

Gymnázium Brno, tř. Kpt. Jaroše 14, 658 70 Brno  
2005/2006, 4.A

# Gaussovská prvočísla

Závěrečná maturitní práce z matematiky

Jakub Opršal

Brno 2006

Prohlašuji, že jsem předloženou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.

Jakub Opršal

V Brně dne 2.4.2006  
Vedoucí závěrečné práce: Mgr. Viktor Ježek

## Abstrakt

Tato práce popisuje konkrétní část matematiky – Gaussova prvočísla, respektive teorii kolem Gaussových celých čísel a její základní věty. Kromě této problematiky řeší některé části teorie čísel (zvláště Legendreovy symboly) a komplexní čísla.

Gaussova celá čísla jsou komplexní čísla s celočíselnou reálnou a imaginární částí. V této množině můžeme definovat dělitelnost obdobně jako v celých číslech. Pokud se hlouběji ponoříme, zjistíme, že Gaussova čísla mají vlastnosti velmi podobné číslům celým, např. věty o dělitelnosti, největší společný dělitel, Euklidův algoritmus, Bezoutova věta, rozklad na prvočinitele a další.

Za zmínku stojí zvlášt Euklidův algoritmus, který je běžně založen na dělení se zbytkem. Náš Euklidův algoritmus, tak jak je popsán v této práci, je založen na podobných základech, ale samotné dělení se zbytkem nepoužívá, a proto se dělením se zbytkem, které je v Gaussových číslech značně složitější než v celých číslech, nemusíme zabývat.

Naším cílem bylo krom dokázání všech základních vět i popsat tvar Gaussových prvočísel (v závislosti na běžných prvočíslech). Dokázání takového faktu nám zjednoduší hledání Gaussových prvočísel, protože velké množství běžných prvočísel známe. A krom toho nám problém rozhodnutí, zda dané Gaussovo číslo je prvočíslo, převádí na více řešený problém o rozhodnutí, zda je celé číslo prvočíslem.

Gaussova čísla mají mnoho uplatnění v běžné teorii čísel. Velmi jednoduše lze například zapsat dané číslo jako součet dvou druhých mocnin pomocí rozkladu na Gaussovy prvočinitele. V závěru práce také ukážeme použití na jednom konkrétním příkladě z letošního ročníku matematické olympiády.

## Resumé

This work describes very concrete part of mathematics. Beside the main problem of Gaussian primes, we have described some parts of number theory (especially Legendre symbols), complex numbers — we have described whole basic theory — and at last Gaussian integers.

Gaussian integers are complex numbers with integer coefficients. In this set, we can define divisibility like in common integers. If we will study deeply, we'll find that Gaussian integers has the same properties as ordinary integers, e.g. theorems about divisibility, greater common divisors, Euclid algorithm, Bezout theorem, prime factorisation, etc.

One thing we've described unusual is Euclid algorithm, because standard Euclid algorithm requires defined divisibility with remainder, which is useful just for it. Our Euclid algorithm is based on the same as the ordinary one, but in a slightly different way.

Gaussian integers has also many appliances in common number theory. It's very easy to write a positive integer as a sum of two squares by factorisation to Gaussian primes. More powerful in these cases is set of "integer" quaternions, because of Lagrange theorem (sometimes called Theorem of Four Squares): Every positive integer can be written as a sum of four (or less) squares.

We would like to warn you, that Gaussian integers aren't only one number set like this. Besides Gaussian integers, there exists Eisenstein integers, which are defined as:  $a + b\omega$ , where  $a, b \in \mathbb{Z}$  and  $\omega = \frac{-1+i\sqrt{3}}{2}$ . That means one of the numbers, which satisfy the equation  $\omega^3 = 1$ .

---

# Obsah

<b>Obsah</b>	<b>5</b>
<b>1. Vybrané kapitoly z teorie čísel</b>	<b>6</b>
1.1. Kongruence . . . . .	6
1.2. Kvadratické zbytky . . . . .	6
1.3. Legendreovy symboly . . . . .	7
<b>2. Komplexní čísla</b>	<b>8</b>
2.1. Zavedení komplexních čísel . . . . .	8
2.2. Absolutní hodnota, goniometrický tvar komplexního čísla . . . . .	9
2.3. Gaussova rovina . . . . .	10
<b>3. Celá komplexní čísla</b>	<b>12</b>
3.1. Dělitelnost v celých komplexních číslech . . . . .	12
3.2. Největší společný dělitel a nejmenší společný násobek . . . . .	12
3.3. Obdoba Euklidova algoritmu a Bezoutovy věty . . . . .	13
<b>4. Gaussova prvočísla</b>	<b>15</b>
4.1. Vlastnosti Gaussových prvočísel . . . . .	15
4.2. Tvar Gaussových prvočísel . . . . .	15
4.3. Využití Gaussových prvočísel . . . . .	17
<b>Použitá literatura</b>	<b>19</b>

## 1. Vybrané kapitoly z teorie čísel

V této kapitole bychom rádi čtenáři přiblížili některé kapitoly z teorie čísel, které se běžně neučí na střední škole a které budeme v dalších kapitolách využívat. Všechna obecně známá tvrzení neuvádíme a nedokazujeme, můžete je nalézt i s důkazy v [2].

### 1.1. Kongruence

**Def.** Říkáme, že  $a$  je *kongruentní s  $b$  modulo  $c$*  právě tehdy, když  $a$  a  $b$  dávají stejný zbytek po dělení číslem  $c$ . Píšeme  $a \equiv b \pmod{c}$ .

**Věta 1.1.1**  $a \equiv b \pmod{m} \iff \exists t \in \mathbb{Z} : a = mt + b \iff m \mid (a - b)$

Důkaz této věty spolu s dalšími vlastnostmi kongruencí naleznete v [2] od strany 178.

### 1.2. Kvadratické zbytky

Budeme-li zkoumat zbytky druhých mocnin celých čísel po dělení nějakým číslem  $n$  snadno zjistíme, že mohou nabývat jen některých hodnot. Které zbytky můžeme dostat snadno ověříme, dosadíme-li do kongruence všechny možné zbytky a umocníme je postupně na druhou, například druhé mocniny mohou modulo 8 nabývat jen zbytky:

$$\begin{array}{ll} 0^2 \equiv 0 \pmod{8} & 4^2 \equiv 16 \equiv 0 \pmod{8} \\ 1^2 \equiv 1 & 5^2 \equiv 25 \equiv 1 \\ 2^2 \equiv 4 & 6^2 \equiv 36 \equiv 4 \\ 3^2 \equiv 9 \equiv 1 & 7^2 \equiv 49 \equiv 1 \end{array}$$

**Def.** Nechť  $n \in \mathbb{N}$ . Říkáme, že číslo  $a \in \{0, 1, \dots, n-1\}$  je *kvadratickým zbytkem modulo  $n$*  pokud existuje celé číslo  $c$  takové, že  $c^2 \equiv a \pmod{n}$ . V opačném případě nazveme číslo  $a$  *kvadratickým nezbytkem modulo  $n$* .

Kromě modulu 8 jsou zajímavé ještě kvadratické zbytky všech jednociferných modulů. Často se dají využít v úlohách z teorie čísel. Přehledně je udává následující tabulka:

<b>3,4</b>	0,1	<b>7</b>	0,1,2,4
<b>5</b>	0,1,4	<b>8</b>	0,1,4
<b>6</b>	0,1,3,4	<b>9</b>	0,1,4,7

**Věta 1.2.1** Nechť  $p$  je liché prvočíslo, pak existuje právě  $\frac{p-1}{2}$  nenulových kvadratických zbytků modulo  $p$ .

*Důkaz:* Všechny nenulové kvadratické zbytky modulo  $p$  najdeme tak, že vezmeme čísla  $1, 2, \dots, p-1$  a umocníme je na druhou. Uvědomme si, že platí:

$$\begin{aligned} x_1^2 &\equiv x_2^2 \pmod{p} \\ x_1^2 - x_2^2 &\equiv 0 \\ (x_1 - x_2)(x_1 + x_2) &\equiv 0 \\ x_1 &\equiv \pm x_2 \end{aligned}$$

Tedy kvadráty dvou různých čísel  $x_1$  a  $x_2$  z množiny  $\{1, 2, \dots, p-1\}$  dávají stejný zbytek po dělení  $p$  právě tehdy, když  $x_1 \equiv -x_2$ . Můžeme tedy tato čísla rozdělit do dvojic, podle kvadratického zbytku a těchto dvojic je pak  $\frac{p-1}{2}$ .

Přímým důsledkem věty 1.2.1 je tvrzení, že existuje právě  $\frac{p-1}{2}$  kvadratických nezbytků modulo lichým prvočíslem  $p$ .

### 1.3. Legendreovy symboly

Ještě si zobecníme definici kvadratického zbytku pro všechna celá čísla logickým rozšířením:

**Def.** Nechť  $n \in \mathbb{Z}$ , pak celé číslo  $a$  nazveme *kvadratický zbytek* modulo  $n$  právě tehdy, když existuje  $c \in \mathbb{Z} : c^2 \equiv a \pmod{n}$ .

**Def.** Mějme liché prvočíslo  $p$  a celé číslo  $a$ , pak číslo  $\left(\frac{a}{p}\right)$  nazýváme *Legendreovým symbolem* a definujeme takto:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{když } a \text{ je nenulovým kvadratickým zbytkem modulo } p \\ 0 & \text{pro } p \mid a \\ -1 & \text{když } a \text{ není kvadratickým zbytkem modulo } p \end{cases}$$

**Věta 1.3.1** Pokud  $a \equiv b \pmod{p}$  pak  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

*Důkaz:* Zřejmý.

**Věta 1.3.2 (Eulerovo kritérium)** Pro každé celé  $a$  a  $p$  liché prvočíslo platí:  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

*Důkaz:* Příklad  $p \mid a$  je jednoduchý, zaměřím se tedy na případ  $\mathcal{NSD}(a, p) = 1$ . Podle malé Fermatovy věty platí:

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) &\equiv 0 \pmod{p} \end{aligned}$$

Tedy  $a^{\frac{p-1}{2}} \equiv \pm 1$ .

Je-li  $a$  kvadratický zbytek pak platí, že existuje  $c \in \mathbb{Z}$  takové, že  $c^2 \equiv a$  tedy  $a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1$  (opět podle malé Fermatovy věty), tedy pro kvadratický zbytek věta platí. Navíc žádné jiné číslo kromě  $\frac{p-1}{2}$  nenulových kvadratických zbytků modulo  $p$  nemůže splňovat  $a^{\frac{p-1}{2}} - 1 \equiv 0$ , protože levá strana této kongruence je mnohočlen stupně  $\frac{p-1}{2}$  a proto má tato rovnice nejvýše  $\frac{p-1}{2}$  kořenů modulo  $p$ . Tedy pro kvadratické nezbytky platí:  $a^{\frac{p-1}{2}} \equiv -1$ .

**Věta 1.3.3** Nechť  $a, b \in \mathbb{Z}$ ;  $p$  je liché prvočíslo, pak platí:  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

*Důkaz:* Podle věty 1.3.2 platí:

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

A protože Legendreovy symboly mohou nabývat pouze hodnot 0, 1 a -1 a zároveň jsou tato čísla nekongruentní modulo  $p$ , pak z této kongruence vyplývá rovnost  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .

**Věta 1.3.4** Pro každé prvočíslo  $p$  tvaru  $4k + 1$  existuje  $n \in \mathbb{N}$  takové, že  $p \mid n^2 + 1$ .

*Důkaz:* Stačí dokázat, že číslo -1 je kvadratický zbytek modulo  $p$ .

Spočteme si symbol:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1.$$

Proto číslo -1 je kvadratickým zbytkem modulo  $p$ .

## 2. Komplexní čísla

V této kapitole bychom chtěli čtenáři přiblížit základy komplexních čísel.

### 2.1. Zavedení komplexních čísel

**Def.** *Komplexním číslem* rozumíme uspořádanou dvojici  $(a, b)$  reálných čísel  $a$  a  $b$ . Množinu všech komplexních čísel označíme  $\mathbb{C}$ . Na komplexních čísel definujeme relaci  $=$ :

$$(a_1, a_2) = (b_1, b_2) \iff a_1 = b_1 \wedge a_2 = b_2,$$

operace  $+$  (sčítání) a  $\cdot$  (násobení) následujícím způsobem:

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2), \\ (a_1, a_2) \cdot (b_1, b_2) &= (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1).\end{aligned}$$

Znaménko  $\cdot$  u operace násobení obvykle vynecháváme.

**Věta 2.1.1** Pro všechna komplexní čísla  $(a_1, a_2)$ ,  $(b_1, b_2)$ ,  $(c_1, c_2)$  platí:

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (b_1, b_2) + (a_1, a_2) \\ (a_1, a_2) + ((b_1, b_2) + (c_1, c_2)) &= ((a_1, a_2) + (b_1, b_2)) + (c_1, c_2) \\ (a_1, a_2) + (0, 0) &= (a_1, a_2) \\ (a_1, a_2) + (-a_1, -a_2) &= (0, 0) \\ (a_1, a_2) \cdot (b_1, b_2) &= (b_1, b_2) \cdot (a_1, a_2) \\ (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2)) &= ((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) \\ (a_1, a_2) \cdot (1, 0) &= (a_1, a_2) \\ \forall (a_1, a_2) \neq (0, 0) \implies (a_1, a_2) \cdot \left(\frac{a_1}{a_1^2 + a_2^2}, \frac{-a_2}{a_1^2 + a_2^2}\right) &= (1, 0) \\ (a_1, a_2) \cdot ((b_1, b_2) + (c_1, c_2)) &= (a_1, a_2) \cdot (b_1, b_2) + (a_1, a_2) \cdot (c_1, c_2)\end{aligned}$$

Toto tvrzení se snadno dokáže rozepsáním a využitím vlastností reálných čísel.

Zavedeme-li bijekci mezi čísla  $(a, 0)$  a  $a$  (kde  $a \in \mathbb{R}$ ), zjistíme, že množina komplexních čísel tvaru  $(a, 0)$  má stejné vlastnosti jako množina všech reálných čísel. Proto můžeme tyto dvě množiny prohlásit za totožné a budeme psát  $(a, 0) = a$ .

**Def.** Komplexní číslo  $(0, 1)$  nazýváme *imaginární jednotkou*, obvykle značíme  $i$ .

**Věta 2.1.2** Každé komplexní číslo  $(a, b)$  lze zapsat jako  $a + bi$ .

*Důkaz:* Vyplývá z jednoduchého rozepsání komplexního čísla:

$$(a, b) = (a, 0) + (0, b) = a \cdot (1, 0) + b \cdot (0, 1) = a + bi$$

Uvědomme si, že  $i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$ . Pak dvě komplexní čísla můžeme násobit jako dvojčleny:

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

Podobně také můžeme dvě komplexní čísla dělit (respektive hledat číslo inverzní k nějakému nenulovému komplexnímu číslu):

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i$$

Tento postup nazýváme *usměrňování* komplexního zlomku.

**Def.** Nechť  $z = a + bi$  je komplexní číslo. Pak reálné číslo  $a$  resp.  $b$  nazýváme *reálnou částí čísla  $z$*  (píšeme  $\Re(z) = a$ ) resp. *imaginární částí čísla  $z$*  (píšeme  $\Im(z) = b$ ).

Platí  $\forall z \in \mathbb{C} : z = \Re(z) + \Im(z) \cdot i$ .

Dále si uvědomme, že každé reálné číslo  $a$ , lze zapsat jako  $a + 0i$ , to znamená, že  $\forall a \in \mathbb{R} : \Re(a) = a \wedge \Im(a) = 0$ .

**Def.** Komplexní číslo, které má nulovou reálnou a nenulovou imaginární část nazýváme *ryze imaginární číslo*. Komplexní číslo, které má nenulovou imaginární část pak pouze *imaginární číslo*.

## 2.2. Absolutní hodnota, goniometrický tvar komplexního čísla

**Def.** Nechť  $z \in \mathbb{C}, z = a + bi$ , pak komplexní číslo  $\bar{z} = a - bi$  nazýváme číslem *komplexně sdruženým* s číslem  $a$ .

Platí  $z = \bar{z} \iff z \in \mathbb{R}$ . Snadno ověříme, protože  $z \in \mathbb{R} \iff \Im(z) = 0$  a  $\Im(z) = -\Im(\bar{z})$ . Pokud tedy má platit  $z = \bar{z}$  pak  $\Im(z) = -\Im(z) \implies \Im(z) = 0$  a naopak.

**Def.** Nechť  $z \in \mathbb{C}, z = a + ib$  pak reálné číslo  $|z| = \sqrt{a^2 + b^2}$  nazýváme *absolutní hodnotou čísla  $z$* .

**Věta 2.2.1** Nechť  $z \in \mathbb{C}$  pak platí:  $|z|^2 = z \cdot \bar{z}$

*Důkaz:* Nechť  $z = a + ib$ , pak  $\bar{z} = a - ib$  a  $z \cdot \bar{z} = (a + ib)(a - ib) = a^2 - (ib)^2 = a^2 + b^2 = |z|^2$ .

**Věta 2.2.2 (goniometrický tvar komplexního čísla)** Pro každé komplexní číslo  $z$  existuje reálné číslo  $\varphi$  takové, že platí:

$$z = |z|(\cos \varphi + i \sin \varphi)$$

*Důkaz:* Nechť  $z = a + bi$ , kde  $a, b \in \mathbb{R}$ . Pak  $|z| = \sqrt{a^2 + b^2}$  a protože platí  $a < |z|$ , pak existuje  $\varphi$  takové, že  $|z| \cdot \cos \varphi = a$ . Navíc pro takové  $\varphi$  platí  $|z| \cdot \sin \varphi = b$ , protože:

$$\begin{aligned} |z|^2 &= a^2 + b^2 \\ |z|^2(\cos^2 \varphi + \sin^2 \varphi) &= a^2 + b^2 \\ (|z| \cos \varphi)^2 + (|z| \sin \varphi)^2 &= a^2 + b^2 \\ (|z| \sin \varphi)^2 &= b^2 \\ |z| \sin \varphi &= b \end{aligned}$$

V důkazu jsme navíc ukázali, jak se takové číslo  $\varphi$  dá najít.

Tomuto číslu říkáme *argument* čísla  $z$  (píšeme  $\arg(z)$ ). Je známo, že takových čísel je víc, protože funkce sinus a kosinus jsou periodické a mají periodu  $2\pi$ , proto pokud nějaké číslo  $\varphi$  splňuje zadání pak i všechna čísla, která dostaneme přičtením nebo odečtením násobku  $2\pi$  jsou také vyhovující. Proto obvykle hledáme  $\varphi$ , které leží v intervalu  $\langle 0, 2\pi \rangle$ . Takové číslo pak nazveme *hlavním argumentem* čísla  $z$  (píšeme  $\text{Arg}(z)$ ).

**Věta 2.2.3 (násobení a dělení čísel v goniometrickém tvaru)** Nechť  $a = |a|(\cos \varphi + i \sin \varphi)$  a  $b = |b|(\cos \psi + i \sin \psi)$  jsou dvě komplexní čísla v goniometrickém tvaru, pak platí:

$$\begin{aligned} ab &= |a||b|(\cos(\varphi + \psi) + i \sin(\varphi + \psi)) \\ \frac{a}{b} &= \frac{|a|}{|b|}(\cos(\varphi - \psi) + i \sin(\varphi - \psi)) \end{aligned}$$

Tuto větu snadno dokážeme pomocí následujícího lemmatu:

**Lemma.**  $\cos(\alpha + \beta) + i \sin(\alpha + \beta) = (\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta)$

*Důkaz:* Podle součtových vzorců platí:

$$\begin{aligned}\cos(\alpha + \beta) &= \cos \alpha \cos \beta - \sin \alpha \sin \beta = \cos \alpha \cos \beta + i^2 \sin \alpha \sin \beta \\ \sin(\alpha + \beta) &= \sin \alpha \cos \beta + \cos \alpha \sin \beta\end{aligned}$$

Jednoduchým rozepsáním pak dostáváme:

$$\begin{aligned}\cos(\alpha + \beta) + i \sin(\alpha + \beta) &= \cos \alpha \cos \beta + i \sin \alpha \cos \beta + i \cos \alpha \sin \beta + i^2 \sin \alpha \sin \beta = \\ &= (\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta)\end{aligned}$$

A nyní se můžeme vrátit k důkazu věty 2.2.3:

$$\begin{aligned}ab &= |a|(\cos \varphi + i \sin \varphi) \cdot |b|(\cos \psi + i \sin \psi) = |a||b|(\cos(\varphi + \psi) + i \sin(\varphi + \psi)) \\ \frac{a}{b} &= \frac{|a|(\cos \varphi + i \sin \varphi)}{|b|(\cos \psi + i \sin \psi)} = \frac{|a|}{|b|} \cdot \frac{(\cos \varphi + i \sin \varphi)(\cos \psi - i \sin \psi)}{(\cos^2 \psi + \sin^2 \psi)} = \\ &= \frac{|a|}{|b|} \cdot (\cos \varphi + i \sin \varphi)(\cos(-\psi) + i \sin(-\psi)) = \frac{|a|}{|b|} \cdot (\cos(\varphi - \psi) + i \sin(\varphi - \psi))\end{aligned}$$

**Věta 2.2.4 (Moivreova věta)** Nechť  $z = |z|(\cos \varphi + i \sin \varphi)$  je goniometrický tvar komplexního čísla  $z$  pak pro každé  $n \in \mathbb{N}$  platí:

$$z^n = |z|^n(\cos n\varphi + i \sin n\varphi)$$

*Důkaz:* Matematickou indukcí:

I.  $n = 1$  Platí triviálně.

II. Předpokládejme, že  $z^n = |z|^n(\cos n\varphi + i \sin n\varphi)$  pak:

$$z^{n+1} = z^n \cdot z = |z|^n(\cos n\varphi + i \sin n\varphi) \cdot |z|(\cos \varphi + i \sin \varphi)$$

Což podle předchozí věty je právě  $|z|^{n+1}(\cos(n\varphi + \varphi) + i \sin(n\varphi + \varphi)) = |z|^{n+1}(\cos(n+1)\varphi + i \sin(n+1)\varphi)$ .

Moivreova věta lze zobecnit i pro libovolnou celou mocninu. Stačí si uvědomit, že pro  $n = 0$  platí  $z^0 = |z|^0 \cdot (\cos 0 + i \sin 0) = 1$  a pro  $n < 0$ :  $z^n = (z^{-1})^{-n}$  a  $z^{-1} = \frac{1}{z}$  je podle věty 2.2.3:  $|z|^{-1} \cdot (\cos(-\varphi) + i \sin(-\varphi))$  a nyní už můžeme použít Moivreovu větu pro přirozené  $-n$ :  $z^n = (z^{-1})^{-n} = (|z|^{-1})^{-n} \cdot (\cos(-n)(-\varphi) + i \sin(-n)(-\varphi)) = |z|^n \cdot (\cos n\varphi + i \sin n\varphi)$ .

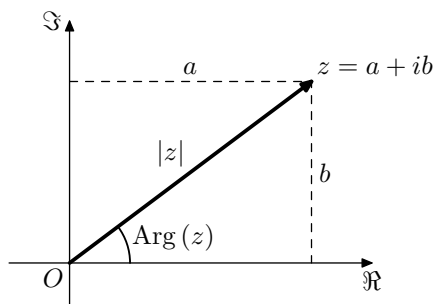
### 2.3. Gaussova rovina

Komplexní čísla jsou uspořádané dvojice čísel reálných, může nám to tedy připomenout souřadnicový systém v rovině. Můžeme tedy zavést bijekci mezi všemi komplexními čísly a všemi body v rovině.

Mějme rovinu s kartézským souřadným systémem. Komplexnímu číslu  $a = a_1 + ia_2$  přiřadíme bod  $A[a_1, a_2]$  roviny a naopak. Tuto rovinu pak nazveme *Gaussovou rovinou*. Osu  $x$  Gaussovy roviny nazveme *reálnou osou* (značíme  $\Re$ ) a osu  $y$  *imaginární* (značíme  $\Im$ ). Podle výše uvedené bijekce budeme komplexní číslo nazývat jak komplexním číslem, tak bodem Gaussovy roviny.

**Def.** Bod  $O = 0 + 0i$  nazveme *počátkem* Gaussovy roviny.

Následující obrázek ukazuje geometrický význam některých vlastností komplexních čísel.



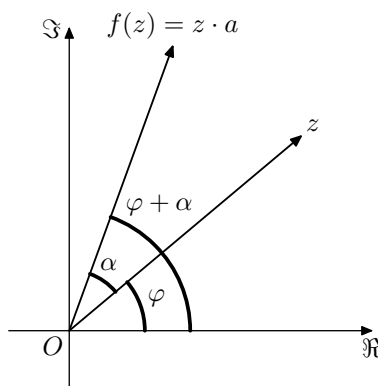
### Otočení kolem počátku

**Def.** Zobrazení  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(z) = z \cdot a$ , kde  $a \in \mathbb{C}$  je takové komplexní číslo, které lze zapsat ve tvaru  $a = \cos \alpha + i \sin \alpha$ , nazveme *otočením* kolem počátku o úhel  $\alpha$ .

Toto otočení je zřejmě shodné s otočením, jak je známe z planimetrie, neboť:

$$z = |z|(\cos \varphi + i \sin \varphi)$$

$$z \cdot a = |z|(\cos \varphi + i \sin \varphi) \cdot (\cos \alpha + i \sin \alpha) = |z|(\cos(\varphi + \alpha) + i \sin(\varphi + \alpha))$$



Otočení o  $\pm \frac{\pi}{2}$  je vlastně násobení číslem  $\pm i$ , o  $\pi$  (neboli středová souměrnost) je násobení číslem  $-1$ .

Obdobně se dají definovat i další zobrazení, která známe z planimetrie.

### 3. Celá komplexní čísla

**Def.** Množinu všech komplexních čísel  $a+ib$  takových, že  $a, b \in \mathbb{Z}$ , nazýváme *množinou všech komplexních celých čísel* nebo také *množinou všech Gaussových celých čísel* (tuto množinu budeme značit  $\mathbb{Z}[i]$ ).

Celá komplexní čísla jsou rozšířením celých čísel, nebo také zúžením komplexních.

#### 3.1. Dělitelnost v celých komplexních číslech

Množina  $\mathbb{Z}[i]$  je uzavřená vůči operacím  $+$ ,  $-$  a  $\cdot$ . Obdobně jak celá čísla však není uzavřená vůči operaci  $/$ , například:

$$\frac{1+i}{2-i} = \frac{(1+i)(2+i)}{(2-i)(2+i)} = \frac{1+3i}{5} = \frac{1}{5} + \frac{3}{5}i \notin \mathbb{Z}[i]$$

Proto má, obdobně jako v celých číslech, smysl definovat dělitelnost.

**Def.** Pro  $a, b \in \mathbb{Z}[i]$  říkáme, že  $a \mid b$  právě tehdy, když existuje  $c \in \mathbb{Z}[i]$  takové, že  $a \cdot c = b$ .

**Věta 3.1.1 (Základní vlastnosti dělitelnosti)** Pro všechna  $a, b, c \in \mathbb{Z}[i]$  platí:

$$a \mid b \wedge b \mid c \implies a \mid c \quad (3.1.1.1)$$

$$a \mid b \wedge a \mid c \implies a \mid b + c \wedge a \mid b - c \quad (3.1.1.2)$$

$$c \neq 0 \implies (a \mid b \iff ac \mid bc) \quad (3.1.1.3)$$

$$a \mid b \wedge b \neq 0 \implies |a| \leq |b| \quad (3.1.1.4)$$

*Důkaz:* Tvzení 1 až 3 se snadno dokáže rozepsáním z definice obdobně jako v celých číslech. Podrobněji se budeme věnovat čtvrtému tvrzení, protože se liší od běžné teorie čísel v celých číslech.

Jestliže  $a \mid b$ , pak existuje  $c$  takové, že  $ac = b$ , tedy podle věty (2.2.3) platí i  $|a| \cdot |c| = |b|$ . A protože  $b \neq 0$  pak i  $c \neq 0$ ,  $|b| \neq 0$  a  $|c| \neq 0$ . Protože  $|c| > 0$  a  $c \in \mathbb{Z}[i]$ , pak  $|c| \geq 1$ . Z toho plyne, že  $|b| \geq |a|$ .

V přirozených číslech je dělitelnost nejjednodušší, protože každé číslo  $n$  (vyjma jedničky) má právě dva nevlastní dělitele (tj. takové, které vždy musí mít) a to jsou 1 a  $n$ . V celých číslech se nám situace komplikuje a číslo  $n$  má čtyři nevlastní dělitele:  $-1$ ,  $1$ ,  $-n$  a  $n$  (samozřejmě kromě čísel 1 a  $-1$ , která mají pouze dva).

V komplexních číslech je situace ještě složitější a nevlastních dělitelů čísla  $n \notin \{1, i, -1, -i\}$  je rovnou osm:  $1, i, -1, -i, n, in, -n$  a  $-in$ .

#### 3.2. Největší společný dělitel a nejmenší společný násobek

**Def.** *Společným dělitelem* komplexních celých čísel  $a$  a  $b$  nazveme takové  $c \in \mathbb{Z}[i]$ , že  $c \mid a \wedge c \mid b$ .

Každá dvě čísla mají společné dělitele čísla  $1, i, -1$  a  $-i$ . Tato čísla mají v množině  $\mathbb{Z}[i]$  stejné postavení, jako číslo 1 v množině  $\mathbb{N}$ , proto je budeme nazývat *jednotkami* a definujeme množinu  $\mathcal{U} = \{1, i, -1, -i\}$  a obecně budeme značit její prvek  $u$ .

Násobení číslem  $u$  neovlivní dělitelnost, protože  $\forall u_1 \in \mathcal{U} \exists u_2 \in \mathcal{U} : u_1 u_2 = 1$ . A navíc  $\forall a \in \mathbb{Z}[i], a \notin \mathcal{U} : a \nmid u \wedge u \mid a$ .

**Def.** Čísla  $a$  a  $b$  nazveme *shodnými* právě tehdy, když  $\exists u \in \mathcal{U} : a = ub$ .

Nechť  $a$  a  $b$  jsou dvě shodná čísla pak zřejmě platí:  $\forall c \in \mathbb{Z}[i] : c \mid a \iff c \mid b$  a  $a \mid c \iff b \mid c$ .

Pokud budeme mluvit o jednoznačnosti vzhledem k dělitelnosti, budeme vždy mluvit o shodnosti takových čísel.

Přímým důsledkem věty 3.1.1.4 je tvrzení:  $\forall a, b \in \mathbb{Z}[i] : a \mid b \wedge b \mid a \iff a$  a  $b$  jsou shodná.

**Def.** *Největším společným dělitelem* komplexních celých čísel  $a$  a  $b$  nazveme takové  $c \in \mathbb{Z}[i]$ , že  $c$  je dělitelné každým společným dělitelem čísel  $a$  a  $b$ . Budeme značit  $c = \mathcal{NSD}(a, b)$ .

**Def.** *Společným násobkem* komplexních celých čísel  $a$  a  $b$  nazveme takové  $c \in \mathbb{Z}[i]$ , že  $a \mid c \wedge b \mid c$ .

Každá dvě čísla  $a, b$  mají společné násobky např. čísla  $ab, iab, -ab, -iab$ . A navíc, pokud je nějaké číslo  $c$  společným násobkem čísel  $a$  a  $b$  pak i libovolný násobek čísla  $c$  je společným násobkem čísel  $a$  a  $b$ .

**Def.** *Nejmenším společným násobkem* komplexních celých čísel  $a$  a  $b$  nazveme takové  $c \in \mathbb{Z}[i]$ , že  $c$  dělí libovolný společný násobek čísel  $a$  a  $b$ . Budeme značit  $c = \mathcal{NSN}(a, b)$ .

Například společným násobkem čísel  $2$  a  $3+i$  je číslo  $4-2i$ , neboť  $4-2i = 2 \cdot (2-i) = (3+i)(1-i)$ . Další společný násobek je číslo  $10 = 2 \cdot 5 = (3+i)(3-i)$ . Všimněte si, že  $4-2i$  dělí  $10$  a jejich podíl je  $2+i$ . Číslo  $4-2i$  je totiž nejmenším společným násobkem čísel  $2$  a  $3+i$ . Protože  $2 \nmid 3+i$  a naopak a nejmenším (podle absolutní hodnoty) dalším možným násobkem čísla  $3+i$  je právě  $4-2i$ , pomocí věty 3.1.1.4 snadno ukážeme, že nejmenší společný násobek je mimo jiné také nejmenší podle absolutní hodnoty.

Jejich společným dělitelem je např. číslo  $1+i$ , protože  $2 = (1+i)(1-i)$  a  $3+i = (1+i)(2-i)$ . A navíc je toto číslo i jejich největším společným dělitelem, protože číslo  $2$  je dělitelné pouze jednotkovými násobky čísel  $1, 1+i$  a  $2$ . A protože  $2 \nmid 3+i$  a  $1 \mid 1+i$ . Obdobně jako u nejmenšího společného násobku i největší společný dělitel je největší podle absolutní hodnoty.

### 3.3. Obdoba Euklidova algoritmu a Bezoutovy věty

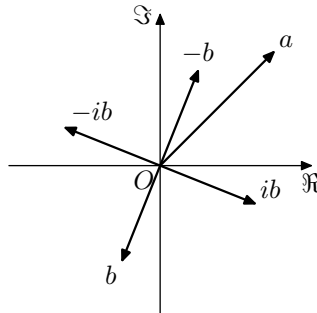
V této kapitole ukážeme, jak se dá najít největší společný dělitel a také jeho jednoznačnost.

#### Euklidův algoritmus

Hledejme  $\mathcal{NSD}(a, b)$ , kde  $a, b \in \mathbb{Z}[i]$ . Bez újmy na obecnosti můžeme předpokládat, že  $|b| \leq |a|$ . Uvažujme čísla  $ub$  pro každé  $u \in \mathcal{U}$ . Představíme-li si tato čísla jako vektory v Gaussově rovině, pak jsou dvojice  $b, ib; ib, -b; -b, -ib$  a  $-ib, b$  dvojicemi na sebe kolmých vektorů a čísla  $b, ib, -b, -ib$  tvoří vrcholy čtverce, který má střed v počátku (viz obrázek).

Vektor  $a$  pak svírá s jedním z těchto čísel úhel  $\alpha \leq \frac{\pi}{4}$  (snadno ukážeme pomocí Dirichletova principu). Uvažují-li trojúhelník, který má jeden vnitřní úhel menší nebo roven  $\frac{\pi}{4}$ , pak strana proti tomuto úhlu je určitě kratší než nejdélší strana tohoto trojúhelníku (např. ze sinové věty, za předpokladu, že funkce sinus je rostoucí na intervalu  $(0, \frac{\pi}{2})$ ).

Proto můžeme říct, že existuje takové  $u \in \mathcal{U}$ , že  $|a - ub| < |a|$ .



Čísla  $b$  a  $a - ub$  mají stejného největšího společného dělitele jako čísla  $a$  a  $b$ , protože:

$$\forall d \in \mathbb{Z}[i], d \mid b : d \mid a \iff d \mid a - ub$$

Zvolíme  $\{a_1, b_1\} = \{b, a - ub\}$  tak, aby znovu platilo  $|b_1| \leq |a_1|$ . A opakujeme postup tak dlouho, dokud jedno z čísel nevychází nula. To se zcela jistě stane, protože absolutní hodnoty  $a_1, b_1$  klesají a mohou

nabývat jen některých diskretních hodnot (druhá mocnina je vždy nezáporné celé číslo). Proto se dříve nebo později dostanu k číslu 0.

Největším společným dělitelem nuly a nenulového čísla  $b_n$  je číslo  $b_n$ , protože nula je dělitelná libovolným  $z \in \mathbb{Z}[i]$ . Takové  $b_n$  pak je i největším společným dělitelem čísel  $a$  a  $b$ .

**Věta 3.3.1 (Bezoutova věta)**  $\forall a, b \in \mathbb{Z}[i] \exists k, l \in \mathbb{Z}[i] : ka + lb = \mathcal{NSD}(a, b)$

*Důkaz:* Vyplývá z Euklidova algoritmu, budeme-li postupovat v opačném pořadí.

Vyjádříme  $\mathcal{NSD}(a, b)$  nejdříve jako  $a_n + ub_n$  a pak za  $a_n$ , respektive  $b_n$ , budeme dosazovat z předchozích vztahů. Budeme-li postupovat dál, z každé rovnice jsme schopni spočítat další (jeden) člen. A po konečném počtu kroků se dostaneme k vyjádření největšího společného dělitele pomocí čísel  $a$  a  $b$ .

Všichni společní dělitelé jsou po dvou shodná čísla. Toto tvrzení můžeme dokázat sporem. Předpokládejme, že existuje taková  $d_1, d_2 \in \mathbb{Z}[i]$ , že  $d_1 \nmid d_2$  nebo  $d_2 \nmid d_1$  a zároveň jsou obě největším společným dělitelem  $a$  a  $b$ . Proto  $d_1$  a  $d_2$  jsou společní dělitelé a navíc největší společní dělitelé čísel  $a, b$ . Musí tedy platit, že  $d_1$  i  $d_2$  se dělí navzájem – spor.

Tímto jsme ukázali jednoznačnost největšího společného dělitele.

**Def.** Čísla  $a, b \in \mathbb{Z}[i]$ , pro která  $\mathcal{NSD}(a, b) \in \mathcal{U}$ , nazýváme *nesoudělná*.

**Věta 3.3.2** Nechť  $a, b, c \in \mathbb{Z}[i] \wedge \mathcal{NSD}(a, b) \in \mathcal{U}$  pak platí:  $a \mid bc \implies a \mid c$ .

*Důkaz:* Podle věty 3.3.1 existují čísla  $k, l \in \mathbb{Z}[i]$  a  $u \in \mathcal{U}$  taková, že  $u \cdot \mathcal{NSD}(a, b) = 1 = ka + lb$ . Vynásobíme-li tuto rovnost číslem  $c$ , dostáváme  $c = kac + lbc$  a protože  $a \mid kac \wedge a \mid lbc$  ( $a \mid bc$ ) tak musí dělit i jejich součet, tedy  $a \mid c$ .

## 4. Gaussova prvočísla

**Def.** Číslo  $z \in \mathbb{Z}[i]$ , které má pouze nevlastní dělitele, nazveme *prvočíslem v komplexních celých číslech* nebo také *Gaussovým prvočíslem*.

Protože se nadále budeme zabývat i běžnými prvočísly, upřesníme ještě trochu názvosloví. budeme-li mluvit o *běžném prvočísle*, máme tím na mysli prvočísla v  $\mathbb{Z}$  (tj. takové kladné číslo, které má právě dva kladné dělitele). V druhém případě prvočísla v  $\mathbb{Z}[i]$  budeme vždy nazývat *Gaussovo prvočísla* nebo jen *prvočísla*. Množinu všech běžných prvočísel budeme značit  $\mathcal{P}$  a množinu všech Gaussových prvočísel  $\mathcal{P}_G$ .

Některá Gaussova prvočísla:  $1 + i, 1 - i, -1 - i, -1 + i, 3, 3i, -3, -3i, 2 + i, 2 - i, \dots$

### 4.1. Vlastnosti Gaussových prvočísel

Pokud  $p \nmid a$ , pak  $\mathcal{NSD}(a, p) \in \mathcal{U}$ , protože kdyby to tak nebylo a  $\mathcal{NSD}(a, p)$  bylo nějaké  $d$  pak platí  $d \mid p$  tj.  $d \in \{1, i, -1, -i, p, -p, ip, -ip\}$ . A protože  $p \nmid a$ , pak  $p \nmid d$  a dostáváme to, co jsme chtěli.

**Věta 4.1.1** Číslo  $p \in \mathbb{Z}[i]$  je Gaussovo prvočísla právě tehdy, když  $\forall a, b \in \mathbb{Z}[i] : p \mid ab \implies p \mid a \vee p \mid b$ .

*Důkaz:* Nejdříve dokážeme implikaci zleva doprava:

Rozebereme dva případy:  $p \mid a$  pak je implikace triviálně splněna. Pokud  $p \nmid a$  pak  $\mathcal{NSD}(p, a) \in \mathcal{U}$  a proto pro  $p, a$  a  $b$  platí věta 3.3.2 tj.  $p \mid b$ .

Nyní budeme předpokládat, že pro nějaké  $p \in \mathbb{Z}[i]$  platí  $\forall a, b \in \mathbb{Z}[i] : p \mid ab \implies p \mid a \vee p \mid b$ . Důkaz povedeme sporem: předpokládejme, že existuje nějaké  $d$  tak, že  $d$  je vlastní dělitel čísla  $p$ . Proto existuje  $c \in \mathbb{Z}[i]$  takové, že  $c \cdot d = p$  a navíc  $c, d \notin \mathcal{U}$ , tak  $p$  nedělí ani  $c$  ani  $d$ , ale  $p$  dělí jejich součin a dostáváme spor.

Tím dostáváme ekvivalentní podmínku prvočíselnosti a také velmi důležitou vlastnost prvočísel.

**Věta 4.1.2 (Věta o rozkladu čísla na prvočísla)** Každé Gaussovo celé číslo různé od jednotky a od nuly lze napsat jako součin Gaussových prvočísel.

*Důkaz:* Větu budeme dokazovat indukcí vzhledem k druhé mocnině absolutní hodnoty. Mějme číslo  $a$  a  $|a|$  nechť je jeho absolutní hodnota.

I.  $|a|^2 = 2$  Tuto podmínku splňují čísla  $1 + i, 1 - i$  a jejich  $u$ -násobky. Tato čísla jsou prvočísla a proto je netřeba rozkládat.

II. Předpokládejme, že všechna čísla s druhou mocninou absolutní hodnoty menší než  $|a|^2$  jdou rozložit na součin prvočísel. Číslo  $a$  buď je prvočíslem, pak je rozklad jasný, nebo není prvočíslem, pak existuje nějaký jeho vlastní dělitel  $d$  a podíl  $c$  tak, aby  $cd = a$ . Navíc  $|c|$  i  $|d|$  je menší než  $|a|$  takže pro ně platí indukční předpoklad, a proto i číslo  $a$  umíme rozložit na součin prvočísel.

**Věta 4.1.3** Existuje nekonečně mnoho Gaussových prvočísel.

*Důkaz:* Sporem. Předpokládejme, že existuje konečně mnoho Gaussových prvočísel. Označme je  $p_1, p_2, \dots, p_k$ , kde  $k \in \mathbb{N}$ . Uvažujme číslo  $a = p_1 p_2 \dots p_k + 1$ . Toto číslo není dělitelné žádným prvočíslem, pokud by tomu bylo jinak, pak  $\exists i \in \{1, 2, \dots, k\} : p_i \mid a \implies p_i \mid a - p_1 p_2 \dots p_k$ , dostáváme  $p_i \mid 1$ , což je spor. Ale podle předchozí věty číslo  $a$  lze rozložit na prvočinitele  $\implies$  spor.

### 4.2. Tvar Gaussových prvočísel

**Věta 4.2.1** Číslo  $z \in \mathbb{Z}[i]$  je Gaussovým prvočíslem právě tehdy, když nabývá jednoho z těchto tvarů:

$$z = \begin{cases} a + ib & a^2 + b^2 \text{ je běžné prvočíslo a } a, b \neq 0 \\ up & u \in \mathcal{U} \text{ a } p \text{ je běžné prvočíslo, které nelze zapsat jako součet dvou kvadrátů} \end{cases}$$

*Důkaz:* Rozdělíme si problém na dva případy: I.  $z = a + ib \wedge a, b \neq 0$  a II.  $z = ua, u \in \mathcal{U}$ .

**I.**  $z = a + bi$ : Uvažme číslo  $z\bar{z} \in \mathbb{Z}$  a jeho rozklad na běžná prvočísla. Pak  $z$  dělí jedno z těchto prvočísel. Nechť  $p$  je toto prvočíslo a  $x = \frac{p}{z}, x = c + id$ . Platí  $p = xz = (ac - bd) + i(ad + bc)$  proto:

$$\begin{aligned} ad + bc &= 0 \\ ad &= -bc \\ \frac{a}{b} &= \frac{c}{-d} \end{aligned}$$

Poslední úpravu si můžeme dovolit, protože  $a, b \neq 0 \wedge p \neq 0$  a proto  $i, d \neq 0$ .

Zlomek  $\frac{a}{b}$  je v základním tvaru, protože kdyby nebyl a existovalo by nějaké celé  $k \mid a \wedge k \mid b$ , ale takové  $k$  dělí i  $z$ , což je spor s prvočíselností čísla  $z$ . Proto platí:  $\exists k \in \mathbb{Z} : c = ka \wedge -d = kb$ .

$$\begin{aligned} zx &= p \\ a \cdot ka - b \cdot (-kb) &= p \\ k(a^2 + b^2) &= p \end{aligned}$$

A protože  $a^2 + b^2 \geq 2$  ( $z \in \mathcal{P}_G$ ) pak  $k = 1$  tj.  $p = |z|^2$ .

Ještě druhou implikaci: Mějme běžné prvočíslo  $p = a^2 + b^2$ . Pak  $p = (a + ib)(a - ib)$ . Uvažujme nějaké Gaussovo prvočíslo  $z \mid a \pm ib$  pak i  $z \mid p$  tj.  $z = a \pm ib$ . Proto čísla  $a \pm ib$  jsou Gaussovská prvočísla.

**II.** Pokud  $z = up$ , pak mohu místo  $z$  uvažovat  $p$ , co se týče dělitelnosti. A protože neexistuje žádné číslo, které má nulovou reálnou nebo imaginární část a dělí číslo  $p$  (z důvodu, že  $p$  je obyčejné prvočíslo), jediné číslo, které by mohlo dělit  $p$  je Gaussovo prvočíslo předchozího tvaru, ale to by  $p$  muselo být součtem dvou kvadrátů – spor. Všechny úvahy se dají i obrátit, a proto je věta dokázána.

**Věta 4.2.2** Každé běžné prvočíslo tvaru  $4k + 1$  lze zapsat jako součet dvou kvadrátů.

*Důkaz:* Podle věty 1.3.4 platí, že každé takové prvočíslo dělí nějaké  $n^2 + 1$ . Uvažujme rozklad čísla  $n^2 + 1 = (n + i)(n - i)$ . Jak  $n + i$  tak  $n - i$  nemůže být dělitelné žádným Gaussovým prvočíslem tvaru  $up$ , kde  $p$  je běžné prvočíslo (které nelze zapsat jako součet dvou druhých mocnin) a  $u \in \mathcal{U}$ , protože pak by bylo dělitelné i prvočíslem  $p$  tedy  $\frac{n \pm i}{p} \in \mathbb{Z}[i]$ :

$$\frac{n \pm i}{p} = \frac{n}{p} \pm \frac{1}{p}i \in \mathbb{Z}[i] \implies \frac{1}{p} \in \mathbb{Z}$$

což je spor.

Čísla  $n \pm i$  jsou tedy dělitelná pouze Gaussovými prvočísly  $z$  takovými, že  $|z|^2$  je běžné prvočíslo. Takže v rozkladu čísla  $n^2 + 1$  na Gaussovy prvočinitele se nachází jen tato prvočísla, navíc ke každému je tam i komplexně sdružené, protože pokud  $z \mid (n \pm i)$  pak  $\bar{z} \mid (n \mp i)$ . Když vynásobíme dvě komplexně sdružená prvočísla, vyjde nám běžné prvočíslo, které lze zapsat jako součet dvou druhých mocnin. Tedy  $n^2 + 1$  je dělitelné pouze prvočísly, které lze zapsat jako součet dvou druhých mocnin. Mějme prvočíslo tvaru  $4k + 1$  ( $k \in \mathbb{Z}$ ), pak dělí  $n^2 + 1$  a lze ho tedy zapsat jako součin dvou druhých mocnin.

**Lemma.** Běžné prvočíslo lze zapsat jako součet dvou kvadrátů právě tehdy když není tvaru  $4k + 3$ .

*Důkaz:* Prvočísla tvaru  $4k$  neexistují. Prvočísla tvaru  $4k + 1$  jdou zapsat jako součet dvou kvadrátů podle věty 4.2.2. Tvaru  $4k + 2$  je pouze dvojka a  $2 = 1^2 + 1^2$ . A číslo tvaru  $4k + 3$  nelze zapsat jako součet dvou kvadrátů, protože kvadratické zbytky modulo 4 jsou 0 a 1. A žádným součtem dvou z těchto čísel nedostaneme 3.

Větu 4.2.1 lze tedy ekvivalentně formulovat takto:

Číslo  $z \in \mathbb{Z}[i]$  je Gaussovým prvočíslem právě tehdy, když je jednoho z těchto tvarů:

$$z = \begin{cases} a + ib & a^2 + b^2 = p, \text{ kde } p \text{ je běžné prvočíсло tvaru } 4k + 1, \text{ nebo } 2 \\ up & u \in \mathcal{U} \text{ a } p \text{ je běžné prvočíсло tvaru } 4k + 3 \end{cases}$$

### 4.3. Využití Gaussových prvočísel

Gaussova prvočísla mají mnohé využití v běžné teorii čísel, pro ukázkou zde uvádíme větu:

**Věta 4.3.1** Celé číslo  $a$ , které lze zapsat jako součin dvou čísel  $b, c$  takových, že je lze zapsat jako součet dvou kvadrátů, lze zapsat jako součet dvou kvadrátů.

*Důkaz:* Nechtě  $b = b_1^2 + b_2^2$  a  $c = c_1^2 + c_2^2$ . Pak platí:

$$\begin{aligned} a = b \cdot c &= (b_1^2 + b_2^2)(c_1^2 + c_2^2) = (b_1 + ib_2)(b_1 - ib_2)(c_1 + ic_2)(c_1 - ic_2) = \\ &= ((b_1 + ib_2)(c_1 + ic_2))((b_1 - ib_2)(c_1 - ic_2)) \end{aligned}$$

Což je součin dvou komplexně sdružených čísel  $z = x + iy$  a  $\bar{z} = x - iy$ :  $a = z\bar{z} = x^2 + y^2$ .

A jeden příklad:

**Příklad:** (Matematická olympiáda 55. roč. A-I-6)

Najděte všechny uspořádané dvojice  $(x, y)$  přirozených čísel, pro něž platí

$$x^2 + y^2 = 2005(x - y).$$

*Řešení:* Nejdříve si zadanou rovnici upravíme a vynásobíme čtyřmi.

$$\begin{aligned} \left(x - \frac{2005}{2}\right)^2 + \left(y + \frac{2005}{2}\right)^2 &= 2 \cdot \frac{2005^2}{4} \\ (2x - 2005)^2 + (2y + 2005)^2 &= 2 \cdot 2005^2 \end{aligned}$$

Rozložíme si číslo  $2 \cdot 2005^2$  na Gaussova prvočísla:

$$2 \cdot 2005^2 = (1 + i)(1 - i)(2 + i)^2(2 - i)^2(20 + i)^2(20 - i)^2$$

Snažíme se vyjádřit číslo  $2 \cdot 2005^2$  jako součet dvou kvadrátů, neboli jako součin dvou komplexně sdružených Gaussových čísel. Aby nějaká dvě čísla byla komplexně sdružená musí se v jejich rozkladu na prvočísla nacházet komplexně sdružená čísla. Proto rozdělíme prvočinitele čísla  $2 \cdot 2005^2$  do komplexně sdružených dvojic a z každé vybereme jedno číslo. Vybraná čísla pak vynásobíme a dostaneme takové číslo  $a + ib$ , že  $a^2 + b^2 = 2 \cdot 2005^2$ . Tzn. nemusíme ani počítat druhý součin, ba co víc, všechna čísla tvaru  $u \cdot (a + ib)$ , kde  $u \in \mathcal{U}$ , nám dají stejné dvojice druhých mocnin. Proto si můžeme počítání velmi urychlit.

Uvědomíme si, že  $1 + i = i \cdot (1 - i)$  takže výběr v dvojici  $1 + i, 1 - i$  nebude mít na výsledek efekt. Dále si můžeme ještě jedno číslo zvolit za konstantní, protože jinak bychom ke všem součinům dostali i komplexně sdružená čísla.

Bude nám stačit spočítat „jen“ šest součinů:

$$\begin{aligned} (1 + i)(2 + i)(2 + i)(20 + i)(20 + i) &= -679 + 2753i \\ (1 + i)(2 + i)(2 - i)(20 + i)(20 + i) &= 1795 + 2195i \\ (1 + i)(2 + i)(2 + i)(20 + i)(20 - i) &= -401 + 2807i \\ (1 + i)(2 + i)(2 - i)(20 + i)(20 - i) &= 2005 + 2005i \\ (1 + i)(2 + i)(2 + i)(20 - i)(20 - i) &= -119 + 2833i \\ (1 + i)(2 + i)(2 - i)(20 - i)(20 - i) &= 2195 + 1795i \end{aligned}$$

Všechny neuspořádané dvojice přirozených čísel  $(a, b)$  takových, že  $a^2 + b^2 = 2 \cdot 2005^2$  jsou tedy:  $(119, 2833)$ ,  $(401, 2807)$ ,  $(679, 2753)$ ,  $(1795, 2195)$ ,  $(2005, 2005)$  Na dvojici  $(2005, 2005)$  můžeme s klidem v duši zapomenout, protože víme, že  $y$  je přirozené tedy  $2005 + 2y \geq 2007$ . Tato nerovnost nám také říká, které číslo z dvojice přiřadíme k  $2005 + 2y$  a které k  $2005 - 2x$ . Dále nesmíme zapomenout, že číslo  $2005 - 2x$  může být i záporné a pak nám zbude jen dopočítat řešení.

Úloha má celkem osm řešení:  $(x, y) \in \{(1062, 414), (943, 414), (105, 95), (1900, 95), (663, 374), (1342, 374), (802, 401), (1203, 401)\}$

## Použitá literatura

- [1] Prof. RNDr. Miloš Ráb, DrSc.: *Komplexní čísla v elementární matematice*, Masarykova univerzita, Brno, 1997; ISBN 80-210-1475-X
- [2] RNDr. Jiří Herman, Ph.D., Doc. RNDr. Radan Kučera, CSc., Doc. RNDr. Jaromír Šimša, CSc.: *Metody řešení matematických úloh I*, Masarykova univerzita, Brno, 2001; ISBN 80-210-1202-1
- [3] Eric W. Weisstein: *Gaussian Prime*, From MathWorld – A Wolfram Web Resource  
<http://mathworld.wolfram.com/GaussianPrime.html>
- [4] Eric W. Weisstein: *Gaussian Integer*, From MathWorld – A Wolfram Web Resource  
<http://mathworld.wolfram.com/GaussianInteger.html>
- [5] Martin Klazar: *Introduction in Number Theory*,  
<http://www.ms.mff.cuni.cz/acad/kam/klazar/utc04.ps>
- [6] 55. ročník Matematické olympiády: *Úlohy domácí části I. kola kategorie A*,  
<http://www.math.muni.cz/~rvmo/mo/55/a55i.pdf>