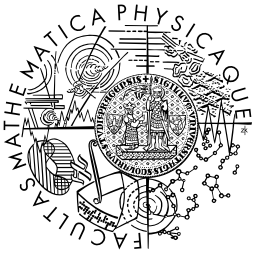


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Daniela Lněničková

Geometrické řešení kvadratických diofantických rovnic

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D.
Studijní program: MOMP
Studijní obor: Obecná matematika

Praha 2022

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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 má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Děkuji panu doc. Mgr. Vítězslavu Kalovi, Ph.D. za trpělivost a ochotu při vedení mé práce.

Název práce: Geometrické řešení kvadratických diofantických rovnic

Autor: Daniela Lněničková

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Hlavní motivací práce je shrnutí a zobecnění metody na řešení kvadratických diofantických rovnic. Problém hledání řešení diofantických rovnic převedeme na hledání průsečíků přímek a dané kvadriky. Teorie pracuje s obecným tělesem a je schopná řešit rovnice vedoucí na kvadriky o n neznámých. Pak teorii aplikujeme na vyřešení některých příkladů, konkrétně hledání pythagorejských trojic nad $Z[i]$ a rovnici vedoucí na hyperboloid, kde využijeme naše zobecnění.

Klíčová slova: kvadrika, diofantická rovnice, největší společný dělitel, gaussovská celá čísla

Title: Geometric solution of quadratic diophantine equations

Author: Daniela Lněničková

Department: Department of algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of algebra

Abstract: The main goal of the work is to summarize and generalize a method for solving quadratic Diophantine equations. We transform the problem of finding the solution of Diophantine equations to finding the intersections of lines and a given quadric. The theory works over a general field and is able to solve equations leading to quadrics of n variables. We then apply the theory to solve some examples, namely the search for Pythagorean triplets over $\mathbb{Z}[i]$ and the equation leading to the hyperboloid, where we use our generalization.

Keywords: quadric, Diophantine equation, greatest common divisor, Gaussian integer

Obsah

Úvod

Na úvod si něco povíme o tom, co je to diofantická rovnice a něco k historii. V těchto dvou odstavcích vycházíme ze zdroje (4).

Diofantická rovnice je rovnice, kde proměnné mohou nabývat pouze celočíselných hodnot. Dlouhou dobu se zkoumaly jen jako nějaké hádanky, ale obecná teorie diofantických rovnic byla vybudována až ve 20. století.

Hledáním celočíselných řešení rovnic se poprvé zabýval řecký matematik Diofantos z Alexandrie, který žil ve 3. století před naším letopočtem. Matematice věnoval své dílo Aritmetika, kterým se inspirovali matematici jako byl Pierre de Fermat se svou Velkou Fermatovou větou. Proto se Diofantovi přezdívalo "otec algebry". Podle něj jsou pojmenovány diofantické rovnice, které také studoval.

Problém řešení diofantických rovnic je značně komplikovaný. Je dokázané, že neexistuje obecný algoritmus, který by šel použít na každou diofantickou rovnici podle zdroje (1).

Tato bakalářská práce se zabývá zkoumáním metody na řešení kvadratických diofantických rovnic. Taková rovnice lze pomocí vhodných úprav převést na rovnici kvadriky, kde na ní hledáme všechny racionální body. Tím se celá úloha změní a budeme na příklad nahlížet geometricky. Úlohu transformujeme na hledání průsečíků přímek a kvadriky. Poté, co průsečíky najdeme, je nutné je převézt zpátky a vrátit se z racionálních čísel do čísel celých. To vede na hledání největších společných dělitelů hodnot jistých polynomů, což se pro více proměnných může zkomplikovat. Tuto metodu popíšeme obecněji, kde místo celých čísel budeme uvažovat nějaký okruh (například gaussovská celá čísla) a místo racionálních čísel budeme používat podílové těleso.

V první kapitole si ukážeme na motivačním příkladu hledání pythagorejských trojic nad celými čísly. Tato rovnice $a^2+b^2 = c^2$ se převede na rovnici kružnice $x^2+y^2 = 1$, se kterou budeme geometricky pracovat a na které spočítáme průsečíky s konkrétními přímkami. Pak celou úlohu převedeme zpět a získáme řešení zadané diofantické rovnice.

Ve druhé kapitole zobecníme věty a definice z racionálních čísel na libovolná tělesa. Cílem je zde shrnout a dokázat věty, které ukazují korektnost naší metody. V sekci 2.1 si zavedeme základní definice a snazší tvrzení 11 o poloze bodu a přímky, které dokážeme a tvrzení 12. V sekci 2.2 vyslovíme a dokážeme věty pro definitní kvadriky, kde je věta 17 nejzásadnější. K jejímu důkazu bude zapotřebí věta 15, která se také nachází v této kapitole. V poslední sekci této kapitoly 2.3 si ukážeme jak řešit příklady, které nevedou na definitní kvadriky. K tomu si vyslovíme a dokážeme větu 18. Rozebereme si všechny možné případy, které mohou nastat pro polohu přímky a kvadriky v pozorování 19, což budeme ilustrovat na dvou příkladech v podsekci.

Ve třetí kapitole využijeme dokázané věty při hledání řešení konkrétních vybraných příkladů. V sekci 3.1 budeme hledat řešení rovnice $a^2 + b^2 = c^2$, tentokrát nad gaussovskými celými čísly. Zjistíme, že z toho důvodu se nejedná o definitní kvadriku a navíc si na začátku sekce zformulujeme lemma 20 a lemma 21 i s důkazem, které nám pomůže při hledání největšího společného dělitele. V sekci 3.2 vyřešíme příklad, který povede na kružnici. Na řešení tohoto příkladu nebudeme demonstrovat nic nového. Jedná se o něco těžší variantu motivačního

příkladu z první kapitoly. Řešení tohoto příkladu využijeme v řešení posledního příkladu. Nakonec v sekci 3.3 vyřešíme rovnici vedoucí na hyperboloid, tedy rovnici $a^2 + b^2 - 2c^2 = d^2$, kde se řešení trochu zkomplikuje při hledání největších společných dělitelů, ale i přesto ho zvládneme vyřešit.

Celá práce vychází z (2), což je článek psaný především pro střední školy. Inspirujeme se jím jen v první kapitole, konkrétně jsme převzali znění vět spolu s definicemi, ale i to jsme do jisté míry upravili a pozměnili. Samotné řešení příkladu se už liší, jelikož jsme si při řešení příkladu zvolili jiný bod ležící na kružnici. Zbytek bakalářské práce staví na rozvinutí a zobecnění metody představené v článku. Příslušné věty a definice jsme zformulovali samostatně, stejně tak v případě jejich důkazu. Také řešení příkladu 2. a 3. kapitole je původní nepřevzaté z žádného zdroje.

1. Motivační příklad

Cílem práce je shrnutí a zobecnění metody na řešení kvadratických diofantických rovnic. V této kapitole si tuto metodu ilustrujme na konkrétním příkladu a budeme se opírat o věty, které zde zmíníme, ale neuvedeme jejich důkaz. Důkazy vět si ukážeme ve druhé kapitole v obecnější formě. Celá tato kapitola vychází z článku (2), kde se konkrétně inspirujeme zněním vět a definic. V metodě řešení jsme si zvolili jiný společný bod kuželosečky a přímky, a proto se řešení lehce liší.

Příklad (Pythagorejské trojice). Najděte všechna řešení diofantické rovnice

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

taková, že jsou celá čísla a, b, c nesoudělná.

Nejprve si rozmysleme, že z toho, že jsou proměnné a, b, c po třech nesoudělné, plyne jejich nesoudělnost po dvou. Kdyby existovalo prvočíslo $p \mid \mathbf{NSD}(a, b)$, pak by $p \mid \mathbf{NSD}(a^2, b^2)$ a také $p \mid (a^2+b^2)$. Z rovnosti $a^2+b^2 = c^2$ bude p dělit i pravou stranu. To je ale spor s nesoudělností všech třech proměnných a, b, c. Stejně by se ukázalo, že pokud by existovalo nějaké prvočíslo p, které by dělilo a, c nebo b, c, pak by nutně p dělilo všechny tři proměnné a, b, c. To je spor s nesoudělností proměnných a, b, c, máme proto nesoudělnost po dvou.

Zaveďme si ještě potřebné pojmy, aby se nám snáz pracovalo. Analogické pojmy, ale pro obecnou dimenzi a těleso, se objeví v druhé kapitole.

Definice 1. ***Racionální bod*** *je bod* $(x,y) \in \mathbb{R}^2$*, kde* $x, y \in \mathbb{Q}$*.*

Definice 2. ***Racionální přímka*** *je přímka s rovnicí* $ax + by + c = 0$*, kde* $a, b, c \in \mathbb{Q}$ *a navíc* a, b *nesmí být zároveň rovny* 0*.*

Definice 3. ***Racionální kuželosečka*** *je kuželosečka určená rovnicí* $ax^2+bxy+cy^2+dx+ey = f$*, kde* $a, b, c, d, e, f \in \mathbb{Q}$ *a kde je aslespoň jedna proměnná* a, b, c *nenulová.*

Potřebujeme pracovat s kuželosečkami, které mají s každou přímkou nejvýše dva průsečíky, jinak bude celé řešení o něco komplikovanější, jak si ukážeme ve 3. kapitole. To ale není úplně snadné zařídit, např. podle naší definice je kuželosečkou i sjednocení dvou přímek dané rovnicí $xy = 0$. Tohle obejdeme v další kapitole tím, že budeme uvažovat definitní kvadriky. K tomu si ještě zavedeme následující definici:

Definice 4. ***Definitní kuželosečka*** *je kuželosečka s rovnicí* $ax^2 + bxy + cy^2 + dx + ey = f$*, pro kterou platí, že* $ax^2 + +bxy + cy^2 = 0$ *jen když* $x = 0, y = 0$*.*

Dále si zformulujeme věty, které se budou hodit při řešení našeho příkladu.

Věta 5 (O průsečících)**.** *Nechť* A *je racionální bod ležící na racionální kuželosečce* k *a nechť* p *je racionální přímka procházející bodem* A*, která protíná kuželosečku v právě dvou bodech* A, B*. Potom je bod* B *také racionální.*

Důkaz této věty je snadný, stačí rozepsat definice a dopočítat z Viétových vzorců, stejně jako to uděláme v důkazu jiné verze této věty číslo 15. Tato věta se využije ve větě další. Tam dáme do souvislosti pojmy jako všechny racionální body na kuželosečce a všechny průsečíky přímky a kuželosečky. Ve znění věty se objevuje pojem jako tečna, který je zde využit v tradičním smyslu, nebo ji můžeme definovat pro definitní racionální kuželosečky jako racionální přímky, které mají s kuželosečkou pouze jeden společný bod. Více si k tomu povíme ve druhé kapitole.

Věta 6 (O racionálních bodech na kuželosečce)**.** *Mějme racionální definitní kuželosečku k a racionální bod A, který leží na k. Označme M množinu všech racionálních bodů ležících na k a N množinu všech průsečíků (i bod dotyku tečny se zde počítá jako průsečík) kuželosečky k s nějakou racionální přímkou p procházející bodem A. Pak $N = M$.*

Věta o racionálních bodech na kružnici je jiná verze věty 17 z 2. kapitoly.

Vraťme se zpátky k našemu příkladu. Chtěli bychom celou rovnici upravit a hledání řešení v $\mathbb{Z}$ převést na hledání řešení v $\mathbb{Q}$.

Rozdělme si to na dva případy:

- Pro $c^2 = 0$ řešíme, kdy $a^2 + b^2 = 0$. Tím získáme jediné řešení $(0, 0, 0)$.
- Kdyby $c^2 \neq 0$, tak můžeme celou rovnici vydělit c^2 a získáme

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1.$$

  Zde provedeme substituci, $\frac{a}{c}$ si označíme jako x a $\frac{b}{c}$ jako y.

Nyní máme rovnici

$$x^2 + y^2 = 1,$$

kde chceme najít řešení pro všechna racionální čísla x, y. Tím jsme přeformulovali původní úlohu a místo všech celočíselných řešení potřebujeme najít všechna racionální řešení.

Vidíme, že rovnice $x^2 + y^2 = 0$ nemá jiné řešení než $x = 0, y = 0$ nad $\mathbb{Q}$. Proto je naše kuželosečka definitní, a budeme moc využít naši uvedenou větu.

Poznamenejme ještě, že při změně tělesa, nad kterým počítáme, se může změnit i definitnost kuželosečky. Nad $\mathbb{Q}[i]$ už totiž není definitní, jak si ukážeme ve třetí kapitole.

Pojďme se vrátit zpět a najít všechny racionální body na této kružnici. K tomu už můžeme použít dříve větu 6 O racionálních bodech.

Nejprve najdeme nějaký racionální bod, který na naší kružnici leží. Obecně by se mohlo stát, že na kuželosečce neleží žádný racionální bod. To nastane, pokud zadaná diofantická rovnice nemá žádné řešení, což se zjistí jinými metodami z teorie čísel.

V našem případě je snadné najít nějaké racionální řešení, použijme třeba bod $(0, 1)$ a napišme rovnici přímky, která prochází bodem $(0, 1)$. Snadno vidíme, že všechny takové přímky mají rovnice $x = ky - k$, kde $k \in \mathbb{Q}$. a $y = 1$. Kuželosečka má s přímkou $y = 1$ jediný společný bod $(0, 1)$, jedná se o tečnu.

Pro připomenutí zmíníme Viétův vzorec, který využijeme při zjišťování průsečíků kružnice a přímky.

Věta 7 (Viétův vzorec)**.** *Mějme kvadratickou rovnici* $ax^2 + by + c = 0$*, s kořeny* x_1, x_2*. Potom platí, že*

$$x_1 + x_2 = -\frac{b}{a}.$$

Spočítáme průnik kružnice $x^2 + y^2 = 1$ s rovnicí přímky $x = ky - k$:

$$(ky - k)^2 + y^2 - 1 = 0$$

To ještě roznásobíme a přeuspořádáme na

$$y^2(1 + k^2) - 2k^2y + k^2 - 1 = 0.$$

Považujeme-li k za pevné jde o kvadratickou rovnici v proměnné y. Navíc známe jeden z kořenů a to $y = 1$, který odpovídá zvolenému bodu $(0, 1)$. Můžeme tedy použít Vietův vzorec 7, abychom snadněji našli druhý kořen:

$$y + 1 = -\frac{-2k^2}{1 + k^2}.$$

To ještě trochu upravíme na

$$y = \frac{k^2 - 1}{1 + k^2}.$$

Dosazením a následnou úpravou dostaneme první souřadnici

$$x = \frac{-2k}{1 + k^2}.$$

Díky větě 5 O průsečících víme, že jsme získali všechny racionální body na kružnici, tedy

$$\left\{ \left(\frac{-2k}{1 + k^2}, \frac{k^2 - 1}{1 + k^2} \right); k \in \mathbb{Q} \right\} \cup \{(0,1)\}.$$

Nyní potřebujeme z řešení v $\mathbb{Q}$ opět udělat řešení v $\mathbb{Z}$. Číslo k si napíšeme jako zlomek v základním tvaru, tedy $k = \frac{u}{v}$, kde $u, v \in \mathbb{Z}$, $v > 0$ a také $\mathbf{NSD}(u,v) = 1$. Tím získáme řešení tvaru

$$\left\{ \left(\frac{-2uv}{u^2 + v^2}, \frac{u^2 - v^2}{u^2 + v^2} \right); v, u \in \mathbb{Z}, v \geq 0, \mathbf{NSD}(u,v) = 1 \right\}.$$

V této množině jsme povolili $v = 0$, protože tím získáme bod $(0, 1)$.

To plyne z dosazení za $k = \frac{u}{v}$ do rovnice přímky $x = ky - k$. Úpravou získáme rovnici $vx = u(y - 1)$, po dosazení $v = 0$ získáme řešení dostaneme rovnici $uy = u1$, z nesoudělnosti u, v může být $u = \pm 1$, což vede na jediný bod (0,1).

Řešení už skoro máme. Ještě je třeba si dát pozor na soudělnost čitatele se jmenovatelem. Mohlo by nastat, že jsou dané zlomky soudělné, a potom bychom mohli přijít o nějaká řešení. Musíme tedy zjistit, jak vypadá $\mathbf{NSD}(u^2 - v^2, u^2 + v^2)$ a $\mathbf{NSD}(-2uv, u^2 + v^2)$.

Začněme s $\mathbf{NSD}(u^2 - v^2, u^2 + v^2) = \mathbf{NSD}(2u^2, u^2 + v^2)$, kde jsme použili vlastnost dělitelnosti $\mathbf{NSD}(a, b) = \mathbf{NSD}(a, a + b)$. Nechť p je prvočíslo, které dělí $\mathbf{NSD}(2u^2, u^2 + v^2)$. Proto platí, že $p \mid 2u^2$. Využijeme toho, že v $\mathbb{Z}$ je ireducibilní prvek a prvočinitel totéž, což nám dává následující případy.

- Nechť $p \mid u^2$, pak p musí dělit i u. Také platí, že $p \mid \mathbf{NSD}(u^2, u^2+v^2) = \mathbf{NSD}(u^2, v^2)$. Je jasné, že p dělí v^2, a proto $p \mid v$. To je ovšem spor s nesoudělností u, v.

- Nechť $p \mid 2$, pak můžeme bez újmy na obecnosti předpokládat, že $p = 2$. Pro u, v obě liché bude $2 \mid u^2+v^2$. Pokud je totiž u liché, pak bude liché i u^2, kde součet dvou lichých čísel je číslo sudé. Pro u, v liché bude $\mathbf{NSD}(2u^2, u^2 + v^2) = 2^\kappa$ pro $\kappa \in \mathbb{N}$. Předpokládejme, že $\kappa > 1$. V tom případě musí $2 \mid u^2$ a rovnou $2 \mid u$. Víme, že $2 \mid \mathbf{NSD}(u^2, u^2 + v^2) = \mathbf{NSD}(u^2, v^2)$, takže $2 \mid v^2$. Potom musí $2 \mid v$, což je spor s nesoudělností u, v. Takže $\kappa = 1$.

- Závěrem jsme získali, že $\mathbf{NSD}(u^2 - v^2, u^2 + v^2) = 1$ pro u, v různé parity a $\mathbf{NSD}(u^2 - v^2, u^2 + v^2) = 2$ pro u, v obě lichá.

Podobně musíme vyřešit nesoudělnost $\mathbf{NSD}(-2uv, u^2 + v^2)$. Budeme postupovat stejně jako výše.

Nechť p je prvočíslo, které dělí $\mathbf{NSD}(-2uv, u^2 + v^2)$. Potom $p \mid 2uv$, což si rozdělíme na následující případy.

- Nechť p dělí u, pak rovnou platí, že $p \mid u^2$. Dále $p \mid \mathbf{NSD}(u^2, u^2 + v^2) = \mathbf{NSD}(u^2, v^2)$. Odtud máme, že $p \mid v^2$, a také $p \mid v$. To je ale spor s nesoudělností u, v.

- Případ, kdy $p \mid v$ dopadne identicky s případem $p \mid u$. Pokud budeme na výrazy $-2uv$ a $u^2 + v^2$ nahlížet jako na polynomy, pak vidíme, že jsou symetrické, můžeme tedy zaměnit v za u.

- Nechť $p \mid 2$, pak ze stejného důvodu jako v první nesoudělnosti máme $p \mid u^2 + v^2$, pokud jsou u, v obě lichá.

- Dospěli jsme k $\mathbf{NSD}(-2uv, u^2 + v^2) = 2^\lambda$ pro $\lambda \in \mathbb{N}$. Předpokládejme, že $\lambda > 1$, pak $2 \mid uv$. Můžeme bez újmy na obecnosti předpokládat, že 2 dělí u. Pak $2 \mid u^2$ a také $2 \mid \mathbf{NSD}(u^2, u^2 + v^2) = \mathbf{NSD}(u^2, v^2)$. To dopadne stejně jako v předchozích případech, jsme v situaci, kdy $p \mid v^2$, tedy $p \mid v$. Nalezli jsme spor s nesoudělností u, v, proto $\lambda = 1$.

- Pokud dáme všechny předchozí úvahy dohromady, máme $\mathbf{NSD}(-2uv, u^2 + v^2) = 1$ pro u, v různé parity a $\mathbf{NSD}(-2uv, u^2 + v^2) = 2$ pro u, v obě lichá.

Když už jsme vyřešili nesoudělnost čitatelů a jmenovatelů v množině

$$\left\{ \left(\frac{-2uv}{u^2+v^2}, \frac{u^2-v^2}{u^2+v^2} \right); v, u \in \mathbb{Z}, v \geq 0, \mathbf{NSD}(u,v) = 1 \right\},$$

můžeme sepsat řešení zadané rovnice. Pro u, v s různou paritou získáme $a = -2uv, b = u^2 - v^2, c = u^2 + v^2$. A pro u, v obě lichá budeme mít řešení $a = -uv, b = \frac{u^2-v^2}{2}, c = \frac{u^2+v^2}{2}$.

Ještě nesmíme zapomenou, že pokud je $\frac{-2uv}{u^2+v^2} = \frac{a}{c}$, tak budeme mít dvě řešení, a to $a = -2uv, c = u^2 + v^2$ a $a = 2uv, c = -u^2 - v^2$. Stejně tak pro b, c.

Nyní zformulujeme větu, která shrne všechna nalezená řešení.

Věta 8. *Rovnice $a^2 + b^2 = c^2$ pro (a, b, c) nesoudělná má právě tato řešení:*

- $\pm(-2uv, u^2 - v^2, u^2 + v^2)$, *kde* $u, v \in \mathbb{Z}$ *mají různou paritu a* $v \geq 0$, $\mathbf{NSD}(u,v) = 1$.
- $\pm(\frac{-2uv}{2}, \frac{u^2-v^2}{2}, \frac{u^2+v^2}{2})$, *kde* u, v *jsou obě lichá a* $u, v \in \mathbb{Z}, v > 0$ $\mathbf{NSD}(u,v) = 1$.
- $(0, 0, 0)$.

2. Základní pojmy a tvrzení

V této kapitole zobecníme věty a definice, které jsou potřebné k metodě řešení ilustrované v minulé kapitole. V celé sekci bude $\mathbf{T}$ značit těleso a n bude vždy přirozené číslo.

2.1 Základní pojmy

V této sekci definujeme základní pojmy, se kterými budeme pracovat. Naším cílem je zobecnit pojmy použité v první kapitole pro obecné těleso. Tam jsme používali pojmy jako racionální bod, racionální přímka a racionální kuželosečka. Z toho důvodu se nám přirozeně nabízí zobecnit pojmy na $\mathbf{T}$-racionální, kde zdůrazníme i těleso, nad kterým počítáme.

Jelikož ale uvažujeme v celé kapitole obecné těleso $\mathbf{T}$, bude snazší $\mathbf{T}$ vynechat. Zároveň pracujeme pouze s $\mathbf{T}$-racionálními body, přímkami a kvadrikami, proto budeme vynechávat i slovo racionální. Pokud budeme chtít zdůraznit, že je něco $\mathbf{T}$-racionální, tak to nevynecháme. Takže místo pojmů $\mathbf{T}$-racionální bod, $\mathbf{T}$-racionální přímka, $\mathbf{T}$-racionální kvadrika budeme používat pojmy bod, přímka, kvadrika.

Definice 9. ***Bod*** *je n-tice* $(x_1, x_2, \dots x_n)$*, pro kterou platí* $x_1, x_2, \dots, x_n \in \mathbf{T}$*.*

Definice 10. ***Přímka*** *je množina bodů*

$$\{(a_1 + tb_1, a_2 + tb_2, \dots, a_n + tb_n); t \in \mathbf{T}\},$$

kde $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbf{T}$ *a kde existuje* $i \in \{1, \dots, n\}$ *takové, že* $b_i \neq 0$*.*

Nyní si pro úplnost dokážeme větu o tom, že každými dvěma různými body prochází právě jedna přímka, kterou je možné najít v různých formulacích v algebře nebo geometrii. Tuto větu využijeme později v další sekci při hledání bijekce mezi všemi body na kvadrice a přímkami procházejícími jedním bodem.

Tvrzení 11. *Každé dva různé body lze spojit právě jednou přímkou.*

Důkaz. Mějme dva různé body, které si označíme jako $A = (a_1, \dots, a_n)$ a jako $B = (b_1, b_2, \dots, b_n)$. Přímku zde definujeme jako množinu bodů $p = \{(a_1 + t(b_1 - a_1), \dots, a_n + t(b_n - a_n)); t \in \mathbf{T}\}$. Tato přímka pro volbu $t = 0$ dává bod A a pro volbu $t = 1$ bod B. Navíc $b_i - a_i$ je rozdíl, který leží v tělese T. Jelikož jsou body A, B různé, bude existovat alespoň jedno i, pro které bude $b_i - a_i \neq 0$. Z toho důvodu je p opravdu přímka.

Zbývá ukázat, že neexistuje jiná přímka, která by procházela oběma body. Nechť máme přímku $q = \{(c_1 - td_1, \dots, c_n - td_n) : t \in \mathbf{T}\}$ a tato přímka prochází body A a B. Musí tedy platit $a_i = c_i + t_1 d_i$ a také $b_i = c_i + t_2 d_i$ pro pevné $t_1, t_2 \in \mathbf{T}$. Abychom si to zjednodušili, předpokládejme, že $t_1 = 0$. To můžeme udělat, protože by šlo ke každému prvku z $\mathbf{T}$ přičíst nebo odečíst nějaké t, aby to platilo a aby přímka zůstala stejná. Také víme, že bod A je různý od bodu B, takže $t_1 \neq t_2$. Rovnice upravíme a vyjádříme si proměnné c_i, d_i vzhledem k proměnným a_i, b_i, protože víme, že body A, B leží na přímce q:

$$c_i = a_i - t_1 d_i$$

$$c_i = b_i - t_2 d_i$$

Obě rovnice dáme dohromady a dostaneme

$$a_i - t_1 d_i = b_i - t_2 d_i.$$

Vyjádříme si d_i pomocí proměnných a_i, b_i a čísel t_1, t_2 jako

$$d_i = \frac{b_i - a_i}{t_2 - t_1}.$$

Dále si pomocí d_i podobně vyjádříme c_i jako

$$c_i = b_i - \frac{t_2(b_i - a_i)}{t_2 - t_1}.$$

Tím jsme dostali i-tou složku bodu ležícího na přímce. Pro $t \in \mathbf{T}$ vypadá následovně

$$b_i - \frac{t_2}{t_2 - t_1}(b_i - a_i) + t\frac{b_i - a_i}{t_2 - t_1}.$$

Celé to ještě upravíme, aby se tvar podobal souřadnici přímky z definice

$$\frac{t_2}{t_2 - t_1}\left(a_i + \frac{t}{t_2}(b_i - a_i)\right).$$

Tam dosadíme $t_1 = 0$ a získáme

$$\left(a_i + \frac{t}{t_2}(b_i - a_i)\right).$$

Ještě si označme $\frac{t}{t_2} = e$ a dostaneme následující přímku, která je stejná jako přímka q.

$$\{(a_1 + e(b_1 - a_1), \ldots, a_n + e(b_n - a_n)) : t \in \mathbf{T}\}$$

Také platí $e \in \mathbf{T}$. Konečně si všimneme, že pro množinu $\{t; t \in \mathbf{T}\}$ bude stejná jako $\{\frac{t}{t_2}; t \in \mathbf{T}\}$ Proto je tahle přímka stejná jako $\{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) : t \in \mathbf{T}\}$. Tímto jsme ukázali jednoznačnost.

□

Následující větu je možné opět dohledat v geometrii nebo algebře, kdy by byl důkaz podobný důkazu předchozí věty, a tak ji tentokrát nebudeme dokazovat. Tuto větu opět využijeme ve větě 18, kde bereme všechny různé přímky, které procházejí jedním bodem na kvadrice a hledáme další průsečíky.

Tvrzení 12. *Dvě různé přímky mají nejvýše jeden společný bod*

Kuželosečka je vlastně množina řešení kvadratická rovnice o dvou proměnných. Pokud se budeme pohybovat v obecné dimenzi, tak potřebujeme definovat kvadratické rovnice o n proměnných. Takovým útvarům říkáme kvadriky.

Definice 13. *Nechť $a_{ij}, b_i, c \in \mathbf{T}$, a zároveň platí, že $a_{ij} \neq 0$ pro nějaké $i, j \in \{1, \ldots, n\}$.* ***Obecná kvadrika*** *je množina bodů*

$$\left\{(x_1, \ldots, x_n); \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j + \sum_{1 \leq i \leq n} b_i x_i + c = 0\right\}.$$

Často budeme zkracovat a místo obecná kvadrika budeme psát pouze kvadrika.

2.2 Věty pro definitní kvadriky

Nyní bychom chtěli formulovat věty podobné větám z první kapitoly. Tam jsme pracovali pouze s definitními kuželosečkami, a proto budeme postupovat podobně. Definujme si, co to je definitní kvadrika.

Definice 14. *Kvadrika*

$$\left\{(x_1,\ldots,x_n);\sum_{1\le i\le j\le n} a_{ij}x_ix_j+\sum_{1\le i\le n} b_ix_i+c=0\right\}$$

*je **definitní**, pokud je kvadratický člen* $\sum_{1\le i\le j\le n} a_{ij}x_ix_j = 0$ *jen pokud* $x_1 = 0, x_2 = 0, \ldots, x_n = 0$.

Věta 15. *Nechť k je definitní kvadrika a p je přímka, která protíná kvadriku k alespoň ve dvou bodech, tj. $|k \cap p| \ge 2$. Potom přímka p protíná kvadriku k právě ve dvou bodech, tj. $|k \cap p| = 2$.*

Tahle věta je zobecněná verze věty 5. Ukažme si její důkaz.

Důkaz. Bod $R = (r_1, \ldots, r_n)$ je společný bod přímky p a kvadriky k. Pojďme spočítat ostatní průsečíky. Kvadrika k je definovaná jako

$$\left\{(x_1,\ldots,x_n);\sum_{1\le i\le j\le n} a_{ij}x_ix_j+\sum_{1\le i\le n} b_ix_i+c=0\right\}$$

a přímka p jako $\{(r_1+ts_1,\ldots,r_n+ts_n); t \in \mathbf{T}\}$. Dosaďme do rovnice, která určuje kvadriku, za $x_i = r_i + ts_i$:

$$\sum_{1\le i\le j\le n} a_{ij}(r_i+ts_i)(r_j+ts_j)+\sum_{1\le i\le n} b_i(r_i+ts_i)+c=0.$$

Roznásobme:

$$\sum_{1\le i\le j\le n} a_{ij}(r_ir_j+tr_is_j+tr_js_i+t^2s_is_j)+\sum_{1\le i\le n}(b_ir_i+ts_ib_i)+c=0.$$

Přeuspořádejme do tvaru kvadratické rovnice

$$(*)\quad t^2\left(\sum_{1\le i\le j\le n} a_{ij}s_is_j\right)+t\left(\sum_{1\le i\le j\le n}(r_is_j+r_js_i)a_{ij}+\sum_{1\le i\le n} s_ib_i\right)+\sum_{1\le i\le j\le n} a_{ij}r_ir_j+\sum_{1\le i\le n} b_ir_i+c=0.$$

Z definitnosti kvadriky máme $\sum_{1\le i\le j\le n} a_{ij}s_is_j \neq 0$, takže se jedná o kvadratickou rovnici s proměnnou t. Konstantní člen této rovnice

$$\sum_{1\le i\le j\le n} a_{ij}r_ir_j+\sum_{1\le i\le n} b_ir_i+c$$

je dosazení bodu R do rovnice kvadriky k. Jelikož bod R na kvadrice k leží, tento člen je nutně nulový. Víme, že má přímka s kvadrikou alespoň dva průsečíky, zároveň víme, že kvadratická rovnice má nejvýše 2 řešení. Z toho dostáváme, že

musí přímka p protínat kvadriku k v právě dvou bodech a tím je důkaz hotov. □

Pojďme v důkazu předešlé věty ještě chvíli pokračovat, chceme zjistit, jak budou průsečíky vypadat. Podívejme se opět na rovnici (*).

Jeden kořen známe, to je bod R, který získáme pro $t = 0$. Není už těžké určit druhý kořen:

$$t = -\frac{\sum_{1\leq i\leq j\leq n}(r_i s_j + r_j s_i)a_{ij} + \sum_{1\leq i\leq n} s_i b_i}{\sum_{1\leq i\leq j\leq n} a_{ij} s_i s_j}.$$

Po dosazení do rovnice přímky, získáme následující tvar druhého průsečíku

$$\left(r_1 + \left(-\frac{\sum_{1\leq i\leq j\leq n}(r_i s_j + r_j s_i)a_{ij} + \sum_{1\leq i\leq n} s_i b_i}{\sum_{1\leq i\leq j\leq n} a_{ij} s_i s_j}\right) s_1, \ldots, \right.$$
$$\left. r_n + \left(-\frac{\sum_{1\leq i\leq j\leq n}(r_i s_j + r_j s_i)a_{ij} + \sum_{1\leq i\leq n} s_i b_i}{\sum_{1\leq i\leq j\leq n} a_{ij} s_i s_j}\right) s_n\right).$$

Všechny hodnoty $s_1, s_2, \ldots, s_n$ známe ze zadané přímky, stejně tak proměnné $r_1, \ldots, r_n$ jsou souřadnice bodu R. Podobně jako b_i, a_{ij} známe z rovnice kvadriky.

Pro zjednodušení znění následující věty si definujme, co je to tečna k definitní kvadrice. Tuto definici by bylo těžší zobecnit pro obecné kvadriky a tady to ani nebude zapotřebí.

Definice 16. *Řekneme, že přímka p je **tečna k definitní kvadrice** k, pokud je velikost jejich průniku jednobodová množina, tedy pokud $|p \cap k| = 1$.*

Jelikož je tahle definice zjednodušená a liší se od definice z geometrie, pro jiné než definitní kvadriky nemusí fungovat. Stačí si vzít například hyperbolu v $\mathbb{R}^2$. Pokud zvolíme na hyperbole libovolný bod a tím bodem povedeme přímku rovnoběžnou s asymptotami, budeme mít pouze jeden průsečík, ale daná přímka nebude tečna.

Následující věta je důležitá a dává do vztahu průsečíky kvadriky a přímek s body na kvadrice. Jedná se o zobecněnou verzi věty 6 z 1. kapitoly, jejíž důkaz si zde ukážeme.

Věta 17. *Nechť k je definitní kvadrika, R je bod, který leží na kvadrice. Existuje bijekce mezi množinou bodů na kvadrice k bez bodu R a mezi všemi přímkami procházejícími bodem R, které nejsou tečny.*

Důkaz. Označme si M jako množinu všech bodů ležících na definitní kvadrice k bez bodu R a jako množinu N všechny přímky procházející bodem R, které nejsou tečny. Chceme definovat bijekci ϕ :

$$\phi : M \longrightarrow N$$

To uděláme tak, že každý bod $P \in M$ zobrazíme na přímku procházející body P a R.

Každá přímka, která prochází bodem R a není tečna musí mít nutně s definitní kvadrikou k alespoň dva průsečíky. Díky předchozí větě 15 víme, že průsečíky jsou pak právě dva. To nám dává, že je **zobrazení ϕ na**.

Zobrazení ϕ je prosté díky tomu, že každými dvěma body prochází právě jedna přímka, což víme díky tvrzení 11.

□

2.3 Věty pro obecné kvadriky

Pokud bychom vynechali předpoklad definitnosti u kvadrik, tak by věta 17 dokázaná na konci předešlé kapitoly neplatila. Mohl by totiž nastat případ, kde bychom měli více než dva společné body přímky a kvadriky. To nastane v situaci, kdy přímka leží na kvadrice. Nebo by naopak přímka s kvadrikou měla pouze jeden průsečík a nebyla by tečna. Proto potřebujeme větu přeformulovat a pozměnit, abychom mohli řešit diofantické rovnice, které vedou na jiné, než definitní kvadriky. To celé řešení trošku ztíží.

Zformulujme si podobnou větu pro kvadriky, které nejsou definitní.

Věta 18. *Nechť k je obecná kvadrika a R je bod na kvadrice k. Pak platí, že množina všech bodů kvadriky lze napsat jako sjednocení průniků této množiny se všemi přímkami procházejícím bodem R. Neboli*

$$k = \bigcup_{p \text{ přímka, } R \in p} k \cap p.$$

Důkaz. Jedna inkluze je zřejmá

$$k \supseteq \bigcup_{p \text{ přímka, } R \in p} k \cap p.$$

Druhá inkluze $\subseteq$ se ukáže tak, že si vezmeme nějaký bod $S \in M$. Společně s bodem R, těmito body prochází právě jedna přímka p podle věty 11, čímž máme dokázanou druhou inkluzi.

□

Takové sjednocení je skoro disjunktní. Tím myslíme, že by bylo disjunktní, pokud bychom vynechali bod R, který se jako jediný opakuje vícekrát.

Na začátku minulé kapitoly jsme zmínili důsledek 12 o tom, že různé přímky mají nejvýš jeden společný bod. Pokud budeme brát všechny různé přímky procházející jedním společným bodem, víme, že se už v žádném dalším bodě vzájemně neprotnou. Proto můžeme zkoumat, v jaké vzájemné pozici může být přímka a kvadrika, čímž se zabývá následující věta.

Věta 19. *Nechť k je obecná kvadrika, p je přímka. Pak mohou nastat pouze následující případy:*

- $k \cap p = \emptyset$
- $k \cap p = \{A\}$*, kde A je bod*
- $k \cap p = \{A,B\}$*, kde A, B jsou body*
- $k \cap p = p$

Důkaz. Rozebereme si jednotlivé případy.

Může se stát, že přímka p neprotíná kvadriku k, v takovém případě máme $k \cap p = \{\emptyset\}$.

Pokud má přímka p a kvadrika k nějaký společný bod, označme ho jako $R = (r_1, \ldots, r_n)$. Kvadrika k je definovaná jako

$$\left\{(x_1, \ldots, x_n); \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j + \sum_{1 \leq i \leq n} b_i x_i + c = 0\right\}$$

pro alespoň jedno $a_{ij} \neq 0$ a přímka p jako $\{(r_1 + ts_1, \ldots, r_n + ts_n); t \in \mathbf{T}\}$. Důkaz je podobný důkazu věty 15, stejnými postupy dojdeme k rovnici (*). Tuto rovnici rozebereme.

$$(*) \quad t^2 \left(\sum_{1 \leq i \leq j \leq n} a_{ij} s_i s_j\right) + t \left(\sum_{1 \leq i \leq j \leq n} (r_i s_j + r_j s_i) a_{ij} + \sum_{1 \leq i \leq n} s_i b_i\right) + \sum_{1 \leq i \leq j \leq n} a_{ij} r_i r_j + \sum_{1 \leq i \leq n} b_i r_i + c = 0$$

Jelikož bod R leží na kvadrice k, konstantní člen je nulový, tedy

$$\sum_{1 \leq i \leq j \leq n} a_{ij} r_i r_j + \sum_{1 \leq i \leq n} b_i r_i + c = 0.$$

Pro $t = 0$ získáme jeden kořen. Pojďme si rozebrat jednotlivé situace, které mohou nastat.

Pokud platí, že $\left(\sum_{1 \leq i \leq j \leq n} a_{ij} s_i s_j\right) \neq 0$, bude mít kvadratická rovnice jeden dvojnásobný kořen, nebo dva různé kořeny. Pokud se jedná a dvojnásobný kořen musí být $t = 0$. To nastane, pokud je koeficient u lineárního členu nulový, tedy pokud

$$\sum_{1 \leq i \leq j \leq n} (r_i s_j + r_j s_i) a_{ij} = 0.$$

Jindy bude mít rovnice dva různé kořeny.

Pokud platí, že $\left(\sum_{1 \leq i \leq j \leq n} a_{ij} s_i s_j\right) = 0$, pak tento případ rozdělíme na dva podpřípady.

Pokud by byl koeficient u lineárního členu nenulový, tedy pokud by se stalo, že $\sum_{1 \leq i \leq j \leq n} (r_i s_j + r_j s_i) a_{ij} + \sum_{1 \leq i \leq n} s_i b_i \neq 0$, pak bude mít rovnice

$$t \left(\sum_{1 \leq i \leq j \leq n} (r_i s_j + r_j s_i) a_{ij} + \sum_{1 \leq i \leq n} s_i b_i\right) = 0$$

právě jeden kořen a to bod R. To plyne z toho, že v této situaci hledáme kořen lineární rovnice.

Pokud by byl koeficient u lineárního členu nulový, tedy pokud $\sum_{1 \leq i \leq j \leq n} (r_i s_j + r_j s_i) a_{ij} + \sum_{1 \leq i \leq n} s_i b_i = 0$, pak bude rovnost platit pro libovolné t. Potom leží na kuželosečce celá přímka p.

Tímto jsme rozebrali všechny možné případy, čímž jsme větu dokázali.

□

Zajímavé je si všimnout, že kvadriky, které nejsou definitní mohou mít jeden průsečík s přímkou, která není nutně tečna. Využití uvedených vět si ukážeme na následujících příkladech, společně s různými polohami přímek a kvadrik.

2.4 Ukázka vět na příkladech

2.4.1 Hyperbola

Příklad. Nechť $Q = \{(x,y); xy = 1\}$ je kvadrika nad $\mathbb{Q}$. Určete její průsečíky se všemi přímkami.

Ze zadání je jasné, že se nejedná o definitní kvadriku. Všimněme si, že hledáme průsečíky přímek s hyperbolou. K nějaké lepší představě poslouží obrázek 2.1.

Zkusme zde použít větu 18. Vidíme, že zrovna s přímkami $x = 0$ nebo $y = 0$ nemá naše kvadrika Q žádný průsečík. Zvolme bod na této hyperbole, například bod $(1, 1)$. Postupně budeme do nové množiny N přidávat průsečíky kvadriky a přímek, dokud nezískáme všechny. Přidejme tam tedy bod $A = (1, 1)$.

Zkusme nyní nalézt průsečíky kvadriky se všemi přímkami procházející zvoleným bodem, tedy s přímkou

$$\{(1 + \alpha t, 1 + \beta t); t \in \mathbb{Q}\}.$$

Kdyby bylo $a = 0$, získaly bychom přímku $x = 1$, která je rovnoběžná s osou hyperboly, a proto má s ní jen jeden průsečík, čili bod $(1, 1)$.

Stejně kdyby bylo $\beta = 0$, to bychom získaly přímku $y = 1$, která opět protíná hyperbolu v jediném bodě a není tečna. Je znázorněna na obrázku fialově. Případ, kdy $\alpha = 0$ máme ošetřený a tak můžeme použít drobný trik a zbavit se této proměnné navíc. Stačí, když si vezmeme $\alpha = 1$. To plyne z toho, že množina $\{t; t \in \mathbb{Q}\}$ je stejná jako množina $\{\frac{t}{\alpha}; t \in \mathbb{Q}\}$, čehož docílíme například nahrazením konstanty $t \in \mathbb{Q}$ konstantou $\frac{t}{\alpha}$. To dosaďme do rovnice $xy = 1$ a získáme

$$(1 + t)(1 + t\beta) = 1.$$

Rovnici přeuspořádáme do tvaru kvadratické rovnice

$$\beta t^2 + t(\beta + 1) = 0.$$

A zjistíme hodnotu t:

$$t = \frac{-\beta - 1}{\beta} \text{ nebo } t = 0.$$

Pro $t = 0$ Získáme pouze bod B, který jsme do naší množiny N už přidali. Pro $\frac{-\beta-1}{\beta} = 0$ bychom nezískali nové průsečíky, protože by rovnice měla dvojnásobný kořen. Jednalo by se o rovnici tečny. Což nastane, pokud $-\beta - 1 = 0$, nebo-li když $\beta = -1$. To dosadíme zpátky do rovnice přímky a získáme druhý průsečík. tedy

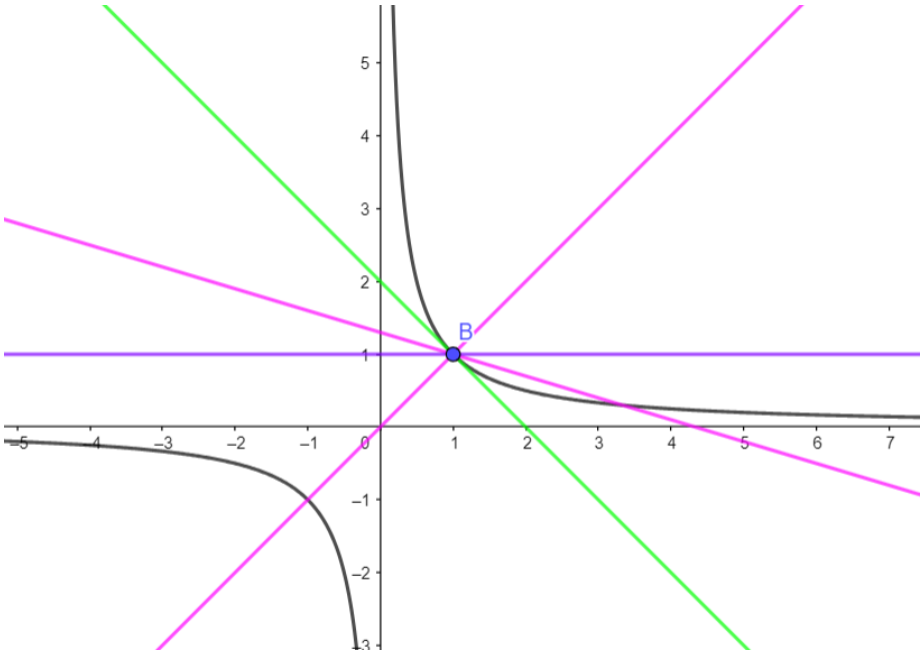
$$\left(1 + \frac{-\beta - 1}{\beta}, 1 + \beta t\right).$$

Takže v množině N máme body $N = \{(1 + \frac{-\beta-1}{\beta}, 1 + \beta t), \beta \in \mathbb{Q}, (1,1)\}$

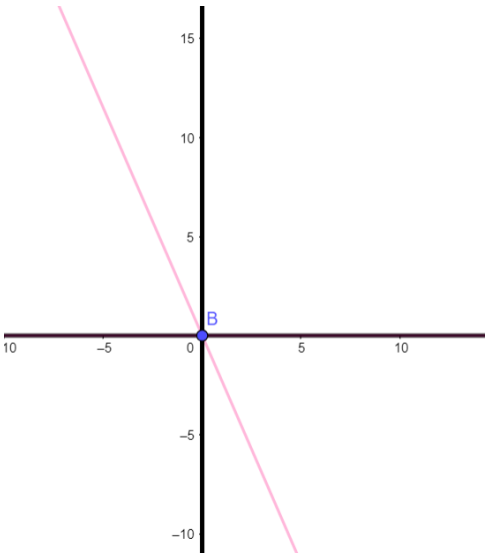
Z věty 18 víme, že $Q = N$. Všimněme si, že zde nastaly skoro všechny případy uvedené ve větě 19, kromě toho posledního.

Pro ilustraci si přiložíme obrázek 2.1. Ten znázorňuje všechny možné případy poloh přímky a hyperboly. Černě je zakreslený graf $y = \frac{1}{x}$, růžově jsou znázorněny přímky, které mají s hyperbolou dva společné body, zeleně je označena tečna a fialově přímka, která hyperbolu protíná v jediném bodě, ale není tečna.

Uvedeme si ještě jeden příklad, kde se bude nacházet i poslední případ z věty 19, tedy, že na hyperbole leží celá přímka.



Obrázek 2.1: Hledání průsečíků přímky a hyperboly



Obrázek 2.2: Hledání průsečíků přímky a kvadriky $xy = 0$

2.4.2 Kvadrika jako sjednocení dvou přímek

Příklad. Nechť $Q = \{(x,y); xy = 0\}$ je kvadrika nad racionálními čísly. Určete všechny její průsečíky s přímkou p.

Zvolme bod $B = (0, 0)$. Přímky tvaru $y = 0$, nebo $x = 0$ leží na této kvadrice, což je poslední případ z 19. Budeme opět do množiny N přidávat průsečíky přímek a kvadriky, takže tam přidáme obě přímky $y = 0$ a $x = 0$. Obecná přímka procházející bodem $(0, 0)$ vypadá následovně $(\alpha t, \beta t)$. Pro $\alpha = 0$ máme předchozí případ, tedy $y = 0$.

Proto můžeme bez újmy na obecnosti brát $\alpha = 1$ a dosadit do kvadriky

$$t(\beta t) = 0$$

$$\beta t^2 = 0.$$

A vyjádřením t opět máme $t = 0$. Tato rovnice má tedy jediný dvojnásobný kořen, a proto už žádné další body nezískáme. Máme $N = \{(0,t), (t,0); t \in \mathbb{Q}\}$

Příklad je znázorněn na obrázku, kde máme modře označený bod B, černě kvadriku Q a růžově nějakou přímku p, která jím prochází.

3. Příklady

Na následujících příkladech si ukážeme použití předcházejících vět z kapitoly 2.2 a 2.3. Konkrétně si ukážeme příklad nad gaussovskými celými čísly a příklad se čtyřmi proměnnými.

3.1 Rovnice nad gaussovskými celými čísly

Na začátek si připomeneme základní pojmy, jako ireducibilní prvek, prvočinitel, norma prvku v $\mathbb{Z}[i]$ a co je to kongruence v $\mathbb{Z}[i]$. Tyto definice jsme převzali ze zdroje (3). Na straně 22-23 jsou vlastnosti kongruencí nad $Z[i]$, které budeme používat.

Prvočinitel v okruhu $\mathbf{R}$ je prvek $p \in \mathbf{R}$, který není 0 a není asociovaný s 1, navíc musí platit, že pokud $p \mid ab$, pak $p \mid a$ nebo $p \mid b$ pro $a, b \in \mathbf{R}$.

Ireducibilní prvek je prvek $p \in \mathbf{R}$, kde pro všechny ostatní prvky $q \in \mathbf{R}$ platí, pokud $q \mid p$, pak $q \parallel 1$.

Normu prvku $\alpha \in \mathbb{Z}[i]$ definujeme jako $N(\alpha) = \alpha\bar{\alpha}$, kde $\bar{\alpha} \in \mathbb{Z}[i]$ je komplexně sdružené číslo k α.

Nechť R je okruh a $\omega \in \mathbb{R}$. Vezměme si dva prvky α, β. Potom řekneme, že $\alpha \equiv \beta \pmod{\omega}$, pokud $\omega \mid \alpha - \beta$.

Budeme využívat toho, že $\mathbb{Z}[i]$ je gaussovský okruh, a proto pojmy jako prvočinitel a ireducibilní prvek zde splývají. Také budeme používat tvrzení, které říká, že pokud má číslo $\alpha \in \mathbb{Z}[i]$ prvočíselnou normu, pak je α prvočinitel v $\mathbb{Z}[i]$. Toho využijeme při určování největších společných dělitelů. Proto je například prvek $1 + i$ prvočinitel, zatímco 2 je možné rozložit na $2 = (1 + i)(1 - i)$.

Ukážeme si nějaká pomocná lemmata, která využijeme při hledání největších společných dělitelů v následujícím příkladu.

Lemma 20. *Nechť máme $\alpha \in \mathbb{Z}[i]$.*

a) Potom platí, že $\alpha \equiv 0 \pmod{1+i}$ nebo $\alpha \equiv 1 \pmod{1+i}$.

b) Také platí, že $\alpha \equiv 0, 1, i, 1+i \pmod{2}$ a zároveň $\alpha^2 \equiv 0, 1 \pmod{2}$.

Důkaz.

Začneme důkazem části a). Nejprve ukážeme, že $i \equiv 1 \pmod{1+i}$. To je možné nahlédnout z toho, že $(i+1) \mid (i-1)$, jelikož $i(i+1) = i - 1$. Tím pádem z definice kongruence dostaneme $i \equiv 1 \pmod{1+i}$.

Číslo $\alpha \in \mathbb{Z}[i]$ si zapíšeme ve tvaru $\alpha = a + bi$, kde jsou $a, b \in \mathbb{Z}$. Ověřme, že platí $a+bi \equiv a+b \pmod{1+i}$. Po rozepsání z definice dostaneme $1+i \mid a+bi-a-b$. To upravíme na $1 + i \mid b(i-1)$, což platí, jelikož $1 + i \mid 1 - i$.

Musí zároveň platit, že $2 \equiv 0 \pmod{1+i}$, neboť $1 + i \mid 2$, takže $a + bi \equiv 0, 1 \pmod{1+i}$ a důkaz je hotov pro část a).

Pro část b) začneme s důkazem toho, že $\alpha \equiv 0, 1, i, 1 + i \pmod{2}$. Nechť $\alpha = a + bi$, kde jsou $a, b \in \mathbb{Z}$.

Předpokládejme, že je $a \geq 2$, ověříme, že platí $a + bi \equiv a - 2 + bi \pmod{2}$. Rozepíšeme podle definice kongruence 3.1 na $2 \mid a + bi - a + bi = 2$, z čehož vidíme, že daná kongruence platí.

Předpokládejme, že $b \geq 2$, tak platí $a + bi \equiv a + (b-2)i \pmod{2}$, jelikož platí, že $2 \mid a + bi - a - bi + 2i = 2i$.

Došli jsme k tomu, že $a < 2, b < 2$, což nám dává možnosti $0, 1, i, 1+i$ pro hodnotu α.

K důkazu druhé části rozebereme jednotlivé případy. Pro čísla 0 a 1 to zřejmě platí, jelikož se po umocnění nezmění. Rozepíšeme si případ, kde $\alpha \equiv i \pmod 2$ a dostaneme $i^2 \equiv -1 \pmod 2$. Taky musí platit, že $-1 \equiv 1 \pmod 2$, jelikož $2 \mid -2$. Zbývá nám případ $\alpha \equiv 1 + i \pmod 2$, to je možné nahlédnout z $(1+i)^2 \equiv 2i \equiv 0 \pmod 2$, protože $2 \mid -2i$. Tím je hotov důkaz části b).

□

Lemma 21. *Buď $u, v \in \mathbb{Z}[i]$.*

a) Platí, že $(1+i) \mid (u^2+v^2)$ právě tehdy, když $u \equiv v \pmod{1+i}$.

b) Také platí, že $2 \parallel (1+i)^2 \mid u^2+v^2$ právě tehdy, když $u \equiv v \pmod{1+i}$.

Důkaz. Pojďme se podívat na důkaz části a). Začneme implikací, pokud $(1+i) \mid (u^2+v^2)$, potom $u^2+v^2 \equiv 0 \pmod{1+i}$. Z předchozího lemma 20 víme, že $u \equiv 0, 1 \pmod{1+i}$ stejně jako $v \equiv 0, 1 \pmod{1+i}$. Kdybychom vzali $u \not\equiv v \pmod{1+i}$, pak by $u^2+v^2 \equiv 1 \pmod{1+i}$, což je spor s tím, že $(1+i) \mid (u^2+v^2)$.

Naopak, pokud $u \equiv v \pmod{1+i}$, chceme ukázat, že $(1+i) \mid u^2+v^2$. Podle předchozího lemmatu 20 máme $u \equiv v \equiv 0{,}1 \pmod{1+i}$, rozlišíme tedy tyto dvě možnosti

1. Pokud $u \equiv v \equiv 0 \pmod{i+1}$, pak $u^2 \equiv v^2 \equiv 0 \pmod{1+i}$ a opravdu $u^2+v^2 \equiv 0 \pmod{1+i}$.

2. Pokud $u \equiv v \equiv 1 \pmod{1+i}$, pak $u^2 \equiv v^2 \equiv 1 \pmod{1+i}$ a opět $u^2+v^2 \equiv 2 \equiv 0 \pmod{1+i}$.

V důkazu části b) začneme s implikací zleva doprava. Máme, že $u^2+v^2 \equiv 0 \pmod 2$. Díky lemmatu 20 části b) víme, že $u^2 \equiv 0, 1 \pmod 2$. Aby kongruence $u^2+v^2 \equiv 0 \pmod 2$ platila, musí $u^2 \equiv v^2 \pmod 2$.

1. Pokud je $u^2 \equiv v^2 \equiv 0 \pmod 2$, pak $(1+i)^2 \mid u^2$, z čehož plyne, že $1+i \mid u$. Stejně tak s v a dostaneme $0 \equiv u \equiv v \pmod{i+1}$.

2. Pokud je $u^2 \equiv v^2 \equiv 1 \pmod 2$, potom $2 \mid u^2-1$. Také víme, že $u^2-1 \equiv u^2+1 \equiv (u+1)^2 \pmod 2$. Tedy $(1+i)^2 \mid (u+1)^2$ a z toho dostaneme $1+i \mid u+1$. Úplně stejně budeme postupovat pro p v až dojdeme k tomu, že $1 \equiv u \equiv v \pmod{i+1}$, což jsme chtěli dokázat.

Podíváme se na implikaci zprava doleva. To uděláme opět tak, že si rozebereme všechny možnosti.

1. Pokud je $u \equiv v \equiv 0 \pmod{i+1}$, pak $1+i \mid u$ a zároveň $1+i \mid v$. Jelikož je $1+i$ prvočinitel, bude také platit, že $(1+i)^2 \mid u^2$ a $(1+i)^2 \mid v^2$. Proto bude dělit i jejich součet a tedy $(1+i)^2 \mid u^2+v^2$.

2. Pokud $u \equiv v \equiv 1 \pmod{1+i}$, pak $u-1 \equiv 0 \pmod{1+i}$, a také $(u-1)^2 = u^2-2u+1 \equiv (1+i)^2$. Jelikož platí, že $2 \parallel (1+i)^2$, můžeme použít předchozí lemma 20 a dostaneme $u^2 \equiv 1 \pmod 2$. Stejně tak pro v dojdeme k $v^2 \equiv 1 \pmod 2$, což nám dává $u^2+v^2 \equiv 0 \pmod 2$, což znamená, že $2 \mid u^2+v^2$ podle definice 3.1.

Tím je důkaz hotov.

□

Nyní se už můžeme pustit do řešení diofantické rovnice nad $\mathbb{Z}[i]$.

Příklad. Najděte všechna řešení rovnice nad gaussovskými celými čísly

$$a^2 + b^2 = c^2$$

taková, že jsou celá čísla a, b, c po dvou nesoudělná.

Tento příklad je stejný jako příklad 1 z první kapitoly, akorát ho řešíme nad jiným okruhem, čímž se změní celá množina řešení.

Všimněme si, že se už nejedná o definitní kvadriku. Například pro $a = i$ a pro $b = 1$ získáme 0, takže $a^2 + b^2 = 0$, i když není a i b nulové.

Pokud je $c = 0$, musíme vyřešit, kdy $a^2 + b^2 = 0$:

$$a^2 = -b^2.$$

Polynom $a^2+b^2 = 0$ má nad tělesem $\mathbb{Q}[i]$ právě dva kořeny a to $\pm ib$. Tím získáme právě dvě možnosti

$$a = \pm ib.$$

Dostaneme body $(a, ib, 0)$, $(a, -ib, 0)$. Ze zadání předpokládáme nesoudělnost každých dvou složek řešení takže $\mathbf{NSD}(a, 0) = 1$ a $\mathbf{NSD}(b, 0) = 1$. Proto platí, že $a \parallel 1$ a $b \parallel 1$. Takhle získáme řešení $\pm(1, i, 0), \pm(-1, i, 0), \pm i(1, i, 0), \pm i(-1, i, 0)$.

Pokud $c \neq 0$, pak celou rovnici vydělíme c^2 stejně jako v motivačním příkladu z první kapitoly. Získáme

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1.$$

Tady provedeme substituci, $\frac{a}{c}$ si označíme jako x a $\frac{b}{c}$ jako y. Nyní máme rovnici

$$x^2 + y^2 = 1,$$

kde chceme najít řešení pro všechna čísla $x, y \in \mathbb{Q}[i]$.

Opět jako v příkladu z 1. kapitoly zvolíme nějaký racionální bod, který na naší kružnici leží. Vyberme si ten stejný bod $(0, 1)$. Přímky zde zapíšeme v obecném tvaru místo tvaru z definice 10, který jsme si definovali, aby příklad lépe připomínal řešený příklad z 1. kapitoly. Stejně jako v první kapitole budeme hledat průsečíky s přímkou v obecném tvaru. To nezmění nijak řešení, protože lze přímku $\{(tk,1+tl); t \in \mathbb{Q}\}$ snadno převést na rovnice $x = ky-k$ a $y = 1$. Všechny přímky procházející bodem $(0, 1)$ jsou $x = ky - k$, kde $k \in \mathbb{Q}[i]$ a tečna $y = 1$, díky které ale nezískáme žádné nové body.

Spočítáme průnik kružnice $x^2 + y^2 = 1$ s přímkou $x = ky - k$:

$$(ky - k)^2 + y^2 - 1 = 0$$

Celou rovnici upravíme do tvaru kvadratické rovnice

$$y^2(1 + k^2) - 2k^2y + k^2 - 1 = 0.$$

To si opět rozdělíme na dva případy.

V případě, kdy $1 + k^2 = 0$ se nejedná o kvadratickou rovnici.Vyřešíme pro k a dostaneme, že $k = \pm i$. Pro tyto hodnoty k vyřešíme rovnici

$$-2k^2y + k^2 - 1 = 0.$$

Dosadíme do této rovnice za k:

$$2y - 1 - 1 = 0.$$

Tím získáme jediné řešení a to $y = 1$. Dopočítáme z rovnice $x = ky - k$ hodnotu pro x a dostaneme bod $(1, 0)$.

V případě, kdy $k \neq \pm i$, řešíme kvadratickou rovnici. To vede na stejná řešení jako v příkladu 1. Jeden z kořenů $y = 1$ známe, protože odpovídá zvolenému bodu $(0, 1)$, a tak použijeme Vietův vzorec 7 a dostaneme rovnici

$$y + 1 = -\frac{-2k^2}{1 + k^2}.$$

Z toho vyjádříme y

$$y = \frac{k^2 - 1}{1 + k^2}.$$

Úpravou jsme získali všechny souřadnice y průsečíků přímky s kružnicí. Po dosazení do rovnice přímky vyřešíme pro x:

$$x = \frac{-2k}{1 + k^2}.$$

Bod, který jsme nalezli pro volbu $k = \pm i$ lze získat i dosazením za $k = -1$. Nalezli jsme průsečíky, které zatím vypadají identicky s průsečíky nalezenými v motivačním příkladu.

$$\left\{ \left(\frac{-2k}{1 + k^2}, \frac{k^2 - 1}{1 + k^2} \right); k \in \mathbb{Q}[i], \text{ kde } k \neq \pm i \right\} \cup \{(0, 1)\}.$$

Číslo k opět vyjádříme zlomkem, takže $k = \frac{u}{v}$, kde $u, v \in \mathbb{Z}[i], v \neq 0$ a také $\mathbf{NSD}(u,v) = 1$. Celou dobu si musíme dát pozor, aby se $\frac{u}{v} \neq \pm i$, což upravíme a dostaneme $u \neq \pm vi$. To můžeme dále upravit, jelikož jsou proměnné u, v nesoudělné a zjistíme, že tato podmínka přesně vyloučí ty body, které jsme získali v případě, kde $c = 0$. Poznamenejme, že toto vyjádření není jednoznačné, jako bylo v příkladu 1. Například číslo 1 lze zapsat několika způsoby $1 = \frac{1}{1} = \frac{i}{i}$. Všimněme si ještě, že pro $v = 0$ získáme bod $(0, 1)$. Tím získáme řešení tvaru

$$\left\{ \left(\frac{-2uv}{u^2 + v^2}, \frac{u^2 - v^2}{u^2 + v^2} \right); v, u \in \mathbb{Z}[i], \mathbf{NSD}(u, v) = 1, u \neq vi \right\}.$$

Nyní musíme vyřešit nesoudělnost čitatele se jmenovatelem. V 1. kapitole jsme to řešili úvahou přes paritu čísel. V $\mathbb{Z}[i]$ ale není nic takového definované, a proto to bude složitější. Z toho důvodu jsme si na začátku kapitoly zavedli lemmata 20 a 21, která zde využijeme.

Potřebujeme najít $\mathbf{NSD}(u^2 - v^2, u^2 + v^2)$ a $\mathbf{NSD}(-2uv, u^2 + v^2)$.

Podívejme se na $\mathbf{NSD}(-2u^2, u^2 + v^2)$. Nechť p je prvočinitel, který dělí $2u^2$ a $u^2 + v^2$. Protože p dělí $2u^2$, musí nastat alespoň jedna z následujících možností.

Kdyby $p \mid u$, to by znamenalo, že $p \mid u^2$. My víme, že $p \mid u^2 + v^2$, a tak by nutně $p \mid v^2$ a nebo rovnou $p \mid v$, takže by $p \mid \mathbf{NSD}(u, v) = 1$, což je spor s tím, že je p prvočinitel.

Kdyby $p \mid 2$, víme, že $2 \parallel (1+i)^2$, a tedy $p \equiv 1+i$, bez újmy na obecnosti můžeme předpokládat, že $p = 1+i$. Podívejme se na možné zbytky $\pmod{1+i}$. To je podle lemmatu 20 jen 0 nebo 1. A lemma 21 říká, že pro $u \equiv v \pmod{1+i}$ máme $\mathbf{NSD}(u^2+v^2, 2u^2) = (1+i)^\kappa$ pro $\kappa \geq 1$ a $\mathbf{NSD}(u^2+v^2, 2u^2) = 1$ pro $u \not\equiv v \pmod{1+i}$

Pojďme zjistit, pro jaká κ platí $\mathbf{NSD}(2u^2, u^2+v^2) = (1+i)^\kappa$. Pro $\kappa \geq 3$ dostaneme, že $(1+i) \mid u^2$ a také musí $(1+i) \mid u^2+v^2$. To dáme dohromady a získáme $(1+i) \mid v^2$, a proto $(1+i) \mid v$, což je spor s nesoudělností u, v.

Z lemmatu 21 víme, že $2 \mid u^2+v^2$ právě tehdy, když $u \equiv v \pmod{1+i}$.

Závěrem máme, že $\mathbf{NSD}(u^2+v^2, 2v^2) = 1$ pro $u \not\equiv v \pmod{1+i}$. Z toho je možné spatřit analogii v $\mathbb{Z}$. Pokud bychom čísla $u \equiv 0 \pmod{1+i}$ nazvali sudá a číslům $u \equiv 1 \pmod{1+i}$ bychom říkali lichá, máme skoro stejnou úvahu.

Pojďme se podívat na řešení druhé části $\mathbf{NSD}(-2uv, u^2+v^2)$. Opět předpokládejme, že p je prvočinitel, který $p \mid 2uv$.

Kdyby $p \mid u$, pak platí, že $p \mid u^2$ a měli bychom $p \mid \mathbf{NSD}(u^2, u^2+v^2) = \mathbf{NSD}(u^2, v^2)$. To je ale spor s nesoudělností u, v. Proto máme $\mathbf{NSD}(u^2+v^2, 2v^2) = 1$.

Kdyby $p \mid v$ máme ze symetrie totéž.

Kdyby $p \mid 2$, pak budeme postupovat stejně, jako v předchozí části. Jelikož je $2 \equiv (1+i)^2$, je $p = 1+i$. Pojďme ověřit, zda $1+i \mid u^2+v^2$. Víme, z lemmatu 21, že to platí, pokud $u \parallel v \pmod{1+i}$. Takže $\mathbf{NSD}(-2uv, u^2+v^2) = (1+i)^\lambda$. Pojďme zjistit, zda to platí pro $\lambda \geq 3$. To nastane, pokud $(1+i) \mid u$. Potom $(1+i) \mid u^2$ a počítáme $\mathbf{NSD}(u^2, u^2+v^2) = \mathbf{NSD}(u^2, v^2)$. Tedy $(1+i) \mid v^2$ a z toho máme, že $(1+i \mid v$, to je opět spor s nesoudělností u, v.

Ještě si musíme dát pozor na to, že z toho, že jsou proměnné po dvou nesoudělné plyne, že pokud je (a, b, c) řešení, pak je i $\varepsilon(a, b, c)$, kde ε je jednotka v $\mathbb{Z}[i]$, tedy $\varepsilon \in \{1, -1, i, -i\}$.

Nyní jsme už schopni zformulovat řešení celého příkladu.

Věta 22. *Všechna řešení rovnice $a^2+b^2 = c^2$, kde jsou proměnné (a, b, c) po dvou nesoudělné nad $\mathbb{Z}[i]$, jsou*

- $\{\varepsilon(-2uv, u^2-v^2, u^2+v^2); u \not\equiv v \pmod{1+i}, \mathbf{NSD}(u, v) = 1, v \neq iu\}$
- $\varepsilon(1, i, 0)$, $\varepsilon(-1, i, 0)$, $(0, 0, 0)$,
- $\left\{\varepsilon(-uv, \frac{u^2-v^2}{2}, \frac{u^2+v^2}{2}); u \equiv v \pmod{1+i}, \mathbf{NSD}(u, v) = 1, v \neq iu\right\}$,

kde je $\varepsilon = \pm 1 \pm i$.

3.2 Rovnice vedoucí na kružnici

Tento příklad nám nepřinese příliš nového, ale bude zapotřebí k řešení následujícího příkladu se čtyřmi proměnnými.

Příklad. Najděte všechna celočíselná řešení rovnice

$$a^2 + b^2 = 2c^2$$

taková, že jsou celá čísla a, b, c po dvou nesoudělná.

Nejprve začneme s případem, kde je pravá strana nulová, tedy když $c = 0$. To nastane pouze v případě, kdy je $a = 0$ a $b = 0$. Takže platí, že je kvadrika $\{(a, b, c), a^2 + b^2 = 2c^2\}$ definitní.

Pro $c \neq 0$ vydělíme a dostaneme rovnici

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 2.$$

Označíme si $\frac{a}{c}$ jako x a $\frac{b}{c}$ jako y. Máme rovnici tvaru

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

Jako bod zvolme třeba $(1, 1)$. Všechny přímky procházející tímto bodem jsou přímky tvaru $p = \{(1 + \alpha t, 1 + \beta t); t \in \mathbb{Q}\}$, kde $\alpha, \beta \in \mathbb{Q}$.

Pro $\alpha = 0$, $\beta \neq 0$ bychom získali přímku $\{(1, 1 + \beta t); t \in \mathbb{Q}\}$, což je přímka, která má s kružnicí dva průsečíky $(1, 1), (1, -1)$.

Ať $\alpha \neq 0$. Místo t dosadíme $\frac{t}{\alpha}$, protože množina $\{t; t \in \mathbb{Q}\}$ je stejná jako množina $\{\frac{t}{\alpha}; t \in \mathbb{Q}\}$. Takhle můžeme vyjádřit uvažované přímky ve tvaru

$$p = \{(1 + t, 1 + \beta t); t \in \mathbb{Q}\}.$$

Hledáme průsečíky přímky p s rovnicí $x^2 + y^2 = 2$. Dostaneme následující rovnost:

$$(1 + t)^2 + (1 + \beta t)^2 = 2.$$

To přeuspořádáme na tvar kvadratické rovnice v proměnné t

$$t^2(1 + \beta^2) + t(2 + 2\beta) = 0.$$

Klasickým způsobem najdeme kořeny

$$t = -\frac{2 + 2\beta}{1 + \beta^2} \text{ nebo } t = 0.$$

Všimněme si, že $1 + \beta^2 \neq 0$, takže nikdy nedělíme 0. To nastalo díky tomu, že pracujeme s definitní kvadrikou.

Dosadíme zpátky do přímky p a dostaneme

$$x = 1 - \frac{2 + 2\beta}{1 + \beta^2},$$

kde si vyjádříme x jako

$$x = \frac{\beta^2 - 2\beta - 1}{1 + \beta^2}.$$

Stejně tak pro druhou souřadnici

$$y = 1 - \beta\left(\frac{2 + 2\beta}{1 + \beta^2}\right).$$

Ještě to upravíme na společného jmenovatele

$$y = \frac{-\beta^2 - \beta + 1}{1 + \beta^2}.$$

Množina všech racionálních bodů na kružnici $x^2 + y^2 = 2$ tedy je

$$\left\{\left(\frac{\beta^2 - 2\beta - 1}{1+\beta^2}, \frac{-\beta^2 - \beta + 1}{1+\beta^2}\right); \beta \in \mathbb{Q}\right\} \cup \{(1,1),(1,-1)\}.$$

Potřebujeme se dostat z $\mathbb{Q}$ zpátky do $\mathbb{Z}$, a tak dosadíme $\beta = \frac{u}{v}$, kde $u, v \in \mathbb{Z}$ $\mathbf{NSD}(u,v) = 1$ a $v > 0$. Máme tedy množinu řešení, kdy budeme muset dořešit nesoudělnost jednotlivých činitelů.

$$\left\{\left(\frac{u^2 - 2uv - v^2}{u^2+v^2}, \frac{-u^2 - 2uv + v^2}{u^2+v^2}\right); u, v \in \mathbb{Z}, \mathbf{NSD}(u,v) = 1, v > 0\right\}$$

$$\cup (1,1),(1,-1)$$

Spočítejme $\mathbf{NSD}(u^2 - 2uv - v^2, u^2 + v^2), \mathbf{NSD}(v^2 - 2uv - u^2, u^2 + v^2)$.

Začneme nejprve s $\mathbf{NSD}(u^2 - 2uv - v^2, u^2 + v^2)$. Pomocí vlastnosti $\mathbf{NSD}(a,b) = \mathbf{NSD}(a, b+a)$ upravíme $\mathbf{NSD}(u^2 - 2uv - v^2, u^2 + v^2) = \mathbf{NSD}(2u^2 - 2uv, u^2 + v^2)$. Nechť p je prvočíslo, kde $p \mid \mathbf{NSD}(2u^2 - 2uv, u^2 + v^2)$. Pak $p \mid 2u^2 - 2uv$ takže p dělí $2u(u - v)$. To si rozložíme na následující případy.

Kdyby $p \mid 2$, pak by muselo platit, že $p = 2$. To, že $2 \mid u^2 + v^2$ nastane v případě, kde jsou u, v obě lichá

Nechť $2^\kappa \mid (u^2 - 2uv)$ a $2\kappa \mid (u^2 + v^2)$. Pro u, v liché bude $\kappa \geq 1$. Kdyby $\kappa \geq 2$, pak bychom došli k tomu, že $u^2 + v^2 \equiv 0 \pmod 4$. Jelikož jsou u, v liché, pak musíme mít $u^2 + v^2 \equiv 2 \pmod 4$, což je spor. Vidíme tedy, že $\kappa = 1$, právě tehdy, když u, v jsou obě lichá. Takže $\mathbf{NSD}(2u^2 - 2uv, u^2 + v^2) = 2$ pro u, v obě lichá.

Kdyby $p \mid u$, pak $p \mid u^2$. Ale potom aby p dělilo $u^2 + v^2$ muselo by dělit v^2, a proto by p dělilo rovnou v, což je spor s nesoudělností u, v.

Kdyby $p \mid (u - v)$ a $p \neq 2$, to zapišme jako $u \equiv v \pmod p$. Bude také platit, že $u^2 \equiv v^2 \pmod p$ Podobně si rozepišme to, že p dělí $u^2 + v^2$, takže $0 \equiv u^2 + v^2 \pmod p$. Pokud odečteme jednu rovnici od druhé získáme $0 \equiv 2v^2 \pmod p$. Z toho vidíme, že $p \mid 2v^2$, takže p dělí v, protože předpokládáme, že $p \neq 2$. Pak by ale muselo p dělit i u, což by byl spor s nesoudělností. Proto pro u, v různé parity máme $\mathbf{NSD}(u^2 - 2uv - v^2, u^2 + v^2) = 1$.

Ještě pojďme vyřešit nesoudělnost $\mathbf{NSD}(v^2 - 2uv - u^2, u^2 + v^2) = \mathbf{NSD}(-2u^2 + 2uv)$, čímž získáme totéž, co v minulém případě. Máme tedy $\mathbf{NSD}(v^2 - 2uv - u^2, u^2 + v^2) = 1$ pro u, v různé parity a $\mathbf{NSD}(v^2 - 2uv - u^2, u^2 + v^2) = 2$, pro u, v obě lichá.

Také nesmíme zapomenout na to, že díky $\mathbf{NSD}(a,c) = 1$ a $\mathbf{NSD}(b,c)$ dostáváme, že pokud je (a,b,c) řešení, pak je řešení i $-1(a,b,c)$.

Věta 23. *Všechna celočíselná řešení rovnice $a^2 + b^2 = 2c^2$, kde jsou proměnné (a,b,c) po dvou nesoudělné, jsou*

- $\{\pm(u^2 - 2uv - v^2, -u^2 - 2uv + v^2, u^2 + v^2)$, *pro u, v různé parity, kde* $\mathbf{NSD}(u,v) = 1, v > 0\}$
- $\{\pm(\frac{u^2 - 2uv - v^2}{2}, \frac{-u^2 - 2uv + v^2}{2}, \frac{u^2 + v^2}{2})$, *pro u, v obě lichá, kde* $\mathbf{NSD}(u,v) = 1, v > 0\}$
- $\pm(1,1,1)$, *nebo* $\pm(1,-1,1)$

3.3 Rovnice vedoucí na hyperboloid

Příklad. Najděte všechna řešení rovnice

$$a^2 + b^2 - 2c^2 = d^2$$

taková, že jsou celá čísla a, b, c, d po dvou nesoudělná.

Nejprve vyřešíme případ, kde $a^2+b^2-2c^2 = 0$. To vede na rovnici $a^2+b^2 = 2c^2$, což jsme vyřešili v předchozím příkladě v sekci 3.2. Tato řešení nyní vyloučíme, čímž zajistíme, že nebudeme dělit nulou.

Pro $d \neq 0$ celou rovnici vydělíme a dostaneme

$$\frac{a^2}{d^2} + \frac{b^2}{d^2} - \frac{2c^2}{d^2} = 1.$$

Provedeme substituci $x = \frac{a}{b}, y = \frac{b}{d}, z = \frac{c}{d}$, čímž získáme rovnici

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

To je rovnice hyperboloidu. Chceme najít všechny racionální body, které na něm leží. Všimněme si, že se nejedná o definitní kvadriku. Zvolme bod $(1, 0, 0)$. Přímka procházející tímto bodem má tvar

$$\{(1 + \alpha t, \beta t, \gamma t); t \in \mathbb{Q}\}$$

pro $\alpha, \beta, \gamma \in \mathbb{Q}$.

Pro $\alpha = 0$ máme přímky

$$\{(1, \beta t, \gamma t); t \in \mathbb{Q}\}.$$

Pokud je $\beta = 0$, pak nutně $\gamma \neq 0$ a můžeme nahradit $\frac{t}{\gamma}$ za t, čímž dostaneme

$$\{(1, 0, t); t \in \mathbb{Q}\}.$$

Když se podíváme na průsečíky této přímky s hyperboloidem, dostaneme $-2t^2 = 0$, což má jeden dvojnásobný kořen $t = 0$. Jedná se proto o tečnu a nedostaneme jiný bod než $(1, 0, 0)$.

Pro $\beta \neq 0$ budeme mít přímky

$$\{(1, \beta t, \gamma t); t \in \mathbb{Q}\}.$$

Můžeme nahradit $\frac{t}{\beta}$ za t, čímž dostaneme rovnici

$$\{(1, t, \gamma t); t \in \mathbb{Q}\}.$$

Spočítejme průsečíky s hyperboloidem:

$$1^2 + t^2 - 2\gamma^2 t^2 = 1.$$

To přeuspořádejme a upravíme na kvadratickou rovnici v proměnné t

$$t^2(1 - 2\gamma^2) = 0.$$

Ta má pouze jeden dvojnásobný kořen $t = 0$, takže nezískáme nová řešení.

Pro $\alpha \neq 0$ můžeme nahradit $\frac{t}{\alpha}$ za t získáme přímky

$$\{(1 + t, \beta t, \gamma t); t \in \mathbb{Q}\}.$$

To dosadíme do naší rovnice hyperboloidu $x^2 + y^2 - 2z^2 = 1$

$$(1 + t)^2 + (\beta t)^2 - 2(\gamma t)^2 = 1$$

Rovnici přeuspořádejme do tvaru kvadratické rovnice v proměnné t

$$t^2(\beta^2 - 2\gamma^2 + 1) + 2t = 0.$$

Vyjádřeme si její kořeny jako

$$t = \frac{-2}{1 + \beta^2 - 2\gamma^2} \text{ nebo } t = 0.$$

Po opětovném dosazení do rovnice přímky za t získáme body

$$\left\{ \left(\frac{\beta^2 - 2\gamma^2 - 1}{\beta^2 - 2\gamma^2 + 1}, \frac{-2\beta}{1 + \beta^2 - 2\gamma^2}, \frac{-2\gamma}{\beta^2 - 2\gamma^2 + 1} \right); \beta, \gamma \in \mathbb{Q} \right\}.$$

Potřebujeme dosadit zpátky za $\beta = \frac{u}{v}$ a za $\gamma = \frac{w}{v}$, kde už nutně nemáme nesoudělnost obou prvků, ale místo toho můžeme předpokládat, že $\mathbf{NSD}(u, v, w) = 1$ a $v > 0$. Získáme

$$\left\{ \left(\frac{u^2 - v^2 - 2w^2}{u^2 + v^2 - 2w^2}, \frac{-2uv}{u^2 + v^2 - 2w^2}, \frac{-2vw}{u^2 + v^2 - 2w^2} \right); \mathbf{NSD}(u, v, w) = 1, v \geq 0 \right\}.$$

Nyní potřebujeme z řešení v $\mathbb{Q}$ získat řešení v $\mathbb{Z}$. Zde máme o jednu proměnnou navíc, a tak je velice obtížné spočítat největšího společného dělitele. Označme si ho prozatím jako

$$D = \mathbf{NSD}(-2uv, v^2 + u^2 - 2w^2).$$

Potom máme $b = \frac{-2uv}{D}, d = \frac{v^2+u^2-2w^2}{D}$. Proměnné jsou po dvou nesoudělné podle předpokladu ze zadání, tedy máme $\mathbf{NSD}(a, d) = 1$. Z čehož můžeme odvodit

$$\frac{u^2 - v^2 - 2w^2}{u^2 + v^2 - 2w^2} = \frac{a}{d} = \frac{a}{\frac{u^2+v^2-2w^2}{D}}.$$

Aby rovnosti platily, musí být nutně $a = \frac{u^2-v^2-2w^2}{D}$. Stejně dostaneme, že $c = \frac{-2vw}{D}$. Z toho vidíme, že také $D = \mathbf{NSD}(u^2 - v^2 - 2w^2, u^2 + v^2 - 2w^2) = \mathbf{NSD}(-2vw, u^2 + v^2 - 2w^2)$.

Zde nebude možné získat nějaké explicitní podmínky na největšího společného dělitele, ale můžeme se pokusit zjistit, jaký musí mít tvar.

Nechť je p prvočíslo takové, že $p \mid D$. Rozebereme si jednotlivé případy.

Kdyby $p \mid 2$, pak by $p = 2$ a tedy $2 \mid u^2 + v^2 - 2w^2$. Platí, že $2 \mid u^2 + v^2$, pokud mají u i v stejnou paritu. Buď $k \in \mathbb{N}$ největší takové, že $2^k \mid \mathbf{NSD}(u, v)$. Kdyby byly u, v obě stejné parity, pak platí, že $k \geq 1$.

Kdyby bylo $k = 2$, platí, že $4 \mid u^2 + v^2 - 2w^2$, $4 \mid u^2 - v^2 - 2w^2$, a z toho vidíme, že $4 \mid -2v^2$, takže taky $2 \mid v^2$ a rovnou $2 \mid v$. To bude potom splňovat podmínky $2 \mid uv$ a $2 \mid vw$.

Pro $k \geq 3$ platí, že $2^k \mid 2v^2$ tedy $2^{k-1} \mid v^2$. Zároveň platí, že $2^k \mid u^2+v^2-2w^2$.

Kdyby $p \mid v^2$ pro $p \neq 2$, pak by platilo, že $p \mid v$. Počítejme kongruence, aby $p \mid u^2+v^2-2w^2$ z toho získáme

$$u^2 \equiv 2w^2 \pmod{p}.$$

Všimněme si, že pokud by $w \equiv 0 \pmod{p}$, potom by $p \mid u$, což by byl spor s nesoudělností $\mathbf{NSD}(u,v,w)$. Můžeme tedy kongruenci vydělit w^2 a dostaneme

$$\left(\frac{u}{w}\right)^2 \equiv 2 \pmod{p}.$$

To má řešení pro $p \equiv \pm 1 \pmod 8$, což víme ze zdroje (3), konkrétně používáme tvrzení 4.4 na straně 31.

Stejnými postupy můžeme zjistit, jak je to s kongruencemi modulo p^k pro $k \in \mathbb{N}$. Dojdeme ke kongruenci

$$\left(\frac{u}{w}\right)^2 \equiv 2 \pmod{p^k}.$$

Všechno by platilo i naopak, pokud je splněná podmínka $\left(\frac{u}{w}\right)^2 \equiv 2 \pmod{p^k}$, potom platí, že $p^k \mid D$ a z podmínky $\left(\frac{u}{w}\right)^2 \equiv 2 \pmod{p}$ dostaneme, že $p \mid D$.

Všechno, co jsme zjistili o číslu D si shrneme v následující větě.

Věta 24. *Buďte u,v,w celá čísla taková, že $v>0$ a $\mathbf{NSD}(u,v,w)=1$, a buď $D=\mathbf{NSD}(-2uv, v^2+u^2-2w^2)$. Potom platí, že $D=2^{k_0}p_1^{k_1}p_2^{k_2}\dots p_l^{k_l}$ pro $k,l \in \mathbb{N}$ a po dvou různá lichá prvočísla $p_1,\dots,p_l$ a přirozená čísla $k_0,k_1,\dots,k_l$, přičemž $p_i \equiv \pm 1 \pmod 8$ pro všechna i. Navíc k_i je největší celé číslo takové, že $p_i^{k_i} \mid (u^2-2w^2)$ a zároveň $p_i^{k_i} \mid v^2$. Číslo k_0 je největší celé číslo, pro které platí, že $2^{k_0-1} \mid v^2$ a $2^{k_0} \mid u^2+v^2-2w^2$.*

Jedná se o dost složité podmínky, které je nejspíš nemožné vyjádřit explicitněji. Například pro $w=1, u=3, v=7$ dostaneme $D=7$.

Dejme dohromady všechna řešení, která jsme zatím nalezli. Stejně jako v předchozích příkladech si musíme dát pozor na to, že pokud je (a,b,c,d) řešení, pak je i $-(a,b,c,d)$ řešení.

Věta 25. *Všechna celočíselná řešení rovnice $a^2+b^2-2c^2=d^2$, kde jsou proměnné (a,b,c,d) po dvou nesoudělné, jsou*

- $\pm(\frac{u^2-v^2-2w^2}{D}, \frac{-2uv}{D}, \frac{-2vw}{D}, \frac{u^2+v^2-2w^2}{D}); \mathbf{NSD}(u,v,w)=1, v>0$
- $\pm(1,0,0,1)$
- $\{\pm(u^2-2uv-v^2, -u^2-2uv+v^2, u^2+v^2, 0),$ *pro u,v různé parity, kde* $\mathbf{NSD}(u,v)=1, v>0\}$
- $\{\pm(\frac{u^2-2uv-v^2}{2}, \frac{-u^2-2uv+v^2}{2}, \frac{u^2+v^2}{2}, 0),$ *pro u,v obě lichá, kde* $\mathbf{NSD}(u,v)=1, v>0\}$
- $\pm(1,1,1,0)$, *nebo* $\pm(1,-1,1,0)$

Kde $D=\mathbf{NSD}(-2uv, u^2+v^2-2w^2)$, pro které platí podmínky uvedené ve větě 24.

Závěr

Hlavním cílem práce bylo zobecnit metodu řešení kvadratických diofantických rovnic, což se povedlo. Podívali jsme se i na to, jak řešit příklady vedoucí na jiné než definitní kvadriky. K těmto kvadrikám jsme vypracovali teorii, kterou jsme využili při řešení takových příkladů ve třetí kapitole. Konkrétně se jednalo o příklady 3.1 a příklad 3.3. Řešení obecných příkladů bylo trochu obtížnější a občas jsme si museli přidat do zadání příkladu předpoklad toho, že jsou proměnné po dvou nesoudělné. To jsme udělali v každém příkladu ve 3. kapitole. Bylo by možné příklad řešit i bez toho, ale bylo by to o dost komplikovanější.

V posledním příkladu ze 3. kapitoly jsme získali složité podmínky pro největšího společné dělitele, ty jsme se pokusili formulovat ve větě 24. Bylo by zajímavé prozkoumat, za jakých podmínek dostaneme takového komplikovaného největšího společného dělitele. Jestli tomu tak například je u všech rovnic s alespoň 4 proměnnými nebo jestli to souvisí s tím, že kvadrika nebyla definitní.

Seznam použité literatury

[1] Davis, M. (1973). Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, **80**(3), 233–269. ISSN 00029890, 19300972. URL http://www.jstor.org/stable/2318447.

[2] Kala, V. a Opršal, J. (2009). Seriál pro Matematický korespondenční seminář. [online]. URL https://prase.cz/library/TeorieCiselJOVK/TeorieCiselJOVK.pdf.

[3] Kala, V. (2022). Teorie čísel. [online]. URL https://www.karlin.mff.cuni.cz/~kala/files/TC22.pdf.

[4] Reichl, J. a Všetička, M. (2022). Diofantos z alexandrie. [online]. URL http://fyzika.jreichl.com/main.article/view/1436-diofantos-z-alexandrie.