

## Seriál III. – Komplexní teorie čísel

V posledním soutěžním díle seriálu se budeme zabývat tím, jak lze komplexní čísla využít v teorii čísel. Na začátku si uvedeme malý trik s rozkládáním polynomů v komplexních číslech. V celém zbytku budeme budovat jakousi obdobu dělitelnosti, kterou známe z celých čísel, v číslech komplexních. Speciálně nás budou zajímat obory Gaussových celých čísel a Eisensteinových celých čísel, něco o nich se dočtete dále.

Tento díl je relativně náročný, co se týče znalostí z teorie čísel, některé potřebné věci si vyložíme, některé alespoň připomeneme. Kdybys i přesto měl s něčím problém, můžeš zkusit zapátrat v následujících doporučených zdrojích. Prvním z nich je předloňský seriál o teorii čísel, který najdeš na PraSečích stránkách,<sup>1</sup> druhým je kniha *Metody řešení matematických úloh I*. Znalosti, které z teorie čísel předpokládáme, jsou však docela elementární a jistě s nimi potíže mít nebudeš.

### Užití rozkladů v teorii čísel

V této kapitole si ukážeme, jak lze využít umění rozkládání polynomů pomocí komplexních čísel v některých úlohách z teorie čísel. Není to světoborná metoda a dá se obejít, pokud potřebný rozklad známe. Výhodou však je, že s její pomocí umíme rozklad najít, i když ho neznáme, a tedy je tato metoda univerzálnější.

**Příklad.** Najděte všechna prvočísla tvaru  $n^4 + 4^n$ , kde  $n$  je přirozené číslo.

*Řešení.* Dosadíme-li  $n = 1$ , dostaneme  $1^4 + 4 = 5$ , takže jedno řešení je 5. Když budeme ještě chvíli zkoušet, zjistíme, že už mnoho nových řešení nedostaneme, a tedy bychom chtěli dokázat, že je-li  $n > 1$ , pak  $n^4 + 4^n$  je složené.

Nejprve nahlédneme, že pro sudé  $n$  je číslo  $n^4 + 4^n$  sudé (a různé od 2), buď tedy  $n = 2k + 1$ ,  $k$  celé. Chceme dokázat, že

$$p = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot 2^{4k}$$

je číslo složené. Nejlepší by bylo nalézt přímo rozklad  $x^4 + 4y^4$ . Rozložme si tedy polynom  $x^4 + 4$  v reálných číslech metodou z prvního dílu seriálu:

$$x^4 + 4 = (x - 1 + i)(x - 1 - i)(x + 1 + i)(x + 1 - i) = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Tedy platí

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

V našem speciálním případě dostaneme rozklad

$$p = (n^2 - 2^{k+1}n + 2^{2k+1}) (n^2 + 2^{k+1}n + 2^{2k+1}),$$

přičemž druhá závorka je určité ostře větší než 1, tedy  $p$  může být prvočíslo jediné tehdy, když první závorka je  $\pm 1$ . Platí ale nerovnost

$$n^2 + 2^{2k+1} \geq n^2 + 2^{2k} + 1 \geq 2 \cdot 2^k n + 1, \quad (*)$$

---

<sup>1</sup><http://mks.mff.cuni.cz/archive/28/9.pdf>

(její druhá část je důsledkem AG-nerovnosti  $a^2 + b^2 \geq 2ab$ ), tedy

$$n^2 - 2^{k+1}n + 2^{2k+1} \geq 1.$$

Rovnost nastane, právě když nastane rovnost v obou nerovnostech z  $(\star)$ , tj.  $2^k = 1$  a  $n = 2^k$ , což odpovídá  $k = 0$ ,  $n = 2k + 1 = 1$  a  $p = n^4 + 4^n = 5$ . Jediné prvočíslo tohoto tvaru je tedy 5.

**Příklad.** Dokažte, že součin dvou čísel tvaru  $x^2 + xy + y^2$ , kde  $x, y$  jsou celá čísla, je také tvaru  $x^2 + xy + y^2$ .

*Řešení.* Označme si  $\omega = e^{(2\pi/3)i}$  kořen polynomu  $x^2 + x + 1$ . Platí

$$x^2 + xy + y^2 = (x - \omega y)(x - \bar{\omega}y).$$

Jsou-li tedy  $a = x_1^2 + x_1y_1 + y_1^2$  a  $b = x_2^2 + x_2y_2 + y_2^2$ , pak použitím vztahu  $\omega^2 = -1 - \omega$  odvodíme, že

$$\begin{aligned} ab &= ((x_1 - \omega y_1)(x_2 - \omega y_2))((x_1 - \bar{\omega}y_1)(x_2 - \bar{\omega}y_2)) \\ &= (x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1 - y_1y_2)\omega) \cdot (x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1 - y_1y_2)\bar{\omega}). \end{aligned}$$

Přitom druhý součin jsme ani nemuseli počítat, neboť je komplexně sdružený s prvním. Z posledního řádku už je vidět, že vhodná  $x$  a  $y$  taková, že  $ab = x^2 + xy + y^2$ , jsou právě koeficienty u 1 a u  $\omega$  z prvního součinu, tedy jsou to čísla

$$\begin{aligned} x &= x_1x_2 - y_1y_2, \\ y &= x_1y_2 + x_2y_1 - y_1y_2. \end{aligned}$$

**Cvičení 1.** Najděte všechna prvočísla tvaru  $a^4 + a^2 + 1$ .

**Úloha 2.** Je-li  $n$  přirozené a  $4^n + 2^n + 1$  je prvočíslo, pak je  $n$  mocninou 3. Dokažte.

**Úloha 3.** Dokažte, že  $2^{2^{2011}} + 2^{2^{2010}} + 1$  má alespoň 2011 prvočíselných dělitelů.

Teorie čísel není jenom dělitelnost celých čísel, ale i dělitelnost a rozložitelnost mnohočlenů s celočíselnými koeficienty. Podívejme se tedy na pár souvisejících úloh.

Připomeňme si, že pokud polynom  $f(x)$  dělí polynom  $g(x)$ , znamená to, že existuje polynom  $h(x)$  takový, že  $f(x) = g(x)h(x)$ . Neřekneme-li jinak, předpokládáme, že všechny koeficienty polynomů jsou reálná čísla.

Občas nás budou zajímat i polynomy s celočíselnými koeficienty. Pak budeme při dělitelnosti chtít, aby i polynom  $h(x)$  měl celočíselné koeficienty.

**Příklad.** Buďte  $m, n$  přirozená. Dokažte, že  $x^n - 1$  dělí polynom  $x^m - 1$ , právě když  $n \mid m$ .

*Řešení.* Nejprve si vzpomeneme na několik vlastností mnohočlenů. Ani jeden ze zadaných mnohočlenů nemá vícenásobný kořen, neboť kořeny jsou  $n$ -té (resp.  $m$ -té) odmocniny z jedné, které v Gaussově rovině tvoří vrcholy pravidelného  $n$ -úhelníku (resp.  $m$ -úhelníku) s jedním vrcholem v bodě 1, vepsaného do jednotkové kružnice. Proto platí, že  $x^n - 1 \mid x^m - 1$ , pokud všechny kořeny  $x^n - 1$  jsou zároveň kořeny  $x^m - 1$ .<sup>2</sup>

<sup>2</sup>Platí totiž  $x^n - 1 = (x - k_1)(x - k_2) \cdots (x - k_n)$ , kde  $k_i$  jsou právě kořeny  $x^n - 1$ . Přitom kořenoví činitele jsou navzájem nesoudělní.

Nejdříve dokážeme opačnou implikaci. Označme  $\varepsilon_n = e^{(2\pi/n)i}$   $n$ -tou odmocninou z jedné, která je na jednotkovém kruhu následující po 1 v kladném smyslu. Zřejmě  $\varepsilon_n^n = 1$ , tedy  $\varepsilon_n$  je kořenem polynomu  $x^n - 1$ . Přitom ale  $\varepsilon_n^m = e^{(2\pi m/n)i}$ , a to může být rovno 1, jen pokud je exponent násobkem  $2\pi i$ , tj.  $m/n \in \mathbb{Z}$  a  $n \mid m$ .

Naopak nechť  $m = kn$  a buď  $\alpha$  kořen mnohočlenu  $x^n - 1$ . Pak

$$\alpha^m - 1 = \alpha^{kn} - 1 = (\alpha^n)^k - 1 = 1^k - 1 = 0,$$

a tedy  $\alpha$  je kořenem polynomu  $x^m - 1$ .

Budeš-li s kořeny obou polynomů (které jsou odmocninami z jedné) nakládat trochu opatrněji, určitě snadno vyřešíš následující cvičení. Zkus si jej poté vyřešit i bez komplexních čísel. Poradíme ti, že je výhodné použít Euklidův algoritmus.

**Cvícení 4.** Nalezněte největšího společného dělitele<sup>3</sup> mnohočlenů  $x^m - 1$  a  $x^n - 1$  v závislosti na přirozených číslech  $n$  a  $m$ .

**Cvícení 5.** S využitím poznatků z posledního uvedeného příkladu ukažte, že  $2^n - 1$  dělí  $2^m - 1$ , právě když  $n \mid m$ .

Na závěr si uvedeme jednu úlohu k zamyšlení. Při jejím řešení zkus použít vlastnosti  $n$ -tých odmocnin z jedné a zkus přijít na to, jak tato úloha souvisí s předchozími dvěma úlohami.

**Úloha 6.** Číslo  $\varphi \in \mathbb{C}$  nazveme *primitivní*  $n$ -tou odmocninou z jedné, pokud  $\varphi^n = 1$  a pro žádné přirozené  $d$ ,  $d \mid n$  a  $d \neq n$ , neplatí, že  $\varphi^d = 1$ .

Nechť čísla  $\varphi_1, \varphi_2, \dots, \varphi_k$  jsou všechny primitivní  $n$ -té odmocniny z jedné.<sup>4</sup> Dokažte, že mnohočlen

$$c_n(x) = (x - \varphi_1)(x - \varphi_2) \cdots (x - \varphi_k)$$

má racionální koeficienty.

## Tři klíčové věty z dělitelnosti

V tomto díle seriálu budeme definovat něco, co bychom intuitivně nazvali komplexní celá čísla. Rozumné přístupy jsou dva, Gaussova a Eisensteinova čísla. Než se do nich pustíme, shrneme si klíčové vlastnosti dělitelnosti na celých číslech. Pokud víš, jak se pracuje s dělitelností polynomů, všimni si, že následující tři tvrzení platí nejen pro celá čísla, ale rovněž pro polynomy.

Řekneme, že číslo<sup>5</sup>  $a$  dělí číslo  $b$ , pokud existuje číslo  $c$  takové, že  $ac = b$ . Píšeme  $a \mid b$ . Číslo  $a$  nazýváme *dělitelem* čísla  $b$  a číslo  $b$  *násobkem* čísla  $a$ . Pokud  $a \mid b$  a zároveň  $b \mid a$ , budeme říkat, že čísla  $a$  a  $b$  jsou *asociovaná*, a budeme psát  $a \parallel b$ . Čísla asociovaná s jedničkou nazveme *invertibilní*. Invertibilními čísly jsou právě ta čísla  $a$ , pro něž je  $1/a$  celé, tedy v celých číslech se jedná o  $\pm 1$ .<sup>6</sup>

Důležitou vlastností celých čísel je dělení se zbytkem, formálně to popíšeme v následující větě.

<sup>3</sup>Největším společným dělitelem mnohočlenů  $f(x)$  a  $g(x)$  nazveme takový mnohočlen  $d(x)$ , pro který platí  $d(x) \mid f(x)$  a  $d(x) \mid g(x)$ , a zároveň pro každý jiný polynom  $c(x)$ , který dělí jak  $f(x)$ , tak  $g(x)$ , platí  $c(x) \mid d(x)$ . Jinými slovy,  $d(x)$  je společný dělitel a každý jiný společný dělitel ho dělí – tím zaručíme, že  $d(x)$  je mezi všemi společnými děliteli ten o „největší“.

<sup>4</sup>Jestlipak víš, čemu je rovno  $k$ ? K řešení úlohy to ovšem není potřeba.

<sup>5</sup>Nebo taky mnohočlen, chceš-li.

<sup>6</sup>V polynomech nad reálnými čísly jsou to všechny konstantní nenulové polynomy.

**Věta.** (dělení se zbytkem) Jsou-li  $a, b$  libovolná celá čísla, pak existuje jediné  $r \geq 0$ ,  $|r| < |b|$ , a jediné  $q \in \mathbb{Z}$  takové, že

$$a = qb + r.$$

Číslo  $q$  nazveme celočíselným podílem  $a : b$  a číslo  $r$  zbytkem  $a$  po dělení  $b$ .

Dělení se zbytkem je velmi užitečné, neboť nám zaručuje, že každá dvě čísla mají největšího společného dělitele. Společným dělitelem čísel  $a, b$  nazveme každé  $c$ , pro které platí, že  $c \mid a$  a současně  $c \mid b$  (česky řečeno,  $c$  je společným dělitelem čísel  $a$  a  $b$ ), největším společným dělitelem pak nazveme takového společného dělitele, který je „největší“ ve smyslu dělitelnosti. Tedy  $d$  je největší společný dělitel  $a$  a  $b$ , pokud ho dělí každý společný dělitel  $a$  a  $b$ . Největšího společného dělitele  $a$  a  $b$  budeme značit  $(a, b)$ . Pokud nastane případ  $(a, b) = 1$ , řekneme, že čísla  $a$  a  $b$  jsou nesoudělná.

Všimni si, že tato definice největšího společného dělitele není jednoznačná, neboť je-li  $d = (a, b)$ , pak i  $-d = (a, b)$ . Z toho si ale nebudeme dělat hlavu, protože platí  $d \parallel -d$ , tedy tato čísla mají z pohledu dělitelnosti stejné vlastnosti. Obecně platí, že společný dělitel je určen jednoznačně až na přenásobení invertibilním prvkem. Měli bychom tedy správně psát  $(a, b) \parallel d$  místo  $(a, b) = d$ , ale to dělat nebudeme. Rovností  $(a, b) = d$  budeme mít vždy na mysli asociovanost  $(a, b) \parallel d$ .

Jak vlastně využijeme dělení se zbytkem k výpočtu největšího společného dělitele? Běžně se používá Euklidův algoritmus, jehož výhodou je, že funguje i v obecnějších případech. Chceš-li se o jeho možnostech dozvědět podrobněji, podívej se do prvního dílu předloňského seriálu o teorii čísel.

Uvažme množinu

$$I = \{ka + lb : k, l \in \mathbb{Z}\}.$$

Předně si všimni, že všechna  $i \in I$  jsou násobky libovolného společného dělitele  $c$  ( $c \mid a$  a  $c \mid b$ , tedy  $i \in c \mid ka, lb$  a  $c \mid ka + lb = i$ ). Všimni si také, že tato vlastnost charakterizuje společného dělitele  $a$  a  $b$ , neboť pokud  $c$  dělí každý prvek  $I$ , pak speciálně dělí  $i, a$  i  $b$ .

Nyní si vezmeme nejmenší kladný prvek  $d$  množiny  $I$  a dokážeme, že všechna čísla  $v \in I$  jsou násobky  $d$ . Nechť tedy pro spor  $na + mb \in I$  není násobek  $d$ . Pak  $na + mb$  vydělíme se zbytkem číslem  $d$ :

$$na + mb = qd + r.$$

Protože  $d \nmid n$ , dostáváme, že  $r \neq 0$ . Přitom  $r = na + mb - qd$  a  $d = ka + lb$ , tedy  $r = (n - kq)a + (m - ql)b$ , neboli  $r \in I$ . To je ale spor s volbou  $d$ , protože zřejmě  $r < d$ .

Ukázali jsme tedy, že  $d$  je společným dělitelem  $a$  a  $b$  a současně násobkem libovolného jiného společného dělitele, neboť je to prvek  $I$ , tj.  $(a, b) = d$ .

Jedním pěkným důsledkem tohoto postupu je další důležité tvrzení. Všimni si však, že celé to zatím visí jen na dělení se zbytkem a mohli bychom sem dospět stejně tak Euklidovým algoritmem.

**Věta.** (Bézoutova) Jsou-li  $a, b$  celá čísla, pak existují  $k, l \in \mathbb{Z}$ , že platí

$$ka + lb = (a, b).$$

**Cvičení 7.** Pomocí Bézoutovy věty dokažte, že platí  $(a, bc) \mid (a, b) \cdot (a, c)$ .

**Cvičení 8.** Jsou-li  $b$  a  $c$  nesoudělná, ukažte, že platí dokonce  $(a, bc) = (a, b) \cdot (a, c)$ .

Podíváme se dále, a to na prvočísla. Číslo  $p$  nazveme *prvočíslem*, jestliže není invertibilní<sup>7</sup> a platí, že kdykoliv  $p \mid ab$ , pak  $p \mid a$  nebo  $p \mid b$ .<sup>8</sup> Kdybychom se tě zeptali, co je to prvočíslo, odpověděl bys možná, že je to číslo, které nemá žádné vlastní dělitele, tedy každý dělitel je asociovaný s 1 nebo s  $p$ . Tyto dvě definice jsou v celých číslech ekvivalentní, ale není to úplně zřejmé.

Čísla, která nemají netriviální rozklad na součin, nazveme *ireducibilní*. Tedy  $r$  je ireducibilní, jestliže není invertibilní, a kdykoliv  $r = ab$ , je  $a$  nebo  $b$  invertibilní.

Dokažme nejdříve, že každé prvočíslo je ireducibilní. Kdyby  $p = ab$ , muselo by platit  $p \mid a$  nebo  $p \mid b$ . Bez újmy na obecnosti můžeme předpokládat, že  $p \mid a$ , ale zároveň  $a \mid p$ , neboť  $ab = p$ , tedy  $p \mid a$ . Tedy  $ba = p = ja$ , kde  $j$  je invertibilní, tj.  $j = b$  a  $b$  je invertibilní.

Důkaz opačné implikace je trochu složitější a potřebujeme k němu Bézoutovu větu. Nechť tedy  $r$  je ireducibilní a  $r \mid ab$ . Platí

$$r = (r, ab) \mid (r, a) \cdot (r, b),$$

přičemž  $(r, x)$  může nabývat pouze hodnot 1 a  $r$  (až na přenásobení invertibilním prvkem). Přitom nemůže nastat případ  $(r, a) = (r, b) = 1$ , neboť pak by  $r \mid 1$ . Tedy buď  $(r, a) = r$ , nebo  $(r, b) = r$ , v prvním případě  $r \mid a$ , v druhém  $r \mid b$ .  $\square$

**Věta.** (o jednoznačném rozkladu) *Je-li  $n$  celé číslo, tak existuje jednoznačný rozklad čísla  $n$  na prvočísla (až na pořadí a přenásobení invertibilními prvky).*

*Důkaz.* Pouze naznačíme základní myšlenku, exaktní důkaz je zbytečně technicky náročný. Nejprve budeme chtít dokázat, že se číslo  $n$  rozkládá. Budeme postupovat indukcí podle  $|n|$ . Invertibilní čísla  $\pm 1$  se rozkládají triviálně jako prázdný součin se znaménkem.<sup>9</sup> Buď tedy  $n$  celé a předpokládáme, že tvrzení platí pro všechna čísla s menší absolutní hodnotou.

Mohou nastat dvě možnosti. Buď  $n$  je ireducibilní, pak  $n$  je prvočíslo a  $n = n$  je roklad na prvočinitele, nebo je  $n$  rozložitelné, tedy existují  $a$  a  $b$ , že  $n = ab$ ,  $|a| < n$  a  $|b| < n$ , neboť jde o netriviální rozklad. Pro  $a$  a  $b$  použijeme indukční předpoklad a dostaneme rozklad  $n$  na prvočinitele.

K důkazu jednoznačnosti využijeme poznatku, že prvočísla jsou ireducibilní prvky. Stačí dokázat, že kdykoliv  $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$  pro prvočísla  $p_i$  a  $q_i$ , pak  $k = l$  a při vhodném očíslování  $p_1 \parallel q_1$ ,  $p_2 \parallel q_2$  atd. Platí totiž, že  $p_1 \mid q_1 q_2 \cdots q_l$ , tedy  $p_1$  dělí jedno z čísel  $q_i$ , označme ho  $q_1$ . Přitom  $q_1$  je nerozložitelné, takže  $p_1 \parallel q_1$ . Dále postupujeme analogicky.  $\square$

K čemu se nám hodí jednoznačný roklad na prvočinitele? Například k vyslovení následujícího tvrzení, které nám pomůže řešit některé diofantické rovnice.

**Tvrzení.** (o mocninách) *Je-li  $n$  přirozené a  $a, b$  jsou celá nesoudělná čísla taková, že  $ab = c^n$  pro nějaké celé  $c$ , potom jak  $a$ , tak  $b$  jsou  $n$ -té mocniny (až na přenásobení invertibilním prvkem). Tedy existují  $x$  a  $y$  taková, že  $a = \pm x^n$  a  $b = \pm y^n$ .*

*Důkaz.* Důkaz je docela jednoduchý a my ho zde pouze naznačíme, detaily si rozmysli sám. Klíčovým krokem je rozložit  $a$ ,  $b$  i  $c$  na prvočinitele a porovnat rozklady čísel  $ab$  a  $c^n$ . Pak už

<sup>7</sup>Jedničku za prvočíslo nepovažujeme.

<sup>8</sup>V celých číslech navíc požadujeme, aby byla prvočísla kladná. Dělá se to proto, abychom se zbavili nejednoznačnosti typu  $4 = 2^2 = (-2)^2$ . V jiných oborech by tato podmínka byla příliš složitá, a proto ji raději vypouštíme.

<sup>9</sup>Vnásobíme-li nula čísel, dostaneme jedničku – ze stejného důvodu je  $0! = 1$ .

si stačí jen uvědomit, že tvrzení „ $a$  a  $b$  jsou nesoudělná“ vlastně znamená, že se v prvočíselném rozkladu čísla  $a$  nevyskytuje žádné prvočíсло, které je obsaženo v prvočíselném rozkladu  $b$ , a naopak. V neposlední řadě to, že číslo je  $n$ -tou mocninou, znamená, že všechna prvočísla v jeho rozkladu se vyskytují v mocnině, která je násobkem  $n$ .  $\square$

U tohoto tvrzení si musíme dát velký pozor, abychom nezapomněli na znaménka u  $a$  a  $b$ . Může totiž platit  $ab = 6^2 = 36$ , ale  $a = -4$  a  $b = -9$ , což jsou nesoudělná čísla, ale ani jedno z nich není čtverec.

**Příklad.** Nalezňte všechny dvojice celých čísel  $x, y$ , pro něž platí

$$x = (y + x)(y - x).$$

*Řešení.* Upravme si rovnici do tvaru

$$(x + 1)x = y^2.$$

Čísla  $x + 1$  a  $x$  jsou po sobě jdoucí, a tudíž nesoudělná. Každý jejich společný dělitel musí dělit i jejich rozdíl, který je 1. Musí tedy existovat čísla  $a$  a  $b$  taková, že  $\pm a^2 = x$  a  $\pm b^2 = x + 1$ , obě se stejným znaménkem.

Nejprve se podíváme na případ, kdy jsou  $x$  a  $x + 1$  nezáporná. Platí

$$1 = (x + 1) - x = b^2 - a^2 = (b - a)(b + a).$$

Víme tedy, že  $b - a = b + a = \pm 1$ . Můžeme vyjádřit  $2b = \pm 2$ , tj.  $b = \pm 1$ ,  $a = 0$  a  $x = 0$ . Dosadíme-li do původní rovnice, dostaneme  $y = 0$ .

Jsou-li  $x$  a  $x + 1$  nekladná, pak podobně dostaneme

$$1 = (x + 1) - x = a^2 - b^2 = (a - b)(a + b).$$

Jestliže budeme stejným způsobem postupovat dále, dostaneme řešení  $x + 1 = 0$ , tj.  $x = -1$  a  $y = 0$ .

Úloha má tedy dvě řešení, jimiž jsou dvojice  $(x, y) = (0, 0)$  a  $(-1, 0)$ .

Tento postup funguje, umíme-li rovnici upravit do pěkného tvaru. Co bychom ale dělali například s rovnicí  $x^2 + 1 = y^3$ ? Jediný rozumný tvar, do něhož jsme schopni ji upravit, je  $(x + i)(x - i) = y^3$ . Potom ale potřebujeme nějakou teorii a větu o rozkladu na prvočinitele v komplexních číslech. Na to se podíváme v několika následujících kapitolách. Nejdříve však musíme vybudovat nějakou teorii.

## Něco málo o kvadratických zbytcích

K tomu, abychom si odvodili některé poznatky z teorie čísel v komplexním oboru, se nám bude hodit vědět něco málo o kvadratických zbytcích. Podíváme na celá čísla a na jejich zbytky po dělení prvočíslem  $p$  a položíme si otázku, které zbytky mohou být druhou mocninou nějakého (celého) čísla.

Připomeňme si nejdříve definici kongruence. Říkáme, že čísla  $a$  a  $b$  jsou *kongruentní* modulo  $n$ , jestliže  $n \mid a - b$ , píšeme  $a \equiv b \pmod{n}$ . Znamená to, že čísla  $a$  a  $b$  dávají stejný zbytek modulo  $n$ . Často budeme mluvit jen o zbytcích modulo  $n$ , pod tím si může představit nějakou

množinu reprezentantů zbytků, obvykle množinu  $\{0, 1, \dots, n-1\}$  nebo pro  $n = 2k + 1$  množinu  $\{-k, -k+1, \dots, k\}$ .

Pokud řekneme, že  $x$  je jednoznačné modulo  $n$ , myslíme tím, že existuje číslo  $b$  takové, že  $x$  je vždy kongruentní s  $b$  modulo  $n$ , tedy dvě různé hodnoty  $x$  se liší jen o násobek čísla  $n$ . Například kongruence  $x \equiv 3$  má modulo 5 jednoznačné řešení, přestože má nekonečně mnoho řešení tvaru  $5k + 3$ , kde  $k$  je celé číslo.

Konečně tedy přistupme k definici kvadratického zbytku pro číslo  $n$ . Řekneme, že  $a \in \mathbb{Z}$  je *kvadratický zbytek*, pokud existuje  $b$  takové, že  $b^2$  dává po dělení číslem  $n$  stejný zbytek jako  $a$ , tj.  $n \mid b^2 - a$ . V jazyce kongruencí,  $a$  je kvadratický zbytek modulo  $n$  právě tehdy, když má kongruence  $x^2 \equiv a \pmod{n}$  řešení.

Kvadratické zbytky se hodí při řešení některých diofantických rovnic. Velmi užitečné je znát kvadratické zbytky malých modulů. Například kvadratické zbytky modulo 3 jsou 0 a 1, modulo 4 rovněž 0 a 1, modulo 8 jsou to 0, 1 a 4.

Na ostatní kvadratické zbytky snadno přijdeš, když si vypíšeš všechny zbytky modulo  $n$  a spočítáš jejich druhé mocniny. Ukážeme si to pro modul 4:  $0^2 = 0$ ,  $1^2 = 1$ ,  $2^2 = 4 \equiv 0$  a  $3^2 = 9 \equiv 1 \pmod{4}$ . Skutečně, kvadratické zbytky modulo 4 jsou právě 0 a 1. Toto pozorování využijeme v následující úloze.

**Příklad.** Najděte všechna celá čísla  $x$ ,  $y$  a  $k$ , která řeší rovnici

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

*Řešení.* Podíváme se na rovnici modulo 4. Platí

$$x^2 + y^2 \equiv 3 \pmod{4},$$

ale možné kvadratické zbytky modulo 4 jsou jen 0 a 1. Tedy ať sečteme jakoukoli dvojici čtverců, nemůžeme nikdy dostat zbytek 3. Úloha proto nemá v celých číslech žádné řešení.

**Příklad.** Najděte všechna celá čísla  $x$ ,  $y$  a  $k$ , která řeší rovnici

$$x^2 + xy + y^2 = 3k + 2.$$

*Řešení.* V tomto příkladu použijeme kvadratické zbytky modulo 3. Levou stranu vynásobíme čtyřmi a počítáme modulo 3:

$$4(x^2 + xy + y^2) = (2x + y)^2 + 3y^2 \equiv (2x + y)^2.$$

Protože  $4 \equiv 1 \pmod{3}$ , zbytek pravé strany po dělení třemi se při násobení čtyřmi nezmění. Musí tedy platit kongruence

$$(2x + y)^2 \equiv 2 \pmod{3}.$$

Číslo 2 však není kvadratický zbytek modulo 3, rovnice proto nemá řešení.

Do konce této kapitoly se budeme zabývat už jen kvadratickými zbytky modulo lichá prvočísla, které pro nás budou užitečné. Speciálně se pak zaměříme na zbytky  $-1$  a  $-3$ .

Následující lemma, které budeme dále používat, je spíše technické. Jeho důkaz není příliš zajímavý, uvádíme ho jen pro úplnost.

**Lemma.** Je-li  $p$  prvočíslo a  $f(x)$  polynom stupně  $n$  s celočíselnými koeficienty takový, že  $p$  nedělí alespoň jeden z koeficientů  $f(x)$ , pak existuje nejvýše  $n$  řešení kongruence  $f(x) \equiv 0$  modulo  $p$ .

Tedy existuje nejvýše  $n$  čísel  $0 \leq a_1 < a_2 < \dots < a_k < p$ , že  $f(a_i) \equiv 0 \pmod{p}$  pro všechna  $i = 1, 2, \dots, k$ . Navíc každé  $b$  takové, že  $f(b) \equiv 0 \pmod{p}$ , je kongruentní s jedním z čísel  $a_1, a_2, \dots, a_k$ .

*Důkaz.* V tomto důkazu bude modul u všech kongruencí  $p$ . Tvrzení dokážeme indukcí. Začneme polynomem stupně 0, tedy konstantním polynomem  $f(x) = k$ . Přitom  $p \nmid k$ , tedy kongruence  $k = f(x) \equiv 0$  neplatí a nemá žádné řešení  $x$ .

Nechť je tvrzení splněno pro všechny polynomy stupně nejvýše  $n - 1$ . Buď  $f(x)$  polynom stupně  $n$ , který má alespoň jeden kořen modulo  $n$  (nemá-li žádný kořen, tvrzení zřejmě platí), označme ho  $a_0$  (tj.  $f(a_0) \equiv 0$ ). Z dělení polynomů se zbytkem víme, že existuje polynom  $g(x)$  s celočíselnými koeficienty a existuje celé číslo  $r$ , že

$$f(x) = (x - a_0)g(x) + r.$$

Zbytek  $r$  je navíc roven  $f(a_0)$ , neboť po dosazení  $a_0$  musí nastat rovnost. Dále víme, že  $p \mid f(a_0) = r$ . Pro každé  $a$  tedy platí

$$f(a) \equiv f(a) - r = (a - a_0)g(a) \pmod{p}.$$

Buďte  $a_1, a_2, \dots, a_k$  kořeny  $g(x)$  modulo  $p$  z indukčního předpokladu. Přidáme-li k nim  $a_0$ , dostaneme kořeny  $a_0, a_1, \dots, a_k$  polynomu  $f(x)$  modulo  $p$ . Číslo  $a_0$  můžeme vypustit, pokud se už nachází mezi ostatními čísly. Všechných čísel je dohromady nejvýše  $k + 1$ , což určitě není více než  $n$ , protože  $k \leq n - 1$  podle indukčního předpokladu.

Nyní ukážeme, že kongruence  $f(x) \equiv 0$  nemá žádné další řešení. Je-li  $b$  takové, že  $f(b) \equiv 0$ , pak

$$p \mid f(b) \equiv f(b) - r = (b - a_0)g(b),$$

a protože  $p$  je prvočíslo, víme, že buď  $p \mid b - a_0$ , nebo  $p \mid g(b)$ . Nechť jsou  $a_1, a_2, \dots, a_k$  čísla z indukčního předpokladu pro  $g(x)$ . Pak první možnost říká, že  $b \equiv a_0$ , druhá, že  $b$  je kongruentní s jedním z  $a_1, a_2, \dots, a_k$ .

Dohromady dostáváme, že  $b$  je kongruentní s jedním z čísel  $a_i$  pro  $i = 0, 1, \dots, k$ .  $\square$

V tomto lemmatu je potřeba, aby bylo  $p$  prvočíslo, neboť například pro  $n = 6$  má kongruence  $x(x-1) \equiv 0 \pmod{6}$  řešení 0, 1, 3 a 4. Všimni si, že podobné tvrzení platí pro kořeny mnohočlenů v reálných nebo komplexních číslech.

**Tvrzení.** Je-li  $p > 2$  prvočíslo, pak existuje právě  $(p - 1)/2$  navzájem nekongruentních nenulových kvadratických zbytků modulo  $p$ .

*Důkaz.* Je-li  $a$  kvadratický zbytek, tj.  $a \equiv b^2$ , pak kongruence  $x^2 \equiv a \pmod{p}$  má právě dvě řešení, a to  $b$  a  $-b$ .

Navíc každé  $b^2$  dává nějaký zbytek, tedy kvadratické zbytky jsou právě zbytky

$$1^2 = (-1)^2, 2^2 = (-2)^2, \dots, \left(\frac{p-1}{2}\right)^2 = \left(\frac{p+1}{2}\right)^2,$$

kteří jsou po dvou různé.  $\square$

**Tvrzení.** Je-li  $p = 4k + 1$  kladné prvočíslo, pak  $-1$  je kvadratický zbytek modulo  $p$ .

*Důkaz.* Tvrzení odvodíme z tzv. Wilsonovy věty. Ta říká, že  $(p - 1)! \equiv -1 \pmod{p}$  pro každé prvočíslo  $p$ . Vyjádříme si tedy  $(p - 1)!$  trochu jinak:

$$\begin{aligned} (p - 1)! &= 1 \cdot 2 \cdots (p - 1) \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) \\ &= \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 (-1)^{\frac{p-1}{2}} = a^2, \end{aligned}$$

kde  $a = \left(\frac{p-1}{2}\right)!$ , protože  $(p-1)/2 = 4k/2 = 2k$  je sudé. Tedy  $a^2 \equiv -1$  podle Wilsonovy věty.  $\square$

**Tvrzení.** Je-li  $p = 3k + 1$  kladné prvočíslo, pak  $-3$  je kvadratický zbytek modulo  $p$ .

*Důkaz.* Nejprve ukážeme, že kongruence  $x^2 + x + 1 \equiv 0$  má řešení modulo  $p$ . Pokud  $x^2 + x + 1$  vynásobíme  $x - 1$ , dostaneme kongruenci

$$x^3 \equiv 1 \pmod{p},$$

kteřá má určitě řešení  $x = 1$ . My potřebujeme najít jiné řešení. Z malé Fermatovy věty víme, že  $a^{p-1} \equiv 1 \pmod{p}$  pro každé prvočíslo  $p$  a  $a$  nesoudělné s  $p$ , zde speciálně  $a^{3k} \equiv 1$ , tedy každé  $a^k$ ,  $p \nmid a$ , je řešením naší kongruence.

Co kdyby ovšem  $a^k \equiv 1$  pro každé takové  $a$ ? To podle lemmatu z této kapitoly může nastat pro nejvýše  $k$  hodnot  $a$ . My však máme k dispozici celkem  $3k$  navzájem nekongruentních čísel  $1, 2, \dots, p - 1$ , tedy pro alespoň jedno  $a$  musí platit  $a^k \not\equiv 1$ . Našli jsme tedy řešení  $b = a^k$  kongruence  $x^3 - 1 \equiv 0$ , které není kongruentní s  $1$  modulo  $p$ .

Platí  $p \mid (b - 1)(b^2 + b + 1)$ , přičemž  $b = a^k \not\equiv 1$ , a tedy  $p \mid b^2 + b + 1$ , neboť  $p$  je prvočíslo, a  $b$  je kořenem  $x^2 + x + 1$  modulo  $p$ .

Nyní upravíme kongruenci. Všimneme si, že  $p \neq 2$ , takže násobení čtyřmi je ekvivalentní úpravou.

$$\begin{aligned} x^2 + x + 1 &\equiv 0 \pmod{p} \\ 4x^2 + 4x + 4 &\equiv 0 \\ (2x + 1)^2 &\equiv -3 \end{aligned}$$

Tedy  $(2b + 1)^2 \equiv -3$ , což dokazuje, že  $-3$  je kvadratický zbytek modulo  $p$ .  $\square$

## Gaussova celá čísla

Prvním z oborů, kterými se zde budeme zabývat, jsou Gaussova celá čísla.<sup>10</sup> *Gaussovým celým číslem* rozumíme komplexní číslo tvaru  $a + ib$ , kde  $a, b \in \mathbb{Z}$  jsou celá čísla. Tam, kde nemůže dojít k záměně s Eisensteinovými čísly nebo jinými obory, budeme občas nazývat Gaussova celá čísla zkráceně *celistvá čísla*. Množinu všech Gaussových celých čísel budeme značit  $\mathbb{Z}[i]$ .<sup>11</sup> Gaussova čísla jsou vlastně jakési mřížové body v Gaussově rovině.

<sup>10</sup> angl. Gaussian integers

<sup>11</sup> Toto značení znamená, že k celým číslům přidáme komplexní jednotku  $i$  a všechny součty a součiny. Až budeme mít Eisensteinova celá čísla, budeme je značit  $\mathbb{Z}[\omega]$ . Možná už zvládněš uhodnout, jak budou vypadat.

Na Gaussových číslech definujeme dělitelnost stejně jako na celých číslech. Číslo  $a$  dělí číslo  $b$ , pokud existuje celistvé číslo  $c$ , že  $ac = b$ . Tedy například číslo 2 dělí číslo  $2 + 2i$ , číslo  $1 + i$  dělí 2, neboť  $(1 + i)(1 - i) = 2$ , číslo  $1 + 2i$  dělí  $5 - 5i$ , neboť  $(1 + 2i)(-1 - 3i) = 5 - 5i$ , atd.

Invertibilní prvky, tj. dělitelé jedničky, jsou na Gaussových číslech právě čtyři, a to  $\pm 1 \pm i$ . Takže budeme-li zkoumat dělitelnost, nebude nás zajímat přenásobení některým z těchto prvků, podobně jako nás v celých číslech nezajímalo znaménko.

Všimni si, že některá prvočísla z celých čísel se v Gaussových číslech rozkládají, například  $2 = -i(1 + i)^2$  a  $5 = (1 + 2i)(1 - 2i)$ .

**Cvičení 9.** Rozhodněte, zda pro celé číslo  $a$  platí, že  $1 + i \mid a$  právě tehdy, když  $a$  je sudé. Podle čeho lze poznat, jestli je číslo  $a + ib$  dělitelné  $1 + i$ ?

Nyní se podíváme se na dělení se zbytkem. Zformulujeme tvrzení, které pro nás bude v Gaussových číslech jedním z klíčových, přestože je vlastně jednoduché a naprosto stejné, jako v číslech celých.

Začneme Gaussovou normou, neboli velikostí Gaussova čísla. Definujeme (*Gaussovou*) *normu* Gaussova čísla  $a + ib$  jako

$$N_i(a + ib) = (a + ib)(a - ib) = a^2 + b^2.$$

Nejprve si všimni, že norma je vždy nezáporné celé číslo, přičemž nulová je pouze pro nulu. Srovnáme-li definici s obyčejnou normou komplexních čísel, máme  $N_i(x) = |x|^2$  (druhá mocnina zajišťuje, že bude norma vždy kladná, a tedy přes ni můžeme dokazovat matematickou indukci). Pokud nebude hrozit, že by došlo k záměně, budeme často normu  $x$  značit jen  $N(x)$ .

**Cvičení 10.** Ukažte, že norma součinu je součinem norem, tedy že pro libovolné  $a$  a  $b \in \mathbb{Z}[i]$  platí  $N(ab) = N(a)N(b)$ . Z této rovnosti odvoďte, že pokud  $a \mid b$ , pak  $N(a) \mid N(b)$ .

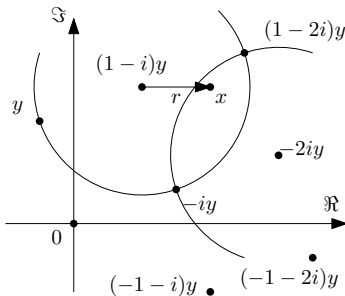
Všimni si, že platí-li  $x \mid y$  a  $y \neq 0$ , pak  $N_i(x) \leq N_i(y)$ , což je obdoba tvrzení v celých číslech, které říká, že  $x \mid y$  implikuje  $|x| \leq |y|$ . Platí-li totiž  $xc = y$ , pak  $N(x)N(c) = N(xc) = N(y)$ , a navíc pokud  $y \neq 0$ , pak  $c \neq 0$  a  $N(c) \geq 1$ . Z definice normy je vidět také to, že pro každé Gaussovo číslo  $a + ib$  platí  $a + ib \mid N(a + ib)$ .

Tedy už tě jistě napadne, jak bude vypadat tvrzení o dělení se zbytkem, ve kterém se vyskytuje velikost čísla.

**Věta.** (dělení se zbytkem) *Jsou-li  $x, y \in \mathbb{Z}[i]$ , pak existují čísla  $q, r \in \mathbb{Z}[i]$ ,  $N(r) < N(y)$ , že*

$$x = qy + r.$$

*Důkaz.* Zkusme si situaci přestavit v Gaussově rovině. Vezmeme všechny násobky čísla  $y$  (tj. všechna čísla tvaru  $(a + ib)y = ay + b(iy)$ , kde  $a, b \in \mathbb{Z}$ ), ty tvoří zvětšenou a otočenou mřížku.



Chceme dokázat, že každé číslo  $x$  má k nějakému mřížovému bodu blíže než  $|y|$ . Pak bude totiž platit  $qy - x = r$ , kde  $qy$  je onen nejbližší mřížový bod a čísla  $q$  a  $r$  jsou právě ta, která hledáme, neboť

$$N(r) = |r|^2 = |qy - x|^2 < |y|^2 = N(y).$$

Zbývá ještě zdůvodnit, proč vnitřky kruhů o poloměru  $|y|$  a středech v mřížových bodech  $ky$  ( $k \in \mathbb{Z}[i]$ ) pokrývají celou Gaussovu rovinu. To je ale jasné z geometrické představy a z toho, že kruhy se středem ve vrcholech čtverce a poloměrem délky jeho strany tento čtverec pokrývají.  $\square$

V přechodím tvrzení jsme nevyslovili jednoznačnost zbytku po dělení, což sice není úplně šťastné, nicméně nám to vlastně vůbec nevadí, protože používáme především existenci. Pokud bychom chtěli jednoznačné zbytky, stačí si vybrat vhodnější reprezentanty, například čísla tvaru  $a + ib$ , kde  $0 \leq a < \Re(y)$  a  $0 \leq b < \Im(y)$ .

Vzpomeňme si na Euklidův algoritmus, ten bude v Gaussových číslech fungovat velmi podobně jako v číslech celých. Je založen na tom, že jsou-li  $a, b$  celistvá, pak  $(a, b) = (a, b - ka)$  pro libovolné  $k$ . Většinou se používá tak, že za  $k$  zvolíme celočíselný podíl  $a$  a  $b$ . Nám ale bude bohatě stačit, když  $N(b - ka) < N(b)$ . Díky tomu budeme mít zaručeno, že normy obou čísel nám postupně klesají. Protože jsou to přirozená čísla, po konečném počtu kroků se dostaneme k nule a získáme  $(a, b) = (d, 0) = d$ .

Ukážeme si tento postup třeba na dvojici čísel  $8 + i$  a  $13$ . Všimni si, že normy se opravdu postupně zmenšují.

$$\begin{aligned} 13 &= (8 + i) + (5 - i) \\ 8 + i &= (5 - i) + (3 + 2i) \\ 5 - i &= (1 - i)(3 + 2i) + 0 \end{aligned}$$

Tedy  $(8 + i, 13) = 3 + 2i$ .

Obráceným postupem umíme najít řešení Bézoutovy rovnice  $xa + yb = (a, b)$ , což už bude probíhat naprosto stejně jako v celých číslech. Například pro předchozí dvojici

$$3 + 2i = (8 + i) - (5 - i) = (8 + i) - (13 - (8 + i)) = 2(8 + i) - 13.$$

**Věta.** (Bézoutova) *Jsou-li  $a, b$  libovolná Gaussova celá čísla, pak existují  $x, y \in \mathbb{Z}[i]$  taková, že platí*

$$ax + by = (a, b).$$

**Cvičení 11.** Najděte největšího společného dělitele a řešení Bézoutovy rovnice pro čísla  $3 + 5i$  a  $4 + 2i$ .

### Gaussova prvočísla

*Gaussovým prvočíslem* nazveme takové celistvé číslo  $p = a + bi$ , že kdykoliv  $p \mid xy$ , pak  $p \mid x$  nebo  $p \mid y$ . Díky Bézoutově větě je toto ekvivalentní s tím, že kdykoliv  $p = xy$ , pak  $x$  nebo  $y$  je invertibilní, což se dokáže naprosto stejně jako v celých číslech. Podívej se do předcházející kapitoly a přesvědč se o tom sám.

Otázkou je, jak vypadají Gaussova prvočísla. Některá prvočísla z celých čísel se totiž v Gaussových číslech rozkládají, např.  $2 = -i(1 + i)^2$  nebo  $5 = (1 + 2i)(1 - 2i)$ .

**Cvičení 12.** Najděte rozklad prvočísla  $17$  v Gaussových číslech.

**Cvičení 13.** Dokažte, že číslo  $3$  se v Gaussových celých číslech nerozkládá, a jde tedy o Gaussovo prvočíslu.

Máme před sebou obtížný úkol charakterizovat Gaussova prvočísla, popsat, která běžná prvočísla se rozkládají a jak, a která naopak zůstávají nerozložitelná. Ještě než se do toho pustíme, podíváme se na jednoznačnost rozkladu. Podobně jako v celých číslech i tady platí věta o jednoznačnosti rozkladu na prvočísla.

**Věta.** (o jednoznačnosti rozkladu na prvočísla) *Každé Gaussovo celé číslo lze jednoznačně (až na pořadí a přenásobení jednotlivých činitelů invertibilním prvkem) rozložit na součin Gaussových prvočísel.*

Důkaz je stejný jako v případě celých čísel, jen indukce se provádí podle Gaussovy normy.

**Cvičení 14.** Proč není rovnost  $5 = (1 + 2i)(1 - 2i) = (2 + i)(2 - i)$  ve sporu s jednoznačným rozkladem na prvočísla?

Zamysleme se nad tím, jak můžou vypadat Gaussova prvočísla. Budou zjevně dvou typů – první z nich jsou obyčejná prvočísla, která se nerozkládají v Gaussových číslech (např. 3, 7 nebo 31), druhá budou prvočísla tvaru  $a + bi$ , kde jak  $a$ , tak  $b$  je nenulové. Podívejme se nyní blíže na prvočísla druhého typu a na jejich normu. Více řekne následující tvrzení:

**Tvrzení.** *Je-li  $p = a + ib$ , kde  $a, b \in \mathbb{Z}$  jsou nenulová a  $p$  je Gaussovo prvočíslu, pak  $N(p)$  je prvočíslu.*

*Důkaz.* Dokážeme tvrzení přímo. Definice říká, že kdykoliv máme  $x, y$  celá čísla taková, že  $N(p) \mid xy$ , pak  $N(p) \mid x$  nebo  $N(p) \mid y$ .

V Gaussových číslech platí

$$p \mid N(p) \mid xy,$$

tedy z toho, že  $p$  je Gaussovo prvočíslu, víme, že  $p \mid x$  nebo  $p \mid y$ . Nechť tedy BÚNO  $p \mid x$ . Protože  $x$  má nulovou imaginární část, platí  $\bar{p} \mid \bar{x} = x$  a číslo  $\bar{p}$  musí být také Gaussovo prvočíslu, neboť má stejné algebraické vlastnosti jako  $p$ .

Často nastane situace, že  $p$  a  $\bar{p}$  jsou nesoudělná. Spočteme-li jejich největší společný dělitel, dostaneme  $(a + ib, a - ib) = (a + ib, 2b)$ .

Rozeberme dva případy. Když  $p$  je nesoudělné s 2, pak  $(a + ib, 2b) = (a + ib, b) = (a, b)$ , což je celé číslo, které dělí  $p$ , s normou ostře menší, než je norma  $p$ . Jediné takové číslo je 1. Vzhledem k tomu, že  $p$  a  $\bar{p}$  jsou nesoudělná a obě dělí  $x$ , platí  $N(p) = p \cdot \bar{p} \mid x$ .

Zbývá dokázat tvrzení pro  $p$  soudělná s 2 =  $-i(1 + i)^2$ . Takové je ale pouze prvočíslu  $p = 1 + i$ , pro které je tvrzení zřejmé, neboť  $N(1 + i) = 2$ .  $\square$

O něco snažší je popsat běžná prvočísla, která se nerozkládají v Gaussových číslech. Mějme nějaké takové kladné prvočíslu  $p$ . Víme, že  $p$  se nerozkládá v  $\mathbb{Z}$ . Předpokládejme, že  $p$  se je dělitelné nějakým Gaussovým prvočíslem  $a + bi$ , které není asociované s  $p$ . Pak ale  $N(a + bi) \mid N(p) = p^2$  a  $N(a + bi)$  je také kladné prvočíslu, tedy jediné  $N(a + bi) = p$ . Řešíme rovnici

$$a^2 + b^2 = p$$

s neznámými  $a, b$  v celých číslech. Podíváme-li se na situaci modulo 4, vidíme, že  $a^2$  i  $b^2$  mohou dávat zbytek 0 nebo 1, tedy možné zbytky pravé strany jsou 0, 1 a 2. Tedy pro prvočísla tvaru  $4k + 3$  nemá rovnice řešení, a tudíž jsou prvočísla tohoto tvaru Gaussovými prvočísly. O těch ostatních zatím rozhodnout neumíme, ale za chvíli dokážeme, že se všechna rozkládají. K tomu se nám bude hodit následující tvrzení.

**Věta.** Je-li  $p$  prvočíslo v celých číslech a existuje-li  $a \in \mathbb{Z}$  takové, že  $p \mid a^2 + 1$ , tedy kongruence  $x^2 + 1 \equiv 0 \pmod{p}$  má řešení  $a$ , pak se prvočíslo  $p$  rozkládá v Gaussově oboru jako

$$p = (p, a + i) \cdot (p, a - i),$$

přičemž  $(p, a + i)$  a  $(p, a - i)$  jsou Gaussova prvočísla.

*Důkaz.* Nejprve ukážeme, že platí rovnost  $p = (p, a + i) \cdot (p, a - i)$ . Tu snadno odvodíme ze vztahu

$$p = (p, a^2 + 1) = (p, (a + i) \cdot (a - i)) \mid (p, a + i)(p, a - i).$$

Čísla  $a + i$  a  $a - i$  se liší právě o  $2i$ , tedy jejich společný dělitel je rozhodně dělitelem dvojky. Díky tomu pro  $p \neq 2$  víme, že dokonce  $(p, a + i)(p, a - i) = (p, (a + i)(a - i)) = p$ .

Pro  $p = 2$  zdůvodníme situaci zvlášť. Řešeními kongruence  $x^2 + 1 \equiv 0 \pmod{2}$  jsou právě lichá čísla  $a$ . Chceme ukázat, že pro lichá  $a$  je  $2 = (2, a + i)(2, a - i)$ .

Platí  $(2, a + i) = (2, a - i)$ . Protože  $a$  je liché, je  $(2, a + i) = (2, 1 + i) = 1 + i$ . Přitom  $(1 + i)^2 = 2i$ , tedy rovnost  $2 = (2, a + i)^2 = (2, a + i)(2, a - i)$  opravdu platí (až na přenásobení invertibilním prvkem).

Dokážeme, že  $(p, a - i)$  je Gaussovo prvočíslo. Nejprve spočítáme  $N((p, a - i))$ . Zřejmě jsou čísla  $(p, a - i)$  a  $(p, a + i)$  komplexně sdružená, neboť  $p$  je celé a  $\overline{a - i} = a + i$ . Tedy

$$N((p, a - i)) = N((p, a + i)) = (p, a - i)(p, a + i) = p.$$

Nechť  $x \mid (p, a - i)$ , tedy  $N(x) \mid N((p, a - i)) = p$ , a norma  $x$  je 1 nebo  $p$ , neboť  $p$  je prvočíslo. V prvním případě je  $x$  invertibilní a v druhém platí  $N(x) = N((p, a - i))$ , tedy vzhledem k tomu, že  $x \mid (p, a - i)$ , víme, že  $x \parallel (p, a - i)$ . Dokázali jsme, že pokud  $x \mid (p, a - i)$  a  $x$  není invertibilní, pak  $x \parallel (p, a - i)$ . Tedy  $(p, a - i)$  je ireducibilní a je to prvočíslo.  $\square$

Všimni si, že přechodí věta nám dává i návod, jak spočítat rozklad nějakého prvočísla (pokud existuje). Například prvočíslo 5 se rozkládá, neboť  $2^2 + 1 \equiv 0 \pmod{5}$ , a jeho rozklad je

$$5 = (5, 2 + i)(5, 2 - i) = (2 + i)(2 - i).$$

Podobně třeba prvočíslo 13 se rozkládá, neboť  $5^2 + 1 \equiv 0 \pmod{13}$ . Jeden z činitelů v rozkladu je pak

$$(13, 5 + i) = (3 - 2i, 5 + i) = 3 - 2i,$$

druhý je s ním komplexně sdružený, tedy  $13 = (3 - 2i)(3 + 2i)$ .

**Cvičení 15.** Najděte rozklady prvočísel 29 a 401 v Gaussových celých číslech.

Zbývá nám poslední krok v charakterizaci Gaussových prvočísel, a sice jak poznat, že kongruence  $x^2 + 1 \equiv 0 \pmod{p}$  má řešení. Totéž pro celá čísla jsme zkoumali v sekci o kvadratických zbytcích.

Kongruence má řešení pro všechna prvočísla tvaru  $4k + 1$ , tedy tato prvočísla se rozkládají v Gaussově oboru. Prvočísla tvaru  $4k + 3$  se nerozkládají, to jsme dokázali samostatně na začátku. Osamoceně stojí prvočíslo 2, které se rozkládá jako  $(1 + i)^2$ .

Uvedeme ještě jednu finální větu, která shrne naše poznatky.

**Věta.** Gaussova prvočísla jsou právě jednoho z tvarů

- (1)  $a + ib$ , kde  $a^2 + b^2 = p$  je 2 nebo prvočíslo tvaru  $4k + 1$ ,
- (2)  $up$ , kde  $u$  je invertibilní a  $p$  je přirozené prvočíslo tvaru  $4k + 3$ .

**Cvičení 16.** Čísla tvaru  $4k + 3$  nikdy nejsou součtem dvou čtverců, to jsme dokázali současně s tím, že prvočísla tvaru  $4k + 3$  se nerozkládají. Může ale existovat číslo tvaru  $4k + 1$ , které nelze zapsat jako součet dvou čtverců?

**Cvičení 17.** Rozložte číslo  $8 - 6i$  na Gaussova prvočísla.

**Úloha.** Najděte všechna přirozená čísla  $x$  a  $y$ , která řeší rovnici

$$x^2 + y^2 = 2009.$$

*Řešení.* Rozklad pravé strany na prvočísla je  $2009 = 7^2 \cdot 41$ , chtěli bychom ji rozložit na Gaussova prvočísla. V případě prvočísla 7 je to snadné, 7 je tvaru  $4k + 3$ , tedy je to Gaussovo prvočíсло. Avšak prvočíсло 41 je tvaru  $4k + 1$ , takže se bude rozkládat.

Platí  $41 \mid 9^2 + 1 = 82$ . Tedy 41 se rozkládá na  $(41, 9 + i) \cdot (41, 9 - i)$ . Spočteme jeden z těchto největších společných dělitelů

$$(41, 9 + i) = (5 - 4i, 9 + i) = (4 + 5i, 9 + i) = (4 + 5i, 5 - 4i) = 4 + 5i$$

Tedy  $41 = (4 + 5i)(4 - 5i)$ .

Upravme konečně rovnici do tvaru

$$(x + iy)(x - iy) = 7^2(4 + 5i)(4 - 5i).$$

Máme-li rozklad součinu  $(x + iy)(x - iy)$  na Gaussova prvočísla, zbývá si uvědomit, že čísla  $x + iy$  a  $x - iy$  jsou komplexně sdružená, což nám velmi omezí možnost volby. Když nezapomeneme na invertibilní prvky, dostaneme pro  $x + iy$  celkem osm možností

$$\pm 7(4 + 5i), \pm 7i(4 + 5i), \pm 7(4 - 5i) \text{ a } \pm 7i(4 - 5i).$$

Úloha má tedy osm řešení, jimiž jsou dvojice

$$(x, y) = (\pm 35, \pm 28) \text{ a } (\pm 28, \pm 35).$$

**Úloha 18.** (MO 56, domácí kolo A) Najděte všechny dvojice  $(x, y)$  přirozených čísel, pro něž platí

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

Při řešení některých úloh pomocí Gaussových celých čísel se nám bude hodit tvrzení o mocninách, jak je uvedeno v kapitole o dělitelnosti v celých číslech. Zopakujme si ho ještě jednou v Gaussových celých číslech, tentokrát již bez důkazu. Důkaz je stejný jako u celých čísel.

**Tvrzení.** (o mocninách) *Buď  $n$  přirozené,  $a, b \in \mathbb{Z}[i]$  nesoudělná a  $c \in \mathbb{Z}[i]$  libovolné a necht' platí  $ab = c^n$ . Pak  $a$  i  $b$  jsou  $n$ -té mocniny až na přenásobení invertibilním prvkem. Tedy existují  $x, y$  a  $k \in \{0, 1, 2, 3\}$ , že  $a = i^k x^n$  a  $b = i^{-k} y^n$ .*

**Úloha.** Nalezněte všechna celá čísla  $x, y$ , která splňují rovnici

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

*Řešení.* Nejdříve si rozložíme levou stranu rovnice:

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

V tuto chvíli bychom chtěli použít tvrzení, bohužel ale nevíme, jestli jsou  $x+i$  a  $x-i$  nesoudělná. Rozhodně však platí  $(x+i, x-i) = (x+i, 2i) \mid 2i = (1+i)^2$ , tedy máme celkem tři možnosti pro největšího společného dělitele.

Je-li  $(x+i, x-i) = 1$ , můžeme použít tvrzení. Než to uděláme, uvědomíme si, že každý invertibilní prvek můžeme napsat jako třetí mocninu ( $i = (-i)^3$ ,  $-1 = (-1)^3$ , atd.), tedy se nemusíme zabývat invertibilními prvky a víme, že

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

pro nějaká celá  $a, b$ . Srovnáním imaginárních částí dostaneme

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

Všichni činitelé jsou celočíselní dělitelé čísla 1, tedy musí být rovni  $\pm 1$ . Speciálně  $b = \pm 1$ . Čísla  $a-b$  a  $a+b$  se liší o 2 a obě jsou  $\pm 1$ , což znamená, že jedno z nich je 1 a druhé  $-1$ , každopádně však  $a = 0$ . Rovnice tak můžeme upravit do tvaru  $-b^3 = 1$ , odkud už je vidět, že  $b = -1$ . Máme tedy  $x+i = (0-1i)^3 = (-i)^3 = i$  a  $x=0$ , z čehož vyplývá, že  $y^3 = 1$  a  $y = 1$ .

Zbývá nám ověřit, jestli může nastat  $(x+i, x-i) > 1$ , tedy  $1+i \mid x+i$  i  $x-i$ . Pak ale  $-i(1+i)^2 = 2 \mid (x+i)(x-i) = y^3$ , tedy dokonce  $8 \mid y^3 = x^2 + 1$ . To ale v celých číslech nastat nemůže, neboť pak by  $x$  muselo být liché a  $x^2$  by po dělení 8 dávalo zbytek 1.

Dohromady máme jediné, triviální řešení  $x = 0$  a  $y = 1$ .

**Úloha 19.** Najděte všechny dvojice celých čísel  $x, y$  takové, že  $x$  je liché a platí

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

**Úloha 20.** S využitím Gaussových čísel najděte všechny pythagorejské trojice celých čísel  $x, y$  a  $z$ . Tedy vyřešte diofantickou rovnici

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

## Eisensteinova celá čísla

Druhý způsob, jak definovat celá čísla v číslech komplexních, nám dávají Eisensteinova čísla. Podobně jako Gaussova čísla byla vlastně mřížovými body ve čtvercové mřížce v Gaussově rovině, Eisensteinova celá čísla jsou mřížové body v trojúhelníkové mřížce. Trojúhelníková mřížka přichází jak se spoustou zajímavých vlastností, které postupně objevíme, tak i s několika zákeřnostmi, o kterých si povíme.

Začněme definicí. Označme si  $\omega$  jednu ze třetích odmocnin z jedné, a to

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Každé číslo tvaru  $a + \omega b$ , kde  $a, b \in \mathbb{Z}$ , nazveme *Eisensteinovým celým číslem*<sup>12</sup>. Množinu všech Eisensteinových čísel označíme  $\mathbb{Z}[\omega]$ .

Nejtěžší věc, na kterou si budeš muset zvyknout, je způsob, jakým se s těmito čísly počítá. Platí totiž  $\omega^2 = -\omega - 1$  (trochu horší vztah, než  $i^2 = -1$ , že?), tedy součin dvou Eisensteinových čísel je

$$(a + b\omega)(c + d\omega) = (ab - bd) + (bc + ad - bd)\omega.$$

---

<sup>12</sup>angl. Eisenstein integer

Velmi často budeme užívat také vztahů  $\omega^3 = 1$  a  $\omega^2 + \omega = -1$ . Ještě se podívejme na komplexní sdružení, které můžeme vyjádřit jako

$$\overline{a + b\omega} = a + b\omega^2 = (a - b) - b\omega.$$

Podobně jako v Gaussových číslech definujeme *Eisensteinovu normu* čísla  $a + b\omega$  jako

$$N_\omega(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

Také zde platí, že  $N_\omega(x) = x \cdot \bar{x} = |x|^2$ , tedy norma je vždy nezáporná, přičemž nulová je pouze pro  $x = 0$ . Ještě připomeneme, že pokud  $x \mid y$  v Eisensteinových číslech, pak  $N_\omega(x) \mid N_\omega(y)$ , zejména je-li  $y \neq 0$ , pak  $N_\omega(x) \leq N_\omega(y)$ .

Tam, kde nebude hrozit, že by došlo k záměně, budeme psát pouze  $N(x)$  místo  $N_\omega(x)$ .

Invertibilních prvků v Eisensteinových celých číslech je ještě více než v Gaussových číslech. Jsou to všechna Eisensteinova čísla s normou 1, tedy k jejich nalezení vyřešíme rovnici

$$a^2 - ab + b^2 = 1.$$

Mohou nastat dvě možnosti. Buď mají  $a$  a  $b$  stejné znaménko, nebo mají opačné znaménko. V prvním případě můžeme navíc předpokládat, že jsou obě nenulová. Rovnici upravíme do tvaru

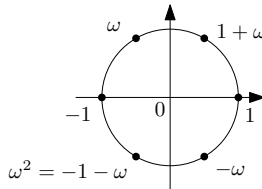
$$(a - b)^2 + ab = 1,$$

odkud vidíme, že všechny členy na levé straně jsou nezáporné a  $ab > 0$ , tedy jediná možnost je  $ab = 1$  a  $a = b$ . Máme tak invertibilní čísla  $1 + \omega$  a  $1 - \omega$ .

V druhém případě si rovnici upravíme do tvaru

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

Přitom  $1 \geq -3ab \geq 0$ , tedy  $-3ab = 0$ , a víme, že jeden z koeficientů musí být nulový. Ze vztahu  $(a + b)^2 = 1$  odvodíme, že druhý koeficient je  $\pm 1$ . Čísla  $\pm 1$  a  $\pm \omega$  jsou tedy také invertibilní. Máme celkem šest invertibilních prvků v  $\mathbb{Z}[\omega]$ , které si můžeme znázornit na jednotkové kružnici. Jsou to právě všechny šesté odmocniny z jedné.



**Věta.** (dělení se zbytkem) *Jsou-li  $x, y$  Eisensteinova celá čísla, pak existují  $q, r \in \mathbb{Z}[\omega]$ ,  $N(r) < N(y)$ , taková, že*

$$x = qy + r.$$

Důkaz pouze naznačíme. Postup je obdobný jako u Gaussových čísel, ale tentokrát tvoří násobky čísla  $y$  trojúhelníkovou mřížku a naším cílem je pokrýt rovnostranný trojúhelník kruhy se středy ve vrcholech a poloměry rovnými délce strany.

Euklidův algoritmus tu vypadá stejně jako v Gaussových číslech, stačí nám zaručit, že normy budou postupně klesat. Spočítáme tedy na ukázkou největšího společného dělitele čísel  $13$  a  $6 + 8\omega$ .

$$\begin{aligned} 13 &= -\omega(6 + 8\omega) + (5 - 2\omega) \\ 6 + 8\omega &= \omega(5 - 2\omega) + (4 + \omega) \\ 5 - 2\omega &= (1 - \omega)(4 + \omega) + 0 \end{aligned}$$

Platí  $(13, 6 + 8\omega) = 4 + \omega$ .

**Cvičení 21.** Najděte největšího společného dělitele  $(7 + 14\omega, 4 - 2\omega)$ .

Konečně zde máme opět větu o dělení se zbytkem a všechny její důsledky, Bézoutovu větu a větu o jednoznačném rozkladu na prvočinitele. Důkazy jsou velmi podobné těm již provedeným, a tedy je už nebudeme opakovat.

**Věta.** (Bézoutova) *Jsou-li  $a, b \in \mathbb{Z}[\omega]$ , pak existují Eisensteinova celá čísla  $x, y$ , že platí*

$$ax + by = (a, b).$$

*Eisensteinovým prvočíslem nazveme Eisensteinovo celé číslo  $p$ , které není invertibilní, a kdykoliv  $p \mid ab$  ( $a, b \in \mathbb{Z}[\omega]$ ), pak  $p \mid a$  nebo  $p \mid b$ . Stejně jako v Gaussově oboru lze ekvivalentně říct, že  $p$  je ireducibilní.*

**Věta.** (o rozkladu na prvočinitele) *Každé Eisensteinovo celé číslo  $a$  se rozkládá jednoznačně (až na pořadí a invertibilní prvky) na součin Eisensteinových prvočísel. Tedy existují Eisensteinova prvočísla  $p_1, p_2, \dots, p_k$ , že  $a = p_1 p_2 \cdots p_k$ , a kdykoliv  $a = q_1 q_2 \cdots q_l$  pro Eisensteinova prvočísla  $q_i$ ,  $0 < i \leq l$ , pak  $l = k$  a při vhodném očíslování  $p_i \parallel q_i$  pro každé  $i$ .*

Dále nás bude zajímat, jak poznat Eisensteinovo prvočíslo. Situace je zde velmi podobná jako v Gaussových číslech. Některá běžná prvočísla se budou rozkládat, některá ne a na výjimečné pozici prvočísla  $2$  bude tentokrát prvočíslo  $3$ , protože v Eisensteinově oboru můžeme odmocnit číslo  $-3$ , vskutku

$$(1 + 2\omega)^2 = 1 + 4\omega + 4\omega^2 = 1 - 4 = -3.$$

Tedy prvočíslo  $3$  se rozloží jako  $3 = -(1 + 2\omega)^2$ . Všimni si, že  $1 + 2\omega$  je Eisensteinovo prvočíslo, neboť žádné neinvertibilní číslo s menší normou ho nedělí (žádné takové ani není).

**Tvrzení.** *Je-li  $p = a + b\omega$  Eisensteinovo prvočíslo, pak buď  $p$  je asociované s nějakým běžným prvočíslem, nebo  $N(p)$  je prvočíslo.*

*Důkaz.* Předpokládejme, že  $p = a + b\omega$  je Eisensteinovo prvočíslo, které není asociované s běžným prvočíslem. Platí, že  $\bar{p} = (a - b) - b\omega$  je také Eisensteinovo prvočíslo, neboť kdykoliv  $\bar{p} \mid xy$ , pak po komplexním sdružení dostaneme, že  $p \mid \bar{x} \cdot \bar{y}$ , tedy  $p \mid \bar{x}$  nebo  $p \mid \bar{y}$ . Dalším komplexním sdružením dostaneme  $\bar{p} \mid x$  nebo  $\bar{p} \mid y$ .

Platí  $N(p) = p \cdot \bar{p}$ . Předpokládejme navíc, že neplatí  $p \parallel \bar{p}$  a dokažme, že  $N(p)$  je prvočíslo. Nechť  $N(p) \mid ab$  pro nějaká celá  $a, b$ . Pak

$$p \mid N(p) \mid ab$$

a  $p$  je Eisensteinovo prvočíslo, tedy  $p \mid a$  nebo  $p \mid b$ . BÚNO  $p \mid a$ . Přitom  $a$  je celé, tedy  $\bar{p} \mid \bar{a} = a$ . Protože  $p$  a  $\bar{p}$  jsou dvě neasociovaná, a tudíž nesoudělná prvočísla, dostáváme nakonec  $N(p) = p \cdot \bar{p} \mid a$ .

Zbývá vyšetřit, co se stane, když  $p \parallel \bar{p}$ , což nastane tehdy a jen tehdy, když  $(p, \bar{p}) = p$ . Počítejme:

$$(a + b\omega, (a - b) - b\omega) = (a + b\omega, -b - 2b\omega) = (a + b\omega, b(1 + 2\omega)).$$

Platí  $(a + b\omega, b) = (a, b) = 1$ , neboť  $(a, b)$  je celé číslo, které dělí  $p$ . Tedy

$$(p, \bar{p}) = (p, 1 + 2\omega).$$

Jediná možnost tedy je, že  $p \parallel 1 + 2\omega$ , a proto  $N(p) = N(1 + 2\omega) = 1 - 2 + 4 = 3$ , což je běžné prvočíslo.  $\square$

**Tvrzení.** *Je-li  $p$  nezáporné prvočíslo tvaru  $3k + 2$ , pak  $p$  je také Eisensteinovo prvočíslo.*

*Důkaz.* Dokážeme, že takové  $p$  je v Eisensteinově oboru ireducibilní. Nechť tedy  $a + b\omega$  je Eisensteinovo prvočíslo, které dělí  $p$  a není asociované s  $p$ . Pak nutně platí, že  $N(a + b\omega) = a^2 - ab + b^2 = p$ , neboť norma je nezáporné prvočíslo v  $\mathbb{Z}$ , které dělí prvočíslo  $p$ .

Ovšem rovnice  $a^2 - ab + b^2 = 3k + 2$  nemá v celých číslech řešení, neboť vynásobíme-li ji čtyřmi a upravíme modulo 3, dostaneme

$$(2a - b)^2 + 3b^2 = 4a^2 - 4ab + 4b^2 \equiv 2 \pmod{3},$$

tedy  $(2a - b)^2 \equiv -1 \pmod{3}$ , ale  $-1$  není kvadratickým zbytkem modulo 3.  $\square$

Už tedy víme, že prvočísla tvaru  $3k + 2$  se nerozkládají. Nyní dokážeme, že prvočísla tvaru  $3k + 1$  se rozkládají, o čemž svědčí například rozklad  $7 = (1 - 2\omega)(3 + 2\omega)$ . To bude trochu obtížnější, zato však velmi podobné důkazu tvrzení, že prvočísla tvaru  $4k + 1$  se rozkládají v Gaussových číslech.

**Věta.** *Je-li  $p$  prvočíslo takové, že kongruence  $x^2 + x + 1 \equiv 0$  má řešení  $a$  modulo  $p$ , pak se  $p$  rozkládá v Eisensteinových číslech jako*

$$p = (p, a - \omega)(p, \overline{a - \omega})$$

a obě čísla  $(p, a - \omega)$  a  $(p, \overline{a - \omega})$  jsou Eisensteinova prvočísla.

*Důkaz.* Důkaz této věty pouze naznačíme. Proveďte se podobně jako důkaz obdobné věty z Gaussových čísel.

Nejdříve ukážeme, že platí rovnost  $p = (p, a - \omega)(p, \overline{a - \omega})$ . Rozebereme dvě možnosti. V první řadě vezmeme prvočísla, která nejsou dělitelná  $1 + 2\omega$ , což jsou všechna prvočísla  $p$  kromě 3. V tomto případě jsou oba činitelé nesoudělní. Pro druhou možnost,  $p = 3$ , se rovnost dokáže přímo. Nakonec zbyde ověřit, že  $(p, a - \omega)$  je prvočíslo s normou  $p$ .

Detaily důkazu si můžeš rozmyslet jako (poněkud obtížné) cvičení.

Například budeme-li chtít rozložit prvočíslo 13, můžeme postupovat tak, že budeme hledat řešení kongruence  $x^2 + x + 1 \equiv 0 \pmod{13}$ . Zkusíme několik malých zbytků. Zbytky 1 ani 2 rozhodně řešením nejsou, ale už  $3^2 + 3 + 1$  dává součet 13, takže 3 řešením je. Víme tedy, že  $13 = (13, 3 - \omega)(13, 4 + \omega)$ . Přitom platí

$$(3 - \omega)(4 + \omega) = 12 - \omega - \omega^2 = 13,$$

tedy musí být  $(13, 3 - \omega) = 3 - \omega$  a máme rozklad  $13 = (3 - \omega)(4 + \omega)$ .

Je užitečné si uvědomit, že k rozkladu prvočísla na Eisensteinova prvočísla nám stačí spočítat jen jednoho činitele, neboť ten druhý bude k němu komplexně sdružený. Opravdu platí  $\overline{3 - \omega} = 4 + \omega$ .

**Cvčení 22.** Rozložte prvočísla 19, 31 a 421 na Eisensteinova prvočísla.

K dokončení charakterizace Eisensteinových prvočísel už nám chybí jen dokázat, že kongruence  $x^2 + x + 1 \equiv 0 \pmod{p}$  má řešení modulo  $p$  pro nezáporné prvočíslu  $p = 3k + 1$ . Z kapitoly o kvadratických zbytcích víme, že pro taková čísla je  $-3$  kvadratický zbytek (připomínáme, že  $-3$  se dá v Eisensteinových číslech odmocnit).

Upravujme tedy zadanou kongruenci, všechny úpravy budou ekvivalentní.

$$\begin{aligned}x^2 + x + 1 &\equiv 0 \pmod{p} \\4x^2 + 4x + 4 &\equiv 0 \pmod{p} \\(2x + 1)^2 &\equiv -3 \pmod{p}\end{aligned}$$

Je-li  $b^2 \equiv -3$ , řešíme rovnici  $2x + 1 \equiv b \pmod{p}$ . Upravíme ji přenásobením  $(p + 1)/2$ :

$$\begin{aligned}x + \frac{p+1}{2} &\equiv \frac{p+1}{2}b \pmod{p} \\x &\equiv \frac{p+1}{2}(b-1)\end{aligned}$$

Našli jsme tedy řešení  $x$ , čímž jsme dokázali, že prvočísla tvaru  $3k + 1$  se rozkládají na součin dvou Eisensteinových prvočísel. Konečně můžeme zformulovat závěrečnou větu.

**Věta.** Eisensteinova prvočísla jsou právě jednoho z tvarů

- (1)  $a + \omega b$ , kde  $a^2 - ab + b^2 = p$  je 3 nebo prvočíslu tvaru  $3k + 1$ ,
- (2)  $up$ , kde  $u$  je invertibilní a  $p$  je kladné prvočíslu tvaru  $3k + 2$ .

**Cvčení 23.** Rozložte Eisensteinovo číslo  $9 - 15\omega$  na Eisensteinova prvočísla.

**Úloha.** Najděte všechny dvojice celých čísel  $x, y$  splňujících rovnici

$$(x + y)^2 = xy + 2011.$$

*Řešení.* Upravíme si rovnici do tvaru

$$x^2 + xy + y^2 = 2011$$

a rozložíme

$$(x - \omega y)(x + (1 + \omega)y) = 2011.$$

Zbývá rozložit pravou stranu na Eisensteinova prvočísla. Číslo 2011 je prvočíslu a po dělení třemi dává zbytek 1, tedy se rozkládá na součin dvou Eisensteinových prvočísel. Nyní potřebujeme nalézt aspoň jedno řešení kongruence

$$x^2 + x + 1 \equiv 0 \pmod{2011}.$$

K tomu můžeme použít třeba počítač. Zjistíme, že nejmenší celočíselné řešení je 205, a tedy platí, že prvočíslu v rozkladu 2011 je

$$(2011, 205 - \omega) = (-39 + 10\omega, 205 - \omega).$$

Přitom  $N(-39 + 10\omega) = 39^2 + 39 \cdot 10 + 10^2 = 2011$ . Tedy rozklad 2011 je

$$2011 = (-39 + 10\omega)(-49 - 10\omega).$$

Může nastat celkem 12 možností, prvních šest je  $x - \omega y = \varepsilon(-39 + 10\omega)$ , dalších šest pak  $x - \omega y = \varepsilon(-49 - 10\omega)$ , kde  $\varepsilon$  je jeden ze šesti invertibilních prvků. UVědomíme-li si, že můžeme prohodit  $x$  a  $y$  a u obou čísel změnit znaménko, stačí nám vlastně spočítat jen tři možnosti:

$$\begin{aligned}x - y\omega &= -39 + 10\omega, \\x - y\omega &= (1 + \omega)(-39 + 10\omega) = -49 - 39\omega, \\x - y\omega &= \omega(-39 + 10\omega) = -10 - 49\omega,\end{aligned}$$

Úloha má celkem dvanáct řešení. Zapišeme-li je jako neuspořádané dvojice, budou to  $\{x, y\} = \{39, 10\}$ ,  $\{-39, -10\}$ ,  $\{49, -39\}$ ,  $\{-49, 39\}$ ,  $\{49, -10\}$  a  $\{-49, 10\}$ .

**Úloha.** Dokažte, že je-li  $p = 3k + 1$  prvočíslo, pak existuje jednoznačný zápis  $p = a^2 + 3b^2$ , kde  $a$  a  $b$  jsou nezáporná celá čísla.

*Řešení.* Víme, že prvočíslo  $p = 3k + 1$  se rozkládá v Eisensteinově oboru na součin dvou prvočísel, tj.

$$p = (x - \omega y)(x + y + \omega y).$$

Stejně tak se rozkládá i výraz

$$a^2 + 3b^2 = (a - (1 + 2\omega)b)(a + (1 + 2\omega)b) = (a - b - 2b\omega)(a + b + 2b\omega).$$

Je-li  $y$  kladné a sudé, z předchozího vztahu dostáváme  $y = 2b$ ,  $a - b = x$  a  $a + b = x + y$ . Vyřešíme soustavu tří rovnic o dvou neznámých  $a$  a  $b$ , řešením je  $b = y/2$  a  $a = x + y/2$ , pokud  $x > -y/2$ , jinak  $a = -x - y/2$ .

Pro ostatní případy musíme najít lepší rozklad prvočísla  $p$ . Víme ovšem, že rozklad je jednoznačný až na asociovanost činitelů, tedy můžeme pouze přenásobovat závorky jedním z šesti invertibilních prvků v  $\mathbb{Z}[\omega]$ . Všimni si, že všechny invertibilní prvky jsou mocninami  $1 + \omega$ , např.  $\omega = (1 + \omega)^2$ . Podívejme se tedy, co se stane s činitelem  $x - y\omega$  po přenásobení  $(1 + \omega)$ :

$$(x - y\omega)(1 + \omega) = (x + y) + x\omega \tag{**}$$

Pokud je  $x$  kladné a sudé, máme také řešení. Stačí položit  $b = x/2$  a  $a$  dopočítat jako v předchozím případě.

Zbývá nejnepříjemnější situace, kdy jsou obě čísla  $x$  a  $y$  lichá. Pak se ale ještě jednou podívejme na vzoreček (\*\*). Číslo  $x + y$  je sudé, zvolíme tedy  $x' = x + y$  a  $y' = x$ , čímž převedeme situaci na již rozebraný případ. Přenásobením  $1 + \omega$  pak dostaneme opět koeficient u  $\omega$  sudý.

Jediný problém bychom mohli mít se znaménky, ten se ale snadno vyřeší přenásobíme  $x - y\omega$  číslem  $-1$ .

Zatím jsme dokázali, že úloha má alespoň jedno řešení, které ovšem ještě zdaleka nemusí být jednoznačné. Dokažme tedy jednoznačnost. Buďte  $a$  a  $b$  kladná čísla taková, aby platilo  $a^2 + 3b^2 = p$ . Opět zvolme rozklad  $p = (x - y\omega)(x + y + y\omega)$ . Vzhledem k jednoznačnosti rozkladu musí platit jedna z dvanácti rovností

$$\begin{aligned}(a + b + 2\omega b) &= (x - y\omega)(1 + \omega)^k, \\(a + b + 2\omega b) &= (x + y + y\omega)(1 + \omega)^k,\end{aligned}$$

kde  $k = 0, 1, \dots, 5$ . Ukážeme, že nejvýše jedna z těchto rovností může být splněna. Připomeňme, že obě čísla  $a$  i  $b$  jsou kladná (ani jedno nemůže být nulové, neboť pak by  $p$  nebylo prvočíslo). Napišme si tedy pravé strany těchto rovností:

$$\begin{aligned} & \pm(x - y\omega), \pm((x + y) + x\omega), \pm(y + (x + y)\omega), \\ & \pm((x + y) + y\omega), \pm(x + (x + y)\omega), \pm(-y + x\omega). \end{aligned}$$

Dokažme, že právě jedno z čísel  $x$ ,  $y$  a  $x + y$  je sudé. Rozhodně nemohou být sudá obě čísla  $x$  a  $y$ , protože pak by  $p = x^2 + xy + y^2$  bylo sudé prvočíslo tvaru  $3k + 1$ , a takové neexistuje. Zbývá tedy ukázat, že je-li jedno z čísel  $x$  a  $y$  sudé a druhé liché, pak  $x + y$  je liché, a že jsou-li obě čísla  $x$  a  $y$  lichá, pak  $x + y$  je sudé, což je zřejmé.

Zbydou nám pouze čtyři pravé strany, a to ty, které mají u  $\omega$  sudý koeficient. Například je-li  $y$  sudé, pak možné pravé strany jsou

$$(x - y\omega), (-x + y\omega), ((x + y) + y\omega) \text{ a } (-(x + y) - y\omega).$$

Navíc víme, že  $b$  musí být kladné, což nám vyloučí ještě další dvě závorky se záporným koeficientem. Je-li například  $y$  záporné a sudé, zbydou závorky

$$(x - y\omega) \text{ a } (-(x + y) - y\omega).$$

Dopočítejme  $a$ , pokud nastane rovnost v prvním či druhém případě:

$$a = \begin{cases} x + y/2, & \text{když } (a + b + 2b\omega) = (x - y\omega), \\ -(x + y) + y/2 = -x - y/2, & \text{když } (a + b + 2b\omega) = ((x + y) - y\omega). \end{cases}$$

všimni si, že tyto dvě hodnoty mají stejnou velikost a opačné znaménko, tedy jen jedna z nich může být kladná. Stejná situace nastane i u všech (šesti) ostatních případů, a to proto, že  $a^2 + 3b^2 = (-a)^2 + 3b^2$ . veškeré podmínky, které jsme zatím použili jsme použili kvůli  $b$ , takže nutně i výraz

$$(-a + b) + 2\omega b$$

musí nabývat jedné ze dvou zatím nevyloučených hodnot. Rozhodně platí  $(a + b) + 2\omega \neq (-a + b) + 2\omega$ , tedy jsme vyloučili poslední závorku a zbyla nám už jen jediná, což jsme chtěli dokázat.

**Úloha 24.** Najděte všechny trojice celých čísel  $(x, y, z)$  splňujících

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

## ... a další imaginární teorie

V poslední krátké kapitole si ukážeme, jak lze v teorii čísel využít kvaterniony. Kvaterniony jsou taková „komplexní čísla na druhou“, mají tři imaginární jednotky a velmi nepříjemnou vlastnost, že *nejsou komutativní*, tj. neplatí  $ab = ba$  pro každé  $a$  a  $b$ .

Nejprve si definujeme imaginární jednotky v kvaternionech. Buďte  $i$ ,  $j$  a  $k$  formální symboly pro imaginární jednotky. Definujeme operaci  $\cdot$  na množině  $\{\pm 1, \pm i, \pm j, \pm k\}$  tak, aby splňovala

$$i^2 = j^2 = k^2 = ijk = -1,$$

přičemž 1 a  $-1$  se chovají obvykle, tedy  $1 \cdot a = a$  pro každé  $a$  a  $(-1)^2 = 1$ ,  $-1 \cdot i = i \cdot -1 = -i$ ,  $-1 \cdot j = -j$ , atd. Z těchto vztahů si můžeš odvodit všechny součiny.

Pro jistotu uvádíme tabulku pro násobení, tedy vlastně jen její část, neboť zbytek se odvodí snadno. Pokud násobíme dvě čísla s různými znaménky, musíme v tabulce znaménko změnit, pokud se stejnými, necháváme stejné znaménko součinu.

$\cdot$	1	$i$	$j$	$k$
1	1	$i$	$j$	$k$
$i$	$i$	$-1$	$k$	$-j$
$j$	$j$	$-k$	$-1$	$i$
$k$	$k$	$j$	$-i$	$-1$

Všimni si, že pro imaginární jednotky platí  $ij = -ji$ ,  $ik = -ki$  a  $jk = -kj$ .

**Cvičení 25.** Spočítejte  $jik$ .

Nyní umíme násobit komplexní jednotky. To už je prakticky všechno, co potřebujeme k tomu, abychom mohli definovat kvaterniony.

*Kvaternionem* rozumíme čtyřčlen  $a_1 + a_2i + a_3j + a_4k$ . Sčítání kvaternionů definujeme jako

$$(a_1 + a_2i + a_3j + a_4k) + (b_1 + b_2i + b_3j + b_4k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

a násobení kvaternionů jako násobení polynomů s proměnnými  $i, j$  a  $k$  za použití tabulky uvedené výše, tj.

$$\begin{aligned} (a_1 + a_2i + a_3j + a_4k) \cdot (b_1 + b_2i + b_3j + b_4k) &= \\ &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_4b_3 - a_3b_4)i + \\ &+ (a_1b_3 + a_3b_1 + a_4b_2 - a_2b_4)j + (a_1b_4 + a_4b_1 + a_2b_3 - a_3b_2)k. \end{aligned}$$

Množina všech kvaternionů se obvykle značí  $\mathbb{H}$ .<sup>13</sup>

K čemu se taková věc hodí? Podobně jako jsme definovali Gaussova celá čísla, můžeme definovat kvaterniony s celočíselnými koeficienty – *Lipshitzova celá čísla* jsou kvaterniony tvaru  $a + bi + cj + dk$ , kde  $a, b, c, d$  jsou celá čísla. Množinu všech takových čísel budeme značit  $\mathbb{Z}[i, j, k]$ .

Definujeme si i jejich normu jako

$$N_L(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2.$$

Všimni si, že i pro tuto normu je  $N(xy) = N(x)N(y)$  pro každé  $x, y \in \mathbb{Z}[i, j, k]$ , což se snadno odvodí ze vztahu

$$N(a + bi + cj + dk) = N(a - bi - cj - dk) = (a + bi + cj + dk)(a - bi - cj - dk).$$

Už jen z této úvahy umíme dokázat následující lemmátka.

**Lemma.** Jsou-li  $a$  a  $b$  celá čísla, která lze napsat jako součet čtyř čtverců celých čísel, pak i číslo  $ab$  lze napsat jako součet čtyř čtverců celých čísel.

<sup>13</sup>Objevil je a poprvé popsal irský matematik William Rowan Hamilton.

*Důkaz.* Stačí si uvědomit, že číslo  $a$  lze zapsat jako součet čtverců čísel  $a_1, a_2, a_3$  a  $a_4$ , právě když je normou Lipschitzova celého čísla  $q_a = a_1 + a_2i + a_3j + a_4k$ . Podobně označme  $q_b$  Lipschitzovo celé číslo, že  $N(q_b) = b$ . Pak zřejmě  $N(q_a q_b) = ab$ , a tedy celá čísla, která hledáme, jsou právě koeficienty Lipschitzova čísla  $q_a q_b$ .  $\square$

Toto lemmátka je užitečné například pro důkaz slavné Lagrangeovy věty o čtyřech čtvercích, díky němu se totiž můžeme omezit jen prvočísla  $x$ .

**Věta.** (Lagrangeova věta o čtyřech čtvercích) *Je-li  $x$  libovolné přirozené číslo, pak existují celá čísla  $a, b, c$  a  $d$  taková, že*

$$x = a^2 + b^2 + c^2 + d^2.$$

Důkaz je složitý a vynecháme ho.

Všimni si však, že o prvočíslech tvaru  $4k + 1$  umíme na základě teorie o Gaussových číslech dokázat, že jsou součtem dokonce dvou čtverců, a o prvočíslech tvaru  $3k + 1$  umíme z teorie o Eisensteinových číslech dokázat, že jsou tvaru  $a^2 + 3b^2$ , a tedy jsou součtem čtyř čtverců (z nichž tři jsou stejné). Lagrangeovu větu tedy neumíme dokázat pouze pro prvočísla tvaru  $12k + 11$ .

Například platí

$$2 = 1^2 + 1^2 + 0^2 + 0^2, \quad 5 = 1^2 + 2^2 \quad \text{a} \quad 7 = 2^2 + 3 \cdot 1^2.$$

**Cvičení 26.** Dokažte, že čísla tvaru  $4^{m-1}(8k + 7)$  pro  $k$  a  $m$  přirozená nelze napsat jako součet pouze tří čtverců celých čísel (tedy že čtyři je opravdu nejmenší možný počet čtverců, který potřebujeme).

## Problémové úlohy

V poslední kapitole ti přinášíme problémové (těžké) úlohy k zamyslení. Jsou to úlohy, ke kterým se může hodit znát něco z teorie, kterou jsme vyložili v tomto díle seriálu, avšak někdy ani to nebude stačit (jako v případě předposlední a poslední úlohy) a budeš se muset zamyslet nad vlastní teorií nebo vymyslet jiný trikový způsob.

**Úloha 27.** Dokažte, že následující dvě rovnice nemají žádné netriviální celočíselné řešení  $(x, y, z)$ . Netriviálním řešením se myslí takové trojice, že všechna tři čísla jsou nenulová.

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

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

**Úloha 28.** Je-li  $p$  prvočíslo, řešte rovnici

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

v celých číslech.

**Úloha 29.** Najděte všechna celá čísla  $x, y$  splňující

$$y^6 = x^5 + 1.$$

**Úloha 30.** Řešte v celých číslech rovnici

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

**Úloha 31.** Najděte všechny dvojice celých čísel  $(x, y)$ , která splňují

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

**Úloha 32.** Najděte všechny dvojice  $(x, y)$  celých čísel splňujících

$$x^2 + 3 = y^5.$$

**Úloha 33.** Řešte v celých číslech

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

**Úloha 34.** Dokažte, že neexistují taková celá čísla  $x$  a  $y$ , že

$$x^2 + 5 = y^3.$$