Teorie nejen čísel 2 – Jednotky

Milý příteli,
vítej u druhé části našeho povídání o tom, že teorii čísel lze potkat i mimo obor celých čísel. V prvním díle jsme se s cílem rozkládat věci na součiny ponořili do světa komutativních okruhů – struktur, kde dovedeme sčítat a násobit podle obvyklých pravidel. Naučili jsme se rozeznávat některé speciální prvky okruhů – ireducibilní prvky, prvočinitele či jednotky. Přidáváním koření v podobě dalších užitečných vlastností jsme pak dostávali různé příchutě okruhů: Pokud jsme v rovnicích mohli krátit, jednalo se o obor integrity. Dělení se zbytkem nám dávalo eukleidovský obor, zatímco jednoznačný rozklad na prvočinitele značil gaussovský obor. Ukázali jsme si, že dělení se zbytkem už zaručuje jednoznačný rozklad (ale ne naopak!) a že jednoznačný rozklad se může hodit k řešení diofantických rovnic. Získané dovednosti jsme si poté vyzkoušeli na zkoumání součtů dvou čtverců skrze vlastnosti okruhu $\mathbb{Z}[i]$.

V tomto díle si katalog okruhů rozšíříme o dvě významné rodinky: *reálné kvadratické okruhy* a *konečná tělesa*. Ač jsou tyto dvě skupiny na první pohled zcela odlišné, společná jim je jedna vlastnost: lze říci mnoho zajímavého o jejich jednotkách, tedy prvcích, které dělí jedničku, a v důsledku toho jimi lze dělit. Ukážeme si, že u obou dovedeme v jistém smyslu všechny jednotky vyrobit z jedné „základní“, a následně toho využijeme při řešení úloh. Stejně jako minule uvidíme, že tyto nové okruhy nám pomohou řešit úlohy zadané čistě v řeči celých čísel, nad kterými bychom bez nich jen tápali.

Jak seriál číst

Obdobně jako v prvním díle na Tebe opět čeká spousta cvičení a úloh. K obojímu nalezneš na konci seriálu návody a ke cvičením též řešení. Opět také některá cvičení odlišujeme co do významu: cvičení s vykřičníkem jsou opravdu důležitá a často je později využíváme, zatímco cvičení s hvězdičkou jsou různá rozšiřující zamyšlení a zajímavosti, které k dalšímu pochopení seriálu nejsou nutné.

V tomto dílu jsme hvězdičkou označili i dvě celé kapitolky – o existenci netriviální jednotky v reálných kvadratických okruzích a o charakteristice v konečných tělesech. Ty mohou být i v porovnání se zbytkem seriálu náročnější, takže pokud se na nich zasekneš, neboj se je přeskočit a vrátit se k nim později. Ani jedna není nutná k vyřešení soutěžních úloh, ani k chápání zbytku seriálu. Přesto si však myslíme, že dávají dobrou představu o příslušných rodinkách okruhů a stojí za to je (zkusit) přečíst.

Reálné kvadratické okruhy

Zavzpomínejme krátce na první díl. V něm jsme všechny vybudované pojmy a nástroje, jako prvočinitele, ireducibilní prvky, jednotky, eukleidovské a gaussovské okruhy, použili na spoustu okruhů, z nichž většina měla jeden společný rys – vznikly tak, že jsme k celým číslům přidali nějaké komplexní číslo. Přesněji, přidávali jsme k $\mathbb{Z}$ nějakou odmocninu ze *záporného* čísla (třeba i nebo $\sqrt{-2}$), anebo o chlup obecněji komplexní číslo splňující nějakou kvadratickou rovnici (například $\alpha = \frac{1+\sqrt{-7}}{2}$ splňující $\alpha^2 - \alpha + 2 = 0$). To nás přivádí k prvnímu tématu druhého dílu. Co kdy-

bychom k celým (anebo racionálním) číslům přidávali opět čísla splňující nějakou kvadratickou rovnici – co třeba nějaké odmocniny z *kladných* čísel? Ukážeme si, že takto vzniklé okruhy se od $\mathbb{Z}[i]$ a komplexních okruhů z prvního dílu v některých ohledech o mnoho neliší, zatímco v jiných jsou úplně jiné.

Definice. Nechť je d přirozené číslo, které není čtverec[1]. Potom definujeme okruhy

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, \qquad \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

Jejich prvkům pak budeme říkat *(reálná) kvadratická čísla.*

Poznámka. Jak jsme zmínili v prvním díle, zápisem $R[m]$ obecně značíme, že k okruhu R přidáme nějaké m a vezmeme si všechno, co se z m a prvků R dá vyrobit (klidně opakovaným) sčítáním a násobením. Množina $\{a+b\sqrt{d} : a, b \in \mathbb{Q}\}$ by tedy měla být zapsána spíše $\mathbb{Q}[\sqrt{d}]$. Zápis $R(m)$ obecně značí, že bereme vše, co se z m a prvků R dá vyrobit sčítáním, násobením a *dělením.* V tuto chvíli by se mohlo zdát, že okruh $\mathbb{Q}(\sqrt{d})$ bude obsahovat něco navíc oproti $\mathbb{Q}[\sqrt{d}]$, ale jak zanedlouho ukážeme, v $\mathbb{Q}[\sqrt{d}]$ dovedeme dělit, takže $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. Pokud bychom tak všude psali $\mathbb{Q}[\sqrt{d}]$ místo $\mathbb{Q}(\sqrt{d})$, nic by se nezměnilo. Většinou se však používá $\mathbb{Q}(\sqrt{d})$, čehož se budeme držet i my.

Již v definici jsme prohlásili, že se jedná o okruhy, slušelo by se tedy ověřit, že jsou tyto množiny skutečně uzavřené na sčítání a násobení. Uzavřenost na sčítání je zřejmá – prostě sečteme odpovídající složky. Při násobení využijeme $(\sqrt{d})^2 = d$, což je prvek $\mathbb{Z}$ i $\mathbb{Q}$. Pro celá čísla a_1, b_1, a_2, b_2 máme

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = a_1b_1 + a_1b_2\sqrt{d} + a_2b_1\sqrt{d} + a_2b_2d = (a_1b_1 + da_2b_2) + (a_1b_2 + a_2b_1)\sqrt{d},$$

což je zase prvek $\mathbb{Z}[\sqrt{d}]$. Pro $\mathbb{Q}(\sqrt{d})$ bychom postupovali úplně stejně. Díky tomu, že $\mathbb{Q}(\sqrt{d})$ i $\mathbb{Z}[\sqrt{d}]$ jsou podmnožiny $\mathbb{R}$, se musí jednat o obory integrity: součin nenulových prvků v těchto okruzích nemůže být nula, a v rovnicích tak můžeme krátit.

Proč je v definici podmínka, aby d nebylo čtvercem? Kdyby $d = a^2$, pak by $\sqrt{d} = a$ bylo celé číslo, takže bychom jeho přidáním k $\mathbb{Z}$, resp. ke $\mathbb{Q}$ nezískali nic navíc. Naopak když d není čtverec, pak už je zaručeno, že přidáním $\sqrt{d}$ skutečně něco navíc dostaneme.

Tvrzení. *Pokud přirozené číslo d není čtverec v $\mathbb{Z}$, pak $\sqrt{d} \notin \mathbb{Q}$.*

Důkaz. Pro spor nechť $\sqrt{d} \in \mathbb{Q}$. Potom je $\sqrt{d}$ rovno nějakému zlomku $\frac{a}{b}$ v základním tvaru (tedy a, b jsou nesoudělná). Umocněním na druhou pak

$$d = \frac{a^2}{b^2}.$$

To znamená, že $b^2 \mid a^2$, jelikož d je celé číslo. Jenže a^2 je nesoudělné s b^2, takže v dělitelnosti nehraje roli, z čehož $b^2 \mid 1$. To však znamená $b^2 = 1$, takže v rovnosti výše zbude $d = a^2$. Jinými slovy, d musel být čtverec, což je spor. □

Cvičení(*) 1. Nahlédni, pro jaká přirozená čísla d_1, d_2, jež nejsou čtverce, mohou být množiny $\mathbb{Q}(\sqrt{d_1})$ a $\mathbb{Q}(\sqrt{d_2})$ totožné.

Reálná kvadratická čísla leží někde na reálné přímce, nicméně často se zase hodí představovat si je spíše „dvojrozměrně“ jako dvojice (a, b) celých, resp. racionálních čísel odpovídajících prvku $a + b\sqrt{d}$. Taková představa by měla zásadní vadu na kráse, kdyby dvěma takovýmto dvojicím mohlo odpovídat stejné reálné číslo. Díky tomu, že a, b bereme pouze z množiny $\mathbb{Q}$ (anebo z její podmnožiny $\mathbb{Z}$), nemůže něco takového nastat.

[1] Připomeňme, že slovem „čtverec“ míníme druhou mocninu nějakého prvku z daného oboru. Není-li řečeno jinak, míníme čtverec v $\mathbb{Z}$.

Tvrzení. *Nechť jsou a_1, b_1, a_2, b_2 racionální čísla. Potom z $a_1+b_1\sqrt{d} = a_2+b_2\sqrt{d}$ plyne $a_1 = a_2$ a $b_1 = b_2$.*

Důkaz. Rovnost upravme na $(a_1 - a_2) = (b_2 - b_1)\sqrt{d}$. Kdyby nyní $b_2 - b_1$ bylo nenulové číslo, pak bychom jím mohli vydělit a dostat $\sqrt{d} = \frac{a_1-a_2}{b_2-b_1}$, což by znamenalo, že $\sqrt{d}$ je racionální. To by byl spor s předchozím tvrzením, takže určitě $b_2 - b_1 = 0$. Z toho pak i $a_1 - a_2 = 0$, takže musí být (a_1, b_1) a (a_2, b_2) totožné dvojice. □

Cvičení 2. Průnikem množin $\mathbb{Q}$ a $\mathbb{Z}[\sqrt{d}]$ je $\mathbb{Z}$.

I když tedy reálné kvadratické číslo leží na reálné přímce, schovává se v něm informace o dvojici racionálních čísel. S jejich pomocí nyní podobně, jako tomu bylo v případě komplexních čísel, zavedeme sdružená čísla a normu.

Definice. K číslu $\alpha = a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definujeme jeho *sdružené* číslo $\overline{\alpha} = a-b\sqrt{d}$ a jeho *normu* $N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2$.

Stejně jako v $\mathbb{Z}[i]$ a dalších komplexních okruzích se i zde sdružená čísla chovají hezky ke sčítání a násobení, v důsledku čehož je norma multiplikativní. Rozdílem je však to, že norma může být záporná – například $N(1 + \sqrt{2}) = -1$. Stále také platí, že norma celého (případně racionálního) čísla je prostě jeho čtverec.

Cvičení(!) 3. Nechť $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Potom platí

$$\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}, \qquad \overline{(\alpha\beta)} = \overline{\alpha} \cdot \overline{\beta} \qquad \text{a} \qquad N(\alpha\beta) = N(\alpha) \cdot N(\beta).$$

Cvičení(!) 4. Jediný prvek $\mathbb{Q}(\sqrt{d})$, který má normu 0, je sama 0.

Cvičení(!) 5. V $\mathbb{Q}[\sqrt{d}]$ lze dělit. Přesněji, pro $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$, $\beta \neq 0$ platí i $\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{d}]$.

Později v seriálu uvidíme, že ačkoliv je většinou lepší zacházet s reálným kvadratickým číslem jako s dvojicí, někdy se přece jenom hodí, že je to jedno reálné číslo. Abychom mezi těmito pohledy uměli jednoduše přecházet, vyplatí se umět získat z $\alpha \in \mathbb{Q}(\sqrt{d})$ jeho racionální a iracionální složku. To však s pomocí sdružených čísel není příliš těžké.

Tvrzení. (vzorec pro (i)racionální složku) *Nechť $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Potom platí*

$$a = \frac{\alpha + \overline{\alpha}}{2}, \qquad b = \frac{\alpha - \overline{\alpha}}{2\sqrt{d}}.$$

Důkaz. Stačí dosadit podle definice. □

Cvičení 6. Kvadratické číslo α je racionální, právě pokud $\alpha = \overline{\alpha}$.

Tímto jsme se v $\mathbb{Z}[\sqrt{d}]$ a $\mathbb{Q}(\sqrt{d})$ náležitě zabydleli a máme k dispozici většinu vymožeností, na něž jsme zvyklí ze $\mathbb{Z}[i]$. Mohli bychom si tak položit otázku, jak je to v reálných kvadratických okruzích s prvočiniteli, ireducibilními prvky a jednotkami. Jednotky jsou zajímavou kapitolou samy o sobě, proto je ještě na moment odložíme. Říci něco o tom, zda funguje rozklad na prvočinitele, je obecně těžké, ale v některých konkrétních případech lze vymyslet, jak v $\mathbb{Z}[\sqrt{d}]$ dělit se zbytkem, což nám jednoznačný rozklad zaručí. Opět tak budeme gaussovskost oboru (jednoznačný rozklad) dokazovat skrze eukleidovskost (dělení se zbytkem). Podobně jako v $\mathbb{Z}[i]$ a komplexních okruzích bývalo dobrým nápadem zkusit jako eukleidovskou funkci normu, tak i zde se norma hodí. Jelikož ale norma může být záporná, typicky ji pro potřeby dělení se zbytkem budeme dávat do absolutní hodnoty.

Příklad. $\mathbb{Z}[\sqrt{2}]$ je eukleidovský obor.

Řešení. Dokážeme, že $|N(x)|$ vyhovuje jako eukleidovská funkce. Na to potřebujeme ukázat, že kdykoliv jsou dána $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$, $\beta \neq 0$, pak dovedeme nalézt takové $\gamma \in \mathbb{Z}[\sqrt{2}]$, že $|N(\alpha - \gamma\beta)| <$

$|N(\beta)|$. Díky tomu, že se norma (stejně jako absolutní hodnota) chová hezky k násobení, můžeme tuhle nerovnost vydělit $|N(\beta)|$ a ekvivalentně upravit na

$$\left|N\left(\frac{\alpha}{\beta}-\gamma\right)\right|<1.$$

Chceme tedy, aby γ byla „blízko“ $\frac{\alpha}{\beta}$, tak ji podobně, jako když jsme dokazovali eukleidovskost $\mathbb{Z}[i]$, položíme jako zaokrouhlení $\frac{\alpha}{\beta}$. Vydělme tedy $\frac{\alpha}{\beta}=x+y\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ a zvolme x_0 a y_0 jako ta celá čísla, která jsou nejblíž k (racionálním) číslům x a y. To zaručí, že $|x-x_0|$ i $|y-y_0|$ jsou nanejvýš $\frac{1}{2}$, takže když zvolíme $\gamma=x_0+y_0\sqrt{2}$, pak už máme

$$\left|N\left(\frac{\alpha}{\beta}-\gamma\right)\right|=\left|N\Big((x-x_0)+(y-y_0)\sqrt{2}\Big)\right|=\left|(x-x_0)^2-2(y-y_0)^2\right|\leq$$
$$\leq|x-x_0|^2+2|y-y_0|^2\leq\frac{1}{4}+2\cdot\frac{1}{4}=\frac{3}{4}<1.$$

Během předchozí úpravy jsme použili tzv. *trojúhelníkovou nerovnost.* Když vyšetřujeme výraz tvaru $|A+B|$, tak mohou A, B mít opačná znaménka a navzájem se vyrušovat, anebo mohou mít stejné znaménko a táhnout za jeden provaz. Když tedy dáme do absolutních hodnot A a B každé zvlášť, tak jenom zaručíme, že táhnou za jeden provaz, takže celkovou hodnotu výrazu možná o něco zvýšíme, ale určitě nesnížíme. V našem případě bylo $A=(x-x_0)^2$, $B=-2(y-y_0)^2$, takže jsme absolutní hodnotu rozdílu odhadli součtem.

V souhrnu jsme tak skutečně ukázali, že dovedeme zvolit γ tak, aby dělení se zbytkem fungovalo, takže $\mathbb{Z}[\sqrt{2}]$ je eukleidovský obor.

Cvičení 7. Dokaž, že $\mathbb{Z}[\sqrt{3}]$ je eukleidovský obor.

Úloha 1. Dokaž, že $\mathbb{Z}[\sqrt{7}]$ je eukleidovský obor.

Cvičení(*) 8. Nechť $d\equiv 1 \pmod 4$ není čtverec. Rozmysli si, že $\left\{a+b\cdot\frac{1+\sqrt{d}}{2}:a,b\in\mathbb{Z}\right\}$ je množina uzavřená na násobení, a tvoří tak okruh.

Pellova[2] rovnice aneb jednotky v $\mathbb{Z}[\sqrt{d}]$

Při našem průzkumu okruhů $\mathbb{Z}[\sqrt{d}]$ jsme dosud nezmínili, jak v nich vypadají jednotky. V nich se totiž reálná kvadratická čísla výrazně liší od těch komplexních. Zatímco v Gaussových celých číslech $\mathbb{Z}[i]$ jsme měli čtyři jednotky 1, i, -1 a $-i$ a v Eisensteinových číslech $\mathbb{Z}[\omega]$ šest jednotek ±1, $\pm\omega$, $\pm\omega^2$, v okruhu $\mathbb{Z}[\sqrt{d}]$ budeme mít jednotek nekonečně mnoho.

Nejprve nahlédněme souvislost jednotek s normou.

Tvrzení. *Číslo $\omega\in\mathbb{Z}[\sqrt{d}]$ je jednotka právě tehdy, když $|N(\omega)|=1$.*

Důkaz. Nechť je nejprve ω jednotka. To znamená, že existuje nějaké $\omega'\in\mathbb{Z}[\sqrt{d}]$ takové, že $\omega\omega'=1$. Vzetím norem pak $N(\omega)\cdot N(\omega')=1$. Máme tedy dvě celá čísla, jejichž součin je 1, takže jsou to buď dvě jedničky, nebo dvě mínus jedničky. V obou případech však $|N(\omega)|=1$.

Naopak nechť je $N(\omega)=\pm1$ neboli $\omega\cdot\overline{\omega}=\pm1$. To znamená, že ω dělí ±1, což nehledě na znaménko dělí 1. Celkově tedy $\omega\mid 1$, takže ω je jednotka. □

Z tohoto plyne, že mocněním jednotky dostaneme zase jednotku. To není nic nového, když v $\mathbb{Z}[i]$ budeme brát mocniny i, dostaneme postupně všechny čtyři jednotky v tomto okruhu. V reálných kvadratických číslech však narazíme na to, že se nám toto mocnění nemusí zacyklit. Jednotky

[2] John Pell (1611–1685), anglický matematik, přišel k „vlastnictví“ Pellovy rovnice spíše omylem: její vyřešení mu chybně připsal Leonhard Euler a stejně jako spousta jiných mylných označení se i toto ujalo. Ve skutečnosti bylo řešení Pellovy rovnice nalezeno už o staletí dříve v Indii.

v $\mathbb{Z}[\sqrt{d}]$ jsou totiž reálná čísla, a když mocníme reálné číslo ω, tak budeme buďto dostávat větší a větší (pokud $|\omega| > 1$), anebo menší a menší (pokud $|\omega| < 1$) hodnoty. To ale znamená, že to budou navzájem různá čísla. Nekonečně mnoho jednotek bychom tedy takovýmto mocněním nevyrobili jen tehdy, kdybychom začali s něčím, co má absolutní hodnotu 0 (to jednotka nebude), anebo 1 (to mohou být 1 a -1, což jsou jednotky).

V souhrnu tedy: když najdeme jednotku, která není ± 1, pak už z ní mocněním vyrobíme nekonečně mnoho jednotek. Například v $\mathbb{Z}[\sqrt{2}]$ máme $N(1+\sqrt{2}) = -1$, takže je to jednotka, pročež jsou jednotkami i její mocniny

$$(1+\sqrt{2})^2 = 3+2\sqrt{2}, \qquad (1+\sqrt{2})^3 = 7+5\sqrt{2}, \qquad (1+\sqrt{2})^4 = 17+12\sqrt{2} \qquad \text{a tak dále.}$$

Nekonečně mnoho jednotek by nám mohlo činit obtíže, například kdybychom chtěli řešit nějakou rovnici tvaru $ab = c^n$. Když víme, že a, b jsou nesoudělná, tak v gaussovkém oboru chceme vyvodit, že i a, b musí samy být n-té mocniny. Jenže tohle platí s jedním háčkem – jsou to n-té mocniny *přenásobené jednotkami*. Bez znalosti jednotek bychom tedy v $\mathbb{Z}[\sqrt{d}]$ nemohli ani použít nástroje z prvního dílu.

Pojďme tedy hledat jednotky. Aby $x + y\sqrt{d}$ bylo jednotkou, má jeho norma být buďto 1, nebo -1. První z těchto možností odpovídá rovnici

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

která si svým významem vysloužila vlastní jméno. Říká se jí *Pellova rovnice* a její řešení odpovídají jednotkám v $\mathbb{Z}[\sqrt{d}]$ s normou 1 (ještě by mohly existovat jednotky s normou -1). Takto přeformulovaný problém hledání jednotek už můžeme potkat často potkat v úlohách: mnohé diofantické rovnice se dají vhodnou úpravou dostat do tvaru $x^2 - dy^2 = 1$ a v tu chvíli na ně můžeme vrhnout mašinérii okruhu $\mathbb{Z}[\sqrt{d}]$ a jeho jednotek, kterou si postupně rozkryjeme.

Dvě řešení Pellovy rovnice dovedeme zaručit vždy: jsou jimi $y = 0$ a $x = 1$, resp. $x = -1$. To odpovídá tomu, že 1 a -1 mají normu jedna, a jsou tak jednotkami, což příliš nepřekvapí. Protože jsou tato řešení celkem nezajímavá, nazýváme je *triviální*. Obdobně taky říkáme, že 1 a -1 jsou triviální jednotky v $\mathbb{Z}[\sqrt{d}]$. Obecně budeme v povídání o Pellově rovnici ztotožňovat dvojici (x, y) a číslo $x + y\sqrt{d}$, takže třeba klidně řekneme, že $x + y\sqrt{d}$ je řešení Pellovy rovnice.

Obecněji se rovnicím $x^2 - dy^2 = c$, kde c je nějaké celé číslo, říká „rovnice Pellova typu“. Speciálně pro $c = -1$, což popisuje jednotky s normou -1, budeme této rovnici říkat „záporná Pellova rovnice“.

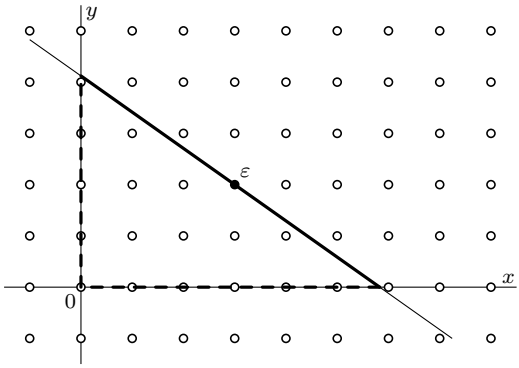
Cvičení 9. Jaká by byla řešení Pellovy rovnice, kdybychom povolili, aby $d = a^2$ byl čtverec celého čísla?

Za chvíli si ukážeme, že vždy existují i nějaké další, *netriviální* jednotky. Začneme ale tvrzením o jednotkách v $\mathbb{Z}[\sqrt{d}]$, které je jak snazší na dokázání, tak i mnohem užitečnější při řešení úloh. Ukážeme, že všechny jednotky se dají vyrobit z té „nejmenší“. Nejprve si pořádně zadefinujme, co tím přesně budeme myslet. Budeme u toho předpokládat, že vůbec nějaké netriviální jednotky existují, avšak tento předpoklad se později ukáže býti automaticky splněn, neboť existenci netriviální jednotky budeme mít zaručenu vždy, když d není čtverec.

Definice. Předpokládejme, že v $\mathbb{Z}[\sqrt{d}]$ existují netriviální jednotky. *Fundamentální jednotkou* potom rozumíme takovou jednotku $x+y\sqrt{d}$, které má kladné složky, a navíc je mezi všemi takovými jednotkami hodnota $x + y\sqrt{d}$ jakožto reálného čísla nejmenší.

Nad touto definicí se stojí zato pořádně zarazit, jelikož na první pohled není ani zřejmé, že vždy dává dobrý smysl. Některé nekonečné množiny totiž mezi sebou žádný nejmenší prvek mít nemusí: když například vezmeme převrácené hodnoty přirozených čísel $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5} \ldots$, pak mezi nimi žádné nejmenší číslo nenajdeme, protože pro každé $\frac{1}{n}$ je $\frac{1}{n+1}$ ještě menší. Množina jednotek v $\mathbb{Z}[\sqrt{d}]$ přitom dost možná nekonečná bude, takže tady máme zavařeno na pořádný problém.

Podívejme se na definici geometricky. Čísla $x+y\sqrt{d}$ si představme jako celočíselné body v rovině, to jest jako body s celočíselnými souřadnicemi (x, y). Podmínka $x, y > 0$ říká, že se díváme jenom na body nad osou x, napravo od osy y. Dále si vezměme nějakou netriviální jednotku $\varepsilon = x_0+y_0\sqrt{d}$. BÚNO nechť jsou x_0, y_0 obě kladná – vždy můžeme namísto ε vzít $-\varepsilon$, což obrátí znaménka obou složek, či $\overline{\varepsilon}$, což obrátí znaménko y_0 (anebo $-\overline{\varepsilon}$ obrátí znaménko x_0). Když takto máme jednu zvolenou jednotku, pak už tu nejmenší, pokud tedy existuje jedna nejmenší, stačí hledat mezi těmi, které jsou menší než ε. K podmínce $x, y > 0$ nám tak přibude $x + y\sqrt{d} \leq \varepsilon$. Rovnice $x + y\sqrt{d} = \varepsilon$ přestavuje nějakou přímku se záporným sklonem a nerovnost $x+y\sqrt{d} \leq \varepsilon$ povoluje jenom body pod touto přímkou. Dohromady tak podmínky vymezí trojúhelník (jeho odvěsny do něj nezahrnujeme, zatímco přeponu obsahující ε už ano).



V něm je jakožto v omezené množině jen konečně mnoho celočíselných bodů, což odpovídá konečně mnoha prvkům $\mathbb{Z}[\sqrt{d}]$. Z těch si vybereme ty, které jsou jednotkami, a vezmeme už bez problému minimum z konečně mnoha čísel (určitě v trojúhelníku máme jednotku ε, takže nebereme minimum z prázdné množiny). Nejmenší jednotka v trojúhelníku bude zároveň také menší než ostatní jednotky mimo trojúhelník, ale stále nad osou x a napravo od osy y, takže to celkově bude fundamentální jednotka, kterou hledáme. Tím je rozmyšleno, že definice fundamentální jednotky dává smysl.

S fundamentální jednotkou řádně zadefinovanou si už dokážeme, že z ní dovedeme vyrobit všechny ostatní.

Věta. *Nechť v $\mathbb{Z}[\sqrt{d}]$ existují netriviální jednotky a ω je fundamentální jednotka. Potom se každá jednotka dá zapsat jako $\pm\omega^n$ pro nějaké $n \in \mathbb{Z}$.*

Před důkazem samotné věty si vyrobíme drobné lemma.

Lemma. *Pro jednotku $x + y\sqrt{d}$ platí $x, y > 0$ právě tehdy, když $x + y\sqrt{d} > 1$.*

Důkaz lemmatu. Jedna implikace je zřejmá: pokud $x, y > 0$, znamená to $x, y \geq 1$, takže i

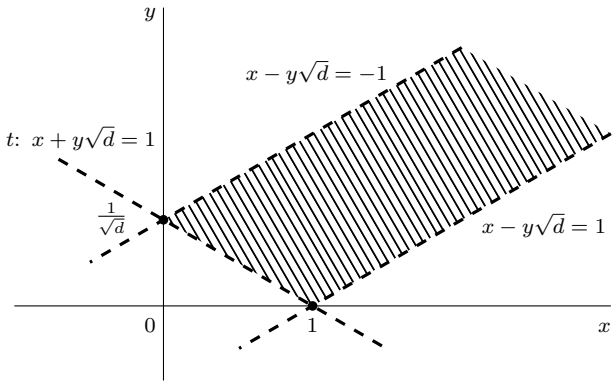
$$x + y\sqrt{d} > x \geq 1,$$

neboť $\sqrt{d}$ je kladné číslo. Nadále tedy naopak předpokládejme, že $x + y\sqrt{d}$ je jednotka větší než 1, a vyvoďme $x, y > 0$.

Rovnice $x + y\sqrt{d} = 1$ určuje v rovině přímku t, která protíná osu x v bodě $(1, 0)$ a osu y v bodě $\left(0, \frac{1}{\sqrt{d}}\right)$, takže nerovnost $x + y\sqrt{d} > 1$ určuje polorovinu nad přímkou t. Tím, že číslo $x + y\sqrt{d}$ je větší než 1, musí i jeho absolutní hodnota být větší než 1. Také předpokládáme, že $x + y\sqrt{d}$ je jednotka, což je ekvivalentní s $|x^2 - dy^2| = 1$. To upravíme na

$$1 = |x^2 - dy^2| = |x + y\sqrt{d}| \cdot |x - y\sqrt{d}| > 1 \cdot |x - y\sqrt{d}|,$$

takže $|x - y\sqrt{d}| < 1$ neboli $-1 < x - y\sqrt{d} < 1$. Přímka $x - y\sqrt{d} = 1$ je jenom přímka t převrácená podle osy x, zatímco $x - y\sqrt{d} = -1$ je t převrácená podle osy y.



Jednotka, která je větší než 1, tedy musí odpovídat bodu v polorovině nad t a zároveň v pruhu mezi rovnoběžkami $x - y\sqrt{d} = \pm 1$. Z obrázku je ale vidět, že celá tato oblast leží nad osou x a napravo od osy y, takže $x, y > 0$. □

Důkaz věty. Jelikož je ω fundamentální jednotka, máme $|N(\omega)| = 1$. Vzhledem k $\omega\overline{\omega} = \pm 1$ je $\overline{\omega} = \pm\omega^{-1}$, takže i ω^{-1} je prvek $\mathbb{Z}[\sqrt{d}]$, a tedy jednotka. Mocněním jednotky dostaneme opět jednotku, neboť

$$|N(\omega^n)| = |N(\omega)|^n = 1^n = 1,$$

takže všechny $\pm\omega^n$ budou jednotky. Povolujeme přitom i záporné n, protože z definice jednotky $\omega \mid 1$, takže $\omega^{-1} \in \mathbb{Z}[\sqrt{d}]$. Zbývá tak dokázat, že žádné další jednotky neexistují.

Nechť pro spor nějaká jednotka ε nejde vyjádřit ve tvaru $\pm\omega^n$. BÚNO nechť má ε obě složky kladné – kdyby nemělo, vzali bychom namísto něj $-\varepsilon$, $\overline{\varepsilon}$ nebo $-\overline{\varepsilon}$. Potom podle lemmatu $\varepsilon > 1$. Stejně tak $\omega > 1$, takže můžeme interval $(1, \infty)$ rozdělit na menší intervaly pomocí posloupnosti čísel $1 = \omega^0, \omega^1, \omega^2, \ldots$ Předpokládáme, že se ε žádnému z nich nerovná, takže leží ostře mezi některými dvěma. To dává nerovnosti

$$\omega^n < \varepsilon < \omega^{n+1}$$

pro nějaké n. Vše přenásobíme ω^{-n}, čímž dostaneme

$$1 < \varepsilon\omega^{-n} < \omega.$$

Číslo $\varepsilon\omega^{-n}$ je zase jednotka v $\mathbb{Z}[\sqrt{d}]$, protože je to jenom součin dvou jednotek. Také je to jednotka větší než 1, takže podle lemmatu má obě složky kladné. Přitom je ale menší než ω. To je spor s tím, že ω má být fundamentální, tedy „nejmenší“ jednotka. Úspěšně jsme vyvodili spor, takže takové ε, které by se nedalo vyjádřit jako $\pm\omega^n$, neexistuje. □

Poznámka. Z lemmatu, které jsme použili v důkazu věty, nám také plyne, jak bude $\pm\omega^n$ vypadat v závislosti na znaménku n a znaménku $\pm$. Především jednotky s oběma složkami kladnými budou vždy odpovídat ω^n pro přirozená n. Pro záporná n už bude situace záviset na normě ω, pro $N(\omega) = 1$ bude $\omega^{-1} = \overline{\omega}$, zatímco pro $N(\omega) = -1$ platí $\omega^{-1} = -\overline{\omega}$. Znaménko minus pak jenom obě složky obrátí.

Definice. Předpokládejme, že Pellova rovnice pro nějaké d má netriviální řešení. *Fundamentálním řešením* potom rozumíme takové řešení $x + y\sqrt{d}$, které má $x, y > 0$ a navíc je mezi všemi takovými řešeními hodnota $x + y\sqrt{d}$ jakožto reálného čísla nejmenší.

Fundamentální řešení Pellovy rovnice tak plní stejnou roli jako fundamentální jednotka, jenom jsme se omezili pouze na ty jednotky, které mají normu 1. Nepřekvapí tedy, že stejně jako všechny jednotky lze vyrobit z té fundamentální, tak i všechna řešení Pellovy rovnice jde vyrobit z toho fundamentálního.

Nechť je ω fundamentální jednotka a ω_1 fundamentální řešení Pellovy rovnice. Kdyby $N(\omega) = 1$, pak už to znamená, že všechny jednotky mají normu 1, žádné jednotky s normou -1 neexistují a jednotkami jsou právě řešení Pellovy rovnice. Potom je tedy $\omega = \omega_1$.

Kdyby naopak $N(\omega) = -1$, pak potom stejně $N(\omega^2) = 1$. Kdyby nyní $\omega_1 \neq \omega^2$, byl by to spor, protože jakožto jednotka musí ω_1 být rovno nějakému ω^n, a kdyby $n > 2$, pak by ω^2 bylo menší řešení Pellovy rovnice než ω_1. V tomto případě je také každé řešení Pellovy rovnice rovno $\pm\omega_1^n$. Musí se totiž jednat o jednotku, takže lze vyjádřit jako $\pm\omega^m$. Jeho norma však má být 1, takže $1 = N(\pm\omega^m) = (-1)^m$, což znamená, že m je sudé neboli $m = 2n$, takže $\pm\omega^m = \pm\omega^{2n} = \pm\omega_1^n$. Naopak mocniny $\pm\omega^\ell$ pro liché ℓ budou mít normu $(-1)^\ell = -1$. Shrňme:

Věta. *Nechť je ω fundamentální jednotka a ω_1 fundamentální řešení Pellovy rovnice. Potom:*

(i) *Pokud $N(\omega) = 1$, pak je $\omega_1 = \omega$ a jednotky s normou -1 neexistují.*

(ii) *Pokud $N(\omega) = -1$, pak $\omega_1 = \omega^2$. Všechny jednotky jsou tvaru $\pm\omega^n$, přičemž pro sudá n se jedná o řešení Pellovy rovnice, zatímco pro lichá n o jednotky s normou -1.*

V obou případech jsou řešeními Pellovy rovnice právě všechna $\pm\omega_1^n$ pro $n \in \mathbb{Z}$.

Příklad. V $\mathbb{Z}[\sqrt{5}]$ je fundamentálním řešením Pellovy rovnice $9 + 4\sqrt{5}$. Fundamentální jednotkou je však $2 + \sqrt{5}$ a platí $9 + 4\sqrt{5} = (2 + \sqrt{5})^2$.

Úloha 2. Dokaž, že záporná Pellova rovnice $x^2 - 34y^2 = -1$ nemá celočíselné řešení.

Nabízí se ještě otázka, jak fundamentální jednotku či fundamentální řešení Pellovy rovnice najít. Zde však trochu zklameme: v seriálu se nebudeme zabývat[3] čímkoliv lepším, než že prostě vyzkoušíme nějaká malá y a budeme doufat, že $dy^2 \pm 1$ bude nějaký čtverec x^2. Pokud tímto najdeme nějakou jednotku, pak už skutečně najdeme tu nejmenší, neboť fundamentální jednotka $x + y\sqrt{d}$ má mezi jednotkami s $x, y > 0$ zároveň i nejmenší x a nejmenší y. Při hledání fundamentální jednotky tímto způsobem je však třeba nemít smůlu, neboť i pro některá malá d může být fundamentální jednotka veliká: například pro $d = 61$ je fundamentální jednotkou $29718 + 3805\sqrt{61}$.

Cvičení 10. Pro některé speciální tvary d si lze nějaké řešení Pellovy rovnice hned tipnout. Najdi nějaký předpis pro x a y závislý na a, tak aby $x + y\sqrt{d}$ bylo řešení Pellovy rovnice pro

(i) $d = a^2 - 1$, (ii) $d = a^2 - 2$, (iii) $d = a^2 + 2$, (iv) $d = a^2 + 1$.

Pellova rovnice a řešení diofantických rovnic

Příklad. Najdi všechny dvojice přirozených čísel $n < m$ takové, že

$$1 + 2 + \cdots + n = (n + 1) + (n + 2) + \cdots + m.$$

Řešení. Použijeme vzorec $1 + \cdots + n = \frac{n(n+1)}{2}$. Na obě strany přičteme $1 + \cdots + n$, čímž rovnici upravíme do tvaru $2 \cdot \frac{n(n+1)}{2} = \frac{m(m+1)}{2}$. Obě strany vynásobíme osmi a potom přeuspořádáme na

$$(4m^2 + 4m + 1) + 1 = 2(4n^2 + 4n + 1)$$

neboli $(2m + 1)^2 - 2(2n + 1)^2 = -1$. Substitucí $x = 2m + 1$, $y = 2n + 1$ je toto záporná Pellova rovnice v $\mathbb{Z}[\sqrt{2}]$, kde je fundamentální jednotkou $\omega = 1 + \sqrt{2}$. Ta má normu -1, takže budeme brát

[3]Pokud by ses chtěl(a) dozvědět o tom, jak hledat řešení Pellovy rovnice pomocí řetězových zlomků, odkážeme Tě na tento příspěvek: *https://prase.cz/library/PellADL/PellADL.pdf*.

její liché mocniny. Zároveň chceme, aby n, m byla přirozená, takže určitě $x, y > 0$, pročež můžeme brát jenom $x + y\sqrt{2} = \omega^\ell$ pro kladná lichá ℓ. Jelikož $n, m \geq 1$, tak však dokonce $x, y \geq 3$, což pro $\ell = 1$ nedostaneme, uvažujeme tedy dokonce jenom lichá $\ell \geq 3$ (pro $\ell = 3$ máme $x = 7$, $y = 5$, takže už jsme v suchu). Zároveň také musíme splnit, že x, y jsou lichá. To je ale splněno pro každé řešení záporné Pellovy rovnice $x^2 - 2y^2 = -1$. Když se na ni podíváme modulo 2, pak uvidíme, že x je liché. Potom $x^2 \equiv 1 \pmod 4$, takže už $2y^2 \equiv -2 \equiv 2 \pmod 4$, což by pro sudé y neplatilo, takže y je také liché.

V souhrnu jsme ukázali, že validní řešení dostaneme právě pro každé liché $\ell \geq 3$. Když tedy ještě zapíšeme $\ell = 2k + 1$ pro přirozené k, pak už skrze $m = \frac{x-1}{2}$, $n = \frac{y-1}{2}$ dopočítáme

$$m = \frac{1}{2}\left(\frac{\omega^\ell + (\overline{\omega})^\ell}{2} - 1\right) = \frac{(1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1} - 2}{4},$$
$$n = \frac{1}{2}\left(\frac{\omega^\ell - (\overline{\omega})^\ell}{2\sqrt{2}} - 1\right) = \frac{(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1} - 2}{4}.$$

Řešení obnášelo spoustu drobných technických detailů, ale základní myšlenka je jednoduchá – převést na Pellovu rovnici, vzít mocniny fundamentální jednotky (či fundamentálního řešení) a rozmyslet, které z nich dávají smysluplná řešení původní úlohy. Také si můžeme všimnout toho, co se obvykle stane, když něco vyřešíme Pellovou rovnicí: dostaneme předpis, který vypadá dost složitě (vyrábíme celé číslo pomocí mocnění nějakých výrazů s odmocninami), a na první pohled není vidět, co se v něm děje, ale přesto nám umožňuje všechna řešení popsat a dosazením nějakého ℓ si jakékoliv z nich spočítat.

Cvičení 11. Řeš v celých číslech rovnici $x^2 + y^2 - 1 = 4xy$.

Cvičení 12. Najdi třetí nejmenší přirozené číslo n, pro něž je $\frac{n(n+1)}{2}$ čtverec.

Příklad. Dokaž, že když je $m = 2\sqrt{12n^2 + 1} + 2$ celé číslo pro nějaké $n \in \mathbb{N}$, pak už je m čtverec celého čísla.

Řešení. Aby m bylo celé, tak musí výraz pod odmocninou být čtverec, takže máme $12n^2 + 1 = x^2$ pro nějaké $x \in \mathbb{N}$ (určitě $12n^2 + 1 > 0$). To je jenom přeuspořádaná Pellova rovnice $x^2 - 12n^2 = 1$. Fundamentální řešení Pellovy rovnice pro $d = 12$ je $\omega = 7 + 2\sqrt{12}$ a $x + n\sqrt{12}$ je také nějaké řešení, takže $x + n\sqrt{12} = \pm\omega^k$ pro nějaké $k \in \mathbb{Z}$. Víme ale, že x i n jsou přirozená, tedy kladná, takže v předchozím vyjádření bude určitě $\pm = +$ a exponent k bude kladný.

Ze vzorce pro racionální složku nyní vyjádříme $x = \frac{\omega^k + (\overline{\omega})^k}{2} = \frac{\omega^k + \omega^{-k}}{2}$, následně pak vyjádříme

$$m = 2x + 2 = \omega^k + 2 + \omega^{-k}.$$

Když se pohybujeme kolem Pellovy rovnice, tak takovýto výraz zpravidla nemá daleko k tomu, aby byl čtvercem, neboť $2 = 2\omega^{\frac{k}{2}}\omega^{-\frac{k}{2}}$. Potřebovali bychom tudíž, aby ω^k a ω^{-k} byly čtverce nějakých A, B, neboť potom už budeme moci vyjádřit m jako $(A+B)^2$. Tady však využijeme toho, že okruh $\mathbb{Z}[\sqrt{12}]$ leží uvnitř $\mathbb{Z}[\sqrt{3}]$, jelikož $\sqrt{12} = 2\sqrt{3}$. Přitom v $\mathbb{Z}[\sqrt{3}]$ máme i jednotky, které v $\mathbb{Z}[\sqrt{12}]$ neleží. Jmenovitě $\omega_0 = 2 + \sqrt{3}$ splňuje $\omega = \omega_0^2$. Z toho už dostaneme

$$m = \omega^k + 2 + \omega^{-k} = \omega_0^{2k} + 2 \cdot \omega_0^k \cdot \omega_0^{-k} + \omega_0^{-2k} = (\omega_0^k + \omega_0^{-k})^2.$$

Zde ještě není vyhráno – co kdyby výraz uvnitř závorky nebyl celé číslo? Býti čtvercem v $\mathbb{Z}[\sqrt{3}]$ a býti čtvercem v $\mathbb{Z}$ totiž není totéž – viz třeba $3 = (\sqrt{3})^2$. Toto dořešíme následovně: ω_0^k má v $\mathbb{Z}[\sqrt{3}]$ normu 1, takže $\omega_0^{-k} = \overline{(\omega_0^k)}$. Číslo $\omega_0^k + \omega_0^{-k}$ je tak jenom dvojnásobek racionální složky ω_0^k, což je určitě celé číslo, a m je tak čtvercem v $\mathbb{Z}$, jak jsme chtěli.

Cvičení 13. Číslo $m = 2 + 2\sqrt{28n^2 + 1}$ je celé pro nějaké $n \in \mathbb{N}$. Dokaž, že m je čtverec celého čísla.

Úloha 3. Je dáno přirozené číslo n takové, že n^2 lze vyjádřit jako rozdíl dvou po sobě jdoucích třetích mocnin. Dokaž, že $2n-1$ je čtverec.

Úloha 4. (těžší) Dokaž, že existují rostoucí nekonečné posloupnosti $\{a_n\}$, $\{b_n\}$ přirozených čísel takové, že $a_n(a_n+1) \mid b_n^2+1$ pro každé n.

Existence netriviální jednotky*

Nastal čas splnit ten velký rest, který nám doposud zůstával – dokážeme, že vždy když je d přirozené a není to čtverec, má Pellova rovnice $x^2-dy^2=1$ netriviální řešení. Tento důkaz je trochu náročný, takže pokud se zasekneš, neboj se tento oddíl přeskočit a vrátit se k němu později.

Během důkazu na několika místech použijeme Dirichletův[4] princip[5]. To také způsobí, že nám tento důkaz nedá žádný dobrý algoritmus na to, jak netriviální řešení Pellovy rovnice najít – jenom dokážeme, že existuje.

Tvrzení. (Dirichletův princip) *Když rozdělíme $n+1$ předmětů do n přihrádek, pak v alespoň jedné přihrádce skončí alespoň dva předměty.*

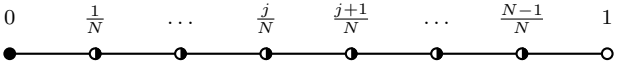
Jak to tak někdy v matematice bývá, i takto zřejmé a jednoduché tvrzení dovede být silným nástrojem a dokázat velké věci – malá ochutnávka přijde již za chvíli. Kromě obyčejného Dirichletova principu máme ještě jeho nekonečnou odrůdu.

Tvrzení. (nekonečný Dirichletův princip) *Když rozdělíme nekonečně mnoho předmětů do konečně mnoha přihrádek, pak v alespoň jedné přihrádce skončí nekonečně mnoho předmětů.*

S touto výzbrojí se již můžeme vrhnout na Pellovu rovnici. Přiblížíme se k ní postupně: začneme tím, jak se dá $\sqrt{d}$ aproximovat pomocí racionálních čísel. Intuice, proč by toto mohlo souviset s Pellovou rovnicí je následovná: když rovnici $x^2-dy^2=1$ upravíme na $d=\frac{x^2}{y^2}+\frac{1}{y^2}$, pak si můžeme říct, že $\frac{1}{y^2}$ bude typicky něco dost malého, takže to můžeme zahodit. Potom nám zbude $d\approx\frac{x^2}{y^2}$ neboli $\sqrt{d}\approx\frac{x}{y}$. To znamená, že když je $x+y\sqrt{d}$ řešení Pellovy rovnice, pak zlomek $\frac{x}{y}$ leží dost blízko $\sqrt{d}$.

Věta. (Dirichletova o diofantických aproximacích) *Nechť je dáno reálné číslo α a přirozené N. Potom existuje $q\in\{1,\dots,N\}$ a celé číslo p tak, že $|q\alpha-p|<\frac{1}{N}$.*

Důkaz. Půjdeme na to postupně. Pro každé $k\in\{1,\dots,N\}$ se podívejme na reálné číslo $k\alpha$ a zvolme celé číslo p_k jako $\lfloor k\alpha\rfloor$, tedy největší celé číslo, které nepřevyšuje $k\alpha$. Potom budou $k\alpha-p_k$ zbylé necelé části z $k\alpha$, takže budou všechny ležet někde v intervalu $\langle 0,1)$. Tenhle interval si rozřežeme na N přihrádek délky $\frac{1}{N}$, tedy na intervaly $\left\langle\frac{j}{N},\frac{j+1}{N}\right)$ pro $j=0,1,\dots,N-1$.



Nejprve koukněme na přihrádku $\langle 0,\frac{1}{N}\right)$. Kdyby v ní leželo nějaké $k\alpha-p_k$, pak by to znamenalo $|k\alpha-p_k|<\frac{1}{N}$, takže stačí zvolit $q=k$, $p=p_k$ a máme vyhráno. Nadále tedy předpokládejme, že v přihrádce $\left\langle 0,\frac{1}{N}\right)$ žádné z našich čísel neleží. Potom jsme ale do zbylých $N-1$ přihrádek museli rozmístit N předmětů $k\alpha-p_k$, takže z Dirichletova principu v některém $\left\langle\frac{j}{N},\frac{j+1}{N}\right)$ skončily dvě čísla $k_1\alpha-p_{k_1}$, $k_2\alpha-p_{k_2}$, BÚNO $k_1<k_2$. Jelikož ale tato čísla leží uvnitř intervalu délky $\frac{1}{N}$,

[4]Peter Gustav Lejeune Dirichlet (1805–1859), německý matematik, má kromě principu se svým jménem spojeny hned tři důležité věty v teorii čísel – jednu z nich si zde dokážeme.

[5]Též známý jako princip holubníku.

který neobsahuje svůj pravý koncový bod, tak jejich vzdálenost od sebe musí být ostře menší než $\frac{1}{N}$. Když tedy zvolíme $q = k_2 - k_1$ a $p = p_{k_2} - p_{k_1}$, dostaneme

$$\frac{1}{N} > |(k_2\alpha - p_{k_2}) - (k_1\alpha - p_{k_1})| = |(k_2 - k_1)\alpha - (p_{k_2} - p_{k_1})| = |q\alpha - p|,$$

jak jsme chtěli. Přitom q je rozdíl dvou přirozených čísel (větší mínus menší) z množiny $\{1, \ldots, N\}$, takže samo musí taky ležet někde v této množině. Tím jsme splnili vše, co q a p měla splňovat. □

Důsledek. *Nechť je α iracionální. Potom existuje nekonečně mnoho dvojic p, q takových, že* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Důkaz. Použijeme Dirichletovu větu. Když platí $|q\alpha - p| < \frac{1}{N}$ a zároveň $q \in \{1, \ldots, N\}$, takže $q \leq N$ neboli $\frac{1}{N} \leq \frac{1}{q}$, z čehož $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} \leq \frac{1}{q^2}$. Každá dvojice, kterou dostaneme z Dirichletovy věty, tak vyhovuje důsledku.

Už tedy jenom potřebujeme těchto dvojic vyrobit nekonečně mnoho. Začněme tím, že si pro $N_1 = 1$ vyrobíme nějakou dvojici p_1, q_1. Jelikož předpokládáme, že α je iracionální, tak platí $\left|\alpha - \frac{p_1}{q_1}\right| \neq 0$, takže můžeme zvolit nějaké N_2 dost velké na to, aby $\frac{1}{N_2} < \left|\alpha - \frac{p_1}{q_1}\right|$. Pro tohle N_2 pak použijeme Dirichletovu větu, což nám dá nějakou dvojici p_2, q_2. Vzhledem k volbě N bude platit

$$\left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{q_2 N_2} \leq \frac{1}{N_2} < \left|\alpha - \frac{p_1}{q_1}\right|.$$

Zlomek $\frac{p_2}{q_2}$ tedy aproximuje α ostře lépe než $\frac{p_1}{q_1}$, takže to nemohou být stejné zlomky, a ani tedy stejné dvojice čísel. Takto postupujeme stále dál: vždy zvolíme N_{j+1} tak, aby $\frac{1}{N_{j+1}} < \left|\alpha - \frac{p_j}{q_j}\right|$, a touto volbou N_{j+1} vyrobíme další dvojici p_{j+1}, q_{j+1}. Každý další zlomek bude ležet blíž k α než ten předchozí, takže budou všechny tyto dvojice p, q navzájem různé a vyrobíme jich tak nekonečně mnoho. □

Důsledek věty nyní použijeme pro $\alpha = \sqrt{d}$. To bude fungovat, neboť předpokládáme, že d není čtverec, a už víme, že potom je $\sqrt{d}$ iracionální.

Lemma. (první) *Když* $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$, *pak* $|N(p + q\sqrt{d})| < 2\sqrt{d} + 1$.

Důkaz. Označme si $\beta = -p + q\sqrt{d}$, potom chceme dokázat $|N(\beta)| < 2\sqrt{d} + 1$ (obrácení znaménka u p oproti znění lemmatu nemá na normu vliv). Dále máme předpoklad $|\beta| = q \cdot \left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q}$. Chceme odhadnout výraz $|\beta\overline{\beta}|$, takže ještě chceme omezit $\overline{\beta}$. K tomu použijeme trojúhelníkovou nerovnost na

$$|\overline{\beta}| = |-p - q\sqrt{d}| = |-2q\sqrt{d} + (-p + q\sqrt{d})| \leq |-2q\sqrt{d}| + |-p + q\sqrt{d}| < 2q\sqrt{d} + \frac{1}{q}.$$

Následně už máme $|N(\beta)| = |\beta| \cdot |\overline{\beta}| < \frac{1}{q} \cdot \left(2q\sqrt{d} + \frac{1}{q}\right) = 2\sqrt{d} + \frac{1}{q^2} \leq 2\sqrt{d} + 1$, jak jsme chtěli. □

Lemma. (druhé) *Nechť je $k \neq 0$ celé číslo. Potom pokud $N(a + b\sqrt{d}) = N(x + y\sqrt{d}) = k$ a zároveň modulo k platí $a \equiv x$ a $b \equiv y$, pak už je $\frac{x+y\sqrt{d}}{a+b\sqrt{d}}$ řešení Pellovy rovnice.*

Důkaz. Lemma v podstatě říká dvě nezřejmé věci: podíl $\frac{x+y\sqrt{d}}{a+b\sqrt{d}}$ je prvek $\mathbb{Z}[\sqrt{d}]$ a zároveň má normu 1. To, že bude mít normu 1 je zjevné – multiplikativitou normy máme

$$N\left(\frac{x + y\sqrt{d}}{a + b\sqrt{d}}\right) = \frac{N(x + y\sqrt{d})}{N(a + b\sqrt{d})} = \frac{k}{k} = 1.$$

Zbývá se tedy zaměřit na to, aby zkoumaný podíl byl prvek $\mathbb{Z}[\sqrt{d}]$. Nu, zkusme prostě přímočaře vydělit s pomocí sdruženého čísla. Dostaneme

$$\frac{x+y\sqrt{d}}{a+b\sqrt{d}} = \frac{(x+y\sqrt{d})(a-b\sqrt{d})}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{(xa-byd)+(ya-xb)\sqrt{d}}{a^2-db^2}.$$

Jmenovatel je nyní norma $a+b\sqrt{d}$, což je k. Modulo k pak pro složky čitatele platí

$$xa-byd \equiv a\cdot a - b\cdot bd \equiv k \equiv 0 \pmod{k}, \qquad ya-xb \equiv b\cdot a - a\cdot b \equiv 0 \pmod{k}.$$

To značí, že k dělí obě složky čitatele, takže $\frac{xa-byd}{k} + \frac{ya-xb}{k}\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, jak jsme chtěli. □

Máme již všechny potřebné ingredience, zbývá už je jen naházet do hrnce.

Věta. *Když přirozené d není čtverec, pak má Pellova rovnice $x^2-dy^2=1$ netriviální řešení.*

Důkaz. Budeme postupovat takto: seženeme si hromadu prvků $\mathbb{Z}[\sqrt{d}]$ se stejnou normou k, které navíc mají stejné složky modulo k. Z těch nám potom druhé lemma vyrobí spoustu jednotek. Na to, abychom takovou hromádku prvků našli, použijeme důsledek Dirichletovy věty, první lemma a nekonečný Dirichletův princip.

Z důsledku Dirichletovy věty máme hromádku nekonečně mnoha dvojic p, q takových, že $\left|\sqrt{d}-\frac{p}{q}\right| < \frac{1}{q^2}$. Dále podle prvního lemmatu každá taková dvojice splňuje $N(p+q\sqrt{d}) < 2\sqrt{d}+1$. Přitom je ale tato norma celé číslo. Máme tedy nekonečnou hromádku čísel $p+q\sqrt{d}$, z nichž každé si vybere jedno z konečně mnoha celých čísel s absolutní hodnotou menší než $2\sqrt{d}+1$. Takových čísel je jen konečně mnoho, takže podle nekonečného Dirichletova principu pro nějaké celé číslo k, $|k| < 2\sqrt{d}+1$ má nekonečně mnoho z našich čísel $p+q\sqrt{d}$ normu k.

Dále chceme z této (stále nekonečné) hromádky čísel vybrat taková, aby všechny racionální složky dávaly stejný zbytek modulo k i všechny iracionální složky dávaly stejný zbytek modulo k. Číslu $p+q\sqrt{d}$ tak prostě přiřaďme dvojici zbytků ($p \bmod k, q \bmod k$). To je nějaká dvojice prvků $\mathbb{Z}_k$ a těch je $|\mathbb{Z}_k|^2 = k^2$, což je konečně mnoho. Opětovným použitím nekonečného Dirichletova principu tak musí být některé dvojici zbytků přiřazeno nekonečně mnoho z našich čísel $p+q\sqrt{d}$.

Máme tedy nekonečnou hromádku čísel, na které můžeme vrhnout druhé lemma. To nám vyrobí velikou spoustu jednotek v $\mathbb{Z}[\sqrt{d}]$. Přesněji, zvolme pevně jedno $a+b\sqrt{d}$ z naší výsledné hromádky. Potom můžeme za $x+y\sqrt{d}$ volit postupně všechna ostatní čísla z hromádky a vždy dostaneme jednotku $\frac{x+y\sqrt{d}}{a+b\sqrt{d}}$ s normou 1. Navíc díky tomu, že jednotlivá $x+y\sqrt{d}$ jsou navzájem různá, zatímco $a+b\sqrt{d}$ je stále stejné, budou takto získané jednotky navzájem různé. Tímto tedy vyrobíme nekonečně mnoho různých jednotek s normou 1 v $\mathbb{Z}[\sqrt{d}]$. Přitom ale triviální jednotky existují jen dvě (1 a -1), takže takto určitě vyrobíme alespoň jedno (resp. dokonce nekonečně mnoho) netriviální řešení Pellovy rovnice. Tím je důkaz hotov. □

Cvičení(*) 14. Nechť je $p \equiv 1 \pmod 4$ prvočíslo. Potom záporná Pellova rovnice $x^2-py^2=-1$ má řešení.

Úloha 5. Nechť je $x+y\sqrt{d}$ fundamentální jednotka v $\mathbb{Z}[\sqrt{d}]$. Dokaž, že pro každé $q \in \mathbb{N}$ existuje $n \in \mathbb{N}$ takové, že číslo $a+b\sqrt{d} = (x+y\sqrt{d})^n$ splňuje $q \mid b$.

Pellova rovnice a dělitelnost

Na závěr našeho povídání o reálných kvadratických okruzích a Pellově rovnici se podíváme na to, co se děje, když při mocnění nějakého $x+y\sqrt{d}$ chceme roznásobit a spočítat racionální a iracionální složku. Toto jsme dosud při vyjadřování jednotek ve tvaru $\pm\omega^n$ taktně obcházeli, avšak ukazuje se, že když trochu nahlédneme pod pokličku, získáme užitečné informace o dělitelnosti v situacích kolem Pellovy rovnice a jednotek v $\mathbb{Z}[\sqrt{d}]$.

Na to si nejprve pořídíme nástroj na roznásobení mocniny součtu $(A+B)^n$, přitom pro nás A, B budou libovolné prvky v nějakém komutativním okruhu R a n bude přirozené číslo. Když rozepíšeme

$$(A+B)^n = \underbrace{(A+B)\cdot(A+B)\cdots(A+B)}_{n\text{-krát}}$$

a budeme roznásobovat, určitě dostaneme nějaký výraz s členy tvaru A^aB^b. Každý takový člen přitom vznikne tak, že si postupně z každé z n závorek vybereme buďto A, nebo B a vynásobíme dohromady, co jsme dostali. Tím pádem mohou vzniknout jen ty členy A^aB^b, v nichž jsou $a, b \in \{0, 1, \ldots, n\}$ a zároveň $a+b=n$, takže budeme mít jen členy ve tvaru $A^{n-k}B^k$.

Kolik celkem takových členů $A^{n-k}B^k$ dostaneme? Každý vznikne z toho, že si při roznásobování v k závorkách vybereme B, zatímco ve zbylých vybereme A. Koeficient u $A^{n-k}B^k$ ve výsledném roznásobení mocniny tak musí být roven počtu způsobů, jak si mezi n nerozlišitelnými předměty (závorkami $(A+B)$) zvolit k z nich (ty, z nichž vezmeme B a nikoliv A). Takovýto počet se v různých oblastech matematiky vyskytuje celkem často, proto pro něj máme značení

$$\binom{n}{k},$$

čemuž říkáme *kombinační číslo* a čteme jej „n nad k“. Kombinační čísla splňují spoustu krásných kombinatorických identit a vztahů, my je však nebudeme potřebovat – postačíme si pouze s definicí „kolika způsoby lze mezi n nerozlišitelnými předměty zvolit k z nich“.

Nahlédli jsme tedy následující:

Věta. (binomická) *V libovolném komutativním okruhu platí*

$$(A+B)^n = \binom{n}{0}A^n + \binom{n}{1}A^{n-1}B + \cdots + \binom{n}{k}A^{n-k}B^k + \cdots + \binom{n}{n-1}AB^{n-1} + \binom{n}{n}B^n.$$

My zde binomickou větu použijeme na rozepsání $(x+y\sqrt{d})^n$. Když nás bude zajímat racionální a iracionální složka výsledku, prostě posbíráme ty členy, ve kterých se $\sqrt{d}$ umocnilo na racionální číslo, a ty, kde zůstalo iracionální $\sqrt{d}$.

Tvrzení. *Nechť v $\mathbb{Z}[\sqrt{d}]$ platí rovnost $a+b\sqrt{d} = (x+y\sqrt{d})^n$, přičemž n je přirozené číslo. Potom $y \mid b$. Pokud je n sudé, pak dokonce $xy \mid b$, zatímco když je n liché, pak $x \mid a$.*

Důkaz. Rozepišme podle binomické věty

$$(x+y\sqrt{d})^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y\sqrt{d} + \binom{n}{2}x^{n-2}y^2d + \cdots + \binom{n}{n}y^n(\sqrt{d})^n.$$

Když budeme procházet členy zleva doprava, tak každý druhý dostane $\sqrt{d}$ v mocnině s lichým exponentem, takže bude iracionální, zatímco zbylé budou mít $\left(\sqrt{d}\right)^{2k}$, z čehož nám vyjde racionální číslo. Má-li tedy být $a+b\sqrt{d} = (x+y\sqrt{d})^n$, můžeme posbírat

$$\begin{aligned} a &= \binom{n}{0}x^n + \binom{n}{2}x^{n-2}y^2d + \binom{n}{4}x^{n-4}y^4d^2 + \cdots, \\ b\sqrt{d} &= \binom{n}{1}x^{n-1}y\sqrt{d} + \binom{n}{3}x^{n-3}y^3d\sqrt{d} + \cdots \end{aligned}$$

Když u $b\sqrt{d}$ pokrátíme všechny $\sqrt{d}$, dostaneme dvě rovnosti v celých číslech, jelikož všechna $\binom{n}{k}$ jsou celá. Důležité je, že nevíme přesně, jakým členem která rovnost končí – pro liché n je $(y\sqrt{d})^n$ iracionální, takže se připočte do $b\sqrt{d}$, zatímco pro sudé je racionální, a přibude tak k a.

Pro b je jedna věc jistá – první člen v

$$b = \binom{n}{1} x^{n-1}y + \binom{n}{3} x^{n-3}y^3 d + \cdots$$

je násobkem y, a když pokračujeme zleva doprava k dalšímu členu, exponent u y se jenom zvýší, takže všechny jednotlivé členy napravo budou násobky y nehledě na to, jakým členem končíme. Tímto posledním členem by mohl být $\binom{n}{n-1} xy^{n-1}d^{\frac{n-2}{2}}$, ten do b přibude pro sudé n. Kdyby tomu tak bylo, pak i člen nejvíce napravo, tedy s nejmenším exponentem u x, byl násobkem xy. Když potom budeme procházet členy směrem doleva, budeme zmenšovat exponent u y a zvětšovat ten u x, až skončíme u členu $\binom{n}{1} x^{n-1}y$, který je stále dělitelný xy. To znamená, že všechny členy budou násobky xy, takže i $xy \mid b$.

Když bude naopak n liché, pak bude člen $\binom{n}{n-1} xy^{n-1}d^{\frac{n-1}{2}}$ (změnil se exponent u d, jelikož v a jsme nekrátili $\sqrt{d}$) posledním členem ve vyjádření a. To ale znamená, že jsem cestou zleva doprava šli od členu s x^n až do členu s xy^{n-1}, takže všechny byly násobky x. To znamená, že v tomto případě $x \mid a$, jak jsme chtěli. □

Cvičení(!) 15. Nechť je $x_0 + y_0\sqrt{d}$ fundamentální jednotka. Potom pro každou jednotku $x + y\sqrt{d}$ platí $x_0y_0 \mid xy$. Totéž platí, když namísto jednotek uvážíme řešení Pellovy rovnice.

Cvičení 16. Pokud celá čísla x, y splňují $x^2 - 37y^2 = 1$, pak $876 \mid xy$.

Příklad. Je dáno přirozené číslo n takové, že $3n+1$ i $4n+1$ jsou čtverce. Dokaž, že n je násobek sedmi.

Řešení. Označme si $a^2 = 3n+1$, $b^2 = 4n+1$ a BÚNO $a, b > 0$. Jakmile budeme něco vědět o a, b, pak dopočteme $n = b^2 - a^2 = (b-a)(a+b)$. Také dovedeme odečíst takové násobky a^2, b^2, abychom vyrušili n, konkrétně

$$4a^2 - 3b^2 = 1.$$

Chceme tedy, aby $2a + b\sqrt{3}$ bylo řešení Pellovy rovnice pro $d = 3$. V $\mathbb{Z}[\sqrt{3}]$ je fundamentálním řešením $\omega = 2 + \sqrt{3}$, takže budeme mít $2a + b\sqrt{3} = \omega^k$ pro nějaké $k \in \mathbb{N}$ (chceme $a, b > 0$, takže před ω^k nemusíme uvažovat $\pm$). Označme $x + y\sqrt{3} = \omega^k$. Potřebujeme, aby x vyšlo sudé – nahlédněme, že to nastane právě pro lichá k. Jelikož 2 je racionální složka ω, tak podle tvrzení pro sudé k vyjde sudé y, zatímco pro lichá k bude x sudé. Přitom x, y musí být nesoudělná, jelikož $x^2 - 3y^2 = 1$, takže pro sudá k je nutně x liché. To značí, že v této úloze potřebujeme uvažovat jen lichá k.

Zapišme $k = 2\ell - 1$ pro nějaké $\ell \in \mathbb{N}$. Platí $\omega^2 = (2+\sqrt{3})^2 = 7 + 4\sqrt{3}$. My chceme stran a a b něco říci o dělitelnosti sedmi, takže přítomnost 7 jako racionální části ω^2 může být poněkud návodná. Upravme

$$\begin{aligned} 2a + b\sqrt{3} &= (2+\sqrt{3})^{2\ell-1}, \\ (2a + b\sqrt{3})(2+\sqrt{3}) &= (2+\sqrt{3})^{2\ell}, \\ (4a+3b) + (2a+2b)\sqrt{3} &= (7+4\sqrt{3})^{\ell}. \end{aligned}$$

Pokud je ℓ sudé, pak podle tvrzení bude 7 jakožto racionální složka na pravé straně dělit $2a + 2b$ jakožto iracionální složku na levé straně, takže $7 \mid a+b$. Pokud bude ℓ naopak liché, pak $7 \mid 4a+3b$. Jenže $4a+3b \equiv 4a+3b-7b \equiv 4(a-b) \pmod 7$, takže toto znamená $7 \mid a-b$. Díky $n = (b-a)(a+b)$ tak platí $7 \mid n$ nehledě na paritu ℓ. Tím je úloha vyřešena.

Úloha 6. Ukaž, že v předchozím příkladu platí i $8 \mid n$, takže $56 \mid n$.

Úloha 7. Je dáno přirozené číslo n takové, že $2n+1$ i $3n+1$ jsou čtverce. Dokaž, že n je násobek čtyřiceti.

Modulíme, tentokráte obecně

V druhé polovině tohoto dílu se podíváme znovu a obecněji na to, jak dělit se zbytkem. V prvním díle jsme si ukázali, jak modulit v celých číslech, a nyní provedeme totéž v obecném okruhu.

Definice. Budiž R komutativní okruh. Pro $a, b, m \in R$ řekneme, že a je *kongruentní* s b *modulo* m (značíme $a \equiv b \pmod{m}$), pokud $m \mid a - b$.

V této definici používáme zcela obecnou definici dělitelnosti – zápis $m \mid a - b$ značí prostě to, že existuje $c \in R$ splňující $a - b = c \cdot m$. Obdobně jako v celých číslech si dále ukážeme, že modulení se chová hezky ke sčítání i násobení.

Tvrzení. *Nechť modulo m platí $a \equiv b$ a zároveň $c \equiv d$. Potom platí i*

$$a + c \equiv b + d \pmod{m} \qquad \text{a} \qquad ac \equiv bd \pmod{m}.$$

Důkaz. Z definice kongruence jsou $a - b$ i $c - d$ násobky m. Potom je ale násobkem m i výraz $(a - b) + (c - d) = (a + c) - (b + d)$, což znamená $a + c \equiv b + d \pmod{m}$. Dále je i každý násobek $a - b$ a $c - d$ stále násobkem m, takže

$$m \mid (a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd$$

neboli $ac \equiv bd \pmod{m}$. □

Cvičení 17. Modulení se chová hezky ke sčítání a násobení, ale k jiným operacím už se hezky chovat nemusí. Rozmysli, že v $\mathbb{Z}[\sqrt{d}]$ (pro kladná i záporná d) obecně $a \equiv b \pmod{m}$ neimplikuje $\overline{a} \equiv \overline{b} \pmod{m}$. Pro $m \in \mathbb{Z}$ už to však platí.

Díky tomu, že se modulení chová hezky ke sčítání a násobení, můžeme v kongruencích provádět úpravy podobně jako v rovnicích, i když tyto úpravy nemusí vždy být ekvivalentní. Můžeme také „zapomenout“, přesně s jakými čísly počítáme – důležitý je jenom jejich zbytek po dělení m.

Definice. Budiž R okruh a $m \in R$. Pro $a \in R$ množinu

$$a \bmod m = \{a + xm : x \in R\}$$

nazýváme *zbytkovou třídou* prvku a modulo m. Množinu všech zbytkových tříd modulo m značíme $R/(m)$.

Víme, že při počítání (sčítání a násobení) modulo m nezáleží na tom, který konkrétní prvek ze zbytkové třídy si vezmeme, na což můžeme nahlížet tak, že počítáme přímo se zbytkovými třídami. Nehledě na to, které a ze zbytkové třídy $a_0 \bmod m$ a b ze zbytkové třídy $b_0 \bmod m$ vezmeme, součet $a + b$ bude patřit do stejné zbytkové třídy. Analogicky platí totéž pro součin ab.

Definice. Na množině $R/(m)$ definujeme sčítání a násobení zbytkových tříd pomocí

$$(a \bmod m) + (b \bmod m) = (a + b) \bmod m, \qquad (a \bmod m) \cdot (b \bmod m) = ab \bmod m.$$

Množina $R/(m)$ s těmito operacemi tvoří okruh a okruhy tohoto tvaru nazýváme *faktorokruhy*.

Poznámka. V definici jsme důsledně zapisovali zbytkovou třídu z okruhu $R/(m)$ jako $a \bmod m$, abychom ji odlišili od prvku a z okruhu R. Běžně však budeme počítání v $R/(m)$ zapisovat jako kongruence, takže místo $(7 \bmod 5) \cdot (-3 \bmod 5) = -21 \bmod 5 = 4 \bmod 5$ zapíšeme jenom $7 \cdot (-3) \equiv -21 \equiv 4 \pmod{5}$. Důležitá je změna pohledu: 7 a -3 zde nejsou celá čísla 7 a -3,

ale jejich zbytkové třídy modulo 5. Nebydlí již v okruhu $\mathbb{Z}$, který má nekonečně mnoho prvků, ale v okruhu $\mathbb{Z}/(5)$, který má jen pět prvků.

Příklad. Počítání modulo m jsem již viděli na celých číslech. Pro nenulové $m \in \mathbb{Z}$ je $\mathbb{Z}/(m)$ jenom jiný zápis pro $\mathbb{Z}_m$. Tato množina má $|m|$ prvků, které můžeme reprezentovat čísly $0, 1, \ldots, m-1$. Z prvního dílu také víme, že faktorokruh $\mathbb{Z}/(m)$ je oborem integrity, právě když je m prvočíslo nebo ± 1.

Příklad. Zbytkové třídy modulo 0 jsou vždy prostě jednoprvkové množiny $a \bmod 0 = \{a\}$, takže faktorokruh $R/(0)$ se chová úplně stejně jako původní R.

Obecně může mít faktorokruh $R/(m)$ nekonečně mnoho prvků i pro $m \neq 0$, nicméně okruhy, se kterými jsme doteď pracovali, nám takto divoké faktorokruhy nedávají. Příklady nekonečných faktorokruhů však potkáme v příštím dílu.

Cvičení 18. Rozmysli si, že když je $u \in R$ jednotka, pak má $R/(u)$ jen jeden prvek (je to tedy triviální okruh).

Příklad. Pro celé číslo $m \neq 0$ má faktorokruh $\mathbb{Z}[\sqrt{d}]/(m)$ přesně m^2 prvků. Tyto zbytkové třídy můžeme reprezentovat čísly $a + b\sqrt{d}$ pro $a, b \in \{0, 1, \ldots, m-1\}$.

Příklad. Ukažme, že faktorokruh $\mathbb{Z}[i]/(2+i)$ má pět prvků. Zaprvé $2 + i \mid N(2+i) = 5$, takže stačí jenom určit, které z prvků $a + bi$, $a, b \in \{0, 1, 2, 3, 4\}$ jsou si kongruentní. Modulo $2 + i$ však platí $i \equiv -2$, takže $a + bi \equiv a - 2b$. Ale $a - 2b$ je celé číslo, takže libovolný prvek $\mathbb{Z}[i]$ je modulo $2+i$ kongruentní nějakému celému číslu. Každá zbytková třída modulo $2 + i$ se tedy dá reprezentovat jedním z čísel 0, 1, 2, 3, 4. Ta jsou však navzájem nekongruentní (stačí uvážit normu rozdílu), takže $\mathbb{Z}[i]/(2+i)$ má přesně pět prvků.

Úloha 8. Pro nenulové $\alpha \in \mathbb{Z}[\sqrt{d}]$ (i pro záporná d) má faktorokruh $\mathbb{Z}[\sqrt{d}]/(\alpha)$ přesně $|N(\alpha)|$ prvků.

Kromě počtu prvků $R/(m)$ se můžeme zajímat i o vlastnosti tohoto faktorokruhu. Následující tvrzení nám bude oslím můstkem do další kapitoly.

Tvrzení. *Nechť $p \in R$ není jednotka. Potom je faktorokruh $R/(p)$ oborem integrity, právě když je p prvočinitel v R.*

Důkaz. Stačí si důsledně rozmyslet definice jednotlivých pojmů a rozklíčovat, že výroky „$R/(p)$ je obor integrity“ a „p je prvočinitel“ říkají doslova to samé. $R/(p)$ je oborem integrity, pokud

$$ab \equiv 0 \pmod{p}$$

nastává právě tehdy, když je a nebo b kongruentní nule modulo p. Jinými slovy, $p \mid ab$ jen tehdy, když $p \mid a$ nebo $p \mid b$, což je však přesně definice prvočinitele. □

V tvrzení požadujeme, aby p nebyla jednotka, neboť modulení jednotkou dá triviální okruh, což je obor integrity, ačkoliv jednotky za prvočinitele nepovažujeme.

Konečná tělesa

Před chvíli jsme si ukázali, že prvočísla jsou hezká v tom smyslu, že nám umí vyrábět obory integrity, tedy okruhy, ve kterých dovedeme krátit v rovnicích.

Ale krácení by se dalo zlepšit. Třeba libovolné dělení by bylo ještě lepší. Ano, ono krácení a dělení je k sobě velmi blízko, ale není to to samé. Například v celých číslech krátit můžeme ($2a = 2b$ je to stejné jako $a = b$), ale dělit již nemůžeme, protože například $2x = 1$ není v celých číslech to stejné jako $x = \frac{1}{2}$, jelikož $\frac{1}{2}$ už je číslo racionální, nikoli celé.

Vidíme, že náš protipříklad na to, že krácení a dělení není to stejné, pracuje s nekonečným oborem integrity. To není náhodou. Kdybychom se omezili pouze na konečné obory, už bychom mohli i beztrestně dělit.

Definice. *Tělesem* rozumíme okruh s alespoň dvěma prvky, kde jsou všechny nenulové prvky jednotkami.

Poznámka. Ekvivalentně řečeno: pro každé $x \in T \setminus \{0\}$ existuje (právě jedno) $y \in T$ takové, že $x \cdot y = 1$. Pro nás je spíše přirozené, že existuje zlomek $\frac{1}{x}$, který leží v tomto tělese, protože jsme na zlomky zvyklí z $\mathbb{Q}$ a používali jsme je i v okruzích $\mathbb{Z}_p$.

To, aby těleso mělo alespoň dva prvky, požadujeme prostě proto, že jednoprvkové (triviální) těleso by často odporovalo tvrzením, která platí pro „rozumná“ tělesa. *Konečným tělesem* rozumíme těleso s konečným počtem prvků. Tělesa se často značí K, F nebo T.[6]

Příklad. $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ jsou tělesa, neboť v nich umíme dělit kterýmkoliv nenulovým prvkem.

Příklad. Pro prvočíslo p je $\mathbb{Z}_p$ těleso. Pro $a \not\equiv 0 \pmod p$ je totiž 1 největším společným dělitelem a a p, takže máme Bézoutovy koeficienty x, y splňující $xa + yp = 1$, z čehož $xa \equiv 1 \pmod p$.

To, že nám prvočísla vyrobí konečné těleso, není náhodou. $\mathbb{Z}_p = \mathbb{Z}/(p)$ má konečně mnoho prvků a jedná se o obor integrity (p je prvočinitel v $\mathbb{Z}$). Dokážeme si, že tyto dvě podmínky stačí k tomu, aby okruh byl tělesem.

Příklad. Okruh $\mathbb{Z}$ je oborem integrity, ale není tělesem. Má přitom nekonečně mnoho prvků. Naproti tomu $\mathbb{Q}$ je také nekonečný obor integrity a tělesem je.

Tvrzení. *Každý konečný obor integrity je též konečným tělesem.*

Důkaz. Z příkladu vidíme, že musíme nějak využít konečnosti. Budiž R konečný obor integrity a a jeho nenulový prvek. Ukažme, že k němu najdeme prvek b takový, že $a \cdot b = 1$.

Vezměme si nekonečnou posloupnost $a, a^2, a^3, a^4, \dots$ Z konečnosti R se v ní někdy musí nějaký prvek zopakovat, takže pro nějaká $m < n$ nastane $a^m = a^n$. To znamená, že $0 = a^n - a^m = a^m(a^{n-m} - 1)$. Z definice oboru integrity je tak a^m nebo $a^{n-m} - 1$ nulové. Pokud $a^m = 0$, tak můžeme definici oboru integrity aplikovat znovu – pokud je součin $a \cdots a$ nulový, je nulový alespoň jeden činitel, z čehož už nutně plyne, že samotné a je nulové, což odporuje předpokladu.

Proto nutně platí, že mocnina a^{m-n} je rovna 1. Pokud tedy zvolíme $b = a^{n-m-1}$, pak splníme $a \cdot b = a \cdot a^{n-m-1} = a^{n-m} = 1$. □

Důsledek. *Když je $p \in R$ prvočinitel a zároveň je $R/(p)$ konečná množina, pak už je $R/(p)$ těleso.*

Důkaz tvrzení lze vést více způsoby. My jsme si vybrali tento, protože jak za chvíli uvidíme, nejmenší exponent r splňující $a^r = 1$ je sám o sobě zajímavý a využívá se v mnoha úlohách. Důsledek tvrzení dává dobrou představu, v jaké podobě nejčastěji konečná tělesa potkáme – jako faktorokruhy modulo prvočinitel.

Příklad. V $\mathbb{Z}[i]$ je $2+i$ prvočinitelem, takže $\mathbb{Z}[i]/(2+i)$ je těleso. Dříve jsme už viděli, že má pět prvků, které můžeme reprezentovat jako 0, 1, 2, 3 a 4. Za povšimnutí stojí, že díky $2+i \mid N(2+i) = 5$ se tento okruh v podstatě chová stejně jako obyčejné $\mathbb{Z}_5$.

Příklad. Taktéž 3 je prvočinitelem v $\mathbb{Z}[i]$, takže $\mathbb{Z}[i]/(3)$ je těleso, neboť má $3^2 = 9$ prvků. Ty můžeme zapsat jako 0, 1, 2, i, $1+i$, $2+i$, $2i$, $1+2i$, $2+2i$. Můžeme ověřit, že ke každému $a \in \mathbb{Z}[i]/(3)$ lze nalézt $\frac{1}{a}$, kupříkladu k $a = 2 + i$ máme $(2 + i)(1 + i) \equiv 1 + 3i \equiv 1 \pmod 3$.

Cvičení(!) 19. Každé těleso je i obor integrity. To značí, že schopnost dělit je silnější než jen krátit v rovnicích.

---

[6] Po řadě z německého *Körper*, anglického *field* a (překvapivě) českého *těleso*. V češtině se lze občas potkat i s označením „pole“, my jej však používat nebudeme.

Z toho už například plyne, že pro složené číslo n okruh $\mathbb{Z}_n$ není těleso, protože není ani obor integrity.

Cvičení 20. Připomeň si, proč $\mathbb{Z}_n$ pro složené n není obor integrity.

Ukažme si některé věty, které nám v konečných tělesech pomohou se zjednodušováním výrazů.

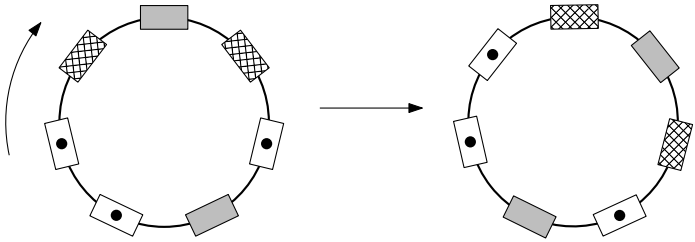
Věta. (malá Fermatova[7]) *Mějme konečné těleso s n prvky. Potom pro každý nenulový prvek a tohoto tělesa platí, že $a^{n-1} = 1$.*

Ukážeme si dva důkazy. První je názorně kombinatorický, nicméně provedeme jej jen pro tělesa $\mathbb{Z}_p$, zatímco druhý funguje pro libovolné konečně těleso.

Důkaz. (korálkový) Představme si, že si chceme vyrobit náhrdelník z korálků. Jak takový náhrdelník vypadá? Jelikož jsme matematici a máme tolik rádi prvočísla, řekli jsme si, že náš náhrdelník bude tvořen p korálky spojenými do kruhu (pro prvočíslo p).

Mít jednobarevný náhrdelník je ale nuda, a tak si každý korálek obarvíme jednou z a barviček. Nyní nás jako matematiky zajímá, kolik různých náhrdelníků takto můžeme vyrobit. To je ale jednoduše a^p, protože na každém z p korálků si vybíráme z a barev.

Po nějaké době, co takový náhrdelník nosíme, si však uvědomíme, že se nám na krku pořád točí, a tudíž jsou náhrdelníky, které se liší jenom pootočením, vlastně stejné. To ale znamená, že jsme některé náhrdelníky započítali ve více otočeních.



Které to jsou? Jednobarevný náhrdelník (těch je přesně a) jsme dvakrát nezapočítali. Naproti tomu náhrdelník, který není jednobarevný, jsme započítali právě p-krát, neboť p je prvočíslo.

Proč tomu tak je? Nechť je pro spor nějaký nejednobarevný náhrdelník započítán méně než p-krát. Pro nějaké k tedy otočením o $k < p$ korálků dostaneme stejný náhrdelník (stejné barvy na jednotlivých pozicích). Toto otočení nyní můžeme provádět opakovaně a vždy tím dostaneme stejný náhrdelník. Díky $k < p$ a prvočíselnosti p jsou k a p nesoudělná, takže pro nějaké x platí $xk \equiv 1 \pmod{p}$. To odpovídá tomu, že když x-krát zopakujeme otočení o k korálků, dostaneme ve výsledku otočení o jeden korálek. Nyní však i toto otočení o jediný korálek vyrobí stále stejný náhrdelník, takže všechny korálky mají stejnou barvu, což je spor.

Všechny náhrdelníky kromě jednobarevných jsme tedy původně započítali p-krát. Celkový počet náhrdelníků, u nichž nehledíme na otočení, je potom $\frac{a^p - a}{p} + a$, neboť z původního počtu a^p bylo a náhrdelníků jednobarevných a pro zbylých $a^p - a$ jsme započítali jen jedno z p otočení. Počet náhrdelníků ale musí být celočíselný, takže $p \mid a^p - a$. Pokud je navíc a nesoudělné s p, pak kongruenci $a^p \equiv a \pmod{p}$ zkrátíme na $a^{p-1} \equiv 1 \pmod{p}$. □

Důkaz. (obecný) Očíslujme si všech $n-1$ nenulových prvků tělesa jako $x_1, \ldots, x_{n-1}$. Dále každý z nich přenásobme nenulovým prvkem a, pro který budeme chtít větu dokázat. Ukažme, že přenásobení tyto prvky jenom zamíchá mezi sebou. Díky tomu, že jich máme jen konečně mnoho, si stačí rozmyslet, že pro $x_i \neq x_j$ bude i $ax_i \neq ax_j$ a že žádné ax_i nebude nulové. Pro spor nechť

[7]Pierre de Fermat (1607–1665) byl francouzský právník a ve volném čase také matematik. K frustraci budoucích generací k většině tvrzení, která objevil, nezanechal žádné důkazy.

$ax_i = ax_j$ pro nějaká $i \neq j$. Jelikož je a nenulové, můžeme jím vydělit, čímž dostaneme $x_i = x_j$, což je spor. Obdobně kdyby $ax_i = 0$, znamenalo by to $x_i = 0$, což neplatí.

Z toho už nutně plyne, že posloupnost $ax_1, ax_2, \ldots, ax_{n-1}$ se od $x_1, x_2, \ldots, x_{n-1}$ liší jen pořadím svých prvků. Když tedy všechny prvky jedné posloupnosti vynásobíme dohromady a s druhou provedeme totéž, určitě dostaneme stejný součin. To nám dává rovnost

$$x_1 \cdot x_2 \cdots x_{n-1} = ax_1 \cdot ax_2 \cdots ax_{n-1} = a^{n-1} \cdot x_1 \cdot x_2 \cdots x_{n-1}.$$

V součinu $x_1 \cdot x_2 \cdots x_{n-1}$ se vyskytují jen nenulové prvky, takže je sám nenulový (těleso je i obor integrity), tudíž jím můžeme obě strany vydělit Tím už dostáváme kýženou rovnost $a^{n-1} = 1$. □

Cvičení 21. Urči zbytek 29^{25} po dělení 11.

Cvičení 22. Urči zbytek $(11 + 7i)^{18}$ po dělení 3.

Úloha 9. Urči zbytek $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ po dělení 7.

Úloha 10. (těžší) Urči, která přirozená čísla x jsou nesoudělná se všemi členy posloupnosti $a_n = 2^n + 3^n + 6^n - 1$.

Úloha 11. Najdi všechna celočíselná řešení rovnice $x^5 + 2 = 101^y$.

Mějme na paměti, že malá Fermatova věta platí pro konečná *tělesa*, takže pro faktorokruhy, které nejsou konečnými tělesy, taková identita platit nemusí. Když například budeme v $\mathbb{Z}$ modulit složeným číslem $9 = 3 \cdot 3$, narazíme na $2^8 \equiv 4 \not\equiv 1 \pmod 9$. Někdy dokonce mocněním nenulového prvků můžeme dostat nulu, jako třeba $3^2 \equiv 0 \pmod 9$.

Ve skutečnosti i pro složené moduly máme identitu podobnou malé Fermatově větě, jenom s jiným exponentem a s omezením na základ mocniny. Uvedeme ji bez důkazu a budeme se dále věnovat konečným tělesům.

Věta. (Eulerova[8]) *Nechť $\varphi(n)$ značí počet jednotek v okruhu $\mathbb{Z}_n$. Pak pro jednotku $a \in \mathbb{Z}_n$ platí $a^{\varphi(n)} \equiv 1 \pmod n$.*

Zatímco malá Fermatova věta říká, co získáme mocněním jednoho prvku, ta následující zase pomáhá tam, kde vynásobíme (skoro) všechny prvky tělesa.

Věta. (Wilsonova[9]) *Buď T těleso s $n - 1$ nenulovými prvky $a_1, a_2, \ldots, a_{n-1}$. Potom platí*

$$a_1 a_2 \cdots a_n = -1,$$

kde -1 značí prvek splňující $(-1) + 1 = 0$.

Důkaz. Využijeme toho, že v tělese je každý nenulový prvek jednotkou, takže pro $a \in T$ existuje (jednoznačně určené) $\frac{1}{a}$. Můžeme tak spárovat a s $\frac{1}{a}$ a v rámci součinu je znásobit na jedničku.

Párování a s $\frac{1}{a}$ se nám rozbije, pokud $a = \frac{1}{a}$ neboli $a^2 = 1$. To však značí $0 = a^2 - 1 = (a-1)(a+1)$, takže to může nastat jen pro $a = 1$ nebo $a = -1$. Všechny zbylé prvky se nám tudíž podaří spárovat, takže zbude $a_1 a_2 \cdots a_n = 1 \cdot (-1) = -1$. Kdyby platilo $1 = -1$ (například v $\mathbb{Z}_2$), zbude nám jen jeden nespárovaný prvek $1 = -1$, takže součin stále vyjde -1. □

Úloha 12. Je dáno $n > 1$. Urči, jaké $x \in \mathbb{Z}_n$ v závislosti na n splňuje $(n-1)! \equiv x \pmod n$.

---

[8] Leonhard Euler (1707–1783), švýcarský matematik, výrazně rozvinul takřka všechna odvětví tehdejší matematiky, některá další svou prací založil a k tomu také zavedl či ustálil mnoho prvků moderní matematické notace. Výsledky a koncepty po něm pojmenované lze v matematice potkat prakticky kdekoliv.

[9] John Wilson (1741–1793) byl anglický matematik. Jak už to tak bývá, Wilsonova věta byla známa již dlouho před ním.

Charakteristika*

V této sekci se podíváme na vlastnost tělesa naznačující, kterému $\mathbb{Z}_p$ (anebo $\mathbb{Q}$) se toto těleso tak nějak podobá.

Definice. *Charakteristika* tělesa T je nejmenší číslo c takové, že součet c jedniček v T je roven 0. Pokud takové c neexistuje, pak říkáme, že charakteristika je 0.

Cvičení 23. Rozmysli si, která známe tělesa s charakteristikou 0.

Tvrzení. *Každé konečné těleso má nenulovou charakteristiku.*

Důkaz. Stačí použít podobnou techniku jako v důkazu, že konečný obor integrity je těleso. Namísto mocnin si vezměme nekonečnou posloupnost

$$1, \qquad 1+1, \qquad 1+1+1, \qquad 1+1+1+1, \ldots$$

Jelikož máme konečné těleso, víme, že nějaké dva prvky musí být v této posloupnosti stejné. Tedy součet m jedniček je roven součtu n jedniček pro nějaká $m < n$. Potom je jejich rozdíl nula a zároveň součet $n-m$ jedniček, tedy $\underbrace{1+1+\cdots+1}_{(n-m)\text{-krát}} = 0$. Charakteristika tělesa tedy není 0. □

Cvičení(!) 24. Nechť má těleso T charakteristiku $c > 0$. Pak je součet n jedniček nulový, právě když $c \mid n$.

Tvrzení. *Každé těleso, které má nenulovou charakteristikou, ji má dokonce prvočíselnou.*

Důkaz. Nechť je pro spor charakteristika složené číslo $c = ab$, kde a i b jsou vetší než 1. Poté si vezměme prvky představující součty a a b jedniček. Vytknutím závorek potom dostáváme, že

$$0 = \underbrace{1+1+\ldots+1}_{c\text{-krát}} = \underbrace{(1+1+\ldots+1)}_{a\text{-krát}} \cdot \underbrace{(1+1+\ldots+1)}_{b\text{-krát}}.$$

Víme také, že každé těleso je obor integrity, a tudíž alespoň jedna ze závorek na pravé straně musí být nulová. To je ale spor s tím, že c je nejmenší počet jedniček, které se posčítají na nulu, protože a i b jsou obě menší. □

Charakteristika je velmi užitečná vlastnost, protože se dá ukázat, že konečné těleso s charakteristikou p má p^k prvků pro nějaké přirozené k. Lze také dokázat, že pro každé prvočíslo p a přirozené číslo k existuje konečné těleso s p^k prvky. Dá se dokonce dokázat i to, že struktura konečného tělesa je v jistém smyslu jednoznačně určena tím, kolik má prvků, takže všechna tělesa se stejným počtem prvků jsou „stejná“. Poslední dvě tvrzení však poněkud přesahují možnosti našeho seriálu, proto se omezíme na to první.

Tvrzení. *Nechť je prvočíslo p charakteristikou konečného tělesa T. Pak má T právě p^k prvků pro nějaké přirozené k.*

Důkaz. Budiž n počet prvků T. Dokážeme toto: když prvočíslo q dělí n, potom je $q = p$, tedy jiné prvočíslo než charakteristika nemůže dělit počet prvků. Z toho už vyplyne, že n musí být mocnina p, tedy p^k a zároveň $n > 1$, takže $k > 0$.

Mějme tedy nějaké prvočíslo $q \mid n$. Provedeme trik podobný počítání náhrdelníků v důkazu malé Fermatovy věty. Podíváme se, kolik existuje uspořádaných q-tic $(a_0, a_1, \ldots, a_{q-1})$ prvků T takových, že $a_0 + \cdots + a_{q-1} = 0$. Na jednu stranu hned nahlédneme, že jich je n^{q-1}. Vždy si totiž můžeme zcela libovolně zvolit čísla $a_1, \ldots, a_{q-1}$ a zbývající číslo a_0 je pak jednoznačně určeno jako $a_0 = -(a_1 + \cdots + a_{q-1})$. Při výběru každého jednotlivého a_i máme n možností a tyto možnosti jsou nezávislé, což dá celkem n^{q-1} způsobů, jak vybrat prvních $q-1$ čísel.

Nyní tyto q-tice začneme rotovat. Orotováním q-tice $(a_0, a_1, \ldots, a_{q-1})$ o j míst budeme myslet to, že z ní vyrobíme q-tici $(a_j, a_{1+j}, \ldots, a_{q-1+j})$, přičemž se na indexy díváme, jako by byly modulo

q, tedy a_q je totéž co a_0 atp. Takovýmto orotováním nezměníme to, že součet celé q-tice je nula. Rotováním o $j = 0, 1, \ldots, q-1$ tak vyrobíme q nějakých q-tic – budou však navzájem různé. Jsou-li některé dvě stejné, nechť je to BÚNO rotace o 0 a o nějaké $0 < j < q$. To potom znamená, že

$$a_0 = a_j = a_{2j} = a_{3j} = \cdots$$

Jenže q je prvočíslo, takže v posloupnosti $0, j, 2j, 3j \ldots$ se vyskytnou všechny zbytky modulo q.

Z toho plyne, že q-tice složené ze stejných čísel $(a, a, \ldots, a)$ jsou výjimečné. Kolik jich existuje? Pro všechny ostatní q-tice, které obsahují nějaké různé prvky, už máme všech q rotací odlišných, takže počet q-tic s různými prvky je násobek q. Zároveň je ale počet všech q-tic roven n^{q-1}, což je podle předpokladu $q \mid n$ také násobek q. Tím pádem musí i počet q-tic tvaru $(a, a, \ldots, a)$ být násobkem q. Tento počet však není nula, protože máme q-tici $(0, 0, \ldots, 0)$, jejíž součet určitě je 0. Aby tedy počet těchto q-tic byl násobek q, musí existovat ještě nějaká další q-tice $(a, a, \ldots, a)$ jejíž součet je 0 a zároveň $a \neq 0$. Potom však v rovnosti

$$\underbrace{a + a + \cdots + a}_{q\text{-krát}} = 0$$

stačí vynásobit prvkem $\frac{1}{a}$ a dostaneme

$$\underbrace{1 + 1 + \cdots + 1}_{q\text{-krát}} = 0.$$

To podle dřívějšího cvičení znamená $p \mid q$. Jenže p i q jsou prvočísla, takže $p = q$, což jsme přesně chtěli dokázat. □

Příklad. Pro prvočíslo p je $\mathbb{Z}_p$ konečné těleso s charakteristikou p a s p^1 prvky.

Příklad. Okruh $\mathbb{Z}[i]/(3)$ je konečné těleso s charakteristikou 3 a s $9 = 3^2$ prvky.

Příklad. Vyrobme si těleso s charakteristikou 2 a s $8 = 2^3$ prvky. Vezmeme okruh $\mathbb{Z}_2$ a přidáme k němu prvek α, kterému přiřkneme vlastnost $\alpha^3 = \alpha + 1$. Každý prvek okruhu $\mathbb{Z}_2[\alpha]$ potom budeme moci zapsat jako $a + b\alpha + c\alpha^2$ pro $a, b, c \in \mathbb{Z}_2$, a vždy když dva vynásobíme, tak výsledek bude opět možno vyjádřit pomocí 1, α a α^2, neboť každé α^3 přepíšeme na $\alpha+1$ (obdobně s vyššími mocninami). Celkově tak tento okruh bude mít osm prvků

$$0, \qquad 1, \qquad \alpha, \qquad 1+\alpha, \qquad \alpha^2, \qquad 1+\alpha^2, \qquad \alpha+\alpha^2, \qquad 1+\alpha+\alpha^2.$$

Že se jedná o těleso, není na první pohled zřejmé, ale je tomu tak, neboť každé $x \in \mathbb{Z}_2[\alpha]$ k sobě má y takové, že $xy = 1$. Například pro $x = 1 + \alpha^2$ vyhoví $y = \alpha$, neboť

$$(1 + \alpha^2) \cdot \alpha = \alpha + \alpha^3 = \alpha + (\alpha + 1) = (1 + 1)\alpha + 1 = 1.$$

Primitivní prvek

Podívejme se znovu a důkladněji na mocnění v konečných tělesech. Malá Fermatova věta nám dává jistotu, že v n-prvkovém tělese nám umocnění nenulového prvku na $n-1$ vyrobí jedničku. Nestačil by ale nějaký menší exponent?

Definice. *Řádem* nenulového prvku a rozumíme nejmenší přirozené číslo r takové, že $a^r = 1$.

Ekvivalentně nám řád říká, kolik různých prvků se vyskytne v posloupnosti $a^1, a^2, a^3, \ldots$

Tvrzení. *Nechť je r řád prvku a. Potom $a^n = 1$, právě když $r \mid n$.*

Důkaz. Když $r \mid n$, pak zjevně $a^n = 1^{\frac{n}{r}} = 1$. Pokud naopak $r \nmid n$, pak skrze dělení se zbytkem platí $n = rq + x$ pro nějaké $0 < x < r$. Následně platí $a^n = a^{x+rq} = a^x \cdot 1^q = a^x$, což nemůže být jedna, neboť to by byl vzhledem k $0 < x < r$ spor s definicí řádu. □

Cvičení(!) 25. Mějme řád r nenulového prvku a nějakého n-prvkového tělesa. Dokaž, že $r \mid n-1$.

Cvičení 26. Najdi nejmenší liché prvočíslo p, které dělí $89^8 + 1$.

Cvičení(!) 27. Budiž r řádem a. Potom když $k \mid r$, pak má a^k řád $\frac{r}{k}$.

Spousta prvků může mít řád menší než $n-1$. Zaměříme se na ty, které jej mají největší možný.

Definice. *Primitivním prvkem* tělesa s n prvky rozumíme takový prvek g, který má řád $n-1$.

Poznámka. Ekvivalentně můžeme říci, že v posloupnosti $g^1, g^2, \ldots, g^{n-1}$ vystupuje každý nenulový prvek tělesa právě jednou. Z tohoto důvodu se primitivnímu prvku též někdy říká *generátor*, a proto jej často značíme g.

Příklad. V tělese $\mathbb{Z}_7$ je 3 primitivním prvkem, neboť

$$3^1 \equiv 3, \qquad 3^2 \equiv 2, \qquad 3^3 \equiv 6, \qquad 3^4 \equiv 4, \qquad 3^5 \equiv 5, \qquad 3^6 \equiv 1.$$

Příklad. V tělese $\mathbb{Z}[i]/(3)$ je $1+i$ primitivním prvkem, neboť

$$(1+i)^1 \equiv 1+i, \qquad (1+i)^2 \equiv 2i, \qquad (1+i)^3 \equiv 1+2i, \qquad (1+i)^4 \equiv 2,$$
$$(1+i)^5 \equiv 2+2i, \qquad (1+i)^6 \equiv i, \qquad (1+i)^7 \equiv 2+i, \qquad (1+i)^8 \equiv 1.$$

Věta. *Každé konečné těleso obsahuje primitivní prvek.*

Důkaz je trochu techničtější, proto se k němu propracujeme postupně přes několik lemmat.

Lemma. (první) *Rovnice $x^n = 1$ má v konečném tělese nanejvýš n řešení.*

Ve třetím díle seriálu si dokážeme o něco obecnější tvrzení. Nyní si ukážeme alespoň náznak důkazu, proč by něco takového mělo platit.

Náznak důkazu. Převedeme 1 na levou stranu a budeme pracovat s $x^n - 1 = 0$. Myšlenka důkazu je, že kdykoliv bude a řešením rovnice, vytkneme na levé straně činitel $(x-a)$. Jak to provedeme? Když je a řešením rovnice, znamená to $a^n - 1 = 0$, takže můžeme levou stranu naší rovnice přepsat jako

$$x^n - 1 = (x^n - 1) - 0 = (x^n - 1) - (a^n - 1) = x^n - a^n = (x-a)(x^{n-1} + x^{n-2}a + \cdots + xa^{n-2} + a^{n-1}).$$

Tím jsme úspěšně vytknuli $(x-a)$. Co když bude nyní nějaké $b \neq a$ dalším řešením? Inu, pokud má při dosazení $x = b$ býti $(x-a)(x^{n-1} + \cdots + a^{n-1}) = 0$, pak musí alespoň jedna ze dvou závorek vyjít nula. Jenže díky $b - a \neq 0$ to nemůže být ta první, musí to být tedy ta druhá. To znamená, že b je řešením nové rovnice vzniklé z druhé závorky, ve které máme o jedna menší největší exponent u x. Dále opakujeme stejný trik: když je b řešením, upravíme

$$x^{n-1} + x^{n-2}a + \cdots + xa^{n-2} + a^{n-1} =$$
$$= (x^{n-1} + x^{n-2}a + \cdots + xa^{n-2} + a^{n-1}) - (b^{n-1} + b^{n-2}a + \cdots + ba^{n-2} + a^{n-1}).$$

Toto však stačí přeuspořádat tak, že dáme k sobě odpovídající mocniny x^k a b^k. Dostaneme tak součet výrazů tvaru $(x^k - b^k) \cdot$ něco. V každém z těchto členů dovedeme vytknout $x - b$, takže toto můžeme vytknout z výrazu jako celku. Tím původní rovnici přepíšeme do tvaru $(x-a)(x-b)$(nějaký výraz s x^{n-2}) $= 0$.

Takto pokračujeme dál a dál. V každém kroku vytkneme dvojčlen odpovídající jednomu řešení a snížíme tím největší exponent u x ve „zbývajícím výrazu“ o jedna. Tím pádem nebudeme moci

vytknout více než n členů: po n vytknutých závorkách by nám zbyla jenom nějaká konstanta, ze které už žádné $x - d$ vytknout nepůjde. □

Zbylá dvě lemmata se budou zabývat tím, jak získat prvek s řádem, který je násobkem řádů dalších prvků.

Lemma. (druhé) *Pokud mají a a b řády m a n, kde m, n jsou nesoudělná, pak má ab řád mn.*

Důkaz. Podívejme se na řád r prvku ab a dokažme, že je roven mn. Jelikož m a n jsou řády a a b, platí $ab^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1$. Každý exponent, který v mocnině vyrobí jedničku, musí být násobek řádu, takže $r \mid mn$.

Nyní dokažme opačnou dělitelnost. Víme, že $1 = (ab)^r = a^r b^r$. Umocněním obou stran rovnosti na m dostáváme $1 = 1^m = a^{rm} b^{rm} = (a^m)^r b^{rm} = b^{rm}$. Řád b tak musí dělit rm, tedy $n \mid rm$. Jenže m je s n nesoudělné, takže v dělitelnosti nehraje roli, pročež $n \mid r$. Analogicky umocněním $1 = a^r b^r$ na n dostaneme $m \mid r$. Dohromady je r násobkem n i m, takže z jejich nesoudělnosti i $mn \mid r$. Spojením dělitelností $r \mid mn$ a $mn \mid r$ pak máme $r = mn$. □

V obecném případě se nám ale stane, že řády nemusí být nesoudělné. Proto si druhé lemma vylepšíme, abychom pro každá a, b byli schopni najít prvek, jehož řád je dělitelný řádem a i b.

Lemma. (třetí) *Pro každé dva prvky a a b s řády m a n umíme najít prvek, jehož řád je nejmenší společný násobek m a n.*

Důkaz. Nechť $\operatorname{nsn}(m,n)$ značí nejmenší společný násobek. Upravme si zadané prvky tak, abychom získali nesoudělné řády – pak budeme moci použít druhé lemma. Nejprve si z m, n vyrobme nějaké jejich dělitele m', n', kteří budou nesoudělní a přitom splní $m' \cdot n' = \operatorname{nsn}(m,n)$. Nechť jsou $p_1, \ldots, p_k$ všechna prvočísla, která dělí m nebo n. Dále nechť jsou $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ prvočíselné rozklady našich řádů. Pro každé $i = 1, \ldots, k$ se podíváme na mocniny p_i v rozkladech m a n. U toho řádu, který má tuto mocninu větší, ji ponecháme, zatímco tomu s menší mocninou ji celou sebereme[10] – a takto vytvoříme m', n'. Formálněji, nechť

$$\alpha_i' = \begin{cases} \alpha_i, & \text{pokud } \alpha_i \geq \beta_i, \\ 0, & \text{pokud } \alpha_i < \beta_i, \end{cases} \qquad \beta_i' = \begin{cases} 0, & \text{pokud } \alpha_i \geq \beta_i, \\ \beta_i, & \text{pokud } \alpha_i < \beta_i \end{cases}$$

a následně položme $m' = p_1^{\alpha_1'} \cdots p_k^{\alpha_k'}$ a $n' = p_1^{\beta_1'} \cdots p_k^{\beta_k'}$. Tím docílíme

$$m' \cdot n' = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} = \operatorname{nsn}(m,n),$$

neboť jsme zachovali největší mocninu každého p_i. Zároveň budou m' a n' nesoudělná, neboť nesdílejí žádná prvočísla ve svých prvočíselných rozkladech.

Nyní ještě vyrobme prvky a', b', které budou mít řády m', n'. Rozmysleme si, že stačí vzít $a' = a^{m/m'}$, $b' = b^{n/n'}$. Z konstrukce m' platí $m' \mid m$, takže m/m' je přirozené číslo, které je také dělitelem m. Pro získání a' tak jenom a mocníme na nějaký dělitel jeho řádu. Podle dřívějšího cvičení už víme, že řád výsledku bude jen původní řád vydělený exponentem, takže a' má řád m'. Obdobně má b' řád n'. V této situaci už můžeme použít druhé lemma, takže $a'b'$ má řád $m'n' = \operatorname{nsn}(m,n)$. □

Skloubením prvního a třetího lemmatu už nyní svedeme dokázat, že primitivní prvek existuje v každém tělese.

Důkaz věty. Nechť má uvažované těleso n prvků. Ty nenulové z nich si očíslujme $a_1, \ldots, a_{n-1}$ a nechť mají řády $r_1, \ldots, r_{n-1}$. Podle třetího lemmatu můžeme vzít kterékoliv dva prvky a nalézt prvek, jehož řád je násobkem obou řádů původních dvou prvků. Opakovaným použitím tohoto

[10] V případě rovnosti příslušnou mocninu ponecháme třeba v m'.

lemmatu (nejprve na první dva prvky, potom na výsledek a na třetí prvek atd.) tak dovedeme najít nějaký prvek g s řádem m, který je násobkem všech r_i.

Ukážeme $m = n-1$, což už bude znamenat, že g je primitivní prvek. Zaprvé m je řádem nějakého prvku tělesa, takže určitě $m \mid n-1$, z čehož $m \leq n-1$. Z druhé strany se podívejme na rovnici $x^m = 1$. Řád každého a_i dělí m, takže $a_i^m = 1$. To je $n-1$ různých řešení rovnice $x^m = 1$, takže podle prvního lemmatu nutně $n-1 \leq m$. Dohromady tak $m = n-1$, takže g je primitivní prvek. □

Poznámka. Dokázali jsme, že existuje alespoň jeden primitivní prvek, což ale neznamená, že existuje právě jeden – typicky jich máme více. Pro použití primitivního prvku nám to nijak nevadí, jde nám jenom o to, abychom dovedli nenulové prvky tělesa vypsat jako geometrickou posloupnost $g^1, g^2, \ldots, g^{n-1}$.

Využití primitivního prvku

Důkaz byl trochu pracnější, ale uvidíme, že primitivní prvek je opravdu silný nástroj. Tvrzení, která by jinak byla nejasná či pracná, se často stávají přímočaře nahlédnutelnými, když si nenulové prvky tělesa zapíšeme jako $g^1, g^2, \ldots, g^{n-1}$.

Tvrzení. (geometrická řada) *Pokud v tělese máme prvek $a \neq 1$, pak $1+a+a^2+\cdots+a^k = \frac{a^{k+1}-1}{a-1}$.*

Důkaz. Stačí obě strany vynásobit $a-1$, potom se na levé straně většina členů vyruší a zbude platná rovnost. □

Pokud řada začíná členem a, je třeba vytknout a, tedy $a + a^2 + \cdots + a^k = a \cdot \frac{a^k-1}{a-1}$.

Příklad. Nechť je p prvočíslo. Najdi všechna přirozená k, pro která p dělí $1^k + \cdots + (p-1)^k$.

Řešení. Nechť je g primitivní prvek v $\mathbb{Z}_p$. Čísla $1, \ldots, p-1$ můžeme (v nějakém jiném pořadí) zapsat jako $g^1, g^2, \ldots, g^{p-1}$. Uvažovaný součet se tím (modulo p) upraví na

$$g^k + g^{2k} + g^{3k} + \cdots + g^{(p-1)k}.$$

Pokud $g^k \not\equiv 1$, pak toto vzorcem pro součet geometrické řady vyjde

$$g^k \cdot \frac{g^{(p-1)k}-1}{g^k-1} \equiv g^k \cdot \frac{1^k-1}{g^k-1} \equiv 0 \pmod{p}.$$

Naopak pokud $g^k \equiv 1$, pak máme v součtu $p-1$ jedniček, takže dostaneme $p-1 \equiv -1 \not\equiv 0$. Zbývá tedy jenom rozhodnout, kdy $g^k \equiv 1$. To však z definice primitivního prvku nastává, právě když $p-1 \mid k$. Zadaný součet je tak násobkem p, právě když $p-1 \nmid k$.

Úloha 13. Rozhodni, zda lze tabulku 10×10 vyplnit čísly $1, 2, \ldots, 100$ a zvolit $A, B \in \mathbb{Z}_{101}$ tak, aby platilo:

(i) Součin prvků libovolného řádku dává po dělení 101 zbytek A.

(ii) Součet prvků libovolného sloupce dává po dělení 101 zbytek B.

Cvičení 28. Dokaž Wilsonovu větu pomocí primitivního prvku pro těleso s lichým počtem prvků.

Definice. Nechť je T těleso. O množině $S \subseteq T$ řekneme, že je *multiplikativní*, pokud je neprázdná, $0 \notin S$ a zároveň je S uzavřená na násobení, tedy kdykoliv $a, b \in S$, pak i $ab \in S$.

Příklad. V tělese $\mathbb{Z}_7$ máme multiplikativní množiny $\{1\}$, $\{1, 6\}$, $\{1, 2, 4\}$ a $\{1, 2, 3, 4, 5, 6\}$.

Tvrzení. *Nechť je T konečné n-prvkové těleso s primitivním prvkem g. Potom jde jeho každou multiplikativní podmnožinu S popsat pomocí vhodného $m \mid n-1$ jako*

$$S = \{g^m, g^{2m}, g^{3m}, \ldots, g^{(n-2)m}, g^{(n-1)m}\}.$$

Posléze pro nenulové $a \in T$ platí $a \in S$, právě pokud $a^{\frac{n-1}{m}} = 1$, a množina S tak má $\frac{n-1}{m}$ prvků.

Důkaz. Vypišme si všechny nenulové prvky T v pořadí $g^1, g^2, g^3, \ldots, g^{n-1}$. Nechť je m nejmenší exponent, pro který $g^m \in S$. Postupným násobením g^m dovedeme vyrobit i $g^{2m}, g^{3m}, \ldots$, takže z definice multiplikativní množiny musí i tyto prvky ležet v S. Dále také platí $g^{-1} = g^{n-2}$, jelikož $g \cdot g^{n-2} = g^{n-1} = 1$, takže i $g^{-m} = g^{(n-2)m} \in S$. Z toho už $g^{xm} \in S$ pro libovolné celé číslo x.

Ukažme, že jiné prvky než mocniny g^m už v S neleží. Uvažujme nějaké $g^k \in S$ a dokažme $m \mid k$. Nechť je d největší společný dělitel m a k. Pak existují Bézoutovy koeficienty x, y takové, že $xm + yk = d$. BÚNO nechť $y > 0$ (vždycky můžeme x snížit o $n-1$ a y zvýšit o m). Potom máme

$$g^d = g^{xm+yk} = g^{xm} \cdot \left(g^k\right)^y.$$

Přitom g^{xm} je prvek S a g^k je prvek S, takže na pravé straně máme jenom součin několika prvků S, což znamená i $g^d \in S$. Jenže m má být nejmenší exponent s touto vlastností, takže $d \geq m$. Ale $d \mid m$, takže $d \leq m$. Proto už nutně $d = m$, takže m je dělitel k, jak jsme chtěli.

Speciálně i $(g^m)^{n-1} = 1 = g^{n-1}$ je prvkem S, takže i $m \mid n-1$, jak jsme chtěli. Zbývá tak dokázat, že $a \in S$, právě pokud $a^{\frac{n-1}{m}} = 1$. Zapišme $a = g^b$ pro nějaké b, pak je rovnost $a^{\frac{n-1}{m}} = 1$ ekvivalentní $g^{\frac{b(n-1)}{m}} = 1$. Jenže g má řád $n-1$, takže toto je ekvivalentní $n-1 \mid \frac{b(n-1)}{m}$ neboli $\frac{b}{m} \in \mathbb{Z}$ neboli $m \mid b$. To ale přesně odpovídá tomu, že $a = g^b = g^{xm} \in S$.

Konečně díky tomu, že každá m-tá mocnina g leží v S a v celém T máme $n-1$ prvků $g^1, g^2, \ldots, g^{n-1}$, už musí S mít $\frac{n-1}{m}$ prvků. □

Cvičení 29. Nechť je S multiplikativní množina v konečném tělese. Potom pokud má S více než jeden prvek, pak je součet všech prvků S roven 0.

Cvičení(!) 30. Mějme n-prvkové těleso T a přirozené číslo k. Zobrazení $f(x) = x^k$ je na T prosté[11], právě když je k nesoudělné s $n-1$.

Úloha 14. (těžší) Posloupnost $\{a_n\}$ je definována předpisem $a_1 = 1$ a pro další členy $a_{k+1} = a_k^3 + 1$. Dokaž, že pro každé prvočíslo p tvaru $3\ell + 2$ (pro $\ell \in \mathbb{N}$) je nějaké a_n násobkem p.

Kvadratické zbytky

Na závěr se podívejme na velmi konkrétní příklad multiplikativní množiny prvků, které se dají zapsat jako druhé mocniny. Během seriálu jsme již několikrát využili, že výraz x^2 většinou nemůže modulo nějaké pevně zvolené n nabývat úplně libovolných hodnot: například modulo 4 dávají čtverce celých čísel jenom zbytky 0 a 1. Podívejme se, jak to vypadá v konečných tělesech.

Definice. O prvku a konečného tělesa T říkáme, že je to *kvadratický zbytek*, pokud pro něj existuje prvek x splňující $x^2 = a$. V opačném případě říkáme, že a je *kvadratický nezbytek*.

Pozorování. *Nenulové kvadratické zbytky tvoří v tělese T multiplikativní množinu.*

Důkaz. Nechť je S množina nenulových kvadratických zbytků. Z $a, b \in S$ plyne $a = x^2$, $b = y^2$ pro nějaká $x, y \in T$, takže $ab = (xy)^2$. Zároveň z nenulovosti a, b je i ab nenulové, takže $ab \in S$. □

Důsledek. (Eulerovo kritérium) *Mějme konečné těleso T s n prvky, kde n je liché. Potom pro nenulový prvek a platí*

$$a^{\frac{n-1}{2}} = \begin{cases} 1, & \text{je-li } a \text{ kvadratický zbytek,} \\ -1, & \text{je-li } a \text{ kvadratickým nezbytkem.} \end{cases}$$

Důkaz. Nechť je g primitivní prvek v T. Pro jaké m tvoří multiplikativní množinu kvadratických zbytků právě $g^m, g^{2m}, g^{3m}, \ldots$? Pro $m = 2$ budou všechny exponenty sudé, takže dostaneme samé

[11] Zobrazení f je *prosté*, zobrazuje-li různé vzory na různé obrazy, tedy $x \neq y \implies f(x) \neq f(y)$.

kvadratické zbytky. Naopak když je $a = x^2$ nenulový kvadratický zbytek, potom $x = g^k$ pro nějaké k, takže $a = g^{2k}$. Zároveň z předpokladu $2 \mid n-1$, takže vše funguje a nenulové kvadratické zbytky jsou přesně $g^2, g^4, g^6 \ldots$

Z tvrzení o multiplikativních množinách to znamená, že $a \neq 0$ je kvadratickým zbytkem, právě když $a^{\frac{n-1}{2}} = 1$. Naopak když je a kvadratickým nezbytkem, tak $a^{\frac{n-1}{2}}$ není 1, ale stále platí $a^{n-1} = 1$, což upravíme na $\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right) = 0$. První závorka není nulová, takže je nulová ta druhá, tedy $a^{\frac{n-1}{2}} = -1$. □

Obvykle se výrazu $a^{\frac{n-1}{2}}$ pro prvek a v n-prvkovém tělese T říká *Legendreův*[12] *symbol* a značí se $\left(\frac{a}{T}\right)$. Pro $T = \mathbb{Z}_p$ se ujalo jednoduší značení $\left(\frac{a}{p}\right)$. Ukažme si nyní, jaké úlohy se tímto dají vyřešit.

Cvičení(!) 31. Pro liché n je v n-prvkovém tělese přesně $\frac{n+1}{2}$ kvadratických zbytků (včetně 0).

Úloha 15. Nechť je T konečné těleso s lichým počtem prvků. Pak pro každé $a \in T$ existují $x, y \in T$ taková, že $a = x^2 + y^2$.

Cvičení 32. Pokud je n liché a větší než 3, pak je součet všech kvadratických zbytků v n-prvkovém tělese roven 0.

Cvičení 33. Modulo liché prvočíslo p je -1 kvadratický zbytek, právě když $p \equiv 1 \pmod 4$.

Cvičení(!) 34. Rozmysli si, že Legendreův symbol je multiplikativní, tedy $\left(\frac{ab}{T}\right) = \left(\frac{a}{T}\right) \cdot \left(\frac{b}{T}\right)$.

Příklad. Mějme liché prvočíslo p. Dokaž, že existuje celé číslo x splňující $p \mid x^2 - x + 3$, právě pokud existuje celé číslo y splňující $p \mid y^2 - y + 25$.

Řešení. Podívejme se na obě dělitelnosti jako na kongruence v $\mathbb{Z}_p$. Potom $0 \equiv x^2 - x + 3$, což je po přenásobení 4 ekvivalentní $0 \equiv 4x^2 - 4x + 12 \equiv (2x-1)^2 + 11$ neboli $-11 \equiv (2x-1)^2$. Když už najdeme $a \in \mathbb{Z}_p$ tak, aby $a^2 \equiv -11$, tak z lichosti p dopočteme $x \equiv \frac{a+1}{2}$, takže x splňující zadanou dělitelnost existuje, právě když je -11 kvadratický zbytek. Obdobně můžeme upravit druhou dělitelnost, abychom zde znovu dostali čtverec. Tedy $0 \equiv 4y^2 - 4y + 100 \equiv (2y-1)^2 + 99$, takže existence takového y je ekvivalentní tomu, že -99 je kvadratickým zbytkem.

Použijme nyní Legendreovy symboly. Pokud $p = 11$, tak jsou -11 i -99 nuly v $\mathbb{Z}_p$, tedy oba kvadratické zbytky. Obdobně když $p = 3$, tak jsou $-11 \equiv 1$ i $-99 \equiv 0$ kvadratické zbytky. Konečně když p není 11 ani 3, jsou -11 i -99 nenulové v $\mathbb{Z}_p$, takže z multiplikativity Legendreova symbolu $\left(\frac{-99}{p}\right) = \left(\frac{-11}{p}\right)\left(\frac{3^2}{p}\right) = \left(\frac{-11}{p}\right)$, neboť 3^2 je čtverec. Tím je příklad vyřešen.

Příklad. Rozhodni, zda má rovnice $x^2 = y^5 + 7$ celočíselné řešení.

Řešení. Nemá. Podívejme se na ni modulo 11. Tím se z y^5 stane Legendreův symbol $\left(\frac{y}{11}\right)$, takže bude nabývat jen hodnot 0 (když $y \equiv 0$) nebo ± 1. Pravá strana tak bude moci nabývat jen hodnot 6, 7 a 8. Snadno však ověříme, že ani jedno z těchto čísel není kvadratický zbytek v $\mathbb{Z}_{11}$, takže $x^2 \equiv y^5 + 7 \pmod{11}$ nemá řešení.

Úloha 16. Nechť p je prvočíslo tvaru $4k - 1$. Nyní pokud modulo p platí $a \equiv x^2$, pak $x \equiv \pm a^k$.

Úloha 17. Nechť je p prvočíslo tvaru $2^k + 1$. Potom je $g \in \mathbb{Z}_p$ primitivním prvkem, právě když je kvadratickým nezbytkem.

[12] Adrien-Marie Legendre (1752–1833), francouzský matematik.

Závěr

Zde končí druhý díl seriálu. Víme již, co dělat s Pellovou rovnicí i jak ji nalézt skrytou v úlohách, nezalekneme se modulení, ať už pracujeme v jakémkoli okruhu, a vidíme dovnitř struktury konečných těles pomocí primitivního prvku. Děkujeme Ti, že ses dočetl(a) až sem. V třetím díle budeme k okruhům místo nějakého konkrétního čísla přidávat úplně obecnou proměnnou. Tím získáme okruhy polynomů, u nichž si opět prozkoumáme, jak je to s dělením se zbytkem či s jednoznačným rozkladem a jak souvisí vlastnosti okruhu polynomů s vlastnostmi původního okruhu.

Mezitím se těšíme na viděnou a přejeme mnoho zdaru při řešení úloh druhé seriálové série!

Návody ke cvičením

1. Kdy je $\frac{\sqrt{d_1}}{\sqrt{d_2}}$ racionální? Až budeš chtít ukázat, že jiné dvojice to být nemohou, zkus ve správnou chvíli umocnit.

2. Porovnej jejich prvky v $\mathbb{Q}(\sqrt{d})$.

3. Stačí prostě všechno rozepsat.

4. Kdyby něco nenulového mělo normu 0, pak by $\sqrt{d}$ bylo racionální.

5. Rozšiř pomocí $\overline{\beta}$.

7. Postupuj stejně jako pro $\mathbb{Z}[\sqrt{2}]$, jen lépe odhadni $|x^2 - 3y^2|$ pro $|x|, |y| \leq \frac{1}{2}$. Trojúhelníková nerovnost nestačí, protože si nemůžeme dovolit rovnost!

8. Prostě to ověř, stačí se dívat jenom na samotné $\frac{1+\sqrt{d}}{2}$.

9. Rozlož na součin v $\mathbb{Z}$.

11. Uprav na čtverce.

12. Uprav na Pellovu rovnici s $d = 8$.

13. Postupuj jako v řešeném příkladu. Pokud Ti nepůjde nalézt fundamentální řešení pro $d = 28$, začni u $d = 7$.

14. Vezmi kladnou Pellovu rovnici a její fundamentální řešení. Uprav ji tak, aby šlo využít nesoudělné činitele a specifickou podobu prvočíselného rozkladu.

15. Každá jednotka je $\pm$ mocninou té fundamentální. Rozliš, zda tato mocnina má sudý či lichý exponent.

16. Speciální případ předchozího cvičení.

17. Rozepiš podle definice kongruence. Využij toho, že celé číslo m dělí $c_1 + c_2\sqrt{d}$, právě když dělí obě složky c_1, c_2.

18. Jednotka dělí cokoliv.

19. Krácení je jenom speciální případ dělení.

20. Najdi dva nenulové prvky, jejichž součin je nulový.

21. Použij malou Fermatovu větu.

22. Použij malou Fermatovu větu v tělese $\mathbb{Z}[i]/(3)$. Neroznásobuj binomickou větou.

24. Ze součtu n jedniček odebírej po c jedničkách.

25. Slož dohromady předchozí tvrzení a malou Fermatovu větu.

26. Rozmysli si, že 89 musí mít v $\mathbb{Z}_p$ řád 16.

27. Každá mocnina a^k je i mocninou a.

28. Zapiš prvky tělesa pomocí primitivního prvku.

29. Posčítej geometrickou řadu.

30. Zapiš prvky tělesa pomocí primitivního prvku. Exponenty jsou modulo $n-1$.

31. Použij tvrzení o multiplikativních množinách.

32. Kvadratické zbytky jsou multiplikativní množina – sečti geometrickou řadu. Toto cvičení je jen speciální případ jednoho předchozího.

33. Eulerovo kritérium.

34. Rozepiš si z definice Legendreova symbolu.

Návody k úlohám

1. Opět vyděl $\frac{\alpha}{\beta} = x + y\sqrt{7}$ a snaž se od x a y odečítat celá čísla tak, aby absolutní hodnota normy spadla pod 1. BÚNO stačí vyřešit $x, y \in \langle 0, \frac{1}{2}\rangle$. Funguje $\gamma = 1$ nebo $\gamma = -1 + \sqrt{7}$. Bacha na to, kde nastává rovnost.

2. Pokud se na rovnici budeš snažit použít kvadratické zbytky, neuspěješ. Radši využij fundamentální řešení kladné Pellovy rovnice, které je v tomto případě $35 + 6\sqrt{34}$

3. Uprav zadání do tvaru Pellovy rovnice a rozmysli, které exponenty dávají zpět platná řešení. Na výrazu, který dostaneš, nemusí být na první pohled vidět, že jde upravit na čtverec, ale skutečně jde. Hodí se $2 \cdot (2 + \sqrt{3}) = (1 + \sqrt{3})^2$.

4. Zvol si nějaké d, které není čtverec, a vztah $b^2 + 1 = d \cdot a(a+1)$ uprav vhodnou substucí na rovnici Pellova typu $N(x + y\sqrt{d}) =$ konstanta. Pokud najdeš jedno řešení, už jich máš nekonečně mnoho – stačí přenásobovat řešeními Pellovy rovnice. Dobře funguje třeba $d = 5$.

5. Využij $\mathbb{Z}[\sqrt{q^2 d}] \subset \mathbb{Z}[\sqrt{d}]$.

6. Využij čtyřku v $7 + 4\sqrt{3} = (2 + \sqrt{3})^2$. Je potřeba důsledně najít všechny činitele dvojky, které se nabízí. Pokud znáš kvadratické zbytky modulo 8, pak může být snazší prostě použít je.

7. Pokud $a^2 = 2n+1$, $b^2 = 3n+1$, pak substituce $a = x+3y$, $b = x+2y$ povede k Pellově rovnici s $d = 6$.

8. Nejprve si rozmysli, že toto platí tehdy, když jsou pro $\alpha = a + b\sqrt{d}$ složky a, b nesoudělné.

9. Použij malou Fermatovu větu.

10. Je to jenom $x = 1$. Hodí se $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

11. 101 je prvočíslo. Pro $y > 0$ získej kongruenci $x^5 \equiv -2 \pmod{101}$, umocni na 20 a použij malou Fermatovu větu.

12. Když je n prvočíslo, použij Wilsonovu větu. Pro složené n si rozmysli $x \equiv 0 \pmod{n}$.

13. Jde to. 101 je prvočíslo.

14. Podívej se na předpis posloupnosti jako na zobrazení v $\mathbb{Z}_p$. Všimni si, že 0 se posílá na 1.

15. Pro spor předpokládej, že rovnice nemá řešení, a najdi příliš mnoho kvadratických nezbytků.

16. Využij, že a je kvadratický zbytek, a připomeň si, co pro něj díky Legendreovu symbolu platí.

17. Když prvek není primitivní, jaký může mít řád? Porovnej s Eulerovým kritériem.

Řesení cvičení

1. Jsou to přesně ty dvojice, kde $\frac{d_1}{d_2} = q^2$ pro nějaké racionální q. Potom určitě $\sqrt{d_1} = q\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_2})$ a obdobně $\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1})$, což značí $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$. Naopak pokud $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$, pak $\sqrt{d_1} = a + b\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_2})$. Pokud $b = 0$, pak je $\sqrt{d_1}$ racionální, což je spor. Pro $b \neq 0$ předchozí vztah upravíme na

$$\begin{aligned} a &= \sqrt{d_1} - b\sqrt{d_2}, \\ a^2 &= d_1 - 2b\sqrt{d_1 d_2} + b^2 d_2, \\ \frac{a^2 - d_2 b^2 - d_1}{2b} &= \sqrt{d_1 d_2}, \end{aligned}$$

takže $\sqrt{d_1 d_2}$ je racionální. Pak je i $q = \sqrt{\frac{d_1}{d_2}} = \frac{\sqrt{d_1 d_2}}{d_2}$ racionální, neboli $\frac{d_1}{d_2} = q^2$.

2. Každý prvek průniku $\mathbb{Q} \cap \mathbb{Z}[\sqrt{d}]$ zároveň vyjádříme jako $q \in \mathbb{Q}$ a jako $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Když to formulujeme jako rovnost $q + 0 \cdot \sqrt{d} = a + b\sqrt{d}$ dvou prvků $\mathbb{Q}(\sqrt{d})$, pak podle předchozího tvrzení $q = a$ a $0 = b$. První rovnost ale znamená, že q je celé číslo, takže každý racionální prvek $\mathbb{Z}[\sqrt{d}]$ je celé číslo.

3. Ověříme takřka stejně jako pro komplexní čísla v prvním díle. Nechť $\alpha = a + b\sqrt{d}$, $\beta = x + y\sqrt{d}$. V případě sčítání je $\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}$ zřejmé. V případě násobení prostě dosadíme a obdržíme

$$\begin{aligned} \alpha\beta &= (a + b\sqrt{d})(x + y\sqrt{d}) = (ax + byd) + (ay + bx)\sqrt{d}, \\ \overline{\alpha} \cdot \overline{\beta} &= (a - b\sqrt{d})(x - y\sqrt{d}) = (ax + byd) - (ay + bx)\sqrt{d}, \end{aligned}$$

takže $\overline{(\alpha\beta)} = \overline{\alpha} \cdot \overline{\beta}$. Z toho následně $N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = N(\alpha) \cdot N(\beta)$.

4. Nechť $\alpha = a + b\sqrt{d}$. Rovnost $N(\alpha) = 0$ upravíme na $a^2 = b^2 \cdot d$. Kdyby nyní $b \neq 0$, mohli bychom vydělit a dostali bychom $\sqrt{d} = \frac{a}{b}$, což je spor. Určitě tedy $b = 0$, takže i $a = 0$ a dohromady $\alpha = 0$.

5. Nechť $\alpha = a + b\sqrt{d}$, $\beta = x + y\sqrt{d}$. Pak

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(a + b\sqrt{d})(x - y\sqrt{d})}{x^2 - dy^2} = \frac{ax - byd}{x^2 - dy^2} + \frac{bx - ay}{x^2 - dy^2}\sqrt{d}.$$

Jelikož $\beta \neq 0$, tak určitě $N(\beta) \neq 0$ čili nedělíme nulou a vše je v pořádku.

6. Pokud je α racionální, pak je zřejmě samo sobě sdružené. Naopak pokud $\alpha = \overline{\alpha}$, pak je jeho racionální složka rovna $\frac{\alpha + \overline{\alpha}}{2} = \alpha$, takže α je racionální.

7. Stejně jako v příkladu $\mathbb{Z}[\sqrt{2}]$ vydělíme a zaokrouhlíme. Potom pro $a = x - x_0$, $b = y - y_0$ chceme dokázat $|a^2 - 3b^2| < 1$, přičemž máme zaručeno $|a|, |b| \leq \frac{1}{2}$. Kdybychom jenom použili trojúhelníkovou nerovnost, dostaneme $|a^2 - 3b^2| \leq \frac{1}{4} + 3 \cdot \frac{1}{4} = 1$, což nám ale nestačí, protože potřebujeme ostrou nerovnost. Využijeme toho, že a^2 i b^2 jsou nezáporná čísla, takže díky omezení

absolutní hodnoty určitě obě leží v intervalu $\langle 0, \frac{1}{4}\rangle$. Výraz $a^2 - 3b^2$ (bez absolutních hodnot) tak bude nejmenší možný, když a^2 bude nejmenší možné a b^2 největší možné, takže $0 - 3 \cdot \frac{1}{4} = -\frac{3}{4}$. Naopak největší hodnoty výrazu dosáhneme při $a^2 = \frac{1}{4}$, $b^2 = 0$, tedy $\frac{1}{4} - 3 \cdot 0 = \frac{1}{4}$. Dohromady $a^2 - 3b^2 \in \langle -\frac{3}{4}, \frac{1}{4}\rangle$, z čehož určitě $|a^2 - 3b^2| \leq \frac{3}{4} < 1$.

8. Uzavřenost na sčítání je jasná. Označme $\alpha = \frac{1+\sqrt{d}}{2}$, potom $\alpha^2 = \frac{1+2\sqrt{d}+d}{4} = \alpha + \frac{d-1}{4} \in \mathbb{Z}[\alpha]$, jelikož $\frac{d-1}{4} \in \mathbb{Z}$. Když pak roznásobíme $(a_1 + b_1\alpha) \cdot (a_2 + b_2\alpha)$, tak už bude každý člen výsledného součtu prvkem $\mathbb{Z}[\alpha]$.

9. Když $d = a^2$, pak rozložíme na součin $x^2 - a^2y^2 = (x - ay)(x + ay) = 1$. Nyní je součin dvou celých čísel roven 1, takže jsou buď obě 1, nebo obě -1. Z první možnosti dostaneme $2x = (x-ay)+(x+ay) = 1+1 = 2$, takže $x = 1$. Obdobně z druhé možnosti $x = -1$ a v obou případech pak nutně $a^2y^2 = 0$, takže $y = 0$. Takže kdyby byl d čtverec, Pellova rovnice by měla jen triviální řešení.

10. (i) $a + \sqrt{d}$, (ii) $(a^2 - 1) + a\sqrt{d}$, $(a^2 + 1) + a\sqrt{d}$,

(iii) Díky $a^2 - 1^2 \cdot (a^2 + 1) = -1$ je $a + \sqrt{d}$ jednotka s normou -1. Její čtverec pak bude jednotka s normou 1, tedy máme řešení $(2a^2 + 1) + 2a\sqrt{d}$.

11. Rovnici upravíme na $(x-2y)^2-3y^2 = 1$, takže je to Pellova rovnice v $\mathbb{Z}[\sqrt{3}]$. Fundamentálním řešením je $\omega = 2 + \sqrt{3}$. Z její mocniny ω^n už dopočteme $y = \frac{\omega^n - \omega^{-n}}{2\sqrt{3}}$ a $x = \frac{\omega^{n+1} - \omega^{-n-1}}{2\sqrt{3}}$. Další řešení bychom dostali obrácením znamének u x i y zároveň.

12. Nechť $\frac{n(n+1)}{2} = y^2$. To upravíme na $4n^2 + 4n = 8y^2$ a následně $(2n + 1)^2 - 8y^2 = 1$. Pojmenujeme-li $x = 2n + 1$, pak pro každé řešení $x + y\sqrt{8}$ musí x být liché, takže nám z něj $n = \frac{x-1}{2}$ dá platné řešení. Stačí tedy vzít třetí nejmenší řešení $x + y\sqrt{8}$, to jest třetí mocninu fundamentálního řešení. Tím je $3 + \sqrt{8}$, takže $x + y\sqrt{8} = (3 + \sqrt{8})^3 = 99 + 35\sqrt{8}$, z čehož $n = 49$.

13. Stačí postupovat podobně jako v řešeném příkladu. Najít fundamentální řešení pro $d = 28$ může být trochu problém, můžeme se však podívat na $d = 7$. Tam je fundamentálním řešením $\omega_0 = 8 + 3\sqrt{7}$. Jeho iracionální složka je lichá, takže to vzhledem $\sqrt{28} = 2\sqrt{7}$ není prvek $\mathbb{Z}[\sqrt{28}]$. Zato $\omega_0^2 = 127 + 48\sqrt{7} = 127 + 24\sqrt{28} = \omega$ už je, takže je to fundamentální řešení pro $d = 28$. Potom už postupujeme úplně stejně jako v řešeném příkladu.

14. Nechť je $x + y\sqrt{p}$ fundamentální řešení Pellovy rovnice $x^2 - py^2 = 1$. Upravme ji do tvaru $x^2 - 1 = py^2$. Podle toho, zda je x sudé či liché, může na levé straně modulo čtyři být buďto -1, či 0. Na pravé straně pak podle parity y může díky $p \equiv 1 \pmod 4$ být buďto 0, nebo 1. Aby tedy mohla nastat rovnost, určitě je x liché a y sudé.

V upravené Pellově rovnici tak můžeme vydělit čtyřmi, čímž dostaneme $\frac{x+1}{2} \cdot \frac{x-1}{2} = p\left(\frac{y}{2}\right)^2$. Na levé straně jsou nesoudělná celá čísla $\frac{x+1}{2}$, $\frac{x-1}{2}$ (jejich rozdíl je 1), zatímco na pravé straně máme číslo, v jehož prvočíselném rozkladu mají všechna prvočísla vyjma p sudý exponent. Jelikož činitelé nalevo jsou nesoudělní, musí jeden z nich být a^2 a druhý pb^2 pro nějaká $a, b \in \mathbb{N}$ (nemůže se zde vyskytnout nula, jelikož pak by i y bylo nulové). Kdyby platilo $\frac{x+1}{2} = a^2$ a $\frac{x-1}{2} = pb^2$, pak dostaneme $a^2 - pb^2 = 1$. To by bylo opět řešení Pellovy rovnice, jenže by muselo být menší než $x + y\sqrt{p}$, které je fundamentální. To by byl spor, takže musí být $\frac{x+1}{2} = pb^2$ a $\frac{x-1}{2} = a^2$, což znamená $a^2 - pb^2 = -1$. Záporná Pellova rovnice tedy má řešení, jak jsme chtěli.

15. Víme, jak vyrobit všechna řešení z toho fundamentálního, takže $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$ pro nějaké $n \in \mathbb{Z}$. Když obrátíme znaménko $\pm$ nebo znaménko exponentu n, jenom tím obrátíme znaménko jedné nebo obou složek x, y, což na dělitelnost $x_0y_0 \mid xy$ nebude mít vliv. BÚNO tedy předpokládejme $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ pro přirozené n.

Nyní když je n liché, tak podle předchozího tvrzení jak x_0, tak y_0 dělí y, z čehož určitě $x_0y_0 \mid xy$. Když je naopak n sudé, tak stále y_0 dělí y, ale x_0 tentokrát dělí x, což však stále implikuje $x_0y_0 \mid xy$. Dohromady tak $x_0y_0 \mid xy$ platí vždy.

Pro fundamentální jednotku a obecnou jednotku bychom postupovali stejně: důležité je jenom to, že máme (třeba s pomocí nějakého BÚNO) $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ pro $n \in \mathbb{N}$.

16. Stačí nalézt fundamentální řešení $73 + 12\sqrt{37}$, načež díky $876 = 73 \cdot 12$ stačí vzít předchozí obecné cvičení. Jak na toto řešení přijít? Třeba díky $37 = 6^2 + 1$ máme jednotku $6 + \sqrt{37}$ s normou -1, která už musí být fundamentální, jelikož žádná jiná jednotka nemůže mít menší iracionální část. Fundamentální řešení Pellovy rovnice je pak čtvercem fundamentální jednotky.

17. Když znění cvičení rozepíšeme podle definice kongruence, pak chceme říci, že $m \mid a - b$ neimplikuje $m \mid \overline{a} - \overline{b} = \overline{(a-b)}$. Naproti tomu $\overline{m} \mid \overline{(a-b)}$ by z $m \mid a - b$ plynulo, ale tím, že provedeme sdružení jen na pravé straně dělitelnosti, nemusíme dostat pravdivé tvrzení: například v $\mathbb{Z}[i]$ máme $2 + i \mid 2 + i$, ale $2 + i \nmid 2 - i$.

Nyní nechť je však $m \in \mathbb{Z}$ a budiž $a - b = c_1 + c_2\sqrt{d}$ pro nějaká $c_1, c_2 \in \mathbb{Z}$. Potom je $m \mid c_1 + c_2\sqrt{d}$ ekvivalentní $m \mid c_1$ a zároveň $m \mid c_2$. Ale $m \mid \overline{(a-b)} = c_1 - c_2\sqrt{d}$ je totéž, jelikož $m \mid c_2$ a $m \mid (-c_2)$ je ekvivalentní.

18. Jednotka u dělí 1 a 1 dělí každý prvek R, takže i u dělí všechno. Potom ale pro každé $a \in R$ máme $u \mid a - 0$, takže $a \equiv 0 \pmod{u}$. Každý prvek je tak kongruentní nule, takže máme jedinou zbytkovou třídu, v níž leží každý prvek okruhu.

19. Nechť je T těleso a mějme $a, b, c \in T$, kde c je nenulové. Víme, že c je jednotka, takže existuje $\frac{1}{c}$. Potom pokud $ac = bc$, pak přenásobíme dostaneme $a = a \cdot 1 = a \cdot \left(c \cdot \frac{1}{c}\right) = bc \cdot \frac{1}{c} = b \cdot 1 = b$, čímž je hotovo.

20. Z definice toho, že n je složené, existuje jeho rozklad $n = ab$, kde a i b jsou větší než 1 a menší než n. Z toho už nutně plyne, že $a, b \not\equiv 0 \pmod{n}$ a zároveň $pq \equiv n \equiv 0 \pmod{n}$.

21. Základ mocniny můžeme zmenšit modulo 11 pomocí $29 \equiv 7 \pmod{11}$. Z malé Fermatovy věty platí $7^{10} = 1$, takže exponent můžeme snížit modulo 10. Dostaneme tak $29^{25} \equiv 7^5$, následně zakončíme třeba trikem $7^5 \equiv (-4)^5 \equiv -4^5 \equiv -\left(2^2\right)^5 \equiv -2^{10} \equiv -1 \pmod{11}$, kde v poslední kongruence opět používáme malou Fermatovu větu.

22. Těleso $\mathbb{Z}[i]/(3)$ má 9 prvků, takže exponent snížíme modulo 8. Dostaneme $(11 + 7i)^{18} \equiv (2 + i)^2 \equiv 3 + 4i \equiv i \pmod{3}$.

23. Třeba racionální čísla. V $\mathbb{Q}$ umíme nenulovými prvky dělit, takže je to těleso, avšak suma libovolně mnoha jedniček nikdy není 0. Stejně tak nadtělesa racionálních čísel jako $\mathbb{R}$, $\mathbb{C}$ nebo kterékoliv $\mathbb{Q}(\sqrt{d})$ mají charakteristiku 0.

24. Nechť $x \times 1$ značí součet x jedniček. Pro spor nechť $c \nmid n$, potom dělení se zbytkem dává $n = cq + r$, kde $0 < r < c$. Máme $n \times 1 = 0$ a zároveň $c \times 1 = 0$. Z $n \times 1$ tak můžeme odečítat $c \times 1$ a vždy dostaneme nulu, takže $r \times 1 = (n - qc) \times 1 = 0$. Přitom ale $0 < r < c$, takže to je spor s definicí charakteristiky.

25. Z malé Fermatovy věty platí $a^{n-1} = 1$, takže musí $n - 1$ být násobek řádu a.

26. Nechť je r řád 89 v $\mathbb{Z}_p$. Vztah $p \mid 89^8 + 1$ upravme na $89^8 \equiv -1 \pmod{p}$, což značí $r \nmid 8$. Umocněním na druhou pak $89^{16} \equiv 1 \pmod{p}$, z čehož $r \mid 16$. Z toho je r dělitel 16, který není dělitelem 8, takže už $r = 16$. Těleso $\mathbb{Z}_p$ má p prvků, takže vzhledem k $r \mid p - 1$ hledáme prvočísla se zbytkem 1 modulo 16. Prvním takovým je 17, jenže spočítáme, že

$$89^8 + 1 \equiv 4^8 + 1 \equiv 16^4 + 1 \equiv (-1)^4 + 1 \equiv 2 \pmod{17}.$$

Další čísla se zbytkem 1 modulo 16 jsou 33, 49, 65 a 81, což nejsou prvočísla. Další se tedy nabízí teprve $p = 97$, což vyjde díky

$$89^8 + 1 \equiv (-8)^8 + 1 \equiv 64^4 + 1 \equiv (-33)^4 + 1 \equiv 1089^2 + 1 \equiv 22^2 + 1 \equiv 484 + 1 \equiv 0 \pmod{97}.$$

27. Nechť je s řád a^k. Víme, že $\left(a^k\right)^{\frac{r}{k}} = a^r = 1$, takže $s \leq \frac{r}{k}$. Zároveň kdyby $s < \frac{r}{k}$, znamenalo by to $a^{ks} = \left(a^k\right)^s = 1$ a zároveň $ks < r$, což by byl spor s tím, že r je řád a.

28. Nechť je g primitivní prvek. Wilsonova věta říká, že součin všech nenulových prvků konečného tělesa je roven -1. Tedy součin nenulových prvků tělesa je

$$a_1 a_2 \cdots a_{n-1} = g^0 \cdot g^1 \cdots g^{n-2} = g^{\frac{(n-1)(n-2)}{2}} = \left(g^{\frac{n-1}{2}}\right)^{n-2} = (-1)^{n-2} = -1.$$

Rozeberme postupně všechny rovnosti. V první prostě zapíšeme prvky tělesa pomocí primitivního prvku. Druhá rovnost je jen součet exponentů a použití vzorce $1 + \cdots + (n-2) = \frac{(n-1)(n-2)}{2}$. Poté nahlédněme $g^{\frac{n-1}{2}} = -1$. Z malé Fermatovy věty máme $\left(g^{\frac{n-1}{2}}\right)^2 = g^{n-1} = 1$, takže $\left(g^{\frac{n-1}{2}} - 1\right)\left(g^{\frac{n-1}{2}} + 1\right) = 0$. Z definice primitivního prvku nemůže nastat $g^{\frac{n-1}{2}} = 1$, takže $g^{\frac{n-1}{2}} = -1$. Poslední rovnost plyne lichostí $n-2$.

29. Podle tvrzení máme $S = \left\{g^m, g^{2m}, \ldots, g^{\frac{n-1}{m}\cdot m}\right\}$. Navíc jelikož $|S| > 1$, pak určitě $m < n-1$, takže $g^m \neq 1$. Součet prvků S je potom jenom

$$g^m + g^{2m} + \cdots + g^{(\frac{n-1}{m}-1)m} + g^{\frac{n-1}{m}\cdot m} = g^m \cdot \frac{g^{(n-1)m} - 1}{g^m - 1} = g^m \cdot \frac{1^m - 1}{g^m - 1} = 0.$$

30. Nechť je g primitivní prvek. Nehledě na k platí $0^k = 0$ a pro $x \neq 0$ je x^k nenulové, takže nulu nadále nemusíme řešit. Prostost f je ekvivalentní tomu, že se každé $a \in T$ objeví jako obraz nějakého x. Pokud je k nesoudělné s $n-1$, tak máme Bézoutovy koeficienty u, v splňující $uk + v(n-1) = 1$. Pro $a = g^r$ potom $f(g^{ru}) = g^{ruk} = g^{r(uk+v(n-1))} = g^r = a$, takže už je f skutečně prosté.

Pokud naopak mají k a $n-1$ nějakého společného dělitele $d > 1$, pak už každé $f(x)$ bude ležet v multiplikativní množině $\{g^d, g^{2d}, g^{3d}, \ldots\}$, která neobsahuje všechny prvky T. Zobrazení f tak nemůže být prosté.

31. Je-li g primitivní prvek, jsou kvadratickými zbytky právě $g^2, g^4, g^6, \ldots$, takže jich je $\frac{n-1}{2}$. Poté ještě přičteme 1 za nulu, která je vždy kvadratickým zbytkem.

32. Nula součet nezmění, takže se stačí dívat na nenulové kvadratické zbytky. Ty tvoří multiplikativní množinu o $\frac{n-1}{2} > 1$ prvcích, takže už se podle dřívějšího cvičení o součtu multiplikativní množiny musí kvadratické zbytky posčítat na 0.

33. Platí $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$. Dále bude -1 kvadratickým zbytkem, právě když uvedený Legendreův symbol vyjde jedna, což nastane právě tehdy, když bude $\frac{p-1}{2}$ sudé, tedy když $4 \mid p-1$.

34. $\left(\frac{ab}{T}\right) = (ab)^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} = \left(\frac{a}{T}\right)\left(\frac{b}{T}\right)$.