývalo $x = 4$, no tým by sme dostali spor s predpokladom nepárneho x. Ako je z dôkazu tvrdenia patrné, $x = 4$ je skutočne riešením rovnice $x^2 - c^2d = x^2 - 32 = -y^4$.

Každopádne týmto spôsobom sme dostali Thueho rovnicu, ktorá má celočíselné riešenia, hoci pôvodná rovnica riešenie zjavne nemá žiadne, a preto je aj tento predpoklad tvrdenia nutný.

Triedové číslo

Úvodný predpoklad nesúdeliteľnosti n s veľkosťou triedovej grupy je zrejmý, nakoľko nám podľa Vety 2.4.3 umožňuje pracovať len s hlavnými ideálmi daného okruhu celistvých prvkov.

Poznámka.

- Predpoklady tvrdení sa potenciálne dajú ešte trochu oslabiť použitím silnejšej verzie Henselovho lemma, viz [Shu12].
- V úvode kapitoly sme chceli nájsť triviálne neriešiteľnú rovnicu tvaru $x^2 - dc^2 = y^n$, $n \geq 2$, z ktorej plynúca Thueho rovnica by už riešenia modulo q^l mala pre všetky prvočísla q a ľubovolné $l \in \mathbb{Z}_{>0}$. Zistili sme, že pokiaľ je pôvodná rovnica neriešiteľná modulo nejakú mocninu prvočísla, takú Thueho rovnicu sa nám nájsť nepodarí. Otázkou však zostáva, či by sme tieto zaujímavé prípady nevedeli získať v prípade neriešiteľnosti pôvodnej rovnice v $\mathbb{Z}$ dokázanej nejakou inou metódou, podobne ako sa to podarilo v Kapitole 4 v súvislosti s rovnicou rozkladanou v kubickom telese a eliptickými krivkami.

Záver

V práci sme popísali nástroj algebraickej teórie čísel na riešenie určitého typu Diofantických rovníc a demonštrovali ho na vzorovom súbore úloh odlišnej náročnosti. Popísali sme možné úskalia, ktoré metóda rozkladu v číselnom telese so sebou prináša, čím sme pokryli niekoľko rozdielnych typov rovníc a pripravili návod na riešenie množstva ďalších.

Naviac sme zistili, že riešenie rovníc závisí aj na znalosti triedovej grupy a grupy jednotiek príslušného číselného telesa, rovnako ako na niektorých kľúčových výsledkoch v oblasti Diofantických rovníc z histórie, napríklad známych algoritmov na riešenie Pellovej a Thueho rovnice. Niekoré skupiny Thueho rovníc sme skúmali aj v p–adických číslach, pričom sme sa snažili najmä o efektívnejšie overenie ich neriešiteľnosti. Dokázali sme, že faktorizácia v číselnom telese a prosté modulenie na netriviálne prípady nestačia, no otázka, či by princíp neplatil pri použití silnejšej teórie, zostáva otvorená. Isté možnosti nám však ukázal prípad rovnice rozkladanej v kubickom telese.

Pre lepšie pochopenie tejto práce odporúčame čitateľom aplikovať metódu aj na ďalšie rovnice riešiteľné analogickým postupom, z ktorých ako ilustráciu uvádzame viacero možných príkladov. Z elementárnych za zmienku stojí rovnica $x^2 + 2 = y^3$, pričom tú ako prvý vyriešil už Pierre Fermat, ďalej rovnice s nekonečnou grupou jednotiek $x^2 - 7 = y^3$, $x^2 - 22 = y^3$ alebo $x^2 - 158 = y^3$, ktoré celočíselné riešenia nemajú.

Naopak nejaké riešenia existujú pri rovniciach $x^2 + 13 = y^3$, $x^2 + 193 = y^3$ a $x^2 + 74 = y^3$, ale u tých najskôr treba správne určiť triedovú grupu číselného telesa. Zložitejšia je rovnica $x^2 + 31 = y^3$, nakoľko triedové číslo $\mathbb{Q}(\sqrt{-31})$ nie je nesúdeliteľné s exponentom pri y. Vhodným príkladom rovnice o troch premenných je $x^4+y^4 = z^2$ a rovnice s rozkladom v kubickom telese $x^3-4x+2 = 2y^2$. Vyššie mocniny zasa treba brať do úvahy v rovniciach $x^2 + 1 = y^5$, $x^2 - 7 = y^5$ alebo $x^2 + 13 = y^7$.

Na prácu by sa dalo nadviazať vytvorením a implementáciou všeobecného algoritmu na riešenie rovníc tvaru $x^2 - dc^2 = y^n$ skúmanou metódou, prípadne hlbšou analýzou rovníc iného typu. Takisto by sa v téme dalo pokračovať rozborom niektorých rovníc vyšších stupňov a rozkladom v cyklotomických telesách.

Literatúra

[AW03] Saban Alaca and Kenneth S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2003.

[Coh93] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, 1993.

[Coh07] Henri Cohen, *Number Theory: Volume I: Tools and Diophantine Equations*, Graduate Texts in Mathematics, Springer, 2007.

[IR98] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, Springer, 1998.

[ME05] Jody Murty and Maruti Ram Esmonde, *Problems In Algebraic Number Theory*, Springer Verlag, Secaucus, New Jersey, U.S.A., 2005.

[Mil14] James S. Milne, *Algebraic Number Theory (v3.06)*, 2014, http://www.jmilne.org/math/CourseNotes/ANT.pdf.

[Shu12] Jerry Shurman, *Math 361: Number Theory - Sixth Lecture*, 2012, http://people.reed.edu/∼jerry/361/lectures/lec06.pdf.

[Sil09] Joseph H. Silverman, *The Arithmetic of Eliptic Curves*, 2nd ed., Graduate Texts in Mathematics, Springer, 2009.

[TMK10] Zerzaihi Tahar, Kecies Mohamed, and Michael Knapp, *Hensel Codes of Square Roots of p–adic Numbers*, Applicable Analysis and Discrete Mathematics 4 (2010), 32–44.

Značenie

$\mathbb{Z}_{>0}$	množina prirodzených čísel, $\{1,2,\dots\}$
$\mathbb{Z}$	okruh celých čísel, $\{0,\pm 1,\pm 2,\dots\}$
$\mathbb{Z}_p$	okruh p–adických celých čísel
$\mathbb{Q}$	teleso racionálnych čísel
$\mathbb{Q}_p$	teleso p–adických čísel
$\mathbb{R}$	teleso reálnych čísel
$\mathbb{C}$	teleso komplexných čísel
$\mathbb{Z}/m\mathbb{Z}$	okruh celočíselných zbytkov modulo m, $\{0,1,\dots,m-1\}$
$\mathcal{O}_K$	okruh celistvých prvkov telesa K
$H(K)$, $Cl(\mathcal{O}_K)$	triedová grupa telesa K
$h(K)$	triedové číslo telesa K
$\mathcal{U}(\mathcal{O}_K)$	grupa jednotiek telesa K
$d(K)$	diskriminant telesa K
M_K	Minkowského hranica pre teleso K
$a \equiv b \bmod p$	prvok a je kongruentný prvku b modulo p
$a \approx b$	a je približne rovné b
$[a]$	trieda ekvivalencie obsahujúca prvok a
$\lvert M\rvert$	veľkosť (kardinalita) množiny M
$\lvert m\rvert$	absolútna hodnota čísla m
$a \mid b$	a delí b, t.j. $\exists\, c$ také, že $ac = b$
NSD(a,b)	najväčší spoločný deliteľ prvkov a,b
$\left(\frac{m}{p}\right)$	Legendrov symbol m nad p
$\phi(m)$	Eulerova funkcia ϕ celého čísla m
$\deg(f)$	stupeň polynómu f
g'	derivácia funkcie g
∇g	gradient $\left(\frac{\partial g}{\partial x_1}, \frac{\partial g}{\partial x_2}, \dots, \frac{\partial g}{\partial x_n}\right)$ funkcie $g(x_1, x_2, \dots, x_n)$
$R[a_1,\dots,a_n]$	ak R je podobor S, $a_1,\dots,a_n \in S$, $R[a_1,\dots,a_n]$ je najmenší podobor S obsahujúci R a $\{a_1,\dots,a_n\}$
$K(a_1,\dots,a_n)$	ak $K \leq L$ je rozšírenie telies, $a_1,\dots,a_n \in L$, $K(a_1,\dots,a_n)$ je najmenšie podteleso L obsahujúce K a $\{a_1,\dots,a_n\}$
$m_{\alpha,K}(x)$	minimálny polynóm prvku α nad telesom K
$a \sim b$	$a = ub$, kde u je nejaká jednotka
(a)	hlavný ideál generovaný prvkom a
$N(a)$, $N(I)$	norma prvku a (respektíve ideálu I)
G/H	faktorgrupa grupy G podľa podgrupy H
$(R : I)$	veľkosť faktorokruhu R/I, kde R je okruh a I jeho ideál
$[L : K]$	stupeň telesového rozšírenia L nad K