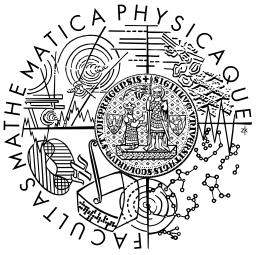

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Samuel Staško

Kubická a bikvadratická reciprocita

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika

Studijní obor: Matematika pro informační technologie

Praha 2019

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Děkuji doc. Mgr. Pavlu Příhodovi, Ph.D. za velice profesionální a ochotné vedení mé práce.

Název práce: Kubická a bikvadratická reciprocita

Autor: Samuel Staško

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Hlavní motivací pro zkoumání kubické a bikvadratické reciprocity je rozhodnout, zda mají kongruence $x^3 \equiv a\,(p)$ nebo $x^4 \equiv a\,(p)$, kde $a \in \mathbb{Z}$, p prvočíslo, nějaké celočíselné řešení. Jádrem této práce je prostřednictvím postupně vybudované teorie v okruzích Eisensteinových a Gaussových celých čísel dokázat zákony kubické a bikvadratické reciprocity. U obou těchto tvrzení se navíc podrobněji podíváme na speciální případy, ve kterých je nelze použít. To nás povede k odvození tzv. doplňku k zákonu kubické (resp. bikvadratické) reciprocity. Nakonec ukážeme, jak lze tyto výsledky aplikovat na problém řešitelnosti zmíněných kongruencí.

Klíčová slova: kubická reciprocita, bikvadratická reciprocita, zbytkový symbol, kongruence

Title: Cubic and biquadratic reciprocity

Author: Samuel Staško

Department: Department of Algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: The main motivation for studying cubic and biquadratic reciprocity is to decide, whether the congruences $x^3 \equiv a\,(p)$ or $x^4 \equiv a\,(p)$, where $a \in \mathbb{Z}$, p prime, have any integer solution. The core of this thesis will be to prove the laws of cubic and biquadratic reciprocity through gradually built theory in the rings of Eisenstein and Gaussian integers. In addition, for both of these theorems, we will take a closer look at the special cases, in which they cannot be used. This will lead us to the derivation of the supplement to the law of cubic (or biquadratic) reciprocity. Finally, we will show how these results can be applied to the problem of solvability of mentioned congruences.

Keywords: cubic reciprocity, biquadratic reciprocity, residue symbol, congruence

Obsah

Úvod

Studium zákonů reciprocity mělo velký vliv na vývoj moderní teorie čísel. Vše to začalo v roce 1783, kdy Euler a Legendre zformulovali zákon kvadratické reciprocity (důkaz nicméně provedl až Gauss o 13 let později), který dával odpověď na otázku, pro která $a \in \mathbb{Z}$ a prvočísla p má $x^2 \equiv a\,(p)$ nějaké řešení.

Logickým pokračováním byla snaha dosáhnout podobného výsledku i pro jiné volby $n \in \mathbb{N}$ v kongruenci $x^n \equiv a\,(p)$. Postupem času se ukázalo, že za podmínky $n > 2$ je problém mnohem složitější. Na důkazy dalších recipročních zákonů se čekalo bezmála 50 let. Zásluhou německého matematika Gottholda Eisensteina se v roce 1844 objevily hned dva, a sice pro případ kubické ($n = 3$) a bikvadratické ($n = 4$) reciprocity.

Hlavní náplní práce budou právě tyto dva důkazy. Každá kapitola se zaměří na jeden z nich. Celková struktura bude přibližně odpovídat kapitole 9 knihy Ireland a Rosen (2013). Navíc ale přidáme rozšiřující teorii, jejíž podstatou je usnadnění výpočtu kubického, resp. bikvadratického zbytkového symbolu pro každou dvojici prvků, pro niž je korektně definovaný, a zároveň na ni nelze aplikovat příslušný reciproční zákon. Na základě toho budeme schopni plně zodpovědět původní otázku, tj. zda je pro dané $a \in \mathbb{Z}$ a prvočíslo p řešitelná kongruence $x^n \equiv a\,(p)$, kde $n = 3$, nebo $n = 4$. Tyto doplňující části jsou pokryté sekcí 1.5 (str. 14–17) a stranami 26–28, přičemž odpovídají cvičením 17–20, 24–26 a 32–37 z kapitoly 9 uvedeného zdroje.

1. Kubická reciprocita

V této kapitole se budeme zabývat především otázkou řešitelnosti kongruence $x^3 \equiv a \pmod{p}$, kde $a \in \mathbb{Z}$, p prvočíslo. Vypracujeme hlubší teorii okruhu Eisensteinových celých čísel $\mathbb{Z}[\omega]$ a kubických zbytků, díky níž zformulujeme a dokážeme zákon kubické reciprocity (Věta 1.16), což můžeme považovat za analogii zákona kvadratické reciprocity pro stupeň 3. Na závěr se podíváme i na jeho zobecněnou verzi a některá další doplňující tvrzení.

1.1 Okruh $\mathbb{Z}[\omega]$

Položme $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i = \frac{-1+\sqrt{-3}}{2}$. Množina $R = \mathbb{Z}[\omega] = \{a + b\omega;\ a, b \in \mathbb{Z}\}$ pak spolu se sčítáním a násobením na komplexních číslech tvoří okruh, někdy nazývaný Eisensteinova celá čísla. Pro $\alpha = a + b\omega \in R$ definujeme jeho normu předpisem $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$, kde $\overline{\alpha}$ je komplexně sdružený prvek k α, čili $\overline{\alpha} = \overline{a + b\omega} = a + b\overline{\omega} = (a - b) - b\omega$, neboť $\overline{\omega} = \frac{-1-\sqrt{-3}}{2} = \omega^2 = -1 - \omega$. Takto definované zobrazení $N : R \to \mathbb{N}_0$ je zřejmě multiplikativní (tedy $\forall \alpha, \beta \in R$ platí $N\alpha\beta = N\alpha N\beta$). Kromě toho splňuje vlastnosti eukleidovské normy, takže R je eukleidovský obor - důkaz lze najít např. v Ireland a Rosen (2013, Tvrzení 1.4.2). Z toho mimo jiné plyne, že je taky OHI (obor hlavních ideálů) a gaussovský.

Dále se podíváme na invertibilní prvky okruhu R. K jejich výpočtu použijeme následující charakterizaci.

Věta 1.1. *Nechť $\alpha \in R$. Pak $N\alpha = 1 \Leftrightarrow \alpha$ je invertibilní.*

Důkaz.

„$\Rightarrow$“ Máme $\alpha\overline{\alpha} = 1$. Dle úvahy výše $\overline{\alpha} \in R$, stačí tedy vzít $\alpha^{-1} = \overline{\alpha}$.

„$\Leftarrow$“ Ať je α invertibilní. Pak $\exists \beta \in R : \alpha\beta = 1$. Tudíž $N\alpha\beta = N\alpha N\beta = 1$. Protože $N\alpha$ i $N\beta$ jsou nezáporná celá čísla, tak $N\alpha = 1$.

□

Nyní jsme schopni určit všechny invertibilní prvky R. Podle předchozí Věty to jsou právě prvky $a + b\omega$ splňující $a^2 - ab + b^2 = 1$, neboli $(a - b)^2 + a^2 + b^2 = 2$. Mohou tedy nastat tyto možnosti:

(i) $(a - b)^2 = 0$, $a^2 = 1$, $b^2 = 1$: dostáváme prvky $1 + \omega = -\omega^2$, $-1 - \omega = \omega^2$

(ii) $(a - b)^2 = 1$, $a^2 = 1$, $b^2 = 0$: dostáváme prvky 1, -1

(iii) $(a - b)^2 = 1$, $a^2 = 0$, $b^2 = 1$: dostáváme prvky ω, $-\omega$.

Naším dalším cílem bude popsat, jak vypadají prvočinitele (ekvivalentně ireducibilní prvky – v gaussovských oborech totiž oba tyto pojmy splývají) v R. Předně je potřeba si uvědomit, že prvočíslo (v $\mathbb{Z}$) nemusí nutně být i prvočinitel v R. Nejjednodušším protipříkladem je $3 = -\omega^2(1 - \omega)^2$. Z tohoto důvodu budeme pojmem *prvočinitel* označovat prvočinitel v R a pojmem *prvočíslo* kladný prvočinitel v $\mathbb{Z}$.

Věta 1.2. *Je-li π prvočinitel v R, pak existuje prvočíslo p takové, že:*

- *$N\pi = p$, přičemž π není asociované s žádným prvočíslem, nebo*
- *$N\pi = p^2$, $\pi \parallel p$.*

Důkaz. Buď π prvočinitel v R. Potom π není invertibilní, takže $N\pi = \pi\overline{\pi} = n > 1$, $n \in \mathbb{N}$. Tedy $\pi \mid n$. Protože je π prvočinitel, tak $\pi \mid p$ pro nějaké prvočíslo p z prvočíselného rozkladu n. Čili $p = \pi\gamma$ pro vhodné $\gamma \in R$. Dostáváme $N\pi N\gamma = Np = p^2$, tedy buď $N\pi = N\gamma = p$, nebo $N\pi = p^2$ a $N\gamma = 1$. V prvním případě $\pi \nmid q$ pro každé prvočíslo q, neboť kdyby $\pi = qu$, u invertibilní, tak by muselo platit $p = N\pi = NqNu = q^2$, což je spor. Ve druhém případě je γ invertibilní, tedy $\pi \parallel p$. □

Věta 1.3. *Jestliže pro $\pi \in R$ platí $N\pi = p$ prvočíslo, pak je π prvočinitel v R.*

Důkaz. Předpokládejme, že $\pi = \beta\gamma$, kde $N\beta, N\gamma > 1$. Pak ale $p = N\pi = N\beta N\gamma$, což je spor s prvočíselností p. Takže π je prvočinitel. □

Věta 1.4. *Nechť p je prvočíslo.*

(a) Pokud $p = 3$ nebo $p \equiv 1\,(3)$, pak $p = \pi\overline{\pi}$, kde π je prvočinitel v R.

(b) Pokud $p \equiv 2\,(3)$, pak p je prvočinitel v R.

Každý prvočinitel v R je asociovaný s některým z těchto prvočinitelů.

Důkaz.

(a) Pro $p \equiv 1\,(3)$ je podle zákona kvadratické reciprocity

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

To znamená, že $\exists a \in \mathbb{Z} : a^2 \equiv -3\,(p)$. Čili $pb = a^2 + 3$ pro nějaké $b \in \mathbb{Z}$. Je-li $p = 3$, stačí vzít $a = 0$, $b = 1$. V obou případech tedy p dělí $\left(a + \sqrt{-3}\right)\left(a - \sqrt{-3}\right) = (a + 1 + 2\omega)(a - 1 - 2\omega)$. Pro spor ať p dělí některý z těchto dvou činitelů. Potom $\frac{a+1+2\omega}{p} = \frac{a+1}{p} + \frac{2\omega}{p} \in R$ nebo $\frac{a-1-2\omega}{p} = \frac{a-1}{p} - \frac{2\omega}{p} \in R$. Každopádně musí platit $\frac{2}{p} \in \mathbb{Z}$, což je spor, neboť $p \neq 2$. Tedy p není prvočinitel v R. Z toho plyne, že $p = \pi\gamma$, $\pi \nmid 1 \nmid \gamma$. Navíc $p^2 = Np = N\pi N\gamma$, takže $N\pi = \pi\overline{\pi} = p$. Podle Věty 1.3 je π prvočinitel.

(b) Ať $p = \pi\gamma$, kde $N\pi, N\gamma > 1$, $\pi = a + b\omega$. Potom $p^2 = N\pi N\gamma$, tedy $p = N\pi = a^2 - ab + b^2$, ekvivalentně $4p = (2a - b)^2 + 3b^2$. Tím pádem je $p \equiv (2a - b)^2\,(3)$. Protože $x^2 \equiv 0$ nebo $1 \pmod 3$ pro libovolné $x \in \mathbb{Z}$, tak $p \equiv 0$ nebo $1 \pmod 3$ a dostáváme spor s předpokladem $p \equiv 2\,(3)$. Tedy p je prvočinitel.

Nechť π je prvočinitel. Podle Věty 1.2 je $\pi\overline{\pi} = p$ nebo $\pi\overline{\pi} = p^2$ pro vhodné prvočíslo p. Tedy π dělí p nebo p^2, přičemž oba tyto prvky se dle výše dokázaného rozkládají na součin prvočinitelů ze skupiny *(a)* nebo *(b)*. Ale π je prvočinitel, takže musí dělit nějaký prvek p_i z tohoto rozkladu. Ten je taky prvočinitel, tudíž jsou π a p_i asociované. □

1.2 Kubický zbytkový symbol

Analogicky jako v $\mathbb{Z}$ můžeme i v R definovat pojem kongruence. Pro jakékoli $\alpha, \beta, \gamma \in R$ budeme značit $\alpha \equiv \beta\,(\gamma)$, jestliže $\gamma \mid \alpha - \beta$. To nám umožňuje zkoumat zbytkové třídy modulo $\pi \in R$ a faktorokruhy $R/\pi R$. Speciálně nás bude zajímat případ, kdy je π prvočinitel. V celých číslech pro libovolné prvočíslo p platí, že $\mathbb{Z}/p\mathbb{Z}$ je p-prvkové těleso. Podobné tvrzení platí také v oboru R.

Věta 1.5. *Je-li $\pi \in R$ prvočinitel, pak $R/\pi R$ je těleso s $N\pi$ prvky.*

Důkaz. Víme, že ideál $I < R$ je maximální právě tehdy, když R/I je těleso. Ukážeme tedy, že $I = (\pi)$ je maximální. Buď $\gamma \in R \setminus I$. Obor R je eukleidovský, takže v něm platí Bézoutova věta. Existují tedy $\alpha, \beta \in R$ takové, že $\alpha\pi + \beta\gamma = 1$, neboli $1 \in (\alpha) + (\beta)$. Jinými slovy, $(\alpha) + (\beta) = R$. Z toho již plyne, že $I = (\pi)$ je maximální.

Zbývá ukázat, že počet prvků $R/\pi R$ je roven $N\pi$. K tomu potřebujeme důkaz rozdělit na případy uvedené ve Větě 1.4.

Předně ať $\pi = p \equiv 2\,(3)$, kde p je prvočíslo. Pro libovolné $\mu = c + d\omega$ existují (dělení se zbytkem) jednoznačně určené $e, f, g, h \in \mathbb{Z}$, $0 \leq f, h < p$ takové, že $\mu = (ep + f) + (gp + h)\,\omega \equiv f + h\omega\,(p)$. Předpokládejme, že $f + h\omega \equiv f' + h'\omega\,(p)$, přičemž $0 \leq f', h' < p$. Pak $\frac{f-f'}{p} + \frac{h-h'}{p}\omega \in R$, tedy $\frac{f-f'}{p} \in \mathbb{Z}$, $\frac{h-h'}{p} \in \mathbb{Z}$. Ovšem $|f - f'| < p$, $|h - h'| < p$, takže taková situace může nastat pouze v případě, že $f = f'$, $h = h'$. Tím jsme dokázali, že pro každé $\mu \in R$ existují jednoznačně určená čísla $a, b \in \mathbb{Z}$, $0 \leq a, b < p$ splňující $\mu \equiv a + b\omega\,(p)$. Tudíž $R/\pi R = \{[a + b\omega]\,;\ 0 \leq a,\, b < p\}$ a zjevně $|R/\pi R| = p^2 = N\pi$.

Nyní ať $p = 3$ nebo $p \equiv 1\,(3)$ je prvočíslo, $\pi = a + b\omega$ a $\pi\overline{\pi} = N\pi = p = a^2 - ab + b^2$. Kdyby p dělilo b, tak by muselo dělit i a, z čeho by plynulo $p^2 \mid p = a^2 - ab + b^2$. Takže $p \nmid b$. Díky tomu $\forall d \in \mathbb{Z}\ \exists x \in \mathbb{Z} : xb = d\,(p)$. Je-li tedy $\mu = c + d\omega$, potom pro vhodné x platí $\mu - x\pi = c - xa + (d - xb)\,\omega \equiv c - xa\,(p)$. Jelikož $\pi \mid p$, tím spíš $\mu - x\pi \equiv c - xa\,(\pi)$, a tedy $\mu \equiv c - xa\,(\pi)$. Vidíme, že každý prvek R je modulo π kongruentní nějakému celému číslu r z intervalu $[0,\, p)$. Pokud $r \equiv r'\,(\pi)$, kde $r' \in \mathbb{Z}$, $0 \leq r' < p$, jistě $r - r' = \pi\lambda$ pro vhodné $\lambda \in R$. Po znormování máme $(r - r')^2 = pN\lambda$, co znamená, že $p \mid r - r'$. Ale $|r - r'| < p$, takže $r = r'$. Z toho plyne, že pro každé $\mu \in R$ existuje jednoznačně určené $r \in \mathbb{Z}$, $0 \leq r < p$ splňující $\mu \equiv r\,(\pi)$. Tudíž $R/\pi R = \{[r]\,;\ 0 \leq r < p\}$ a opět zřejmě $|R/\pi R| = p = N\pi$. □

Důsledek 1.6. *Nechť $\pi \nmid \alpha$, kde $\alpha, \pi \in R$, π prvočinitel. Pak*

$$\alpha^{N\pi - 1} \equiv 1\,(\pi)\,.$$

Důkaz. Podle Věty 1.5 je velikost multiplikativní grupy $(R/\pi R)^*$ rovna $N\pi - 1$. Tvrzení pak plyne z Malé Fermatovy věty. □

Podívejme se blíže na zmíněnou grupu $(R/\pi R)^*$ pro prvočinitel π, jehož norma je různá od 3. Dle Věty 1.4 může být $\pi = q \equiv 2\,(3)$ prvočíslo, pak $N\pi = q^2 \equiv 1\,(3)$, nebo $\pi\overline{\pi} = N\pi = p \equiv 1\,(3)$. Každopádně ale platí $N\pi \equiv 1\,(3)$. Tohoto faktu využijeme nejen v důkazu následujícího tvrzení.

Věta 1.7. *Buď $\alpha \in R$. Je-li $\pi \in R$ prvočinitel takový, že $N\pi \neq 3$ a $\pi \nmid \alpha$, potom existuje právě jedno $m \in \{0, 1, 2\}$ splňující $\alpha^{\frac{N\pi - 1}{3}} \equiv \omega^m\,(\pi)$.*

Důkaz. Z Důsledku 1.6 a toho, že 1, ω, ω^2 jsou kořeny rovnice $x^3 - 1 = 0$, dostáváme:

$$\pi \mid \alpha^{N\pi-1} - 1 = \left(\alpha^{\frac{N\pi-1}{3}} - 1\right)\left(\alpha^{\frac{N\pi-1}{3}} - \omega\right)\left(\alpha^{\frac{N\pi-1}{3}} - \omega^2\right).$$

Takže π dělí nějaký ze tří činitelů na pravé straně. Kdyby dělil alespoň 2 z nich, pak by dělil i jejich rozdíl, tedy $1-\omega$, $1-\omega^2$ nebo $\omega - \omega^2$. Předpokládejme, že $\pi \mid 1-\omega$. Protože $1-\omega$ je prvočinitel, tak musí být s π asociovaný. To ovšem znamená, že mají stejnou normu, čili $N\pi = 3$, což je ve sporu s předpokladem věty. Zbylé možnosti se vyloučí podobně přímočaře. □

Tato věta nám umožňuje korektně zavést analogii Legendreova symbolu v Eisensteinových celých číslech, tzv. kubický zbytkový symbol.

Definice. Nechť $\alpha, \pi \in R$, π prvočinitel s $N\pi \neq 3$. *Kubický zbytkový symbol* $\left(\frac{\alpha}{\pi}\right)_3$ definujeme předpisem

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{pokud } \pi \mid \alpha \\ \omega^m \equiv \alpha^{\frac{N\pi-1}{3}}\,(\pi)\text{, kde } m \in \{0,1,2\} & \text{jinak.} \end{cases}$$

Řekneme, že α je *kubický zbytek modulo* π, jestliže existuje $x \in R$ takové, že $x^3 \equiv \alpha\,(\pi)$. V opačném případě je α *kubický nezbytek modulo* π.

Vzpomeňme si opět na Legendreův symbol. Jeho nejvýznamnější vlastností je to, že pro všechna $a, p \in \mathbb{Z}$, p prvočíslo, $p \nmid a$, platí $\left(\frac{a}{p}\right)_2 = 1$ právě tehdy, když je a kvadratickým zbytkem modulo p (v případě $p \mid a$ je a zbytkem triviálně). Podobně i pro α, $\pi \in R$ očekáváme, že nám hodnota kubického zbytkového symbolu $\left(\frac{\alpha}{\pi}\right)_3$ řekne, zda je α kubickým zbytkem, či nezbytkem modulo π. Správnost tohoto očekávání teď potvrdíme.

Věta 1.8. *Nechť $\alpha, \pi \in R$, π prvočinitel, $N\pi \neq 3$, $\pi \nmid \alpha$. Pak $\left(\frac{\alpha}{\pi}\right)_3 = 1$ právě tehdy, když má kongruence $x^3 \equiv \alpha\,(\pi)$ řešení v R.*

Důkaz.

„⇒“ Protože $R/\pi R$ je konečné těleso, tak multiplikativní grupa $(R/\pi R)^*$ je cyklická řádu $N\pi - 1$ (viz Věta 1.5). Zvolme $\gamma \in R$ takové, že $[\gamma] = \gamma + \pi R$ je její generátor. Tudíž $\alpha \equiv \gamma^k\,(\pi)$ pro nějaké $k \in \mathbb{N}$. Máme tedy

$$1 = \left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} \equiv \left(\gamma^k\right)^{\frac{N\pi-1}{3}} \equiv \gamma^{\frac{k(N\pi-1)}{3}}\,(\pi),$$

takže $ord\,([\gamma]) = N\pi - 1 \mid \frac{k(N\pi-1)}{3}$, což implikuje $3 \mid k$. Položíme-li $x = \gamma^{\frac{k}{3}}$, dostaneme $x^3 \equiv \left(\gamma^{\frac{k}{3}}\right)^3 \equiv \gamma^k \equiv \alpha\,(\pi)$.

„⇐“ $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} \equiv (x^3)^{\frac{N\pi-1}{3}} \equiv x^{N\pi-1} \equiv 1\,(\pi)$ dle Důsledku 1.6 ($\pi \nmid x$ plyne z předpokladu $\pi \nmid \alpha$).

□

Uveďme si ještě některé další základní vlastnosti kubického zbytkového symbolu.

Věta 1.9. *Pro každé $\alpha, \beta, \pi \in R$, π prvočinitel, $N\pi \neq 3$ platí:*

(a) $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} (\pi)$,

(b) $\alpha \equiv \beta (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$,

(c) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$,

(d) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\alpha^2}{\pi}\right)_3 = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$.

Důkaz.

(a) Pokud $\pi \nmid \alpha$, tvrzení plyne přímo z definice, jinak $\left(\frac{\alpha}{\pi}\right)_3 = 0 \equiv \alpha^{\frac{N\pi-1}{3}} (\pi)$.

(b) $\alpha \equiv \beta (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} \equiv \beta^{\frac{N\pi-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$, neboť oba symboly můžou nabývat pouze hodnot 0, 1, ω, nebo ω^2, a každé dvě z nich dávají různý zbytek po dělení π (viz Věta 1.7).

(c) $\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{\frac{N\pi-1}{3}} \equiv \alpha^{\frac{N\pi-1}{3}} \beta^{\frac{N\pi-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$.

(d) Snadno lze ověřit, že $\forall x \in \{0, 1, \omega, \omega^2\} : x^2 = \overline{x}$. Z toho plyne první rovnost. Druhá je jasná díky *(c)*. Podle části *(a)* a proto, že $N\pi = N\overline{\pi}$, je

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} \equiv \overline{\alpha^{\frac{N\pi-1}{3}}} \equiv \overline{\alpha}^{\frac{N\pi-1}{3}} \equiv \overline{\alpha}^{\frac{N\overline{\pi}-1}{3}} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3 \pmod{\overline{\pi}},$$

takže platí i poslední rovnost.

□

Přímým důsledkem poslední části předchozí věty je $\left(\frac{n}{p}\right)_3 = \left(\frac{n}{p}\right)_3^2$ pro $n, p \in \mathbb{Z}$, $p \equiv 2 (3)$ prvočíslo. Pokud navíc platí $p \nmid n$, pak jistě $\left(\frac{n}{p}\right)_3 \neq 0$, tudíž $\left(\frac{n}{p}\right)_3 = 1$. Jinými slovy, n je kubickým zbytkem modulo p. Obecněji, jsou-li $p \equiv q \equiv 2 (3)$ dvě různá prvočísla, dostáváme $\left(\frac{p}{q}\right)_3 = \left(\frac{q}{p}\right)_3$. Tím jsme, jak brzy uvidíme, dokázali speciální případ zákona kubické reciprocity. Než jej zformulujeme, vybudujeme si další potřebnou – byť na první pohled možná nesouvisící – teorii k jeho důkazu.

1.3 Jacobiho sumy

Poznámka. Připomeňme si definici a základní vlastnosti multiplikativních charakterů a Gaussových součtů.

Nechť p je prvočíslo. *Multiplikativním charakterem modulo p* nazýváme každý grupový homomorfismus $\chi : \mathbb{Z}_p^* \to \mathbb{C}^*$. Triviální charakter značíme ε, platí tedy $\varepsilon (a) = 1 \ \forall a \in \mathbb{Z}_p^*$. Někdy se nám hodí pracovat na celém $\mathbb{Z}_p$, v tom případě klademe $\chi (0) = 0$, je-li $\chi \neq \varepsilon$ a $\varepsilon (0) = 1$. Snadno si lze rozmyslet, že se tím vlastnost homomorfismu zachová. Tato rozšířená definice je proto korektní.

Množina všech charakterů modulo p, kterou značíme $X(\mathbb{Z}_p^*)$, tvoří grupu (vzhledem k násobení). Řádem charakteru χ tedy budeme rozumět jeho řád jakožto prvku této grupy. Inverzním prvkem k χ je sdružený charakter $\overline{\chi}$, kde $\forall t \in \mathbb{Z}_p^* : \overline{\chi} (t) = \overline{\chi (t)}$, jelikož hodnoty χ leží na jednotkové kružnici.

Pro $a \in \mathbb{Z}_p$, $\xi = e^{\frac{2\pi i}{p}}$ primitivní p-tou odmocninu z jedné a χ multiplikativní charakter modulo p nazýváme výraz $g_a(\chi) = \sum_{t \in \mathbb{Z}_p^*} \chi(t)\, \xi^{at}$ *Gaussovým součtem* charakteru χ. Neuvedeme-li dolní index a, budeme implicitně předpokládat $a = 1$.

Libovolný charakter χ splňuje $\overline{\chi(-1)} = \chi(-1)$, neboť $\chi(-1) = \pm 1$. Tudíž

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)\, \xi^t} = \overline{\chi(-1)} \sum_t \overline{\chi}(-t)\, \xi^{-t} = \chi(-1)\, g(\overline{\chi}).$$

V závislosti na hodnotách parametrů a a χ mají Gaussovy součty následující vlastnosti:

- $a = 0$, $\chi = \varepsilon \Rightarrow g_0(\varepsilon) = \sum_{t \in \mathbb{Z}_p^*} \varepsilon(t) = p - 1$,
- $a = 0$, $\chi \neq \varepsilon \Rightarrow g_0(\chi) = \sum_{t \in \mathbb{Z}_p^*} \chi(t) = 0$,
- $a \neq 0$, $\chi = \varepsilon \Rightarrow g_a(\varepsilon) = -1$,
- $a = 1$, $\chi \neq \varepsilon \Rightarrow |g(\chi)| = \sqrt{p}$ (důkaz je uveden v Drápal, str. 38), a tedy $g(\chi)\, g(\overline{\chi}) = \chi(-1)\, g(\chi)\, \overline{g(\chi)} = \chi(-1)\, p$.

Definice. Nechť χ_1, χ_2 jsou multiplikativní charaktery modulo p. *Jacobiho sumu* χ_1 a χ_2 pak definujeme předpisem $J(\chi_1, \chi_2) = \sum_{a+b=1} \chi_1(a)\, \chi_2(b)$, kde $a, b \in \mathbb{Z}_p$.

Následující věta nám ukazuje souvislost mezi Gaussovými a Jacobiho sumami.

Věta 1.10. *Buďte χ, λ netriviální charaktery modulo p takové, že $\chi\lambda \neq \varepsilon$. Potom*

$$J(\chi, \lambda) = \frac{g(\chi)\, g(\lambda)}{g(\chi\lambda)}.$$

Důkaz.

$$\begin{aligned} g(\chi)\, g(\lambda) &= \sum_{u \in \mathbb{Z}_p^*} \chi(u)\, \xi^u \sum_{v \in \mathbb{Z}_p^*} \lambda(v)\, \xi^v \\ &= \sum_u \sum_v \chi(u)\, \lambda(v)\, \xi^{u+v} \\ &= \sum_{t \in \mathbb{Z}_p} \left(\sum_{u+v=t} \chi(u)\, \lambda(v) \right) \xi^t. \end{aligned}$$

Pokud $t = 0$, pak dle předchozí Poznámky a předpokladu $\chi\lambda \neq \varepsilon$ platí $\sum_{u+v=0} \chi(u)\, \lambda(v) = \sum_u \chi(u)\, \lambda(-u) = \lambda(-1) \sum_u \chi\lambda(u) = 0$. Pro každé $t \in \mathbb{Z}_p^*$ definujme $u', v' \in \mathbb{Z}_p$ tak, aby $u = tu'$ a $v = tv'$. Potom

$$\sum_{u+v=t} \chi(u)\, \lambda(v) = \sum_{u'+v'=1} \chi(tu')\, \lambda(tv') = \chi\lambda(t)\, J(\chi, \lambda).$$

Celkem tedy máme

$$g(\chi)\, g(\lambda) = \sum_{t \in \mathbb{Z}_p^*} \chi\lambda(t)\, J(\chi, \lambda)\, \xi^t = J(\chi, \lambda)\, g(\chi\lambda).$$

Jelikož $\chi\lambda \neq \varepsilon$, tak z předchozí Poznámky plyne $g(\chi\lambda) \neq 0$, tudíž můžeme tímto členem dělit a dostaneme požadovaný vztah. □

Důsledek 1.11. *Jsou-li $\chi, \lambda, \chi\lambda \neq \varepsilon$ charaktery modulo p, pak $|J(\chi,\lambda)| = \sqrt{p}$.*

Důkaz. Stačí použít Větu 1.10 a vzít absolutní hodnoty. □

Lemma 1.12. *Nechť χ je multiplikativní charakter modulo p řádu $n > 2$. Potom*

$$g(\chi)^n = p\chi(-1)\prod_{k=1}^{n-2} J\left(\chi, \chi^k\right).$$

Důkaz. Podle Věty 1.10 platí $g(\chi)^2 = J(\chi,\chi)\, g(\chi^2)$. Opakovaným násobením rovnice prvkem $g(\chi)$ a užitím této Věty obdržíme

$$g(\chi)^n = g(\chi)\, g\left(\chi^{n-1}\right)\prod_{k=1}^{n-2} J\left(\chi, \chi^k\right).$$

χ je řádu n, takže $\chi^{n-1} = \chi^{-1} = \overline{\chi}$. Tvrzení teď plyne z poznámky na začátku sekce, neboť $g(\chi)\, g(\chi^{n-1}) = g(\chi)\, g(\overline{\chi}) = \chi(-1)\, p$. □

Poznámka. Nechť p je prvočíslo a $n \in \mathbb{N}$. Z teorie konečných těles víme, že

$$\forall a_1, \ldots, a_k \in \mathbb{Z} : \left(\sum_{i=1}^{k} a_i\right)^{p^n} \equiv \sum_{i=1}^{k} a_i^{p^n} \,(p).$$

Důkaz (pro $k = 2$) lze najít například v Barto a Tůma (2008, Lemma 2.5), zobecnění na libovolné $k > 2$ se provede indukcí. Tvrzení můžeme snadno rozšířit i na okruh celistvých prvků $\mathbb{C}$ nad $\mathbb{Z}$, v němž budeme počítat v následujícím důkazu. Kongruenci v tomto okruhu označme pro lepší přehlednost $\equiv_S$.

Věta 1.13. *Buď $p \equiv 1\,(3)$ prvočíslo a χ kubický (řádu 3) multiplikativní charakter modulo p. Položme $J(\chi,\chi) = a + b\omega$. Pak*

- $a \equiv -1\,(3)$,
- $b \equiv 0\,(3)$.

Důkaz. Předně je potřeba ověřit, že $J(\chi,\chi) \in \mathbb{Z}[\omega]$. χ je řádu 3, takže $\forall t \in \mathbb{Z}_p^*$ platí $\chi(t)^3 = 1$. To znamená, že $\chi(t) \in \{1, \omega, \omega^2\}$. Protože tato množina tvoří multiplikativní grupu a $\omega^2 = -1 - \omega$, tak $J(\chi,\chi) = \sum_{t+u=1} \chi(t)\,\chi(u) \in \mathbb{Z}[\omega]$.

Jelikož pro všechna $t \in \mathbb{Z}_p^*$ jsou $\chi(t)$ i ξ^t celistvé nad $\mathbb{Z}$ (jakožto odmocniny z jedné), tak dle předchozí Poznámky

$$g(\chi)^3 = \left(\sum_{t\in\mathbb{Z}_p^*} \chi(t)\,\xi^t\right)^3 \equiv_S \sum_{t\in\mathbb{Z}_p^*} \chi(t)^3\,\xi^{3t} = \sum_{t\in\mathbb{Z}_p^*} \xi^{3t} = -1\,(3).$$

Dále platí $\chi(-1) = \chi\left((-1)^3\right) = \chi(-1)^3 = 1$, takže $\overline{g(\chi)} = g(\overline{\chi})$ dle poznámky ze začátku sekce. Kombinací tohoto vztahu, Lemmatu 1.12 a kongruence výše získáváme

$$g(\chi)^3 = pJ(\chi,\chi) \equiv_S a + b\omega \equiv_S -1\,(3),$$
$$\overline{g(\chi)^3} = g(\overline{\chi})^3 = pJ(\overline{\chi},\overline{\chi}) \equiv_S a + b\overline{\omega} \equiv_S -1\,(3),$$

což po odečtení dává

$$\begin{aligned} b\,(\omega - \overline{\omega}) &\equiv_S 0\,(3) \\ b\sqrt{-3} &\equiv_S 0\,(3) \\ -3b^2 &\equiv_S 0\,(9) \\ b^2 &\equiv_S 0\,(3)\,. \end{aligned}$$

To znamená, že $3k = b^2$ pro vhodné k celistvé nad $\mathbb{Z}$. Ale $b \in \mathbb{Z}$, takže i $k \in \mathbb{Z}$. Tím pádem $b^2 \equiv b \equiv 0\,(3)$ v $\mathbb{Z}$. Tedy $a + b\omega \equiv a \equiv -1\,(3)$ v okruhu celistvých prvků nad $\mathbb{Z}$, což ze stejného důvodu implikuje $a \equiv -1\,(3)$ v $\mathbb{Z}$. □

1.4 Zákon kubické reciprocity

Jak již víme, existuje 6 invertibilních prvků v okruhu R. Každý prvočinitel je tedy asociovaný se sebou samým a pěti dalšími různými prvočiniteli. Z této šestice vybereme jeden „výjimečný“ prvek.

Definice. Prvočinitel $\pi = a + b\omega \in R$ se nazývá *primární*, pokud $\pi \equiv 2\,(3)$, neboli $a \equiv 2\,(3)$ a $b \equiv 0\,(3)$.

Věta 1.14. *Nechť $\pi = a + b\omega \in R$, $p \equiv 1\,(3)$ prvočíslo takové, že $N\pi = p$. Pak existuje právě jeden primární prvočinitel asociovaný s π.*

Důkaz. Všechny asociované prvky s π jsou:

$$\begin{aligned} \pi &= a + b\omega, \\ -\pi &= -a - b\omega, \\ \omega\pi &= -b + (a - b)\,\omega, \\ -\omega\pi &= b + (b - a)\,\omega, \\ \omega^2\pi &= (b - a) - a\omega, \\ -\omega^2\pi &= (a - b) + a\omega. \end{aligned}$$

Protože $N\pi = a^2 - ab + b^2 = p \equiv 1\,(3)$, stačí rozebrat 6 případů uvedených v následující tabulce (hodnoty jsou modulo 3):

a	b	π	$-\pi$	$\omega\pi$	$-\omega\pi$	$\omega^2\pi$	$-\omega^2\pi$
0	1	ω	2ω	$2+2\omega$	$1+\omega$	1	2
0	2	2ω	ω	$1+\omega$	$2+2\omega$	2	1
1	0	1	2	ω	2ω	$2+2\omega$	$1+\omega$
1	1	$1+\omega$	$2+2\omega$	2	1	2ω	ω
2	0	2	1	2ω	ω	$1+\omega$	$2+2\omega$
2	2	$2+2\omega$	$1+\omega$	1	2	ω	2ω

Vidíme, že v každém řádku je právě jedna hodnota 2, čili existuje právě jeden prvek asociovaný s π, jenž dává zbytek 2 modulo 3, což jsme chtěli dokázat. □

Buď $\pi \in R$ prvočinitel a $p \in \mathbb{Z}$ prvočíslo takové, že $N\pi = p \equiv 1\,(3)$. Věta 1.5 říká, že za těchto podmínek je $R/\pi R \cong \mathbb{Z}_p$. Uvažujme zobrazení $\chi_\pi : R/\pi R \to \mathbb{C}^*$

definované předpisem $\chi_\pi([\alpha]) = \left(\frac{\alpha}{\pi}\right)_3$. Podle Věty 1.9 je χ_π homomorfismus. To nás opravňuje mluvit o kubickém zbytkovém symbolu jako o multiplikativním charakteru modulo p (ve smyslu rozšířené definice, viz Poznámku na začátku sekce 1.3). Díky tomu tedy budeme moci pracovat s Gaussovými i Jacobiho sumami a uplatnit tak teorii vybudovanou v předchozí sekci. Pro lepší přehlednost budeme dále značit $\chi_\pi(\alpha) := \chi_\pi([\alpha])$.

Věta 1.15. *Buď $\pi \in R$ primární prvočinitel, $N\pi = p \equiv 1\,(3)$ prvočíslo. Pak*

$$g(\chi_\pi)^3 = p\pi.$$

Důkaz. Podle Lemmatu 1.12 platí $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$. Stačí proto dokázat, že $J(\chi_\pi, \chi_\pi) = \pi$.

Máme-li libovolný kubický charakter χ modulo p, pak z Důsledku 1.11 plyne $J(\chi,\chi)\,\overline{J(\chi,\chi)} = p$. Kombinací s Větou 1.13 dostáváme, že $J(\chi,\chi)$ je primární prvočinitel s normou p.

Ať tedy π' je primární prvočinitel s normou p, $J(\chi_\pi, \chi_\pi) = \pi'$. Chceme $\pi = \pi'$. Protože $p = \pi\overline{\pi} = \pi'\overline{\pi'}$, tak $\pi \mid \pi'$ nebo $\pi \mid \overline{\pi'}$, resp. $\pi = \pi'$ nebo $\pi = \overline{\pi'}$ (neboť všechny tyto prvočinitele jsou primární téže normy). Potřebujeme ukázat, že nastane první možnost.

Ještě před tím si dokažme malé pozorování. Jestliže $p-1 \nmid n$, kde p je prvočíslo a $n \in \mathbb{N}$, tak $1^n + 2^n + \cdots + (p-1)^n \equiv 0\,(p)$. Označíme-li totiž γ generátor $\mathbb{Z}_p^*$, pak

$$1^n + 2^n + \cdots + (p-1)^n = \gamma^n + \gamma^{2n} + \cdots + \gamma^{(p-1)n} = \gamma^n \frac{\gamma^{(p-1)n} - 1}{\gamma^n - 1} = 0$$

v tělese $\mathbb{Z}_p^*$, neboť $\gamma^{p-1} \equiv 1\,(p)$. Ve druhé rovnosti jsme využili vzorec pro součet geometrické posloupnosti, přičemž $\gamma^n - 1 \not\equiv 0\,(p)$ z předpokladu $p - 1 \nmid n$.

Vraťme se nyní k důkazu Věty. Podle definice máme

$$J(\chi_\pi, \chi_\pi) = \sum_{a+b=1} \chi_\pi(a)\,\chi_\pi(b) = \sum_{a \in \mathbb{Z}_p} \chi_\pi(a)\,\chi_\pi(1-a) \equiv \sum_a a^{\frac{p-1}{3}} (1-a)^{\frac{p-1}{3}} \,(\pi).$$

Poslední sumu si můžeme seskupit dle exponentů a následně aplikovat výše uvedené pozorování, tj.

$$\sum_{a=0}^{p-1} a^{\frac{p-1}{3}} (1-a)^{\frac{p-1}{3}} = \sum_{i=\frac{p-1}{3}}^{\frac{2(p-1)}{3}} \sum_{a=0}^{p-1} c_i a^i = \sum_{i=\frac{p-1}{3}}^{\frac{2(p-1)}{3}} c_i \sum_{a=0}^{p-1} a^i \equiv 0\,(p),$$

kde c_i je koeficient u x^i v polynomu $x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}}$ (předpoklad pozorování je splněn pro každé i, jelikož $0 < \frac{p-1}{3} \le i \le \frac{2(p-1)}{3} < p-1$).

Dohromady máme $J(\chi_\pi, \chi_\pi) \equiv 0\,(p)$. Tím spíš taky $J(\chi_\pi, \chi_\pi) = \pi' \equiv 0\,(\pi)$. Tudíž $\pi \mid \pi'$, a tedy $\pi = \pi'$. □

Poznámka. Gaussovské obory jsou celistvě uzavřené. Jinými slovy, je-li S gaussovský, T jeho podílové těleso a $u \in T$ celistvý nad S, pak $u \in S$. Důkaz lze provést několika snadnými úpravami, viz Růžička (2008, Tvrzení 6.12).

Nyní jsme konečně připraveni dokázat hlavní Větu této kapitoly.

Věta 1.16 (Zákon kubické reciprocity)**.** *Ať π_1, π_2 jsou primární prvočinitele v R, $N\pi_1 \neq N\pi_2$. Pak*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

Důkaz. Nejdřív si rozmysleme, zda má uvedená rovnost vůbec smysl. K tomu, aby byly korektně definovány kubické zbytkové symboly $\left(\frac{\pi_1}{\pi_2}\right)_3$ a $\left(\frac{\pi_2}{\pi_1}\right)_3$, je potřeba $N\pi_1, N\pi_2 \neq 3$. To ale plyne z toho, že jsou π_1 a π_2 primární prvočinitele, neboť je-li $\pi = a + b\omega$ primární, tak $N\pi = a^2 - ab + b^2 \equiv 1\,(3)$. Dále budeme pro kubické zbytkové symboly opět používat značení pomocí multiplikativních charakterů a pro kongruenci v okruhu celistvých prvků nad $\mathbb{Z}$ symbol $\equiv_S$. Rozdělme si nyní důkaz do 3 případů.

(a) Pro $\pi_1, \pi_2 \in \mathbb{Z}$ jsme tvrzení již dokázali v diskuzi za Větou 1.9.

(b) Nechť $\pi_1 \in \mathbb{Z}$, $\pi_2 \notin \mathbb{Z}$. Čili $\pi_1 = q \equiv 2\,(3)$ a $N\pi = p \equiv 1\,(3)$ jsou různá prvočísla, označíme-li $\pi = \pi_2$. Vyjdeme z rovnosti z Věty 1.15:

$$\begin{aligned} g(\chi_\pi)^3 &= p\pi \\ g(\chi_\pi)^{q^2-1} &= (p\pi)^{\frac{q^2-1}{3}} \\ g(\chi_\pi)^{q^2-1} &\equiv \chi_q(p\pi) \pmod{q} \\ g(\chi_\pi)^{q^2} &\equiv_S \chi_q(\pi)\, g(\chi_\pi) \pmod{q}. \end{aligned}$$

Pro přechod od předposledního řádku k poslednímu jsme použili $\chi_q(p\pi) = \chi_q(p)\,\chi_q(\pi) = \chi_q(\pi)$, což plyne z Věty 1.9 a diskuze za ní. Je taky dobré si uvědomit, že poslední kongruence již formálně není v okruhu R. Násobili jsme totiž prvkem $g(\chi_\pi)$, který obecně v R neleží. Proto, podobně jako v důkazu Věty 1.13, musíme počítat v okruhu celistvých prvků nad $\mathbb{Z}$.

Zaměřme se podrobněji na levou stranu kongruence. Protože $q^2 \equiv 1\,(3)$, tak $\chi_\pi(t)^{q^2} = \chi_\pi(t)\ \ \forall t \in \mathbb{Z}_p^*$. Dle Poznámky před Větou 1.13 pak

$$g(\chi_\pi)^{q^2} = \left(\sum_{t\in\mathbb{Z}_p^*} \chi_\pi(t)\,\xi^t\right)^{q^2} \equiv_S \sum_{t\in\mathbb{Z}_p^*} \chi_\pi(t)^{q^2}\,\xi^{q^2 t} = g_{q^2}(\chi_\pi) \pmod{q}.$$

Snadnou úpravou lze odvodit $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})\,g(\chi_\pi) = \chi_\pi(q)\,g(\chi_\pi)$. Dostáváme tedy

$$\begin{aligned} \chi_\pi(q)\,g(\chi_\pi) &\equiv_S \chi_q(\pi)\,g(\chi_\pi) \pmod{q} \\ \chi_\pi(q)\,p &\equiv_S \chi_q(\pi)\,p \pmod{q} \\ \chi_\pi(q) &\equiv_S \chi_q(\pi) \pmod{q}, \end{aligned}$$

kde druhý řádek jsme z prvního získali vynásobením prvkem $\overline{g(\chi_\pi)}$.

Pořád ale máme kongruenci v okruhu celistvých prvků nad $\mathbb{Z}$. Potřebujeme přejít ke kongruenci v okruhu R. Víme tedy, že $\chi_\pi(q) - \chi_q(\pi) = \alpha q$, kde α celistvé nad $\mathbb{Z}$, tím spíš i nad R. Protože $\chi_\pi(q), \chi_q(\pi) \in R$, tak zřejmě α leží v podílovém tělese oboru R. Ten je navíc gaussovský, čímž jsou splněny všechny podmínky tvrzení z předchozí Poznámky. Takže $\alpha \in R$ a tedy $\chi_\pi(q) \equiv \chi_q(\pi) \pmod{q}$ v R. Z Věty 1.7 pak plyne $\chi_\pi(q) = \chi_q(\pi)$.

(c) Konečně ať $\pi_1, \pi_2 \notin \mathbb{Z}$. Tedy $N\pi_1 = p_1 \equiv 1\,(3)$, $N\pi_2 = p_2 \equiv 1\,(3)$, $p_1 \neq p_2$. Navíc $\overline{\pi_1}$ i $\overline{\pi_2}$ jsou primární prvočinitele. Důkaz bude probíhat podobně jako v části *(b)*, některé detaily proto vynecháme. Vyjdeme opět ze vztahu ve Větě 1.15:

$$\begin{aligned} g\left(\chi_{\overline{\pi_1}}\right)^3 &= p_1\overline{\pi_1} \\ g\left(\chi_{\overline{\pi_1}}\right)^{p_2-1} &= \left(p_1\overline{\pi_1}\right)^{\frac{p_2-1}{3}} \\ g\left(\chi_{\overline{\pi_1}}\right)^{p_2-1} &\equiv \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) \pmod{\pi_2} \\ g\left(\chi_{\overline{\pi_1}}\right)^{p_2} &\equiv_S \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) g\left(\chi_{\overline{\pi_1}}\right) \pmod{\pi_2}. \end{aligned}$$

Využitím Poznámky před Větou 1.13 a toho, že $p_2 \equiv 1\,(3)$ získáme

$$g\left(\chi_{\overline{\pi_1}}\right)^{p_2} = \left(\sum_{t\in\mathbb{Z}_{p_1}^*} \chi_{\overline{\pi_1}}(t)\,\xi^t\right)^{p_2} \equiv_S \sum_t \chi_{\overline{\pi_1}}(t)^{p_2}\,\xi^{p_2 t} = g_{p_2}\left(\chi_{\overline{\pi_1}}\right) \pmod{p_2}.$$

Jelikož $\pi_2 \mid p_2$, platí tato kongruence jistě také modulo π_2. Navíc $g_{p_2}\left(\chi_{\overline{\pi_1}}\right) = \chi_{\overline{\pi_1}}\left(p_2^{-1}\right) g\left(\chi_{\overline{\pi_1}}\right) = \chi_{\overline{\pi_1}}\left(p_2^2\right) g\left(\chi_{\overline{\pi_1}}\right)$, takže dohromady máme

$$\begin{aligned} \chi_{\overline{\pi_1}}\left(p_2^2\right) g\left(\chi_{\overline{\pi_1}}\right) &\equiv_S \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) g\left(\chi_{\overline{\pi_1}}\right) \pmod{\pi_2} \\ \chi_{\overline{\pi_1}}\left(p_2^2\right) p_1 &\equiv_S \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) p_1 \pmod{\pi_2} \\ \chi_{\overline{\pi_1}}\left(p_2^2\right) &\equiv_S \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) \pmod{\pi_2} \\ \chi_{\overline{\pi_1}}\left(p_2^2\right) &\equiv \chi_{\pi_2}\left(p_1\overline{\pi_1}\right) \pmod{\pi_2} \\ \chi_{\overline{\pi_1}}\left(p_2^2\right) &= \chi_{\pi_2}\left(p_1\overline{\pi_1}\right). \end{aligned}$$

Analogickým postupem bychom ze vztahu $g\left(\chi_{\pi_2}\right)^3 = p_2\pi_2$ dostali

$$\chi_{\pi_2}\left(p_1^2\right) = \chi_{\pi_1}\left(p_2\pi_2\right).$$

Dále, dle Věty 1.9*(d)*, $\chi_{\overline{\pi_1}}\left(p_2^2\right) = \overline{\chi_{\pi_1}\left(p_2\right)} = \chi_{\overline{\pi_1}}\left(\overline{p_2}\right) = \chi_{\pi_1}\left(p_2\right)$. Kombinací všech tří odvozených vztahů dostaneme

$$\begin{aligned} \chi_{\pi_1}(\pi_2)\,\chi_{\pi_2}\left(p_1\overline{\pi_1}\right) &= \chi_{\pi_1}(\pi_2)\,\chi_{\overline{\pi_1}}\left(p_2^2\right) \\ &= \chi_{\pi_1}(\pi_2)\,\chi_{\pi_1}(p_2) \\ &= \chi_{\pi_1}(\pi_2 p_2) \\ &= \chi_{\pi_2}\left(p_1^2\right) \\ &= \chi_{\pi_2}(\pi_1)\,\chi_{\pi_2}\left(p_1\overline{\pi_1}\right). \end{aligned}$$

Protože $N\pi_1 = p_1 \neq p_2 = N\pi_2$, tak $\pi_2 \nmid p_1\overline{\pi_1}$. Tím pádem je $\chi_{\pi_2}\left(p_1\overline{\pi_1}\right) \neq 0$, takže ním můžeme rovnici vydělit a získáme $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.

□

Princip výpočtu zbytkového symbolu na základě této Věty je jednoduchý. Máme-li $\pi_1, \pi_2 \in R$ splňující její předpoklady, potom $\chi_{\pi_2}(\pi_1) = \chi_{\pi_1}(\pi_2) = \chi_{\pi_1}(\pi_2 \bmod \pi_1)$ a opět můžeme prvky uvnitř charakteru prohodit (jsou-li splněny předpoklady). Tím postupně snižujeme normy obou prvků, až dokud nedojdeme k dostatečně malým, pro něž již výslednou hodnotu určíme přímo. Požadované předpoklady ovšem často splněny nejsou. Řešením tohoto problému se budeme detailněji zabývat v následující sekci.

1.5 Jacobiho kubický zbytkový symbol

Definice. Buď $\alpha \in R$ neinvertibilní, $1-\omega \nmid \alpha$. Ať je $\alpha = \alpha_1 \cdots \alpha_n$ jeho rozklad na (ne nutně různé) prvočinitele. Pak pro každé $\beta \in R$ definujeme *Jacobiho kubický zbytkový symbol* $\chi_\alpha(\beta) = \chi_{\alpha_1}(\beta) \cdots \chi_{\alpha_n}(\beta)$.

Korektnost této definice plyne jednak z rovnosti ideálů $(\alpha) = (u\alpha)$ a norem $N\alpha = N(u\alpha)$ pro libovolné $\alpha, u \in R$, u invertibilní, jednak z jednoznačnosti rozkladu na prvočinitele až na asociovanost.

Dále přirozeným způsobem zavedeme pojem primární prvek.

Definice. Neinvertibilní prvek $\alpha \in R$ se nazývá *primární*, pokud $\alpha \equiv 2\,(3)$.

Věta 1.17. *Každý primární prvek $\alpha \in R$ má jednoznačný primární rozklad, tj. lze jej jednoznačně rozložit na součin ± 1 a primárních prvočinitelů.*

Důkaz. Existují primární prvočinitele $\alpha_1, \ldots, \alpha_n$ a invertibilní prvek u takové, že $\alpha = u\alpha_1 \cdots \alpha_n$. Ty jsou díky Větě 1.14 a tomu, že R je gaussovský, určeny jednoznačně. Jelikož $\forall i \in \{1, \ldots, n\} : \alpha_i \equiv 2 \equiv -1\,(3)$, tak $\alpha_1 \cdots \alpha_n \equiv (-1)^n\,(3)$. Ale $\alpha \equiv -1\,(3)$, čili $u = \pm 1$, což jsme chtěli dokázat. □

Věta 1.18. *Pro každé $\alpha, \beta, \gamma, \delta \in R$, γ, δ neinvertibilní, $1-\omega \nmid \gamma, \delta$ platí:*

(a) $\alpha \equiv \beta\,(\gamma) \Rightarrow \chi_\gamma(\alpha) = \chi_\gamma(\beta)$,

(b) $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\,\chi_\gamma(\beta)$,

(c) $\chi_\gamma(\alpha)\,\chi_\delta(\alpha) = \chi_{\gamma\delta}(\alpha)$,

(d) $\overline{\chi_\gamma(\alpha)} = \chi_\gamma(\alpha)^2 = \chi_{\overline{\gamma}}(\overline{\alpha})$.

Důkaz. Nechť $\gamma = \gamma_1 \cdots \gamma_n$ a $\delta = \delta_1 \cdots \delta_m$ jsou rozklady na prvočinitele.

(a) $\alpha \equiv \beta\,(\gamma) \Rightarrow \forall i : \alpha \equiv \beta\,(\gamma_i) \Rightarrow \forall i : \chi_{\gamma_i}(\alpha) = \chi_{\gamma_i}(\beta) \Rightarrow \chi_\gamma(\alpha) = \chi_\gamma(\beta)$.

(b) $\chi_\gamma(\alpha)\,\chi_\gamma(\beta) = \chi_{\gamma_1}(\alpha\beta) \cdots \chi_{\gamma_n}(\alpha\beta) = \chi_\gamma(\alpha\beta)$.

(c) $\chi_{\gamma\delta}(\alpha) = \chi_{\gamma_1}(\alpha) \cdots \chi_{\gamma_n}(\alpha)\,\chi_{\delta_1}(\alpha) \cdots \chi_{\delta_m}(\alpha) = \chi_\gamma(\alpha)\,\chi_\delta(\alpha)$.

(d) První rovnost plyne z toho, že $\forall x \in \{0, 1, \omega, \omega^2\} : x^2 = \overline{x}$. Využitím Věty 1.9*(d)* získáme $\overline{\chi_\gamma(\alpha)} = \overline{\chi_{\gamma_1}(\alpha)} \cdots \overline{\chi_{\gamma_n}(\alpha)} = \chi_{\overline{\gamma_1}}(\overline{\alpha}) \cdots \chi_{\overline{\gamma_n}}(\overline{\alpha}) = \chi_{\overline{\gamma}}(\overline{\alpha})$.

□

Naším cílem nyní bude určit $\chi_\pi(\lambda)$ pro každé $\pi, \lambda \in R$, π neinvertibilní, $1-\omega \nmid \pi$. Většina úvah bude vycházet z Věty 1.16. Ta má v předpokladech několik omezení na π a λ, které budeme postupně odstraňovat.

Nejdříve ať π, λ jsou obecné (tj. ne nutně primární) prvočinitele. Pro přechod k primárním si stačí uvědomit, že $\chi_{v\pi}(u\lambda) = \chi_\pi(u)\,\chi_\pi(\lambda)$, kde $u, v \in R$ jsou invertibilní. Tutéž úvahu lze samozřejmě aplikovat na jakékoli prvky R, nejen prvočinitele. Nelze ji ale použít v situaci, kdy $1-\omega \mid \lambda$ (neboť $\nexists \lambda' \parallel \lambda$ primární). Tu vyřešíme později.

Podívejme se tedy na invertibilní prvky. Ať $\pi = a + b\omega \in R$ je primární prvočinitel, $N\pi \neq 3$. Zřejmě $1^3 = 1$, $(-1)^3 = -1$, takže $\chi_\pi(1) = \chi_\pi(-1) = 1$

(a to dokonce pro jakékoli $1-\omega \nmid \pi$). Případ $\chi_\pi(\omega)$ je trochu složitější. Označme $a = 3m-1$, $b = 3n$. Pak

$$\frac{N\pi - 1}{3} = \frac{a^2 - ab + b^2 - 1}{3} = \frac{9m^2 - 6m - 9mn + 3n + 9n^2}{3} \equiv m + n\,(3)\,.$$

Tudíž $\chi_\pi(\omega) = \omega^{\frac{N\pi-1}{3}} = \omega^{m+n}$. Hodnoty pro zbylé invertibilní prvky již určíme rychle díky multiplikativitě.

Dále můžeme z Věty 1.16 vypustit předpoklad odlišnosti norem. Když $\pi \parallel \lambda$, potom $\chi_\pi(\lambda) = \chi_\lambda(\pi) = 0$. Podle Věty 1.4 tedy stačí rozebrat pouze možnost $\pi \nparallel \lambda = \overline{\pi}$. Uvažujme $\pi + \overline{\pi} = 2a - b \equiv 1\,(3)$. Pokud $2a - b = 1$, máme

$$\chi_\pi(\overline{\pi}) = \chi_\pi(1-\pi) = \chi_\pi(1) = 1 = \chi_{\overline{\pi}}(1) = \chi_{\overline{\pi}}(1-\overline{\pi}) = \chi_{\overline{\pi}}(\pi)\,.$$

Jinak je $-(\pi+\overline{\pi}) = b - 2a$ primární. Buď tedy $\pi + \overline{\pi} = \pm\alpha_1 \cdots \alpha_n$ primární rozklad. Jistě $\forall i \in \{1,\ldots,n\} : \pi \nparallel \alpha_i \nparallel \overline{\pi}$, čili $N\pi \neq N\alpha_i$. Smíme proto použít Větu 1.16, čím dostaneme

$$\chi_\pi(\pi+\overline{\pi}) = \chi_\pi(\pm 1)\,\chi_\pi(\alpha_1)\cdots\chi_\pi(\alpha_n) = \chi_{\alpha_1}(\pi)\cdots\chi_{\alpha_n}(\pi) = \chi_{\pi+\overline{\pi}}(\pi)\,.$$

Analogicky lze odvodit $\chi_{\overline{\pi}}(\pi+\overline{\pi}) = \chi_{\pi+\overline{\pi}}(\overline{\pi})$. Z toho již plyne

$$\chi_\pi(\overline{\pi}) = \chi_\pi(\pi+\overline{\pi}) = \chi_{\pi+\overline{\pi}}(\pi) = \chi_{\pi+\overline{\pi}}(-\pi) = \chi_{\pi+\overline{\pi}}(\overline{\pi}) = \chi_{\overline{\pi}}(\pi+\overline{\pi}) = \chi_{\overline{\pi}}(\pi)\,.$$

Nyní jsme připraveni odstranit nejvýznamnější omezení Věty 1.16, a sice ireducibilnost π a λ. Částečně se nám to povedlo již v předchozím odstavci, kde jsme ukázali, že $\chi_\pi(\pi+\overline{\pi}) = \chi_{\pi+\overline{\pi}}(\pi)$. Ideu uvedeného důkazu použijeme i v obecné situaci.

Věta 1.19 (Zobecněný zákon kubické reciprocity)**.** *Nechť α, β jsou primární prvky okruhu R. Potom*

$$\chi_\alpha(\beta) = \chi_\beta(\alpha)\,.$$

Důkaz. Buďte $\alpha = \pm\alpha_1\cdots\alpha_n$, $\beta = \pm\beta_1\cdots\beta_m$ primární rozklady. Pak

$$\begin{aligned}
\chi_\alpha(\beta) &= \chi_\alpha(\pm 1)\,\chi_\alpha(\beta_1)\cdots\chi_\alpha(\beta_m)\\
&= \chi_{\alpha_1}(\beta_1)\cdots\chi_{\alpha_1}(\beta_m)\,\chi_{\alpha_2}(\beta_1)\cdots\chi_{\alpha_n}(\beta_m)\\
&= \chi_{\beta_1}(\alpha_1)\cdots\chi_{\beta_m}(\alpha_1)\,\chi_{\beta_1}(\alpha_2)\cdots\chi_{\beta_m}(\alpha_n)\\
&= \chi_\beta(\alpha_1)\cdots\chi_\beta(\alpha_n)\\
&= \chi_\beta(\pm\alpha)\\
&= \chi_\beta(\alpha)\,.
\end{aligned}$$

□

Díky tomuto tvrzení můžeme rozšířit naše poznatky o $\chi_\pi(u)$, kde u je invertibilní, na jakýkoli primární prvek π. Již víme $\chi_\pi(\pm 1) = 1$. Zbývá tedy vyřešit pouze $\chi_\pi(\omega)$. Dokážeme, že jeho hodnotu lze spočítat stejným způsobem jako pro ireducibilní π.

Lemma 1.20. *Nechť $\alpha = 3a - 1 + 3b\omega$, $\alpha_1 = 3a_1 - 1 + 3b_1\omega$, $\alpha_2 = 3a_2 - 1 + 3b_2\omega$ jsou primární prvky R splňující $\alpha = -\alpha_1\alpha_2$. Pak $a \equiv a_1 + a_2\,(3)$, $b \equiv b_1 + b_2\,(3)$.*

Důkaz.

$$\begin{aligned}-\alpha_1\alpha_2 &= -\left(3a_1 - 1 + 3b_1\omega\right)\left(3a_2 - 1 + 3b_2\omega\right)\\ &= 3\left(3b_1b_2 - 3a_1a_2 + a_1 + a_2\right) - 1 + 3\left(b_1 + b_2 - 3a_1b_2 - 3b_1a_2 + 3b_1b_2\right)\omega,\end{aligned}$$

takže $a = 3b_1b_2 - 3a_1a_2 + a_1 + a_2 \equiv a_1 + a_2\,(3)$ a podobně $b \equiv b_1 + b_2\,(3)$. □

Věta 1.21. *Je-li $\pi = a + b\omega \in R$ primární, $a = 3m - 1$, $b = 3n$, tak*

$$\chi_\pi(\omega) = \omega^{m+n}.$$

Důkaz. Budeme postupovat indukcí podle r, kde $\pi = \pm\pi_1 \cdots \pi_r$ je primární rozklad. Pro $r = 1$ již víme. Předpokládejme platnost tvrzení $\forall i \in \{1, \ldots, r\}$. Ať $\pi = \pm\pi_1 \cdots \pi_{r+1}$ je primární rozklad. Rozdělme ho na součin ± 1 a dvou primárních prvků $\pm\pi_1 \cdots \pi_r =: (3m_0 - 1) + 3n_0\omega$ a $\pi_{r+1} =: (3m_{r+1} - 1) + 3n_{r+1}\omega$. Aplikací indukčního předpokladu a Lemmatu 1.20 získáváme

$$\chi_\pi(\omega) = \chi_{\pm\pi_1\cdots\pi_r}(\omega)\,\chi_{\pi_{r+1}}(\omega) = \omega^{m_0+n_0+m_{r+1}+n_{r+1}} = \omega^{m+n}.$$

□

Zbývá odstranit poslední omezení, a sice podmínku $1 - \omega \nmid \lambda$. Ta zaručuje, že $\exists\lambda' \parallel \lambda$ primární. V případě $1 - \omega \mid \lambda$ tedy musíme postupovat jinak. Rozložíme λ na součin $u\lambda'(1-\omega)^k$, kde $u, \lambda' \in R$, u invertibilní, λ' primární, $k \in \mathbb{N}$. To nás dovede k výpočtu $\chi_\pi(1-\omega)$. Ten nejdřív provedeme pro primární celá čísla a poté výsledek rozšíříme na všechny primární prvky.

Věta 1.22 (Doplněk k zákonu kubické reciprocity)**.** *Buď $\pi = a + b\omega \in R$ primární prvek. Označme $a = 3m - 1$. Potom*

$$\chi_\pi(1 - \omega) = \omega^{2m}.$$

Důkaz. Začneme snadným pozorováním. Jestliže $k, l \in \mathbb{Z}$, $k \equiv 2\,(3)$, $(k, l) = 1$, pak $\chi_k(l) = 1$. Podle Věty 1.18*(d)* totiž $\chi_k(l) = \chi_k(l)^2$, což díky předpokladu nesoudělnosti k, l implikuje $\chi_k(l) = 1$.

Pokud $\pi = k \equiv 2\,(3) \in \mathbb{Z}$, tak z tohoto pozorování, vlastností kubického zbytkového symbolu a Věty 1.21 plyne

$$\chi_k(1-\omega) = \chi_k(1-\omega)^4 = \chi_k\left((1-\omega)^2\right)^2 = \chi_k(-3)^2\,\chi_k(\omega)^2 = \chi_k(\omega)^2 = \omega^{2m}.$$

Nechť tedy dále $\pi \notin \mathbb{Z}$. Označme $b = 3n$. Nejdříve vyřešíme případ, kdy je π prvočinitel. Vyjádříme výraz $\chi_\pi(a+b)$ dvěma způsoby. V tom prvním opět použijeme výše uvedené pozorování a taky již dokázané pro $\pi = k \equiv 2\,(3)$. Je-li $a + b = -1$, máme $m + n = 0$, takže $\chi_\pi(a+b) = \chi_\pi(-1) = 1 = \omega^0 = \omega^{2(m+n)}$. Jinak

$$\begin{aligned}\chi_\pi(a+b) &= \chi_{a+b}(\pi) && \text{podle Věty 1.19}\\ &= \chi_{a+b}(a + b + b\omega - b) && \text{přičtením a odečtením } b\\ &= \chi_{a+b}(b(\omega - 1)) && \text{podle Věty 1.18}\textit{(a)}\\ &= \chi_{a+b}(-b)\,\chi_{a+b}(1-\omega) && \text{podle Věty 1.18}\textit{(b)}\\ &= \omega^{2(m+n)} && \text{neboť } (a+b, -b) = (a, b) = 1.\end{aligned}$$

Druhý způsob je založený na vztahu $\chi_\pi(a) = \chi_a(\pi) = \chi_a(b)\,\chi_a(\omega) = \omega^m$ (pro $a = -1$ je $m = 0$, čili $\chi_\pi(a) = \chi_\pi(-1) = 1 = \omega^0 = \omega^m$). Z něj totiž plyne:

$$\begin{aligned}\chi_\pi(a+b) &= \chi_\pi(b(1-\omega)) \\ &= \chi_\pi(b\omega)\,\chi_\pi(\omega)^2\,\chi_\pi(1-\omega) \\ &= \chi_\pi(-1)\,\chi_\pi(a)\,\omega^{2(m+n)}\chi_\pi(1-\omega) \\ &= \omega^{2n}\chi_\pi(1-\omega)\end{aligned}$$

Dohromady dostáváme $\chi_\pi(1-\omega) = \omega^n\chi_\pi(a+b) = \omega^n\omega^{2(m+n)} = \omega^{2m}$.

Tento výsledek nyní zobecníme na libovolné primární $\pi \in R$. Podobně jako ve Větě 1.21 budeme postupovat indukcí podle r, kde $\pi = \pm\pi_1 \cdots \pi_r$ je primární rozklad. Pro $r = 1$ již máme. Ať tvrzení platí $\forall i \in \{1, \ldots, r\}$ a $\pi = \pm\pi_1 \cdots \pi_{r+1}$ je primární rozklad. Rozdělme si ho na součin ± 1 a dvou primárních prvků $\pm\pi_1 \cdots \pi_r =: 3m_0 - 1 + n_0\omega$ a $\pi_{r+1} =: 3m_{r+1} - 1 + n_{r+1}\omega$. Potom dle indukčního předpokladu a Lemmatu 1.20 platí

$$\chi_\pi(1-\omega) = \chi_{\pm\pi_1\cdots\pi_r}(1-\omega)\,\chi_{\pi_{r+1}}(1-\omega) = \omega^{2(m_0+m_{r+1})} = \omega^{2m}.$$

□

Shrňme tedy postup výpočtu $\chi_\beta(\alpha)$ pro libovolné $\alpha, \beta \in R$, $1-\omega \nmid \beta$. Můžeme BÚNO vzít $\alpha := \alpha \bmod \beta$. Pokud $\alpha = 0$ nebo $\alpha \parallel 1$, určíme $\chi_\beta(\alpha)$ přímo. Jinak nalezneme $u \in R$ invertibilní, $k \in \mathbb{N}_0$ a $\alpha', \beta' \in R$ primární, $\beta \parallel \beta'$ takové, že

$$\chi_\beta(\alpha) = \chi_{\beta'}(u)\,\chi_{\beta'}(1-\omega)^k\,\chi_{\beta'}(\alpha').$$

První dva členy spočteme přímo, na třetí aplikujeme Větu 1.19. Tím dostaneme $\chi_{\beta'}(\alpha') = \chi_{\alpha'}(\beta')$ a zopakujeme uvedený postup pro tento symbol.

Na závěr ukažme, jak aplikovat nabyté poznatky o řešitelnosti kongruencí $x^3 \equiv \alpha\,(\beta)$ v okruhu R na problém řešitelnosti $x^3 \equiv a\,(p)$ v $\mathbb{Z}$ (pro p prvočíslo). Diskuzi provedeme v závislosti na možnostech uvedených ve Větě 1.4.

Věta 1.5 nám říká, že pokud $p = 3$ nebo $p \equiv 1\,(3)$, kde $p = \pi\overline{\pi}$ je rozklad na prvočinitele v R, pak $R/\pi R \cong \mathbb{Z}_p$. Z toho tedy plyne, že $x^3 \equiv a\,(p)$ má řešení v $\mathbb{Z}$ právě tehdy, když má $x^3 \equiv a\,(\pi)$ řešení v R. Podle Malé Fermatovy Věty dokonce v případě $p = 3$ existuje takové řešení vždy – stačí vzít $x = a$.

Jestliže $p \equiv 2\,(3)$, je kubickým zbytkem modulo p každé celé číslo. Pro a dělitelné p je to jasné, jinak opět použijeme Malou Fermatovu Větu. Je-li $p = 3k - 1$, tak $a = 1 \cdot a \equiv a^{3k-2} \cdot a^{3k-1} = a^{6k-3} = \left(a^{2k-1}\right)^3 \pmod p$, vezmeme tedy $x = a^{2k-1}$.

2. Bikvadratická reciprocita

Nyní se posuneme o stupeň výš – budeme zkoumat řešení kongruence $x^4 \equiv a \pmod{p}$, přičemž $a \in \mathbb{Z}$, p prvočíslo. V předchozí kapitole jsme pracovali v okruhu $R = \mathbb{Z}[\omega]$, kde $\omega = \frac{-1+\sqrt{-3}}{2}$ je primitivní třetí odmocnina z 1. V této kapitole budeme používat značení $R = \mathbb{Z}[i]$, neboť primitivní čtvrtá odmocnina z 1 je i. Analogicky jako u kubické reciprocity si nejdřív v tomto okruhu vybudujeme základní teorii, poté zavedeme bikvadratický zbytkový symbol a nakonec zformulujeme a dokážeme zákon bikvadratické reciprocity (Věta 2.15). Podíváme se také na rozšiřující teorii vedoucí k výpočtu zbytkového symbolu pro jakékoli prvky okruhu $R = \mathbb{Z}[i]$, pro něž je korektně definovaný.

2.1 Okruh $\mathbb{Z}[i]$

Množina Gaussových celých čísel $\{a + bi;\ a, b \in \mathbb{Z}\}$ tvoří eukleidovský obor $\mathbb{Z}[i]$ s normou $N : \mathbb{Z}[i] \to \mathbb{N}_0$ definovanou pro $\alpha = a + bi \in \mathbb{Z}[i]$ předpisem $N\alpha = \alpha\overline{\alpha} = a^2 + b^2$. Všechny invertibilní prvky v $R = \mathbb{Z}[i]$ jsou právě prvky normy 1 (důkaz stejně jako ve Větě 1.1), čili ± 1 a $\pm i$. Pro každé $\pi \in R$ navíc platí $N\pi = p$ prvočíslo $\Rightarrow$ π prvočinitel (obdoba Věty 1.3). Dále potřebujeme charakterizovat prvočinitele, neboli ireducibilní prvky (v gaussovských oborech tyto pojmy splývají) v R.

Věta 2.1. *Nechť p je prvočíslo.*

(a) Pokud $p = 2$ nebo $p \equiv 1\,(4)$, pak $p = \pi\overline{\pi}$, kde π je prvočinitel v R.

(b) Pokud $p \equiv 3\,(4)$, pak p je prvočinitel v R.

Každý prvočinitel v R je asociovaný s některým z těchto prvočinitelů.

Důkaz.

(a) Je-li $p \equiv 1\,(4)$, pak $(-1)^{\frac{p-1}{2}} = 1$, takže -1 je kvadratický zbytek mod p. Tudíž $\exists x \in \mathbb{Z} : x^2 \equiv -1\,(p)$. V případě $p = 2$ stačí vzít $x = 1$. Potom p dělí $x^2 + 1 = (x - i)(x + i)$. Kdyby byl p prvočinitel, pak by dělil alespoň jeden z těchto činitelů, což zřejmě nemůže nastat. Tedy $p = \pi\lambda$, kde $N\pi, N\lambda > 1$. Znormováním dostaneme $p^2 = N\pi N\lambda$. Z toho plyne $N\pi = \pi\overline{\pi} = p$, takže π je prvočinitel.

(b) Pro spor ať p není prvočinitel. Pak $p = \pi\lambda$, přičemž $N\pi, N\lambda > 1$. Z toho opět dostaneme $N\pi = p$. Je-li $\pi = a + bi$, tak $p = a^2 + b^2$, což je spor, neboť součet dvou čtverců je kongruentní 0, 1, nebo 2 modulo 4.

Zbytek důkazu probíhá podobně jako ve Větě 1.4, neboť Věta 1.2 platí beze změny i pro $R = \mathbb{Z}[i]$. □

2.2 Bikvadratický zbytkový symbol

Jenom pro pořádek připomeňme zavedení pojmu kongruence v $R = \mathbb{Z}[i]$. Nechť $\alpha, \beta, \gamma \in R$. Budeme značit $\alpha \equiv \beta\,(\gamma)$, jestliže $\gamma \mid \alpha - \beta$. Můžeme tedy mimo jiné pracovat s faktorokruhy $R/\alpha R$.

Věta 2.2. *Je-li $\pi \in R$ prvočinitel, pak $R/\pi R$ je těleso s $N\pi$ prvky.*

Důkaz. Analogicky jako v předchozí kapitole ve Větě 1.5. □

Důsledek 2.3. *Nechť $\pi \nmid \alpha$, kde $\alpha, \pi \in R$, π prvočinitel. Pak*

$$\alpha^{N\pi-1} \equiv 1\,(\pi).$$

Důkaz. Podle Věty 2.2 je velikost multiplikativní grupy $(R/\pi R)^*$ rovna $N\pi - 1$. Tvrzení pak plyne z Malé Fermatovy věty. □

Ať $\pi \in R$ je prvočinitel, přičemž $N\pi \neq 2$. Věta 2.1 říká, že buď $\pi\overline{\pi} = N\pi = p \equiv 1\,(4)$, anebo $\pi = q \equiv 3\,(4)$ prvočíslo a pak $N\pi = q^2 \equiv 1\,(4)$. Každopádně ale platí $N\pi \equiv 1\,(4)$. Důležitým poznatkem pro nás je, že $\frac{N\pi-1}{4} \in \mathbb{Z}$.

Věta 2.4. *Nechť $\alpha \in R$. Je-li $\pi \in R$ prvočinitel takový, že $N\pi \neq 2$ a $\pi \nmid \alpha$, potom existuje právě jedno $m \in \{0,1,2,3\}$ splňující $\alpha^{\frac{N\pi-1}{4}} \equiv i^m\,(\pi)$.*

Důkaz. Z Důsledku 2.3 a toho, že $\pm 1, \pm i$ jsou kořeny rovnice $x^4 - 1 = 0$ dostáváme:

$$\pi \mid \alpha^{N\pi-1} - 1 = \left(\alpha^{\frac{N\pi-1}{4}} - 1\right)\left(\alpha^{\frac{N\pi-1}{4}} + 1\right)\left(\alpha^{\frac{N\pi-1}{4}} - i\right)\left(\alpha^{\frac{N\pi-1}{4}} + i\right).$$

Takže π dělí nějaký ze čtyř činitelů na pravé straně. Kdyby dělil alespoň 2 z nich, pak by dělil i jejich rozdíl, tedy 2, $2i$, $1+i$ nebo $1-i$.

Předpokládejme pro spor, že $\pi \mid 2$. Pak $N\pi \mid N(2) = 4$. π není invertibilní, takže $N\pi \neq 1$. Případ $N\pi = 2$ vylučuje předpoklad Věty. Zbývá možnost $N\pi = 4$, ta je ale ve sporu s tím, že π je prvočinitel. Tedy $\pi \nmid 2$. Podobně snadno lze vyloučit i ostatní rozdíly. □

Nyní můžeme korektně zavést bikvadratický zbytkový symbol.

Definice. Nechť $\alpha, \pi \in R$, π prvočinitel, $N\pi \neq 2$. *Bikvadratický zbytkový symbol* $\left(\frac{\alpha}{\pi}\right)_4$ definujeme předpisem

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 0 & \text{pokud } \pi \mid \alpha \\ i^m \equiv \alpha^{\frac{N\pi-1}{4}}\,(\pi), \text{ kde } m \in \{0,1,2,3\} & \text{jinak.} \end{cases}$$

Řekneme, že α je *bikvadratický zbytek modulo* π, jestliže existuje $x \in R$ takové, že $x^4 \equiv \alpha\,(\pi)$. V opačném případě je α *bikvadratický nezbytek modulo* π.

Bikvadratický zbytkový symbol $\left(\frac{\alpha}{\pi}\right)_4$ bude podobně jako ten kvadratický a kubický určovat, zda je α bikvadratickým zbytkem modulo π, či nikoli.

Věta 2.5. *Nechť $\alpha, \pi \in R$, π prvočinitel, $N\pi \neq 2$, $\pi \nmid \alpha$. Pak $\left(\frac{\alpha}{\pi}\right)_4 = 1$ právě tehdy, když má kongruence $x^4 \equiv \alpha\,(\pi)$ řešení v R.*

Důkaz. Probíhá přesně jako ve Větě 1.8. □

Věta 2.6. *Pro každé $\alpha, \beta, \pi \in R$, π prvočinitel, $N\pi \neq 2$ platí:*

(a) $\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N\pi-1}{4}} (\pi)$,

(b) $\alpha \equiv \beta (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$,

(c) $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$,

(d) $\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4$.

Důkaz. Opět zcela analogicky jako v předchozí kapitole, konkrétně ve Větě 1.9.

(a) Pokud $\pi \nmid \alpha$, tvrzení plyne přímo z definice, jinak $\left(\frac{\alpha}{\pi}\right)_4 = 0 \equiv \alpha^{\frac{N\pi-1}{4}} (\pi)$.

(b) $\alpha \equiv \beta (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N\pi-1}{4}} \equiv \beta^{\frac{N\pi-1}{4}} \equiv \left(\frac{\beta}{\pi}\right)_4 (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$, neboť oba symboly můžou nabývat pouze hodnot 0, ± 1, nebo $\pm i$, přičemž každé dvě z nich dávají různý zbytek po dělení π (viz Věta 2.4).

(c) $\left(\frac{\alpha\beta}{\pi}\right)_4 \equiv (\alpha\beta)^{\frac{N\pi-1}{4}} \equiv \alpha^{\frac{N\pi-1}{4}} \beta^{\frac{N\pi-1}{4}} \equiv \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4 \pmod{\pi}$.

(d) Podle části *(a)* a proto, že $N\pi = N\overline{\pi}$ je

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} \equiv \overline{\alpha^{\frac{N\pi-1}{4}}} \equiv \overline{\alpha}^{\frac{N\pi-1}{4}} \equiv \overline{\alpha}^{\frac{N\overline{\pi}-1}{4}} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 \pmod{\overline{\pi}}.$$

□

Definice. Nechť $\alpha, \beta \in R$, β neinvertibilní, $1 + i \nmid \beta$. Buď $\beta = \beta_1 \cdots \beta_n$ rozklad na (ne nutně různé) prvočinitele. Pak definujeme *Jacobiho bikvadratický zbytkový symbol* $\left(\frac{\alpha}{\beta}\right)_4$ předpisem

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{\beta_1}\right)_4 \cdots \left(\frac{\alpha}{\beta_n}\right)_4.$$

Rozklad na prvočinitele je jednoznačný až na asociovanost, nicméně Jacobiho symbol je dobře definovaný, neboť pro libovolné $\gamma \in R$ a $u \parallel 1$ platí jednak $(\gamma) = (u\gamma)$, jednak $N\gamma = N(u\gamma)$. Velice snadno lze také dokázat multiplikativitu v čitateli i jmenovateli či vlastnost $\alpha \equiv \gamma (\beta) \Rightarrow \left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\gamma}{\beta}\right)_4$.

Ve zbytku sekce spočítáme hodnotu (Jacobiho) bikvadratického zbytkového symbolu v některých speciálních případech, které využijeme i v důkazu zákona bikvadratické reciprocity. Nejdřív si ale řekneme něco o primárních prvcích.

Definice. Prvek $\alpha \in R$ se nazývá *primární*, pokud $\alpha \nparallel 1$ a $\alpha \equiv 1 (2 + 2i)$.

Rozhodování, zda je zkoumaný prvek primární, nám často výrazně usnadní následující tvrzení.

Věta 2.7. *Neinvertibilní prvek $\alpha = a + bi \in R$ je primární právě tehdy, když*

- $a \equiv 1 (4) \wedge b \equiv 0 (4)$, *nebo*
- $a \equiv 3 (4) \wedge b \equiv 2 (4)$.

Důkaz. Podle definice je α primární právě tehdy, když $2+2i \mid \alpha - 1$, neboli

$$\frac{a-1+bi}{2+2i} = \frac{a-1+bi}{2+2i} \cdot \frac{2-2i}{2-2i} = \frac{a+b-1}{4} + \frac{b-a+1}{4} i \in R.$$

To ekvivalentně znamená $a+b \equiv a-b \equiv 1\,(4)$, z čeho již snadno plyne tvrzení. □

Věta 2.8. *Ke každému neinvertibilnímu $\alpha \in R$ splňujícímu $1+i \nmid \alpha$ existuje právě jedno invertibilní $u \in R$ takové, že $u\alpha$ je primární.*

Důkaz. Označme $\alpha = a+bi$. Protože

$$1+i \mid \alpha \Leftrightarrow \frac{a+bi}{1+i} = \frac{a+bi}{1+i} \cdot \frac{1-i}{1-i} = \frac{a+b}{2} + \frac{b-a}{2} i \in R \Leftrightarrow a \equiv b\,(2)\,,$$

tak a, b mají různou paritu. Je-li a liché, pak b musí být sudé, a tedy dávat po dělení 4 zbytek 0 nebo 2. V tomto případě platí $b \equiv -b\,(4)$, jeden z dvojice prvků $\alpha, -\alpha$ je proto podle Věty 2.7 primární. Pokud je a sudé a b liché, vynásobením i se dostaneme do předchozí situace. Podobnou úvahou si lze rozmyslet, že kdykoli je $\alpha = a+bi$ primární, pak žádný z prvků $-\alpha, \pm i\alpha$ nemůže být primární. Tím je dokázaná i jednoznačnost. □

Věta 2.9. *Každý primární prvek $\alpha \in R$ má jednoznačný primární rozklad, tj. lze jej jednoznačně rozložit na součin primárních prvočinitelů.*

Důkaz. Obor R je gaussovský a platí Věta 2.8, takže existuje jednoznačný rozklad na primární prvočinitele tvaru $\alpha = u\pi_1 \cdots \pi_j\,(-q_1) \cdots (-q_k)$, $N\pi_i = p \equiv 1\,(4)$, $q_i \equiv 3\,(4)$, $u \parallel 1$. Protože $\alpha \equiv 1\,(2+2i)$, tak $u \equiv 1\,(2+2i)$, a tedy $u = 1$. □

Věta 2.10. *Ať $a, b \in \mathbb{Z}$, $a \neq 0$, b liché, $b \neq \pm 1$, $(a,b) = 1$. Pak $\left(\frac{a}{b}\right)_4 = 1$.*

Důkaz. BÚNO můžeme předpokládat $b > 0$. Je-li $p_1 \cdots p_n$ prvočíselný rozklad b, tak $\left(\frac{a}{b}\right)_4 = \left(\frac{a}{p_1}\right)_4 \cdots \left(\frac{a}{p_n}\right)_4$. Pokud $p_i \equiv 1\,(4)$, což podle Věty 2.1 znamená $p_i = \pi\overline{\pi}$, kde $\pi \in R$ je prvočinitel, potom využitím Věty 2.6*(d)* dostáváme

$$\left(\frac{a}{p_i}\right)_4 = \left(\frac{a}{\pi}\right)_4 \left(\frac{a}{\overline{\pi}}\right)_4 = \left(\frac{a}{\pi}\right)_4 \overline{\left(\frac{a}{\pi}\right)_4} = N\left(\frac{a}{\pi}\right)_4 = 1.$$

Rovněž pro $p_i \equiv 3\,(4)$ platí $\left(\frac{a}{p_i}\right)_4 = 1$, neboť dle Malé Fermatovy věty máme

$$\left(\frac{a}{p_i}\right)_4 \equiv a^{\frac{p_i^2-1}{4}} \equiv \left(a^{p_i-1}\right)^{\frac{p_i+1}{4}} \equiv 1\,(p_i)\,.$$

Tedy $\left(\frac{a}{b}\right)_4 = 1$. □

Věta 2.11. *Pro každý primární prvek $\alpha = a+bi \in R$ platí*

- $\left(\frac{i}{\alpha}\right)_4 = i^{\frac{1-a}{2}} = (-1)^{\frac{1-a}{4}}$,
- $\left(\frac{-1}{\alpha}\right)_4 = (-1)^{\frac{1-a}{2}} = (-1)^{\frac{a-1}{2}}$.

Důkaz. Stačí ukázat první část, druhá je jejím přímým důsledkem.

Předpokládejme nejdřív, že α je prvočinitel. Z definice tedy $\left(\frac{i}{\alpha}\right)_4 = i^{\frac{a^2+b^2-1}{4}}$, takže chceme $a^2+b^2-1 \equiv 2-2a\,(16)$, neboli

$$a^2+2a-3+b^2 = (a-1)(a+3)+b^2 = (a+1)^2+(b-2)(b+2) \equiv 0\,(16).$$

Z druhého tvaru je vidět platnost pro případ $a \equiv 1\,(4)$, $b \equiv 0\,(4)$, z třetího naopak pro $a \equiv 3\,(4)$, $b \equiv 2\,(4)$.

Buďte $\alpha = a+bi$, $\beta = c+di$ primární prvočinitele okruhu R. Potom

$$\left(\frac{i}{\alpha}\right)_4 \left(\frac{i}{\beta}\right)_4 = i^{\frac{1-a}{2}} i^{\frac{1-c}{2}} = i^{\frac{1-a+1-c}{2}},$$

potřebujeme tedy dokázat $2-a-c \equiv 1-ac+bd\,(8)$. Je-li $b \equiv d \equiv 2\,(4)$, pak $bd \equiv 4\,(8)$, jinak $bd \equiv 0\,(8)$. Díky tomu snadno rozebráním všech možností (podle Věty 2.7) ověříme, že kongruence opravdu platí.

Z toho již (použitím jednoduché indukce) plyne tvrzení. □

2.3 Zákon bikvadratické reciprocity

Zaveďme opět značení $\chi_\beta(\alpha) = \left(\frac{\alpha}{\beta}\right)_4$. Je-li totiž $\pi \in R$ prvočinitel takový, že $N\pi = p \equiv 1\,(4)$, pak se na bikvadratický zbytkový symbol modulo π lze na základě Věty 2.2 dívat taky jako na multiplikativní charakter modulo p. To nám umožní počítat s Gaussovými a Jacobiho sumami příslušnými χ_π. Pomocí nich dokážeme pomocná tvrzení, jež budeme potřebovat k důkazu zákona bikvadratické reciprocity.

Lemma 2.12. *Buď $\pi \in R$ prvočinitel, $N\pi = p \equiv 1\,(4)$. Pak*

$$g(\chi_\pi)^4 = pJ(\chi_\pi,\chi_\pi)^2.$$

Důkaz. Podle Věty 1.10 platí $g(\chi_\pi)^2 = J(\chi_\pi,\chi_\pi)\,g(\chi_\pi^2)$, umocněním na druhou dostaneme $g(\chi_\pi)^4 = J(\chi_\pi,\chi_\pi)^2\,g(\chi_\pi^2)^2$. Stačí tedy dokázat $g(\chi_\pi^2)^2 = p$. Jelikož χ_π je řádu 4, tak $\chi_\pi^2 = \overline{\chi_\pi^2}$. Z Poznámky na začátku sekce 1.3 potom plyne

$$g\left(\chi_\pi^2\right)^2 = g\left(\chi_\pi^2\right) g\left(\overline{\chi_\pi^2}\right) = \chi_\pi^2(-1)\,p = (-1)^{\frac{p-1}{2}}\,p = p.$$

□

Lemma 2.13. *Je-li $\pi \in R$ primární prvočinitel, pak $\pi = -\chi_\pi(-1)\,J(\chi_\pi,\chi_\pi)$.*

Důkaz. Označme $N\pi = p \equiv 1\,(4)$. Nejdřív dokážeme, že $\pi \parallel J(\chi_\pi,\chi_\pi)$. Postup bude podobný jako v důkazu Věty 1.15. Z definice máme

$$J(\chi_\pi,\chi_\pi) = \sum_{a+b=1} \chi_\pi(a)\,\chi_\pi(b) = \sum_{a\in\mathbb{Z}_p} \chi_\pi(a)\,\chi_\pi(1-a) \equiv \sum_a a^{\frac{p-1}{4}}(1-a)^{\frac{p-1}{4}}\,(\pi).$$

Poslední sumu si seskupíme dle exponentů a aplikujeme pozorovaní uvedené ve zmíněném důkazu, tj. že pro každé prvočíslo p a $n \in \mathbb{N}$ splňující $p-1 \nmid n$ platí $1^n+2^n+\cdots+(p-1)^n \equiv 0\,(p)$. Dostaneme tedy

$$\sum_{a=0}^{p-1} a^{\frac{p-1}{4}}(1-a)^{\frac{p-1}{4}} = \sum_{i=\frac{p-1}{4}}^{\frac{p-1}{2}} \sum_{a=0}^{p-1} c_i a^i = \sum_{i=\frac{p-1}{4}}^{\frac{p-1}{2}} c_i \sum_{a=0}^{p-1} a^i \equiv 0\,(p),$$

kde c_i je koeficient u x^i v polynomu $x^{\frac{p-1}{4}}(1-x)^{\frac{p-1}{4}}$ (předpoklad pozorování je splněn pro každé i, jelikož $0 < \frac{p-1}{4} \leq i \leq \frac{p-1}{2} < p-1$).

Celkem tedy máme $J(\chi_\pi, \chi_\pi) \equiv 0\,(p)$, tím spíš také $J(\chi_\pi, \chi_\pi) \equiv 0\,(\pi)$. Kromě toho podle Důsledku 1.11 platí $N(J(\chi_\pi, \chi_\pi)) = p$, tudíž opravdu $\pi \parallel J(\chi_\pi, \chi_\pi)$.

Zbývá proto ukázat, že $-\chi_\pi(-1) J(\chi_\pi, \chi_\pi)$ je primární. Uvnitř Jacobiho sumy jsou 2 totožné charaktery, můžeme ji tedy přepsat do tvaru

$$J(\chi_\pi, \chi_\pi) = 2\sum_{a=2}^{\frac{p-1}{2}} \chi_\pi(a)\,\chi_\pi(1-a) + \chi_\pi\left(\frac{p+1}{2}\right)^2.$$

Není těžké spočítat, že $\forall u \in R, u \parallel 1 : u \equiv 1\,(1+i)$, čili rovněž $2u \equiv 2\,(2+2i)$. Tím pádem

$$2\sum_{a=2}^{\frac{p-1}{2}} \chi_\pi(a)\,\chi_\pi(1-a) \equiv 2\left(\frac{p-3}{2}\right) = p-3 \equiv -2 \pmod{2+2i},$$

kde v posledním kroku jsme využili toho, že p je primární (viz Věta 2.7). Navíc

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

takže dohromady máme

$$-\chi_\pi(-1) J(\chi_\pi, \chi_\pi) \equiv -\chi_\pi(-1)(-2+\chi_\pi(-1)) \equiv 2\chi_\pi(-1) - 1 \equiv 1\,(2+2i),$$

jelikož $\chi_\pi(-1) = \pm 1$ a $-3 \equiv 1\,(2+2i)$. Z toho již plyne tvrzení. □

Kombinací předchozích dvou Lemmat získáme následující Větu.

Věta 2.14. *Buď $\pi \in R$ primární prvočinitel, $N\pi = p \equiv 1\,(4)$ prvočíslo. Pak*

$$g(\chi_\pi)^4 = \pi^3\overline{\pi}.$$

Veškerou teorii potřebnou k důkazu zákona bikvadratické reciprocity máme tímto přichystanou. Tvrzení bude oproti zákonu kubické reciprocity (Věta 1.16) obecnější – nebudeme se omezovat na prvočinitele, obsáhneme rovnou i případ rovnosti norem. Na první pohled ale přidáme zásadní požadavek nesoudělnosti. Ve skutečnosti nám to ovšem vůbec nevadí - pro $\alpha, \beta \in R$ primární a soudělné totiž zřejmě platí $\chi_\beta(\alpha) = \chi_\alpha(\beta) = 0$.

Věta 2.15 (Zákon bikvadratické reciprocity)**.** *Ať $\alpha = a + bi$, $\beta = c + di$ jsou primární prvky R, $(\alpha, \beta) = 1$. Pak*

$$\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} = (-1)^{\frac{N\alpha-1}{4}\frac{N\beta-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}.$$

Důkaz. Ověřením všech možností lze zjistit, že $\frac{N\alpha-1}{4}\frac{N\beta-1}{4} \equiv \frac{a-1}{2}\frac{c-1}{2} \equiv \frac{bd}{4}\,(2)$. Dále si důkaz rozdělíme na několik případů.

Předně nechť $\alpha \in \mathbb{Z}$. Protože $b = 0$, dokazujeme $\chi_\beta(\alpha) = \chi_\alpha(\beta)$. Předpokládejme navíc, že $\alpha = p \equiv 1\,(4)$, nebo $\alpha = -q$, $q \equiv 3\,(4)$, kde p, q jsou prvočísla. Je-li $\beta \in \mathbb{Z}$, tvrzení plyne z Věty 2.10. Uvažujme tedy $\beta \notin \mathbb{Z}$.

Začneme případem $\alpha = p \equiv 1\,(4)$, $\beta = \pi$ prvočinitel. Označme $r = N\pi$ (čili r je prvočíslo). Obdobně jako v důkazu zákona kubické reciprocity (Věta 1.16), s pomocí Poznámky před Větou 1.13 odvodíme

$$g\left(\chi_\pi\right)^p \equiv_S \sum_{t\in\mathbb{Z}_r^*} \chi_\pi\left(t\right)^p \xi^{pt} \equiv_S \sum_{t\in\mathbb{Z}_r^*} \chi_\pi\left(t\right)\xi^{pt} = \overline{\chi_\pi\left(p\right)} g\left(\chi_\pi\right) \pmod p.$$

Vynásobením prvkem $g\left(\chi_\pi\right)^3$ a použitím Věty 2.14 dostaneme

$$\begin{aligned} g\left(\chi_\pi\right)^{p+3} &\equiv_S \overline{\chi_\pi\left(p\right)} g\left(\chi_\pi\right)^4 \pmod p \\ \left(\pi^3\overline{\pi}\right)^{\frac{p+3}{4}} &\equiv \overline{\chi_\pi\left(p\right)}\pi^3\overline{\pi} \pmod p. \end{aligned}$$

Protože předpokládáme $(p,\pi) = (p,\overline{\pi}) = 1$, můžeme tuto kongruenci vydělit členem $\pi^3\overline{\pi}$:

$$\left(\pi^3\overline{\pi}\right)^{\frac{p-1}{4}} \equiv \overline{\chi_\pi\left(p\right)} \pmod p.$$

Víme, že $p = \lambda\overline{\lambda}$ pro vhodný prvočinitel $\lambda \in R$. Uvedená kongruence proto platí rovněž modulo λ. Potom tedy máme

$$\begin{aligned} \chi_\lambda\left(\pi^3\right)\chi_\lambda\left(\overline{\pi}\right) &\equiv \overline{\chi_\pi\left(p\right)} \pmod\lambda \\ \chi_\lambda\left(\pi^3\right)\chi_\lambda\left(\overline{\pi}\right) &= \overline{\chi_\pi\left(p\right)} \\ \overline{\chi_\lambda\left(\pi\right)}\chi_\lambda\left(\overline{\pi}\right) &= \overline{\chi_\pi\left(p\right)} \\ \chi_{\overline{\lambda}}\left(\overline{\pi}\right)\chi_\lambda\left(\overline{\pi}\right) &= \overline{\chi_\pi\left(p\right)} \\ \chi_p\left(\overline{\pi}\right) &= \overline{\chi_\pi\left(p\right)} \end{aligned}$$

a požadovaný výsledek získáme komplexním sdružením obou stran rovnosti.

Podobně dokážeme i případ $\alpha = -q$, $q \equiv 3\,(4)$, $\beta = \pi$ prvočinitel, $N\pi = r$. Opět podle Poznámky před Větou 1.13 platí

$$g\left(\chi_\pi\right)^q \equiv_S \sum_{t\in\mathbb{Z}_r^*} \chi_\pi\left(t\right)^q \xi^{qt} \equiv_S \sum_{t\in\mathbb{Z}_r^*} \overline{\chi_\pi\left(t\right)}\xi^{qt} = \chi_\pi\left(q\right) g\left(\overline{\chi_\pi}\right) \pmod q.$$

Z téže Poznámky plyne $\pi^q = (c+di)^q \equiv c^q + (di)^q \equiv c + di^q \equiv c - di = \overline{\pi}\,(q)$. Tím pádem

$$\begin{aligned} g\left(\chi_\pi\right)^{q+1} &\equiv_S \chi_\pi\left(q\right) g\left(\overline{\chi}_\pi\right) g\left(\chi_\pi\right) \pmod q \\ \left(g\left(\chi_\pi\right)^4\right)^{\frac{q+1}{4}} &\equiv_S \chi_\pi\left(q\right)\chi_\pi\left(-1\right) r \pmod q \\ \pi^{\frac{(q+1)(q+3)}{4}} &\equiv \chi_\pi\left(-q\right)\pi^{q+1} \pmod q \\ \pi^{\frac{q^2-1}{4}} &\equiv \chi_\pi\left(-q\right) \pmod q \\ \chi_{-q}\left(\pi\right) &= \chi_\pi\left(-q\right). \end{aligned}$$

Zobecnění na libovolné primární $\alpha, \beta \in R$, $\alpha \equiv 1\,(4) \in \mathbb{Z}$, $\beta \notin \mathbb{Z}$, $(\alpha,\beta) = 1$ je nasnadě. Jestliže $\beta = \beta_1 \cdots \beta_n$ je primární rozklad, $\alpha = p_1 \cdots p_j\,(-q_1)\cdots(-q_k)$, $p_i \equiv 1\,(4)$, $q_i \equiv 3\,(4)$ jsou prvočísla, tak dle výše dokázaného platí

$$\begin{aligned} \chi_\beta\left(\alpha\right) &= \chi_\beta\left(p_1\right)\cdots\chi_\beta\left(-q_k\right) \\ &= \chi_{\beta_1}\left(p_1\right)\cdots\chi_{\beta_n}\left(p_1\right)\chi_{\beta_1}\left(p_2\right)\cdots\chi_{\beta_n}\left(-q_k\right) \\ &= \chi_{p_1}\left(\beta_1\right)\cdots\chi_{p_1}\left(\beta_n\right)\chi_{p_2}\left(\beta_1\right)\cdots\chi_{-q_k}\left(\beta_n\right) \\ &= \chi_{p_1}\left(\beta\right)\cdots\chi_{-q_k}\left(\beta\right) \\ &= \chi_\alpha\left(\beta\right). \end{aligned}$$

Zbývá tedy vyřešit situaci $\alpha, \beta \notin \mathbb{Z}$. Předpokládejme navíc $(a,b) = (c,d) = 1$. Tím pádem také $(a,\alpha) = (b,\alpha) = (c,\beta) = (d,\beta) = 1$. Z toho dále můžeme vyvodit $(c\alpha,\beta) = 1$, což díky kongruenci $c\alpha \equiv ac + bd\,(\beta)$ znamená $(ac+bd,\beta) = 1$. Obdobně, pomocí $a\beta \equiv ac + bd\,(\alpha)$, lze ukázat $(ac+bd,\alpha) = 1$. Platí tedy taky $(ac+bd,\overline{\alpha}) = 1$, takže $1 = (ac+bd,\overline{\alpha}\beta) = (ac+bd, ac+bd+(ad-bc)\,i) = (ac+bd, ad-bc)$. Z uvedených kongruencí plyne též

$$\chi_\beta(c)\,\chi_\beta(\alpha) = \chi_\beta(ac+bd)$$
$$\chi_\alpha(a)\,\chi_\alpha(\beta) = \chi_\alpha(ac+bd)\,.$$

Vynásobením první rovnice komplexně sdruženou druhou rovnicí získáme

$$\chi_\beta(c)\,\chi_\beta(\alpha)\,\overline{\chi_\alpha(a)\chi_\alpha(\beta)} = \chi_{\overline{\alpha}\beta}(ac+bd)$$
$$\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} = \chi_{\overline{\beta}}(c)\,\chi_\alpha(a)\,\chi_{\overline{\alpha}\beta}(ac+bd)\,.$$

Položme $A, C = \pm 1$ tak, aby $A \equiv a\,(4)$, $C \equiv c\,(4)$. Lze tedy brát $A = (-1)^{\frac{a-1}{2}}$, $C = (-1)^{\frac{c-1}{2}}$. Za těchto podmínek platí $Aa \equiv Cc \equiv AC\,(ac+bd) \equiv 1\,(4)$, neboť $bd \equiv 0\,(4)$ (viz Věta 2.7). Tudíž

$$\begin{aligned}\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} &= \chi_{\overline{\beta}}(Cc)\,\chi_\alpha(Aa)\,\chi_{\overline{\alpha}\beta}(AC\,(ac+bd))\,\chi_\alpha(A)\,\chi_{\overline{\beta}}(C)\,\chi_{\overline{\alpha}\beta}(AC)\\ &= \chi_{\overline{\beta}}(Cc)\,\chi_\alpha(Aa)\,\chi_{\overline{\alpha}\beta}(AC\,(ac+bd))\,\chi_{\overline{\alpha}}(C)\,\chi_\beta(A)\\ &= \chi_{\overline{\beta}}(Cc)\,\chi_\alpha(Aa)\,\chi_{\overline{\alpha}\beta}(AC\,(ac+bd))\,,\end{aligned}$$

protože $\chi_{\overline{\alpha}}(C)\,\chi_\beta(A) = (-1)^{\frac{c-1}{2}\frac{a-1}{2}}\,(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = 1$ podle Věty 2.11.

Jsou-li a, c, $ac+bd$ neinvertibilní, tak díky již dokázané části a Větě 2.10 je

$$\chi_{\overline{\beta}}(Cc) = \chi_{Cc}\left(\overline{\beta}\right) = \chi_c(c-di) = \chi_c(-di) = \chi_c(i)\,,$$
$$\chi_\alpha(Aa) = \chi_{Aa}(\alpha) = \chi_a(a+bi) = \chi_a(bi) = \chi_a(i)\,,$$
$$\chi_{\overline{\alpha}\beta}(AC\,(ac+bd)) = \chi_{AC(ac+bd)}(\overline{\alpha}\beta) = \chi_{ac+bd}((ad-bc)\,i) = \chi_{ac+bd}(i)\,.$$

Celkem tedy máme $\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} = \chi_{ac(ac+bd)}(i) = (-1)^{\frac{ac(ac+bd)-1}{4}}$. Takže potřebujeme ukázat $ac\,(ac+bd) - 1 \equiv bd\,(8)$. Pokud $bd \equiv 0\,(8)$, kongruence se redukuje na $(ac)^2 \equiv 1\,(8)$, pokud $bd \equiv 4\,(8)$, dostáváme $(ac+2)^2 \equiv 1\,(8)$. Obě kongruence jsou rozhodně platné, neboť čtverec lichého čísla dává po dělení 8 vždy zbytek 1. Čili $\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} = (-1)^{\frac{bd}{4}}$.

Co když je některý z prvků a, c, $ac+bd$ invertibilní? Určitě to nemůžou být všechny tři zároveň. Řešení ilustrujeme na případě $a, c = \pm 1$. Tehdy platí $\chi_{\overline{\beta}}(Cc) = \chi_\alpha(Aa) = 1$, takže $\chi_\beta(\alpha)\,\overline{\chi_\alpha(\beta)} = \chi_{ac+bd}(i) = \chi_{ac(ac+bd)}(i)$ a opět jsme v situaci jako výše.

Konečně ať $(a,b) = m$, $(c,d) = n$. Z Věty 2.7 vyplývá, že m, n jsou kongruentní 1 nebo 3 modulo 4. Nastane-li druhá možnost, můžeme položit $m := -m$, resp. $n := -n$. Tedy $m \equiv n \equiv 1\,(4)$ a $\alpha = m\alpha'$, $\beta = n\beta'$ pro nějaké primární $\alpha' = a' + b'i$, $\beta' = c' + d'i$, přičemž $(a',b') = (c',d') = (m,n) = 1$. Potom

$$\begin{aligned}\chi_\beta(\alpha) &= \chi_n(m)\,\chi_n(\alpha')\,\chi_{\beta'}(m)\,\chi_{\beta'}(\alpha')\\ &= \chi_m(n)\,\chi_{\alpha'}(n)\,\chi_m(\beta')\,\chi_{\alpha'}(\beta')\,(-1)^{\frac{b'd'}{4}}\\ &= \chi_\alpha(\beta)\,(-1)^{\frac{b'}{2}\cdot\frac{d'}{2}}\\ &= \chi_\alpha(\beta)\,(-1)^{\frac{b}{2}\cdot\frac{d}{2}}\,,\end{aligned}$$

neboť $b = mb' \equiv b'\,(4)$, $d = nd' \equiv d'\,(4)$. Tím je důkaz celého tvrzení ukončen. □

Nyní už umíme počítat $\chi_\beta(\alpha)$ téměř ve všech případech, kdy je tento výraz korektně definovaný, a to především pomocí Věty 2.15 nebo Věty 2.11. Jediná situace, se kterou si ještě nedovedeme poradit, je když $1+i \mid \alpha$. Pak totiž neexistuje primární prvek asociovaný s α. Tato situace nás přivede přivede k výpočtu $\chi_\alpha(1+i)$. Můžeme samozřejmě počítat podle definice, existuje ovšem tvrzení, které nám to ve většině případů výrazně urychlí. Závěrečná část této kapitoly bude věnována jeho odvození.

Věta 2.16. *Buď $\alpha = a + bi \in R$ primární, $(a,b) = 1$. Potom*

$$\chi_\alpha(a) = \begin{cases} i^{\frac{a-1}{2}} & \text{pokud } a \equiv 1\,(4)\,,\ b \equiv 0\,(4) \\ -i^{\frac{a+1}{2}} & \text{pokud } a \equiv 3\,(4)\,,\ b \equiv 2\,(4)\,. \end{cases}$$

Důkaz. Pro $a = 1$ zřejmé, pro $a = -1$ plyne z Věty 2.11. Můžeme tedy předpokládat, že $a \neq \pm 1$. Jestliže $a \equiv 1\,(4)$, $b \equiv 0\,(4)$, tak

$$\chi_\alpha(a) = \chi_a(\alpha) = \chi_a(a+bi) = \chi_a(bi) = \chi_a(b)\,\chi_a(i) = i^{\frac{1-a}{2}} = i^{\frac{a-1}{2}}.$$

Podobně, nastane-li druhá možnost, dostaneme

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

V obou výpočtech jsme využili Větu 2.10, Větu 2.11 a Větu 2.15. □

Lemma 2.17. *Nechť $s_1, \ldots, s_k \in \mathbb{Z}$, $s_i \equiv 1\,(4)$ pro každé $i \in \{1, \ldots, k\}$. Pak*

$$\frac{s_1 - 1}{4} + \cdots + \frac{s_k - 1}{4} \equiv \frac{s_1 \cdots s_k - 1}{4}\,(4)\,.$$

Důkaz. Indukcí podle k. Pro $k = 1$ triviální. Buď tedy $k > 1$ a předpokládejme platnost tvrzení pro $k-1$. Potom

$$\begin{aligned} \frac{s_1 \cdots s_k - s_1 - \cdots - s_k + k - 1}{4} &\equiv \frac{s_k(s_1 \cdots s_{k-1} - 1) - s_1 - \cdots - s_{k-1} + k - 1}{4} \\ &\equiv \frac{s_k(s_1 \cdots s_{k-1} - 1)}{4} - \frac{s_1 - 1}{4} - \cdots - \frac{s_{k-1} - 1}{4} \\ &\overset{\text{IP}}{\equiv} \frac{s_k(s_1 \cdots s_{k-1} - 1)}{4} - \frac{s_1 \cdots s_{k-1} - 1}{4} \\ &\equiv (s_k - 1)\,\frac{s_1 \cdots s_{k-1} - 1}{4} \equiv 0 \pmod 4\,, \end{aligned}$$

takže tvrzení platí i pro k. □

Věta 2.18 (Doplněk k zákonu bikvadratické reciprocity)**.** *Jestliže $\alpha = a + bi$ je primární prvek okruhu R, pak*

$$\chi_\alpha(1+i) = i^{\frac{a-b-b^2-1}{4}}.$$

Důkaz. Nejdřív nechť $\alpha = p \equiv 1\,(4)$ prvočíslo. Na základě Věty 2.1 je pak

$$\chi_p(1+i) = \chi_\pi(1+i)\,\chi_{\overline{\pi}}(1+i) = \chi_\pi(i)\,\chi_\pi(1-i)\,\chi_{\overline{\pi}}(1+i)$$

pro nějaký prvočinitel $\pi \in R$. Všimněme si, že $\chi_\pi(1-i) = \overline{\chi_{\overline{\pi}}(1+i)}$. Tím pádem dostáváme $\chi_p(1+i) = \chi_\pi(i)$, což je z definice rovno $i^{\frac{p-1}{4}}$.

Dále uvažme $\alpha = -q$, $q \equiv 3\,(4)$ prvočíslo. Protože $\forall j \in \mathbb{Z}_q^* : q \mid \binom{q}{j}$, z binomické věty nám vyplývá $(1+i)^q \equiv 1^q + i^q \equiv 1 - i\,(q)$. Zřejmě $(1+i, q) = 1$, neboť se jedná o různá (neasociovaná) prvočísla. Můžeme tedy kongruenci vydělit prvkem $1+i$, čím získáme $(1+i)^{q-1} \equiv -i \equiv i^{-1}\,(q)$. Tudíž

$$\chi_{-q}(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} \equiv \left((1+i)^{q-1}\right)^{\frac{q+1}{4}} \equiv \left(i^{-1}\right)^{\frac{q+1}{4}} \equiv i^{\frac{-q-1}{4}}\,(q)\,.$$

Nyní buď $\alpha = p_1 \cdots p_n\,(-q_1) \cdots (-q_m)$, $p_i \equiv 1\,(4)$, $q_i \equiv 3\,(4)$ prvočísla. Pak

$$\begin{aligned}\chi_\alpha(1+i) &= \chi_{p_1}(1+i) \cdots \chi_{p_n}(1+i)\,\chi_{-q_1}(1+i) \cdots \chi_{-q_m}(1+i)\\ &= i^{\frac{p_1-1}{4}+\cdots+\frac{p_n-1}{4}+\frac{-q_1-1}{4}+\cdots+\frac{-q_m-1}{4}}\\ &= i^{\frac{p_1\cdots p_n(-q_1)\cdots(-q_m)-1}{4}}\end{aligned}$$

podle Lemmatu 2.17.

Tím je situace $\alpha \in \mathbb{Z}$ hotová. Nechť tedy $\alpha \notin \mathbb{Z}$. Je-li navíc $(a, b) = 1$, tak

$$\begin{aligned}\chi_\alpha(a)\,\chi_\alpha(1+i) &= \chi_\alpha(a+ai) = \chi_\alpha(a+b+i(a+bi)) = \chi_\alpha(a+b) = \chi_{a+b}(\alpha)\\ &= \chi_{a+b}(a+bi) = \chi_{a+b}(bi-b) = \chi_{a+b}(b)\,\chi_{a+b}(i-1)\\ &= \chi_{a+b}(i-1) = \chi_{a+b}(i)\,\chi_{a+b}(1+i)\\ &= i^{\frac{1-a-b}{2}} \cdot i^{\frac{a+b-1}{4}} = i^{\frac{1-a-b}{4}},\end{aligned}$$

pokud $a + b \neq 1$. Jinak $\chi_\alpha(a)\,\chi_\alpha(1+i) = \chi_\alpha(a+b) = 1 = i^{\frac{1-a-b}{4}}$. Z toho na základě Věty 2.16 plyne, že

$$\chi_\alpha(1+i) = \begin{cases} i^{\frac{1-a-b}{4}-\frac{a-1}{2}} = i^{\frac{3-3a-b}{4}} & \text{pokud } a \equiv 1\,(4)\,,\ b \equiv 0\,(4)\\ -i^{\frac{1-a-b}{4}-\frac{a+1}{2}} = i^{\frac{7-3a-b}{4}} & \text{pokud } a \equiv 3\,(4)\,,\ b \equiv 2\,(4)\,.\end{cases}$$

V prvním případě potřebujeme dokázat $3-3a-b \equiv a-b-b^2-1\,(16)$. Jelikož $b \equiv 0\,(4)$, tak $b^2 \equiv 0\,(16)$. Dostáváme tedy ekvivalentní kongruenci $4 \equiv 4a\,(16)$, neboli $a \equiv 1\,(4)$, což předpokládáme.

Jestliže $a \equiv 3\,(4)$, $b \equiv 2\,(4)$, pak $b^2 \equiv 4\,(16)$. Proto $7-3a-b \equiv a-b-b^2-1\,(16)$ právě tehdy, když $12 \equiv 4a\,(16)$, resp. $a \equiv 3\,(4)$.

Zbývá už jenom zobecnění na $(a, b) = k$. BÚNO uvažujme $k \equiv 1\,(4)$. To lze, neboť možnosti $k \equiv 0\,(4)$ a $k \equiv 2\,(4)$ vylučuje Věta 2.7 a pro $k \equiv 3\,(4)$ vezmeme $k := -k$. Je-li tedy $\alpha = k\alpha'$, $\alpha' = c + di$ primární (přičemž $(c, d) = 1$), potom

$$\chi_\alpha(1+i) = \chi_k(1+i)\,\chi_{\alpha'}(1+i) = i^{\frac{k-1}{4}} \cdot i^{\frac{c-d-d^2-1}{4}} = i^{\frac{k+c-d-d^2-2}{4}}.$$

Chceme $a-b-b^2-1 = kc-kd-(kd)^2-1 \equiv k+c-d-d^2-2\,(16)$. Ekvivalentně můžeme dokazovat

$$\begin{aligned}c(k-1) - d(k-1) - d^2\left(k^2-1\right) - k + 1 &\equiv 0\,(16)\,,\\ (k-1)\left(c - d - d^2(k+1) - 1\right) &\equiv 0\,(16)\,.\end{aligned}$$

Získanou kongruenci ověříme pouhým rozebráním všech možností. V případě $k \equiv 1\,(16)$ je to zřejmé. Pokud $k \equiv 5\,(16)$, nebo $k \equiv 13\,(16)$, dojdeme ke tvaru

$4\,(c-d-6d^2-1) \equiv 0\,(16)$, resp. $-4\,(c-d-14d^2-1) \equiv 0\,(16)$. Každopádně ale dostáváme $c-d+2d^2-1 \equiv 0\,(4)$, což je jasné díky vztahu $c-d \equiv 1\,(4)$. Také pro $k \equiv 9\,(16)$ je ověření snadné - vede totiž ke kongruenci $c+d+1 \equiv 0\,(2)$, která nepochybně platí.

Celkem tedy máme

$$\chi_\alpha\,(1+i) = i^{\frac{k+c-d-d^2-2}{4}} = i^{\frac{kc-kd-(kd)^2-1}{4}} = i^{\frac{a-b-b^2-1}{4}},$$

takže tvrzení je nyní kompletně dokázané. □

Výpočet $\chi_\beta\,(\alpha)$ pro libovolné $\alpha, \beta \in R$, $1+i \nmid \beta$ je analogický jako v kubickém případě. Předně můžeme BÚNO brát $\alpha := \alpha \bmod \beta$. Pokud $\alpha = 0$ nebo $\alpha \parallel 1$, určíme $\chi_\beta\,(\alpha)$ přímo. Jinak najdeme invertibilní prvek $u \in R$, $k \in \mathbb{N}_0$ a $\alpha', \beta' \in R$ primární, $\beta \parallel \beta'$ takové, že

$$\chi_\beta\,(\alpha) = \chi_{\beta'}\,(u)\,\chi_{\beta'}\,(1+i)^k\,\chi_{\beta'}\,(\alpha')\,.$$

První dva členy umíme spočítat přímo, na třetí použijeme Větu 2.15. Tedy $\chi_{\beta'}\,(\alpha') = (-1)^{\frac{N\alpha'-1}{4}\frac{N\beta'-1}{4}}\,\chi_{\alpha'}\,(\beta')$. Hodnotu $\chi_{\alpha'}\,(\beta')$ zjistíme zopakováním uvedeného postupu.

Závěrem se podívejme, co jsme zjistili o řešitelnosti kongruence $x^4 \equiv a\,(p)$ v $\mathbb{Z}$ (pro p prvočíslo). Uvažujme jednotlivé možnosti na základě Věty 2.1.

Je-li $p = 2$ nebo $p \equiv 1\,(4)$, přičemž $p = \pi\overline{\pi}$ je rozklad na prvočinitele, pak podle Věty 2.2 máme $R/\pi R \cong \mathbb{Z}_p$, takže $x^4 \equiv a\,(p)$ má řešení v $\mathbb{Z}$ právě tehdy, když ho má $x^4 \equiv a\,(\pi)$ v R. Speciálně pro $p = 2$ řešení zřejmě existuje vždycky.

Nechť $p \equiv 3\,(4)$. Pokud $p \mid a$, pak je zřejmě a bikvadratickým zbytkem modulo p. Jinak je $x^4 \equiv a\,(p)$ řešitelná v $\mathbb{Z} \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1\,(p)$, což nastává právě tehdy, když je a kvadratickým zbytkem modulo p (první ekvivalenci lze odvodit poměrně snadno z vlastností cyklických grup, důkaz viz např. Ireland a Rosen (2013, Tvrzení 7.1.2)). To, zda jím je, už ale umíme zjistit pomocí teorie kvadratických zbytků, zejména zákona kvadratické reciprocity.

Závěr

Ačkoli bylo primárním cílem dokázat kubický a bikvadratický zákon reciprocity, nezůstalo jen u toho a podívali jsme se na věc širším pohledem. Poukázali jsme na problém řešitelnosti celočíselných kongruencí $x^n \equiv a\,(p)$ pro prvočíslo p a pevně zvolené $n \in \mathbb{N}$ (v našem případě rovno 3 nebo 4), který byl hlavním důvodem podrobného zkoumání reciprocních zákonů. Proto jsme navíc uvedli doplňující teorii nezbytnou k jeho vyřešení, a to jak u kubické, tak bikvadratické reciprocity.

Celá práce přinesla i několik vedlejších výsledků. Důkazy, k nimž jsme směřovali, vyžadovali hlubší poznatky o okruzích $\mathbb{Z}[\omega]$ a $\mathbb{Z}[i]$. Kromě toho bylo potřeba využít netriviálních vlastností Gaussových a Jacobiho sum. V neposlední řadě již taky umíme rozhodnout, zda jsou řešitelné kongruence $x^3 \equiv \alpha\,(\beta)$ v $\mathbb{Z}[\omega]$, resp. $x^4 \equiv \alpha\,(\beta)$ v $\mathbb{Z}[i]$.

Uvedená teorie kubické a bikvadratické reciprocity poskytuje dobrý základ k dalšímu studiu v oblasti reciprocních zákonů. Jedná se především o různá zobecnění, jako například Eisensteinův nebo Artinův zákon reciprocity, ale také tzv. racionální reciproční zákony, které se zabývají zbytkovými symboly lišícími se pouze o znaménko. To už ovšem výrazně překračuje rozsah této práce.

Seznam použité literatury

Barto, L. a Tůma, J. (2008). Konečná tělesa. URL http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf.

Drápal, A. Teorie čísel. URL http://www.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf.

Ireland, K. a Rosen, M. (2013). *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media.

Růžička, P. (2008). Celistvost a dedekindovy obory. URL http://www.karlin.mff.cuni.cz/~ruzicka/komalg/celistvost.pdf.