Teorie čísel

Vítězslav Kala

19. května 2022

Obsah

1 Počet prvočísel **6**
- 1.1 Čebyševův horní odhad . . . 6
- 1.2 Valuace . . . 8
- 1.3 Dolní odhad a Bertrandův postulát . . . 9

2 Řetězové zlomky **11**
- 2.1 Pellova rovnice . . . 11
- 2.2 Aproximace reálných čísel . . . 12
- 2.3 Existence řešení Pellovy rovnice . . . 13
- 2.4 Řetězové zlomky a polynomy . . . 14
- 2.5 Sblížené zlomky . . . 16
- 2.6 Dobré aproximace . . . 18
- 2.7 Periodické řetězové zlomky . . . 20
- 2.8 Zpět k Pellově rovnici . . . 21

3 Odmocniny z jedné **22**
- 3.1 Gaussovská celá čísla . . . 22
- 3.2 Cyklotomické polynomy . . . 25
- 3.3 Prvočísla $kn + 1$ . . . 27
- 3.4 Ireducibilita cyklotomických polynomů . . . 28

4 Charaktery a kvadratická reciprocita **30**
- 4.1 Kvadratické zbytky . . . 30
- 4.2 Charaktery . . . 32
- 4.3 Gaussovy součty . . . 35
- 4.4 Zákon reciprocity . . . 37
- 4.5 Jacobiho symbol . . . 39
- 4.6 Prvočísla tvaru $a^2 + 2b^2$ . . . 41

5 Testování prvočíselnosti **42**
- 5.1 Opakování a Fermatův test . . . 42
- 5.2 Pravděpodobnostní testy obecně . . . 42
- 5.3 Solovay–Strassenův test prvočíselnosti . . . 43
- 5.4 Primitivní prvky . . . 44
- 5.5 Valuace a mocniny . . . 45
- 5.6 Multiplikativní grupa modulo p^e . . . 45
- 5.7 Rabin-Millerův test . . . 49
- 5.8 Míjení involucí . . . 50

5.9 Počet Rabin-Millerových lhářů 52

6 Příklady **54**
6.1 Základy 54
6.2 Eulerova a Malá Fermatova věta 54
6.3 Čínská zbytková věta 55
6.4 Cyklické grupy 55
6.5 Fareyho zlomky 57
6.6 Řetězové zlomky 57
6.7 Pellova rovnice 59
6.8 Dobré aproximace 60
6.9 Gaussovská celá čísla 61
6.10 Diofantické rovnice 62
6.11 Kvadratické zbytky a Legendreovy symboly 63
6.12 Charaktery a Gaussovy součty 64
6.13 Jacobiho symboly 65
6.14 Prvočísla speciálních tvarů 66
6.15 Rozklad na součin cyklických grup 66
6.16 Primitivní prvky 67
6.17 Valuace 67
6.18 Řešení kongruencí pomocí primitivních prvků 68
6.19 Carmichaelova čísla 69
6.20 Involuce 69
6.21 Míjení prvků 69
6.22 Rabin-Millerovi svědci a lháři 70
6.23 RSA 70
6.24 Cyklotomické polynomy 71
6.25 Dirichletova věta o prvočíslech 72
6.26 Jiné 72

Úvod

Toto je pracovní verze skript k přednášce Teorie čísel.

Jejich cílem je být poměrně minimalistickým shrnutím probrané látky, jež blízce kopíruje průběh přednášek a nezahrnuje téměř žádné rozšiřující informace.
Materiál v těchto skriptech a jeho prezentace není vůbec původní: jeho většina je založená na skriptech Aleše Drápala [Dr]. 2. kapitola primárně vychází ze skript Zuzany Masákové a Edity Pelantové [MP]; sekce 3.3 pak z textu Martina Klazara.

Za sepsání první verze skript děkuju Martinu Žuravovi; za upozorňování na chyby a překlepy děkuju studentům, kteří přednášku se mnou absolvovali (zejména v koronavirovém letním semestru 2019/20, ale pak taky 2021/22). Příklady do závěrečné 6. kapitoly připravila Žaneta Semanišinová (s využitím příkladů od dřívějších cvičících, zejména Martina Čecha a Martina Žurava). Řadu dalších úprav a vylepšení navrhl David Stanovský podle svého kurzu v roce 2020/21. I přes naši snahu v současné verzi nepochybně obsahují řadu chyb, překlepů a nejasností, takže uvítám jakékoli komentáře a návrhy na zlepšení.

[Dr] Aleš Drápal, *Teorie čísel a RSA*
http://www.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf

[Kl] Martin Klazar, *Analytic and Combinatorial Number Theory*, summer term 2017
https://kam.mff.cuni.cz/~klazar/anktc17.pdf

[MP] Zuzana Masáková, Edita Pelantová, *Teorie čísel*, skripta pro FJFI ČVUT

Poslední změny
2022 duben. Oprava sekce 2.6.
2022. Poměrně výrazná restrukturalizace a doplnění podle návrhů Davida Stanovského.

Motivace

O co jde v teorii čísel? Hlavními tématy, kterými se budeme zabývat, jsou celá čísla, dělitelnost, prvočísla a tak dále. Uvidíme například, že funkce $\pi(x)$, která označuje počet prvočísel menších nebo rovných nějakému reálnému číslu x, je rovna zhruba $\frac{x}{\log x}$. My časem (v kapitole 4) dokážeme, že $c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$ pro nějaká $c_1, c_2 > 0$.

Podíváme se také na následující tvrzení, které však nebudeme dokazovat v úplné obecnosti: V každé aritmetické posloupnosti $ax + b$ (pro nesoudělná a, b) existuje nekonečně mnoho prvočísel.

Základním nástrojem pro nás budou kongruence a počítání v $\mathbb{Z}_n$. Jak vypadají invertibilní prvky v $\mathbb{Z}_n$?
Eulerova věta říká, že $a^{\varphi(n)} \equiv 1 \pmod{n}$. Výpočet $\varphi(n)$ závisí na prvočíselném rozkladu n, proto nás bude také zajímat testování, jestli je n prvočíslo. Jelikož je faktorizace výpočetně náročná, je možné využít úvahy z teorie čísel například v kryptografii (konkrétně např. RSA).

Také se budeme věnovat diofantickým rovnicím. Velká Fermatova věta říká, že $x^n + y^n = z^n$ nemá řešení pro $x, y, z \in \mathbb{N}, n \geq 3$. To pochopitelně nedokážeme, ale vyřešíme například $x^2 + y^2 = z^2$ nebo $x^2 + 1 = y^3$ pomocí počítaní v Gaussových celých číslech $\mathbb{Z}[i]$ (více oproti Algebře).
Budeme dále řešit kvadratické kongruence $x^2 \equiv a \pmod{p}$, což vede k zákonu kvadratické reciprocity, který dokážeme pomocí počítaní v $\mathbb{Z}\left[e^{\frac{2\pi i}{n}}\right]$.

Jak dobře jde dané číslo aproximovat pomocí racionálních čísel? Například π je přibližně rovno $\frac{355}{113} = 3,1415929\ldots$ Ukážeme, že řetězové zlomky dávají takovéto dobré aproximace.

Mimochodem, číslo $6789012\ldots901\ldots0\ldots0\ldots1$ je prvočíslo, které si můžeme pamatovat jako 600001 (nebo i jako 641).

1. Počet prvočísel

Existence prvočísel se týkají dvě klíčové těžké věty:

Věta 1.1 (Prvočíselná věta)**.** *Buď* $\pi(x) =$ *počet prvočísel* $\leq x$ *(pro* $x \in \mathbb{R}^+$*). Pak*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1,$$

kde log *je přirozený logaritmus.*

Zhruba řečeno, pravděpodobnost jevu, že náhodné celé číslo n je prvočíslo, je přibližně

$$\frac{1}{\log n} = \frac{1}{\log 10 \cdot \log_{10} n} \sim \frac{1}{2,3 \cdot \text{ počet cifer } n}.$$

Věta 1.2 (Dirichletova věta o aritmetické posloupnosti)**.** *Mějme* $a \in \mathbb{N}, b \in \mathbb{Z}, (a, b) = 1$*. Pak existuje nekonečně mnoho prvočísel tvaru* $ax + b, x \in \mathbb{N}$*.*

Oba důkazy z 19. století využívají komplexní analýzu. Dá se ale poměrně elementárně dokázat:

- Existují $c_1, c_2 > 0$ taková, že pro všechna dostatečně velká x platí
$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}.$$
- Bertrandův postulát: pro každé přirozené číslo $n \geq 2$ existuje prvočíslo p takové, že $n < p < 2n$.
- Pro každé přirozené číslo a existuje nekonečně mnoho prvočísel p tvaru $ax + 1$.

První dvě tvrzení si dokážeme v této úvodní kapitole.
Třetí tvrzení, což je speciální případ Dirichletovy věty, si později dokážeme pomocí cyklotomických polynomů.

1.1 Čebyševův horní odhad

Začněme nejjednodušším z odhadů počtu prvočísel, a sice že

$$\pi(n) < c \cdot \frac{n}{\log n} \text{ pro nějaké } c > 1.$$

Definice. *Théta funkce* je definovaná jako

$$\vartheta(x) = \sum_{p \leq x} \log p \text{ pro } x \in \mathbb{R}^+,$$

kde sčítáme přes prvočísla $p \leq x$.

Odhadneme $\vartheta(n)$ pomocí kombinačních čísel a z toho pak odhadneme $\pi(n)$.

Lemma 1.3. *Pro $k \in \mathbb{Z}, k \geq 0$, máme*

$$\frac{2^{2k}}{2k+1} \leq \binom{2k}{k} \quad \textit{a také} \quad \binom{2k+1}{k} \leq 2^{2k}.$$

Důkaz. $\binom{2k}{k}$ je největší z kombinačních čísel $\binom{2k}{i}$ pro $0 \leq i \leq 2k$ (cvičení). Tedy

$$2^{2k} = (1+1)^{2k} = \binom{2k}{0} + \binom{2k}{1} + \cdots + \binom{2k}{2k} \leq (2k+1) \cdot \binom{2k}{k}.$$

Pro druhou nerovnost máme

$$2 \cdot \binom{2k+1}{k} = \binom{2k+1}{k} + \binom{2k+1}{k+1} \leq 2^{2k+1}. \qquad \square$$

Tvrzení 1.4 (Čebyšev)**.** *Pro $n \in \mathbb{N}$ máme*

$$\vartheta(n) < n \cdot \log 4, \ \textit{neboli} \ \prod_{p \leq n} p < 4^n.$$

Důkaz. Dokážeme druhou nerovnost, tu první pak dostaneme zlogaritmováním.
Pro $n = 1, 2$ je tvrzení zřejmé. Ať teď $n > 2$, budeme dokazovat indukcí.
a) Platí-li tvrzení pro $n = 2k+1$ liché, pak platí i pro $n+1 = 2k+2$, protože $2k+2$ není prvočíslo, takže se levá strana nezvětší.
b) Ať teď $n = 2k$ a nerovnost platí pro n a všechna menší čísla; chceme nerovnost pro $2k+1$.
Rozdělme $\prod_{p \leq 2k+1} p$ na součin přes $p \leq k+1$ (pro který použijeme IP) a přes $k+2 \leq p \leq 2k+1$.
Máme $\binom{2k+1}{k} = \frac{(2k+1)!}{k!(k+1)!}$ a tedy každé p, které splňuje $k+2 \leq p \leq 2k+1$, dělí čitatel v první mocnině a nedělí jmenovatel. Tedy $p \mid \binom{2k+1}{k}$ a také

$$\left(\prod_{k+2 \leq p \leq 2k+1} p \right) \mid \binom{2k+1}{k} \overset{1.3}{\leq} 2^{2k} = 4^k.$$

Máme tedy

$$\prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \prod_{k+2 \leq p \leq 2k+1} p \overset{\text{IP}}{<} 4^{k+1} \cdot 4^k = 4^{2k+1}. \qquad \square$$

Věta 1.5. *Existuje konstanta $c > 1$ taková, že $\pi(n) < c \cdot \frac{n}{\log n}$ (pro $n \geq 2$).*

Důkaz. Máme

$$n \log 4 \overset{1.4}{>} \vartheta(n) = \sum_{p \leq n} \log p \geq \sum_{\sqrt{n} < p \leq n} \log p \geq \sum_{\sqrt{n} < p \leq n} \log \sqrt{n} \geq \frac{1}{2} \left(\pi(n) - \sqrt{n} \right) \cdot \log n,$$

kde poslední nerovnost platí proto, že počet sčítanců na její levé straně je menší nebo rovna počtu prvočísel $\leq n$ mínus počtu všech čísel $\leq \sqrt{n}$.
Tedy

$$\pi(n) \cdot \log n \leq 2n \log 4 + \sqrt{n} \cdot \log n < (2 \log 4 + c')n.$$

Zde jsme ve druhé nerovnosti využili toho, že máme $\sqrt{n} \cdot \log n = o(n)$, čili existuje konstanta c' taková, že $\sqrt{n} \cdot \log n < c'n$. $\square$

Konkrétně např. platí $\sqrt{n} \cdot \log n < \frac{2}{e} \cdot n$ pro $n \geq 2$. Tedy

$$\pi(n) \cdot \log n < n \cdot \left(2 \log 4 + \frac{2}{e}\right)$$

a můžeme vzít $c = 2 \log 4 + \frac{2}{e} \approx 3,54$.

1.2 Valuace

Jedním ze základních nástrojů v teorii čísel jsou valuace.

Definice. Buď p prvočíslo a $n \in \mathbb{Z}$. Pak $v_p(n)$ značí největší $j \geq 0$ takové, že $p^j \mid n$; jde o *p-valuaci čísla n*. Zároveň definujeme $v_p(0) := \infty$.

Například tedy máme, že $n = \prod p^{v_p(n)}$ pro každé $n \in \mathbb{N}$. Jedná se sice formálně o nekonečný součin, ale pokud $p \nmid n$, pak $v_p(n) = 0$ a příslušný součinitel $p^{v_p(n)} = p^0 = 1$ můžeme ignorovat.

Cvičení. Základní vlastnosti valuací jsou (pro prvočíslo p a $m, n \in \mathbb{Z}$)

- multiplikativita: $v_p(mn) = v_p(m) + v_p(n)$,
- trojúhelníková nerovnost: $v_p(m+n) \geq \min(v_p(m), v_p(n))$.

Pro zbytek kapitoly označme $\binom{2n}{n} = \prod p^{v_p}$ prvočíselný rozklad, čili $v_p = v_p\binom{2n}{n}$.
Zřejmě máme $v_p = 0$ pro všechna $p > 2n$.

Lemma 1.6. *$p^{v_p} \leq 2n$ pro všechna prvočísla p.*

Důkaz. Máme

$$v_p = v_p\binom{2n}{n} = v_p\left(\frac{(2n)!}{(n!)^2}\right) = v_p((2n)!) - 2v_p(n!).$$

Dále si všimněme, že

$$v_p(k!) = \sum_{j \geq 1} \left\lfloor \frac{k}{p^j} \right\rfloor .$$

Je to proto, že přesně $\left\lfloor \frac{k}{p} \right\rfloor$ z čísel $1, 2, \ldots, k$ je dělitelných p, a tedy každé z nich přispěje 1 do exponentu p v prvočíselném rozkladu. Dále $\left\lfloor \frac{k}{p^2} \right\rfloor$ z těchto čísel je dokonce dělitelných p^2 (a proto přispějí další 1 do exponentu p), atd. s postupným uvažováním čísel dělitelných $p^3, p^4, \ldots$
Dosazením do vzorečku pro v_p dostáváme

$$v_p = v_p((2n)!) - 2v_p(n!) = \sum_{j \geq 1} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right).$$

Zde si uvědomme, že stačí uvažovat indexy $j \leq \log_p(2n)$, protože pro větší j máme $p^j > 2n$, a tedy $\left\lfloor \frac{2n}{p^j} \right\rfloor = 0 = \left\lfloor \frac{n}{p^j} \right\rfloor$.

Cvičení. Pro každé n, m platí $\left\lfloor \frac{2n}{m} \right\rfloor - 2 \left\lfloor \frac{n}{m} \right\rfloor = 0, 1$.

Pomocí tohoto snadného cvičení už dokončíme důkaz: v_p je součtem nejvýše $\log_p(2n)$ sčítanců, z nichž každý je roven 0 nebo 1. Tedy $v_p \leq \log_p(2n)$, jak jsme chtěli. □

1.3 Dolní odhad a Bertrandův postulát

Věta 1.7. *Existují $c, n_0 > 0$ taková, že pro všechna $n \geq n_0$ platí $\pi(n) > c\frac{n}{\log n}$.*

Důkaz. Vzhledem k tomu, že $\pi(2n-1) = \pi(2n)$, stačí větu dokázat pro sudá čísla. Pomocí lemmat 1.3 a 1.6 odhadneme

$$\frac{2^{2n}}{2n+1} \overset{1.3}{\leq} \binom{2n}{n} = \prod p^{v_p} \leq (2n)^{\pi(2n)},$$

kde poslední nerovnost platí proto, že pokud $p \mid \binom{2n}{n}$, pak zřejmě $p \leq 2n$, a tedy počet prvočísel p v prvočíselném rozkladu je nejvýše $\pi(2n)$. Pro každé z nich pak použijeme lemma 1.6.
Čili $2^{2n} \leq (2n+1) \cdot (2n)^{\pi(2n)}$ a po zlogaritmování

$$2n \log 2 \leq \log(2n+1) + \pi(2n) \log(2n).$$

Z této nerovnosti dostaneme odhad

$$\pi(2n) \geq \frac{2n \log 2}{\log(2n)} - \frac{\log(2n+1)}{\log(2n)} > c\frac{2n}{\log(2n)}$$

pro vhodné c, neboť $\log(2n+1) = o(2n)$. □

Poznámka: z poslední nerovnosti je vidět, že lze zvolit $c = \log 2 - \varepsilon$ pro libovolné $\varepsilon > 0$ (čím menší, tím větší bude n_0).

Věta 1.8 (Bertrandův postulát)**.** *Pro každé přirozené číslo $n \geq 2$ existuje prvočíslo p takové, že $n < p < 2n$.*

Důkaz. Pro spor uvažujme n, pro které neexistuje prvočíslo p splňující $n < p < 2n$.
Opět označme $\binom{2n}{n} = \prod p^{v_p}$ prvočíselný rozklad. Z dřívějšího pozorování víme, že $v_p = 0$ pro všechna $p > 2n$. Z předpokladu plyne, mezi n a $2n$ žádné prvočíslo není.
Dále si všimněme, že $v_p = 0$ pro všechna $2n/3 < p \leq n$, protože taková prvočísla se vyskytují právě jednou v čitateli i jmenovateli zlomku $\binom{2n}{n} = \frac{(2n)\cdots(n+1)}{n\cdots 1}$. A nakonec si všimněme, že $v_p \leq 1$ pro všechna $p > \sqrt{2n}$, protože $p^{v_p} \leq 2n$ podle lemmatu 1.6.
Použitím lemmatu 1.3 a těchto pozorování dostaneme odhad

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} p^{v_p} \cdot \prod_{\sqrt{2n} < p \leq 2n/3} p < (2n)^{\sqrt{2n}} \cdot 4^{2n/3},$$

přičemž pro odhad prvního součinu jsme opět použili $p^{v_p} \leq 2n$ a pro odhad druhého součinu jsme použili Čebyševovu nerovnost.
Pro $n \geq 18$ lze pokračovat v odhadech

$$2^{2n} \leq (2n+1) \cdot (2n)^{\sqrt{2n}} \cdot 4^{2n/3} < (2n)^{\sqrt{2n}+2} \cdot 4^{2n/3} \leq (2n)^{\frac{4}{3}\cdot\sqrt{2n}} \cdot 4^{2n/3}.$$

Druhá a třetí nerovnost plyne z následujících úvah: $k+1 < k^2$ pro všechna $k \geq 2$, a dále $l + 2 \leq \frac{4}{3}l$ pro všechna $l \geq 6$.
Po zlogaritmování dostaneme

$$2n \log 2 < \frac{4}{3}\left(\sqrt{2n}\log(2n) + n \log 2\right),$$

lineární člen převedeme vlevo, vydělíme $\sqrt{n}$ a dostaneme nerovnost

$$\sqrt{n}\log 2 < 2\sqrt{2}\log(2n).$$

Obě strany jsou rostoucí posloupnosti, ovšem levá strana roste mnohem rychleji a již pro $n = 2^{10}$ nerovnost neplatí.
Závěr tedy je, že pokud pro číslo n neplatí Bertrandův postulát, pak $n < 2^{10}$. Ovšem posloupnost prvočísel $3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259$ prokazuje, že pro malá n Bertrandův postulát platí, spor. □

2. Řetězové zlomky

2.1 Pellova rovnice

Spousta motivace pro teorii čísel pochází ze snahy řešit diofantické rovnice (např. velká Fermatova věta).

Pellova rovnice: rovnice $x^2 - my^2 = 1$, kde m je dané přirozené číslo, které není čtverec. Vždy má řešení $(\pm 1, 0)$, které se nazývá triviální.
Všimněme si, že na znaménkách čísel x, y nezáleží, často tedy budeme búno předpokládat, že jsou obě čísla kladná.

Kdyby $m = d^2$, pak $1 = x^2 - d^2y^2 = (x - dy)(x + dy)$, takže $x \pm dy = \pm 1$. Odtud $2x = \pm 2$, takže $x = \pm 1$. Pak $y = 0$, což dává pouze triviální řešení.

Někdy se Pellova rovnice definuje i lehce obecněji, například s -1 nebo ± 4 napravo.

Brahmagupta (cca. 600 n.l.): „Za matematika se může považovat ten, kdo umí vyřešit $x^2 - 29y^2 = 1$.“ (řešení je (9801, 1820))
Fermat vyzval svého kamaráda k řešení pro $m = 61$: (1766319049,226153980).

K řešení se využívá podobná myšlenka jako výše: rozklad $(x - \sqrt{m}y)(x + \sqrt{m}y) = 1$ v okruhu $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$.

Pozorování. Pokud jsou $(x_1, y_1), (x_2, y_2)$ řešení, pak také (x_3, y_3) je řešení, kde

$$x_3 + y_3\sqrt{m} = (x_1 + y_1\sqrt{m})(x_2 + y_2\sqrt{m}).$$

Důkaz. Máme $x_3 - y_3\sqrt{m} = (x_1 - y_1\sqrt{m})(x_2 - y_2\sqrt{m})$, a tedy

$$x_3^2 - y_3^2 m = (x_1 + y_1\sqrt{m})(x_2 + y_2\sqrt{m})(x_1 - y_1\sqrt{m})(x_2 - y_2\sqrt{m}) = 1. \quad \square$$

Všechna řešení tedy tvoří grupu: neutrální prvek je $(1, 0)$, inverzní prvek k (x, y) je $(x, -y)$.

Tvrzení 2.1. *Buď $m \in \mathbb{N}$ takové, že m není čtverec. Předpokládejme, že Pellova rovnice $x^2 - my^2 = 1$ má alespoň jedno netriviální řešení. Pak existuje řešení (a_0, b_0) takové, že*

$$\left\{(a, b) \mid a + b\sqrt{m} = \pm(a_0 + b_0\sqrt{m})^n, n \in \mathbb{Z}\right\}$$

jsou právě všechna řešení.

Rovnou poznamenejme, že netriviální řešení existuje vždy, jak si dokážeme ve větě 2.3.
Často budeme říkat, že $a + b\sqrt{m}$ je řešení Pellovy rovnice, když dvojice (a, b) je řešením.

Důkaz. 1. Buď (a', b') netriviální řešení, búno $a' > 0, b' > 0$. Položme

$$a_0 + b_0\sqrt{m} := \min\{a + b\sqrt{m} \text{ řešení Pellovy rovnice} \mid a, b > 0, a + b\sqrt{m}\}.$$

Označme tuto množinu M. Proč minimum z množiny M existuje?
Množina M je neprázdná, neboť obsahuje prvek $a' + b'\sqrt{m}$.
Všimněme si, že pokud $a_1 + b_1\sqrt{m}, a_2 + b_2\sqrt{m} \in M$, pak

$$a_1 < a_2 \Leftrightarrow a_1^2 < a_2^2 \Leftrightarrow 1 + mb_1^2 < 1 + mb_2^2 \Leftrightarrow b_1^2 < b_2^2 \Leftrightarrow b_1 < b_2.$$

Buď $a_0 + b_0\sqrt{m} \in M$ takový, že a_0 je nejmenší možné (to existuje, neboť $a_0 \in \mathbb{N}$). Pak je také b_0 nejmenší možné. Odtud $a_0 + b_0\sqrt{m}$ je také nejmenší prvek M, a proto minimum existuje.

2. Pozorování dává, že $\pm(a_0 + b_0\sqrt{m})^n$ je řešení pro každé $n \in \mathbb{Z}$: pro $n > 0$ je to v pořádku. Dále máme $a_0 - b_0\sqrt{m} = (a_0 + b_0\sqrt{m})^{-1}$, čili pro pro $n = -k < 0$ je $(a_0 + b_0\sqrt{m})^{-k} = (a_0 - b_0\sqrt{m})^k$.

3. Vezměme nyní řešení $c + d\sqrt{m}$, búno $c, d > 0$.
Máme $a_0 + b_0\sqrt{m} \geq 1 + \sqrt{m} > 1$, a tedy posloupnost $(a_0 + b_0\sqrt{m})^n$ má limitu ∞ pro $n \to \infty$.
Proto existuje $n \in \mathbb{N}_0$ takové, že $(a_0 + b_0\sqrt{m})^n \leq c + d\sqrt{m} < (a_0 + b_0\sqrt{m})^{n+1}$. Pak $(a_0 + b_0\sqrt{m})^{-n}(c + d\sqrt{m}) = (a_0 - b_0\sqrt{m})^n(c + d\sqrt{m})$ je také řešení a máme

$$1 \leq x + y\sqrt{m} = (a_0 + b_0\sqrt{m})^{-n}(c + d\sqrt{m}) < a_0 + b_0\sqrt{m}.$$

Cvičení. Buď $x + y\sqrt{m}$ řešení. Pak $x + y\sqrt{m} > 1 \Leftrightarrow x > 0$ a $y > 0$.
Tedy kdyby $x + y\sqrt{m} > 1$, pak $x + y\sqrt{m} \in M$, což je spor s minimalitou $a_0 + b_0\sqrt{m}$.
Takže $x + y\sqrt{m} = 1$, což dává $c + d\sqrt{m} = (a_0 + b_0\sqrt{m})^n$. □

(a_0, b_0), resp. $a_0 + b_0\sqrt{m}$ se nazývá *minimální řešení Pellovy rovnice*. Např.

$$3 + 2\sqrt{2}, 2 + \sqrt{3}, \ldots, 649 + 180\sqrt{13}, \ldots, 1766319049 + 226153980\sqrt{61}, \ldots$$

Víc si toho k řetězovým zlomkům můžete přečíst v článku Martina Kuděje pro Pokroky matematiky, fyziky a astronomie:
http://www.karlin.mff.cuni.cz/~kala/1920%20tc/kudej.pdf

2.2 Aproximace reálných čísel

Potřebujeme dokázat předpoklad z tvrzení 2.1 o existenci nějakého netriviálního řešení.
Myšlenka: $x^2 - my^2 = 1 \Rightarrow x^2 = my^2 + 1 \Rightarrow \frac{x^2}{y^2} = m + \frac{1}{y^2}$, proto přibližně platí $\frac{x}{y} \approx \sqrt{m}$.
Hledáme tedy zlomky, které dobře aproximují $\sqrt{m}$.

Buď $\alpha \in \mathbb{R}$ a uvažujme zlomky $\cdots < -\frac{1}{q} < 0 < \frac{1}{q} < \frac{2}{q} < \frac{3}{q} < \ldots$. Pak α leží v nějakém z intervalů $\left[\frac{i}{q}, \frac{i+1}{q}\right)$, takže existuje p splňující $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q}$. Můžeme ale aproximovat mnohem lépe!

Věta 2.2 (Dirichlet)**.** *Buď $\alpha \in \mathbb{R}$ iracionální.*
a) Pro každé $Q \in \mathbb{N}, Q \geq 2$, existují čísla $p, q \in \mathbb{Z}$ taková, že $1 \leq q < Q$ a $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq}$.
b) Existuje nekonečně mnoho zlomků $\frac{p}{q}$ (v základním tvaru) takových, že $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Poznámka. Pro $\alpha \in \mathbb{Q}$ první část platí s $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq}$, druhá část neplatí – cvičení.
Před důkazem připomeňme, že $\{\beta\} := \beta - \lfloor\beta\rfloor$ značí necelou část čísla β.

Důkaz. a) Rozdělme interval $[0,1]$ na Q podintervalů s koncovými body

$$0 = \frac{0}{Q}, \frac{1}{Q}, \frac{2}{Q}, \ldots, \frac{Q-1}{Q}, 1 = \frac{Q}{Q}.$$

Vezměme reálná čísla $0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\} \in [0,1]$.
Každé z těchto čísel je tvaru $a\alpha - b$ pro nějaká $a, b \in \mathbb{Z}, 0 \leq a < Q$, protože $\{j\alpha\} = j\alpha - \lfloor j\alpha\rfloor$.

Máme $Q+1$ čísel v Q intervalech $\left[\frac{i}{Q}, \frac{i+1}{Q}\right]$, takže aspoň dvě čísla leží v jednom intervalu. Zřejmě to není dvojice $0, 1$, tedy búno ať to je $a\alpha - b, c\alpha - d$, kde $0 \leq a < c < Q$. Pak máme $|(c-a)\alpha - (d-b)| = |(c\alpha - d) - (a\alpha - b)| \leq \frac{1}{Q}$.
Tedy pro $p := d - b, q := c - a$ máme

$$\left|\alpha - \frac{p}{q}\right| = \frac{1}{q} \cdot |(c-a)\alpha - (d-b)| \leq \frac{1}{Qq}.$$

Z faktu, že α je iracionální, na závěr plyne, že rovnost nenastane.

b) Pokud je $\frac{p}{q}$ podle části a) (pro nějaké Q), pak

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq} < \frac{1}{q^2}. \qquad (*)$$

Zároveň každý zlomek $\frac{p}{q}$ splňuje nerovnost $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq}$ jen pro *konečně mnoho* hodnot Q, protože levá strana této nerovnosti je reálné číslo > 0 a její pravá strana jde k 0 pro $Q \to \infty$.
Q ale můžeme v části a) volit libovolně velké, takže musí existovat nekonečně mnoho různých zlomků $\frac{p}{q}$ splňujících (*). □

2.3 Existence řešení Pellovy rovnice

Věta 2.3. *Buď $m \in \mathbb{N}$ takové, že $m \neq d^2$ pro všechna $d \in \mathbb{N}$. Pak má Pellova rovnice $x^2 - my^2 = 1$ netriviální řešení v $\mathbb{Z}$.*

Důkaz. Podle Dirichletovy věty 2.2b) existuje nekonečně mnoho zlomků $\frac{p}{q}$ takových, že $|p - q\sqrt{m}| < \frac{1}{q}$ a p, q jsou nesoudělná. Pak

$$\left|p^2 - mq^2\right| = |p - q\sqrt{m}| \cdot |p - q\sqrt{m} + 2q\sqrt{m}| < \frac{1}{q} \cdot \left(\frac{1}{q} + 2q\sqrt{m}\right) \leq 1 + 2\sqrt{m}.$$

Proto v intervalu $(-1 - 2\sqrt{m}, 1 + 2\sqrt{m})$ existuje celé číslo k takové, že $p^2 - mq^2 = k$ platí pro nekonečně mnoho dvojic (p, q). Zároveň je $\sqrt{m}$ iracionální, takže $k \neq 0$.

Navíc můžeme rozdělit (p, q) podle jejich hodnot mod k: Máme k^2 možných dvojic $(p \pmod k, q \pmod k)$, a tedy aspoň jedna z nich nastane pro nekonečně mnoho zlomků $\frac{p}{q}$.

Existují tedy $(p_1, q_1) \neq (p_2, q_2)$ takové, že

$$p_1^2 - mq_1^2 = k, \quad p_2^2 - mq_2^2 = k, \quad p_1 \equiv p_2 \pmod{k}, \quad q_1 \equiv q_2 \pmod{k}.$$

Pak

$$\begin{aligned} k^2 = (p_1^2 - mq_1^2)(p_2^2 - mq_2^2) &= \left[(p_1 + q_1\sqrt{m})(p_2 - q_2\sqrt{m})\right]\left[(p_1 - q_1\sqrt{m})(p_2 + q_2\sqrt{m})\right] \\ &= (A + B\sqrt{m})(A - B\sqrt{m}) = A^2 - B^2 m, \end{aligned}$$

kde $A := p_1p_2 - q_1q_2m, B := q_1p_2 - p_1q_2$.
Navíc $A \equiv p_1^2 - q_1^2 m = k \equiv 0 \pmod{k}, B \equiv q_1p_1 - p_1q_1 = 0 \pmod{k}$.

Buď $X := \frac{A}{k}, Y := \frac{B}{k}$. Máme $Y \neq 0$ (cvičení: proč?) a platí $k^2 = A^2 - B^2m = k^2 \cdot (X^2 - Y^2m)$, a tedy $X^2 - Y^2m = 1$. Tedy (X, Y) je hledané netriviální řešení. □

Poznámka. Věta neříká, jak minimální řešení najít. K tomu použijeme řetězové zlomky – viz větu 2.15 níže.

2.4 Řetězové zlomky a polynomy

Ze cvičení víme, že řetězový zlomek je $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}} =: [a_0, a_1, a_2, \dots]$. Teď toto formalizujeme a dokážeme si řadu poměrně silných vlastností.

Definice. Buď $\xi \in \mathbb{R}$. Definujme posloupnost celých čísel a_i takto:

$$\xi_0 := \xi, a_i := \lfloor \xi_i \rfloor, \xi_{i+1} := \frac{1}{\xi_i - a_i} \text{ pokud } \xi_i \neq a_i.$$

Vznikne konečná posloupnost $a_0, a_1, \dots, a_k$ nebo nekonečná posloupnost $a_0, a_1, \dots$, jež se nazývá řetězový zlomek čísla $\xi \in \mathbb{R}$ a značí $\xi = [a_0, a_1, \dots, a_k]$ nebo $\xi = [a_0, a_1, \dots]$.

Poznámka. Zatím jde o čistě formální zápis, obzvlášť v případě nekonečného řetězového zlomku.

Máme $a_0 \in \mathbb{Z}$ a $a_i \in \mathbb{N}$ pro $i \geq 1$.

Tvrzení 2.4. *Číslo ξ je racionální, právě když ξ má konečný řetězový zlomek $[a_0, \dots, a_k]$.*

Důkaz. „⇒“ Ať $\xi = \frac{p}{q}$. Uvažujme Eukleidův algoritmus:

$$\begin{aligned} p &= a_0 q + r_1 \\ q &= a_1 r_1 + r_2 \\ r_1 &= a_2 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= a_k r_k + 0. \end{aligned}$$

Pak $\frac{p}{q} = \xi = [a_0, \dots, a_k]$ a $\xi_i = \frac{r_{i-1}}{r_i}$.

„⇐“ Máme-li konečný řetězový zlomek $[a_0, \dots, a_k]$, pak $\xi = a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{a_k}}}$ (což se dokáže například indukcí). □

Máme $a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1}, a_0 + \frac{1}{a_1+\frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2+1} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1}$. Pojďme se na čitatele a jmenovatele dívat jako na polynomy v proměnných a_i.

Definice. *n-tý řetězový (kontinuální) polynom v proměnných $x_1, \dots, x_n$* je definován rekurentně: $K_{-1} := 0, K_0 := 1$,

$$K_n(x_1, \dots, x_n) := x_n \cdot K_{n-1}(x_1, \dots, x_{n-1}) + K_{n-2}(x_1, \dots, x_{n-2}) \text{ pro } n \geq 1.$$

Za chvíli si dokážeme, že řetězové polynomy opravdu dávají čitatele i jmenovatele konečného řetězového zlomku:

Tvrzení 2.5. *Pro $a_0 \in \mathbb{R}, a_i \in \mathbb{R}^+$ máme*

$$[a_0, a_1, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_n}}} = \frac{K_{n+1}(a_0, \dots, a_n)}{K_n(a_1, \dots, a_n)}.$$

Pro řetězové polynomy platí řada užitečných, byť trochu technických, identit. Klíčová je část a), z níž potom zbytek poměrně snadno vyplývá. Zejména e) si není potřeba pamatovat.

Tvrzení 2.6. *Pokud není níže uvedeno jinak, buď $n \geq 1$. Pak:*
a)

$$\begin{pmatrix} K_n(x_1, \dots, x_n) & K_{n-1}(x_1, \dots, x_{n-1}) \\ K_{n-1}(x_2, \dots, x_n) & K_{n-2}(x_2, \dots, x_{n-1}) \end{pmatrix} = \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix} = M_{x_1} \cdots M_{x_n},$$

kde $M_a = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$.
b) $K_n(x_1, \dots, x_n) = \begin{pmatrix} 1 & 0 \end{pmatrix} M_{x_1} \cdots M_{x_n} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
c) $K_n(x_1, \dots, x_n) = K_n(x_n, \dots, x_1)$, *což platí pro* $n \geq -1$.
d)

$$K_n(x_1, \dots, x_n)K_{n-2}(x_2, \dots, x_{n-1}) - K_{n-1}(x_1, \dots, x_{n-1})K_{n-1}(x_2, \dots, x_n) = (-1)^n.$$

e) Pro $n \geq 2, 1 \leq l \leq n-1$ *platí*

$$K_n(x_1, \dots, x_n) = K_l(x_1, \dots, x_l)K_{n-l}(x_{l+1}, \dots, x_n) + K_{l-1}(x_1, \dots, x_{l-1})K_{n-l-1}(x_{l+2}, \dots, x_n).$$

Důkaz. a) Indukcí:
$n = 1 : K_1(x_1) = x_1K_0 + K_{-1} = x_1$. Tedy levá strana se rovná $\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix}$, což odpovídá pravé straně.
$n + 1 \geq 2$:

$$\begin{pmatrix} K_n(x_1, \dots, x_n) & K_{n-1}(x_1, \dots, x_{n-1}) \\ K_{n-1}(x_2, \dots, x_n) & K_{n-2}(x_2, \dots, x_{n-1}) \end{pmatrix} \begin{pmatrix} x_{n+1} & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} x_{n+1}K_n(x_1, \dots, x_n) + K_{n-1}(x_1, \dots, x_{n-1}) & K_n(x_1, \dots, x_n) \\ x_{n+1}K_{n-1}(x_2, \dots, x_n) + K_{n-2}(x_2, \dots, x_{n-1}) & K_{n-1}(x_2, \dots, x_n) \end{pmatrix}$$

$$= \begin{pmatrix} K_{n+1}(x_1,\dots,x_{n+1}) & K_n(x_1,\dots,x_n) \\ K_n(x_2,\dots,x_{n+1}) & K_{n-1}(x_2,\dots,x_n) \end{pmatrix}.$$

b) Zřejmé z a).
c) Transponováním matice 1×1 jako první rovnost dostaneme

$$(K_n(x_1,\dots,x_n)) = (K_n(x_1,\dots,x_n))^T = \left[\begin{pmatrix} 1 & 0 \end{pmatrix} M_{x_1} \cdots M_{x_n} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^T$$

$$= \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T M_{x_n}^T \cdots M_{x_1}^T \begin{pmatrix} 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \end{pmatrix} M_{x_n} \cdots M_{x_1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (K_n(x_n,\dots,x_1)).$$

d) Vezmeme determinant obou stran rovnosti a).
e) Platí $M_{x_l} M_{x_{l+1}} = M_{x_l} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} M_{x_{l+1}} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix}$. Tohle dosadíme dovnitř pravé strany rovnosti b). □

Důkaz tvrzení 2.5. Indukcí:

$$\mathrm{LS} = a_0 + \frac{1}{\frac{K_n(a_1,\dots,a_n)}{K_{n-1}(a_2,\dots,a_n)}} = \frac{a_0 K_n(a_1,\dots,a_n) + K_{n-1}(a_2,\dots,a_n)}{K_n(a_1,\dots,a_n)}.$$

Potřebujeme tedy dokázat, že $K_{n+1}(a_0,\dots,a_n) = a_0 K_n(a_1,\dots,a_n) + K_{n-1}(a_2,\dots,a_n)$. K tomu použijeme tvrzení 2.6c):

$$a_0 K_n(a_1,\dots,a_n) + K_{n-1}(a_2,\dots,a_n) \overset{2.6c)}{=} a_0 K_n(a_n,\dots,a_1) + K_{n-1}(a_n,\dots,a_2)$$
$$\overset{\text{def}}{=} K_{n+1}(a_n,\dots,a_0) \overset{2.6c)}{=} K_{n+1}(a_0,\dots,a_n). \quad \square$$

2.5 Sblížené zlomky

Chceme aproximovat $\xi = [a_0, a_1, \dots]$ pomocí $[a_0,\dots,a_n]$: ty aproximují dobře (ve smyslu věty 2.2b)), čehož využijeme k formalizaci nekonečného zlomku $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$. Pro zjednodušení budeme předpokládat, že $\xi > 0$ (to ovlivní jenom a_0).

Definice. Buď $\xi > 0$ a $[a_0, a_1, \dots, a_k]$ (respektive $[a_0, a_1, \dots]$) jeho konečný (respektive nekonečný) řetězový zlomek. Pro $n \geq -1$ buď

$$p_{-1} := 1, q_{-1} := 0, p_n := K_{n+1}(a_0,\dots,a_n), q_n := K_n(a_1,\dots,a_n).$$

Zlomek $\frac{p_n}{q_n}$ (pro $n \geq 0$) nazýváme *n-tý sblížený zlomek* (nebo také konvergent) čísla ξ.

Platí následující rekurence pro p_n, q_n, kde $n \geq 0$:
$p_{-1} = 1, p_0 = a_0, p_{n+1} = a_{n+1} p_n + p_{n-1}$;
$q_{-1} = 0, q_0 = 1, q_{n+1} = a_{n+1} q_n + q_{n-1}$.

Posloupnosti $\{p_n\}_{n\geq 0}$ a $\{q_n\}_{n\geq 1}$ jsou ostře rostoucí, protože $a_0 \geq 0, a_i > 0$.

Samozřejmě pokud $\xi \in \mathbb{Q}$, máme vše definované jen do p_k, q_k a $\frac{p_k}{q_k} = \xi$. V tomto případě je třeba příslušně omezit n v následujících tvrzeních. Jelikož se jedná o snadné úpravy, nebudeme je zde uvádět explicitně.
Všimněme si také, že definice p_n, q_n dává smysl i pro posloupnost $a_0, a_1, \dots$, která nemusí být nutně řetězovým zlomkem nějakého čísla.

Tvrzení 2.7. $p_{n-1}q_n - p_nq_{n-1} = (-1)^n$ *pro* $n \geq 0$.

Důkaz. Plyne ihned z tvrzení 2.6d): Místo n vezmeme $n+1$ a dosadíme $x_1 = a_0, x_2 = a_1, \ldots, x_{n+1} = a_n$. Dostaneme

$$\begin{aligned} &p_{n-1}q_n - p_nq_{n-1} \\ &\quad = K_n(a_0, \ldots, a_{n-1})K_n(a_1, \ldots, a_n) - K_{n+1}(a_0, \ldots, a_n)K_{n-1}(a_1, \ldots, a_{n-1}) = (-1)^n. \end{aligned}$$

□

Tvrzení 2.8. *Buď* $\xi > 0$ *a* ξ_i *jako v definici řetězového zlomku, tedy*

$$\xi_0 = \xi, a_i = \lfloor \xi_i \rfloor, \xi_{i+1} = \frac{1}{\xi_i - a_i} \text{ pro } \xi_i \neq a_i.$$

Pak

$$\xi = \frac{\xi_{n+1}p_n + p_{n-1}}{\xi_{n+1}q_n + q_{n-1}}, \text{ kde } \frac{p_n}{q_n} \text{ jsou sblížené zlomky ke } \xi.$$

Důkaz. Máme

$$\begin{aligned} \xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\xi_{n+1}}}}} &\overset{2.5}{=} \frac{K_{n+2}(a_0, \ldots, a_n, \xi_{n+1})}{K_{n+1}(a_1, \ldots, a_n, \xi_{n+1})} \\ &\overset{\text{definice } K_i}{=} \frac{\xi_{n+1}K_{n+1}(a_0, \ldots, a_n) + K_n(a_0, \ldots, a_{n-1})}{\xi_{n+1}K_n(a_1, \ldots, a_n) + K_{n-1}(a_1, \ldots, a_{n-1})} = \frac{\xi_{n+1}p_n + p_{n-1}}{\xi_{n+1}q_n + q_{n-1}}. \end{aligned}$$

□

Věta 2.9. *Buď* $\xi > 0$. *Pak:*
a)

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \xi,$$

a tedy posloupnost sblížených zlomků konverguje ke ξ.
b)

$$\frac{p_{2n}}{q_{2n}} < \xi < \frac{p_{2n+1}}{q_{2n+1}} \text{ pro } n \geq 0.$$

c)

$$\frac{1}{q_nq_{n+2}} < \left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_nq_{n+1}} \left(< \frac{1}{q_n^2} \right).$$

d)

$$\cdots < |p_{n+1} - q_{n+1}\xi| < \frac{1}{q_{n+2}} < |p_n - q_n\xi| < \frac{1}{q_{n+1}} < \cdots$$

(tedy vzdálenosti $q_n\xi$ *od nejbližšího celého čísla, typicky* p_n*, se zmenšují).*

Část a) nám dává způsob, jak precizovat definici nekonečného řetězového zlomku jako reálného čísla, a sice jako

$$[a_0, a_1, \ldots] := \lim_{n\to\infty} [a_0, a_1, \ldots, a_n].$$

Teď také vidíme, že každá posloupnost $a_0 \in \mathbb{Z}$, $a_1, a_2, \cdots \in \mathbb{N}$ je řetězovým zlomkem nějakého reálného čísla, a sice čísla $\xi = [a_0, a_1, \ldots] := \lim_{n\to\infty}[a_0, a_1, \ldots, a_n]$ (*cvičení:*

napřed dokažte existenci limity pomocí Cauchyovskosti a pak to, že $a_0 = \lfloor \lim \dots \rfloor$, *a podobně pro další koeficienty* a_i). Toto vůbec nebylo jasné z původní definice v sekci 2.4! Řetězové zlomky nám tedy dávají bijekci mezi reálnými čísly ξ a posloupnostmi a_i.

V tvrzení je potřeba si dát pozor, kde zastavit pro racionální ξ.

Důkaz. Pro důkaz předpokládejme, že ξ je iracionální. Máme

$$\xi - \frac{p_n}{q_n} \overset{2.8}{=} \frac{\xi_{n+1}p_n + p_{n-1}}{\xi_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(\xi_{n+1}q_n + q_{n-1})} \overset{2.7}{=} \frac{(-1)^n}{q_n(\xi_{n+1}q_n + q_{n-1})}.$$

Číslo na pravé straně je kladné, resp. záporné podle parity n, a tedy platí b).

Protože $a_{n+1} = \lfloor \xi_{n+1} \rfloor < \xi_{n+1}$, máme

$$\left| \xi - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\xi_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_nq_{n+1}},$$

kde jsme v poslední rovnosti využili rekurenci pro q_{n+1}. To dokazuje a) (protože pravá strana jde k 0) a horní odhad v c).
Použitím $1 + a_{n+1} > \xi_{n+1}$ podobně dostaneme dolní odhad v c):

$$\left| \xi - \frac{p_n}{q_n} \right| > \frac{1}{q_n((1 + a_{n+1})q_n + q_{n-1})} = \frac{1}{q_n(q_{n+1} + q_n)} \geq \frac{1}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{1}{q_nq_{n+2}}.$$

Konečně d) plyne ihned z c) vynásobením q_n. □

Z části c) vidíme, že sblížené zlomky nám dávají aproximace s malou chybou ve smyslu Dirichletovy věty 2.2b) (což v podstatě dává její další důkaz).

2.6 Dobré aproximace

Definice. Buď $\xi \in \mathbb{R}$. Zlomek $\frac{r}{s}$, kde $(r, s) = 1$ a $s > 0$, je *dobrá aproximace* čísla ξ, pokud

$$\text{pro každé } \frac{p}{q} \in \mathbb{Q}, \text{ kde } 1 \leq q < s, \text{ platí } |r - s\xi| < |p - q\xi|$$

a

$$|r - s\xi| \leq |p - s\xi| \text{ platí pro všechna } p \in \mathbb{Z}.$$

V definici jde tedy o to, že $\frac{r}{s}$ má nejmenší „relativní chybu“

$$\frac{\left|\frac{r}{s} - \xi\right|}{\frac{1}{s}} = |r - s\xi|.$$

Postupně teď dokážeme, že sblížené zlomky pro $\xi > 0$ dávají všechny jeho dobré aproximace:

Věta 2.10. *Buď* $\xi > 0$, $\{\xi\} \neq 0, \frac{1}{2}$. *Pak jeho sblížené zlomky*

$$\frac{p_n}{q_n}, \text{ kde } \begin{cases} n \geq 0, & \text{pokud } 0 < \{\xi\} < \frac{1}{2}, \\ n \geq 1, & \text{pokud } \frac{1}{2} < \{\xi\} < 1, \end{cases}$$

dávají právě všechny dobré aproximace čísla ξ.

Případy, kdy $\{\xi\} = 0, \frac{1}{2}$, stejně jako dobré aproximace se jmenovatelem 1, bude třeba vyřešit samostatně, to je ale jednoduché přímo z definice dobré aproximace.

Cvičení. a) Určete všechny dobré aproximace čísla ξ, pokud $\{\xi\} = 0, \frac{1}{2}$.
b) Určete všechny dobré aproximace tvaru $\frac{p}{1}$ čísla ξ.

Lemma 2.11. *Buď $\xi > 0$. Ať $q > 1$, $\frac{p}{q}$ **není** sblížený zlomek ξ a buď $n \geq 1$ index takový, že $q_{n-1} < q \leq q_n$. Pak*

$$|q\xi - p| \geq |q_n\xi - p_n| + |q_{n-1}\xi - p_{n-1}|.$$

(Je-li $\xi \in \mathbb{Q}$ a q dostatečně velké, pak takové n neexistuje.)

Důkaz. Myšlenka: vyjádříme p, q pomocí p_i, q_i a odhadneme.
Uvažujme proto soustavu rovnic

$$xp_{n-1} + yp_n = p, xq_{n-1} + yq_n = q.$$

Tvrzení 2.7 dává, že determinant soustavy je $(-1)^n$, proto má soustava řešení v $\mathbb{Z}$. Díky Cramérovu pravidlu je tímto řešením

$$x = (-1)^n(pq_n - qp_n), y = (-1)^{n-1}(pq_{n-1} - qp_{n-1}).$$

Protože $\frac{p}{q} \neq \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$, máme $x \neq 0 \neq y$. Navíc x, y mají různé znaménka díky 2. rovnici, protože platí $1 \leq q_{n-1} < q \leq q_n$ a protože $x, y \in \mathbb{Z}$.
Už můžeme odhadnout:

$$\begin{aligned}|p - q\xi| =& |xp_{n-1} + yp_n - (xq_{n-1} + yq_n)\xi| = |x(p_{n-1} - q_{n-1}\xi) + y(p_n - q_n\xi)| \\ =& |x| \cdot |p_{n-1} - q_{n-1}\xi| + |y| \cdot |p_n - q_n\xi| \geq |p_{n-1} - q_{n-1}\xi| + |p_n - q_n\xi|,\end{aligned}$$

kde třetí rovnost platí, protože výrazy v závorkách mají opačná znaménka podle věty 2.9b), takže po vynásobení x, y mají znaménka stejná. □

Důkaz věty 2.10. Dobré aproximace se jmenovatelem 1 je potřeba vyřešit samostatně (což bude odpovídat mezím $n \geq 0$, resp. $n \geq 1$ ze znění věty).
Dále budeme uvažovat jen zlomky se jmenovatelem ≥ 2, pro které můžeme používat lemma 2.11 (protože jmenovatele můžeme umístit mezi dva sousední členy posloupnosti $q_0 = 1 < q_1 < q_2 < \dots$).

Buď $\frac{p_n}{q_n}$ sblížený zlomek. Proč jde o dobrou aproximaci?
Mějme $\frac{p}{q}$ se jmenovatelem $q_m < q \leq q_{m+1} \leq q_n$. Rozlišíme dva případy:
a) $\frac{p}{q}$ není sblížený zlomek. Pak

$$|q\xi - p| \overset{2.11}{>} |q_{m+1}\xi - p_{m+1}| \overset{2.9d}{\geq} |q_n\xi - p_n|,$$

tedy $\frac{p}{q}$ není lepší aproximace než $\frac{p_n}{q_n}$.
b) $\frac{p}{q} = \frac{p_{m+1}}{q_{m+1}}$ je sblížený zlomek. Pak to není lepší aproximace opět podle věty 2.9d).

Buď naopak $\frac{r}{s}$ dobrá aproximace ξ. Berme n takové, že $q_{n-1} < s \leq q_n$ (pokud $\xi \in \mathbb{Q}, \xi = [a_0, \dots, a_k]$ a $s > q_k$, pak se určitě nejedná o dobrou aproximaci, protože $\frac{p_k}{q_k}$ má chybu 0). Pokud $\frac{r}{s} \neq \frac{p_n}{q_n}$, pak můžeme použít lemma 2.11:

$$|s\xi - r| \geq |q_n\xi - p_n| + |q_{n-1}\xi - p_{n-1}| \geq |q_{n-1}\xi - p_{n-1}|,$$

což je spor s tím, že $\frac{r}{s}$ je dobrá aproximace. Tedy $\frac{r}{s} = \frac{p_n}{q_n}$. □

Ve větě 2.9c) jsme viděli, že sblížené zlomky dávají aproximace s malou chybou $\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$. Platí i částečný opak: pokud má aproximace malou chybu, pak musí jít o sblížený zlomek:

Tvrzení 2.12. *Buď $\xi > 0$ iracionální. Je-li $\frac{p}{q} \in \mathbb{Q}$ takové, že*

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}, \text{ pak } \frac{p}{q} = \frac{p_n}{q_n} \text{ pro nějaké } n.$$

Důkaz. Pro spor ať $\frac{p}{q}$ není sblížený zlomek a buď n takové, že $q_{n-1} < q \leq q_n$ (případ $q = 1$ je opět potřeba ošetřit samostatně).
Lemma 2.11 dává, že $|p_{n-1} - q_{n-1}\xi| < |p - q\xi| < \frac{1}{2q}$. Pak

$$\frac{1}{qq_{n-1}} \leq \frac{\text{něco}}{qq_{n-1}} = \left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| \overset{\Delta-\text{ner.}}{\leq} \left|\frac{p}{q} - \xi\right| + \left|\xi - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q^2} + \frac{1}{2qq_{n-1}}.$$

Odtud úpravou dostáváme $q < q_{n-1}$, spor. □

Ještě poznamenejme, že vždy aspoň jeden ze dvou sousedních sblížených zlomků $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$ splňuje $\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}$.

2.7 Periodické řetězové zlomky

Věta 2.13. *Ať je ξ iracionální. Jeho řetězový zlomek $\xi = [a_0, a_1, \dots]$ je od jistého místa periodický, právě když je ξ algebraické číslo stupně 2 (čili iracionální kořen nějakého kvadratického polynomu s celočíselnými koeficienty).*

Důkaz. „⇒“ Ať $\xi = [a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+l-1}}]$.
Máme $\xi = [a_0, \dots, a_{k-1}, \xi_k]$, kde $\xi_k = [\overline{a_k, \dots, a_{k+l-1}}]$. Číslo ξ_k má čistě periodický řetězový zlomek, neboli platí $\xi_{k+l} = \xi_k$. Použijeme tvrzení 2.8 pro ξ_k místo ξ a $n = k+l-1$. Pak $\xi_k = \xi_{k+l}$ odpovídá ξ_{n+1} z tvrzení, a tedy

$$\xi_k \overset{2.8}{=} \frac{\xi_{k+l}p_n + p_{n-1}}{\xi_{k+l}q_n + q_{n-1}} = \frac{\xi_k p_n + p_{n-1}}{\xi_k q_n + q_{n-1}},$$

kde $\frac{p_i}{q_i}$ jsou sblížené zlomky pro ξ_k.
Vynásobením jmenovatelem pravé strany vidíme, že ξ_k je kořen kvadratického polynomu s celočíselnými koeficienty.
Dále opět použijeme tvrzení 2.8, které nám dává vyjádření čísla ξ pomocí ξ_k. Úpravou tohoto vzorce dostaneme

$$\xi_k = \frac{a\xi + b}{c\xi + d}$$

pro vhodná celá čísla a, b, c, d. Dosazením tohoto vyjádření do kvadratického polynomu pro ξ_k dostaneme hledaný kvadratický polynom pro ξ.

„⇐“ Jenom naznačíme myšlenku:
Ať ξ splňuje $a\xi^2 + b\xi + c = 0$ pro nějaká $a, b, c \in \mathbb{Z}, a \neq 0$.

Dosadíme sem vztah z tvrzení 2.8, což se upraví na kvadratickou rovnici $A_n\xi_{n+1}^2+B_n\xi_{n+1}+C_n=0$, kde $A_n, B_n, C_n \in \mathbb{Z}$ vyjádříme pomocí a, b, c, p_i, q_i (například $A_n = C_{n+1} = ap_n^2 + bp_nq_n + cq_n^2$).
Pak se dokáže, že existuje $K \in \mathbb{N}$ takové, že $-K < A_n, B_n, C_n < K$ pro všechna n.
Teď můžeme použít oblíbený trik z důkazu věty 2.3: máme nekonečně mnoho trojic (A_n, B_n, C_n), ale jen konečně možných hodnot pro ně. Odtud plyne, že existuje trojice $(A, B, C) \in \mathbb{Z}^3$ taková, že $(A, B, C) = (A_n, B_n, C_n)$ pro aspoň tři různá $n = n_1, n_2, n_3$.
Tedy $\xi_{n_1+1}, \zeta_{n_2+1}, \zeta_{n_3+1}$ splňují stejnou kvadratickou rovnici $Ax^2 + Bx + C = 0$. Tedy aspoň dvě z nich se rovnají, búno $\xi_{n_1+1} = \xi_{n_2+1}$. Pak řetězový zlomek pro ξ je periodický s periodou $|n_1 - n_2|$.
Detaily jsou např. v článku Martina Kuděje
http://www.karlin.mff.cuni.cz/~kala/1920%20tc/kudej.pdf □

2.8 Zpět k Pellově rovnici

Věta 2.14. *Ať dvojice $p, q \in \mathbb{N}, (p, q) = 1$, je řešením rovnice $x^2 - my^2 = B$, kde $m \in \mathbb{N}$, m není čtverec a $B \in \mathbb{Z}, |B| < \sqrt{m}$. Pak $\frac{p}{q}$ je sblížený zlomek čísla $\sqrt{m}$.*

Poznámka. Speciálně věta funguje pro $B = 1$, takže netriviální řešení vznikne ze sblíženého zlomku.

Důkaz. Rozlišíme dva případy podle znaménka čísla B (pro $B = 0$ rovnice zřejmě žádné řešení nemá):
a) $0 < B < \sqrt{m}$. Pak

$$\left(\frac{p}{q} + \sqrt{m}\right)\left(\frac{p}{q} - \sqrt{m}\right) = \frac{p^2}{q^2} - m = \frac{B}{q^2} > 0,$$

a tedy

$$0 < \frac{p}{q} - \sqrt{m} = \frac{B}{q^2 \cdot \left(\frac{p}{q} + \sqrt{m}\right)} \overset{\frac{p}{q} > \sqrt{m}}{<} \frac{\sqrt{m}}{q^2 \cdot 2\sqrt{m}} = \frac{1}{2q^2}.$$

Tedy $\frac{p}{q}$ je sblížený zlomek podle tvrzení 2.12.

b) $-\sqrt{m} < B < 0$. Pak $q^2 - \frac{1}{m}p^2 = -\frac{B}{m} > 0$. Jako v předchozím bodě pak dokážeme, že $\frac{q}{p}$ je sblížený zlomek pro $\frac{1}{\sqrt{m}}$. Ale $\frac{1}{\sqrt{m}} = [0, a_0, a_1, \dots]$, kde $\sqrt{m} = [a_0, a_1, \dots]$. Tudíž $\frac{p}{q}$ je sblížený zlomek pro $\sqrt{m}$. □

Pro Pellovou rovnici $x^2 - my^2 = \pm 1$ větu ještě můžeme výrazně zlepšit, což ale nebudeme dokazovat:

Věta 2.15. *Ať $m \in \mathbb{N}$, m není čtverec přirozeného čísla.*
Pak existuje nejmenší $\ell \in \mathbb{N}$ takové,že $\sqrt{m} = [a_0, \overline{a_1, \dots, a_{\ell-1}, 2a_0}]$, kde $a_i = a_{\ell-i} < 2a_0$ pro $i = 1, \dots, \ell - 1$.
Je-li ℓ sudé, pak $x^2 - my^2 = -1$ nemá řešení v $\mathbb{Z}$ a minimální řešení rovnice $x^2 - my^2 = 1$ je $(p_{\ell-1}, q_{\ell-1})$.
Naopak, je-li ℓ liché, pak minimální řešení $x^2 - my^2 = -1$ je $(p_{\ell-1}, q_{\ell-1})$ a minimální řešení $x^2 - my^2 = 1$ je $(p_{2\ell-1}, q_{2\ell-1})$.

Konečně poznamenejme, že až na přenásobení minimálním řešením ve větě 2.14 platí, že $\frac{p}{q} = \frac{p_n}{q_n}$ pro $0 \le n \le 2l - 1$ (stačí tedy uvažovat jen těchto prvních 2ℓ sblížených zlomků).

3. Odmocniny z jedné

Zásadní roli v teorii čísel hrají komplexní odmocniny z jedné.

Definice. Komplexní číslo $z \in \mathbb{C}$ je *n-tá odmocnina z jedné*, pokud $z^n = 1$ pro nějaké přirozené číslo n.
Komplexní číslo $z \in \mathbb{C}$ je *primitivní n-tá odmocnina z jedné*, pokud $z^n = 1$ a navíc $z^m \neq 1$ pro žádné $1 \leq m < n$.

Pomocí komplexní exponenciály je můžeme snadno vyjádřit. Všimněme si totiž, že

$$\zeta_n := e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

je primitivní n-tá odmocnina z 1.

Cvičení. α je primitivní n-tá odmocnina z $1 \Leftrightarrow \alpha = \zeta_n^a$ pro nějaké $(a, n) = 1$.

3.1 Gaussovská celá čísla

Speciálně máme $\zeta_4 = i = \sqrt{-1}$.

Trochu obecněji, buď $D \neq 0, 1$ bezčtvercové (klidně záporné). Na řešení diofantických rovnic se hodí pracovat v $\mathbb{Z}\left[\sqrt{D}\right] = \left\{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\right\}$ (respektive někdy v $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$).
Pro malé D se jedná o eukleidovský obor (norma $|N(a + b\sqrt{D})| = |a^2 - Db^2|$ je eukleidovská).

Příklad. $\mathbb{Z}\left[\sqrt{D}\right]$ je eukleidovské pro $D = -2, -1, 2, 3$ (a pro řadu dalších kladných D, kde ovšem často musíme volit jinou normu).
$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ je eukleidovské pro $D = -3, 5$ (a další kladná D).

Důvod, proč někdy uvažujeme $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ je ten, že chceme brát všechny „celistvé prvky“ v tělese $\mathbb{Q}\left(\sqrt{D}\right)$, čili prvky, jež mají monický minimální polynom s celočíselnými koeficienty.

Případ $D = -1$, to jest $\mathbb{Z}[i]$, nazýváme *gaussovská celá čísla.*
Jejich základní vlastnosti a pojmy:

- Příslušnou normou je $N(a + bi) = a^2 + b^2$.
- Konjugace: $\overline{a + bi} = a - bi$.
- Pro normu platí $N(\alpha) = \alpha\overline{\alpha}$.

- α dělí β, $\alpha \mid \beta$, pokud $\beta = \alpha\gamma$ pro nějaké γ.
- Jednotky (neboli invertibilní prvky) jsou $\pm 1, \pm i$
- α je invertibilní $\Leftrightarrow N(\alpha) = 1$.
- prvky α, β jsou asociované, $\alpha \| \beta$, pokud $\alpha = \varepsilon\beta$ pro nějakou jednotku ε.
- Eukleidovský $\Rightarrow$ gaussovský, čili máme jednoznačné rozklady na součin prvočinitelů.

Zdůrazněme, že formálně vzato je potřeba rozlišovat mezi dělitelností v $\mathbb{Z}$ a dělitelností v $\mathbb{Z}[i]$. Pro oboje ale používáme stejné značení, takže je dobré si rozmyslet, co se daným značením vždy myslí. Zároveň ale naštěstí platí:

Cvičení. Ať $a, b \in \mathbb{Z}$. Pak a dělí b v $\mathbb{Z}$, právě když a dělí b v $\mathbb{Z}[i]$.

Ale pozor! Platnost tohoto cvičení vůbec není samozřejmá!

Cvičení. Najdi příklad okruhu $R \supset \mathbb{Z}$ takového, že pro některá $a, b \in \mathbb{Z}$ platí:
a dělí b v R, ale a nedělí b v $\mathbb{Z}$.

Jak vypadají prvočinitele v $\mathbb{Z}[i]$?

Lemma 3.1. *Buď $p \in \mathbb{Z}$ prvočíslo.*
Pokud p nejde vyjádřit jako $a^2 + b^2$ (pro $a, b \in \mathbb{Z}$), pak je p prvočinitel v $\mathbb{Z}[i]$.
Pokud $p = a^2 + b^2$, pak jsou prvočinitele $a \pm bi$ (a také jejich násobky jednotkami).
Všechny prvočinitele v $\mathbb{Z}[i]$ jsou jednoho z těchto dvou tvarů.

Příklad.

- $2 = 1^2 + 1^2 \Rightarrow 1 + i$ je prvočinitel. Všimněme si, že $2 = -i(1+i)^2$.
- $3 \neq a^2 + b^2$.
- $5 = 2^2 + 1^2 \Rightarrow 2 \pm i$ jsou prvočinitele.

Důkaz. Je-li α prvočinitel, pak je také $\overline{\alpha}$ prvočinitel (protože $\alpha = \beta\gamma \Leftrightarrow \overline{\alpha} = \overline{\beta}\overline{\gamma}$).

Buď nyní $\alpha \in \mathbb{Z}[i]$ prvočinitel, $\alpha = a + bi$. Máme $N(\alpha) = \alpha\overline{\alpha}$, což je rozklad na součin prvočinitelů. Pak máme dvě možnosti:
a) $N(\alpha) = p$ je prvočíslo v $\mathbb{Z}$. Pak $p = a^2 + b^2$.

b) $N(\alpha)$ není prvočíslo v $\mathbb{Z}$, tedy $N(\alpha) = uv$ pro celá čísla $u, v > 1$.
Tedy platí $uv = \alpha\overline{\alpha}$ a z jednoznačnosti rozkladu v $\mathbb{Z}[i]$ dostáváme búno $u \| \alpha, v \| \overline{\alpha}$ (protože $\alpha, \overline{\alpha}$ jsou prvočinitele a u, v nejsou invertibilní). To pak implikuje $v = \overline{v} \| \alpha \| u$.
Tedy $v = \pm u$ nebo $\pm iu$.
$v = \pm iu$ zřejmě nemůže nastat (protože u, v jsou celá, a tedy reálná, čísla), a protože $u, v > 1$, nemůže nastat ani $v = -u$. Tedy nutně $v = u$ a máme $N(\alpha) = u^2$.
u musí být nějaké prvočíslo p (jinak $u = yz$ a $y^2z^2 = \alpha\overline{\alpha}$, což by byl spor s jednoznačností rozkladů).

Dostali jsme tedy, že $N(\alpha) = p^2$ a $\alpha \| p$. Navíc kdyby $p = c^2 + d^2$, pak $\alpha \| (c + di)(c - di)$, což by byl spor s tím, že α je prvočinitel.

Tedy jsme dokázali: Pokud je α prvočinitel, pak
a) $\alpha = a + bi$ pro prvočíslo $p = a^2 + b^2 \in \mathbb{Z}$, nebo
b) $\alpha \| p$ pro prvočíslo $p \in \mathbb{Z}, p \neq c^2 + d^2$.

Naopak máme:

Cvičení. Ať $\beta \in \mathbb{Z}[i]$. Pokud $N(\beta) = p$ je prvočíslo v $\mathbb{Z}$, pak β je prvočinitel v $\mathbb{Z}[i]$.
Tedy pokud $p = a^2 + b^2$, pak $\alpha = a \pm bi$ má normu $N(\alpha) = p$, a tedy α je prvočinitel.

Konečně ať je p prvočíslo, $p \neq a^2 + b^2$, a pro spor ať p není prvočinitel v $\mathbb{Z}[i]$, čili $p = (c + di)(e + fi)$ je jeho rozklad na součin dvou neinvertibilních prvků.
Pak $p^2 = N(p) = N(c + di)N(e + fi)$, a tedy $N(c + di) = p$ (protože $N(e + fi) \neq 1$). To ale znamená, že $c^2 + d^2 = p$, což je spor. □

Která prvočísla jdou vyjádřit jako součet dvou čtverců?

Věta 3.2. *a) Prvočíslo $p \in \mathbb{N}$ jde vyjádřit jako $p = a^2 + b^2$, právě když $p = 2$ nebo $p \equiv 1 \pmod 4$.*
b) Všichni prvočinitele v $\mathbb{Z}[i]$ jsou (až na přenásobení jednotkami):

- $p \in \mathbb{N}, p \equiv 3 \pmod 4$,
- $a \pm bi$, *kde* $p = a^2 + b^2 \equiv 1 \pmod 4$ *pro* $a, b \in \mathbb{N}$,
- $1 + i$

(kde $p \in \mathbb{N}$ je vždy prvočíslo).

Důkaz. Stačí dokázat první část a).
„⇒“ Cvičení (použij, že $x^2 \equiv 0, 1 \pmod 4$).
„⇐“ Ať $p \equiv 1 \pmod 4$. Wilsonova věta 3.3 říká, že $(p-1)! \equiv -1 \pmod p$. Máme tedy

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdots (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (-1)^{\frac{p-1}{2}} \cdot \frac{p-1}{2} \cdots 2 \cdot 1 \overset{p\equiv 1(4)}{=} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod p.\end{aligned}$$

Tedy existuje $x = \left(\frac{p-1}{2}\right)!$ takové, že $p \mid x^2 + 1 = (x + i)(x - i)$. Kdyby p byl prvočinitel v $\mathbb{Z}[i]$, pak $p \mid x \pm i$.
Ale $x \pm i = p(c + di) \Rightarrow \pm 1 = pd$, což je spor. Tedy p není prvočinitel v $\mathbb{Z}[i]$. Lemma 3.1 pak implikuje, že $p = a^2 + b^2$. □

Zbývá tedy dokázat Wilsonovu větu:

Věta 3.3 (Wilsonova)**.** *Pro prvočíslo p platí $(p-1)! \equiv -1 \pmod p$.*
Pro složené $n > 4$ platí $(n-1)! \equiv 0 \pmod n$.

Důkaz. Dokážeme pouze první část pro liché prvočíslo p (pro $p = 2$ platí zřejmě), druhou necháme jako cvičení.
Polynom $x^{p-1} - 1$ nad tělesem $\mathbb{Z}_p$ má kořeny $1, 2, \ldots, p-1$, takže se rovná součinu příslušných kořenových činitelů

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)).$$

Porovnáním konstantních členů vidíme, že $(p-1)! = (-1)^{p-1}(p-1)! \equiv -1 \pmod p$. □

To byl ale zvláštní trik s Wilsonem! Naštěstí se dá nahradit kvadratickými zbytky: v tvrzení 4.16 například popíšeme, kdy $p = a^2 + 2b^2$, což charakterizuje prvočinitele v $\mathbb{Z}\left[\sqrt{-2}\right]$.

3.2 Cyklotomické polynomy

Nyní budeme zkoumat ireducibilní rozklad polynomu $x^n - 1$, který má za kořeny n-té odmocniny z jedné. Příslušné ireducibilní faktory se nazývají cyklotomické polynomy a my jich využijime k důkazu speciálního případu Dirichletovy věty, čili že *pro každé přirozené číslo a existuje nekonečně mnoho prvočísel p tvaru $ax + 1$.*

Zajímá nás ireducibilní rozklad polynomu $x^n - 1$.
Začněme nejjednodušším případem, kdy $n = p$ je prvočíslo. Máme $\zeta_p^p = 1$, tedy ζ_p je kořen $x^p - 1$. Dokonce $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$, a tedy ζ_p je kořen polynomu $f(x) = x^{p-1} + \cdots + x + 1$. Dokažme teď, že $f(x)$ je ireducibilní (což ještě obecněji uvidíme ve větě 3.9):

Lemma 3.4. *$f(x) = x^{p-1} + \cdots + x + 1$ je ireducibilní polynom.*

Důkaz. Uvažujme substituci $x = y + 1$. Pak

$$f(x) = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \frac{y^p + \binom{p}{1} y^{p-1} + \cdots + \binom{p}{p-1} y}{y}$$
$$= y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-2} y + \binom{p}{p-1}.$$

Vidíme, že p dělí všechny koeficienty $\binom{p}{j}$ pro $j = 1, \ldots, p-1$ a p^2 nedělí konstantní koeficient $\binom{p}{p-1}$. Takže jde o ireducibilní polynom podle Eisensteinova kritéria. □

Definice. Buď $\zeta_n = e^{\frac{2\pi i}{n}}$ primitivní n-tá odmocnina z 1.
n-tý *cyklotomický* (kruhový) *polynom* definujeme jako

$$t_n(x) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta_n^a),$$

kde násobíme přes všechna a, která jsou nesoudělná s n

Příklad. $t_1(x) = x - 1$, protože $\zeta_1 = 1$.
$t_2(x) = (x - \zeta_2^1) = x + 1$, protože $\zeta_2 = -1$.
$t_4(x)$: Máme $\zeta_4 = i$, a tedy

$$t_4(x) = (x - i^1)(x - i^3) = (x - i)(x + i) = x^2 + 1.$$

Je-li p prvočíslo, pak

$$t_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1},$$

což se dokáže ověřením, že polynomy nalevo i napravo mají stejný stupeň $p - 1$ a stejné kořeny.

Tvrzení 3.5.
a) $\deg(t_n) = \varphi(n)$.
b)

$$x^n - 1 = \prod_{d|n} t_d(x),$$

kde násobíme přes všechna přirozená čísla d, která dělí n.
c) $t_n(x) \in \mathbb{Z}[x]$ a jeho konstantní člen $t_n(0) = \pm 1$.

Příklad. Části b) z tvrzení můžeme výhodně použít k tomu, abychom indukcí počítali cyklotomické polynomy:
Například známe-li už

$$t_1(x) = x - 1, t_2(x) = x + 1, t_3(x) = x^2 + x + 1,$$

pak víme, že

$$t_1 t_2 t_3 t_6 = x^6 - 1 = (x^3 - 1)(x^3 + 1),$$

přičemž $t_1 t_3 = x^3 - 1$, takže

$$t_2 t_6 = x^3 + 1 = (x + 1)(x^2 - x + 1),$$

čili konečně $t_6(x) = x^2 - x + 1$.

Důkaz. a) Zřejmé.

b) Každé ζ_n^a pro $1 \leq a \leq n$, je kořen $x^n - 1$, a tedy

$$x^n - 1 = \prod_{1 \leq a \leq n} (x - \zeta_n^a).$$

Rozdělíme si teď různé hodnoty a v součinu podle jejich největšího společného dělitele s n. Pro a buď $d := (a, n)$, takže máme $a = d \cdot b$, kde $\left(b, \frac{n}{d}\right) = 1$ (cvičení).
Máme pak

$$\zeta_n^a = \zeta_n^{db} = e^{2\pi i \frac{b}{n/d}} = \zeta_{n/d}^b.$$

Tedy

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \leq a \leq n \\ (a,n)=d}} (x - \zeta_n^a) \overset{b=a/d}{=} \prod_{d|n} \prod_{\substack{1 \leq b \leq n/d \\ (b,n/d)=1}} (x - \zeta_{n/d}^b) = \prod_{d|n} t_{n/d}(x) \overset{e=n/d}{=} \prod_{e|n} t_e(x).$$

c) Indukcí podle n:
$n = 1 : t_1(x) = x - 1$ – zřejmé.
$n > 1$: Ať

$$t_n(x) = \sum a_i x^i (a_i \in \mathbb{C}) \text{ a } \prod_{d|n, d<n} t_d(x) = \sum b_j x^j.$$

Podle IP víme, že $b_j \in \mathbb{Z}$ a $b_0 = \pm 1$.
Máme

$$x^n - 1 = \prod_{d|n} t_d(x) = (a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots),$$

takže můžeme porovnat koeficienty:

- $-1 = a_0 b_0 \Rightarrow a_0 = \pm 1$.
- $0 = a_0 b_1 + b_0 a_1 \Rightarrow \pm a_1 = -a_0 b_1 \in \mathbb{Z}$.
- $\vdots$

V každém dalším kroku dostaneme $a_i \in \mathbb{Z}$. □

Poznamenejme, že v důkazu části c) jsme také mohli použít tvrzení z algebry o vztahu dělitelnosti v oboru $\mathbb{Z}[x]$ a nad podílovým tělesem $\mathbb{Q}[x]$.
Ještě zbývá dokázat ireducibilitu $t_n(x)$, což uděláme na závěr ve větě 3.9. K důkazu věty 3.7 o aritmetických posloupnostech ji ale ani nepotřebujeme.

3.3 Prvočísla $kn+1$

Chceme dokázat, že pro $n \in \mathbb{N}$ existuje nekonečně mnoho prvočísel tvaru $kn+1, k \in \mathbb{N}$. Klíčovým krokem v důkazu je existence aspoň jednoho takového prvočísla, jež je založená na tom, že pokud $p \mid t_n(c)$ pro vhodné c, pak $p \equiv 1 \pmod{n}$ (jak záhy uvidíme):

Tvrzení 3.6. *Pro každé $n \in \mathbb{N}$ existuje aspoň jedno prvočíslo $p \equiv 1 \pmod{n}$.*

Důkaz. Buď

$$g(x) := \prod_{d<n, d\mid n} t_d(x), \text{ čili } t_n(x) \cdot g(x) = x^n - 1.$$

$t_d(x) \in \mathbb{Z}[x]$ podle tvrzení 3.5c), takže i $g(x) \in \mathbb{Z}[x]$.
t_n a g nemají společný kořen v $\mathbb{C}$, takže jsou nesoudělné jako polynomy v $\mathbb{Q}[x]$, což je euklidovský obor. Bézoutova věta pro $\mathbb{Q}[x]$ pak implikuje, že existují polynomy $f_0(x), h_0(x) \in \mathbb{Q}[x]$ takové, že $t_n(x) \cdot f_0(x) + g(x) \cdot h_0(x) = 1$. Můžeme vynásobit f_0, h_0 vhodným společným násobkem jmenovatelů $c \in \mathbb{Z}$ tak, aby $c \geq 3, f(x) := cf_0(x), h(x) := ch_0(x) \in \mathbb{Z}[x]$. Pak

$$(\heartsuit) \quad t_n(x)f(x) + g(x)h(x) = c$$

je rovnost polynomů ze $\mathbb{Z}[x]$.

Uvažujme nyní $t_n(c)$. Máme $c \geq 3$ a $|t_n(c)| = \prod_{(a,n)=1} |c - \zeta_n^a|$. Každý ze součinitelů na pravé straně je > 1 (jde o vzdálenost bodů c a ζ_n^a v komplexní rovině – nakreslete si obrázek!), takže máme $|t_n(c)| > 1$.
Tedy existuje prvočíslo p takové, že $p \mid t_n(c)$.

Pozorování. $p \equiv 1 \pmod{n}$.

Důkaz. $p \mid t_n(c) \mid c^n - 1$, čili $c^n \equiv 1 \pmod{p}$.
Buď d nejmenší přirozené číslo takové, že $c^d \equiv 1 \pmod{p}$ (takovéto d se nazývá *řád* prvku c). Pak nutně $d \mid n$, protože jinak $n = ud + v$ pro $0 < v < d$ a $c^v \equiv c^n \cdot (c^d)^{-u} \equiv 1 \pmod{p}$.
Chceme dokázat, že $d = n$; pro spor ať $d < n$. Pak

$$p \mid c^d - 1 = \prod_{e\mid d} t_e(c) \mid g(c).$$

Zároveň $p \mid t_n(c)$, a tedy $(\heartsuit)$ po dosazení $x = c$ implikuje $p \mid c$, což je spor s $c^n \equiv 1 \pmod{p}$.
Tedy $d = n$ je nejmenší přirozené číslo takové, že $c^n \equiv 1 \pmod{p}$. Ovšem podle Eulerovy věty máme $c^{p-1} \equiv 1 \pmod{p}$, odkud stejnou úvahou jako výše plyne, že $n \mid p-1$ (jinak bychom vydělili se zbytkem $p - 1 = nu' + v'$), neboli $p \equiv 1 \pmod{n}$. □

□

Na konci důkazu jsme dokazovali, že $d \mid n$ a že $n \mid p-1$. V obou případech jde o vlastnosti *řádu prvku*, které také souvisí s *Lagrangeovou větou*, kterou uvidíte v Algebře.

Věta 3.7. *Buď $n \in \mathbb{N}$. Pak existuje nekonečně mnoho prvočísel tvaru $p = kn+1, k \in \mathbb{N}$.*

Důkaz. Uvažujme tvrzení 3.6 pro $n, 2n, 3n, \ldots$. Vždy existuje nějaké prvočíslo, označme je $p_1, p_2, p_3, \ldots$. Zároveň $p_j \geq jn+1$, takže posloupnost $\{p_j\}_{j\geq 1}$ jde do nekonečna. Tudíž tato posloupnost obsahuje nekonečně mnoho různých prvočísel. Pro každé z nich ale máme $p_j \equiv 1 \pmod{jn}$, takže $p_j \equiv 1 \pmod{n}$. □

Poznámka.

- Ve skutečnosti platí: Je-li p dost velké prvočíslo takové, že $p \mid t_n(a)$ pro nějaké a, pak $p \equiv 1 \pmod{n}$. Úzce to souvisí s tím, jestli p zůstane prvočíslem v $\mathbb{Z}[\zeta_n]$, případně jak se tam rozkládá.
- Podobně se dají dokázat další speciální případy Dirichletovy věty použitím $p \mid f(a)$ pro jiné polynomy f: jde o takzvané eukleidovské důkazy. Ale nejde takto dokázat všechny případy, platí:

  Dirichletova věta jde takto dokázat pro $p \equiv m \pmod{n}$, právě když $m^2 \equiv 1 \pmod{n}$.

  Viz bakalářka Martina Čecha

  https://drive.google.com/file/d/1siGFFDJzCqR5cVCL2a_WapJTsWIt7rxY/

3.4 Ireducibilita cyklotomických polynomů

Chceme dokázat, že $t_n(x)$ je ireducibilní polynom v $\mathbb{Q}[x]$. Z Algebry se nám bude hodit:

Lemma 3.8 (Důsledek Gaussova lemmatu)**.** *Ať nekonstantní polynom $f \in \mathbb{Z}[x]$ není ireducibilní v $\mathbb{Q}[x]$. Pak $f(x)$ není ireducibilní v $\mathbb{Z}[x]$, čili existují nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ takové, že $f(x) = g(x) \cdot h(x)$.*

Věta 3.9. *Cyklotomický polynom $t_n(x) \in \mathbb{Z}[x]$ je ireducibilní v $\mathbb{Q}[x]$ pro každé $n \geq 1$.*

Důkaz. $t_n(x) \in \mathbb{Z}[x]$ podle tvrzení 3.5. Ať pro spor je reducibilní, čili $t_n(x) = g(x) \cdot h(x)$, přičemž díky Gaussovu lemmatu 3.8 můžeme předpokládat, že $g, h \in \mathbb{Z}[x]$.
Buď ζ nějaká primitivní n-tá odmocnina z 1. Pak ζ je kořen t_n, takže búno ať ζ je kořen $g(x)$ a g je ireducibilní.

Buď p prvočíslo, $p \nmid n$. Chceme dokázat, že ζ^p je také kořen $g(x)$. Pro spor ať není. ζ^p je kořen $t_n(x)$, takže ζ^p je kořen $h(x)$, a tedy ζ je kořen $h(x^p)$.
Uvažujme nyní $NSD_{\mathbb{Q}[x]}(g(x), h(x^p))$: Polynom $g(x)$ je ireducibilní, takže toto NSD je 1 nebo $g(x)$. Zároveň polynomy $g(x)$ a $h(x^p)$ mají společný kořen ζ, takže nejsou nesoudělné a tedy jejich $NSD = g(x)$. To ale znamená, že $g(x) \mid h(x^p)$ *(poznamenejme, že tato úvaha jde zjednodušit pomocí pojmu minimálního polynomu)*; ať

$$h(x^p) = g(x) \cdot k(x) \text{ pro nějaké } k \in \mathbb{Z}[x].$$

Máme: Pro všechny $f(x) \in \mathbb{Z}_p[x]$, $f(x)^p = f(x^p)$.
Důkaz: $(\sum a_i x^i)^p$ roznásobíme podle multinomické věty, kde všechny koeficienty jsou dělitelné p, až na $\sum a_i^p \cdot x^{pi} = \sum a_i \cdot (x^p)^i = f(x^p)$: Obecně totiž platí, že po roznásobení $(x_1 + \cdots + x_k)^p$ jsou všechny koeficienty, vyjma těch u x_i^p, dělitelné p, jak se dokáže indukcí z binomické věty (cvičení).

Uvažujme projekci modulo p:

$$\begin{aligned}\pi : \mathbb{Z} &\to \mathbb{Z}_p \\ a &\mapsto a \pmod p.\end{aligned}$$

Ta indukuje homomorfismus okruhů polynomů

$$\begin{aligned}\pi_x : \mathbb{Z}[x] &\to \mathbb{Z}_p[x] \\ \sum a_i x^i &\mapsto \sum \pi(a_i) x^i.\end{aligned}$$

Máme tedy

$$\pi_x(g)(x) \cdot \pi_x(k)(x) = \pi_x(h)(x^p) = (\pi_x(h)(x))^p.$$

Buď $a(x) \in \mathbb{Z}_p[x]$ nějaký ireducibilní faktor $\pi_x(g)$. Potom $a(x) \mid \pi_x(g) \mid \pi_x(h)^p$, takže $a \mid \pi_x(h)$, protože a je ireducibilní. Ale pak

$$a(x)^2 \mid \pi_x(g) \cdot \pi_x(h) = \pi_x(t_n) \mid \pi_x(x^n - 1),$$

neboli polynom $\pi_x(x^n - 1) = x^n - 1$ má násobný kořen v kořenovém nadtělese polynomu $a(x)$ nad tělesem $\mathbb{Z}_p$, což je spor s:

Tvrzení 3.10. *Buď T těleso charakteristiky p, kde $p \nmid n$. Pak polynom $x^n - 1$ nemá v T násobné kořeny.*

Toto tvrzení dokážeme za chvíli, až dokončíme důkaz věty.

Dostali jsme tedy spor, čili ζ^p je kořen $g(x)$. Tedy jsme dokázali:
Pokud $g \in \mathbb{Z}[x]$ je ireducibilní, ζ je primitivní n-tá odmocnina z 1 a $p \nmid n$, pak

$$g(\zeta) = 0 \Rightarrow g(\zeta^p) = 0.$$

Ale ζ^p je opět primitivní n-tá odmocnina z 1, můžeme tedy volit další prvočíslo p' (klidně $p = p'$) a dostat $g\left(\zeta^{p \cdot p'}\right) = 0$, a tak dále.
Postupně dostaneme:

$$g\left(\zeta^m\right) = 0 \text{ pro všechna } (m, n) = 1.$$

Tedy g má za kořeny všechny primitivní n-té odmocniny z 1 (protože jsou to ζ^a, kde $1 \leq a \leq n, (a, n) = 1$). Ale ty jsou z definice všechny kořeny t_n, takže $t_n \mid g$. Zároveň na začátku jsme g volili tak, že $g \mid t_n$, a proto $g(x) = t_n(x)$. Navíc g je ireducibilní, a tedy i t_n je ireducibilní. □

Zbývá dokázat tvrzení 3.10:

Důkaz tvrzení 3.10. Uvažujme formální derivaci polynomu $f \in T[x]$, definovanou jako

$$\left(\sum a_i x^i\right)' = \sum i a_i x^{i-1}$$

(čili normálním vzorečkem z analýzy pro derivaci polynomu). Splňuje obvyklé vzorce pro součet a součin, a tedy také:
Ať má $f(x)$ dvojnásobný kořen α, čili $f(x) = (x - \alpha)^2 \cdot g(x)$. Pak

$$f'(x) = 2(x - \alpha) \cdot g(x) + (x - \alpha)^2 \cdot g'(x) = (x - \alpha) \cdot \left[2g(x) + (x - \alpha)g'(x)\right].$$

Tedy $x - \alpha \mid NSD(f, f')$.
Ale $(x^n - 1)' = nx^{n-1}$, takže pokud $n \neq 0$ v $\mathbb{Z}_p$ (čili $p \nmid n$), pak jediná možnost pro násobný kořen je $\alpha = 0$. Ale 0 samozřejmě není kořen $f(x) = x^n - 1$. Tedy $x^n - 1$ nemá násobné kořeny. □

4. Charaktery a kvadratická reciprocita

4.1 Kvadratické zbytky

Definice. Buď p prvočíslo a $a \in \mathbb{Z}$. Pak a je *kvadratický zbytek modulo p*, pokud existuje b takové, že $a \equiv b^2 \pmod{p}$; jinak je to *kvadratický nezbytek*.
Definujeme také Legendreův symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{pokud } p \nmid a \text{ a } a \text{ je kvadratický zbytek modulo } p, \\ -1, & \text{pokud } p \nmid a \text{ a } a \text{ je kvadratický nezbytek modulo } p, \\ 0, & \text{pokud } p \mid a. \end{cases}$$

Zřejmě platí následující základní vlastnosti:

- $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{0}{p}\right) = 0$
- $\left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)$, pokud $c \not\equiv 0 \pmod{p}$.

Poznamenejme, že uvedená definice kvadratických zbytků a nezbytků dává smysl i modulo složené číslo n, v takovém případě ale *nepoužíváme* značení $\left(\frac{a}{n}\right)$ (protože se takto značí Jacobiho symbol, viz sekci 4.5).
Všimněme si také, že v důkazu věty 3.2 jsme dokázali, že $\left(\frac{-1}{p}\right) = 1$, pokud $p \equiv 1 \pmod{4}$. Ve tvrzení 4.3 za chvíli dokážeme, že to platí jako ekvivalence.

Věta 4.1. *Buď p liché prvočíslo a $a \in \mathbb{Z}$. Pak*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Důkaz. Pokud $p \mid a$, je tvrzení zřejmé. Ať tedy $p \nmid a$.
Buď g *primitivní prvek* modulo p, neboli generátor multiplikativní grupy $\mathbb{Z}_p^*$, neboli prvek řádu $p-1$ v $\mathbb{Z}_p^*$, neboli prvek takový, že

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{g^0 = 1, g^1, g^2, \ldots, g^{p-2}\}$$

(kde mocniny g^k samozřejmě počítáme modulo p). Pro důkaz jeho existence viz přednášku z Algebry nebo 5. kapitolu těchto skript.

Všimněme si, že $\left(\frac{g}{p}\right) = -1$, protože kdyby $g \equiv b^2 \pmod p$, pak bychom podle malé Fermatovy věty měli $g^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p$, a tedy řád g by byl nejvýše $\frac{p-1}{2}$.

Máme $a \equiv g^k \pmod p$ pro jednoznačně určené $0 \leq k \leq p-2$. Protože $\left(\frac{bg^2}{p}\right) = \left(\frac{b}{p}\right)$, máme

$$\left(\frac{a}{p}\right) = \left(\frac{g^k}{p}\right) = \begin{cases} \left(\frac{1}{p}\right) = 1, & \text{pokud } 2 \mid k, \\ \left(\frac{g}{p}\right) = -1, & \text{pokud } 2 \nmid k. \end{cases}$$

Zároveň

$$a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \begin{cases} \equiv 1, & \text{pokud } 2 \mid k, \\ \not\equiv 1, & \text{pokud } 2 \nmid k, \end{cases} \pmod p.$$

Navíc $a^{\frac{p-1}{2}}$ je kořen polynomu $x^2 - 1$ nad tělesem $\mathbb{Z}_p$, takže $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. Tedy pokud $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$, pak $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Dohromady vidíme, že pokud $2 \mid k$, pak se levá i pravá strana věty rovnají 1. Pokud $2 \nmid k$, pak se obě strany rovnají -1. □

Důsledek 4.2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *pro* $a, b \in \mathbb{Z}$ *a liché prvočíslo* p.

Důkaz. Podle věty 4.1 máme

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

Pravá a levá strana této kongruence jsou ale $0, 1, -1$, a tedy se musejí rovnat, když jsou kongruentní modulo p. □

Důsledek 4.3. *Buď* p *liché prvočíslo. Pak*

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

čili -1 *je kvadratický zbytek modulo* $p \iff p \equiv 1 \pmod 4$.

Důkaz. Opět vyplývá z věty 4.1. □

Tvrzení 4.4. *Buď* p *liché prvočíslo. Pak*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

čili 2 *je kvadratický zbytek modulo* $p \iff \pm 1 \pmod 8$.

Důkaz. Počítejme modulo p v $\mathbb{Z}[i]$, čili

$$a + bi \equiv c + di \pmod{p\mathbb{Z}[i]} \Leftrightarrow a \equiv c \pmod p, b \equiv d \pmod p.$$

Kongruence modulo p v $\mathbb{Z}[i]$ budeme typicky značit prostě jako $\pmod p$.

Binomická věta dává

$$(1+i)^p = 1 + \binom{p}{1} i + \binom{p}{2} i^2 + \cdots + \binom{p}{p-1} i^{p-1} + i^p \equiv 1 + i^p \pmod p,$$

protože $p \mid \binom{p}{j}$. Zároveň

$$\begin{aligned}(1+i)^p &= (1+i)\left((1+i)^2\right)^{\frac{p-1}{2}} = (1+i)(2i)^{\frac{p-1}{2}} \\ &= (1+i)i^{\frac{p-1}{2}}2^{\frac{p-1}{2}} \overset{4.1}{\equiv} (1+i)i^{\frac{p-1}{2}}\left(\frac{2}{p}\right) \pmod p.\end{aligned}$$

Budeme porovnávat pravé strany těchto dvou kongruencí, k čemuž rozlišíme dva případy:
a) $p \equiv 1 \pmod 4$. Pak $i^p = i$ a $i^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{4}}$, tedy

$$1+i \equiv (1+i)(-1)^{\frac{p-1}{4}}\left(\frac{2}{p}\right) \pmod p.$$

Vynásobením $1-i$ dostaneme

$$2 \equiv 2(-1)^{\frac{p-1}{4}}\left(\frac{2}{p}\right) \pmod p,$$

což platí už jako kongruence v $\mathbb{Z}$. Tedy $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}} \pmod p$. Na obou stranách kongruence máme ± 1, takže nutně máme rovnost $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$.
b) $p \equiv -1 \pmod 4$. Pak $i^p = -i, i^{\frac{p-1}{2}} = i^{-1} \cdot i^{\frac{p+1}{2}} = -i \cdot (-1)^{\frac{p+1}{4}}$ a podobně se ukáže, že $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$. □

Klíčovou větou je zákon kvadratické reciprocity 4.11: Pro různá lichá prvočísla p, q platí

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

Ten si dokážeme časem.

4.2 Charaktery

Při počítání $\left(\frac{2}{p}\right)$ jsme silně využili to, že $(1+i)^2 \| 2$. Podobně pro důkaz kvadratické reciprocity chceme něco, co splňuje (něco)$^2 \| p$. K tomu nám poslouží charaktery a Gaussovy součty.

Definice. *Multiplikativní charakter modulo n* je grupový homomorfismus

$$\chi : \mathbb{Z}_n^* \to \mathbb{C}^*,$$

tedy zobrazení takové, že $\chi(uv) = \chi(u)\chi(v)$ pro všechna $u, v \in \mathbb{Z}_n^*$.

Poznámka. Pro $a \in \mathbb{Z}_n^*$ máme $a^{\varphi(n)} = 1$, a tedy $1 = \chi(1) = \chi\left(a^{\varphi(n)}\right) = \chi(a)^{\varphi(n)}$, takže hodnota $\chi(a)$ je $\varphi(n)$-tá odmocnina z jedné.

Příklad. $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.
2 je primitivní prvek modulo 5 (a $2^4 \equiv 1 \pmod 5$), takže $\mathbb{Z}_5^* = \{2^0, 2^1, 2^2, 2^3\}$. Jak vypadají charaktery modulo 5?

Pro charakter χ máme $\chi(2^k) = (\chi(2))^k$, takže charakter je jednoznačně určený hodnotou $\chi(2)$, jež musí být být čtvrtou odmocninou z 1, protože $1 = \chi(1) = (\chi(2))^4$.
Například volbou $\chi(2) = i$ dostaneme charakter $\chi = \chi_1$ takový, že

$$\chi(1) = 1, \chi(2) = i, \chi(3) = \chi(2)^3 = -i, \chi(4) = \chi(2)^2 = -1.$$

Všechny charaktery modulo 5 pak jsou dané v této tabulce:

	1	2	3	4
$\chi_0 = \varepsilon$	1	1	1	1
χ_1	1	i	$-i$	-1
χ_2	1	-1	-1	1
χ_3	1	$-i$	i	-1

Všimněme si, že $\chi_2(a) = \left(\frac{a}{5}\right)$ je Legendreův symbol modulo 5!
Mezi charaktery platí různé vztahy, například

$$\chi_2(a) = \chi_1(a)^2 \text{ nebo } \overline{\chi_1(a)} = \chi_1(a)\chi_2(a) = \chi_3(a)$$

pro všechna a.

Lemma 4.5. *Buď p prvočíslo, g primitivní prvek modulo p a $b \in \mathbb{Z}$. Pak zobrazení*

$$\begin{aligned} \chi_b : \mathbb{Z}_p^* &\to \mathbb{C}^* \\ g^k &\mapsto \zeta_{p-1}^{kb} \qquad (\textit{pro } 0 \le k \le p-2) \end{aligned}$$

je charakter modulo p.
Pro $0 \le b \le p-2$ jsou tyto charaktery po dvou různé a obecně $\chi_b = \chi_{b \pmod{p-1}}$.

Pokud (pro dané složené n) v grupě $\mathbb{Z}_n^*$ existuje primitivní prvek g, pak podobně máme charaktery $g \mapsto \zeta_{\varphi(n)}^b$ (kde stačí brát $0 \le b < \varphi(n)$). Tento primitivní prvek ale obecně existovat nemusí – viz důsledek 5.6.

Důkaz. Ať $u = g^k, v = g^l \in \mathbb{Z}_p^*$. Pro ověření multiplikativity si uvědomme, že $uv = g^{k+l \pmod{p-1}}$.
Pak

$$\chi_b(uv) = \chi_b(g^{k+l \pmod{p-1}}) = \zeta_{p-1}^{b(k+l \pmod{p-1})} = \zeta_{p-1}^{b(k+l)} = \zeta_{p-1}^{bk}\zeta_{p-1}^{bl} = \chi_b(u)\chi_b(v).$$

Uvědomme si, že ve 3. rovnosti jsme použili toho, že máme $(p-1)$-ní odmocninu ζ_{p-1}.
Zbytek důkazu je jasný (charaktery jsou různé, protože mají různou hodnotu $\chi_b(g)$). □

Definice. Množina všech charakterů modulo n tvoří grupu, kterou značíme $X(\mathbb{Z}_n^*)$.
Grupové operace jsou definované (pro všechna $a \in \mathbb{Z}_n^*$) takto:

- Součin: $(\chi_1\chi_2)(a) := \chi_1(a)\chi_2(a)$.
- Jednotka: *triviální charakter* $\varepsilon(a) := 1$. Ostatní charaktery se nazývají *netriviální*.
- Inverzní prvek: $\overline{\chi}(a) := \overline{\chi(a)}$.

Cvičení. Ověřte, že jde skutečně o grupu.

Tvrzení 4.6. *Buď p prvočíslo. Pak $X(\mathbb{Z}_p^*) \simeq \mathbb{Z}_{p-1}(+)$.*

Podobné tvrzení platí i pro složené n, kde $X(\mathbb{Z}_n^*) \simeq \mathbb{Z}_n^*$, důkaz je ale o něco složitější.

Důkaz. Buď $g \in \mathbb{Z}_p^*$ primitivní prvek, čili $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{g^0 = 1, g^1, g^2, \ldots, g^{p-2}\}$. χ je jednoznačně určený hodnotou $\chi(g)$, což je nějaká $(p-1)$-ní odmocnina z 1, tedy $\chi(g) = \zeta_{p-1}^b$ pro nějaké $b = 0, 1, \ldots, p-2$. Pak $\chi(g^j) = \zeta_{p-1}^{bj} = \chi_b(g^j)$ pro každé j, což je charakter podle lemmatu 4.5.
Teď zbývá jen ověřit, že zobrazení

$$\begin{aligned} X\left(\mathbb{Z}_p^*\right) &\to \mathbb{Z}_{p-1} \\ \chi_b &\mapsto b, \qquad \text{kde } \chi_b(g) = \zeta_{p-1}^b, \end{aligned}$$

je izomorfismus: Surjektivita a injektivita jsou jasné.
K tomu, že jde o homomorfismus, stačí ověřit toto: Označíme-li χ_b charakter takový, že $\chi_b(g^j) = \zeta_{p-1}^{bj}$, pak platí $\chi_b \cdot \chi_c = \chi_{b+c \pmod{p-1}}$ (cvičení). □

Tvrzení 4.7. *Buď $n > 1$, χ charakter modulo n a $b \in \mathbb{Z}_n^*$. Pak*
a)

$$\sum_{a \in \mathbb{Z}_n^*} \chi(a) = \begin{cases} 0, & \text{pokud } \chi \neq \varepsilon, \\ \varphi(n), & \text{pokud } \chi = \varepsilon. \end{cases}$$

b)

$$\sum_{\chi \in X(\mathbb{Z}_n^*)} \chi(b) = \begin{cases} 0, & \text{pokud } b \neq 1, \\ \varphi(n), & \text{pokud } b = 1. \end{cases}$$

Povšimněme si, že části a) a b) tohoto lemmatu dávají vlastně doplňkové vlastnosti: část a) určuje, jak dopadne součet všech různých hodnot daného charakteru, zatímco část b) udává, co se stane, když tutéž hodnotu dosadíme do všech možných charakterů a výsledky sečteme.

Cvičení. Ověřte, že tyto vzorce fungují na příkladě charakterů modulo 5 uvedených výše.

Důkaz. a) Pokud je χ netriviální, existuje nějaké $c \in \mathbb{Z}_n^*$ takové, že $\chi(c) \neq 1$. Pak máme $\mathbb{Z}_n^* = \{ac \mid a \in \mathbb{Z}_n^*\}$, a tedy se rovnají množiny hodnot

$$\{\chi(a) \mid a \in \mathbb{Z}_n^*\} = \{\chi(ac) \mid a \in \mathbb{Z}_n^*\}.$$

Tedy tyto množiny mají i stejné součty

$$\sum \chi(a) = \sum \chi(ac) = \chi(c) \sum \chi(a),$$

takže

$$(\chi(c) - 1) \sum \chi(a) = 0, \text{ a tudíž konečně } \sum \chi(a) = 0.$$

Pro triviální charakter ε zřejmě máme $\sum \varepsilon(a) = \sum 1 = \varphi(n)$, protože v obou sumách sčítáme přes právě $\varphi(n)$ prvků $\mathbb{Z}_n^*$.

b) Tuto část dokážeme jen pokud $n = p$ je prvočíslo.
Pokud $b \neq 1$, pak charakter χ_1 splňuje, že $\chi_1(b) \neq 1$ (cvičení).
Tedy podobně jako v části a) máme

$$\sum_{\chi \in X(\mathbb{Z}_p^*)} \chi(b) = \sum_{\chi \in X(\mathbb{Z}_p^*)} (\chi\chi_1)(b) = \chi_1(b) \sum_{\chi \in X(\mathbb{Z}_p^*)} \chi(b),$$

což opět implikuje $\sum_{\chi\in X(\mathbb{Z}_p^*)}\chi(b)=0$, protože $\chi_1(b)\neq 1$.

Konečně $\sum_{\chi\in X(\mathbb{Z}_p^*)}\chi(1)=\sum_{\chi\in X(\mathbb{Z}_p^*)}1=|X(\mathbb{Z}_p^*)|=p-1$ díky lemmatu 4.6. □

Poznámka. Využili jsme obecného pozorování, že je-li G grupa a $g_0\in G$, pak $\{g\in G\}=\{gg_0\mid g\in G\}$.
Například takto taky $\sum_{a\in\mathbb{Z}_n}\zeta_n^a=0$, protože $\sum\zeta_n^a=\sum\zeta_n^{a+1}=\zeta_n\sum\zeta_n^a$.

4.3 Gaussovy součty

Definice. Ať $\chi\in X(\mathbb{Z}_n^*)$ je charakter modulo n. *Gaussův součet* charakteru χ je

$$g(\chi)=\sum_{a\in\mathbb{Z}_n^*}\chi(a)\zeta_n^a,\ \text{kde } \zeta_n=e^{\frac{2\pi i}{n}}.$$

Všimněme si, že dává smysl sčítat přes $\mathbb{Z}_n^*$, čili že pokud $a\equiv b\pmod n$, pak také $\chi(a)\zeta_n^a=\chi(b)\zeta_n^b$ (protože $\zeta_n^n=1$ a χ je charakter modulo n).

Pokud $n=p$ je prvočíslo, pak

$$g(\varepsilon)=\sum_{a\in\mathbb{Z}_p^*}\zeta_p^a=\left(\sum_{a\in\mathbb{Z}_p}\zeta_p^a\right)-\zeta_p^0=0-1=-1.$$

Tvrzení 4.8. *Buď χ netriviální charakter modulo prvočíslo p. Pak $|g(\chi)|=\sqrt{p}$.*

Důkaz. Chceme dokázat, že $g(\chi)\cdot\overline{g(\chi)}=p$.
Pro $y\in\mathbb{Z}_p^*$ máme $\overline{\chi(y)}=\chi(y^{-1})$ a $\overline{\zeta_p^y}=\zeta_p^{-y}$, takže

$$g(\chi)\overline{g(\chi)}=\left(\sum_x\chi(x)\zeta_p^x\right)\cdot\left(\sum_y\chi(y^{-1})\zeta_p^{-y}\right)=\sum_{x,y}\chi(xy^{-1})\zeta_p^{x-y},$$

kde sčítáme přes uspořádané dvojice $(x,y)\in\mathbb{Z}_p^*\times\mathbb{Z}_p^*$. Abychom tento součet spočítali, uděláme vhodnou substituci.
Buď $z=xy^{-1}$, čili $x=zy$.
Máme $(x,y)\in\mathbb{Z}_p^*\times\mathbb{Z}_p^*$, právě když $(xy^{-1},y)\in\mathbb{Z}_p^*\times\mathbb{Z}_p^*$. Tedy můžeme sčítat přes dvojice (z,y):

$$g(\chi)\overline{g(\chi)}=\sum_{(z,y)\in\mathbb{Z}_p^*\times\mathbb{Z}_p^*}\chi(z)\zeta_p^{y(z-1)}=\sum_{z\in\mathbb{Z}_p^*}\left(\chi(z)\cdot\sum_{y\in\mathbb{Z}_p^*}\zeta_p^{y(z-1)}\right)=\heartsuit.$$

Máme dvě možnosti pro hodnotu vnitřní sumy:
a) $z=1$. Pak $\zeta_p^{y(z-1)}=\zeta_p^0=1$ pro všechna y. Zároveň $\chi(1)=1$, takže dostaneme

$$1\cdot\sum_{y\in\mathbb{Z}_p^*}1=p-1.$$

b) $z\neq 1$. Pak $z-1$ je invertibilní modulo p, takže $\{y(z-1)\pmod p\mid y\in\mathbb{Z}_p^*\}=\mathbb{Z}_p^*$. Tudíž příslušný člen v závorce ve ♡ je

$$\chi(z)\cdot\sum_{a\in\mathbb{Z}_p^*}\zeta_p^a=\chi(z)\cdot(-1)=-\chi(z).$$

Dohromady dostáváme

$$\heartsuit = p - 1 - \sum_{z \neq 1} \chi(z) = p - 1 - (-1) = p,$$

protože $\sum_{z \in \mathbb{Z}_p} \chi(z) = 0$. □

Připomeňme, že Legendreův symbol $\left(\frac{a}{p}\right)$ dává charakter

$$\chi : \mathbb{Z}_p^* \to \{\pm 1\} \subset \mathbb{C}^*$$
$$a \mapsto \chi(a) = \left(\frac{a}{p}\right)$$

Tvrzení 4.7 pak například implikuje (pro liché prvočíslo p), že $\sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) = 0$ (což je ale jasné, protože zbytků je stejně jako nezbytků).

Definice. Buď p liché prvočíslo. *Kvadratický Gaussův součet* je

$$S := \sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right) \zeta_p^a.$$

Jedná se tedy o Gaussův součet odpovídající charakteru $\left(\frac{\cdot}{p}\right)$.

Lemma 4.9. *Buď p liché prvočíslo. Pak $S = i^{\frac{p-1}{2}} \cdot r$ pro $r = \pm\sqrt{p}$.*

Je dobré si rozmyslet, co lemma říká v závislosti na $p \pmod 4$:
Pokud $p \equiv 1 \pmod 4$, pak $\frac{p-1}{2}$ je sudé, čili $i^{\frac{p-1}{2}} = \pm 1$ a lemma říká, že $S \in \mathbb{R}$.
Naopak pokud $p \equiv 3 \pmod 4$, pak $S \in i\mathbb{R}$ leží na imaginární ose.

Důkaz. Rozlišíme dva případy podle $p \pmod 4$.
a) $p \equiv 1 \pmod 4$. Pak $\left(\frac{-1}{p}\right) = 1$ podle tvrzení 4.4, a tedy $\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right)$ a

$$\left(\frac{a}{p}\right) \zeta_p^a + \left(\frac{-a}{p}\right) \zeta_p^{-a} = \left(\frac{a}{p}\right) \cdot (\zeta_p^a + \zeta_p^{-a}) \in \mathbb{R},$$

protože ζ_p^{-a} je komplexně sdružené číslo k ζ_p^a.
S je součet takovýchto výrazů pro $a = 1, \ldots, \frac{p-1}{2}$, takže $S \in \mathbb{R}$, což sedí s tím, že $\frac{p-1}{2}$ je sudé, čili $i^{\frac{p-1}{2}} \in \mathbb{R}$.
b) $p \equiv 3 \pmod 4$. Podobně máme $\left(\frac{-1}{p}\right) = -1$. Teď

$$\left(\frac{a}{p}\right) \zeta_p^a + \left(\frac{-a}{p}\right) \zeta_p^{-a} = \left(\frac{a}{p}\right) \cdot (\zeta_p^a - \zeta_p^{-a}) \in i\mathbb{R}.$$

Toto opět platí pro všechna a, takže $S \in i\mathbb{R}$, což sedí.

Konečně v obou případech díky tvrzení 4.8 víme, že $|S| = \sqrt{p}$, tedy máme $|r| = \sqrt{p}$. □

Důsledek 4.10. *Buď p liché prvočíslo. Pak $S^2 = \left(\frac{-1}{p}\right) \cdot p$.*

Důkaz. Podle lemmatu 4.9 máme $S^2 = (-1)^{\frac{p-1}{2}} \cdot r^2 = \left(\frac{-1}{p}\right) \cdot p.$ □

Toto je obdoba vztahu $2 = -i \cdot (1+i)^2$ z důkazu tvrzení 4.4.
Dokonce se dá přímo určit i S: Platí

$$S = \begin{cases} \sqrt{p}, & \text{pokud } p \equiv 1 \pmod 4 \\ i\sqrt{p}, & \text{pokud } p \equiv 3 \pmod 4 \end{cases}$$

(zatímco my toto víme v obou případech až na $\pm$).

4.4 Zákon reciprocity

Už se konečně můžeme pustit do důkazu zákona reciprocity.

Věta 4.11 (Kvadratická reciprocita)**.** *Buďte p, q různá lichá prvočísla. Potom*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

K důkazu potřebujeme pracovat v okruhu

$$R = \mathbb{Z}[\zeta_p] := \left\{ \sum_{j=0}^{N} a_j \zeta_p^j \mid N \in \mathbb{N}_0, a_j \in \mathbb{Z} \right\},$$

kde stejně jako v celé sekci je p liché prvočíslo a $\zeta_p = e^{2\pi i/p}$.

Tvrzení 4.12. *Máme*

$$R = \mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \mid a_j \in \mathbb{Z}\}$$

a

$$a_0 + \cdots + a_{p-2}\zeta_p^{p-2} = 0 \Leftrightarrow a_0 = \cdots = a_{p-2} = 0.$$

Důkaz. Platí $\zeta_p^{p-1} = -\zeta_p^{p-2} - \ldots - \zeta_p - 1$, a tedy pro $j \geq p-1$ máme $\zeta_p^j = -\zeta_p^{j-1} - \ldots - \zeta_p^{j-(p-1)}$. Každý výraz $\sum_{j=0}^{N} a_j\zeta_p^j$ jde tedy postupně přepsat tak, že zmizí všechny členy ζ_p^j pro $j \geq p-1$.

Ať $a_0 + \cdots + a_{p-2}\zeta_p^{p-2} = 0$. Tedy polynom $A(x) := a_0 + a_1x + \cdots + a_{p-2}x^{p-2}$ má kořen ζ_p. Podle lemmatu 3.4 je cyklotomický polynom $t_p(x) = x^{p-1} + \cdots + x + 1$ ireducibilní a má také kořen ζ_p.
Tedy $NSD_{\mathbb{Q}[x]}(A(x), t_p(x)) = t_p(x)$ (protože tyto polynomy nejsou nesoudělné a $NSD \mid t_p$). To znamená, že $t_p(x) \mid A(x)$, ale stupeň t_p je větší než stupeň A. Takže musí jít o nulový násobek $A(x) = 0 \cdot t_p(x) = 0$. □

Definice. Podobně jako v důkazu tvrzení 4.4 budeme potřebovat počítat modulo ωR, kdy pro $\alpha, \beta \in R$ říkáme, že $\alpha \equiv \beta \pmod{\omega R}$, pokud ω dělí $\alpha - \beta$ v R, čili $\exists \gamma \in R : \alpha - \beta = \omega\gamma$ (neboli $\alpha - \beta \in \omega R$, proto značení).

Důsledek 4.13. *Mějme $a, b, n \in \mathbb{Z}, n > 0$. Pak $a \equiv b \pmod{n\mathbb{Z}}$, právě když $a \equiv b \pmod{nR}$.*

Důkaz. „⇒“ Máme $a - b = nc$ pro nějaké $c \in \mathbb{Z}$. Zároveň taky $c \in R$, takže $a \equiv b \pmod{nR}$.

„⇐“ Ať $a - b = n\gamma$ pro nějaké $\gamma \in R, \gamma = a_0 + \cdots + a_{p-2}\zeta_p^{p-2}$. Tedy

$$(na_0 - a + b) + na_1\zeta_p + \cdots + na_{p-2}\zeta_p^{p-2} = 0,$$

přičemž všechny koeficienty jsou zjevně v $\mathbb{Z}$. Podle tvrzení 4.12 jsou tedy všechny koeficienty rovné 0, takže speciálně $na_0 - a + b = 0$.
Máme tedy $a - b = na_0$, kde $a_0 \in \mathbb{Z}$, čili $a \equiv b \pmod{n\mathbb{Z}}$, jak jsme chtěli. □

Už se konečné můžeme pustit do důkazu kvadratické reciprocity!

Důkaz věty 4.11. Uvažujme kvadratický Gaussův součet

$$S = \sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right) \cdot \zeta_p^a.$$

Spočítáme S^q modulo qR dvěma způsoby:
a) Máme $S^q = S \cdot S^{q-1}$ a dále

$$S^{q-1} = \left(S^2\right)^{\frac{q-1}{2}} \overset{4.10}{=} \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \overset{4.4}{=} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}}.$$

Podle věty 4.1 máme $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q\mathbb{Z}}$. Tato kongruence tedy také platí modulo qR podle důsledku 4.13. Dohromady dostáváme

$$S^q \equiv S \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{qR}.$$

b) Po roznásobení $(x_1 + \cdots + x_k)^q$ jsou všechny koeficienty, vyjma těch u x_i^q, dělitelné q, jak se dokáže indukcí z binomické věty (cvičení). Tedy mod qR máme:

$$\begin{aligned} S^q &= \left(\sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right) \zeta_p^a\right)^q \equiv \sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right)^q \zeta_p^{aq} \overset{q \text{ liché}}{=} \sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right) \zeta_p^{aq} = \sum_{a \in \mathbb{Z}_p^*} \left(\frac{aq^2}{p}\right) \zeta_p^{aq} \\ &= \left(\frac{q}{p}\right) \cdot \sum_{a \in \mathbb{Z}_p^*} \left(\frac{aq}{p}\right) \zeta_p^{aq} \overset{b=aq}{=} \left(\frac{q}{p}\right) \cdot \sum_{b \in \mathbb{Z}_p^*} \left(\frac{b}{p}\right) \zeta_p^b = \left(\frac{q}{p}\right) \cdot S \pmod{qR}. \end{aligned}$$

Porovnáním a) a b) vidíme, že

$$uS \equiv 0 \pmod{qR}, \text{ kde } u := (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) - \left(\frac{q}{p}\right).$$

Zřejmě $u = 0, 2, -2$, protože jde o rozdíl dvou čísel, jež jsou obě ± 1.
My chceme dokázat, že $u = 0$, ať tedy pro spor $u = \pm 2$.

Pak $2S \equiv 0 \pmod{qR}$. Prvočíslo $q = 2k + 1$ je liché, takže

$$S \equiv -2k \cdot S = -k \cdot (2S) \equiv 0 \pmod{qR}.$$

Využitím důsledku 4.10 pak máme $\left(\frac{-1}{p}\right) \cdot p = S^2 \equiv S \cdot 0 = 0 \pmod{qR}$, takže $p \equiv 0 \pmod{qR}$. Důsledek 4.13 pak implikuje $p \equiv 0 \pmod{q\mathbb{Z}}$, což je spor.

Tedy $u = 0$ a věta je dokázaná. □

4.5 Jacobiho symbol

Zákon kvadratické reciprocity se využívá k výpočtu Legendreova symbolu $\left(\frac{a}{p}\right)$, kde můžeme předpokládat $a < p$. Abychom mohli použít reciprocitu, buď $a = p_1^{e_1} \cdots p_k^{e_k}$ je prvočíselný rozklad a.
Pak podle důsledku 4.2 máme

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right)^{e_1} \cdots \left(\frac{p_k}{p}\right)^{e_k},$$

stačí tedy určit $\left(\frac{p_i}{p}\right)$. Je-li nějaké z prvočísel 2, použijeme tvrzení 4.4.

Pro liché prvočíslo p_i příslušný člen pomocí reciprocity převedeme na výpočet $\left(\frac{p}{p_i}\right) = \left(\frac{p \mod p_i}{p_i}\right)$, čímž si pomůžeme, protože $p_i < a < p$.
Opět můžeme $b := p \mod p_i$ rozložit na prvočísla atd. Postupně se čísla snižují, takže časem skončíme a dostaneme výsledek.

Tento postup funguje, ale má dva problémy:
Jednak se nám potenciálně výpočet hodně větví a narůstá počet případů, které uvažujeme. Ale zejména je potřeba rozkládat na součin prvočísel, což je výpočetně velmi náročné!

Hodilo by se tedy postup vylepšit tak, aby nevyžadoval rozklad na prvočísla (čímž by se zároveň vyřešil i první z problémů). To je možné pomocí Jacobiho symbolu.

Definice. Mějme celé číslo a a *liché* přirozené číslo n. *Jacobiho symbol* $\left(\frac{a}{n}\right)$ definujeme jako

$$\left(\frac{a}{n}\right) = \left(\frac{a}{q_1}\right) \cdots \left(\frac{a}{q_k}\right),$$

kde $n = q_1 \cdots q_k$ je součin (ne nutně různých) prvočísel a výrazy na pravé straně jsou Legendreovy symboly.
Také definujeme $\left(\frac{a}{1}\right) = 1$.

Pozor! $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1$, ale $x^2 \equiv 2 \pmod{15}$ nemá řešení.
Hodnota Jacobiho symbolu tedy může být 1 i pokud a je kvadratický nezbytek modulo složené číslo n.

Věta 4.14 (Vlastnosti Jacobiho symbolu)**.** *Mějme celá čísla $a, b \in \mathbb{Z}$ a lichá přirozená $n, m \in \mathbb{N}$. Pak:*
a)

$$\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right), \quad \left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

b)

$$a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

c)

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

d)

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \left(\frac{m}{n}\right)$$

Jacobiho symbol tedy má stejné základní vlastnosti jako Legendreův symbol.

Všimněme si, že díky poslední vlastnosti d) můžeme „převracet“ Jacobiho symboly ve výpočtu bez nutnosti faktorizovat! Potřebujeme jenom umět hledat rozklady tvaru $a = 2^e \cdot b$ pro liché b, což není problém.

Důkaz částí a), b) je jasný. Ke zbytku se nám bude hodit toto lemma:

Lemma 4.15. *Ať jsou $a_1, \dots, a_k$ lichá celá čísla. Pak:*

$$\frac{a_1 - 1}{2} + \cdots + \frac{a_k - 1}{2} \equiv \frac{a_1 \cdots a_k - 1}{2} \pmod 2,$$

$$\frac{a_1^2 - 1}{8} + \cdots + \frac{a_k^2 - 1}{8} \equiv \frac{(a_1 \cdots a_k)^2 - 1}{8} \pmod 8.$$

Důkaz. Cvičení. Dokáže se indukcí podle k, k čemuž je klíčem případ $k = 2$:

$$\frac{a_1 a_2 - 1}{2} - \frac{a_1 - 1}{2} - \frac{a_2 - 1}{2} = \frac{(a_1 - 1)(a_2 - 1)}{2} \equiv 0 \pmod 2,$$

protože $2 \mid a_i - 1$.
Druhý vztah podobně platí díky tomu, že $8 \mid a_i^2 - 1$. □

Důkaz věty 4.14. Ať $n = q_1 \cdots q_k$, kde q_i jsou lichá prvočísla (ne nutně různá).
c)

$$\left(\frac{-1}{n}\right) \overset{\text{def}}{=} \prod \left(\frac{-1}{q_i}\right) \overset{4.4}{=} (-1)^{\frac{q_1-1}{2}+\cdots+\frac{q_k-1}{2}} \overset{4.15}{=} (-1)^{\frac{q_1 \cdots q_k - 1}{2}}.$$

Vzoreček pro $\left(\frac{2}{n}\right)$ se dokáže podobně (cvičení).

d) Ať $m = p_1 \cdots p_l$, kde p_j jsou lichá prvočísla.
Pokud $(n, m) \neq 1$, pak $p_i = q_j$ pro nějaká i, j, a tedy $\left(\frac{n}{m}\right)$ obsahuje $\left(\frac{q_j}{p_i}\right) = 0$ a $\left(\frac{m}{n}\right)$ obsahuje $\left(\frac{p_i}{q_j}\right) = 0$. Obě strany d) se tedy v tomto případě rovnají 0.

Ať dále $(n, m) = 1$. Máme

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right), \left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right).$$

Podle kvadratické reciprocity pro Legendreův symbol 4.11 víme, že

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}}.$$

Tedy

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^s,$$

kde

$$s := \sum_{i,j} \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2} = \left(\sum_i \frac{p_i - 1}{2}\right) \cdot \left(\sum_j \frac{q_j - 1}{2}\right)$$
$$\overset{4.15}{\equiv} \frac{p_1 \cdots p_l - 1}{2} \cdot \frac{q_1 \cdots q_k - 1}{2} = \frac{m - 1}{2} \cdot \frac{n - 1}{2} \pmod 2.$$

Tím jsme tedy dokázali, že

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^s = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

a důkaz je hotov – pokud jsou m, n nesoudělná, Jacobiho symboly jsou ± 1, takže jeden z nich můžeme přehodit na druhou stranu rovnosti. □

4.6 Prvočísla tvaru $a^2 + 2b^2$

Pomocí Legendreových symbolů můžeme rozšířit větu 3.2, která popisovala prvočísla tvaru $a^2 + b^2$.

Tvrzení 4.16. *Buď $p \in \mathbb{N}$ prvočíslo. Pak $p = a^2 + 2b^2$ pro nějaká $a, b \in \mathbb{Z}$, právě když $p = 2$ nebo $p \equiv 1, 3 \pmod 8$.*

Důkaz. Dokážeme jen těžší implikaci zprava doleva (v případě $p \equiv 1, 3 \pmod 8$), tu druhou necháme jako cvičení.
Okruh $\mathbb{Z}\left[\sqrt{-2}\right]$ je eukleidovský, a proto i gaussovský.
Stejně jako v lemmatu 3.1 se dokáže: $p = a^2 + 2b^2$, právě když p není prvočinitel v $\mathbb{Z}\left[\sqrt{-2}\right]$.
Předpokládejme teď pro spor, že $p \equiv 1, 3 \pmod 8$ *je* prvočinitel v $\mathbb{Z}\left[\sqrt{-2}\right]$.
Výpočtem s Legendreovými symboly pro $p \equiv 1, 3 \pmod 8$ dostaneme $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1$ (cvičení).
Tedy existuje x takové, že $x^2 \equiv -2 \pmod p$, čili $p \mid x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$ v $\mathbb{Z}\left[\sqrt{-2}\right]$.
Podle předpokladu je p prvočíslo v $\mathbb{Z}\left[\sqrt{-2}\right]$, takže $p \mid x \pm \sqrt{-2}$. Tedy $x \pm \sqrt{-2} = p \cdot (c + d\sqrt{-2})$, odkud ale porovnáním imaginárních částí dostaneme, že $\pm 1 = pd$, což je spor. □

Poznamenejme, že obecně se kolem zkoumání toho, která prvočísla jsou tvaru $a^2 + nb^2$ pro dané přirozené číslo n rozvinula bohatá teorie. Pro seznámení se s ní doporučuji knížku od Coxe nebo přednášku Kvadratické formy a třídová tělesa I.
David A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Wiley, 1989.
https://is.cuni.cz/studium/predmety/index.php?do=predmet&kod=NMAG455

5. Testování prvočíselnosti

V první části této kapitoly popíšeme obecný princip pravděpodobnostních testů prvočíselnosti a několik konkrétních testů založených na látce z předchozích kapitol.
Ve druhé části kapitoly pak využijeme strukturu $\mathbb{Z}_n^*$ k sestrojení lepšího testu prvočíselnosti.

5.1 Opakování a Fermatův test

Připomeňme, že *Eulerova funkce* $\varphi(n)$ udává počet přirozených čísel k, $1 \leq k \leq n$, jež jsou nesoudělná s n. Platí:

- $\varphi(n) = |\mathbb{Z}_n^*|$.
- $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, kde násobíme přes všechna prvočísla p, která dělí n.
- *Malá Fermatova věta.* $a^{p-1} \equiv 1 \pmod{p}$, pokud je p prvočíslo a $(a, p) = 1$.
- *Eulerova věta.* $a^{\varphi(n)} \equiv 1 \pmod{n}$, pokud $(a, n) = 1$.
- $n = \sum_{d|n} \varphi(d)$, kde sčítáme přes všechna přirozená čísla d, která dělí n.

Fermatův test prvočíselnosti. Buď $a, N \in \mathbb{N}, (N, a) = 1$. Pokud $a^{N-1} \not\equiv 1 \pmod{N}$, pak je N složené.

Existují ale *Carmichaelova čísla*, pro něž $a^{N-1} \equiv 1 \pmod{N}$ platí pro všechna a. Nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ (cvičení).
Fermatův test tedy obecně nefunguje, zanedlouho si ale popíšeme jeho vylepšenou verzi, tzv. Rabin–Millerův test.

5.2 Pravděpodobnostní testy obecně

Napřed si ale popišme obecnou myšlenku pravděpodobnostních testů prvočíselnosti.

Předpokládejme, že máme nějaký efektivní algoritmus $A_a(N)$, který v závislosti na parametru a částečně testuje, jestli je přirozené číslo N prvočíslo.
Výstupem algoritmu je buď „*N je složené*“ nebo „*N je možná prvočíslo*“, a to:

- Pokud N je prvočíslo, pak algoritmus vždy odpoví „*N je možná prvočíslo*“.
- Pokud N je složené, pak algoritmus odpoví „*N je složené*“ s pravděpodobností $\geq \alpha$ (a jinak odpoví „*N je možná prvočíslo*“).

Přičemž α je nějaká fixní pravděpodobnost nezávislá na a ani N, např. $\alpha = 0,5$ nebo $\alpha = 0,1$.

Tedy o prvočíslech algoritmus nikdy nelže, kdežto u složených čísel může dát obě odpovědi (ale pokud odpoví, že N je složené, tak je to pravda).
Pokud byla odpověď „*N je složené*“, pak také říkáme, že a je *svědek složenosti* N; pokud je odpověď „*N je možná prvočíslo*“ (a N je složené), pak a je *lhář*.

Fermatův test, v němž testujeme, jestli $a^{N-1} \equiv 1 \pmod N$, je skoro takovýmto testem – až na to, že pro Carmichaelova čísla žádní svědci neexistují (takže pro ně je pravděpodobnost odhalení složeného čísla $\alpha = 0$).
Poznamenejme, že tento test je efektivní, protože *umocňovat modulo N umíme rychle*. Pro detaily viz kurz Algebry, ale základní myšlenka je založená na tom, že napřed spočítáme hodnoty $a^2 \pmod N$, $a^4 \pmod N$, $a^8 \pmod N, \ldots$ postupným umocňováním na druhou. Číslo n potom vyjádříme ve dvojkové soustavě, takže k výpočtu $a^n \pmod N$ stačí vynásobit příslušné hodnoty $a^{2^j} \pmod N$.
Tyto výpočty navíc jde zrychlit použitím rychlého násobení (např.) založeného na diskrétní Fourierově transformaci.

Mohlo by se zdát, že test s pravděpodobností úspěchu třeba $\alpha = 0,5$ je na nic. Výhodou ale je, že test můžeme opakovat pro různé volby parametru a! Když takto vyzkoušíme 10 různých a (která musí být zvolená náhodně tak, aby příslušné experimenty byly nezávislé), tak hned máme pravděpodobnost odhalení složeného čísla $1 - 0,5^{10} = 0,999$.
Se zvyšujícím počtem opakování testu tedy umíme dostat libovolně velkou pravděpodobnost úspěchu, což pro praktické účely stačí.

5.3 Solovay–Strassenův test prvočíselnosti

Je-li N složené číslo, nemusí platit $\left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod N$ (kdežto pro prvočíslo to platit musí). Obě strany této kongruence umíme rychle počítat (tu levou pomocí kvadratické reciprocity), takže můžeme zkoušet různá a a testovat to, což dává Solovay–Strassenův test prvočíselnosti.
Je-li N složené, tak vždy existuje a, pro které platí $\left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \pmod N$; dokonce většina $a \pmod N$ má tuto vlastnost.
Tento test prvočíselnosti je tedy pravděpodobnostní: pokud najdeme jediný protipříklad na $\left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod N$, tak víme, že N je složené. Naopak pokud vyzkoušíme dost různých a, pak můžeme říct, že N je s vysokou pravděpodobností prvočíslo.

Formálně, pro N přirozené a $(a, N) = 1$,

$$\text{algoritmus } A_a(N) \text{ vrátí } \begin{cases} N \textit{ je složené,} & \text{pokud } \left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \pmod N, \\ N \textit{ je možná prvočíslo,} & \text{pokud } \left(\frac{a}{N}\right) \equiv a^{\frac{N-1}{2}} \pmod N. \end{cases}$$

Přičemž pravděbodnost odhalení složeného čísla $\alpha = 0,5$ (toto je samozřejmě potřeba dokázat, můžete zkusit jako cvičení).

Dokonce za předpokladu platnosti zobecněné Riemannovy hypotézy jde takto sestavit deterministický polynomiální test prvočíselnosti.
Historicky byl tento test poměrně významný, později ho ale zastínil Rabin–Millerův test (viz sekci 5.7).

Pro více detailů o tomto testu viz článek Keitha Conrada nebo bakalářku Sáry Vyhnalové.
https://kconrad.math.uconn.edu/blurbs/ugradnumthy/solovaystrassen.pdf
https://is.cuni.cz/webapps/zzp/detail/209396/

Poznamenejme, že na podobné myšlence je založený také Goldwasser–Micaliho kryptosystém. Jednotlivé bity zprávy jsou v něm kódované pomocí hodnot $a \pmod{pq}$ (pro velká prvočísla p, q) takových, že Jacobiho symbol $\left(\frac{a}{pq}\right) = 1$, přičemž a kóduje 0, pokud je to kvadratický zbytek modulo pq, a 1, pokud jde o nezbytek. Viz například
https://en.wikipedia.org/wiki/Goldwasser%E2%80%93Micali_cryptosystem

5.4 Primitivní prvky

Z algebry už známe:
Primitivní prvky. Buď p prvočíslo. Pak $\mathbb{Z}_p^*(\cdot) \simeq \mathbb{Z}_{p-1}(+)$ je cyklická grupa, libovolný její generátor se nazývá *primitivní prvek*. Jde o speciální případ věty 5.1, jejíž důkaz je níže (ale bere se také na Algebře).

Jak to je se strukturou $\mathbb{Z}_n^*$ pro složené n?

Čínská zbytková věta. $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ jako okruh, kde $n = p_1^{e_1} \cdots p_k^{e_k}$ a izomorfismus je daný zobrazením $a \mapsto (a \pmod{p_1^{e_1}}, \ldots, a \pmod{p_k^{e_k}})$.
Proto $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*$ (cvičení).
Tedy stačí určit strukturu $\mathbb{Z}_{p^e}^*$, což teď uděláme.
Napřed si ale ještě pro úplnost uveďme i důkaz existence primitivních prvků modulo p.

Věta 5.1. *Buď K těleso a G konečná podgrupa multiplikativní grupy $K^*(\cdot)$. Pak je G cyklická.*

Speciálně jde věta použít pro podgrupu $\mathbb{Z}_p^*$ tělesa $\mathbb{Z}_p$.

Důkaz. Buď n řád (= počet prvků) grupy G. Podle Lagrangeovy věty pak řád každého prvku $g \in G$ dělí n. Pro $d \mid n$ buď $\tau(d)$ počet prvků řádu d v G. Zřejmě pak $n = \sum_{d|n} \tau(d)$, kde sčítáme přes všechna přirozená čísla d, která dělí n.
Chceme dokázat, že $\tau(d) \leq \varphi(d)$ pro každé $d \mid n$, protože pak $n = \sum_{d|n} \tau(d) = \sum_{d|n} \varphi(d)$ implikuje, že dokonce $\tau(d) = \varphi(d)$ pro každé $d \mid n$. Každý z $\tau(n) = \varphi(n)$ prvků řádu rovného n pak generuje G.

Pro spor tedy předpokládejme, že $\tau(d) > \varphi(d)$ pro nějaké $d \mid n$. Využijeme toho, že každý prvek řádu d v G je kořenem polynomu $x^d - 1$ nad tělesem K.
Buď g nějaký prvek řádu d. Pak i každý z d prvků cyklické grupy $\{g^i \mid 0 \leq i < d\} \simeq \mathbb{Z}_d$ je kořenem polynomu $x^d - 1$ (neboť $(g^i)^d = (g^d)^i = 1^i = 1$).
Ovšem cyklická grupa $\mathbb{Z}_d$ obsahuje právě $\varphi(d)$ prvků řádu rovného d – jsou to přesně g^i pro $(i, d) = 1$ (cvičení). Protože $\tau(d) > \varphi(d)$, musí v G ležet nějaký prvek h, který má také řád d, ale který *neleží* v $\{g^i \mid 0 \leq i < d\} \simeq \mathbb{Z}_d$.
Dostali jsme, že polynom $x^d - 1$ nad tělesem K má stupeň d, ale aspoň $d + 1$ kořenů, a sice $g^0, g^1, \ldots, g^{d-1}, h$, což je spor. □

5.5 Valuace a mocniny

Pro příští sekci si teď ještě připravíme dvě pomocná tvrzení o valuacích.

Lemma 5.2.
a) $v_p(p^s - a) = v_p(a)$ *pro každé* $s \geq 1, 1 \leq a < p^s$.
b) $v_p\left(\binom{p^s}{k}\right) = s - v_p(k)$ *pro každé* $s \geq 0, 1 \leq k \leq p^s$.

Důkaz.
a) Ať $a = p^j b$, kde $j = v_p(a)$ (tedy $p \nmid b$). Protože $1 \leq a < p^s$, máme $j < s$. Tedy $p^s - a = p^s - p^j b = p^j(p^{s-j} - b)$. Protože $p \nmid p^{s-j} - b$, dostáváme $v_p(p^s - a) = j$.

b) Máme $\binom{p^s}{k} = \frac{p^s(p^s-1)(p^s-2)\ldots(p^s-(k-1))}{1\cdot 2\cdots(k-1)k}$.
Dále podle části a) máme $v_p(p^s - a) = v_p(a)$ pro $a = 1, 2, \ldots, k-1$, takže se nám skoro všechny valuace ve zlomku odečtou:

$$v_p\binom{p^s}{k} = v_p(p^s) + v_p(p^s - 1) \quad + v_p(p^s - 2) + \ldots + v_p(p^s - (k-1))$$
$$- v_p(1) \qquad\qquad - v_p(2) - \ldots - v_p(k-1) - v_p(k) = v_p(p^s) - v_p(k).$$

□

Tvrzení 5.3.
a) Buď p *liché prvočíslo a* $e \geq 2$. *Pak*

$$(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \pmod{p^e}.$$

b) Ať $e \geq 3$. *Pak*

$$5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}.$$

Důkaz.
a) Podle binomické věty máme

$$(1+p)^{p^{e-2}} = 1 + p^{e-2}p + \binom{p^{e-2}}{2}p^2 + \cdots + \binom{p^{e-2}}{p^{e-2}}p^{p^{e-2}}.$$

Chceme: $p^e \mid \binom{p^{e-2}}{k}p^k$ pro $\forall k \geq 2$, protože pak na pravé straně kongruence zůstanou jen první dva členy.
Lemma 5.2b) dává $v_p\left(\binom{p^{e-2}}{k}p^k\right) = e-2-v_p(k)+k$. Aby toto bylo větší než e, potřebujeme $k \geq v_p(k) + 2$.
Ať $k = p^j l, p \nmid l$. Pak $2 + v_p(k) = 2 + j$ a $k \geq p^j$, čili chceme $p^j \geq 2 + j$. To se dokáže snadno indukcí.

b) Dokáže se podobně jako část a) umocněním rozkladu $5 = 1 + 4$: cvičení. □

5.6 Multiplikativní grupa modulo p^e

Buď p prvočíslo a $e \geq 1$. Pak

$$|\mathbb{Z}_{p^e}^*| = \varphi(p^e) = (p-1)p^{e-1}.$$

Zároveň $\mathbb{Z}_p^*(\cdot) \simeq \mathbb{Z}_{p-1}(+)$. Jaká je struktura pro $e \geq 2$?

Budeme často pracovat s řádem prvku g v grupě G. Připomeňme, že tím myslíme nejmenší přirozené číslo m takové, že $g^m = 1$; často ho budeme značit jako $\operatorname{ord} g$.
Také když budeme mluvit o $\mathbb{Z}_n^*$ jako o grupě, myslíme tím vždy multiplikativní grupu $\mathbb{Z}_n^*(\cdot)$. Naopak $\mathbb{Z}_n$ myslíme vždy aditivní grupu $\mathbb{Z}_n(+)$.

Lemma 5.4. *a) Je-li p liché prvočíslo, pak množina*

$$P := \left\{1 + ap \mid 0 \leq a < p^{e-1}\right\} < \mathbb{Z}_{p^e}^*$$

tvoří cyklickou podgrupu $\mathbb{Z}_{p^e}^*$, která má řád p^{e-1} a je generovaná prvkem $1 + p$.
b) $P := \{1 + 4a \mid 0 \leq a < 2^{e-2}\}$ je cyklická podgrupa $\mathbb{Z}_{2^e}^*$ řádu 2^{e-2} generovaná prvkem 5.

Důkaz. a) Máme

$$(1 + ap)(1 + bp) = 1 + (a + b + abp)p = 1 + \left[(a + b + abp) \pmod{p^{e-1}}\right] p \in P,$$

takže P je uzavřené na násobení. P je tedy podgrupa díky následujícímu cvičení; její řád je zřejmě p^{e-1}.
Cvičení (z algebry). Buď $G(\cdot)$ konečná grupa a P její podmnožina, která je uzavřená na násobení. Pak je P podgrupa G.
Prvek $1 + p$ patří do P, takže $\operatorname{ord}(1 + p) \mid p^{e-1}$ podle Lagrangeovy věty. Tvrzení 5.3a) ale říká, že $(1 + p)^{p^{e-2}} \neq 1$ v $\mathbb{Z}_{p^e}^*$. Tedy jediná možnost je $\operatorname{ord}(1 + p) = p^{e-1}$, takže $1 + p$ generuje P.
b) Analogicky. □

Věta 5.5.
a) Je-li p liché prvočíslo a $e \geq 1$, pak

$$\mathbb{Z}_{p^e}^*(\cdot) \simeq \mathbb{Z}_{p-1}(+) \times \mathbb{Z}_{p^{e-1}}(+) \simeq \mathbb{Z}_{(p-1)p^{e-1}}(+)$$

je cyklická grupa.
b) Je-li $e \geq 2$, pak

$$\mathbb{Z}_{2^e}^*(\cdot) \simeq \mathbb{Z}_2(+) \times \mathbb{Z}_{2^{e-2}}(+).$$

Toto není cyklická grupa, pokud $e \geq 3$.

Důkaz. Druhá část je o něco lehčí dokázat, takže s ní začněme.
b) Každý prvek v $\mathbb{Z}_{2^e}^*$ je kongruentní 1 nebo $-1 \pmod 4$, a tedy jde vyjádřit jednoznačně jako

$$\pm 1 \cdot (1 + 4a) \text{ pro nějaké } 0 \leq a < 2^{e-2}.$$

Podle předchozího lemmatu 5.4b) je dále

$$P = \{1 + 4a \mid 0 \leq a < 2^{e-2}\} = \{5^j \mid j = 0, \ldots, 2^{e-2} - 1\} < \mathbb{Z}_{2^e}^*.$$

Tedy každý prvek $\mathbb{Z}_{2^e}^*$ je tvaru $(-1)^i 5^j$ pro jednoznačné $i = 0, 1; j = 0, \ldots, 2^{e-2} - 1$.
Máme tedy zobrazení

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}} &\to \mathbb{Z}_{2^e}^* \\ (i, j) &\mapsto (-1)^i 5^j, \end{aligned}$$

což je bijekce a zřejmě i homomorfismus.
Nejedná se o cyklickou grupu, protože každý prvek $\mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ má řád nejvýše 2^{e-2} (protože $2^{e-2}(i,j) = 0$ v $\mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$).

a) K důkazu první části využijeme následujícího lemmatu; nalezený prvek u bude hrát roli prvku -1 z důkazu předchozí části.

Lemma. *Existuje prvek $u \in \mathbb{Z}_{p^e}^*$ takový, že* $\mathrm{ord}(u) = p - 1$.

Důkaz. Buď $g \in \mathbb{Z}_p^*$ primitivní prvek. Máme surjekci

$$\pi : \mathbb{Z}_{p^e} \to \mathbb{Z}_p; a \mapsto a \pmod p.$$

Buď $v \in \mathbb{Z}_{p^e}$ nějaký vzor g, tedy $\pi(v) = g$. Protože $p \nmid g$, také $p \nmid v$, čili $v \in \mathbb{Z}_{p^e}^*$.
Buď k řád prvku v v $\mathbb{Z}_{p^e}^*$. Pak v $\mathbb{Z}_p^*$ platí $1 = \pi(v^k) = (\pi(v))^k = g^k$. Jelikož g má řád $p-1$, tak $p-1 \mid k$, proto ať $k = (p-1)l$. Pak prvek $u = v^l$ má řád $k/l = p-1$ v $\mathbb{Z}_{p^e}^*$. □

Připomeňme, že podle lemmatu 5.4a)

$$P = \{1 + ap \mid 0 \le a < p^{e-1}\} = \{(1+p)^j \mid 0 \le j < p^{e-1}\}.$$

Uvažujme nyní prvek u^i pro nějaké $i = 1, \dots, p-2$. Tento prvek má řád, který dělí $p-1$ a je ostře větší než 1. Tedy $\mathrm{ord}(u^i)$ není mocninou p, takže $u^i \notin P$.
Podívejme se teď množinu

$$M = \{u^i(1+p)^j \mid i = 0, \dots, p-2; j = 0, \dots, p^{e-1} - 1\} \subseteq \mathbb{Z}_{p^e}^*.$$

Její prvky jsou po dvou různé (cvičení) a jejich počet je $(p-1)p^{e-1} = |\mathbb{Z}_{p^e}^*|$, takže $M = \mathbb{Z}_{p^e}^*$ a každý prvek $\mathbb{Z}_{p^e}^*$ jde jednoznačně vyjádřit jako $u^i(1+p)^j$.
To dává hledaný izomorfismus

$$\begin{aligned} \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}} &\to \mathbb{Z}_{p^e}^* \\ (i,j) &\mapsto u^i(1+p)^j. \end{aligned}$$

Navíc podle čínské zbytkové věty je tato grupa izomorfní $\mathbb{Z}_{(p-1)p^{e-1}}$. □

Důsledek 5.6. *Buď $n \ge 2$. Pak $\mathbb{Z}_n^*$ je cyklická grupa, právě když $n = 2, 4, p^e, 2p^e$ pro liché prvočíslo $p, e \ge 1$.*

Důkaz. Použijte ČZV (cvičení). □

Dále chceme využít strukturu $\mathbb{Z}_n^*$ ke zformulovaní lepšího testu prvočíselnosti, než je ten Fermatův.

5.6* Alternativní důkaz existence primitivních prvků

Tento důkaz sepsal Martin Čech na základě přednášek Andrewa Granvillea (je psán asi o něco stručněji, než jiné důkazy ve skriptech). Tento důkaz nepřednášíme (ani nebude u zkoušky), a to hlavně proto, že sice dokáže existenci primitivních prvků modulo p^e o něco jednodušeji než důkaz v předcházející sekci, ale zase nic neřekne o tom, jak vypadají grupy $\mathbb{Z}_{2^e}^*(\cdot)$. (Na zkouškové písemce ale příslušnou část věty 5.5 samozřejmě můžete dokázat i

takto; stejně tak v početních zkouškových příkladech můžete případně hledat primitivní prvky takto, pokud správně zformulujete tvrzení, která přitom používáte.)

Buď p liché prvočíslo. Ukážeme, že pokud a je primitivní prvek modulo p, pak a nebo $a+p$ je primitivní prvek modulo p^2. Podobný důkaz navíc funguje indukcí i pro libovolnou vyšší mocninu p.
Navíc platí, že pokud a je primitivní prvek modulo p^2, pak a je primitivní prvek modulo p^ℓ pro všechna ℓ.

Primitivní prvek modulo p^2

Buď a primitivní prvek modulo liché prvočíslo p. Ukážeme, že buď a nebo $a+p$ je primitivní prvek modulo p^2.
Jaký může být řád a modulo p^2? Určitě to musí být násobek $p-1$. Navíc $a^{p-1} \equiv 1 + kp \pmod{p^2}$ pro nějaké k.
Pokud $k \neq 0$, pak

$$a^{r(p-1)} \equiv (1+kp)^r \equiv 1 + rkp \pmod{p^2},$$

což může být $\equiv 1$ jenom když $p|r$. Tím pádem pokud $a^{p-1} \not\equiv 1 \pmod{p^2}$, pak už a je primitivní prvek modulo p^2.
Pokud $a^{p-1} \equiv 1 \pmod{p^2}$, tj. řád a modulo p^2 je přesně $p-1$, pak můžeme místo a vzít $a+p$: to je taky primitivní prvek modulo p, takže jeho řád bude násobek $p-1$ a navíc

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)p \equiv 1 + (p-1)p \pmod{p^2},$$

tudíž „nové k“ pro tenhle prvek je $p-1 \not\equiv 0 \pmod{p}$, a jeho řád je tedy podle důkazu nahoře $p(p-1) = \varphi(p^2)$.

Primitivní prvek modulo p^ℓ pro $\ell \geq 3$

Nechť a je primitivní prvek modulo $p^{\ell-1}$. Pak stejně jako nahoře je buď a nebo $a+p$ primitivní prvek modulo p^ℓ.
Řád a modulo p^ℓ je násobek $\varphi(p^{\ell-1})$ a máme

$$a^{\varphi(p^{\ell-1})} \equiv 1 + kp^{\ell-1} \pmod{p^\ell},$$

takže

$$a^{r\cdot\varphi(p^{l-1})} \equiv (1+kp^{\ell-1})^r \equiv 1 + rkp^{\ell-1} \pmod{p^\ell}.$$

Vidíme, že pokud $k \neq 0$ výsledek je $\equiv 1 \pmod{p^\ell}$ jen když $p|r$, tj. řád bude aspoň $p \cdot \varphi(p^{\ell-1}) = \varphi(p^\ell)$.
Pokud $k = 0$, pak můžeme stejně jako nahoře nahradit a za $a + p^{\ell-1}$.

Primitivní prvek modulo p^2 je primitivní prvek modulo p^ℓ pro všechna $\ell \geq 3$

Z důkazu nahoře víme, že a je primitivní prvek modulo p^2, pokud $a^{p-1} \equiv 1 + kp \pmod{p^2}$ pro nějaké $k \neq 0$. Pro takové a máme

$$a^{r(p-1)} \equiv (1+pk)^r \equiv 1 + \sum_{n=1}^{\ell-1} \binom{r}{n} p^n k^n \pmod{p^\ell}.$$

První člen v sumě je rpk a druhý je $r(r-1)p^2k^2/2$, takže mají různou p-valuaci, první člen je navíc $\equiv 0 \pmod{p^\ell}$, právě když $p^{\ell-1}|r$. Tím pádem řád a je aspoň $(p-1)p^{\ell-1} = \varphi(p^\ell)$, takže a je primitivní prvek modulo p^ℓ.

5.7 Rabin-Millerův test

Idea.
Buď $p > 2$ prvočíslo, $a \in \mathbb{Z}$ nesoudělné s p.
MFV: $a^{p-1} \equiv 1 \pmod{p}$.

Ať $p = 2k+1$, čili $(a^k)^2 \equiv 1 \pmod{p}$. Tedy a^k je kořen polynomu x^2-1 nad *tělesem* $\mathbb{Z}_p$. x^2-1 má právě dva kořeny ± 1 (protože jsme nad tělesem), takže $a^k \equiv 1, -1 \pmod{p}$. Pokud je k sudé a $a^k \equiv 1 \pmod{p}$, můžeme pokračovat.

Obecněji: Ať $p - 1 = 2^e m$ pro m liché.
Pak

$$a^{2^e m} \equiv 1 \pmod{p} \Rightarrow a^{2^{e-1}m} \equiv 1, -1 \pmod{p}.$$

Pokud je to -1, tak skončíme. Jinak opět máme $a^{2^{e-1}m} \equiv 1 \pmod{p}$, takže $a^{2^{e-2}m}$ je kořen x^2-1, a tedy $a^{2^{e-2}m} \equiv \pm 1 \pmod{p}$. Takto pokračujeme, dokud nějaké $a^{2^j m} \equiv -1 \pmod{p}$, nebo než dostaneme $a^m \equiv 1 \pmod{p}$. Dokázali jsme tím následující tvrzení:

Tvrzení 5.7. *Buď $p > 2$ prvočíslo, kde $p - 1 = 2^e m$ pro liché m. Pro každé $a \in \mathbb{Z}_p^*$ máme $a^{m2^j} \equiv -1 \pmod{p}$ pro nějaké $0 \le j < e$ nebo $a^m \equiv 1 \pmod{p}$.*

Definice. Buď $N \in \mathbb{N}$ složené liché, $N - 1 = 2^e m, m$ liché. Pokud pro $0 < a < N$ platí, že

$$(\heartsuit) \quad \begin{cases} a^{m2^j} \equiv -1 & \pmod{N} \text{ pro nějaké } 0 \le j < e, \text{ nebo} \\ a^m \equiv 1 & \pmod{N}, \end{cases}$$

nazývá se N *silné pseudoprvočíslo v bázi* a, neboli a je *lhář* pro N.
Naopak, pokud a nesplňuje podmínku ($\heartsuit$), nazývá se a *svědek* složenosti N.

Několik poznámek:

- N je (slabé) pseudoprvočíslo v bázi a, pokud platí MFV, čili $a^{N-1} \equiv 1 \pmod{N}$.
- Pokud je $(a, N) > 1$, pak je a vždy svědek. Těchto soudělných svědků ale může být velmi málo.

Rabin-Millerův test prvočíselnosti spočívá v testování, zda různá čísla a jsou svědci nebo lháři: jakmile najdeme jednoho svědka, tak podle tvrzení 5.7 víme, že N musí být složené.
Formálněji, algoritmus $A_a(N)$ dle sekce 5.2 testuje, zda platí podmínka ($\heartsuit$).
Existují ale svědci vždy (čili je pravděpodobnost $\alpha > 0$)?
Například pro Fermatův test prvočíselnosti v případě Carmichaelových čísel jsou jedinými svědky, pro které platí $a^{N-1} \not\equiv 1 \pmod{N}$, čísla a soudělná s N.
Pro Rabin-Millerův test naštěstí vždy existuje dostatek svědků:

Věta 5.8. *Buď N liché složené číslo. Pak počet $a, 0 < a < N$, takových, že N je silné pseudoprvočíslo v bázi a, je menší než $\frac{N}{2}$. Tedy existuje alespoň $\frac{N}{2}$ svědků.*

Tuto větu si dokážeme v sekci 5.9 poté, co napřed vybudujeme teorii kolem míjení involucí.

Stačí tedy testovat dostatečně mnoho různých (nezávislých) hodnot a. Otestujeme-li:

- 1 hodnotu ... pravděpodobnost(lhář)$< \frac{1}{2}$;
- 2 hodnoty ... pravděpodobnost(oba lháři)$< \frac{1}{4}$;
- $\vdots$
- k hodnot ... pravděpodobnost(všichni lháři)$< \frac{1}{2^k}$.

Dokonce sa dá dokázat, že počet lhářů je $< \frac{N}{4}$, viz skripta Aleše Drápala [Dr, sekce 2.13] – je to jen trochu techničtější.
Pomocí Bayesovy věty se pak dá i odhadnout, že pokud číslo N Rabin-Millerovým testem k-krát úspěšně prošlo, pak je N prvočíslo s pravděpodobností větší než $1 - \frac{\log N - 1}{4^k}$.

5.8 Míjení involucí

Půjde o technický nástroj užitečný k důkazu správnosti Rabin-Millerova testu.

Definice. Buď $G(\cdot)$ grupa, $a, b \in G$. Prvek a *míjí* prvek b, pokud $a^i \neq b$ a $b^i \neq a$ pro všechna $i \in \mathbb{Z}$, čili $b \notin \langle a \rangle$ a $a \notin \langle b \rangle$.

Zřejmě a míjí b, právě když b míjí a (jde tedy o symetrickou relaci, jež ale např. není tranzitivní ani reflexivní).
Jako první rozcvičku si rozmysleme toto lemma (které se nám později bude hodit).

Lemma 5.9. *Mějme grupu $G = A \times B$, kde A, B jsou konečné grupy, a její prvek $(e, f) \in G$.*
Jestliže počet prvků $a \in A$, jež míjí e, je aspoň $\alpha \cdot |A|$ (pro nějaké $\alpha \in \mathbb{R}$), pak počet prvků $g \in G$, jež míjí (e, f), je aspoň $\alpha \cdot |G|$.

Důkaz. Máme $|G| = |A| \cdot |B|$ a stačí si uvědomit, že pokud a míjí e, pak (a, b) míjí (e, f) pro všechna $b \in B$. □

Definice. Buď $G(\cdot)$ grupa. Prvek $a \in G$ je involuce, pokud má řád 2, čili $a \neq 1$ a $a^2 = 1$.

Příklad. $\mathbb{Z}_{2^k}(+)$ má právě jednu involuci, a to prvek 2^{k-1}.

Poznámka. Je-li e involuce, pak a míjí e, právě když $a \neq 1$ a $e \neq a^i$ pro všechna $i \in \mathbb{Z}$.

Lemma 5.10. *Buď $G = G_1 \times \cdots \times G_k$. Řád prvku $a = (a_1, \ldots, a_k)$ v G je roven nejmenšímu společnému násobku řádů prvků a_1 v G_1, a_2 v G_2,..., a_k v G_k.*

Důkaz. Ať d_i je řád a_i v grupě G_i a d je řád prvku a v grupě G. Buď $n = \mathrm{nsn}(d_1, \ldots, d_k)$. Pak $a_i^n = 1$ pro každé i, a tedy $a^n = 1$. Tedy $d \mid n$, protože d je řád prvku a v G.
Naopak, pokud $a^d = 1$, pak $a_i^d = 1$ pro každé i, takže $d_i \mid d$ pro každé i, tedy $n \mid d$. Dohromady dostáváme $d = n$. □

Důsledek 5.11. *Buď p prvočíslo a $k_1, \ldots, k_r$ přirozená čísla.*
Prvek $a = (a_1, \ldots, a_r) \in \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_r}}$ má řád p^s, kde

$$s = \max\left(k_1 - v_p^*(a_1), \ldots, k_r - v_p^*(a_r)\right).$$

Tady pro $c \in \mathbb{Z}_{p^k}$ používáme upravené značení:

- *$v_p^*(c) := v_p(c)$ je exponent p v prvočíselném rozkladu čísla $c \in \{1, 2, \ldots, p^k - 1\}$,*

- $v_p^*(0) := v_p(p^k) = k$.

Připomeňme, že $v_p(a)$ je exponent p v prvočíselném rozkladu čísla $a \in \mathbb{Z}$, kdežto v důsledku jsme potřebovali pracovat s valuacemi prvků $\mathbb{Z}_{p^k}$.
Naštěstí platí

Cvičení. Pro $a, b \not\equiv 0 \pmod{p^k}$ platí
a) $a \equiv b \pmod{p^k} \Rightarrow v_p(a) = v_p(b)$,
b) $v_p^*(ab) = \min(v_p^*(a) + v_p^*(b), k)$.

Důkaz důsledku 5.11. Klíčem je dokázat důsledek v případě $r = 1$.
Prvek $a = 0$ má řád $1 = p^0$, což sedí s tím, co chceme dokázat.
Mějme prvek $0 \neq a \in \mathbb{Z}_{p^k}$; ať $a = p^v b$, kde $v = v_p^*(a)$ a $p \nmid b$. Pak se ověří, že řád prvku a v $\mathbb{Z}_{p^k}$ je rovný p^{k-v} (cvičení).
Pro $r > 1$ pak podle lemmatu 5.10 a případu $r = 1$ víme, že řád a se rovná

$$\operatorname{nsn}\left(p^{k_1 - v_p^*(a_1)}, \ldots, p^{k_r - v_p^*(a_r)}\right) = p^s. \qquad \square$$

Tvrzení 5.12. *Mějme přirozená čísla $k_1, k_2, \ldots, k_r$, kde $r \geq 2$.*
Prvek $e = (2^{k_1 - 1}, \ldots, 2^{k_r - 1})$ je involuce v aditivní grupě $G = \mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}$.
Počet prvků $a \in G$, které míjí e, je aspoň $\frac{1}{2}|G|$.

Důkaz. $e \neq 0$ a $2e = (2^{k_1}, \ldots, 2^{k_r}) = 0$, takže e opravdu je involuce.

Ať $a = (a_1, \ldots, a_r) \in G$.
Dokažme napřed, že

$$a \text{ nemíjí } e \Leftrightarrow \operatorname{ord}(a_i) \text{ je stejný pro všechna } i.$$

Pro $a = 0$ tato ekvivalence platí; dále ať $a \neq 0$.
„$\Rightarrow$“ Ať

$$ma = (ma_1, \ldots, ma_r) = e.$$

Ať $m = 2^j s$, kde $2 \nmid s$ (čili $j = v_2(m)$).
Prvek $s2^j a_i = 2^{k_i - 1}$ pak má řád 2 v $\mathbb{Z}_{2^{k_i}}$. Důsledek 5.11 aplikovaný na tento prvek (a $r = 1$) dává $2 = 2^1$, tedy $1 = k_i - v_2(s2^j a_i)$.
Odtud vidíme, že $v_2(a_i) = k_i - j - 1$, takže opět podle důsledku je řád $\operatorname{ord}(a_i) = 2^{j+1}$.
Tedy všechny prvky a_i opravdu mají v $\mathbb{Z}_{2^{k_i}}$ stejné řády 2^{j+1}.

„$\Leftarrow$“ Pokud $\operatorname{ord}(a_i) = 2^h$ pro všechna i, pak $m := 2^{h-1}$ splňuje, že $ma = (ma_1, \ldots, ma_r) = e$ (protože ma_i pak má řád 2 v $\mathbb{Z}_{2^{k_i}}$ a jediný takový prvek je $2^{k_i - 1}$).

Dokázali jsme, že

$$a \text{ míjí } e \Leftrightarrow \operatorname{ord}(a_i) \neq \operatorname{ord}(a_j) \text{ pro nějaké } i \neq j.$$

Nyní potřebujeme udělat dolní odhad na počet takovýchto prvků pro $r = 2$, přičemž rozlišíme dva případy:
a) $k_1 = k_2 = k$. Pokud a je liché, pak má řád 2^k, zatímco sudé b má řád $\leq 2^{k-1}$. Tedy (a, b) i (b, a) míjí e. Takovýchto dvojic je

$$\underset{\text{liché}}{2^{k-1}} \cdot \underset{\text{sudé}}{2^{k-1}} + \underset{\text{sudé}}{2^{k-1}} \cdot \underset{\text{liché}}{2^{k-1}} = 2^{2k-1} = \frac{1}{2} 2^{2k} = \frac{1}{2}|G|.$$

b) $k_1 \neq k_2$, přičemž búno předpokládejme $k_1 > k_2$.
Pokud je $a \in \mathbb{Z}^*_{2^{k_1}}$ (čili a je liché), má řád 2^{k_1}, ale každý prvek $b \in \mathbb{Z}_{2^{k_2}}$ má řád $\leq 2^{k_2} < 2^{k_1}$.
Tedy všechny prvky $\{(a,b) \mid a \in \mathbb{Z}^*_{2^{k_1}}, b \in \mathbb{Z}_{2^{k_2}}\}$ míjí e a je jich $2^{k_1-1}2^{k_2} = \frac{|G|}{2}$.

Ať $r \geq 3$. Stačí volit $A = \mathbb{Z}_{2^{k_1}} \times \mathbb{Z}_{2^{k_2}}, B = \mathbb{Z}_{2^{k_3}} \times \cdots \times \mathbb{Z}_{2^{k_r}}$ a použít lemma 5.9. □

5.9 Počet Rabin-Millerových lhářů

Nyní se můžeme vrátit k Rabin-Millerovu testu. V důkazu klíčové věty 5.8 přitom použijeme jak míjení involucí, tak struktury multiplikativních grup $\mathbb{Z}^*_N$.

Cvičení. Argument s $x^2 \equiv 1 \pmod p$ v sekci 5.7 dokázal, že -1 je jediná involuce v $\mathbb{Z}^*_p(\cdot)$. Dokaž to pomocí $\mathbb{Z}^*_p(\cdot) \simeq \mathbb{Z}_{2^e} \times \mathbb{Z}_m(+)$, kde $p - 1 = 2^e m$ pro liché m.

Důkaz věty 5.8. Ať $N - 1 = 2^e m, 2 \nmid m$.
Je-li $0 < a < N$ lhář, pak nutně $a^{2^e m} \equiv 1 \pmod N$. Tedy $a \in \mathbb{Z}_N$ *není* lhář (čili je svědek), pokud
A) a není invertibilní, to jest $a \notin \mathbb{Z}^*_N$, nebo
B) $a \in \mathbb{Z}^*_N$ má řád, který nedělí $2^e m$.
Rozlišme dva hlavní případy:

1. N **není bezčtvercové**, neboli $k = v_p(N) \geq 2$ pro nějaké prvočíslo p (nutně liché). Tedy $N = p^k s, p \nmid s$. Podle ČZV máme

$$\mathbb{Z}_N \simeq \mathbb{Z}_{p^k} \times \mathbb{Z}_s \quad \text{a} \quad \mathbb{Z}^*_N \simeq \mathbb{Z}^*_{p^k} \times \mathbb{Z}^*_s.$$

Spočteme prvky v jednotlivých případech:

A) V $\mathbb{Z}_{p^k}$ je p^{k-1} neinvertibilních prvků u. Pak (u, v) je neinvertibilní pro libovolné $v \in \mathbb{Z}_s$, takže máme aspoň $p^{k-1}s$ neinvertibilních prvků v $\mathbb{Z}_N$.

B) Pokud p dělí řád prvku $a \in \mathbb{Z}^*_N$, pak a splňuje B), protože $p \nmid 2^e m = N - 1$, takže není možné, aby $p \mid \mathrm{ord}(a) \mid 2^e m$. Pojďme tedy odhadnout počet prvků, jejichž řád je dělitelný p.
Podle věty 5.5 máme

$$\mathbb{Z}^*_{p^k}(\cdot) \simeq \mathbb{Z}_{p^{k-1}}(+) \times \mathbb{Z}_{p-1}(+).$$

V $\mathbb{Z}_{p^{k-1}}(+)$ mají všechny nenulové prvky řád dělitelný p, je jich tedy $p^{k-1} - 1$. Řád je dělitelný p po doplnění čímkoli ze $\mathbb{Z}_{p-1}$ (podle lemmatu 5.10), takže $\mathbb{Z}^*_{p^k}(\cdot)$ má aspoň $(p^{k-1} - 1)(p - 1)$ prvků řádu dělitelného p. Připomeňme, že máme $\mathbb{Z}_N \simeq \mathbb{Z}_{p^k} \times \mathbb{Z}_s$, a pojďme tedy tyto prvky $\mathbb{Z}^*_{p^k}$ doplnit, abychom dostali prvky ze $\mathbb{Z}_N$.
Tyto prvky spolu s čímkoli ze $\mathbb{Z}_s$ buďto

- jsou neinvertibilní $\Rightarrow$ započítáme do A (ale jde o jiné prvky, než předtím) nebo
- jsou invertibilní $\Rightarrow$ splňují B.

Tedy máme aspoň $(p^{k-1} - 1)(p - 1)s$ dalších prvků v $\mathbb{Z}_N$ splňujících A nebo B.

Dohromady to je aspoň

$$sp^{k-1} + (p^{k-1} - 1)(p - 1)s = s(p^k - p + 1)$$

svědků z celkem $p^k s$ prvků. Počet lhářů je tedy $\leq (p-1)s < \frac{p^k s}{2}$ (tento odhad dokaž jako cvičení; nápověda: vlož doprostřed $\frac{p^2 s}{2}$).

2. N **je bezčtvercové**, $N = p_1 \cdots p_r$, kde p_i jsou po 2 různá prvočísla. Dokážeme, že $\mathbb{Z}_N^*$ obsahuje nejvýše $\frac{\varphi(N)}{2}$ lhářů: to stačí, protože prvky mimo $\mathbb{Z}_N^*$ splňují A, takže celkem bude lhářů $\leq \frac{\varphi(N)}{2} < \frac{N}{2}$.
Ať $p_i - 1 = 2^{k_i} m_i, 2 \nmid m_i$. Máme

$$\mathbb{Z}_N^* \simeq \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^* \quad \text{a} \quad \mathbb{Z}_{p_i}^*(\cdot) \simeq \mathbb{Z}_{p_i-1}(+) \simeq \mathbb{Z}_{2^{k_i}}(+) \times \mathbb{Z}_{m_i}(+).$$

Tedy máme izomorfismus

$$\alpha : \mathbb{Z}_N^* \simeq \mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}} \times M, \text{ kde } M = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}.$$

Zajímá nás podmínka $a^{m2^j} \equiv -1 \pmod N$, podívejme se tedy na $\alpha(-1) = \alpha(N-1)$:
První izomorfismus využívající ČZV je daný

$$\begin{aligned} \mathbb{Z}_N^* &\simeq \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p^r}^* \\ t &\mapsto (t \pmod{p_1}, \ldots, t \pmod{p_r}) \end{aligned}$$

V něm tedy $-1 \mapsto (-1, \ldots, -1)$.
Dále uvažujme

$$\mathbb{Z}_{p_i}^* \simeq \mathbb{Z}_{2^{k_i}} \times \mathbb{Z}_{m_i}.$$

-1 má řád 2 v $\mathbb{Z}_{p_i}^*$, a tedy její obraz v $\mathbb{Z}_{2^{k_i}} \times \mathbb{Z}_{m_i}$ má taky řád 2. Ale m_i je liché, takže neexistuje prvek řádu 2 v $\mathbb{Z}_{m_i}$, takže -1 se tam zobrazí na 0, což je prvek řádu 1 (v $\mathbb{Z}_{m_i}$ totiž platí, že $2\varphi(-1) = 0 \Rightarrow \varphi(-1) = 0$).
Aby řád v $\mathbb{Z}_{2^{k_i}} \times \mathbb{Z}_{m_i}$ byl rovný 2, musí se -1 v $\mathbb{Z}_{2^{k_i}}$ zobrazit na prvek řádu 2. Ten je jediný, a sice 2^{k_i-1}. Tedy izomorfismus $\mathbb{Z}_{p_i}^* \simeq \mathbb{Z}_{2^{k_i}} \times \mathbb{Z}_{m_i}$ zobrazí -1 na $(2^{k_i-1}, 0)$.
Dohromady jsme dostali, že

$$\alpha(-1) = (2^{k_1-1}, \ldots, 2^{k_r-1}, 0) =: (u, 0).$$

Vraťme se teď k podmínce $a^{m2^j} \equiv -1 \pmod N$; ať $\alpha(a) = (v, c)$, kde $v \in \mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}, c \in M$.

Pozorování. Pokud v míjí involuci u v $\mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}$, pak a není lhář.

Důkaz. Ať pro spor je a lhář.
a) Pokud $a^m = 1$ pro liché m, pak a má lichý řád. Ale jediný prvek lichého řádu v $\mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}$ je 0, takže $v = 0$.
b) Pokud $a^{m2^j} = -1$, pak máme $\alpha(-1) = (u, 0)$ a $\alpha(a^{m2^j}) = m2^j \alpha(a) = (m2^j v, m2^j c)$. Tedy $u = m2^j v$.
Ani v jednom případě v neminulo u. □

Přesně kvůli tomuto jsme si chystali tvrzení 5.12!
Podle něj víme, že počet prvků v, jež míjí u, je aspoň $\frac{1}{2}|\mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}}|$, takže podle lemmatu 5.9 počet (v, c), jež míjí $(u, 0)$, je aspoň

$$\frac{1}{2}|\mathbb{Z}_{2^{k_1}} \times \cdots \times \mathbb{Z}_{2^{k_r}} \times M| = \frac{1}{2}|\mathbb{Z}_N^*| = \frac{\varphi(N)}{2}.$$ □

6. Příklady

Následují sebrané příklady ze cvičení, domácích úkolů a písemek.
Příklady s ! jsou obzvláště důležité, ty s * jsou těžší (rozhodně ne všechny stejně).

6.1 Základy

1. Dokažte následující tvrzení, nebo najděte protipříklady:
   (a) $a^2|b^2$, právě když $a|b$.
   (b) Pokud $a^2|n$, $b^2|n$ a $a^2 \leq b^2$, pak $a|b$.
   (c) Pokud $NSD(a,b) = 1$, pak $NSD(a^n, b^m) = 1$ pro všechna $m, n \in \mathbb{N}$.
   (d) Pokud $n^n|m^m$, pak $n|m$.
2. Rozhodněte, jestli jsou přirozená čísla a a b jednoznačně určena svým nejmenším společným násobkem a největším společným dělitelem.
3. Nechť A je matice typu 7×7 s prvky $a_{ij} = ij \pmod 7$. Jaký je součet všech prvků matice A?
4. Ukažte, že prvočíslo $p \geq 3$ dělí čitatel zlomku $1 + 1/2 + \cdots + 1/(p-1)$. * Ukažte, že pokud $p \geq 5$, je tento čitatel dělitelný dokonce p^2.
5. * Ukažte, že $n^4 + 4$ nikdy není prvočíslo.
6. * Ukažte, že pro každé n existuje n po sobě jdoucích přirozených čísel, z nichž každé je dělitelné čtvercem nějakého prvočísla.
7. * Ukažte, že pro každé n existuje n po sobě jdoucích složených čísel.

6.2 Eulerova a Malá Fermatova věta

1. Nechť $a \in \mathbb{Z}$. Ukažte, že pokud 17 nedělí a, pak $17|a^{80} - 1$.
2. Buď p prvočíslo. Ukažte, že pokud $p|2^{2^n} + 1$, pak $2^{n+1}|p - 1$.
3. Nechť p, q jsou prvočísla taková, že $p \mid 2^q - 1$. Ukažte, že potom $q \mid p - 1$.
4. Najděte příklad $m, n \in \mathbb{N}$ splňující $\varphi(m) = \varphi(n)$.
5. Nechť p, q jsou dvě různá prvočísla a a přirozené číslo nedělitelné p ani q. Ukažte, že pak $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.
6. Ukažte, že prvočíslo p dělí $ab^p - ba^p$ pro libovolná celá čísla a, b.
7. Pro různá prvočísla p, q ukažte, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
8. * Nechť $p > 3$ je prvočíslo. Ukažte, že potom $p|2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

9. * Najděte všechna n, pro která $\varphi(n)|n$.

6.3 Čínská zbytková věta

1. Řešte následující soustavy kongruencí:
   (a) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$;
   (b) $x \equiv 2 \pmod 4$, $x \equiv 5 \pmod 6$, $x \equiv 1 \pmod 7$;
   (c) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$;
   (d) $x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 1 \pmod 6$;
   (e) $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$;
   (f) $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 6$;
   (g) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 6$.
2. Rozmyslete si verzi Čínské zbytkové věty pro grupy:
   (a) Najděte celočíselné řešení rovnice $3x + 5y = 1$.
   (b) S pomocí předchozí úlohy najděte nějaký izomorfismus $\mathbb{Z}_3 \times \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{15}$.
3. Nechť $a_1, \ldots a_k$ jsou po dvou nesoudělná přirozená čísla. Řešte následující soustavy kongruencí:
   (a) $x \equiv 0 \pmod{a_i}$ pro $i = 1, \ldots, k-1$ a $x \equiv 1 \pmod{a_k}$;
   (b) $x \equiv 1 \pmod{a_i}$ pro $i = 1, \ldots, k-1$ a $x \equiv b \pmod{a_k}$ pro nějaké celé číslo b.
4. * Zformulujte kritérium, kdy má soustava kongruencí řešení i pro soudělné moduly.
5. Ukažte, že platí opačná implikace k Čínské zbytkové věte (pro grupy), t.j. pro soudělná m, n nejsou grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ izomorfní, takže grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ není cyklická. Jde to například takto:
   (a) Ukažte, že součin grup $G \times H$ obsahuje podgrupy izomorfní G, H. (Nápověda: Uvažujte množiny $\{(1, g) : g \in G\}$ resp. $\{(1, h) : h \in H\}$.)
   (b) Ukažte, že pokud jsou m a n soudělná, pak $\mathbb{Z}_m \times \mathbb{Z}_n$ obsahuje dvě různé podgrupy řádu $\mathrm{NSD}(m, n)$, takže nemůže být cyklická.
6. Nechť $n_1, \ldots, n_k$ jsou přirozená čísla. Jaký největší řád může mít prvek grupy $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$? Zamyslete se, jak by toho šlo využít k jinému důkazu tvrzení z předchozí úlohy.

6.4 Cyklické grupy

1. Rozhodněte, zda následující jsou (cyklické) grupy:
   (a) Celá čísla se sčítáním.
   (b) Nenulová celá čísla s násobením.
   (c) Celá čísla dělitelná 7 se sčítáním.

(d) Racionální čísla se sčítáním.

(e) Nenulová racionální čísla s násobením.

(f) Iracionální čísla se sčítáním.

(g) Množina $\{0, 1, \ldots, n-1\}$ se sčítáním modulo n.

(h) Množina $\{1, -1, i, -i\}$ s násobením.

(i) Množina $\{z \in \mathbb{C} : |z| = 1\}$ s násobením.

2. Ukažte, že grupa z příkladu 1. h) je izomorfní se $\mathbb{Z}_4$. * Zobecněte.
3. ! Najděte v $\mathbb{Z}_6$ nenulový prvek, který nemá inverz vzhledem k násobení. * Zobecněte.
4. ! Najděte všechny generátory a podgrupy grupy $\mathbb{Z}_{12}$.
5. ! Určete počet prvků řádu 3 a prvků řádu 13 v grupě $\mathbb{Z}_{260}$.
6. * Dokažte, že každá cyklická grupa je izomorfní $\mathbb{Z}$ nebo $\mathbb{Z}_n$ pro nějaké n.
7. ! Najděte nějaký netriviální homomorfismus následujících grup, nebo ukažte, že žádný neexistuje:

   (a) Ze $\mathbb{Z}_3$ do $\mathbb{Z}_6$.

   (b) Ze $\mathbb{Z}_5$ do $\mathbb{Z}_6$.

   (c) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_8$.

   (d) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_6$.

   (e) Ze $\mathbb{Z}_4$ do $\mathbb{Z}_7$.

8. ! Rozhodněte, zda jsou následující grupy cyklické a pokud ano, najděte v nich primitivní prvek:

   (a) $\mathbb{Z}_{11}^*$,

   (b) $\mathbb{Z}_8^*$.

9. ! Ukažte, že pro libovolné n je grupa $\mathbb{Z}_n$ cyklická.
10. Rozmyslete si následující fakty o generátorech grup $\mathbb{Z}_n$:

    (a) ! Najděte všechny generátory grupy $\mathbb{Z}_{18}$.

    (b) Které prvky $\mathbb{Z}_n$ nemohou generovat celou grupu $\mathbb{Z}_n$?

    (c) Popište všechny generátory grupy $\mathbb{Z}_n$. (Nápověda: Bézoutovy koeficienty)

11. Rozhodněte, zda jsou následující zobrazení homomorfismy grup:

    (a) $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3$, $\varphi(a) = a \bmod 3$

    (b) $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_3$, $\varphi(a) = a \bmod 3$

12. ! Najděte všechny homomorfismy z grupy $\mathbb{Z}_9(+)$ do grupy $\mathbb{Z}_6(+)$.
13. ! Určete řády všech prvků v grupách $\mathbb{Z}_7$ a $\mathbb{Z}_7^*$.
14. Rozhodněte, které z grup $\mathbb{Z}_5^*$, $\mathbb{Z}_6^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{12}^*$ jsou cyklické.
15. ! Najděte prvky $\mathbb{Z}_p^*$, kde p je prvočíslo. Kolik má prvků? Kolik má primitivních prvků?
16. ! Z věty víme, že pro každé prvočíslo p existuje primitivní prvek modulo p.

(a) Najděte nějaký primitivní prvek modulo 3, 5 a 7.

(b) Pomocí části a) sestrojte izomorfizmus grup $\mathbb{Z}_7^*$ a $\mathbb{Z}_6$.

17. Najděte všechny primitivní prvky modulo 7.
18. Víme, že grupa $\mathbb{Z}_p^*$, p prvočíslo, je cyklická, označme nějaký její generátor a.

    (a) Jaký řád má a v grupe $\mathbb{Z}_p^*$?

    (b) Najděte izomorfizmus grupy $\mathbb{Z}_p^*$ a grupy $\mathbb{Z}_{p-1}$. (Nápověda: Generátor a grupy $\mathbb{Z}_p^*$ se musí zobrazit na nějaký generátor grupy $\mathbb{Z}_{p-1}$.)

6.5 Fareyho zlomky

1. **!** Dokažte **Cauchyho větu**: Nechť $\frac{a}{b} < \frac{c}{d}$ jsou sousední položky seznamu F_n. Pak $bc - ad = 1$.
2. **!** Najděte posloupnost Fareyho zlomků řádu 6. Jaké vlastnosti má posloupnost jejich jmenovatelů?
3. Znázorněte graf posloupnosti jmenovatelů Fareyho zlomků řádu n pro $n = 6$ a $n = 10$.
4. **!** Určete počet Fareyho zlomků řádu n.
5. **!** Dokažte, že pro libovolné dva zlomky $\frac{a}{b} < \frac{c}{d}$ je $\frac{c}{d} - \frac{a}{b} \geq \frac{1}{bd}$. Ukažte, že pro sousední Fareyho zlomky nastává rovnost. ***** Platí opačná implikace?
6. Ukažte, že posloupnost jmenovatelů prvků F_n tvoří palindrom.
7. **!** Dokažte mediánovou vlastnost Fareyho zlomků: Nechť $\frac{a}{b} < \frac{c}{d} < \frac{e}{f}$ jsou tři po sobě jdoucí položky seznamu F_n, kde $n \in \mathbb{N}$. Pak $\frac{c}{d} = \frac{a+e}{b+f}$.
8. **!** Pomocí Fareyho zlomků dokažte **Dirichletovu větu**: Nechť $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Pak existuje nekonečně mnoho zlomků $\frac{p}{q}$ takových, že $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.
9. ***** Dokažte, že délka posloupnosti F_n splňuje

$$|F_n| = \frac{1}{2} \cdot \left(3 + \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2\right) = \frac{1}{2}(n+3)n - \sum_{d=2}^{n} |F_{\lfloor \frac{n}{d} \rfloor}|,$$

   kde $\mu(d)$ je Möbiova funkce, která je definovaná pro každé $n \in \mathbb{N}$ následovně:

   - $\mu(n) = \ \ 1$, pokud n je bezčtvercové se sudým počtem prvočíselných dělitelů;
   - $\mu(n) = -1$, pokud n je bezčtvercové s lichým počtem prvočíselných dělitelů;
   - $\mu(n) = \ \ 0$, pokud n je dělitelné druhou mocninou nějakého prvočísla.

6.6 Řetězové zlomky

1. **!** Vyjádřete následující konečné řetězové zlomky jako racionální čísla:

   (a) $[3, 5, 8]$;

   (b) $[1, 2, 3, 4]$;

   (c) $[2, 5, 1, 7]$.

2. **!** Spočtěte řetězové zlomky pro následující racionální čísla:
   (a) $\frac{4}{3}$;
   (b) $\frac{25}{7}$;
   (c) $\frac{415}{93}$;
   (d) $\frac{35}{8}$;
   (e) $\frac{50}{23}$;
   (f) $\frac{34}{43}$.
3. **!** Najděte řetězový zlomek a všechny sblížené zlomky čísla $\frac{87}{38}$.
4. V závislosti na n určete, jakému racionálnímu číslu se rovná zlomek $[0, \overbrace{1, 1, ..., 1}^{n}]$.
5. Rozmyslete si následující rekurentní vztahy pro konečné řetězové zlomky:
   (a) $[a_0, a_1, ..., a_n] = a_0 + [a_1, ..., a_n]^{-1}$;
   (b) $[a_0, a_1, ..., a_n] = \left[a_0, ..., a_{n-1} + \frac{1}{a_n}\right]$;
   (c) $[a_0, a_1, ..., a_n] = \left[a_0, ..., a_{k-1}, [a_k, ..., a_n]\right]$ pro každé $0 < k \leq n$.
6. **!** K zadanému periodickému řetězovému zlomku určete příslušné reálné číslo:
   (a) $\left[2, \overline{5, 3}\right]$;
   (b) $\left[5, \overline{2, 4}\right]$;
   (c) $\left[1, \overline{3, 3}\right]$;
   (d) $\left[1, \overline{6, 9}\right]$;
   (e) $\left[1, \overline{1, 1, 2}\right]$;
   (f) $\left[3, \overline{4, 5}\right]$;
   (g) $[1, \overline{1, 2, 3}]$.
7. **!** Určete řetězové zlomky a první tři sblížené zlomky čísla $\sqrt{n}$ pro $n = 2, 3, 11, 13$.
8. Najděte řetězový zlomek zlatého řezu $\phi = \frac{1+\sqrt{5}}{2}$.
9. **!** Nechť $k \in \mathbb{N}$. Určete, čemu se rovná:
   (a) $\left[k, \overline{1, 2k}\right]$;
   (b) $\left[\overline{k}\right]$;
   (c) $\left[1, \overline{2, k}\right]$;
   (d) $[\overline{k, 2}]$.
10. Najděte n-tý sblížený zlomek ke $\frac{k+\sqrt{k^2+4}}{2}$ pro
    (a) $k = 1$;
    (b) ***** obecné k.
11. Nechť $k \in \mathbb{N}$. Vyjádřete $\sqrt{k^2+1}$ a $\sqrt{k^2-1}$ (pro $k > 1$) jako nekonečné řetězové zlomky.

12. **!** Nechť $k \in \mathbb{N}_0$. Najděte řetězový zlomek čísel
    (a) $\sqrt{k^2+k}$,
    (b) $\frac{\sqrt{4n^2+4n+5}+1}{2}$,
    (c) $\sqrt{9n^2+2n}$.
13. ***** Předpokládajte, že znáte řetězový zlomek pro prvek $\frac{p}{q}$ Fareyho posloupnosti F_q. Vyjádřete pomocí něj řetězové zlomky sousedních prvků.
14. ***** Ukažte, že pokud je řetězový zlomek čísla $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ od jistého místa periodický, pak je α algebraické číslo stupně 2.
15. ***** Pokud $D \in \mathbb{N}$ není čtverec, pak je řetězový zlomek čísla $\sqrt{D}$ od jistého místa periodický (můžete taky zkusit ukázat). Ať $\sqrt{D} = \left[\left\lfloor\sqrt{D}\right\rfloor, \overline{a_1, a_2, \dots a_l}\right]$. Ukažte:
    (a) Pokud $l = 1$, $a_1 = 2 \cdot \left\lfloor\sqrt{D}\right\rfloor$.
    (b) Pokud $l = 2$, $a_2 = 2 \cdot \left\lfloor\sqrt{D}\right\rfloor$.
    (c) Pokud $l = 3$, $a_1 = a_2$ a $a_3 = 2 \cdot \left\lfloor\sqrt{D}\right\rfloor$.
    (d) Pro obecné l ukažte, že platí $a_i = a_{l-i}$ pro $i = 1, \dots l-1$ a $a_l = 2 \cdot \left\lfloor\sqrt{D}\right\rfloor$.

6.7 Pellova rovnice

1. **!** Řešte rovnici $x^2 - 2y^2 = 1$ v $\mathbb{Z}^2$ a najděte alespoň dvě konkrétní řešení (x, y) takové, že $x > 0$, $y > 0$.
2. **!** Ukažte, že následující rovnice nemají v $\mathbb{Z}^2$ řešení:
    (a) $x^2 - 3y^2 = -1$;
    (b) $x^2 - 7y^2 = -1$;
    (c) $x^2 - 7y^2 = -4$.
3. **!**V $\mathbb{Z}^2$ řešte rovnice:
    (a) $x^2 - 3y^2 = 1$;
    (b) $x^2 - 5y^2 = 1$;
    (c) $x^2 - 7y^2 = 1$.
4. Ověřte, že množina všech řešení Pellovy rovnice $x^2 - my^2 = 1$ tvoří grupu.
5. Dokažte, že pokud (x, y) je řešením Pellovy rovnice $x^2 - my^2 = 1$, pak $x + y\sqrt{m} > 1 \iff x, y > 0$.
6. Dokažte, že pokud má řešení Pellova rovnice $x^2 - my^2 = -1$, pak má řešení i rovnice $x^2 - my^2 = 1$.
7. Nechť $B \in \mathbb{Z}$, $m \in \mathbb{N}$, $\sqrt{m} \notin \mathbb{Q}$. Dokažte, že pokud má zobecněná Pellova rovnice $x^2 - my^2 = B$ alespoň jedno řešení, potom má nekonečně mnoho řešení.

8. Najděte alespoň čtyři řešení (x, y), $x > 0$, $y > 0$ rovnice $x^2 - 3y^2 = -2$ v $\mathbb{Z}^2$.
   * Vyřešte tuto rovnici.
9. * Vyřešte rovnici $x^2 - 5y^2 = 2$ v $\mathbb{Z}^2$.

   Věta: Nechť $m \in \mathbb{N}, \sqrt{m} \notin \mathbb{N}$. Nechť $l \in \mathbb{N}$ je minimální takové, že $\sqrt{m} = \left[a_0, \overline{a_1, ..., a_{l-1}, 2a_0}\right]$. Označme $\frac{p_n}{q_n}$ n-tý sblížený zlomek čísla $\sqrt{m}$.

   (a) Pokud je l sudé, tak rovnice $x^2 - my^2 = -1$ nemá řešení $(x, y) \in \mathbb{Z}^2$ a minimální řešení (x, y) rovnice $x^2 - my^2 = 1$ je rovné (p_{l-1}, q_{l-1}).

   (b) Pokud je l liché, tak minimální řešení rovnice $x^2 - my^2 = -1$ je rovné (p_{l-1}, q_{l-1}) a minimální řešení rovnice $x^2 - my^2 = 1$ je rovné (p_{2l-1}, q_{2l-1}). Navíc platí, že $p_{2l-1} + q_{2l-1}\sqrt{m} = (p_{l-1} + q_{l-1}\sqrt{m})^2$.

10. ! V $\mathbb{Z}^2$ řešte rovnice:

    (a) $x^2 - 10y^2 = \pm 1$;

    (b) $x^2 - 41y^2 = \pm 1$;

    (c) $x^2 - 14y^2 = \pm 1$;

    (d) $x^2 - 17y^2 = \pm 1$;

    (e) $x^2 - 23y^2 = \pm 1$;

    (f) $x^2 - 13y^2 = \pm 1$;

    (g) $x^2 - 29y^2 = \pm 1$;

    (h) $x^2 - 61y^2 = \pm 1$.

11. * Buď $m \in \mathbb{N}$, $\sqrt{m} \notin \mathbb{Q}$. Předpokládejme, že rovnice $x^2 - my^2 = -1$ má řešení. Buď $a + b\sqrt{m}$, $a, b > 0$, minimální řešení. Dokažte, že pak $\pm(a + b\sqrt{m})^k$, $k \in \mathbb{Z}$, dává všechna řešení rovnice $x^2 - my^2 = \pm 1$.

6.8 Dobré aproximace

1. ! Určete všechny dobré aproximace čísel

   (a) $\frac{2}{5}$,

   (b) $\frac{5}{3}$,

   (c) $\frac{3}{10}$,

   (d) $\frac{7}{8}$,

   (e) $\frac{24}{7}$,

   (f) $\frac{19}{11}$.

2. ! Najděte řetězový zlomek a všechny sblížené zlomky čísla $\frac{78}{47}$. Určete, které z nich dávají dobré aproximace.
3. Nechť $n \in \mathbb{N}$, $\alpha \in \mathbb{R}$, $\{\alpha\} \neq 0, \frac{1}{2}$, $n > \alpha > 0$. Nechť $\alpha = [a_0, a_1, ...]$ a $n - \alpha = [b_0, b_1, ...]$. Ukažte, že pak platí:

(a) $b_0 = n - a_0 - 1$;

(b) $a_1 = 1 \iff \{\alpha\} \in \left(\frac{1}{2}, 1\right) \iff b_1 \geq 2$;

(c) $\frac{r}{s}$ je dobrá aproximace $\alpha \iff n - \frac{r}{s}$ je dobrá aproximace $n - \alpha$.

4. **!** Určete všechny dobré aproximace čísla $\alpha \in \mathbb{R}$, pokud $\{\alpha\} = 0$, nebo $\{\alpha\} = \frac{1}{2}$.
5. **!** Vyjádřete $\sqrt{10}$ jako nekonečný řetězový zlomek a nalezněte první dvě dobré aproximace tohoto čísla.
6. Nalezněte prvních 5 členů řetězového zlomku $\pi = 3.1415926\ldots$ a prvních 5 jeho dobrých aproximací.
7. Nechť $n > 0$ a nechť $\frac{p_n}{q_n}$ je n-tý sblížený zlomek čísla $\alpha \in \mathbb{R} \setminus \mathbb{Z}$, $\alpha > 0$. Pak každý jiný zlomek $\frac{p}{q}$ s jmenovatelem q, $0 < q \leq q_n$, splňuje, že $\left|\alpha - \frac{p}{q}\right| > \left|\alpha - \frac{p_n}{q_n}\right|$.
8. ***** Ukažte, že jeden z libovolných dvou po sobě jdoucích sblížených zlomků čísla $\alpha > 0$ splňuje $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$.
9. ***** Ukažte, že pokud $\{\alpha\} > \frac{1}{2}$, pak sblížené zlomky $\frac{p_n}{q_n}, n \geq 1$, jsou všechny dobré aproximace α.

6.9 Gaussovská celá čísla

1. **!** Určete, čemu se rovná:

   (a) $\frac{5+i}{3+2i}$;

   (b) $N(4 + 3i)$;

   (c) $\overline{7 - 8i}$.

2. **!** V $\mathbb{Z}[i]$ rozložte na prvočinitele čísla 7 a $5 + i$.
3. **!** Ukažte, že pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ platí $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.
4. **!** Ukažte, že prvek $\alpha \in \mathbb{Z}[i]$ je invertibilní právě tehdy, když $N(\alpha) = 1$. Najděte všechny invertibilné prvky v $\mathbb{Z}[i]$.
5. **!** Ukažte, že pokud je $N(\alpha)$ prvočíslo, pak je α prvočinitel v $\mathbb{Z}[i]$.
6. Nechť $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. Rozhodněte o pravdivosti následujících tvrzení a své tvrzení dokažte.

   (a) Pokud $\alpha \mid \beta$, pak $N(\alpha) \mid N(\beta)$.

   (b) Pokud $N(\alpha) \mid N(\beta)$, pak $\alpha \mid \beta$.

   (c) Pokud $\gamma = \alpha^2 + \beta^2$, pak γ není prvočinitel v $\mathbb{Z}[i]$.

7. **!** V $\mathbb{Z}[i]$ platí $5 = (1 + 2i)(1 - 2i) = (2 + i)(2 - i)$. Rozmyslete si, proč to není spor s tím, že $\mathbb{Z}[i]$ je gaussovský obor.
8. Ukažte, že α je prvočinitel v $\mathbb{Z}[i]$ právě tehdy, když $\overline{\alpha}$ je prvočinitel.
9. Ukažte, že pro $n \in \mathbb{Z}$ a $a + bi \in \mathbb{Z}[i]$ platí, že $n|(a + bi) \iff n|a$ a $n|b$.
10. **!** V $\mathbb{Z}[i]$ rozložte na prvočinitele čísla 15, $5 + i$, $12 + 21i$ a $3 + 21i$.
11. V $\mathbb{Z}[i]$ určete $NSD(12 + 21i, 3 + 21i)$:

    (a) z rozkladu na prvočinitele;

(b) pomocí Euklidova algoritmu a určete Bézoutovy koeficienty.

12. Popište, které čísla v $\mathbb{Z}[i]$ jsou dělitelné $1+i$.

6.10 Diofantické rovnice

1. **!** V $\mathbb{Z}^2$ řešte rovnici $x^2+1=y^5$.
2. **!** Dokažte, že obor $\mathbb{Z}\left[\sqrt{2}\right]$ je euklidovský.
3. **!** V $\mathbb{Z}^3$ řešte rovnici $x^2+y^2=z^2$.
4. **!** V $\mathbb{Z}^2$ řešte rovnici $x^2+1=y^3$.
5. **!** Dokažte, že obor $\mathbb{Z}\left[\sqrt{-2}\right]$ je euklidovský.
6. **!** V $\mathbb{Z}^2$ řešte rovnici $x^2+2=y^3$.
7. **!** Najděte všechny jednotky (čili invertibilní prvky) v oboru:
   (a) $\mathbb{Z}\left[\sqrt{-2}\right]$,
   (b) $\mathbb{Z}\left[\sqrt{2}\right]$,
   (c) $\mathbb{Z}\left[\sqrt{79}\right]$,
   (d) $\mathbb{Z}\left[\sqrt{58}\right]$.
8. V $\mathbb{Z}^2$ řešte rovnici $x^2+8=y^3$.
9. V $\mathbb{Z}^3$ řešte rovnici $x^2+y^2=z^3$ pro x, y nesoudělná.
10. V $\mathbb{Z}^2$ řešte rovnici $x^2+4=y^3$ pro:
    (a) x liché,
    (b) * x sudé.
11. V $\mathbb{Z}^2$ řešte rovnici $x^2+4=3y^3$ pro:
    (a) x liché,
    (b) x sudé.
12. V $\mathbb{Z}^2$ řešte rovnici $x^2+36=y^3$.
13. * V $\mathbb{Z}^2$ řešte rovnici $x^2-2=y^3$. (Poznámka: Rovnice $1=a^3+3a^2b+6ab^2+2b^3$ má v $\mathbb{Z}^2$ jediné řešení $(a,b)=(1,0)$.)
14. * V $\mathbb{Z}^2$ řešte rovnici $x^2-1=y^3$.
15. Ukažte, že obor $\mathbb{Z}[\sqrt{-3}]$ není euklidovský, dokonce ani gaussovský. Najděte ireducibilní prvek, který není prvočinitel. (Nápověda: Zkuste rozložit 4 na součin.)
16. * Buď $R=\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]=\mathbb{Z}\left[e^{\frac{2\pi i}{3}}\right]$.
    (a) Dokažte, že R je euklidovský s normou danou $N(x+y\sqrt{-3})=x^2+3y^2$.
    (b) Určete všechny invertibilní prvky v R.
    (c) V $\mathbb{Z}^2$ řešte rovnici $x^2+3=y^3$.

6.11 Kvadratické zbytky a Legendreovy symboly

1. **!** Najděte všechny kvadratické zbytky modulo n, kde $n = 4, 7, 8, 9, 17$.
2. Nechť $x, y, z \in \mathbb{Z}$ a platí $x^2 + y^2 = z^2$. Ukažte, že potom je aspoň jedno z čísel x, y, z dělitelné 3, aspoň jedno je dělitelné 4 a aspoň jedno je dělitelné 5.
3. **!** Určete hodnotu výrazů
   (a) $\left(\frac{3}{7}\right)$,
   (b) $\left(\frac{-1}{7}\right)$,
   (c) $\left(\frac{2}{7}\right)$,
   (d) $\left(\frac{11}{31}\right)$,
   (e) $\left(\frac{17}{37}\right)$,
   (f) $\left(\frac{523}{269}\right)$,
   (g) $\left(\frac{61}{31}\right)$,
   (h) $\left(\frac{337}{211}\right)$,
   (i) $\left(\frac{367}{241}\right)$.
4. **!** V závislosti na prvočísle p určete hodnotu výrazů
   (a) $\left(\frac{3}{p}\right)$,
   (b) $\left(\frac{5}{p}\right)$,
   (c) $\left(\frac{7}{p}\right)$,
   (d) $\left(\frac{13}{p}\right)$,
   (e) $\left(\frac{17}{p}\right)$.
5. Bez použití kvadratické reciprocity spočtěte $\left(\frac{17}{5}\right)$ a $\left(\frac{5}{17}\right)$.
6. **!** Určete kolik řešení má kongruence $x^2 \equiv 31 \pmod{71}$ a $x^2 \equiv 293 \pmod{347}$.
7. **!** Najděte všechna prvočísla p, pro která existuje $a \in \mathbb{Z}$ takové, že $p | a^2 + 7$.
8. Ukažte, že pokud $3 | a^2 + b^2$, pak $3 | a$ a $3 | b$.
9. Ukažte, že pro liché n platí $8 | n^2 - 1$.
10. Najděte všechna celočíselná řešení rovnice $x^2 + y^2 = 4z - 1$.
11. Ukažte, že rovnice $x^2 + y^2 = 8z + 6$ nemá žádné celočíselné řešení. Najděte další rovnici o třech neznámých, která nemá žádné celočíselné řešení.
12. Najděte všechna prvočísla p, pro které platí: Pokud je x kvadratický zbytek modulo p, pak je i $-x$ kvadratický zbytek modulo p.
13. ***** Ukažte, že pokud $p > 3$ je prvočíslo, pak p dělí součet všech kvadratických zbytků modulo p.
14. ***** Buď p prvočíslo, $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}$. Ukažte, že $\sum_{k=0}^{p-1} \left(\frac{ka+b}{p}\right) = 0$
15. ***** Buď p liché prvočíslo a $0, a_1, ..., a_{\frac{p-1}{2}}$ všechny kvadratické zbytky modulo p. Kolik z čísel $a_1 + 1, ..., a_{\frac{p-1}{2}} + 1$ jsou taky kvadratické zbytky modulo p?

16. * Ukažte, že pokud $n \in \mathbb{N}$ je kvadratický zbytek modulo každé prvočíslo, pak n je čtverec.

6.12 Charaktery a Gaussovy součty

1. ! Určete všechny charaktery modulo n a jejich řády v grupě $X(\mathbb{Z}_n^*)$ pro
   (a) $n = 3$,
   (b) $n = 5$,
   (c) $n = 7$,
   (d) $n = 4$,
   (e) $n = 8$,
   (f) $n = 12$,
   (g) $n = 17$,
   (h) $n = 18$.

   Nemusíte vyčíslit hodnoty na jednotlivých prvcích, ale nějak je jednoznačně popište.
2. ! Pro každý charakter modulo 3 spočtěte jeho Gaussův součet.
3. Ověřte, že $X(\mathbb{Z}_n^*)$ s operacemi definovanými výše tvoří grupu.
4. ! Označme $S_n := \left\{ e^{\frac{2\pi ik}{n}} : k = 0, ..., n-1 \right\}$ množinu všech n-tých komplexních odmocnin z 1.
   (a) Ukažte, že S_n s operací násobení (jako v $\mathbb{C}$) je grupa. Které grupě je S_n izomorfní?
   (b) Ukažte, že generátory grupy S_n (čili primitivní n-té odmocniny z 1) jsou právě ζ_n^k, pro které $\mathrm{NSD}(k, n) = 1$. Určete řád zbylých prvků.
   (c) Ukažte, že součet všech prvků S_n je 0.
   (d) Nechť χ je charakter modulo n. Ukažte, že jeho obraz $Im(\chi) := \{x \in \mathbb{C}^* : \exists a \in \mathbb{Z}_n^*; x = \chi(a)\}$ je podgrupa $S_{\varphi(n)}$.
   (e) Popište všechny charaktery modulo 11, jejichž obraz je celá S_{10}.
   (f) Nechť a je kvadratický zbytek a χ charakter modulo n. Popište, jaké hodnoty může nabývat $\chi(a)$.
5. Ukažte, že Legendreův symbol $\left(\frac{a}{p}\right)$ je charakter modulo p (p prvočíslo). Najděte všechny charaktery χ modulo p takové, že $\chi^2 = \varepsilon$, kde ε značí triviální charakter.
6. Určete hodnotu $\sum_{a \in \mathbb{Z}_n} \zeta_n^a$.
7. Spočtěte Gaussův součet nějakého netriviálního charakteru modulo
   (a) 5,
   (b) 7.
8. Ukažte, že pro charakter χ platí $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$.

9. **!** Buď p prvočíslo, $p \equiv 3 \pmod 4$, a buď S kvadratický Gaussův součet. Podrobně ukažte, že $S \in i\mathbb{R}$, tedy že $S = i^{\frac{p-1}{2}} \cdot r$ pro nějaké $r \in \mathbb{R}$.
10. ***** Ukažte, že $X(\mathbb{Z}_n^*) \simeq \mathbb{Z}_n^*$.
11. ***** Ukažte, že pokud $k \in \mathbb{N}, a, n \in \mathbb{Z}_k^*$, pak platí:

$$\frac{1}{\varphi(k)} \sum_{\chi \in X(Z_k^*)} \chi(n) \cdot \overline{\chi}(a) = \begin{cases} 0 & \text{pokud } n \not\equiv a \pmod k \\ 1 & \text{pokud } n \equiv a \pmod k \end{cases}$$

6.13 Jacobiho symboly

1. **!** Určete hodnotu výrazů
   (a) $\left(\frac{477}{247}\right)$,
   (b) $\left(\frac{98}{51}\right)$,
   (c) $\left(\frac{89}{63}\right)$,
   (d) $\left(\frac{347}{221}\right)$,
   (e) $\left(\frac{675}{223}\right)$,
   (f) $\left(\frac{735}{263}\right)$.
2. **!** Řešte kongruenci $x^2 \equiv 53 \pmod{77}$.
3. **!** Vyšetřete vztah Jacobiho symbolů a kongruencí. Konkrétně:
   (a) Rozhodněte, jestli mají kongruence $x^2 \equiv 18 \pmod{127}$ a $x^2 \equiv 14 \pmod{127}$ řešení. (127 je prvočíslo.)
   (b) Řešte kongruenci $x^2 \equiv 58 \pmod{209}$. $(209 = 11 \cdot 19)$
   (c) Rozhodněte, jestli má kongruence $x^2 \equiv 58 \pmod{65}$ řešení.
   (d) Řešte kongruenci $x^2 \equiv 2 \pmod{1081}$. $(1081 = 23 \cdot 47)$
4. **!** V závislosti na lichém prvočísle p určete hodnotu $\left(\frac{5}{3p}\right)$.
5. **!** Nechť n je liché přirozené číslo. Pomocí vztahů pro $\left(\frac{-1}{n}\right)$ a $\left(\frac{2}{n}\right)$ určete explicitně hodnotu $\left(\frac{-1}{n}\right), \left(\frac{2}{n}\right)$ a $\left(\frac{-2}{n}\right)$ v závislosti na n mod 4, resp. 8.
6. Vyšetřete vztah Jacobiho symbolů a kvadratických zbytků. Konkrétně:
   (a) Ukažte, že pokud $n = p_1 \cdots p_k$ je prvočíselný rozklad čísla n, pak kongruence $x^2 \equiv a \pmod n$ má řešení právě tehdy, když má řešení každá z kongruencí $x^2 \equiv a \pmod{p_1}$,..., $x^2 \equiv a \pmod{p_k}$.
   (b) Odvoďte, že pokud $\left(\frac{a}{n}\right) = -1$, pak a není kvadratický zbytek modulo n.
   (c) Najděte příklad, kdy $\left(\frac{a}{n}\right) = 1$ a a není kvadratický zbytek modulo n.
7. Nechť $a_1, ..., a_k$ jsou lichá celá čísla. Pak platí:
   (a) $\frac{a_1-1}{2} + ... + \frac{a_k-1}{2} \equiv \frac{a_1 \cdot ... \cdot a_k - 1}{2} \pmod 2$,
   (b) $\frac{a_1^2-1}{8} + ... + \frac{a_k^2-1}{8} \equiv \frac{(a_1 \cdot ... \cdot a_k)^2-1}{8} \pmod 8$.

8. Vyzkoušejte si testování prvočíselnosti pomocí Solovay-Strassenova testu:
   (a) Ukažte, že 15 není prvočíslo.
   (b) Ukažte, že 7 je prvočíslo.

6.14 Prvočísla speciálních tvarů

1. Dokončete důkaz tvrzení 2.18 ve skriptech:
   (a) Ukažte chybějící implikaci: Pokud pro prvočíslo $p > 2$ platí $p = a^2 + 2b^2$ pro nějaká $a, b \in \mathbb{Z}$, pak platí $p \equiv 1, 3 \pmod 8$.
   (b) Ukažte, že pro prvočíslo p platí: $p = a^2 + 2b^2$ pro nějaké $a, b \in \mathbb{Z}$, právě když p není prvočinitel v $\mathbb{Z}[\sqrt{-2}]$.
2. Uvažte obor $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ s normou danou $N(x + y\sqrt{-3}) = x^2 + 3y^2$.
   (a) Vyjádřete normu prvku $a + b\frac{-1+\sqrt{-3}}{2}$, $a, b \in \mathbb{Z}$.
   (b) * Ukažte, že tento obor je eukleidovský.
   (c) Najděte všechna prvočísla p taková, že kongruence $x^2 \equiv -3 \pmod p$ má řešení.
   (d) * Charakterizujte všechna prvočísla, která jdou napsat ve tvaru $a^2 - ab + b^2$, kde $a, b \in \mathbb{Z}$. Postupujte podobně jako v důkazu tvrzení 2.18 ve skriptech.

6.15 Rozklad na součin cyklických grup

1. ! Rozložte následující grupy na součin cyklických grup:
   (a) $\mathbb{Z}^*_{360}$,
   (b) $\mathbb{Z}^*_{45}$,
   (c) $\mathbb{Z}^*_{200}$,
   (d) $\mathbb{Z}^*_{64}$,
   (e) $\mathbb{Z}^*_{81}$,
   (f) $\mathbb{Z}^*_{120}$,
2. ! Rozložte grupy $\mathbb{Z}^*_{150}$, $\mathbb{Z}^*_{294}$ a $\mathbb{Z}^*_{400}$ na součin cyklických grup, jejichž řády jsou mocniny prvočísel.
3. ! Nechť R a S jsou komutativní okruhy s jednotkou. Dokažte:
   (a) $(R \times S)^* = R^* \times S^*$,
   (b) $R \cong S \Longrightarrow R^* \cong S^*$.
   (c) Pomocí Čínské věty o zbytcích dokažte: Pokud $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$ je rozklad na prvočísla, pak $\mathbb{Z}^*_n \cong \mathbb{Z}^*_{{p_1}^{e_1}} \times ... \times \mathbb{Z}^*_{{p_k}^{e_k}}$.
4. Ukažte, že $\mathbb{Z}^*_{24} \ncong \mathbb{Z}^*_4 \times \mathbb{Z}^*_6$. Rozložte $\mathbb{Z}^*_{24}$ na součin cyklických grup.

6.16 Primitivní prvky

1. **!** Najděte všechny primitivní prvky modulo 5, 11, 13 a 19.
2. **!** Najděte primitivní prvek modulo n, pro
   (a) $n = 125$,
   (b) $n = 17$,
   (c) $n = 49$,
   (d) $n = 81$,
   (e) $n = 26$,
   (f) $n = 98$,
   (g) $n = 45$.
3. **!** Které z následujících grup jsou cyklické?
   (a) $\mathbb{Z}_4^*$,
   (b) $\mathbb{Z}_{14}^*$,
   (c) $\mathbb{Z}_{16}^*$,
   (d) $\mathbb{Z}_{35}^*$.
4. **!** Najděte alespoň dva primitivní prvky modulo 49, 121. Určete celkový počet primitivních prvků modulo tyto čísla.
5. Určete počet primitivních prvků modulo p, kde p je prvočíslo.
6. Najděte izomorfizmus mezi množinou $\{1, -1, i, -i\}$ s násobením a $\mathbb{Z}_4$.
7. ***** Najděte všechny $n \in \mathbb{N}$ takové, že grupa $\mathbb{Z}_n^*$ je cyklická.
8. Buď $G(\cdot)$ konečná grupa a P její podmnožina, která je uzavřená na násobení. Pak je P podgrupa.
9. Dokažte, že pro $e \geq 3$ je $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$.
10. Ukažte, že množina $P = \{1 + 4a |\ 0 \leq a < 2^{e-2}\} \subseteq \mathbb{Z}_{2^e}^*$ je cyklická podgrupa $\mathbb{Z}_{2^e}^*$ generovaná prvkem 5 a její řád je roven 2^{e-2}.
11. Nechť G je podgrupa grupy $\mathbb{Z}_{61}^*$ generovaná prvky 9 a 11. Kolik má grupa G prvků? Je cyklická? Pokud ano, najděte nějaký její generátor.
12. Ukažte, že pokud p, q jsou prvočísla a $q = 4p+1$, potom 2 je primitivní prvek modulo q. (Nápověda: Zamyslete se, jaký řád může mít prvek 2 v grupě $\mathbb{Z}_q^*$, a vylučte zbylé případy.)
13. Nechť a je primitivní prvek modulo prvočíslo p. Ukažte, že a není kvadratický zbytek.
14. Nechť χ je charakter a a primitivní prvek modulo prvočíslo p. V závislosti na řádu $\chi(a)$ v grupě S_{p-1} určete $|\mathrm{Im}(\chi)|$.

6.17 Valuace

1. **!** Spočtěte $v_p(n)$ pro všechna prvočísla p a pro

(a) $n = 250$,

(b) $n = 51$,

(c) $n = 61$,

(d) $n = 170$,

(e) $n = 360$.

2. Spočtěte

   (a) $v_2(2^{60} - 3)$,

   (b) $v_3\left(\binom{81}{40}\right)$.

3. **!** Ukažte, že pro prvočíslo p a $m, n \in \mathbb{Z}$ platí:

   (a) multiplikativita: $v_p(mn) = v_p(m) + v_p(n)$,

   (b) trojúhelníková nerovnost: $v_p(m + n) \geq \min\{v_p(m), v_p(n)\}$. Ukažte, že pokud $v_p(m) \neq v_p(n)$, pak nastává rovnost.

4. Najděte příklad, kdy $v_p(a + b) > \max(v_p(a), v_p(b))$.
5. Nechť p je prvočíslo, pro $c \in \mathbb{Z}_{p^k}$ značíme

   - $v_p^*(c) := v_p(c)$, pokud $c \neq 0$,
   - $v_p^*(0) := v_p(p^k) = k$.

   Ukažte, že pro $a, b \not\equiv 0 \pmod{p^k}$ platí:

   (a) $a \equiv b \pmod{p^k} \Rightarrow v_p(a) = v_p(b)$,

   (b) $v_p^*(ab) = v_p^*(a) + v_p^*(b)$.

6. Rozmyslete si hodnoty valuace faktoriálů:

   (a) Pro přirozené číslo n a kladné reálné číslo $x \geq 1$ určete, kolik čísel z intervalu $[1, x]$ je dělitelných n.

   (b) Ukažte, že pro prvočíslo p je $\varphi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}$.

   (c) Dokažte Legendreův vzorec, že $v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$. (Nápověda: Uvědomte si, že suma je ve skutečnosti konečná. Kolik z činitelů v $n!$ přispěje do $v_p(n!)$ jedničkou? Kolik dvojkou?)

   (d) Spočtěte kolika nulami končí číslo 100!.

6.18 Řešení kongruencí pomocí primitivních prvků

1. **!** Vyřešte kongruence

   (a) $x^3 \equiv 1 \pmod{13}$,

   (b) $x^5 \equiv 1 \pmod{13}$,

   (c) $x^{10} \equiv 1 \pmod{13}$,

   (d) $x^4 \equiv 3 \pmod{13}$,

(e) $x^5 \equiv 2 \pmod{13}$,

(f) $x^5 \equiv 8 \pmod{11}$,

(g) $x^4 \equiv 9 \pmod{11}$,

(h) $x^6 \equiv 4 \pmod{11}$,

(i) $x^{12} \equiv -1 \pmod{17}$,

(j) $x^{10} \equiv 16 \pmod{23}$.

6.19 Carmichaelova čísla

1. **!** Ukažte, že 561 je Carmichaelovo číslo.
2. **!** Ukažte, že 1105 je Carmichaelovo číslo.
3. ***** Zformulujte obecné kritérium, kdy je součin různých prvočísel Carmichaelovo číslo.
4. ***** Buď p prvočíslo. Dokažte, že pak číslo p^k není Carmichaelovo číslo pro libovolné $k \in \mathbb{N}$.
5. ***** Nechť p a q jsou dvě různá prvočísla. Ukažte, že číslo $p \cdot q$ není Carmichaelovo číslo.

6.20 Involuce

1. Dokažte, že pro sudé n obsahuje grupa $\mathbb{Z}_n$ právě jednu involuci a pro liché n neobsahuje $\mathbb{Z}_n$ žádnou involuci. Rozmyslete si, co z toho lze vyvodit pro cyklické grupy.
2. **!** Najděte všechny involuce v $\mathbb{Z}_{15}^*$ a dokažte, že tato grupa není cyklická.
3. **!** Najděte všechny involuce v grupě

   (a) $\mathbb{Z}_{30}^*$,

   (b) $\mathbb{Z}_{35}^*$,

   (c) $\mathbb{Z}_{51}^*$,

   (d) $\mathbb{Z}_{55}^*$.

4. Nechť $p > 2$ je prvočíslo. Pak -1 je jediná involuce v $\mathbb{Z}_p^*$.
5. ***** Najděte všechna $n \in \mathbb{N}$ takové, že všechny prvky $\mathbb{Z}_n^* \setminus \{1\}$ jsou involuce.

6.21 Míjení prvků

1. **!** V grupě $\mathbb{Z}_{45}$ najděte všechny prvky, které míjí prvek

   (a) 5,

   (b) 2,

   (c) 3.

2. **!** V grupě $\mathbb{Z}_{60}$ najděte všechny prvky, které míjí prvek

   (a) 7,
   (b) 2,
   (c) 4,
   (d) 6.

3. **!** V grupě $\mathbb{Z}_{72}$ najděte všechny prvky, které míjí prvek
   (a) 11,
   (b) 4.
4. **!** V grupě $\mathbb{Z}_{100}$ najděte všechny prvky, které míjí prvek
   (a) 7,
   (b) 5.
5. Nechť A, B jsou grupy, $(e, f) \in A \times B$, $a \in A$. Pokud a míjí e v A, pak pro každé $b \in B$ prvek (a, b) míjí prvek (e, f) v $A \times B$.
6. ***** Najděte obecné kritérium, kdy se v $\mathbb{Z}_n$ míjí prvky a a b.

6.22 Rabin-Millerovi svědci a lháři

1. **!** Najděte nějakého lháře a svědka pro
   (a) $N = 51$,
   (b) $N = 221$,
   (c) $N = 39$,
   (d) $N = 121$.
2. **!** Najděte a takové, že a je lhář pro 9.
3. **!** Najděte nějakého lháře (jiného jako 1) pro číslo 85 a nesoudělného svědka pro číslo 85.
4. **!** Najděte všechna $0 < a < N$ taková, že a je lhář pro N pro:
   (a) $N = 15$,
   (b) $N = 21$,
   (c) $N = 27$,
   (d) $N = 35$,
   (e) $N = 77$.
5. **!** Pomocí Rabin-Millerova testu ukažte, že 7 je prvočíslo.

6.23 RSA

1. **!** Uvažte $p = 19$, $q = 31$ a zprávu $a = 123$. Zvolte si veřejný a soukromý klíč pro šifru RSA a zašifrujte tuto zprávu. Ověřte, že je zprávu možné rozšifrovat pomocí soukromého klíče.

2. **!** V této úloze pošlete zprávu zašifrovanou pomocí RSA někomu (spolužákovi, nebo klidně i někomu jinému), kdo ji následně vyluští.
   (a) Zvolte si nějaká dvě prvočísla $p, q \leq 100$.
   (b) Spočtěte $N = pq$ a $m = \text{nsn}(p-1)(q-1)$.
   (c) Najděte nějaká dvě čísla e, d tak, aby $ed \equiv 1 \pmod{m}$. Je možné nejprve zvolit nějaké e nesoudělné s m a dopočítat inverz d pomocí rozšířeného Eukleidova algoritmu. Čísla N, e tvoří veřejný klíč, číslo d je vaším soukromým klíčem. Veřejný klíč dejte spolužákovi, který vám pomocí něj pošle zašifrovanou zprávu. Na oplátku dostanete jeho veřejný klíč, pomocí kterého zašifrujete zprávu vy pro něj.
   (d) Zvolte si nějakou zprávu x (vaše oblíbené číslo od 1 do $N-1$). Pomocí cizího veřejného klíče ji zašifrujte a pošlete (k výpočtu použijte software, případně rychlé mocnění).
   (e) Použijte svůj soukromý klíč k vyluštění zprávy, která vám přišla.
3. **!** Odpovězte na zprávu z předešlé úlohy. Svou odpověď podepište pomocí svého soukromého klíče. Co musí osoba na druhé straně udělat, aby ověřila váš podpis?
4. **!** Můj veřejný klíč (modul N) je 667 a exponent (číslo e) je 47 , přišla mi zpráva 420 zašifrovaná pomocí RSA. Vyluštěte tuto zprávu.
5. **!** Nechť $N = pq$ pro prvočísla p, q. Rozmyslete si, jak můžeme pomocí hodnot čísel N a $\varphi(N)$ určit hodnoty p a q. ***** Uměli byste to pomocí hodnot N a exponentu monoidu $\mathbb{Z}_N(\cdot)$ (např. s pomocí počítače)?
6. Dokažte lemma 3.13 ze skript: Ať jsou $p_1, \ldots, p_r$ po dvou různé lichá prvočísla. Nejmenší možný exponent monoidu $\mathbb{Z}_{p_1 \cdots p_r}(\cdot)$ je $\text{nsn}(p_1 - 1, \ldots, p_r - 1)$.
7. **!** Spočtěte $2^{100} \bmod 121$. (Návod: Napište si exponent v dvojkové soustavě. Pomocí mocnění na druhou spočtěte $2^1 \bmod 121$, $2^2 \bmod 121$, $2^4 \bmod 121$, $\ldots$, $2^{64} \bmod 121$. Vynásobte mezi sebou vhodné výsledky z předchozí části.) ***** Zobecněte a odhadněte počet kroků potřebných na výpočet $k \bmod n$ v závislosti na k.
8. Obecně se věří, že rozložit číslo na prvočísla je výpočetně složité. Pokud je však číslo nějakého speciálního tvaru, lze jej občas rozložit jednoduše. Způsob známý jako *Fermatova metoda* využívá vzorce $x^2 - y^2 = (x+y)(x-y)$.
   (a) Rozložte číslo 249 919 tak, že jej napíšete jako rozdíl čtverců.
   (b) Ukažte, že každé číslo lze zapsat jako rozdíl čtverců.
9. Složitější *Eulerova metoda* je založena na tom, že se nám nějaké číslo podaří napsat jako součet dvou čtverců dvěma různými způsoby, t.j. máme $N = a^2 + b^2 = c^2 + d^2$, kde $a > b > 0$, $c > d > 0$ a N je liché.
   (a) Ukažte, že v tomto tvaru nejde napsat žádné $N \equiv 3 \pmod{4}$.
   (b) Ukažte, že v tomto tvaru nejde napsat žádné prvočíslo $p \equiv 1 \pmod{4}$.
   (c) ***** Ukažte jak pomocí tohoto zápisu najít nějaký rozklad N.

6.24 Cyklotomické polynomy

1. **!** Spočtěte n-tý cyklotomický polynom pro $1 \leq n \leq 6$ a pro $n = 12, 18$.

2. **!** Rozložte polynom $x^n - 1$ na součin ireducibilních polynomů v $\mathbb{Q}[x]$ pro
   (a) $n = 7$,
   (b) $n = 12$,
   (c) $n = 15$,
   (d) $n = 18$,
   (e) $n = 20$.
3. Spočtěte osmý cyklotomický polynom a výpočtem ukažte, že je ireducibilní.

6.25 Dirichletova věta o prvočíslech

1. Rozmyslete si některé speciální případy Dirichletovy věty:
   (a) Připomeňte si Eukleidův důkaz, že existuje nekonečně mnoho prvočísel.
   (b) Upravte ho a ukažte, že existuje nekonečně mnoho prvočísel tvaru $4k+3$ nebo $6k+5$.
   (c) Vysvětlete, proč předchozí postup nefunguje pro prvočísla jiného tvaru, například $4k+1$, nebo obecně $ak-1$ pro nějaké $a \in \mathbb{N}$.
   (d) Ukažte, že pokud pro liché prvočíslo p platí $p|n^2+1$ pro nějaké $n \in \mathbb{N}$, potom p musí být tvaru $4k+1$.
   (e) Pomocí předchozí úlohy a Eukleidova důkazu ukažte, že existuje nekonečně mnoho prvočísel tvaru $4k+1$.
   (f) Ukažte, že pro prvočíslo p je $\left(\frac{-2}{p}\right) = 1$, právě když p je tvaru $8k+1$ nebo $8k+3$.
   (g) Podobně jako v části e) odvoďte, že existuje nekonečně mnoho prvočísel tvaru $8k+3$.
   (h) Najděte všechna prvočísla p, pro která je 5 kvadratický zbytek modulo p.
   (i) Převeďte výsledek předchozí úlohy na podmínku modulo 10 a pomocí toho ukažte, že existuje nekonečně mnoho prvočísel tvaru $10k+9$.
2. Ukažte, že Dirichletova věta je ekvivalentní tvrzení, že pro každé $a \in \mathbb{N}$, $b \in \mathbb{Z}$, pro které $\mathrm{NSD}(a,b) = 1$, existuje alespoň 1 prvočíslo $p \equiv b \pmod{a}$. Uvědomte si, že z toho neplyne, že z existence jednoho prvočísla $p \equiv 5 \pmod{11}$ je takových prvočísel nekonečně mnoho.

6.26 Jiné

1. ***** Ukažte, že pro $n > 1$ výraz $\sum_{k=1}^{n} \frac{1}{k}$ nikdy není celé číslo. (Nápověda: Použijte Bertrandův postulát, že mezi n a $2n$ vždy existuje aspoň jedno prvočíslo).
2. ***** Rozhodněte, jestli existuje nějaká mocnina 2, jejíž cifry lze přeskládat tak, aby vznikla jiná mocnina 2.
3. ***** Ukažte, že každá grupa, jejíž všechny prvky mají řád 2, je komutativní.

4. ***** Dokažte, že pro $n > 1$ platí $n \nmid 2^n - 1$.
5. ***** Ukažte, že pokud čísla a, b jdou zapsat jako součet dvou čtverců, pak jde takto zapsat i ab. Pomocí toho charakterizujte všechna taková čísla.