# Teorie nejen čísel 1 – Součiny

Milý příteli,
vítáme Tě na začátku letošního seriálu, v němž se naučíme vařit teorii čísel z roztodivných a mnohdy exotických ingrediencí. Jako předkrm vhodíme do hrnce celá čísla a ukážeme si, jak z nich ukuchtit něco jednoduchého na zasycení. Po zbytek našich kuchařských lekcí však již uvidíme, co lze získat, když do hrnce přidáme trochu koření a necháme vše bublat nebo když si pokrm rozkrájíme na menší sousta.

Seriál pro Tebe letos píší Fíla Čermák a Matěj Doležálek. Vyvstanou-li Ti při čtení na mysli jakékoliv otázky či nejasnosti, neváhej se na nás obrátit, například nám můžeš napsat mail na adresy *filip.cermak2@gmail.com* a *matej@prase.cz*.

## O co půjde?

Pod honosným názvem *teorie čísel*[1] se skrývá ta oblast matematiky, jež zkoumá hlavně přirozená, celá anebo racionální čísla. Pracuje tedy například s dělitelností, s prvočísly nebo s diofantickými[2] rovnicemi. Tak říkáme rovnicím, v jejichž řešení navíc požadujeme, aby neznámé nabývaly jen celočíselných (někdy dokonce jen přirozených) hodnot.

V tomto seriálu se podíváme na to, jak vést podobné úvahy o dělitelnosti, o speciálních vlastnostech některých „čísel“ a diofantických rovnicích i s jinými objekty než s celými čísly. Typicky tak kupříkladu k celým číslům přidáme nějaký další exotičtější objekt a uvidíme, co nám vznikne a jaké to bude mít vlastnosti. Jindy se naopak rozhodneme něco zapomenout, aby nám zbylo jenom to důležité.

## Proč se vůbec o něco takového zajímat

Důvodů, proč se snažit používat nějakou „teorii čísel“ i na jiné struktury než celá čísla, je hned několik. Jednak je to přirozená matematická snaha zobecňovat to, co již známe – tím si můžeme lépe rozmyslet, které vlastnosti jsou na celých čísel výjimečné a které naprosto tuctové. Dále nám ale počítání s novými objekty a strukturami může přinést i nějaká nová pozorování o celých číslech, která bychom jinak získávali jen obtížně.

Nejčastěji nám přidání nových objektů pomůže s rozkládáním výrazů na součin. V celých číslech dovedeme snadno rozložit výrazy jako třeba $a^2 - b^2 = (a - b)(a + b)$, $a^2 + 2ab + b^2 = (a + b)^2$ nebo $ab - a - b + 1 = (a - 1)(b - 1)$. Díky tomu pak mnohé rovnice, které řešíme v celých číslech, dovedeme rozlousknout vhodnou úpravou na součin.

[1] Zastarale též *aritmetika*. S tímto označením se ještě lze setkat v některých odvozených pojmech. V moderním významu se pod pojmem *aritmetika* rozumí spíše základní početní úkony.

[2] Diofantos z Alexandrie (asi 3. století n. l.), řecký matematik, proslul svým spisem *Aritmetika* o řešení (diofantických) rovnic a dalších úloh.

**Příklad.** (motivační) V diofantické rovnici $ab = a + b$ (tedy hledáme řešení, v němž jsou $a$, $b$ celá čísla) úpravou do tvaru

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

hned zjistíme, že dvě celá čísla $a-1$, $b-1$ dávají v součinu 1. Potom ale nutně buďto $a-1 = 1$ a zároveň $b-1 = 1$ (a tedy $a = b = 2$), anebo $a-1 = b-1 = -1$ (a tedy $a = b = 0$).

Všimněme si, že úprava na součin nám okamžitě omezila možné hodnoty $a-1$, $b-1$. I kdybychom bývali na pravé straně získali jinou hodnotu než 1, stačilo by nám projít konečně mnoho možností, neboť každé celé číslo má jen konečně mnoho dělitelů.

S tímto přístupem ale mnohdy narazíme – výrazy jako $a^2 + b^2$, $a^2 + ab + b^2$, $a^2 - 2b^2$ nebo

$$a^4 + a^3b + a^2b^2 + ab^3 + b^4$$

se nám v celých číslech na součin rozložit nepodaří. Řešením této nesnáze pak může být právě to, že si celá čísla rozšíříme na nějakou „větší“ strukturu, v níž už daný výraz rozložit půjde. Bohužel se však ne vždy budeme moci spolehnout na všechny vlastnosti celých čísel, na něž jsme zvyklí. Klíčové pro nás tedy bude zjišťovat, které hezké vlastnosti celých čísel se při různých způsobech rozšíření zachovají a které již platit přestanou.

## Jak seriál číst

Seriál obsahuje celou řadu úkolů na procvičení. Ty jež, jsou označeny „Cvičení“, po Tobě většinou žádají nějak jednoduše použít zavedené pojmy či tvrzení, anebo rozmyslet si nějaký jejich jednoduchý důsledek. Vykřičníkem jsou označena ta cvičení, jež považujeme za obzvláště důležitá a která později využíváme. Cvičení s hvězdičkou jsou pak ta, která z rozličných důvodů považujeme spíše jen za zajímavosti. Mohou být o něco obtížnější a jejich znalost určitě není třeba k pochopení zbytku seriálu. Posledním druhem úkolů jsou pak „Úlohy“, což jsou (alespoň na první pohled) obyčejné příklady, v nichž lze tvrzení a postupy, které si v seriálu ukážeme, s úspěchem využít.

Na konci dílu nalezneš návody k některým cvičením a všem úlohám a také řešení všech cvičení. Doporučujeme tedy zkusit si souběžně se čtením seriálu řešit cvičení, především ta vykřičníková. Pokud se Ti to nebude dařit, nezoufej, zkus si přečíst návod, a pokud si stále nebudeš vědět rady, nahlédni do řešení. Úlohy jsou dosti nezávislé na zbytku seriálu, ničemu tedy nevadí, když jich vyřešíš jenom pár nebo pokud se k nim vrátíš až po dočtení celého dílu. Hvězdičková cvičení můžeš při prvním čtení s klidným svědomím přeskakovat a vrátit se k nim až později, budeš-li chtít.

Ještě než začneme, zmiňme, že některé části seriálu mohou být náročnější na pochopení. Pokud se tedy například zasekneš na některém důkazu, můžeš jej zkusit přeskočit a později se k němu vrátit. Dokud budeš rozumět definovaným pojmům a vědět, co tvrzení říká, nemělo by Tě vynechání důkazů později příliš omezovat.

**Úmluva.** (značení množin) V seriálu značíme množinu přirozených čísel $\mathbb{N} = \{1, 2, 3, \dots\}$. Nulu nepovažujeme za přirozené číslo. Celá čísla značíme $\mathbb{Z}$, racionální čísla (zlomky) jsou $\mathbb{Q}$ a konečně $\mathbb{R}$ představuje množinu reálných čísel, tedy čehokoliv z reálné přímky: racionální i iracionální čísla jako $\sqrt{2}$, $\pi$ a mnohá další. Komplexní čísla, která si v průběhu seriálu zavedeme, budeme značit $\mathbb{C}$.

Dále budeme někdy množiny psát notací $\{\text{výraz} : \text{podmínky}\}$. Tím myslíme množinu všech možných hodnot výrazu za splnění podmínek. Například $\{2n : n \in \mathbb{N}\}$ je množina všech sudých přirozených čísel, zatímco $\left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\right\}$ je jenom jinak zapsané $\mathbb{Q}$.

## Celá čísla

Celá čísla[3] snad není třeba představovat příliš okázale – jedná se zkrátka o čísla

$$\ldots, \quad -3, \quad -2, \quad -1, \quad 0, \quad 1, \quad 2, \quad 3, \quad \ldots,$$

tedy o nulu, přirozená čísla a jejich záporná dvojčata. S celými čísly umíme provádět některé základní operace: lze je sčítat, odčítat a násobit. Při dělení by však výsledkem nemuselo být celé číslo (a dělení nulou není definováno vůbec).

Shrňme některé základní vlastnosti celých čísel a počítání s nimi. Většina z nich má svůj vznešený matematický název, není však příliš důležité si všechny tyto názvy pamatovat:

(1) Sečtením i vynásobením dvou celých čísel dostaneme opět celé číslo, tedy pro $a, b \in \mathbb{Z}$ platí $a + b \in \mathbb{Z}$ i $a \cdot b \in \mathbb{Z}$. Říkáme, že celá čísla jsou na sčítání i násobení *uzavřená*.

(2) Při sčítání i násobení dvou celých čísel nezáleží na pořadí neboli pro celá $a$, $b$ platí

$$a + b = b + a, \qquad a \cdot b = b \cdot a.$$

Říkáme, že sčítání i násobení celých čísel je *komutativní*.

(3) Při sčítání, resp. násobení tří celých čísel nezáleží na tom, jak tyto operace uzávorkujeme neboli pro celá $a$, $b$, $c$ platí

$$a + (b + c) = (a + b) + c, \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Říkáme, že sčítání i násobení celých čísel je *asociativní*.

(4) Násobí-li celé číslo součet dvou dalších, pak lze „roznásobit závorku“ (anebo naopak vytknout ze součtu součinů společný činitel) neboli

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Říkáme, že násobení je *distributivní* ke sčítání.

(5) V $\mathbb{Z}$ existují výjimečné prvky 0 a 1, které pro každé $a \in \mathbb{Z}$ splňují

$$a + 0 = a, \qquad a \cdot 1 = a, \qquad a \cdot 0 = 0.$$

Říkáme, že 0 je *neutrální prvek* vzhledem ke sčítání, 1 je *neutrální prvek* vzhledem k násobení a 0 je *absorpční prvek* vzhledem k násobení.

(6) Pro každé celé $a$ existuje nějaké celé číslo $-a$, které splňuje $a + (-a) = 0$. Říkáme, že $-a$ je *inverzní prvek* k $a$ vzhledem ke sčítání. Jinými slovy tato vlastnost říká, že celá čísla lze odčítat.

(7) Pro celá $a$, $b$ platí $a \cdot b = 0$ jenom tehdy, když je $a = 0$ nebo $b = 0$.

### Dělitelnost

Když už umíme čísla sčítat, odčítat a násobit, můžeme se podívat i na jejich dělení, které je všem určitě dobře známé. Pro jistotu to ale lehce zopakujeme.

**Definice.** Číslo $a$ *dělí* číslo $b$ (značíme $a \mid b$), pokud existuje nějaké číslo $k$ takové, že $b = ka$.

Dělitelnost má spoustu hezkých vlastností, které si můžeš dokázat v následujícím cvičení.

**Cvičení(!) 1.** Mějme nenulová celá $a$, $b$, $c$, $d$. Potom platí:

(i) Každé $a$ splňuje $1 \mid a$ i $a \mid 0$.

[3] Celá čísla značíme $\mathbb{Z}$, z německého *Zahlen*, v překladu „čísla“ nebo „počty“.

(ii) Když $a \mid b$ a zároveň $b \mid c$, pak i $a \mid c$.

(iii) Když $a \mid b$, pak i $a \mid bc$ pro libovolné $c$.

(iv) Když $a \mid c$ a zároveň $b \mid d$, pak i $ab \mid cd$.

(v) Když $a \mid c$ a zároveň $a \mid d$, pak i $a \mid c + d$.

(vi) Pokud $a \mid b$ a zároveň $b \mid a$, pak $|a| = |b|$.

**Definice.** Pokud $a \mid b$ a zároveň $b \mid a$, říkáme, že čísla $a$, $b$ jsou *asociovaná*, značíme $a \parallel b$. *Jednotkami* jsou ta čísla, která dělí 1.

Jednotkami v $\mathbb{Z}$ jsou tedy čísla 1 a $-1$. Jak také vidíme z bodu (vi) předchozího cvičení, pokud jsou čísla $a$ a $b$ asociovaná, pak je $a = \pm b$ a naopak.

**Cvičení 2.** Rozmysli si, že pokud je $a$ asociované s $b$ a $b$ asociované s $c$, pak je i $a$ asociované s $c$.

Doteď jsme se bavili o dělitelnosti obecně, ale již ze základní školy každý dobře ví, že v dělitelnosti jsou důležitá třeba prvočísla a jiná podobná zvířátka, tak se na ně pojďme podívat zblízka.

**Definice.** *Ireducibilním* nazvěme číslo $q$, které není jednotkou a splňuje, že když $q = ab$, pak jedno z čísel $a$ či $b$ je jednotka.[4]

**Definice.** *Prvočíslo* je takové číslo $p$, které není jednotkou a splňuje, že pokud $p \mid ab$, tak i $p \mid a$ nebo $p \mid b$.

Tyto definice se dají samozřejmě rozšířit na součin více čísel. Všimni si také, že při takovéto definici považujeme za prvočísla i záporná čísla $-2$, $-3$, $-5$, $-7$ a podobně.

**Cvičení(!) 3.** (i) Nechť je $q$ ireducibilní prvek. Pokud $q = a_1 a_2 \cdots a_n$, potom všechny $a_i$ až na jedno jsou jednotky.

(ii) Nechť je $p$ prvočíslo. Pokud $p \mid a_1 a_2 \cdots a_n$, potom $p$ dělí nějaké z $a_i$.

V celých číslech nám definice ireducibilních čísel a prvočísel splývají a to se nám líbí, avšak obecně to platit nemusí a taky neplatí, nicméně odstrašující příklady si ukážeme raději až později v kapitole o komutativních okruzích. Předtím než si ukážeme důkaz, že v celých číslech jsou ireducibilní prvky prvočísly, budeme chtít vědět, že pro každou dvojici máme největšího společného dělitele. Druhou implikaci však zvládneme už teď.

**Tvrzení.** *Každé prvočíslo je ireducibilní.*

*Důkaz.* Nechť $p = ab$, potom z definice prvočísla víme, že $p \mid a$ nebo $p \mid b$. Z druhé strany však platí $a, b \mid ab \mid p$, tedy určitě $a \parallel p$ nebo $b \parallel p$. To už znamená, že ten druhý činitel musí být jednotkou, takže $p$ je ireducibilní. □

## Dělení se zbytkem a Eukleidův[5] algoritmus

Už jsme si ukázali dělení beze zbytku, avšak teď nás čeká i to se zbytkem. Pravděpodobně si jej alespoň matně pamatuješ z prvního stupně, rovnou tedy zformulujeme trochu formálně, o co se jedná.

**Tvrzení.** (dělení se zbytkem) *Pro libovolná celá čísla $a$, $b \neq 0$ existují celá čísla $q$, $r$ taková, že $a = qb + r$ a zároveň $|r| < |b|$.*

Platnost tohoto tvrzení lze snadno nahlédnout. Každé $|b|$-té číslo je násobek $b$, takže některé z čísel $a, a-1, \ldots, a-|b|+1$ je násobek $b$. Stačí nám tedy od $a$ odečíst nějaké $r \in \{0, \ldots, |b|-1\}$ a

[4] Ekvivalentně: pokud $q \parallel ab$, pak jedno z čísel $a$ nebo $b$ je s ním asociované.

[5] Eukleidés, někdy též Euklid (asi 325–260 př. n. l.), řecký matematik, položil *Základy* geometrie svým stejnojmenným spisem. Některé části *Základů* se však věnují i teorii čísel jako např. existenci nekonečně mnoha prvočísel či právě Eukleidovu algoritmu.

získáme tím $qb$. Předtím než pomocí dělení se zbytkem zavedeme *Eukleidův algoritmus*, zadefinujme si největšího společného dělitele, kterého nám tento algoritmus pomůže nalézt.

**Definice.** Číslo $d$ je *společný dělitel* čísel $a$, $b$, pokud $d \mid a$ a zároveň $d \mid b$. *Největším společným dělitelem* (zkráceně NSD) čísel $a$, $b$ pak myslíme největší takové přirozené číslo, které je společným dělitelem $a$, $b$. NSD čísel $a$, $b$ značíme $(a, b)$.

Teď už víme, co největší společný dělitel je, ale jak ho spočteme? No Eukleidův algoritmus je tu pro nás! Standardní Eukleidův algoritmus slouží ke spočtení největšího společného dělitele. My však nebudeme žádná ořezávátka – raději si přiděláme trochu práce a vyrobíme rovnou i takzvané *Bézoutovy*[6] *koeficienty* $x$, $y$, což jsou čísla, pro něž platí $ax+by = (a, b)$. Zároveň tím, že nalezneme algoritmus, který tyto koeficienty najde, dokážeme jejich existenci.[7]

Jak bychom ale mohli začít? Podívejme se na to prvně v přirozených číslech, protože tam je to nejjednodušší. Můžeme si všimnout, že $(a, b) = (b, a - b)$. To lehce ověříme třeba tak, že pokud má $a$ i $b$ společného dělitele, pak dělí i $a - b$. Naopak pokud existuje nějaký společný dělitel $d$ čísel $b$ a $a - b$, pak děli i $d \mid b + (a - b) = a$. Z toho tedy už plyne, že největší společní dělitelé těchto dvojic se rovnají.

Spočítat $(1005, 1000)$ může zprvu vypadat děsivě, ale když si řekneme, že tento NSD je totožný s $(1005, 5)$, už jsme si možnosti značně omezili. Tady vidíme myšlenku, na které je celý Eukleidův algoritmus založený. Budeme stále zmenšovat danou dvojici a u toho zachovávat stejného největšího společného dělitele, až dorazíme na tak malé číslo, že už bude jasné, co tím největším společným dělitelem je.

Ještě si dovolme malou poznámku. Všimněme si, že pokud $a \geq b$, pak se nám vyplatí $b$ odečíst nejvícekrát, co to jde. To tedy znamená $(a, b) = (b, a-b) = (b, a-2b) = \ldots = (b, a-qb)$, kde $a-qb$ chceme nezáporné. To nám ale už určitě připomíná naše dělení se zbytkem.

Pokud se tedy vrátíme k našemu příkladu s čísly 1005 a 1000, dostaneme že $(1005, 1000) = (1000, 5) = (5, 0) = 5$.

Nyní si to jen zformulujeme pořádně a s přidanou hodnotou Bézoutových koeficientů.

**Definice.** (rozšířený Eukleidův algoritmus) Mějme jako vstup dvě nenulová celá čísla $a$, $b$. Zavedeme posloupnosti $\{a_n\}$, $\{x_n\}$, $\{y_n\}$ následovně:

(i) Počáteční hodnoty nastavme jako

$$a_1 = a, \qquad a_2 = b, \qquad x_1 = 1, \qquad y_1 = 0, \qquad x_2 = 0, \qquad y_2 = 1.$$

(ii) Dále postupně pro $n = 2, 3, \ldots$ použijme dělení se zbytkem na vyjádření $a_{n-1} = qa_n + r$ za splnění $|r| < |a_n|$. Další členy posloupností pak definujme

$$a_{n+1} = r = a_{n-1} - qa_n, \qquad x_{n+1} = x_{n-1} - qx_n, \qquad y_{n+1} = y_{n-1} - qy_n.$$

(iii) Skončeme, jakmile pro nějaké $N$ dostaneme $a_N = 0$.

Za okamžik si ukážeme, že z takto definovaného algoritmu získáme na pozici $N - 1$ největší společný dělitel spolu s Bézoutovými koeficienty. Na první pohled však nemusí být zcela průhledné, co že to náš algoritmus dělá. Tak si ho pojďme ukázat na příkladě a poté i dokázat, že opravdu počítá, co chceme.

**Příklad.** Najděme největší společný dělitel čísel 13 a 5:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Posloupnost $\{a_n\}$: | 13 | $\to$ | 5 | $\to$ | 3 | $\to$ | 2 | $\to$ | 1 | $\to$ | 0. |
| Posloupnost $\{x_n\}$: | 1 | $\to$ | 0 | $\to$ | 1 | $\to$ | $-1$ | $\to$ | 2 | $\to$ | $-5$. |
| Posloupnost $\{y_n\}$: | 0 | $\to$ | 1 | $\to$ | $-2$ | $\to$ | 3 | $\to$ | $-5$ | $\to$ | 13. |

[6] Étienne Bézout (1730–1783), francouzský matematik.

[7] Pozor, Bézoutovy koeficienty nejsou jednoznačné. Platí totiž například $a(x - b) + b(y + a) = ax + by = (a, b)$.

Ve sloupečcích si můžeme všimnout, že platí $a_n = x_n a + y_n b$. Ve výsledku jsme spočetli, že NSD je 1 spolu s vyjádřením $1 = 2 \cdot 13 - 5 \cdot 5$.

**Tvrzení.** *Rozšířený Eukleidův algoritmus najde NSD čísel $a$, $b$. Platí $a_{N-1} = (a, b)$ a navíc pro $x = x_{N-1}$, $y = y_{N-1}$ máme vyjádření $(a, b) = ax + by$.*

*Důkaz.* Uvažujme podle definice rozšířeného Eukleidova algoritmu index $N$ takový, že $a_N = 0$, ale $a_{N-1} \neq 0$. Tato situace určitě někdy nastane, jelikož díky dělení se zbytkem máme vždy $|a_n| > |a_{n+1}|$. Označme $D(u, v)$ množinu všech společných dělitelů $u$, $v$. Dokažme si, že pro každé $n$ platí $D(a_{n-1}, a_n) = D(a_n, a_{n+1})$. Tím už bude zřejmé, že

$$(a, b) = (a_1, a_2) = \cdots = (a_{N-1}, a_N) = (a_{N-1}, 0),$$

což je až na znaménko zjevně $a_{N-1}$. Uvažujme jakéhokoliv společného dělitele $d_1$ čísel $a_{n-1}$, $a_n$. Podle bodu (ii) definice rozšířeného Eukleidova algoritmu pro nějaké číslo $q$ platí

$$a_{n+1} = a_{n-1} - q a_n.$$

Když tedy $d_1 \mid a_{n-1}$ a zároveň $d \mid a_n$, pak určitě i $d_1 \mid a_{n+1}$. Stejně tak ale uvedenou rovnost můžeme přepsat jako $a_{n-1} = a_{n+1} + q a_n$, čímž obdobně získáme, že každý společný dělitel $d_2$ čísel $a_n$, $a_{n+1}$ je i dělitelem $a_{n-1}$. Dohromady jsme tak ukázali, že $D(a_{n-1}, a_n) = D(a_n, a_{n+1})$.

Tím jsme již napůl vyhráli, víme, že $(a, b) = a_{N-1}$. Dokažme dále indukcí, že pro každé $n$ platí $a_n = x_n a + y_n b$. Pro $n = 1$ a $n = 2$ to platí díky nastavení počátečních hodnot $\{x_n\}$, $\{y_n\}$. Nyní nechť rovnost platí pro $n-1$ a $n$ a dokažme ji pro $n+1$. Opět pro číslo $q$ získané z dělení se zbytkem s použitím indukčního předpokladu dostaneme

$$\begin{aligned} a_{n+1} &= a_{n-1} - q a_n = (a x_{n-1} + b y_{n-1}) - q(a x_n + b y_n) = \\ &= (x_{n-1} - q x_n) \cdot a + (y_{n-1} - q y_n) \cdot b = x_{n+1} a + y_{n+1} b. \end{aligned}$$

Indukcí pak toto platí pro všechna $n$, takže speciálně $(a, b) = a_{N-1} = x_{N-1} a + y_{N-1} b$, jak jsme chtěli. □

**Úloha 1.** Dokaž, že pro každé přirozené $n$ je zlomek $\frac{21n+17}{5n+4}$ v základním tvaru, tedy že čitatel a jmenovatel jsou nesoudělní.

Pomocí Eukleidova algoritmu jsme již NSD nalezli, takže si pojďme s jeho pomocí dokázat, že každý ireducibilní prvek je také prvočíslo.

**Tvrzení.** *Je-li celé číslo $p$ ireducibilní, pak je to také prvočíslo.*

*Důkaz.* Mějme $p$ ireducibilní a předpokládejme, že platí $p \mid ab$ pro nějaká nenulová $a$, $b$. Chceme dokázat, že $p$ musí dělit jedno z $a$, $b$.

Pro spor předpokládejme, že $p \nmid a$ a zároveň $p \nmid b$. Jelikož je $p$ ireducibilní, tak jsou jeho děliteli pouze $\pm 1$ a $\pm p$. Proto když $p \nmid a$, tak už musí být $(a, p) = 1$. Existují Bézoutovy koeficienty $x_1$, $y_1$ splňující $x_1 a + y_1 p = 1$. Obdobně je $(b, p) = 1$, takže existují Bézoutovy koeficienty $x_2$, $y_2$ splňující $x_2 b + y_2 p = 1$. Znásobením těchto dvou rovností získáme

$$x_1 x_2 ab + x_1 y_2 ap + y_1 x_2 bp + y_1 y_2 p^2 = 1.$$

Na levé straně jsou $ab$, $ap$, $bp$ i $p^2$ násobky $p$, takže i celá levá strana je násobkem $p$. To ale znamená $p \mid 1$, což je spor, protože ireducibilní prvek není jednotkou. To znamená, že určitě muselo nastat $p \mid a$ nebo $p \mid b$, jak jsme chtěli. □

## Proč je prvočíselný rozklad jednoznačný?!

Prvně dokažme, že jsou celá čísla součinem ireducibilních a jednotky (zatím bez jednoznačnosti).

**Lemma.** *Každé nenulové celé číslo $n$ je součinem ireducibilních čísel a jednotky.*

*Důkaz.* Čísla 1 a $-1$ jsou jednotky, tedy součin jednotky a žádných ireducibilních čísel. Dále postupujme silnou indukcí podle velikosti čísel v absolutní hodnotě: nechť pro všechna nenulová $|n| \leq N$ platí, že jsou součinem ireducibilních čísel a jednotky. Poté musí pro $|n| = N+1$ být $n$ buďto samo ireducibilní, nebo platí $n = k\ell$, kde $|k|, |\ell| > 1$. Pak ale musí $|k|$ i $|\ell|$ být menší než $N+1$, tedy menší nebo rovna $N$. Potom z indukce víme, že $k$ i $\ell$ jsou součinem ireducibilních čísel a jednotky. To samé tedy platí pro $n$, neboť nám stačí zapsat činitele z $k$ a z $\ell$ za sebe a vynásobit spolu příslušné jednotky. □

Nyní už máme všechen potřebný aparát k tomu, abychom odpověděli na otázku z nadpisu sekce. Víme, že ireducibilní čísla jsou totéž co prvočísla a že každé celé číslo lze rozložit na součin ireducibilních čísel. Zbývá tak dokázat jednoznačnost.

**Tvrzení.** (Základní věta aritmetiky) *Každé nenulové celé číslo $n$ se dá jednoznačně (až na pořadí a změny znamének) rozložit na součin prvočísel.*

*Důkaz.* Mějme tedy $\pm p_1 \cdots p_r = n = \pm q_1 \cdots q_s$, kde $p_i$ a $q_i$ jsou prvočísla. Potom bychom chtěli dokázat, že $r = s$ a prvočísla napravo lze spárovat s těmi nalevo tak, aby spárovaná prvočísla byla asociovaná neboli se lišila nanejvýš znaménkem.

Použijme znovu silnou indukci podle absolutní hodnoty. Pro $|n| = 1$ je tvrzení triviální. Dále předpokládejme, že tvrzení platí pro všechna $n$ splňující $|n| \leq N$. Jelikož platí $p_1 \cdots p_r = q_1 \cdots q_s$, musí $p_1$ z definice prvočísla dělit některý činitel napravo. BÚNO[8] nechť $p_1 \mid q_1$. Jelikož je $q_1$ ireducibilním prvkem, tak je $p_1 = \pm q_1$. Pokrácením těchto prvočísel dostaneme, že $\pm p_2 \cdots p_r = \pm q_2 \cdots q_s$. Přitom však $|p_2 \cdots p_r| = \left|\frac{n}{p}\right| < |n| = N+1$, takže $|p_2 \cdots p_r| \leq N$. Tento součin už je tedy z indukčního předpokladu jednoznačný. Platí tudíž $r - 1 = s - 1$ neboli $r = s$. Dále musí zbývající prvočísla být spárována do asociovaných dvojiček, takže spolu s $p_1 \parallel q_1$ už je celý rozklad jednoznačně určen. □

**Poznámka.** Určitě všichni víme, že se normálně nepíše $24 = 2 \cdot 2 \cdot 2 \cdot 3$, nýbrž $24 = 2^3 \cdot 3$. Tento zkrácený zápis si můžeme dovolit nyní i my. Když v jednoznačném rozkladu spojíme všechna navzájem asociovaná prvočísla do jedné mocniny, dostaneme rozklad ve tvaru $n = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde pro $i \neq j$ platí $p_i \nmid p_j$. Potom platí $b \mid a$ právě tehdy, když $b = \pm p_1^{\beta_1} \cdot \cdots \cdot p_k^{\beta_k}$ pro nezáporná celá $\beta_i$ splňující $\alpha_i \geq \beta_i$.

**Úloha 2.** Najdi všechny dvojice přirozených čísel $x$, $y$ takové, že $x + y + 1 \mid 2xy$ a zároveň $x + y - 1 \mid x^2 + y^2 - 1$.

Nyní bychom se chtěli podívat, k čemu nám jednoznačný rozklad je.

**Definice.** Řekneme, že celá čísla $a$, $b$ jsou *nesoudělná*, pokud jsou jejich společnými děliteli pouze jednotky neboli když $(a, b) = 1$.

**Tvrzení.** (mocniny a nesoudělnost) *Nechť pro nesoudělná $a$, $b$ platí $ab = c^n$. Potom existují celá čísla $k$, $\ell$ splňující*

$$a = \pm k^n, \qquad b = \pm \ell^n$$

*a zároveň $k\ell = \pm c$.*

*Důkaz.* Zapišme si rozklad na prvočísla $c = \pm p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}$, kde $p_i$ jsou navzájem neasociovaná. Potom víme, že rozklad $c^n$ je $\pm p_1^{n\alpha_1} \cdot \cdots \cdot p_r^{n\alpha_r}$. Jelikož jsou $a$, $b$ nesoudělná, nemůže se v jejich rozkladu vyskytovat stejné prvočíslo. Proto pokud $p_i \mid a$, pak už se v $a$ vyskytuje $p_i$ ve stejné mocnině jako v $c^n$. Stačí tedy definovat $k$ jako součin těch $p_i^{\alpha_i}$, pro která $p_i \mid a$. Totéž provedeme pro $b$. Tím jsme naše tvrzení dokázali. □

[8] Zkratka pro „bez újmy na obecnosti“. Myslíme tím, že se nabízí několik možností, které jsou ale stejné až na nějaký nepodstatný detail, takže si prostě vybereme jen jednu a pokračujeme.

**Příklad.** V celých číslech vyřešme rovnici $x^2 + x = y^3$.

*Řešení.* Upravíme rovnici do tvaru $x(x+1) = y^3$. Jelikož $x$ a $x+1$ jsou nesoudělná, musí být oba činitelé jednotka krát třetí mocnina. Platí však, že 1 i $-1$ lze zapsat jako třetí mocniny celého čísla, takže můžeme BÚNO „vložit“ jednotku do mocniny a předpokládat $x = a^3$, $x+1 = b^3$ pro nějaká $a, b \in \mathbb{Z}$. Z toho máme

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

Musí platit $b > a$, takže už určitě $b - a = 1$. Následně má být

$$1 = b^2 + ba + a^2 = (a+1)^2 + (a+1)a + a^2 = 3a^2 + 3a + 1,$$

takže $3a(a+1) = 0$. To znamená $a = 0$ nebo $a = -1$, z čehož dopočítáme řešení $(x, y) = (0, 0)$ a $(x, y) = (-1, 0)$.

**Poznámka.** Zatím jsme tvrzení o nesoudělnosti a mocninách použili v případě, kdy jsou v rovnici $ab = c^n$ čísla $a$, $b$ nesoudělná. Co když to ale není tak snadné? Nechť jsou $a$, $b$ soudělná nějakým prvočíslem $p$. Pak i $p \mid c$, takže můžeme zapsat $a = pa_0$, $b = pb_0$, $c = pc_0$ a upravit rovnici na

$$a_0 b_0 = p^{n-2} c^n.$$

Takto lze pokračovat, až na levé straně dostaneme nesoudělné činitele. Na pravé straně nám sice mohou zbýt nějaké mocniny prvočísel, ale to příliš nevadí – z nesoudělnosti činitelů nalevo si každá tato mocnina bude muset vybrat, zda dělí $a_0$, nebo $b_0$. Nějaká soudělnost $a$, $b$ nám tedy typicky jenom přidělá práci s rozebíráním několika případů. V následujících cvičeních si můžeš vyzkoušet, jak v takovém případě postupovat.

**Cvičení 4.** Vyřeš v celých číslech rovnici $x^2 = y^3 + 16$.

**Úloha 3.** Najdi všechna celočíselná řešení rovnice $n(n+1)(n+2)(n+3)(n+4) = k^2$.

**Úloha 4.** Najdi všechny dvojice přirozených prvočísel $(p, q)$, pro něž je $p^2 + 5pq + 4q^2$ druhou mocninou celého čísla.

## Modulíme

Nyní už máme spoustu znalostí o dělitelnosti v celých číslech. Pojďme si ještě ale zavést jeden zápis, který je velmi častý, dost možná jej již znáš a ve světe teorie čísel nám usnadní práci.

**Definice.** Skutečnost, že $n \mid a - b$, značíme $a \equiv b \pmod{n}$ a říkáme, že $a$ je *kongruentní* s $b$ *modulo* $n$. Množině všech čísel $a + xn$ pro $x \in \mathbb{Z}$ říkáme *zbytková třída*. Množinu všech zbytkových tříd značíme $\mathbb{Z}_n$.

Možná jsi již s kongruencemi někdy pracoval(a), ale nikdy není na škodu si zopakovat, proč v nich některé věci platí.

Doporučujeme nad kongruencemi nepřemýšlet tak, že se jedná o vztah mezi celými čísly z množiny $\mathbb{Z}$, nýbrž tak, že počítáme se zbytkovými třídami z množiny $\mathbb{Z}_n$. Jak totiž uvidíme v následujícím cvičení, výsledky běžných operací typicky nezáleží na tom, se kterým zástupcem z dané zbytkové třídy je provedeme. Chytrým vybíráním si tak často lze ušetřit práci: například $99^2 \equiv (-1)^2 \equiv 1 \pmod{100}$ je snazší než $99^2 \equiv 9801 \equiv 1 \pmod{100}$.

**Cvičení(!) 5.** Pokud $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ a $k$ je nějaké číslo, pak platí i:

(i) $a + k \equiv b + k \pmod{n}$,
(ii) $a \cdot k \equiv b \cdot k \pmod{n}$,
(iii) $a + c \equiv b + d \pmod{n}$,
(iv) $a \cdot c \equiv b \cdot d \pmod{n}$.

Poslední věc, která nám schází, je krácení. S tím je ale trochu potíž, protože nemůžeme vždy jenom zkrátit čísla na obou stranách kongruence: kongruence $2 \equiv 10 \pmod 8$ je pravdivá, ale „zkrácením“ dvojky bychom dostali $1 \equiv 5 \pmod 8$, což neplatí. Proto musíme zkrátit i modul a získáme platnou kongruenci $1 \equiv 5 \pmod 4$. Nyní si to pojďme dokázat obecně.

**Cvičení 6.** Nechť $ac \equiv bc \pmod n$.

(i) Pokud navíc $(n, c) = 1$, pak $a \equiv b \pmod n$.

(ii) Obecněji bez nároků na $c$ platí $a \equiv b \pmod{\frac{n}{(n,c)}}$.

Abychom si trochu s kongruencemi pohráli, zkusíme si nějaké to lehčí cvičení.

**Cvičení 7.** Urči, jaký zbytek dává $5^{20}$ po dělení 26.

**Cvičení 8.** Urči paritu, poslední cifru a zbytek po dělení sedmi čísla $N = 22 \cdot 31 + 11 \cdot 17 + 13 \cdot 19$.

**Cvičení(!) 9.** Rozmysli si, že $x^2$ dává po dělení čtyřmi zbytek 0, je-li $x$ sudé, či 1, je-li $x$ liché.

Nyní už umíme s kongruencemi nějak pracovat, ještě jednou se pojďme zaměřit na dělení. Přesněji na to, kdy lze zbytkovou třídou $a \bmod n$ dělit.

**Tvrzení.** *Pokud je $a$ nesoudělné s $n$, pak existuje číslo $x$, takové že $ax \equiv 1 \pmod n$. Toto číslo zapisujme jako $\frac{1}{a}$.*

*Důkaz.* Kongruence $ax \equiv 1 \pmod n$ je ekvivalentní s dělitelností $n \mid ax - 1$, což je znovu ekvivalentní s $nk = ax - 1$ neboli $n(-k) + ax = 1$. Díky tomu, že už známe Eukleidův algoritmus, však víme, že pro nesoudělná $a$, $n$ dovedeme najít takové Bézoutovy koeficienty $-k$, $x$. □

## Vzhůru do komplexních čísel

Nyní se ale posuňme o kus dál. V úlohách, které jsme viděli, nám často pomohlo rozložit nějaký výraz na součin. Úskalím je tomu ale fakt, že ne všechny výrazy jde na součin rozložit. Například $a^2 + b^2$ se nám v celých či reálných číslech nepodaří rozložit na součin dvou výrazů s $a$, $b$. Abychom toto zklamání napravili, přidáme si nová čísla. Konkrétně, prohlašme, že existuje nějaké „číslo“ $i$ (bývá nazýváno *imaginární jednotkou*), které splňuje $i^2 = -1$. Takové $i$ určitě nenajdeme mezi reálnými čísly, nenechme se však tímto odradit. Prostě si vymyslíme takové $i$ a řekneme, že se naučíme počítat s čísly tvaru $a + bi$, kde $a$, $b$ mohou být reálná čísla (později se omezíme na celá).

Čísla $a + bi$ nazýváme *komplexní* a jejich množinu značíme $\mathbb{C}$. Hned si rozmysleme, že počítání s nimi není nic děsivého. Chceme-li sečíst $a + bi$ s $c + di$, jednoduše spočteme

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

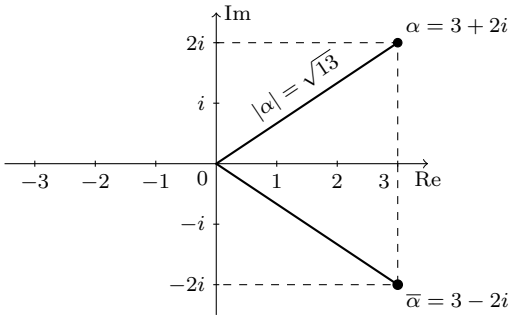
Odečítání provedeme obdobně. Budeme-li chtít komplexní čísla násobit, zkrátka roznásobíme závorky a dostaneme

$$(a + bi) \cdot (c + di) = ac + bci + adi + bdi^2.$$

Když však využijeme $i^2 = -1$, což je jediná podmínka, kterou po $i$ vůbec požadujeme, získáme $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. Takto definované operace s komplexními čísly mají všechny obvyklé vlastnosti, na které jsme zvyklí z reálných čísel: nezáleží v nich na pořadí, můžeme roznásobovat závorky a tak podobně. My tyto vlastnosti nebudeme dokazovat příliš dopodrobna. Pokud se s komplexními čísly potkáváš poprvé, můžeme Tě ujistit, že z hlediska upravování výrazů zde vše funguje stejně jako v reálných číslech.[9]

[9] Pokud se o nich chceš dozvědět více, doporučujeme PraSečí seriál o komplexních číslech: *https://prase.cz/archive/30/9.pdf*.

Abychom mohli vymyslet dělení komplexních čísel, nakreslíme si nejprve obrázek. Stejně jako si reálná čísla kreslíme na reálnou přímku, budeme komplexní čísla kreslit do *komplexní* (nebo též *Gaussovy*[10]) *roviny*. Komplexní číslo $\alpha = a + bi$ zde zakreslíme na pozici se souřadnicí $a$ na *reálné ose* a $b$ na *imaginární ose*. Také nazýváme $a$ *reálnou* a $b$ *imaginární částí* komplexního čísla $\alpha$.




Pro komplexní číslo $\alpha = a + bi$ v komplexní rovině definujeme jeho *komplexně sdružené číslo*[11] jako to, které odpovídá bodu překlopenému podle reálné osy, tedy obrácení znaménka imaginární části. Značíme jej $\overline{\alpha} = a - bi$ (čteme „alfa s pruhem“). Všimněme si, že

$$\alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2.$$

Díky Pythagorově větě je toto druhá mocnina délky úsečky spojující $\alpha$ v komplexní rovině s bodem 0. To nám umožňuje definovat absolutní hodnotu komplexního čísla jako $|\alpha| = \sqrt{\alpha\overline{\alpha}} = \sqrt{a^2 + b^2}$. Rozmysli si, že pro reálné číslo se tato definice shoduje s běžnou absolutní hodnotou.

S pomocí komplexně sdruženého čísla už můžeme zavést dělení. Pokud je komplexní číslo $a + bi$ nenulové, pak $a^2 + b^2 > 0$, takže můžeme při dělení rozšířit komplexně sdruženým číslem a spočíst

$$\frac{c + di}{a + bi} = \frac{(c + di)(a - bi)}{(a + bi)(a - bi)} = \frac{(ac + bd) + (ad - bc)i}{a^2 + b^2} = \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}\,i.$$

## Gaussova celá čísla

Již jsme si zavedli komplexní čísla s reálnými složkami. Abychom se s nimi mohli pustit do nějaké teorie čísel, bylo by záhodno si je omezit na něco podobného celým číslům. Přirozenou volbou je povolit v reálné i imaginární části pouze celá čísla. Dostaneme takzvaná *Gaussova (celá) čísla*, jimiž myslíme komplexní čísla $a + bi$ pro $a, b \in \mathbb{Z}$. Jejich množinu značíme $\mathbb{Z}[i]$. Je snadné si rozmyslet, že součet i součin dvou Gaussových čísel je opět Gaussovo číslo, takže $\mathbb{Z}[i]$ představuje rozumnou „komplexní verzi $\mathbb{Z}$“ (splňuje vlastnosti (1) až (7), které měla celá čísla). Později v kapitole o komutativních okruzích uvidíme, že v komplexních číslech existují i jiné struktury s podobnými vlastnostmi.

**Definice.** Pro $\alpha, \beta \in \mathbb{Z}[i]$ řekneme, že $\alpha$ *dělí* $\beta$ (značíme $\alpha \mid \beta$), pokud existuje $\gamma \in \mathbb{Z}[i]$ splňující $\beta = \alpha\gamma$.

Tato definice dělitelnosti říká v podstatě totéž, co definice dělitelnosti pro celá čísla. Stejně tak pro nenulové $\alpha$ platí $\alpha \mid \beta$, právě když je $\frac{\beta}{\alpha}$ Gaussovo celé číslo. Pojďme si dělitelnost vyzkoušet.

[10] Carl Friedrich Gauss (1777–1855), německý matematik přezdívaný *kníže matematiků*, přispěl k rozvoji mnoha oblastí matematiky i dalších věd. Z jeho díla zmiňme knihu *Disquisitiones Arithmeticae*, kterou položil základy moderní teorie čísel. Jeho jméno v seriálu ještě několikrát potkáme.

[11] V angličtině se setkáme s pojmem *complex conjugate*.

**Cvičení 10.** Rozhodni, zda $9+3i \mid 12-6i$.

V celých číslech jsme ve spoustě důkazů využívali absolutní hodnotu. Ta nám sloužila k tomu, abychom uměli nějakým způsobem určit velikost čísel. Využívali jsme ji například všude, kde jsme potřebovali nějak indukovat podle velikosti, tedy v důkazu lemmatu o rozkladu na ireducibilní prvky nebo (trochu skrytě) v Eukleidově algoritmu. Abychom tedy s Gaussovými čísly mohli pracovat velmi podobně jako s čísly celými, bylo by skvělé, kdybychom na nich měli něco podobného jako absolutní hodnotu. Absolutní hodnota Gaussova celého čísla však nemusí být celé číslo, například $|3+2i| = \sqrt{13}$. To by nám mohlo činit určité nepříjemnosti, proto budeme radši pracovat s druhou mocninou absolutní hodnoty.

**Definice.** *Normu* Gaussova celého čísla $\alpha = a+bi$ definujeme jako $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2$.

Norma nám nejenom říká, jak je Gaussovo číslo velké, ale jak si ukážeme, chová se také hezky k násobení. Všimni si, že každé celé číslo $a$ je i Gaussovo celé číslo a platí pro něj platí $N(a) = a^2$.

**Tvrzení.** *Pro $\alpha, \beta \in \mathbb{C}$ platí $\overline{(\alpha\beta)} = \overline{\alpha} \cdot \overline{\beta}$.*

*Důkaz.* Prostě to rozpočítejme. Nechť $\alpha = a+bi$, $\beta = c+di$. Potom

$$\alpha\beta = (a+bi)(c+di) = (ac-bd)+(ad+bc)i,$$
$$\overline{\alpha} \cdot \overline{\beta} = (a-bi)(c-di) = (ac-bd)+(-ad-bc)i,$$

takže skutečně $\overline{(\alpha\beta)} = \overline{\alpha} \cdot \overline{\beta}$. □

**Důsledek.** (multiplikativita normy) *Norma součinu dvou Gaussových čísel je součin jejich norem. Říkáme, že norma je multiplikativní.*[12]

*Důkaz.* Pro $\alpha, \beta \in \mathbb{Z}[i]$ máme $N(\alpha\beta) = \alpha\beta \cdot \overline{(\alpha\beta)} = \alpha\beta \cdot \overline{\alpha}\overline{\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = N(\alpha) \cdot N(\beta)$. □

**Cvičení 11.** Pokud lze přirozená čísla $m$, $n$ obě vyjádřit ve tvaru $x^2+y^2$ (pro $x, y \in \mathbb{Z}$), pak lze v tomto tvaru vyjádřit i $mn$.

**Cvičení(!) 12.** Pokud $\alpha \mid \beta$, pak i $N(\alpha) \mid N(\beta)$. Opačné tvrzení však neplatí.

**Poznámka.** Můžeme si všimnout, že je to dobrý aparát k tomu, abychom zjistili, kdy čísla dělitelná nejsou.

**Cvičení 13.** Rozhodni, zda je $14-3i$ násobkem $3-i$.

Nyní si rozmysleme, jak vypadají jednotky v Gaussových celých číslech. Stejně jako v $\mathbb{Z}$ jednotkami myslíme ta čísla, jež dělí 1.

**Tvrzení.** *Jednotky jsou právě čísla $\pm 1$ a $\pm i$.*

*Důkaz.* Určitě vidíme, že tato čísla jednotkami jsou, jelikož $\pm 1 \cdot (\pm 1) = 1$ a $\pm i \cdot (\mp i) = 1$.

Nyní se podívejme, zda nemohou existovat další. Pokud $a+bi \mid 1$, pak nutně platí i $N(a+bi) \mid N(1) = 1$. Jinými slovy $a^2+b^2 = N(a+bi) = 1$. Celá čísla $a$, $b$, která splňují naši rovnici, jsou ale pouze ta, která nám dávají jednotky $\pm 1$, $\pm i$. □

Vidíme, že jednotky jsou ta čísla, jejichž norma je jedna, což je dle jejich názvu také velmi přirozené.

Abychom dovršili průzkum vlastností $\mathbb{Z}[i]$, dokážeme si, že i Gaussova celá čísla se rozkládají jednoznačně na součin „prvočísel“. Budeme postupovat stejnou cestou jako v celých číslech. Definice ireducibilního čísla a prvočísla ponechme stejné – ireducibilní číslo nelze rozložit na součin dvou

[12] Obecně říkáme, že funkce $f$ je multiplikativní, pokud splňuje $f(ab) = f(a) \cdot f(b)$. Někdy se tímto označením míní i funkce, která toto splňuje jen pro *nesoudělná* $a$, $b$, v seriálu však tento význam používat nebudeme.

nejednotek, zatímco prvočíslo dělí součin jen tehdy, když dělí jeden z činitelů. Budeme si ale muset upravit některé důkazy a rozmyslet si, že vše funguje tak, jak má, i tady.

Náš postup k důkazu Základní věty aritmetiky se odvíjel od dělení se zbytkem.

**Tvrzení.** *Pro $\alpha, \beta \in \mathbb{Z}[i]$ existují $\gamma, \delta \in \mathbb{Z}[i]$ taková, že $\alpha = \beta\gamma + \delta$ a zároveň $N(\delta) < N(\beta)$.*

V Gaussových číslech to ale není tak snadné. Nechť $\alpha = 27 - 23i$ a $\beta = 8 + i$. Zkusme je vydělit normálně:

$$\frac{\alpha}{\beta} = \frac{27 - 23i}{8 + i} \doteq 2{,}97 - 3{,}25i.$$

V celých číslech bychom si vzali největší násobek $\beta$, který je ještě menší než $\alpha$, tedy podíl $\frac{\alpha}{\beta}$ zaokrouhlený dolů. Kdybychom toto provedli zvlášť v reálné a imaginární složce, bylo by to $2 - 4i$. Potom by ale $\delta = (27 - 23i) - (2 - 4i)(8 + i) = 7 + 7i$. Vidíme, že norma tohoto zbytku je vetší než norma $\beta$, což je něco, čeho se chceme vyvarovat. Není tedy nějaká lepší možnost?

Podívejme se na to prvně zase zpátky v číslech celých. Pokud budeme využívat naše tvrzení pro čísla 33 a 7, dostaneme $33 = 7{\cdot}4{+}5$. Ale také bychom místo toho největšího menšího násobku 7 mohli vzít nejbližší násobek (ať už je vyšší, nebo nižší). V tomto případě bychom zvolili $33 = 7 \cdot 5 - 2$. Za cenu toho, že máme záporný zbytek, jsme ho zmenšili (v absolutní hodnotě) nanejvýš na polovinu absolutní hodnoty původního dělitele.

Toho využijeme i zde v Gaussových číslech. Když si vybereme v každé složce číslo nejbližší, pak dostáváme $\delta = (27 - 23i) - (3 - 3i)(8 + i) = -2i$. Tato hodnota už naše tvrzení splňuje, teď už si to pojďme jen dokázat obecně.

*Důkaz.* Zapíšeme si obecně podíl $\frac{\alpha}{\beta}$, který chceme vyjádřit se zbytkem, jako

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{k + \ell i}{N(\beta)}.$$

Využijeme toho, že v $\mathbb{Z}$ už dělit umíme a umíme to dokonce tak, že jsou zbytky dost malé. Tedy nechť $k = N(\beta)q_1 + x_1$ a $\ell = N(\beta)q_2 + x_2$, kde $|x_1| \leq \frac{N(\beta)}{2}$, $|x_2| \leq \frac{N(\beta)}{2}$. Nyní si to už jenom rozepišme:

$$\frac{\alpha}{\beta} = \frac{k + \ell i}{N(\beta)} = q_1 + q_2 i + \frac{x_1 + x_2 i}{N(\beta)}.$$

Zvolme $\gamma = q_1 + q_2 i$. Potom $\delta = \alpha - \beta\gamma = \frac{x_1 + x_2 i}{\overline{\beta}}$. Potom tedy

$$N(\delta) = N\left(\frac{x_1 + x_2 i}{\overline{\beta}}\right) = \frac{N(x_1 + x_2 i)}{N(\beta)} \leq \frac{\frac{N(\beta)^2}{4} + \frac{N(\beta)^2}{4}}{N(\beta)} = \frac{N(\beta)}{2} < N(\beta). \qquad \square$$

Už tedy umíme dělit se „správným“ zbytkem. V důkazu funkčnosti Eukleidova algoritmu jsme využívali pouze toho, že algoritmus skončí, což bylo způsobeno klesající absolutní hodnotou. S normou namísto absolutní hodnoty bychom mohli téhož využít i zde. Dostali bychom tak rozšířený Eukleidův algoritmus pro Gaussova čísla. Na jeho základě už lze dokázat, že v $\mathbb{Z}[i]$ je každé ireducibilní číslo prvočíslem, z čehož už by vyplynul jednoznačný rozklad Gaussových čísel na prvočísla. Změní se pouze obor čísel, se kterým pracujeme, tedy co pro nás budou prvočísla či jednotky. Jedinou vadou na krase je, že zatím nevíme, jak taková Gaussova prvočísla vypadají.

Nebudeme se s těmito důkazy nyní trápit do detailu, protože si je později ukážeme v obecnější verzi. Namísto Eukléidova algoritmu si ukážeme Bézoutovo lemma, které přináší stejné důsledky, pouze bez algoritmického pohledu na věc.

I bez znalosti Gaussových prvočísel nám jednoznačný rozklad může být užitečný – plyne z něj totiž tvrzení o mocninách a nesoudělnosti.

**Úloha 5.** Najdi všechny dvojice $(x, y)$ celých čísel takových, že splňují $x^2 = y^3 - 1$.

## Komutativní okruhy

Dosud jsme viděli několik struktur, v nichž dovedeme sčítat a násobit s podobnými pravidly jako v celých číslech. Konkrétní podobu těmto strukturám podobným $\mathbb{Z}$ dáme definováním komutativního okruhu.

**Definice.** *Binární operací* $*$ definovanou na množině $M$ rozumíme zobrazení, které dvojici prvků $a, b \in M$ přiřazuje právě jeden prvek $a * b$ z množiny $M$.

Neformálně řečeno: binární operace je cokoliv, co dvěma věcem jednoznačně přiřazuje nějakou třetí věc, přičemž výsledek této operace značíme tak, že mezi dva původní argumenty napíšeme znak pro příslušnou operaci.

**Příklad.** Uveďme některé běžné příklady binárních operací:

- Sčítání „+“, odčítání „−“, násobení „·“ celých čísel nebo dělení „:“ nenulových racionálních čísel. Povšimni si, že při odčítání nebo dělení dvou čísel záleží na pořadí.
- Budiž $X$ nějaká množina. Pro dvě její podmnožiny $A, B \subseteq X$ definujeme
  - jejich *sjednocení* $A \cup B$, jež obsahuje ty prvky, které jsou alespoň v jedné z $A$, $B$,
  - jejich *průnik* $A \cap B$, jež obsahuje ty prvky, které jsou v obou $A$, $B$,
  - jejich *symetrickou diferenci* $A \oplus B$, jež obsahuje ty prvky, které jsou v právě jedné z množin $A$, $B$.
- Uvažme funkce z $\mathbb{R}$ do $\mathbb{R}$. Pro dvě takové funkce $f$, $g$ definujeme jejich složení $g \circ f$ jako funkci $h$ předepsanou $h(x) = g(f(x))$ pro každé $x \in \mathbb{R}$. V této operaci opět záleží na pořadí – např. pro $f(x) = 2x$ a $g(x) = x^2$ dostaneme

$$(g \circ f)(x) = (2x)^2 = 4x^2, \qquad \text{ale} \qquad (f \circ g)(x) = 2x^2.$$

**Definice.** *Komutativním okruhem* nazýváme množinu[13] $R$ (té říkáme *nosná množina* okruhu) spolu s binárními operacemi $+$ a $\cdot$ (nazýváme je „sčítání“ a „násobení“) definovanými na $R$, které splňují:

(1) Množina $R$ je uzavřená na sčítání i násobení neboli pro libovolná $a, b \in R$ platí

$$a + b \in R, \qquad a \cdot b \in R.$$

(2) Sčítání i násobení jsou komutativní neboli pro libovolná $a, b \in R$ platí

$$a + b = b + a, \qquad a \cdot b = b \cdot a.$$

(3) Sčítání i násobení jsou asociativní neboli pro libovolná $a, b, c \in R$ platí

$$a + (b + c) = (a + b) + c, \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(4) Násobení je distributivní na sčítání neboli pro libovolná $a, b, c \in R$ platí

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

(5) V $R$ existují prvky 0 a 1, které pro každé $a \in R$ splňují

$$a + 0 = 0 + a = a, \qquad a \cdot 1 = 1 \cdot a = a, \qquad a \cdot 0 = 0.$$

(6) Pro každé $a \in R$ existuje nějaký prvek $-a \in R$, který splňuje $a + (-a) = 0$.

[13] Obecný okruh budeme často značit $R$ z německého *(Zahl)ring*.

Kdybychom chtěli být zcela formální a přesní, pak bychom měli vždy, když chceme hovořit o nějakém komutativním okruhu, přesně říci, s jakými operacemi $+$ a $\cdot$ pracujeme, či dokonce které prvky jsou 0 a 1 nebo co je $-a$ pro každé $a \in R$. Komutativní okruh by tak měl být určen šesticí $(R, +, \cdot, 0, 1, -)$. Velmi často je však z kontextu zřejmé, o jakých operacích hovoříme, takže budeme říkat pouze „(komutativní) okruh $R$“.[14]

Dále si v komutativních okruzích budeme dovolovat běžné zjednodušování zápisu, jaké známe z celých čísel, budeme psát násobení jako $ab$ namísto $a \cdot b$, odčítání jako $a - b$ namísto $a + (-b)$ a mocnění jako $a^n$ namísto $\underbrace{a \cdot a \cdots a}_{n\text{-krát}}$ pro přirozené číslo $n$.

**Poznámka.** Možná Tě napadlo, proč říkáme „komutativní“ okruh. Samotným slovem *okruh* se nazývá struktura, u které na rozdíl od komutativního okruhu nepředpokládáme, že násobení je komutativní, takže se může stát, že $ab$ je něco jiného než $ba$. Takové okruhy však v seriálu nebudeme potkávat.[15] I když tedy v seriálu řekneme jenom „okruh“, bude se takřka vždy jednat o komutativní okruh.

**Cvičení(!) 14.** Dokaž, že v okruhu existuje právě jedna nula (neutrální prvek vzhledem ke sčítání) a právě jedna jednička (neutrální prvek vzhledem k násobení).

**Cvičení(*) 15.** Podmínku o komutativitě sčítání můžeme v definici (i nekomutativního) okruhu vypustit: pokud $R$ s operacemi $+$, $\cdot$ splňují pouze podmínky (1), (3) až (6), pak už pro libovolná $a, b \in R$ platí $a + b = b + a$.

**Cvičení(*) 16.** Podmínku $0 \cdot a$ můžeme v definici okruhu vypustit – pokud $R$ s operacemi $+$, $\cdot$ splňují všechny ostatní podmínky z definice okruhu, pak už pro libovolné $a \in R$ platí $0 \cdot a = 0$.

## Příklady (komutativních) okruhů

Viděli jsme abstraktní definici okruhu, nyní si ukážeme konkrétní příklady. Mnohé z nich nás budou v seriálu ještě nějakou dobu provázet.

**Příklad.** Celá, racionální, reálná i komplexní čísla tvoří komutativní okruhy s obvyklým sčítáním a násobením. Nula a jednička jsou v nich přesně ty, na které jsme zvyklí.

**Příklad.** Přirozená čísla, lichá celá čísla či sudá celá čísla netvoří s obvyklým sčítáním a násobením okruh. Přirozeným číslům chybí 0, lichým číslům chybí 0 a nejsou uzavřená na sčítání, zatímco sudým číslům chybí 1.

**Příklad.** Pro přirozené číslo $n$ tvoří množina $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ zbytkových tříd mod $n$ komutativní okruh se sčítáním a násobením zbytkových tříd. Nulou je zde zbytková třída 0, jedničkou zbytková třída 1.

**Příklad.** Nechť je $X$ množina. Množina všech jejích podmnožin[16] $\mathcal{P}(X)$ spolu s operacemi symetrické diference (jako sčítání) a průniku (jako násobení) tvoří okruh. K tomu si rozmysli, že pro $A, B, C \in \mathcal{P}(X)$ platí

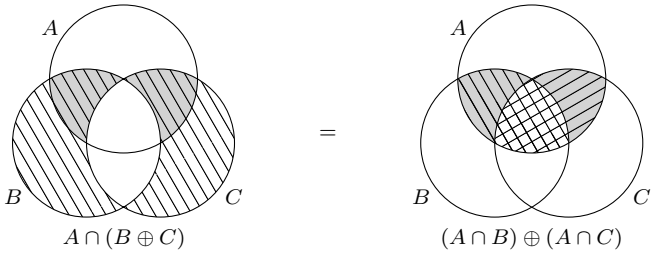
$$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$$

(viz Vennovy diagramy níže). Jedničkou je celá množina $X$, neboť $X \cap A = A$ pro každou $A \subseteq X$. Nulou je prázdná množina $\emptyset$, neboť $\emptyset \oplus A = A$ pro každou $A \subseteq X$. Odčítání je v tomto okruhu totéž jako sčítání, neboť platí $A \oplus A = \emptyset$ pro každou $A \subseteq X$.

[14] A slibujeme, že kdykoliv si vymyslíme okruh s neobvyklými operacemi, tak na to upozorníme.

[15] Kdyby Tě však zajímaly, doporučujeme jako příklady na seznámení s nekomutativními okruhy tzv. *kvaterniony* nebo čtvercové matice řádu $n$.

[16] Říká se jí *potenční množina*.




$A \cap (B \oplus C)$ $(A \cap B) \oplus (A \cap C)$

**Příklad.** Libovolná jednoprvková množina $\{a\}$ tvoří spolu s operacemi sčítání a násobení definovanými jako

$$a + a = a, \qquad a \cdot a = a$$

komutativní okruh. O okruhu s jednoprvkovou nosnou množinou říkáme, že je *triviální*. Všimni si, že v tomto okruhu jsou „nula“ a „jednička“ ten samý prvek.

**Cvičení(!) 17.** Budiž $R$ komutativní okruh s více než jedním prvkem. Dokaž, že potom v $R$ platí $0 \neq 1$.

**Příklad.** Gaussova celá čísla $\mathbb{Z}[i]$ tvoří komutativní okruh se sčítáním a násobením komplexních čísel.

**Příklad.** Nechť $\omega = \frac{1+i\sqrt{3}}{2}$. Potom množina $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ tvoří komutativní okruh, neboť platí $(a+b\omega)(c+d\omega) = (ac-bd)+(ad+bc+bd)\omega$. Číslům tohoto tvaru se říká *Eisensteinova*[17].

**Příklad.** Nechť je $S$ množina všech funkcí $f\colon \mathbb{R} \to \mathbb{R}$. Potom $S$ tvoří okruh se sčítáním a násobením funkcí definovaným jako

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

Nulou a jedničkou jsou konstantní funkce $f_0(x) = 0$ a $f_1(x) = 1$.

**Cvičení 18.** Nahlédni, že se stejnými operacemi jako v předchozím příkladu tvoří okruh i množina $S_2$ všech *sudých* funkcí, tedy funkcí $f\colon \mathbb{R} \to \mathbb{R}$ splňujících $f(-x) = f(x)$ pro každé $x \in \mathbb{R}$.

**Příklad.** Mějme čtyřprvkovou množinu $T = \{0, 1, a, b\}$ a definujme na ní sčítání a násobení pomocí následujících tabulek:

| $+$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $a$ | $b$ |
| $1$ | $1$ | $0$ | $b$ | $a$ |
| $a$ | $a$ | $b$ | $0$ | $1$ |
| $b$ | $b$ | $a$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $a$ | $b$ |
| $a$ | $0$ | $a$ | $b$ | $1$ |
| $b$ | $0$ | $b$ | $1$ | $a$ |

Potom $T$ tvoří s operacemi $+$, $\cdot$ okruh. Všimni si, že ač je to čtyřprvkový okruh, je různý od $\mathbb{Z}_4$.

**Příklad.** Uvažme všechna racionální čísla, jejichž jmenovatelé jsou mocniny dvou, tedy

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}.$$

[17] Gotthold Eisenstein (1823–1852), německý matematik. Ani jeho jméno v seriálu ještě nevidíme naposledy.

Se sčítáním a násobením racionálních čísel tvoří tato množina okruh.

Možná už si všímáš obecného pravidla: když napíšeme $R[m]$, kde $m$ je nějaké „číslo“, myslíme tím nejmenší takový okruh, pro který $R \subseteq R[m]$ a zároveň $m \in R[m]$. Praktičtější je ale představa, že v $R[m]$ prostě leží všechny výrazy $a_n m^n + \cdots + a_1 m + a_0$ pro nezáporné celé $n$ a prvky $a_0, a_1, \ldots, a_n \in R$. V závislosti na tom, co je $m$ zač, se mohou jednotlivá $m^k$ pro $k = 0, 1, 2, \ldots$ postupně opakovat (jako když např. $m = i$ nebo $m = \omega$), anebo se může jednat o navzájem různé prvky $R[m]$ (jako když např. $m = \frac{1}{2}$).

## Speciální vlastnosti okruhů

Víme již, co je okruh, je tedy na čase zkoumat, jaké vlastnosti mohou jednotlivé okruhy či jejich prvky mít. Naším cílem bude dopracovat se k „prvočíslům“ v okruzích. Začněme ale u vlastností nuly a jedničky.

**Definice.** Komutativní okruh nazveme *oborem integrity*, pakliže pro libovolné jeho prvky $a$, $b$ platí $ab = 0$, pouze pokud $a = 0$ nebo $b = 0$.

Ekvivalentní pohled na obory integrity je, že jsou to přesně ty okruhy, v nichž můžeme v rovnicích krátit nenulové činitele:

**Tvrzení.** *V oboru integrity pro $a \neq 0$ platí, že pokud $ab = ac$, pak i $b = c$.*

*Důkaz.* Převedením $ac$ na levou stranu dostaneme $ab - ac = 0$ a poté vytknutím $a$ získáme $a(b - c) = 0$. Následně z definice oboru integrity platí $a = 0$ nebo $b - c = 0$. Předpokládáme však $a \neq 0$, takže už nutně $b - c = 0$ neboli $b = c$. □

Když $R$ není obor integrity, může se stát, že $ab = ac$, i když $b \neq c$. Příkladem budiž okruh $\mathbb{Z}_4$, v němž platí $2 \cdot 1 \equiv 2 \cdot 3 \pmod 4$.

**Cvičení 19.** Rozmysli si, které z následujících okruhů jsou obory integrity:

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, (ii) $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, $\mathbb{Z}[\frac{1}{2}]$, (iii) triviální okruh,

(iv) $\mathbb{Z}_n$ v závislosti na přirozeném $n$,

(v) okruh $\mathcal{P}(X)$ v závislosti na množině $X$,

(vi) čtyřprvkový okruh $T = \{0, 1, a, b\}$ z předposledního příkladu.

Obory integrity nám říkají, že můžeme krátit rovnice, neznamená to ale, že můžeme dělit. Abychom se blíže podívali na to, čím lze dělit, zavedeme si dělitelnost a několik dalších pojmů.

**Definice.** V komutativním okruhu $R$ pro $a, b \in R$ říkáme, že $a$ *dělí* $b$ (značíme $a \mid b$), pokud existuje $c \in R$ takové, že $ac = b$.

**Cvičení(!) 20.** Pokud $a \mid b$ a zároveň $a \mid c$, pak už $a \mid bd + ce$ pro libovolná $d$, $e$.

**Cvičení 21.** V okruhu $\mathcal{P}(X)$ platí $A \mid B$, právě pokud $B \subseteq A$.

**Definice.** V komutativním okruhu $R$ nazveme $u \in R$ *jednotkou*, pokud $u \mid 1$.

Tedy $u$ je jednotka, pokud existuje $v \in R$ takové, že $uv = 1$.

**Cvičení 22.** Najdi množiny všech jednotek v následujících okruzích:

(i) $\mathbb{Z}$, (ii) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, (iii) $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, (iv) $\mathbb{Z}[\frac{1}{2}]$,

(v) $\mathcal{P}(X)$ v závislosti na množině $X$.

**Cvičení 23.** Pokud okruh $R$ není triviální, pak 0 není jednotkou.

**Definice.** V okruhu $R$ řekneme, že jsou prvky $a, b \in R$ *asociované*, pokud platí $a \mid b$ a zároveň $b \mid a$. Tuto skutečnost budeme značit $a \parallel b$.

Asociované prvky se „chovají stejně“ vzhledem k dělitelnosti. Když $a \parallel b$, pak pro všechna $c$ platí

$$a \mid c \iff b \mid c \qquad \text{a zároveň} \qquad c \mid a \iff c \mid b.$$

**Cvičení(!) 24.** V oboru integrity jsou $a$, $b$ asociované, právě pokud existuje jednotka $u$ taková, že $a = ub$.

## Ireducibilní prvky a prvočinitelé

Je na čase, abychom se podívali na zobecnění prvočísel. Podobně jako jsme učinili dříve, rozlišíme dvě vlastnosti, které budeme zkoumat: to, jak se prvky rozkládají na součin a jak dělí součiny. Většinou už odteď budeme pracovat jen v oborech integrity, i když některé pojmy definujeme v obecném komutativním okruhu.

**Definice.** Buď $R$ komutativní okruh a uvažme jeho nenulový prvek $p$, který není jednotkou. Řekneme, že $p$ je *ireducibilní* (v $R$), pokud pro každá $a, b \in R$ splňující $ab = p$ platí, že jedno z $a$, $b$ je jednotka. Řekneme, že $p$ je *prvočinitel* (v $R$), pokud pro libovolná $a, b \in R$ platí, že když $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

Vlastnosti ireducibilních prvků a prvočinitelů se jednoduchou indukcí zobecňují pro součiny libovolně mnoha činitelů. Když je součin $a_1 \cdots a_n$ roven ireducibilnímu prvku, pak jsou všichni činitelé krom jednoho jednotkami. Naproti tomu pokud je tento součin násobkem prvočinitele $p$, pak už musí $p$ dělit některý z činitelů.

**Cvičení(!) 25.** V oboru integrity jsou prvočinitelé vždy ireducibilní.

Dle našich zkušeností ze $\mathbb{Z}$ a $\mathbb{Z}[i]$ bychom rádi, aby všechny ireducibilní prvky byly prvočiniteli. Často to však neplatí.

**Příklad.** (varovný) Uvažme okruh $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, kde $\sqrt{-3}$ je (komplexní) číslo splňující $(\sqrt{-3})^2 = -3$ (kdyby Tě zápis se záporným číslem pod odmocninou zneklidňoval, můžeš si představovat, že $\sqrt{-3} = i\sqrt{3}$). Tento okruh je obor integrity (jelikož $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{C}$) a platí v něm

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Ukážeme, že 2 je ireducibilní. K tomu využijeme normu $N(\alpha) = \alpha\overline{\alpha}$, kterou snadno vyjádříme jako $N(x + y\sqrt{-3}) = x^2 + 3y^2$. Kdyby 2 nebyla ireducibilní, měli bychom $2 = ab$, kde $a$ ani $b$ nejsou jednotky. Norma je multiplikativní, tedy $N(a)N(b) = N(2) = 4$. Přitom prvky s normou 1 jsou jednotky, takže potřebujeme $N(a), N(b) > 1$, proto už nutně $N(a) = N(b) = 2$. Pokud ale $a = x + y\sqrt{-3}$ (kde $x, y \in \mathbb{Z}$), dostáváme $2 = x^2 + 3y^2$.

Ukážeme, že tato rovnice nemá v $\mathbb{Z}$ řešení. Když bude $y \neq 0$, tak už $3y^2 \geq 3 > 2$. Tedy nutně $y = 0$, takže by mělo platit $x^2 = 2$, tato rovnice ale nemá v $\mathbb{Z}$ řešení. Hledané prvky $a$, $b$ tedy neexistují a 2 je ireducibilní. Přitom však není prvočinitelem – dělí součin $(1 + \sqrt{-3})(1 - \sqrt{-3})$, ale nedělí ani jeden z činitelů, neboť ty mají obě složky liché.

Ukážeme si však, jak najít obory, v nichž „prvočísla fungují“, tedy kde všechny ireducibilní prvky jsou prvočinitelé. K tomu si zobecníme postup, který jsme upotřebili v $\mathbb{Z}$. Tam jsme využili vlastnosti dělení se zbytkem a Eukleidova algoritmu, který počítá největšího společného dělitele dvou čísel. Začněme tedy tím, že si tento poslední pojem definujeme i v obecném okruhu.

**Definice.** Buď $R$ komutativní okruh. Prvek $d \in R$ nazveme *společným dělitelem* prvků $a, b \in R$, pokud $d \mid a$ a zároveň $d \mid b$. Prvek $g \in R$ nazveme *největším společným dělitelem* $a$, $b$, pokud současně platí:

(i) Prvek $g$ je společným dělitelem $a$, $b$.

(ii) Libovolný společný dělitel $d$ prvků $a$, $b$ dělí také $g$.

Řečeno jednodušeji: největší společný dělitel je společný dělitel, kterého všichni společní dělitelé dělí. Všimni si, že tímto není definován jeden jediný největší společný dělitel $a$, $b$. Když například největšího společného dělitele přenásobíme jednotkou, dostaneme něco, co je opět největším společným dělitelem. Taky ale nemáme zaručeno, že největší společný dělitel vůbec existuje.

**Příklad.** (varovný) Uvažme znovu okruh $\mathbb{Z}[\sqrt{-3}]$ a ukažme, že prvky 4 a $2+2\sqrt{-3}$ nemají největšího společného dělitele. Pro spor nechť mají nějakého největší společného dělitele $g$. Nejprve pozorujme, že 2 i $1+\sqrt{-3}$ jsou společnými děliteli, takže určitě $2 \mid g$ a zároveň $1+\sqrt{-3} \mid g$. Vzhledem k $2 \mid g$ tedy $g = 2a$ pro nějaké $a \in \mathbb{Z}[\sqrt{-3}]$. Také má platit $g \mid 4$, tedy $2a \mid 4$ neboli $a \mid 2$. Z předchozího příkladu už víme, že 2 je ireducibilní, takže každý jeho dělitel je buďto asociovaný s 2 samotnou, nebo s 1. Pokud $a \parallel 2$, pak máme $4 \mid g$, přitom ale $4 \nmid 2+2\sqrt{-3}$, takže toto nelze. Pokud $a \parallel 1$, pak $g \mid 2$, takže i $1+\sqrt{-3} \mid 2$. Když ale tuto dělitelnost rozšíříme pomocí $1-\sqrt{-3}$, dostaneme

$$4 = (1+\sqrt{-3})(1-\sqrt{-3}) \mid 2(1-\sqrt{-3}) = 2-2\sqrt{-3}.$$

Dělitelnost $4 \mid 2-2\sqrt{-3}$ ale neplatí, takže $a$ nemůže být asociováno ani s 1. Vyčerpali jsme všechny možnosti a v každé jsme nalezli spor, takže největší společný dělitel 4 a $2+2\sqrt{-3}$ nemůže existovat.

**Cvičení 26.** Buď $R$ obor integrity. Pokud jsou oba prvky $g_1, g_2 \in R$ největšími společnými děliteli nějakých $a, b \in R$, pak už jsou $g_1$ a $g_2$ asociované.

## Eukleidovské a gaussovské obory

Vidíme tedy, že s největšími společnými děliteli bychom měli zacházet opatrně. Jak jsme již ale slíbili, za určitých podmínek můžeme na většinu z těchto obav zapomenout. Motto několika následujících stran zní: pokud umíme dělit s malým zbytkem, pak jsou ireducibilní prvky a prvočinitelé totéž a rozklad na ně je až na jednotky jednoznačný. Po příkladech, které jsme již dříve viděli, není příliš těžké si rozmyslet, co od takového dělení se zbytkem chtít – nějaké ohodnocení prvků oboru integrity, ve kterém lze libovolné nenulové prvky vydělit se zbytkem tak, aby ohodnocení zbytku bylo nižší než ohodnocení dělitele.

**Definice.** Obor integrity $R$ nazveme *eukleidovským oborem*, pokud existuje funkce $d\colon R \to \mathbb{N}_0$ splňující pro všechna $a, b \in R$, $b \neq 0$, následující podmínky:

(i) Platí $d(a) = 0$, právě když $a = 0$.

(ii) Platí $d(a) \leq d(ab)$.

(iii) Existují $q, r \in R$ taková, že $a = bq + r$ a zároveň $d(r) < d(b)$.

Funkci $d$ budeme říkat *eukleidovská funkce*.

Eukleidovská funkce nám tedy dává ohodnocení prvků oboru integrity, při kterém pouze nula dává nulu, násobky nejsou nikdy menší než dělitelé a umíme dělit se zbytkem tak, aby zbytek byl menší než dělitel.

**Cvičení(*) 27.** Podmínku (ii) bychom mohli v předchozí definici vynechat. Pokud totiž pro $R$ existuje funkce $d$ splňující (i) a (iii), pak už je funkce $\tilde{d}$ definovaná jako

$$\tilde{d}(a) = \min_{b \neq 0} d(ab)$$

eukleidovskou funkcí.

Nyní v několika krocích dokážeme, že v eukleidovském oboru jsou ireducibilní prvky prvočinitelé a že v nich lze jednoznačně rozkládat na prvočinitele. Začneme Bézoutovou identitou.

**Tvrzení.** (Bézoutova identita) *Budiž $R$ eukleidovský obor. Pro libovolná nenulová $a, b \in R$ pak existuje $g \in R$ takové, že*

(i) *$g$ je největší společný dělitel $a$, $b$,*

(ii) *prvky tvaru $xa + yb$ jsou právě násobky $g$ neboli $\{xa + yb : x, y \in R\} = \{xg : x \in R\}$.*

*Důkaz.* Pojmenujme $S = \{xa + yb : x, y \in R\}$ a nechť je $d$ eukleidovská funkce. Zvolme $g$ jako nenulový prvek $S$, pro který je hodnota $d(g)$ minimální ze všech nenulových $g \in S$. Tady využíváme, že hodnoty $d(x)$ (pro $x \neq 0$) jsou přirozená čísla – každá množina přirozených čísel má totiž minimum.

Nejprve ukážeme, že všechny prvky $S$ jsou násobky $g$. Nechť pro spor existuje nějaké $s \in S$ takové, že $g \nmid s$. Z definice eukleidovského oboru máme $q, r \in R$ taková, že $s = gq + r$ a zároveň $d(r) < d(g)$. Kdyby $r = 0$, znamenalo by to $g \mid s$, takže určitě $r \neq 0$. Nahlédněme také, že $r \in S$, neboť pokud $g = x_1a + y_1b$ a $s = x_2a + y_2b$, pak

$$r = s - gq = (x_2 - qx_1)a + (y_2 - qy_1)b \in S.$$

Získali jsme tedy nenulový prvek $S$, v němž funkce $d$ nabývá menší hodnoty než v $g$. To je spor, protože $g$ jsme zvolili tak, aby $d(g)$ bylo minimální.

Ukažme nyní, že $g$ je největší společný dělitel $a$, $b$. Víme již, že $g$ dělí všechny prvky $S$. Když ale zvolíme $x = 1$, $y = 0$, dostaneme $a \in S$, zatímco $x = 0$, $y = 1$ dá $b \in S$. Takže $g$ je jejich společný dělitel. Zároveň když je $m$ společný dělitel $a$, $b$, pak určitě i

$$m \mid x_1a + y_1b = g.$$

Ověřili jsme tedy, že $g$ je společný dělitel, jehož všichni společní dělitelé dělí, takže je to největší společný dělitel. □

**Důsledek.** *V eukleidovském oboru je každý ireducibilní prvek $p$ prvočinitelem.*

*Důkaz.* Mějme $a, b \in R$ taková, že $p \mid ab$. Pro spor předpokládejme, že $p$ nedělí $a$ ani $b$. Podle právě dokázaného tvrzení mají $a$, $p$ nějakého společného dělitele $g$. Ten může jako dělitel ireducibilního $p$ být buďto asociovaný s 1, nebo s $p$. Kdyby $p \parallel g$, pak by bylo i $p \mid a$, což (z předpokladu sporu) neplatí. Takže $g$ je asociováno s 1, tudíž BÚNO $g = 1$. Z Bézoutovy identity existují $x_1$, $y_1$ taková, že $x_1a + y_1p = 1$. Zcela analogicky je 1 největším společným dělitelem $b$, $p$, takže existují $x_2$, $y_2$ splňující $x_2b + y_2p = 1$. Když dvě získané rovnosti vynásobíme, dostaneme

$$(x_1a + y_1p)(x_2b + y_2p) = 1,$$
$$x_1x_2ab + x_1y_2ap + x_2y_1bp + y_1y_2p^2 = 1.$$

Předpokládáme $p \mid ab$, takže každý sčítanec na levé straně je násobkem $p$. Celá levá strana je tak násobkem $p$, takže jsme dostali $p \mid 1$, což je spor – ireducibilní prvek nemůže být ze své definice jednotkou. Náš předpoklad, že existují $a$, $b$ splňující $p \mid ab$ a zároveň $p \nmid a, b$, tak byl chybný, takže $p$ musí být prvočinitel. □

Víme už tedy, že všechny ireducibilní prvky jsou v eukleidovském oboru prvočinitelé. Tento výsledek ale ještě vylepšíme na zobecnění Základní věty aritmetiky – ukážeme, že prvky eukleidovského oboru lze „jednoznačně“ rozložit na součin ireducibilních prvků. Tato vlastnost není jen výsadou eukleidovských oborů, pročež má své vlastní označení.

**Definice.** Řekneme, že obor $R$ je *gaussovský*[18], pokud v něm lze každý nenulový prvek rozložit na součin ireducibilních prvků jednoznačně až na pořadí a asociovanost. Formálněji: každý prvek $a \in R$ se dá zapsat jako $a = u \cdot p_1 \cdots p_n$ pro nějaké ireducibilní prvky[19] $p_1, \ldots, p_n$ a jednotku $u$, a pokud jsou

$$a = u \cdot p_1 \cdots p_n = v \cdot q_1 \cdots q_m$$

dva takové rozklady na součin ireducibilních prvků, potom $n = m$ a posloupnost $q_1, \ldots, q_n$ se dá přeuspořádat na posloupnost $q'_1, \ldots, q'_n$ takovou, že $p_j \parallel q'_j$ pro $j = 1, 2, \ldots, n$.

[18] V angličtině se setkáme s označením *unique factorization domain*, často zkracováno jako *UFD*.

[19] Může být $n = 0$, v takovém případě je $a$ jednotka.

**Poznámka.** Když už máme rozklad na ireducibilní prvky, můžeme ho ještě mírně zkrášlit tím, že navzájem asociované ireducibilní prvky „sloučíme“ do jedné mocniny. Dostaneme tak

$$a = u \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n},$$

kde pro $i \neq j$ platí $p_i \nmid p_j$. V tomto zápisu je zřejmé, jak vypadají dělitelé $a$ – mají v rozkladu pouze ireducibilní prvky $p_1, \ldots, p_n$ (ne nutně všechny), přičemž exponent u $p_i$ je nanejvýš $\alpha_i$, a libovolnou jednotku.

**Cvičení(!) 28.** Nahlédni, že v gaussovském oboru musí

(i) každý ireducibilní prvek být prvočinitelem,

(ii) každé dva prvky mít největší společný dělitel.

K důkazu, že eukleidovské obory jsou gaussovské, se propracujeme v několika krocích. Nejprve ukážeme, že každý nenulový prvek lze zapsat jako *nějaký* součin ireducibilních prvků a jednotky. Posléze využijeme toho, že ireducibilní prvky jsou prvočinitelé, abychom ukázali, že každé dva takové rozklady jsou stejné až na pořadí a přenásobení ireducibilních prvků jednotkami.

**Lemma.** *Nechť je $R$ eukleidovský obor s eukleidovskou funkcí $d$. Pro nenulová $a, b \in R$ platí $d(a) = d(ab)$ právě tehdy, když je $b$ jednotka.*

*Důkaz.* Dokazujeme ekvivalenci, ukážeme tedy dva směry implikace. Nejprve nechť je $b$ jednotka. Potom existuje $c \in R$ tak, že $bc = 1$. Z vlastnosti (ii) máme $d(a) \leq d(ab)$, ale také

$$d(ab) \leq d(ab \cdot c) = d(a),$$

takže dohromady $d(a) = d(ab)$.

Nyní nechť naopak $d(a) = d(ab)$. Použijeme vlastnost (iii) na dvojici $a$, $ab$. To nám říká, že musí existovat $q, r \in R$ tak, že $a = abq + r$ a zároveň $d(r) < d(ab) = d(a)$. Z toho ale $a(1 - bq) = r$, takže $1 - bq \neq 0$ by vlastností (ii) znamenalo $d(a) \leq d(a(1 - bq)) = d(r)$, což je spor s $d(r) < d(a)$. Určitě tak musí být $1 - bq = 0$ neboli $bq = 1$, což už značí, že $b$ je jednotka. □

**Tvrzení.** *V eukleidovském oboru $R$ lze každé nenulové $a \in R$ zapsat jako součin jednotky a ireducibilních prvků.*

*Důkaz.* Nechť je $d$ eukleidovská funkce. Pokud je $a$ jednotka, pak tvrzení platí triviálně – prostě zapíšeme $a = a$, tzn. nepoužijeme v součinu žádné ireducibilní prvky. Nadále předpokládejme, že $a$ není jednotka.

Budeme postupovat silnou matematickou indukcí vzhledem k $d(a)$. To znamená, že budeme předpokládat, že tvrzení platí pro všechna $d(a) \leq n$, a dokážeme jeho platnost i pro $d(a) = n + 1$. Mějme tedy nějaké $a$ takové, že $d(a) = n + 1$ a rozlišme dva případy. Pokud je $a$ ireducibilní, pak máme vyhráno, protože potom $a = a$ je rozklad na součin jediného ireducibilního prvku. Pokud $a$ není ireducibilní, platí $a = bc$ pro nějaká $b, c \in R$, která nejsou jednotky. Z předcházejícího lemmatu tak platí

$$d(b) < d(bc) = d(a) = n + 1,$$

takže určitě $d(b) \leq n$. Obdobně $d(c) \leq n$. Z indukčního předpokladu se tedy $b$ i $c$ dají rozložit na součin ireducibilních prvků a jednotky. Máme tedy

$$b = u \cdot p_1 \cdots p_k \qquad \text{a} \qquad c = v \cdot q_1 \cdots q_\ell$$

pro nějaké jednotky $u$, $v$ a ireducibilní prvky $p_1, \ldots, p_k, q_1, \ldots, q_\ell$. Z toho pak máme rozklad

$$a = (uv) \cdot p_1 \cdots p_k \cdot q_1 \cdots q_\ell,$$

takže platnost tvrzení je pro dokázána pro $d(a) = n + 1$. Silnou indukcí je tak tvrzení dokázáno pro všechna nenulová $a \in R$. □

**Tvrzení.** *Každý eukleidovský obor $R$ je gaussovský.*

*Důkaz.* Víme už, že každý nenulový prvek $R$ lze rozložit na součin ireducibilních prvků a jednotky. Víme také, že všechny ireducibilní prvky v $R$ jsou prvočinitelé. Mějme tedy jednotky $u$, $v$, nezáporná celá čísla $m$, $n$ a ireducibilní prvky $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$, pro něž

$$u \cdot p_1 \cdots p_n = v \cdot q_1 \cdots q_m.$$

Ukážeme, že potom jsou tyto dva rozklady stejné až na pořadí činitelů a asociovanost.

BÚNO nechť $n \geq m$. Pokud nyní $n = 0$, pak máme v rozkladu na obou stranách jen jednotku a není co dokazovat. Jinak vezměme ireducibilní prvek $p_1$. Jedná se o prvočinitel, který dělí levou stranu, takže musí dělit i některý činitel v součinu na pravé straně. Nemůže být $p_1 \mid v$, protože pak by $p_1$ byla jednotka. Pro nějaké $j \in \{1, \ldots, m\}$ tedy $p_1 \mid q_j$. Jelikož $q_j$ je ireducibilní, každý jeho dělitel je buďto asociovaný s 1, nebo s $q_j$. Přitom $p_1$ není jednotka, takže už musí být $p_1$ a $q_j$ asociované prvky. Platí tedy $q_j = v_1 p_1$ pro nějakou jednotku $v_1$. Nyní tak můžeme zapsat $q_1' = q_j$ a rovnost dvou rozkladů pokrátit na

$$u \cdot p_2 \cdots p_n = (vv_1) \cdot q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$$

a proces opakovat: vezmeme $p_2$, to dělí nějaké $q_k$ na pravé straně, takže $q_2' = q_k$ a opět pokrátíme.

Takto pokračujeme, dokud nepokrátíme všechna $q_1, \ldots, q_m$ na pravé straně (předpokládáme $n \geq m$, takže nám nedojdou ireducibilní prvky na levé straně). Kdyby $n > m$, pak by nám nyní na levé straně zbyly nějaké ireducibilní činitele, které by ale dělili jednotku na pravé straně, což není možné. Určitě tedy $n = m$. Zároveň jsme v procesu krácení získali pořadí ireducibilních prvků $q_1', \ldots, q_n'$, které jsou asociované po řadě s $p_1, \ldots, p_n$. Tím máme dokázáno, že $R$ je gaussovský obor. □

Pozor! Tvrzení neplatí naopak: gaussovský obor vůbec nemusí být eukleidovský.

## Příklady eukleidovských oborů

Dokázali jsme spoustu vlastností eukleidovských oborů a několik jsme jich už viděli ($\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$). Eukleidovské obory nemusí být vždy jednoduché rozpoznat, protože obecně vůbec nevíme, jak by měla vypadat vhodná eukleidovská funkce. Ukážeme si proto alespoň několik příkladů. Budeme v nich volit takové funkce, které se chovají hezky k součinu prvků (ještě o něco hezčeji než jenom $d(a) \leq d(ab)$).

Nyní se podívejme na některé další obory, které dovedeme sestrojit v komplexních číslech. Zde může být dobrým tipem zvolit za eukleidovskou funkci normu definovanou jako $N(a) = a \cdot \overline{a}$. Ta totiž splňuje, že hodnoty 0 nabývá pouze v nule, a když navíc zvolíme obor tak, aby hodnoty normy byly celočíselné, pak už pro $b \neq 0$ platí $N(b) \geq 1$, takže i

$$N(ab) = N(a)N(b) \geq N(a) \cdot 1 = N(a).$$

Když tedy v takovémto oboru budeme chtít jako eukleidovskou funkci použít takto definovanou normu, stačí nám ověřit, že nabývá pouze celočíselných hodnot a že dovedeme dělit se zbytkem.

**Příklad.** Již jsme viděli, že $\mathbb{Z}$ a $\mathbb{Z}[i]$ jsou eukleidovské, neboť jsme v nich zprovoznili dělení se zbytkem. V $\mathbb{Z}$ jsme použili eukleidovskou funkci $d(a) = |a|$, v $\mathbb{Z}[i]$ posloužilo $d(a) = N(a)$.

**Příklad.** $\mathbb{Z}[\sqrt{-2}]$ je eukleidovský obor s normou jako eukleidovskou funkcí.

*Řešení.* Pro $x, y \in \mathbb{Z}$ vyjádříme normu jako $N(x + y\sqrt{-2}) = x^2 + 2y^2$, což je celé číslo. Ukažme tedy, jak budeme dělit se zbytkem. Mějme $a, b \in \mathbb{Z}[\sqrt{-2}]$, kde $b \neq 0$. Chceme zvolit $q \in \mathbb{Z}[\sqrt{-2}]$ tak, že

$$N(a - qb) = N(r) < N(b).$$

Vydělme $\frac{a}{b} = \frac{a\cdot\overline{b}}{N(b)} = x + y\sqrt{-2}$, kde $x, y \in \mathbb{Q}$, protože $\overline{b}$ je prvek $\mathbb{Z}[\sqrt{-2}]$, takže celý čitatel $a\overline{b}$ je prvek $\mathbb{Z}[\sqrt{-2}]$. Můžeme tedy využít multiplikativity normy a naši „cílovou" nerovnost ekvivalentně upravit na

$$N\left(\frac{a}{b} - q\right) < 1.$$

Nyní stačí zvolit $q = x_0 + y_0\sqrt{-2}$ tak, že zaokrouhlíme $x$, $y$ na nejbližší celé číslo (nižší či vyšší podle toho, které je blíž). Tím bude zaručeno $|x - x_0|, |y - y_0| \leq \frac{1}{2}$, což nám dá

$$N\left(\frac{a}{b} - q\right) = (x - x_0)^2 + 2(y - y_0)^2 \leq \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 \leq \frac{3}{4} < 1.$$

Tím už je dokázáno, že norma je eukleidovská funkce v oboru $\mathbb{Z}[\sqrt{-2}]$.

**Příklad.** Uvažme komplexní číslo $\alpha = \frac{1+i\sqrt{7}}{2}$, které splňuje $\alpha^2 = \alpha - 2$. Potom je obor $\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\}$ eukleidovský s normou jako eukleidovskou funkcí.

*Řešení.* Platí $\alpha + \overline{\alpha} = 1$ a $\alpha\overline{\alpha} = \frac{1-(-7)}{4} = 2$, takže pro $x, y \in \mathbb{Z}$ má prvek $x + y\alpha \in \mathbb{Z}[\alpha]$ normu

$$(x + y\alpha)(x + y\overline{\alpha}) = x^2 + xy \cdot (\alpha + \overline{\alpha}) + y^2 \cdot \alpha\overline{\alpha} = x^2 + xy + 2y^2,$$

což je celé číslo. Stejně jako v předchozím příkladu použijeme trik s dělením, takže budeme pro $\frac{a}{b} = x + y\alpha$, kde $x, y \in \mathbb{Q}$, hledat taková $x_0, y_0 \in \mathbb{Z}$, že

$$N\Big((x - x_0) + (y - y_0)\alpha\Big) < 1.$$

Na tento problém můžeme nahlížet geometricky. Nerovnice $x^2 + xy + 2y^2 < 1$ určuje v kartézské rovině vnitřek nějaké elipsy.[20] To, že odečítáme $x_0 + y_0\alpha$, odpovídá tomu, že se souřadnice nějakého zadaného $(x, y)$ snažíme posunout o celá čísla tak, aby výsledek spadl dovnitř této elipsy.

S tím už se lze vypořádat celkem jednoduše. Nejprve zaokrouhlíme $y$ na nejbližší celé číslo $y_0$. Tím bude rozdíl $y - y_0$ ležet mezi $-\frac{1}{2}$ a $\frac{1}{2}$. Když elipsu protneme s přímkou $y = \frac{1}{2}$, budou $x$-ové souřadnice průsečíků řešeními rovnice $x^2 + \frac{x}{2} - \frac{1}{2} = 0$. Těmi jsou $x_{1,2} = \frac{-\frac{1}{2} \pm \sqrt{\frac{1}{4} + 4\cdot\frac{1}{2}}}{2}$, takže tyto dva průsečíky jsou od sebe vzdáleny

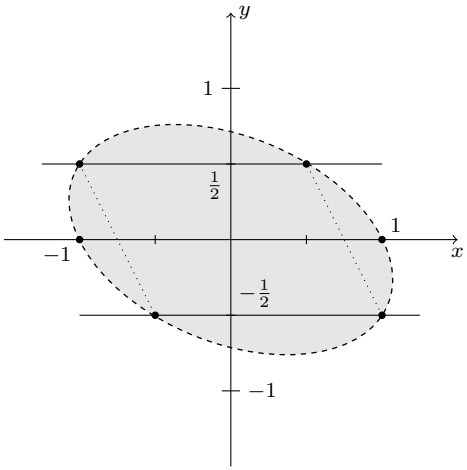
$$\sqrt{\frac{1}{4} + 4 \cdot \frac{1}{2}} = \sqrt{\frac{9}{4}} = \frac{3}{2} > 1.$$

Důležité je, že toto je ostře víc než 1. Na přímce $y = -\frac{1}{2}$ máme další dva průsečíky, středově souměrné podle počátku s prvními dvěma. Tyto čtyři průsečíky jsou vrcholy rovnoběžníku, který leží uvnitř této elipsy (vyjma vrcholů, ty leží na elipse), protože elipsa je konvexní útvar.[21] Tento rovnoběžník má výšku přesně 1 a šířku (délku příslušné strany) ostře větší než 1. Tyto vlastnosti už zaručují, že se do něj dovedeme trefit vhodnou volbou $x_0$, $y_0$ – nejprve se výběrem $y_0$ trefíme mezi $-\frac{1}{2}$ a $\frac{1}{2}$ a následně budeme schopni vybrat $x_0$, protože se trefujeme do intervalu delšího než 1.

Pro formální správnost postupu jenom musíme rovnoběžník o velmi malý kousek zmenšit, aby ležel v elipse celý, včetně vrcholů. Vrcholy leží přímo na elipse, takže jakkoliv malé zmenšení nám postačí. Je tedy zřejmé, že tohle dovedeme provést tak, abychom zachovali šířku větší než 1.

[20] Že tato nerovnice skutečně určuje elipsu, zde nebudeme dokazovat. Pokud si tedy lámeš hlavou nad tím, proč by tomu tak mělo být, prosíme Tě, abys nám to prostě věřil(a) :-).

[21] Je to totiž jenom splácnutá kružnice.




**Cvičení 29.** Z dřívějška už víme, že v $\mathbb{Z}[\sqrt{-3}]$ nejsou ireducibilní prvky vždy prvočinitelé, takže to určitě není eukleidovský obor. Rozmysli si, proč zde norma nevyhovuje jako eukleidovská funkce.

## K čemu nám je jednoznačný rozklad

Ukažme si konečně, k čemu je nám jednoznačný rozklad na ireducibilní prvky dobrý – umožňuje nám získávat užitečné informace z úpravy rovnice na součin.

**Definice.** Nechť je $R$ komutativní okruh. Řekneme, že prvky $a, b \in R$ jsou *nesoudělné*, pokud je 1 jejich největším společným dělitelem.

**Tvrzení.** (mocniny a nesoudělnost) *Nechť je $R$ gaussovský obor. Pokud pro nesoudělná $a, b \in R$, $c \in R$ a přirozené $k$ platí $ab = c^k$, pak už platí*

$$a = ud^k, \qquad b = ve^k,$$

*pro prvky $d, e \in R$ a jednotky $u$, $v$ splňující de $\parallel c$.*

*Důkaz.* Budiž $c = w \cdot p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ rozklad $c$ na součin ireducibilních prvků a jednotky a nechť jsou $p_1, \ldots, p_n$ navzájem neasociované. Potom má prvek $c^k$ rozklad

$$c^k = \left(w^k\right) \cdot p_1^{k\gamma_1} \cdots p_n^{k\gamma_n}.$$

Jelikož $a$, $b$ jsou nesoudělná, nemohou mít ve svých rozkladech žádné společné ireducibilní prvky. Každé $p_i$ se tak musí vyskytovat v rozkladu právě jednoho z $a$, $b$. Z jednoznačnosti rozkladu se v tomto rozkladu už musí vyskytovat v mocnině $p_i^{k\gamma_i}$. Pokud tedy $d$ zavedeme jako součin všech těch $p_i^{\gamma_i}$, pro která $p_i \mid a$, pak můžeme rozklad $a$ zapsat jako $a = ud^k$ pro nějakou jednotku $u$. Analogicky máme i $b = ve^k$. □

**Poznámka.** (schovávání jednotky do mocniny) Drobnou nepříjemností v používání tohoto tvrzení je jednotka, kterou může být mocnina přenásobená. Pokud má $R$ mnoho jednotek, může být poměrně namáhavé je vyzkoušet všechny, a pokud jich má dokonce nekonečně mnoho, jedná už se o podstatný problém, který je třeba řešit nějak „chytřeji“ než rozebráním všech možností. Často si ale lze ušetřit práci tím, že jednotku $u$ „BÚNO“ vložíme do mocniny $d^k$. Pokud totiž víme, že v $R$ lze *každá* jednotka vyjádřit jako $k$-tá mocnina, pak lze prostě vzít $u = u_0^k$ a následně $a = (u_0 d)^k$. Obecněji můžeme jednotky, které procházíme, zredukovat tak, abychom měli zastoupeny „všechny jednotky až na přenásobení $k$-tými mocninami jednotek“.

**Příklad.** Najdi všechna celočíselná řešení rovnice $x^2 = y^3 - 2$.

*Řešení.* Využijeme obor $\mathbb{Z}[\sqrt{-2}]$, o kterém již víme, že je eukleidovský, a tedy i gaussovský. Rovnost upravíme na

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

Rozmysleme si nyní, jaké společně dělitele mohou mít $x + \sqrt{-2}$ a $x - \sqrt{-2}$. Budiž $d$ nějaký jejich společný dělitel. Potom $d$ dělí i

$$(x + \sqrt{-2}) - (x - \sqrt{-2}) = 2\sqrt{-2}.$$

Když vezmeme normu, tak určitě $N(d) \mid N(2\sqrt{-2}) = 8$. Musí tedy být $N(d) \in \{1, 2, 4, 8\}$. Ukážeme, že $2 \nmid N(d)$, takže už $N(d) = 1$ a $d$ je tak jednotka. Nechť pro spor $2 \mid N(d)$. Vzhledem k $d \mid x \pm \sqrt{-2}$ pak už dostaneme (v $\mathbb{Z}$)

$$2 \mid N(x \pm \sqrt{-2}) = x^2 + 2 = y^3,$$

takže $y$ je sudé. Zároveň také $2 \mid x^2$, takže $x$ je také sudé. Jenže potom už jsou $x^2$ i $y^3$ násobky čtyř. Když se nyní na původní rovnici podíváme mod 4, dostaneme $0 \equiv 2 \pmod 4$, což je spor. Určitě $2 \nmid N(d)$, a $d$ je tedy jednotka.

Tímto jsme dokázali, že $x + \sqrt{-2}$ a $x - \sqrt{-2}$ jsou nesoudělná. Když nyní použijeme tvrzení, dostaneme, že $x + \sqrt{-2} = t^3$ pro nějaké $t \in \mathbb{Z}[\sqrt{-2}]$ – jednotku můžeme vložit do mocniny, protože jedinými jednotkami v $\mathbb{Z}[\sqrt{-2}]$ jsou 1 a $-1$, přičemž obě jsou třetími mocninami. Když tedy zapíšeme $t = a + b\sqrt{-2}$ pro $a, b \in \mathbb{Z}$, dostaneme

$$\begin{aligned} x + \sqrt{-2} = (a + b\sqrt{-2})^3 &= a^3 + 3a^2b\sqrt{-2} + 3a(b\sqrt{-2})^2 + (b\sqrt{-2})^3 = \\ &= a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2} = \\ &= \left(a^3 - 6ab^2\right) + \left(3a^2b - 2b^3\right)\sqrt{-2}. \end{aligned}$$

V tomto tvaru se naše rovnice v $\mathbb{Z}[\sqrt{-2}]$ skládá ze dvou rovnic v $\mathbb{Z}$. Když se podíváme jen na koeficienty imaginárních složek, máme rovnici $1 = b\left(3a^2 - 2b^2\right)$. Pravá strana je násobkem $b$, ale levá strana je 1, takže $b$ musí být jednotka, tedy 1 nebo $-1$. Z toho už si můžeme být jisti, že $b^2 = 1$. Upravíme tedy na $\pm 1 = 3a^2 - 2$. Rozlišme dva případy podle toho, jestli je na levé straně 1, nebo $-1$.

(i) Pokud $b = -1$, dostaneme rovnici $1 = 3a^2$. Tento případ tak nemá řešení, jelikož $3 \nmid 1$.

(ii) Pokud $b = 1$, obdržíme $3 = 3a^2$ neboli $a^2 = 1$. To znamená $a = \pm 1$. Když se v rovnici výše podíváme tentokrát na reálné složky, dostaneme

$$x = a\left(a^2 - 6b^2\right) = \pm 1 \cdot (1 - 6).$$

Řešeními tak mohou být pouze $x = \pm 5$. Snadno vyzkoušíme, že tyto hodnoty dávají řešení původní rovnice a oběma odpovídá $y = 3$.

Jedinými celočíselnými řešeními $x^2 = y^3 - 2$ jsou tedy $(x, y) = (\pm 5, 3)$.

Shrňme si, co náš postup obnášel. Nejprve jsme rovnici upravili na součin ve vhodném oboru, poté jsme se zabývali možnými společnými děliteli činitelů. Zde jsme měli štěstí a podařilo se nám vyloučit všechny až na jednotky – kdyby se toto nepodařilo, museli bychom rozebrat možné hodnoty největšího společného dělitele. Jakmile jsme si byli jisti, že máme součin *nesoudělných* činitelů, bylo již možno použít tvrzení, což nám s trochou vytrvalosti a rozebírání jednotek dalo jednodušší rovnice v $\mathbb{Z}$.

**Úloha 6.** Najdi všechna celočíselná řešení rovnice $x^2 = y^5 - 1$.

## Gaussova celá čísla pod drobnohledem

Vezměme nyní vše, co jsme si dokázali o eukleidovských a gaussovských oborech, a podívejme se důkladněji na $\mathbb{Z}[i]$ a jeho využití. Gaussova celá čísla, potažmo komplexní čísla vůbec jsme původně zavedli proto, abychom uměli rozkládat na součin výrazy jako $a^2 + b^2$. Nemělo by tedy příliš překvapit, že $\mathbb{Z}[i]$ nám přijde k užitku tam, kde najdeme nějaký součet dvou čtverců[22].

### Pythagorejské trojice

Jak ví každé školou povinné dítko, v pravoúhlém trojúhelníku je obsah čtverce nad přeponou roven součtu obsahů čtverců nad odvěsnami neboli

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

při obvyklém značení délek stran. Některá z těchto dítek si také možná pamatují, že jeden obzvláště hezký takový trojúhelník se pyšní délkami stran 3, 4 a 5, či možná znají trojúhelník $(5, 12, 13)$. Ta nejbystřejší pak dokonce vymyslí i to, že každý trojúhelník s délkami stran $2n + 1$, $2n^2 + 2n$, $2n^2 + 2n + 1$ je pravoúhlý. Takovémuto popisu však stále uniká spousta pravoúhlých trojúhelníků s celočíselnými délkami stran – pojďme je najít všechny.

**Definice.** Trojici $(a, b, c)$ přirozených čísel nazveme *pythagorejskou trojicí*, pokud $a^2 + b^2 = c^2$. Pythagorejskou trojici $(a, b, c)$ nazveme *primitivní*, pokud jsou $a$, $b$, $c$ nesoudělná.

Máme-li pythagorejskou trojici $(a, b, c)$ a $g$ je největší společný dělitel $a$, $b$, $c$, pak je $\left(\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right)$ primitivní pythagorejská trojice, takže libovolnou pythagorejskou trojici lze získat z nějaké primitivní přenásobením. Dále si všimněme, že když je $(a, b, c)$ primitivní pythagorejská trojice, tak už jsou $a$, $b$, $c$ i *po dvou* nesoudělná. Kdyby totiž např. $a$, $b$ byla soudělná, pak by nějaké prvočíslo $p$ dělilo obě z nich. Potom ale i

$$p \mid a^2 + b^2 = c^2,$$

takže nutně $p \mid c$, což znamená, že $(a, b, c)$ není primitivní.

Dále se podívejme na to, jak je to v primitivní pythagorejské trojici $(a, b, c)$ s paritou. Jelikož členy trojice jsou po dvou nesoudělné, určitě je nanejvýš jeden z nich sudý. Vzpomeňme si, že $x^2$ dává mod 4 zbytek 0, když je $x$ sudé, a zbytek 1, když je $x$ liché. Kdyby tedy $a$, $b$ i $c$ byla lichá čísla, dostaneme $1 + 1 \equiv 1 \pmod 4$, což není možné. Kdyby bylo $c$ sudé, dostaneme $1 + 1 \equiv 0 \pmod 4$, což také neplatí. Musí tedy být sudé jedno z $a$, $b$ – BÚNO nechť je $a$ liché a $b$ sudé.

Po této přípravě se konečně můžeme na rovnici $a^2 + b^2 = c^2$ podívat v $\mathbb{Z}[i]$ a rozložit levou stranu na

$$(a + bi)(a - bi) = c^2.$$

Podívejme se na společně dělitele závorek na levé straně. Když nějaké $d \in \mathbb{Z}[i]$ dělí obě $a \pm bi$, pak nutně dělí i čísla

$$2a = (a + bi) + (a - bi),$$
$$2b = i \cdot (a - bi) - i \cdot (a + bi).$$

Vzetím normy je $N(d)$ v celých číslech dělitelem $N(2a) = 4a^2$ a $N(2b) = 4b^2$. Obdobně díky $d \mid a + bi$ platí

$$N(d) \mid N(a + bi) = a^2 + b^2 = c^2,$$

[22] V kontextu teorie čísel míníme slovem čtverec druhou mocninu.

což je liché číslo, takže i $N(d)$ je liché. Z toho už je $N(d)$ společným dělitelem $a^2$ a $b^2$, což jsou nesoudělná čísla, takže už musí být $N(d) = 1$. V $\mathbb{Z}[i]$ jsou tedy $a + bi$, $a - bi$ nesoudělná.

Na rovnici tak můžeme hodit tvrzení o mocninách a nesoudělnosti. Pro nějaká $x, y \in \mathbb{Z}$ a jednotku $u \in \mathbb{Z}[i]$ tak máme $a+bi = u(x+yi)^2$. Všimni si, že zde nemůžeme jednotku „schovat“ do mocniny, protože např. $i$ je jednotka, kterou nelze vyjádřit jako druhou mocninu. Nahlédněme ale, že násobení jednotkami $u \in \{1, i, -1, -i\}$ nám může jenom prohazovat reálnou a imaginární složku či obracet jejich znaménka. Když se tedy domluvíme, že zanedbáme prohození $a$, $b$ a budeme je hledat pouze jako přirozená čísla, můžeme „BÚNO“ předpokládat $u = 1$. Potom už snadno dopočítáme

$$a + bi = (x + yi)^2 = (x^2 - y^2) + 2xyi,$$

takže (primitivní) pythagorejské trojice v jistém smyslu odpovídají čtvercům (druhým mocninám) v $\mathbb{Z}[i]$.[23] Aby nyní $a$, $b$ byla nenulová, budeme předpokládat, že $x$, $y$ jsou přirozená a navíc $x > y$. Dále dopočítáme

$$c^2 = N(a + bi) = N\left((x + yi)^2\right) = N(x + yi)^2 = (x^2 + y^2)^2,$$

takže $c = x^2 + y^2$.

Doplňme ještě pár podmínek pro $x$, $y$. Aby $a$, $b$ byla nesoudělná, musí i $x$, $y$ být nesoudělná. Kdyby navíc obě $x$, $y$ byla lichá, pak je $a = x^2 - y^2$ sudé, takže $a$, $b$ by byla soudělná, tedy musí *právě jedno* z $x$, $y$ být sudé. Obecnou (ne nutně primitivní) pythagorejskou trojici pak zpět z primitivní získáme přenásobením všech tří $a$, $b$, $c$ nějakým přirozeným $k$. Shrňme:

**Tvrzení.** (parametrizace pythagorejských trojic) *Je-li $(a, b, c)$ pythagorejská trojice, pak lze (po možné záměně $a$, $b$) vyjádřit*

$$a = k(x^2 - y^2), \qquad b = 2kxy, \qquad c = k(x^2 + y^2),$$

*kde $x$, $y$, $k$ jsou přirozená čísla, $x > y$, čísla $x$, $y$ jsou nesoudělná a právě jedno z nich je sudé.*

**Úloha 7.** Pokud přirozená čísla $a$, $b$, $c$ splňují $a^2 + b^2 = c^2$, pak je $\frac{1}{2}(c - a)(c - b)$ čtverec přirozeného čísla.

## Součty čtverců

Pythagorejské trojice byly odpovědí na otázku, kdy je součet čtverců opět čtvercem. Položme si ale obecnější otázku: která přirozená čísla umí být součtem dvou čtverců, tedy pro která $n$ lze vyjádřit $n = x^2 + y^2$ pro $x, y \in \mathbb{Z}$.

Jako dříve toto přeformulujeme pomocí $\mathbb{Z}[i]$. Výraz $x^2 + y^2$ je jenom norma $x + yi$, což můžeme zvolit zcela libovolně, takže nás zajímá, jaká přirozená čísla se vyskytují jako normy prvků $\mathbb{Z}[i]$. Dále si rozmysleme, že nám vesměs stačí zodpovědět, která přirozená čísla se vyskytují jako normy *prvočinitelů* v $\mathbb{Z}[i]$. Každý prvek $\mathbb{Z}[i]$ se totiž rozkládá (jednoznačně) na součin prvočinitelů a jednotky – když

$$x + iy = up_1 \cdots p_n,$$

kde $p_1, \ldots, p_n$ jsou nějací prvočinitelé a $u$ je jednotka, pak multiplikativitou normy

$$x^2 + y^2 = N(x + yi) = N(p_1) \cdots N(p_n).$$

Jakmile tedy budeme vědět, jaké hodnoty mohou mít normy prvočinitelů, dostaneme možné normy všech prvků $\mathbb{Z}[i]$ jejich vzájemným násobením.

**Lemma.** *Nechť je*[24] *$\pi \in \mathbb{Z}[i]$ prvočinitel. Potom pro nějaké prvočíslo $p \in \mathbb{Z}$ platí $\pi \mid p$.*

[23] Hezkou vizualizaci lze shlédnout v tomto videu (anglicky): *https://youtu.be/QJYmyhnaaek*.

[24] Řecké písmenko $\pi$ zde pro nás nemá nic společného s konstantou 3,14159 . . .

*Důkaz.* Rozložme přirozené číslo $N(\pi)$ na součin prvočísel $p_1 \cdots p_n$. Jelikož $N(\pi) = \pi \cdot \overline{\pi}$, platí $\pi \mid N(\pi) = p_1 \cdots p_n$. Předpokládáme ale, že $\pi$ je prvočinitel, takže když dělí součin, musí dělit i některého z činitelů. Pro nějaké $j \in \{1, \ldots, n\}$ tedy platí $\pi \mid p_j$, jak jsme chtěli. □

V důsledku tohoto lemmatu je norma každého prvočinitele rovna $p$ nebo $p^2$ pro nějaké prvočíslo $p$. Zároveň musí každé prvočíslo $p$ mít nějakého prvočinitele, který je dělí, takže se nám stačí podívat na to, jaké prvočinitele které prvočíslo „vyrábí".

Rozmysleme si také, že každému prvočíslu $p \in \mathbb{Z}$ takto přísluší buďto prvočinitelé s normou $p$, anebo prvočinitelé s normou $p^2$ – ne obojí. Kdybychom měli prvočinitele $\pi$, $\rho$ splňující $N(\pi) = p$, $N(\rho) = p^2$, plynulo by z toho

$$\pi \mid p \mid p^2 = \rho\overline{\rho}.$$

Z toho nutně $\pi \mid \rho$ nebo $\pi \mid \overline{\rho}$, BÚNO nechť $\pi \mid \rho$. Jenže $\rho$ je (jakožto prvočinitel) ireducibilní, takže už musí $\pi$ a $\rho$ být asociované neboli $\rho = u\pi$ pro nějakou jednotku $u$. Z toho $N(\rho) = N(u)N(\pi) = 1 \cdot p$, což je spor.

Stačí nám tedy zkoumat jenom to, která prvočísla $p$ lze vyjádřit jako normu, tzn. jako součet dvou čtverců. Zde nám pomůže podívat se na problém mod $p$.

**Tvrzení.** *Prvočíslo $p \in \mathbb{N}$ lze vyjádřit jako součet dvou čtverců, právě pokud má kongruence $x^2 + 1 \equiv 0 \pmod{p}$ řešení.*

*Důkaz.* Chceme dokázat ekvivalenci, dokažme tedy dva směry implikace. Nechť nejprve máme vyjádření $p = a^2 + b^2$. Kdyby $p \mid b$, pak už nutně musí platit i $p \mid a^2$, takže $p \mid a$, tudíž

$$p^2 \mid a^2 + b^2 = p,$$

což je spor. Když se tedy na $p = a^2 + b^2$ podíváme mod $p$, můžeme v kongruenci $a^2 + b^2 \equiv 0 \pmod{p}$ vydělit nenulovým $b^2$ a dostat $x^2 + 1 \equiv 0 \pmod{p}$, kde $x \equiv \frac{a}{b} \pmod{p}$.

Nechť naopak existuje celé číslo $x$ takové, že $p \mid x^2 + 1$. Ukážeme, že $p$ není v $\mathbb{Z}[i]$ prvočinitelem. Vskutku platí

$$p \mid (x + i)(x - i),$$

ale přitom zcela zřejmě $p \nmid x \pm i$, protože imaginární složka je $\pm 1$, což není násobek žádného prvočísla. Víme tedy, že $p$ není prvočinitel, nemůže tedy být ani ireducibilní. To znamená, že existují nějaká $\alpha, \beta \in \mathbb{Z}[i]$, z nichž ani jedno není jednotka, která splňují $\alpha\beta = p$. Obě normy $N(\alpha)$, $N(\beta)$ nyní dělí $N(p) = p^2$. Kdyby ale $N(\alpha)$ bylo $p^2$, značilo by to $N(\beta) = 1$, což nelze, neboť $\beta$ není jednotka. Určitě tedy $N(\alpha) = N(\beta) = p$, čímž jsme vyjádřili $p$ jako normu Gaussova celého čísla neboli jako součet dvou čtverců. □

Zbývá nám tedy zkoumat jen řešitelnost $x^2 \equiv -1 \pmod{p}$. To lze činit mnoha způsoby, my si zde ukážeme jeden kombinatorický argument.

**Tvrzení.** *Pro prvočíslo $p \in \mathbb{N}$ má kongruence $x^2 \equiv -1 \pmod{p}$ řešení, právě pokud $p = 2$ nebo $p \equiv 1 \pmod{4}$.*

*Důkaz.* Vypořádejme se nejprve s dvojkou jako se speciálním případem. Prvočíslo $p = 2$ dovedeme vyjádřit jako $2 = 1^2 + 1^2$a zároveň máme kongruenci $1^2 \equiv -1 \pmod{2}$, takže dokazované tvrzení platí.

Nadále tedy předpokládejme, že $p$ je liché. Provedeme následující trik: všech $p - 1$ nenulových zbytkových tříd mod $p$ rozdělíme do skupinek

$$\left\{x, -x, \frac{1}{x}, -\frac{1}{x}\right\}.$$

Pozor, nemusí se vždy jednat o čtveřičky, neboť pro vhodné $x$ mohou některé z výrazů $x$, $-x$, $\frac{1}{x}$, $-\frac{1}{x}$ být rovny – na tom bude důkaz založen. Rozmysleme si nejprve, že takto korektně rozdělíme

zbytkové třídy do skupinek, tedy že $x \equiv a$ nám vytvoří stejnou skupinku jako $x \equiv -a$ atp. To lze ověřit buďto projitím všech možností, anebo si prostě stačí rozmyslet, jak spolu interagují úpravy $x \mapsto -x$ a $x \mapsto \frac{1}{x}$.

Vytvořili jsme tedy skupinky a každá zbytková třída leží jednoznačně v jedné z nich. Očekávali bychom, že „typicky" bude mít skupinka čtyři prvky. Podívejme se tedy na to, jak mohou vypadat skupinky s méně prvky. Protože nezáleží, od kterého prvku $x$ skupinku vytváříme, budeme BÚNO zkoumat, kdy je $x$ totožné s dalším výrazem. Jelikož je $p$ liché, nemůže nám nastat $x \equiv -x$, neboť kongruenci $2x \equiv 0 \pmod{p}$ splňuje jenom $x \equiv 0$. Každá skupinka má tedy aspoň 2 prvky. Kdyby nastalo $x \equiv \frac{1}{x}$, máme z toho kongruenci

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

což znamená buďto $x \equiv 1$, nebo $x \equiv -1$. Toto nám tedy nastává pouze ve dvouprvkové skupince $\{1, -1\}$. Naproti tomu $x \equiv -\frac{1}{x}$ by nám vedlo na kongruenci $x^2 \equiv -1 \pmod{p}$, což nás přesně zajímá. Zároveň bychom tím dostali dvouprvkovou skupinku, neboť potom i $-x \equiv \frac{1}{x}$. Také si povšimněme, že toto by nám dalo jenom jednu dvouprvkovou skupinku, protože když už nějaké $c$ splňuje $c^2 \equiv -1$, pak pro libovolné $x^2 \equiv -1$ můžeme rozložit

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

tedy $x \equiv \pm c \pmod{p}$.

Shrňme: $p-1$ zbytkových tříd se nám dělí do skupinek. Vždy máme dvouprvkovou skupinku $\{1, -1\}$, následně se *může* vyskytnout nanejvýš jedna další dvouprvková skupinka a všechny ostatní skupinky jsou čtyřprvkové. Pokud tedy tato druhá dvouprvková skupinka existuje, dává celkový počet prvků rozdělených do skupinek mod 4 zbytek $2 + 2 \equiv 0$ neboli $p \equiv 1 \pmod{4}$. Obdobně když tato druhá dvouprvková skupinka neexistuje, dává $p-1$ zbytek 2 mod 4. Nicméně tato druhá dvouprvková skupinka existuje právě tehdy, když má $x^2 \equiv -1 \pmod{p}$ řešení. Tím je důkaz hotov. □

S tímto tvrzením je naše lopota završena. Shrňme, jak to tedy je s prvočiniteli a s normami v $\mathbb{Z}[i]$.

**Věta.** *Prvočinitelé v $\mathbb{Z}[i]$ jsou dvou druhů:*

(i) *Prvky s prvočíselnou normou $p = 2$ nebo $p \equiv 1 \pmod{4}$, např. $1 + i$, $2 - i$, $-2 - 3i$ atp.*

(ii) *Prvočísla $p \equiv 3 \pmod{4}$ a jejich asociované prvky, např. 3, $-7$, $11i$ atp. Jejich norma je pak $p^2$.*

Jelikož norma obecného Gaussova celého čísla je jenom součin norem prvočinitelů, plyne z tohoto, že normy nabývají těch hodnot, které dostaneme násobením dvojky, prvočísel tvaru $4k+1$ a druhých mocnin prvočísel tvaru $4k+3$. Jinými slovy:

**Důsledek.** (čísla tvaru $x^2 + y^2$) *Ve tvaru $n = x^2 + y^2$ se dají vyjádřit právě ta přirozená čísla $n$, v jejichž prvočíselném rozkladu se všechna prvočísla tvaru $4k+3$ vyskytují v sudých mocninách.*

Obecně bychom si z tohoto měli odnést, že vyjadřování ve tvaru $n = x^2 + y^2$ je spjato s rozkladem $n$ na prvočísla, resp. s rozkladem $x + yi$ na prvočinitele. Zkus si to vyzkoušet na následujících cvičeních.

**Cvičení 30.** Nechť je $p \equiv 3 \pmod{4}$ prvočíslo. Pro $a, b \in \mathbb{Z}$ pak platí, že když $p \mid a^2 + b^2$, pak i $p \mid a, b$.

**Cvičení 31.** Nechť je $p = a^2 + b^2 = c^2 + d^2$ prvočíslo. Pak už jsou dvojice $(a, b)$ a $(c, d)$ až na pořadí a změnu znamének stejné, tzn. $\{|a|, |b|\} = \{|c|, |d|\}$.

**Cvičení 32.** Nechť je $\pi \in \mathbb{Z}[i]$ prvočinitel. Pokud $N(\pi) = 2$, pak jsou $\pi$, $\overline{\pi}$ asociované, stejně tak pokud je $N(\pi) = p^2$ pro prvočíslo $p \equiv 3 \pmod 4$. Naopak pokud $N(\pi) = p \equiv 1 \pmod 4$, pak $\pi$, $\overline{\pi}$ nejsou asociované.

**Úloha 8.** Najdi všechna celočíselná řešení rovnice $4xy - x - y = z^2$.

**Úloha 9.** Najdi všechna celočíselná řešení rovnice $x^4 = 4 + y^2 + z^2$.

**Úloha 10.** Dokaž, že rovnice $3^n = x^2 + y^2 + 1$ má nekonečně mnoho řešení $(n, x, y)$ v přirozených číslech.

**Úloha 11.** Najdi všechna celočíselná řešení rovnice $x^2 = y^3 + 7$.

**Úloha 12.** Najdi všechna celočíselná řešení rovnice $x^7 + 7 = y^2$.

**Úloha 13.** Najdi všechna celočíselná řešení rovnice $x^3 - x^2 + 8 = y^2$.

## Závěr

První díl tímto došel svého konce. Víme již, proč funguje prvočíselný rozklad, že dobrou cestou k jednoznačnému rozkladu v komutativních okruzích je dělení se zbytkem i že vyzbrojeni Gaussovými celými čísly se nemusíme zaleknout součtů čtverců. Děkujeme Ti, že ses dočetl(a) až sem. V příštím díle si opět rozšíříme svůj katalog okruhů o pár nových kousků, podíváme se na zub jednotkám v podobě Pellovy rovnice a rozmyslíme si, jak modulit v roztodivných okruzích.

Do té doby na viděnou a hodně zdaru s úlohami první soutěžní série!

### Návody ke cvičením

**1.** Vždy si vše rozepiš definicí dělitelnosti.

**2.** Použij vlastnost (ii) dělitelnosti prvně z $a$ do $c$ přes $b$ a poté naopak.

**3.** Použij indukci.

**4.** Rozlož $(x - 4)(x + 4) = y^3$. Pro liché $x$ použij tvrzení o nesoudělnosti a mocninách. Pro sudé $x$ už musí $x$ i $y$ být násobek čtyř, vhodnou úpravou získáš rovnici, kterou jsme již viděli.

**5.** Rozepiš z definice kongruence. Neboj se sčítat/odečítat dělitelnosti. Všimni si také, že (i) a (ii) jsou jenom speciální případy (iii) a (iv).

**6.** (i) Rozepiš z definice kongruence. (ii) Vytkni největšího společného dělitele.

**7.** Zkus druhou mocninu 5, není to už nějaký hezký zbytek? Pokud Ti nepřijde dostatečně hezký, zkus čtvrtou mocninu.

**8.** Spočti $N \pmod 2$, $\pmod{10}$, $\pmod 7$.

**10.** Znovu zlomek rozšiř číslem sdruženým ke jmenovateli. Alternativně můžeš zkusit zapsat $12-6i$ jako $(9 + 3i) \cdot (a + bi)$ a vyřešit soustavu rovnic.

**12.** Využij definici dělitelnosti a multiplikativity normy.

**13.** No, co ta norma?

**14.** Pokud existují dvě různé nuly, co je jejich součtem?

**15.** Roznásob $(1+1)(a+b)$ dvěma různými způsoby.

**16.** Využij $0 = 0 + 0$.

**17.** Ukaž, že když $0 = 1$, pak už $0 = a$ pro každé $a \in R$.

**25.** Uvaž $p = ab$ a využij definici prvočinitele.

**27.** Nechť $\tilde{d}(b) = d(bc)$, pak využij podmínku (iii) na dvojici $(a, bc)$.

**28.** Použij jednoznačný rozklad.

**32.** Vezmi dělitelnost $\overline{\pi} \mid \pi$ a rozšiř ji na $p \mid \pi^2$.

## Návody k úlohám

**1.** Eukleidův algoritmus. Nelam si hlavu s tím, aby úpravy nutně snižovaly hodnotu pro každé $n$, prostě to „zmenšuj“ jako výraz.

**2.** Ukaž nejprve, že i $x + y - 1 \mid 2xy$.

**3.** Vypořádej se s možnými společnými děliteli jednotlivých činitelů – není jich mnoho.

**4.** Rozlož $p^2 + 5pq + 4q^2 = (p+q)(p+4q)$. Pro $p \neq q$ je NSD závorek buďto 1, nebo 3. Připrav se na rozebírání případů.

**5.** Rozlož v $\mathbb{Z}[i]$ a podívej se na možné společné dělitele činitelů. Pomůže Ti rozmyslet si, že $x$ nemůže být liché – využij $x^2 \equiv 1 \pmod 4$.

**6.** Rozlož v $\mathbb{Z}[i]$. Nesoudělnost závorek ukaž s pomocí mod 4.

**7.** Dosaď parametrizaci pythagorejských trojic.

**8.** Uprav levou stranu na součin a koukni se, co dostaneš na pravé.

**9.** Převeď čtyřku, rozlož na součin a najdi zakázaného dělitele. Pokud je $x$ sudé, vyděl nejprve celou rovnici čtyřmi.

**10.** Vol $n = 2^k$ a rozlož $3^{2^k} - 1$ na součin.

**11.** Přičti jedničku a najdi zakázaného dělitele.

**12.** Nahlédni, že $x$ je liché, přičti 121 a najdi zakázaného dělitele.

**13.** Až vyloučíš $2 \mid x$, přičti $x^2$ a najdi zakázaného dělitele.

## Řesení cvičení

**1.** (i) Platí $a = 1 \cdot a$, $0 = a \cdot 0$.

(ii) Máme $b = ka$, $c = \ell b$, takže $c = (k\ell)a$. Obdobně se dokáží (iii) až (v).

(vi) Pokud $a = 0$, pak už i $b = 0$, neboť jen nula je násobkem nuly. Dále nechť $a, b \neq 0$. Když $b = ka$, $a = \ell a$, dostaneme $a = k\ell a$, tedy $1 = k\ell$, takže $|k| = |\ell| = 1$, z čehož už $|a| = |b|$.

**2.** Stručně: máme $a \mid b$ a zároveň $b \mid c$, takže $a \mid c$. Analogicky $c \mid a$, takže $a \parallel c$.

**3.** (i) Indukujeme podle $n$. Pro $n = 2$ se jedná o definici ireducibility. Dále použijeme definici ireducibilního prvku na $q = (a_1 a_2 \cdots a_{n-1})a_n$. Nyní je jednou možností, že $a_n$ je jednotka a $\pm(a_1 a_2 \cdots a_{n-1}) = q$, pak jsme hotovi z indukčního předpokladu. Pokud by naopak $(a_1 a_2 \cdots a_{n-1})$ byla jednotka, tak všechna $a_i$ jsou pro $i \leq n-1$ jednotky.

(ii) Velmi podobně jako (i).

**4.** Jak už víme z návodu, rozebereme si dva případy. Pokud $d \mid x - 4$, $d \mid x + 4$, pak i $d \mid 8$. Pokud je $x$ liché, jsou však oba výrazy také liché, takže můžeme použít tvrzení o nesoudělnosti a mocninách (jelikož víme, že $\pm 1$ jsou třetí mocniny, můžeme je „schovat“ do mocniny). $x - 4 = a^3$, $x + 4 = b^3$ neboli $(b-a)(a^2 + ab + b^2) = b^3 - a^3 = 8$. Jelikož druhá závorka je vždy kladná ($a^2$ nebo $b^2$ je v absolutní hodnotě vetší roven $ab$). Tudíž stačí vyzkoušet pouze kladné dělitele $b - a$.

Z našich čtyř možností má pouze jediná celočíselné řešení. A to ta, když $(b-a)=2$ s řešením $(a,b)=(0,2),(-2,0)$. Jelikož by nám však z těchto $a$, $b$ vyšlo sudé $x$, můžeme i tuto dvojici vyloučit.

Informaci z návodu lehce ověříme. Díky tomu, že můžeme čísla zapsat ve tvaru $x=4x'$ a $y=4y'$ získáváme $x'^2=4y'^3+1$ neboli $(x'-1)(x'+1)=4y'^3$. Jelikož je NSD těchto dvou závorek nanejvýš 2 a zároveň je pravá strana sudá, je to právě číslo 2. Potom už můžeme zase použít naše známé tvrzení o nesoudělnosti a získáme dvě rovnice. $x'-1=2a^3$ a $x'+1=2b^3$. Použijeme známý trik z jejich odečtením z čehož získáme $(b-a)(a^2+ab+b^2)=b^3-a^3=1$. Jak už víme z minulého případu, stačí nám rozebrat jen jedna možnost a to ta, kde jsou obě závorky na levé straně rovny 1. To nám dá dvojice $(a,b)=(0,1),(-1,0)$.

Celkově máme tedy dvojice původních $(x,y)=(4,0)$, $(-4,0)$.

**5.** (i) $n \mid a-b=a+k-b-k$. (ii) $n \mid a-b$ , tedy i $n \mid k\cdot(a-b)$.

(iii) $n \mid (a-b)+(c-d)=(a+c)-(b+d)$. (iv) $n \mid (a-b)\cdot c-(c-d)\cdot b=ac-bd$.

**6.** (i) Máme tedy $n \mid c(a-b)$. Jelikož máme jednoznačný rozklad a $n$ s $c$ jsou nesoudělné, tak také platí, že $n \mid a-b$.

(ii) V obecné variantě si označme $g=(n,c)$, potom $n=gu$ a $c=gv$ a $n\cdot k=c\cdot(a-b)$. Po dosazení $guk=gv\cdot(a-b)$ neboli $uk=v(a-b)$, tedy i $\frac{n}{(n,c)} \mid a-b$.

**7.** Platí $5^2=25\equiv -1$, tedy $5^{20}=(5^2)^{10}\equiv(-1)^{10}\equiv 1 \pmod{26}$.

**8.** Jak už jsme si řekli, stačí si vybrat jen vhodné reprezentanty. První tedy $N$ modulo 2. $N=22\cdot 31+11\cdot 17+13\cdot 19\equiv 0\cdot 1+1\cdot 1+1\cdot 1\equiv 0 \pmod 2$. Stejně tak to uděláme modulo 10. $22\cdot 31+11\cdot 17+13\cdot 19\equiv 2\cdot 1+1\cdot -3+3\cdot -1\equiv 6 \pmod{10}$. A poslední modulo, které musíme prozkoumat je modulo 7, tedy $22\cdot 31+11\cdot 17+13\cdot 19\equiv 3\cdot -3+4\cdot 3+-1\cdot -2\equiv 5 \pmod 7$.

**9.** Jednou možností je prostě to vyzkoušet pro $x=0,1,2,3$. Alternativně můžeme nahlédnout $(2n)^2=4\cdot n^2$, zatímco $(2n+1)^2=4\cdot(n^2+n)+1$.

**10.** $12-6i=(9+3i)(1-i)$, takže ano.

**11.** Přirozené číslo lze vyjádřit jako $x^2+y^2$, právě když je normou nějakého Gaussova čísla. Máme $m=N(\alpha)$, $n=N(\beta)$, takže multiplikativita normy nám snadno dá $mn=N(\alpha)N(\beta)=N(\alpha\beta)$.

**12.** Z definice máme $\alpha k=\beta$. Podívejme se, jak vypadají normy těchto čísel: $N(\alpha)N(k)=N(\alpha k)=N(\beta)$. Tím pádem $N(\alpha) \mid N(\beta)$. Dělitelnost norem však není postačující k dělitelnosti samotných čísel: kupříkladu $N(2+i) \mid N(3+i)$, ale $2+i \nmid 3+i$.

**13.** Stačí se nám tedy podívat na normu: $N(3-i)=10 \nmid 205=N(14-3i)$. Jelikož se nedělí normy, nemůžou se dělit ani odpovídající Gaussova čísla.

**14.** Nechť existují dva prvky 0, $0'$ splňující $0+a=a=0'+a$ pro každé $a$. Dosazením $a=0'$ máme $0+0'=0'$, zároveň ale dosazením $a=0$ máme $0'+0=0$. Dohromady tak $0'=0$.

Analogicky pokud máme dvě jedničky 1, $1'$, pak dostaneme $1'=1\cdot 1'=1'\cdot 1=1$.

**15.** Uvažme $(1+1)(a+b)$. Když roznásobíme nejprve pravou závorku, dostaneme

$$(1+1)(a+b)=(1+1)a+(1+1)b=a+a+b+b.$$

Když naopak roznásobíme nejprve levou závorku, dostaneme

$$(1+1)(a+b)=1(a+b)+1(a+b)=a+b+a+b.$$

Dohromady taky $a+a+b+b=a+b+a+b$ neboli $a+b=b+a$.

**16.** Využijeme $0=0+0$ a distributivity násobení. Dostaneme

$$0\cdot a=(0+0)a=0\cdot a+0\cdot a,$$

takže odečtením $0 \cdot a$ z obou stran dostaneme $0 = 0 \cdot a$.

**17.** Pro každé $a \in R$ je $0 \cdot a = 0$, zatímco $1 \cdot a = a$. Kdyby tedy platilo $0 = 1$, pak dohromady $0 = 0 \cdot a = 1 \cdot a = a$. Takže každý prvek $R$ je nula neboli $R$ má jen jeden prvek.

**19.** (i) Všechny tyto okruhy jsou podmnožinami $\mathbb{C}$, takže stačí ukázat, že $\mathbb{C}$ je oborem integrity. V $\mathbb{C}$ umíme dělit nenulovými prvky, takže kdyby pro $a, b \in \mathbb{C}$ platilo $ab = 0$ a zároveň $a, b \neq 0$, dostaneme $a = \frac{ab}{b} = \frac{0}{b} = 0$, což je spor. Z toho je $\mathbb{C}$ obor integrity, takže i $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ jsou obory integrity.

(ii) Stejně jako v předchozím odstavci jsou $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ i $\mathbb{Z}\left[\frac{1}{2}\right]$ podmnožinami $\mathbb{C}$ (a jejich sčítání a násobení je jen zúžení sčítání a násobení v $\mathbb{C}$), takže už musí být obory integrity.

(iii) Triviální okruh je oborem integrity. Definice oboru integrity hovoří o tom, že pro $ab = 0$ musí být $a = 0$ nebo $b = 0$. V triviálním okruhu je ale každý prvek roven 0, takže závěr dokazovaného tvrzení platí automaticky.

(iv) Když $n = 1$, pak máme triviální okruh $\mathbb{Z}_1$, tedy obor integrity. Když je $n$ složené číslo, můžeme ho zapsat jako $n = ab$ pro nějaká $a, b > 1$, načež $ab \equiv n \pmod{n}$, ale $a, b \not\equiv 0 \pmod{n}$, takže $\mathbb{Z}_n$ není obor integrity. Konečně když $n = p$ je prvočíslo, tak $ab \equiv 0 \pmod{p}$ znamená $p \mid ab$, takže $p \mid a$ nebo $p \mid b$, což znamená $a \equiv 0$ nebo $b \equiv 0 \pmod{p}$, takže $\mathbb{Z}_p$ je obor integrity. V souhrnu je tedy $\mathbb{Z}_n$ obor integrity, právě když $n$ není složené.

(v) Pro $|X| = 0$ je má $\mathcal{P}(X)$ jediná prvek $\emptyset$, takže je to triviální okruh. Pro $|X| = 1$ máme $\mathcal{P}(X) = \{\emptyset, X\}$. Pro $A, B \in \mathcal{P}(X)$ obě různé od $\emptyset$ tedy nutně $A \cap B = X \cap X = X \neq \emptyset$, takže $\mathcal{P}(X)$ je obor integrity. Pro $|X| \geq 2$ zvolme dva různé prvky $a, b \in X$. Obě množiny $\{a\}, \{b\}$ jsou neprázdné, ale přitom $\{a\} \cap \{b\} = \emptyset$, takže $\mathcal{P}(X)$ není obor integrity. V souhrnu je tedy $\mathcal{P}(X)$ obor integrity, právě pokud $|X| \leq 1$.

(vi) Když se podíváme na tabulku násobení v okruhu $T$, ověříme projitím všech jejích políček, že jediné součiny, které dávají výsledek 0, jsou ty, v nichž je 0 jedním z činitelů. Tedy $T$ je obor integrity.

**20.** Z definice dělitelnosti $a \mid b$ znamená, že $b = ka$ pro nějaké $k$. Obdobně $c = \ell a$. Z toho už $bd + cd = (kd + \ell e)a$ neboli $a \mid bd + cd$.

**21.** Když $B \subseteq A$, tak vskutku $B = A \cap B$. Když $B = A \cap C$ pro nějakou $C$, tak z definice průniku musí být $B \subseteq A$.

**22.** (i) $\{1, -1\}$.

(ii) V těchto okruzích lze dělit každým nenulovým prvkem, takže $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.

(iii) Jsou to přesně prvky s normou 1 (v $\mathbb{Z}[\omega]$ definujeme normu pro $\alpha = a + b\omega$ jako $N(\alpha) = \alpha\overline{\alpha} = a^2 + ab + b^2$). Tedy jednotkami jsou $\{\pm 1, \pm i\}$, resp. $\{\pm 1, \pm\omega, \pm\omega^2\}$.

(iv) Pokud je čitatel násobkem nějakého lichého prvočísla, pak se ho násobením „nezbavíme“ a nevyrobíme tak jedničku. Zbývají tedy jen plus nebo mínus mocniny dvojky (včetně těch se zápornými exponenty). Ty ale jednotkami jsou, neboť $\pm 2^a \cdot (\pm 2^{-a}) = 1$. Množinou všech jednotek v $\mathbb{Z}\left[\frac{1}{2}\right]$ je tedy $\{\pm 2^a : a \in \mathbb{Z}\}$.

(v) Jedinou jednotkou je $X$. Podle dřívějšího cvičení již víme, že aby nějaká podmnožina $A \subseteq X$ dělila $X$, musí být její nadmnožinou, což znamená $A = X$.

**23.** Víme již, že když $R$ není triviální, pak $0 \neq 1$. Potom kdyby $0 \mid 1$, pak pro nějaké $a \in R$ platí $1 = 0 \cdot a = 0$, což je spor.

**24.** Máme dokázat ekvivalenci, ukážeme tedy dvě implikace. Nechť nejprve $a = ub$. Potom zároveň $a = bv$, kde $u$, $v$ jsou jednotky splňující $uv = 1$. To znamená $a \mid b$, $b \mid a$. Nyní nechť naopak $a \parallel b$. To znamená, že pro nějaká $u$, $v$ platí $au = b$ a zároveň $a = bv$. Dohromady tedy $a = bv = auv$, takže $1 = uv$ neboli je $u$ jednotka, jak jsme chtěli.

**25.** Budiž $p$ prvočinitel a nechť $p = ab$. Potom $p \mid ab$, takže z definice prvočinitele máme $p \mid a$ nebo $p \mid b$. BÚNO předpokládejme $p \mid a$. Zároveň ale $a \mid p$, takže $a$, $p$ jsou asociované, tedy $p = au$ pro nějakou jednotku $u$, takže už $au = ab$ neboli $u = b$, a $b$ je tak jednotka.

**26.** Z definice je největší společný dělitel společný dělitel a zároveň každý společný dělitel dělí největšího společného dělitele. To znamená $g_1 \mid g_2$ a zároveň $g_2 \mid g_1$, takže $g_1$ a $g_2$ jsou asociované.

**27.** Je zřejmé, že $\tilde{d}$ splňuje (i). Abychom nahlédli (ii), všimněme si, že $\tilde{d}(a)$ je minimum z $d$ na množině nenulových násobků $a$. Ale každý násobek $ab$ je i násobek $a$, takže $\tilde{d}(ab)$ je jenom minimum z nějaké podmnožiny nenulových násobků $a$. Minimum podmnožiny je větší nebo rovno minimu celé množiny, takže $\tilde{d}(a) \leq \tilde{d}(ab)$.

Zaměřme se nyní na (iii). Jsou dána $a, b \in R$. Z definice $\tilde{d}$ existuje $c \in R$ takové, že $\tilde{d}(b) = d(bc)$. Nyní s funkcí $d$ využijeme vlastnost (iii) na $(a, bc)$. To nám dá $a = b(cq) + r$ pro $d(r) < d(bc)$. Přitom ale z definice $\tilde{d}(r) \leq d(r \cdot 1)$, takže $\tilde{d}(r) \leq d(r) < d(bc) = \tilde{d}(b)$.

**28.** (i) Ireducibilní prvek $p$ dělí nenulový prvek $c$ právě tehdy, když se $p$ nachází (až na asociovanost) v rozkladu $c$ na součin ireducibilních prvků. Když tedy $p$ nedělí ani $a$, ani $b$, pak se nevyskytuje ani v jednom z jejich rozkladů, takže se nevyskytuje ani v rozkladu $ab$. To už značí, že když $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

(ii) Zapišme zkrášlené rozklady prvků $a$, $b$, přičemž použijme pro každou „rodinku“ asociovaných ireducibilních prvků v obou rozkladech jen jednoho zástupce. Můžeme tedy napsat

$$a = u \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \qquad b = v \cdot p_1^{\beta_1} \cdots p_n^{\beta_n},$$

kde $u$, $v$ jsou jednotky, $p_1, \ldots, p_n$ jsou navzájem neasociované ireducibilní prvky a exponenty $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ jsou nezáporná celá čísla – může se jednat o nuly, pokud se příslušný ireducibilní prvek vůbec nenachází v rozkladu. Nyní už je zjevné, že

$$g = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_n^{\min\{\alpha_n, \beta_n\}}$$

je největším společným dělitelem $a$, $b$. Tento prvek totiž určitě dělí obě $a$, $b$ (má menší nebo rovné exponenty) a zároveň každý každý společný dělitel dělí $g$ (nemůže mít větší žádný exponent).

**29.** Analogicky s důkazem eukleidovskosti $\mathbb{Z}[\sqrt{-2}]$ bychom se dostali na ekvivalentní formulaci: pro daná $x, y \in \mathbb{Q}$ najít $x_0, y_0 \in \mathbb{Z}$ takové, že $(x - x_0)^2 + 3(y - y_0)^2 < 1$. Pro $x = y = \frac{1}{2}$ však taková $x_0$, $y_0$ neexistují.

**30.** Platí $p \mid (a + bi)(a - bi)$ a $p$ je prvočinitel, takže už dělí jedno z $a \pm bi$, tudíž dělí obě $a$, $b$.

**31.** Nechť $\pi = a + bi$, $\rho = c + di$. Jelikož je jejich norma prvočíslo, musí to být prvočinitelé. Máme $\pi\overline{\pi} = \rho\overline{\rho}$. Levá strana je násobkem $\pi$, takže i $\pi \mid \rho\overline{\rho}$. To znamená, že buďto $\pi \mid \rho$, načež $\pi \parallel \rho$, nebo $\pi \mid \overline{\rho}$, načež $\pi \parallel \overline{\rho}$. Jenže násobení jednotkou jenom prohazuje reálnou a imaginární složku a mění jejich znaménka, zatímco komplexní sdružení jenom mění znaménko imaginární složky. To znamená, že složky $\pi$, $\rho$ jsou tak stejné až na prohození a změny znamének.

**32.** Pro $\pi \parallel p \equiv 3 \pmod 4$ je tvrzení zřejmé. Dále jsou prvočinitelé normy 2 jenom $1 + i$ a asociované prvky. Přitom $1 + i = (1 - i) \cdot i$, takže tyto dva komplexně sdružené prvky jsou asociované.

Mějme nyní $\pi = a + bi$ a $N(\pi) = p \equiv 1 \pmod 4$. Kdyby $\pi \parallel \overline{\pi}$, pak $\overline{\pi} \mid \pi$, z čehož rozšířením nutně i

$$p = \pi\overline{\pi} \mid \pi^2 = (a^2 - b^2) + 2abi.$$

Jenže $a$, $b$ musí být nesoudělná, takže $a$ i $b$ je nesoudělné s $a^2 + b^2 = p$. Z lichosti $p$ je i 2 nesoudělné s $p$, takže dohromady je $2ab$ nesoudělné s $p$. To znamená, že určitě $p \nmid 2ab$, takže ani $p \nmid \pi^2$. Prvky $\pi$, $\overline{\pi}$ tak nejsou asociované.