UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA
KATEDRA ALGEBRY A GEOMETRIE

DIPLOMOVÁ PRÁCE

Charaktery v teorii čísel, kubický a bikvadratický zákon vzájemnosti

Vedoucí diplomové práce:
Prof. Mgr. Radomír Halaš, Dr.
Rok odevzdání: 2014

Vypracoval:
Jan Mlčůch
M-DG, II. ročník

Prohlášení

Prohlašuji, že jsem vytvořil tuto bakalářskou práci samostatně za vedení Prof. Mgr. Radomíra Halaše, Dr. a že jsem v seznamu použité literatury uvedl všechny zdroje použité při zpracování práce.

V Olomouci dne 10. července 2014

Poděkování

Rád bych na tomto místě poděkoval vedoucímu diplomové práce Prof. Mgr. Radomíru Halašovi, Dr. za obětavou spolupráci i za čas, který mi věnoval při konzultacích.

Obsah

Úvod

Tato práce se zabývá kvadratickým, kubickým a bikvadratickým zákonem vzájemnosti. Tímto tématem se začali zabývat matematici v období druhé poloviny 18. století a zájem o toto téma přetrvává do dneška. Kvadratický zákon vzájemnosti se dnes běžně vyučuje v kurzech algebry a stále se objevují nové důkazy tohoto matematického tvrzení. K dnešnímu dni jich je evidováno na 246.

Tato práce vychází ze základního kurzu teorie čísel a navazuje na něj. Předpokládá se znalost algebraických struktur a celočíselných kongruencí, v rozsahu požadovaném v těchto přednáškách. Použito je standardní značení, tak jak se s ním setkáváme ve většině prací zaměřených na algebru.

Text práce je rozdělen do pěti kapitol. První dvě kapitoly jsou spíše opakovacího rázu. V té první jsou zopakovány základní pojmy z teorie algebry, o kterých se v textu hovoří. Tato kapitola je pojata velice stručně a vychází z úvodních kapitol učebního textu [2]. Druhá kapitola je zaměřena na speciální vlastnosti oborů integrity $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}[\omega]$. Jedná se o vlastnosti norem a o tvary jednotek v těchto algebraických strukturách.

Zbylé tři kapitoly se věnují již zmiňovaným zákonům vzájemnosti. Třetí kapitola se zabývá řešitelností kongruenčních rovnic druhého řádu. Je v ní k tomuto účelu dokázáno Gaussovo lemma a kvadratický zákon vzájemnosti. Kapitola je doplněna o několik příkladů ukazujících aplikaci zmíněné teorie při početní praxi.

Čtvrtá kapitola, zabývající se kubickým zákonem vzájemnosti, je rozsahově největší. Jsou v ní rozšířeny znalosti o oboru integrity $\mathbb{Z}[\omega]$ a vybudován potřebný aparát sloužící k řešení kongruenčních rovnic třetího řádu. Konkrétně rovnic typu $x^3 \equiv a\,(mod\ p)$. Rozhodnout o řešitelnosti těchto typů rovnic nám umožní kubický zákon vzájemnosti, který najdeme na konci této kapitoly. Text je doplněn o několik ukázkových příkladů, umožňujících procvičení popsané teorie.

Závěrečná kapitola se zabývá bikvadratickým zákonem vzájemnosti. Jde vlastně o zobecnění již uvedených zákonů a tomu také odpovídá rozsah a struktura kapitoly. Většina vět a tvrzení je zde analogická předchozím kapitolám. Kapitola

začíná rozšířením vlastností oboru integrity $\mathbb{Z}[i]$ a pokračuje přes bikvadratický zákon vzájemnosti až k několika řešeným příkladům, ukazujícím praktické využití získaných znalostí.

1 Základní pojmy

Uveďme na úvod několik základních pojmů a tvrzení, se kterými budeme v dalších kapitolách pracovat.

Grupa

Definice 1.1 Algebraická struktura $\mathcal{G} = (G, \cdot)$ se nazývá *grupoid*.

Definice 1.2 Prvek $e \in G$ se nazývá *jednotkovým prvkem* grupoidu $\mathcal{G}$, jestliže pro libovolné $a \in G$ platí $e \cdot a = a \cdot e = a$.

Definice 1.3 Grupoid $\mathcal{G} = (G, \cdot)$ se nazývá *grupa*, jestliže je asociativní, má jednotkový prvek a k libovolnému jeho prvku existuje prvek inverzní.

Definice 1.4 Buď $\mathcal{G} = (G, \cdot)$ grupa, H podmnožina množiny G. Řekneme, že H je *podgrupa* grupy $\mathcal{G}$, jestliže platí, že H je uzavřená vzhledem k násobení, obsahuje jednotkový prvek a ke každému svému prvku a obsahuje i inverzní prvek a^{-1}.

Definice 1.5 Buď M podmnožina grupy $\mathcal{G}$. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy $\mathcal{G}$ obsahujících množinu M. Tedy nejmenší podgrupu grupy $\mathcal{G}$ obsahující množinu M. Množinu M nazýváme množinou generátorů grupy $\langle M \rangle$. Je-li množina $M = \{a\}$ jednoprvková, potom grupu $\langle a \rangle$ nazveme cyklickou.

Okruh

Definice 1.6 Algebraickou strukturu $\mathcal{R} = (R, +, \cdot, 0)$ se dvěma binárními operacemi + a $\cdot$, kde $(R, +, 0)$ je komutativní grupa, $(R, \cdot)$ je pologrupa a operace $\cdot$ je distributivní vzhledem k operaci + nazýváme *okruh*.

Definice 1.7 Okruh $\mathcal{R} = (R, +, \cdot, 0)$ nazveme *komutativní*, je-li $(R, \cdot)$ komutativní pologrupa.

Definice 1.8 Má-li okruh $\mathcal{R} = (R, +, \cdot, 0)$ neutrální prvek 1 vzhledem k operaci $\cdot$, budeme jej nazývat *okruh s jedničkou* (nebo také *unitární*).

Definice 1.9 Prvek $a \neq 0$ okruhu $\mathcal{R}$ nazveme *netriviální dělitel nuly*, existuje-li v R prvek $b \neq 0$ takový, že $a \cdot b = 0$ nebo $b \cdot a = 0$.

Obor integrity

Definice 1.10 Každý alespoň dvouprvkový komutativní unární okruh $\mathcal{R}$, v němž neexistují netriviální dělitelé nuly se nazývá *obor integrity*.

Těleso

Definice 1.11 Netriviální komutativní okruh $\mathcal{R}$, v němž ke každému nenulovému prvku existuje prvek inverzní, se nazývá *těleso*.

Věta 1.1 *Netriviální komutativní okruh $\mathcal{R}$ je těleso, právě když $(R \setminus 0, \cdot, 1)$ je grupa.*

Definice 1.12 Množina $\mathcal{R}^*$ všech invertibilních prvků okruhu $\mathcal{R}$, která je uzavřena na násobení se nazývá *multiplikativní grupa okruhu $\mathcal{R}$*.

Věta 1.2 *Multiplikativní grupa $\mathcal{R}^*$ konečného tělesa $\mathcal{R}$ je cyklická.*

Ideál v okruhu

Definice 1.13 Mějme okruh $\mathcal{R}$. Neprázdná podmnožina $I \subseteq R$ se nazývá *ideál* v okruhu $\mathcal{R}$, platí-li:

1. $\forall a, b \in I : a - b \in I$
2. $\forall a \in I, \forall b \in R : a \cdot b \in I, b \cdot a \in I$

Tvrzení 1.1 *Průnik libovolného systému ideálů okruhu $\mathcal{R}$ je opět ideál tohoto okruhu.*

Definice 1.14 Pro danou podmnožinu $M \subseteq R$ existuje nejmenší ideál $I(M)$ v $\mathcal{R}$ obsahující množinu M. Nazýváme jej *ideál generovaný množinou M*. Ideály $I(\{m\}) = I(m)$ pro $m \in M$ nazýváme *hlavní*.

Kongruence na okruhu

Definice 1.15 Mějme okruh $\mathcal{R}$. Relace ekvivalence θ na nosiči R okruhu $\mathcal{R}$ se nazývá *kongruence* na $\mathcal{R}$, platí-li tzv. substituční podmínka:

$$\forall a, b, c, d \in R : ((a, b) \in \theta \wedge (c, d) \in \theta) \Rightarrow ((a + c, b + d) \in \theta, (a \cdot c, b \cdot d) \in \theta) .$$

Tvrzení 1.2 *V každém okruhu $\mathcal{R}$ platí, že pro ideál I na $\mathcal{R}$ je relace $\theta_I = \{(x, y) \in R^2; x - y \in I\}$ kongruence na $\mathcal{R}$.*

Obory integrity a dělitelnost

Definice 1.16 Buď $\mathcal{J} = (J, +, 0, \cdot, 1)$ obor integrity a $a, b, c \in J$:

- řekneme, že prvek a dělí prvek b (zapisujeme $a|b$), existuje-li prvek c tak, že $b = a \cdot c$
- prvek $j \in J$, pro který platí $j|1$, nazveme *jednotka dělení* v $\mathcal{J}$
- prvky a, b nazveme *asociované*, platí-li $(a|b) \wedge (b|a)$, píšeme $a \parallel b$
- prvek $d \in J$ nazveme *společný dělitel prvků* a, b, je-li $(d|a) \wedge (d|b)$
- prvek $d \in J$ nazveme *největší společný dělitel prvků* a, b, je-li d společný dělitel a pro každého dalšího společného dělitele d' prvků a, b platí $d'|d$; píšeme $d = (a, b)$
- prvky $a \in J$, pro které platí $a\|1$ nebo $a\|b$, se nazývají *triviální dělitelé* prvku b
- nenulový prvek, který není jednotka a má pouze triviální dělitele, nazýváme *ireducibilní* (nerozložitelný)
- nenulový prvek a, který není jednotka, a pro který platí implikace

$$a| (b \cdot c) \Rightarrow ((a|b) \vee (a|c)) ,$$

  nazýváme *prvočinitel*.

Tvrzení 1.3 *Každý prvočinitel oboru integrity $\mathcal{J}$ je ireducibilní prvek, opak však obecně neplatí.*

Řekneme, že obor integrity $\mathcal{J}$ splňuje podmínku

- *existence ireducibilních rozkladů* (EIR), lze-li každý prvek $a \in \mathcal{J}$, $a \neq 0$, $a \nmid 1$, rozložit na součin konečného počtu ireducibilních prvků
- *jednoznačnosti ireducibilních rozkladů* (JIR), jsou-li asociovány každé dva rozklady daného prvku $a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ v součin ireducibilních prvků, kde $m = n$ a nezáleží na pořadí součinitelů

Definice 1.17 Obor integrity $\mathcal{J}$ nazveme

- *Gaussův* (G), splňuje-li podmínky (EIR) a (JIR)
- *obor integrity hlavních ideálů* (OIHI), je-li každý ideál v $\mathcal{J}$ hlavní
- *eukleidovský obor integrity* (EOI), existuje-li taková funkce $\delta : J \setminus 0 \to \mathbb{N}_0$, že pro každé dva prvky $a, b \in J$, $b \neq 0$, existují prvky $q, r \in J$ tak, že $a = b \cdot q + r$, kde $r = 0$ nebo $\delta(r) < \delta(b)$ (taková funkce na $\mathcal{J}$ se nazývá eukleidovská)

Tvrzení 1.4 *V každém oboru integrity platí:*

$$(EOI) \Rightarrow (OIHI) \Rightarrow (G)$$

Tvrzení 1.5 *Okruh $\mathbb{Z}$ je eukleidovský obor integrity s eukleidovskou funkcí*

$$\delta : \mathbb{Z} \setminus 0 \to \mathbb{N}, \delta(z) = |z|$$

Z předchozího vyplývá, že $\mathbb{Z}$ je oborem integrity hlavních ideálů a každý ideál v $\mathbb{Z}$ je tvaru $I(n) = \{k \cdot n; k \in \mathbb{Z}\}$ pro $n \in \mathbb{N}$. Každá kongruence na $\mathbb{Z}$ je tedy ve tvaru

$$\theta_{I(n)} = \left\{(x, y) \in \mathbb{Z}^2 : x - y \in I(n)\right\} = \left\{(x, y) \in \mathbb{Z}^2 : n | x - y\right\}$$

Kongruence $\theta_{I(n)}$ bývá označována symbolem $\equiv_n$ a vlastnost $(x, y) \in \equiv_n$ budeme zapisovat

$$x \equiv y \,(mod\ n)$$

(čteme x je kongruentní s y modulo n). V okruhu $\mathbb{Z}$ vzhledem k vlastnosti (EOI) splývají prvočinitelé a ireducibilní prvky a nazývají se *prvočísla*.

Celá algebraická čísla

Definice 1.18 Komplexní číslo α nazveme *algebraické*, je-li kořenem nějakého polynomu s racionálními koeficienty.

Komplexní číslo α nazveme *celé algebraické*, je-li kořenem nějakého normovaného polynomu (tj. polynomu s koeficientem u nejvyšší mocniny rovným jedné) s celočíselnými koeficienty.

Celá část reálného čísla

Definice 1.19 *Celá část reálného čísla* (přesněji dolní celá část) je funkce, která přiřadí reálnému číslu x největší celé číslo, které jej nepřevyšuje. Značíme $\lfloor x \rfloor$.

Poznámka 1.1 *Jiným způsobem by se definice dala napsat tak, že $\lfloor x \rfloor$ je jediné celé číslo, splňující nerovnost*

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Definice 1.20 Necelá část reálného čísla je funkce, kterou můžeme definovat pomocí celé části jako rozdíl

$$\{x\} := x - \lfloor x \rfloor .$$

Lemma 1.1 *Pro libovolné číslo $x \in \mathbb{R}$ platí $\lfloor 2x \rfloor - 2 \lfloor x \rfloor \in \{0, 1\}$. Konkrétně*

$$\lfloor 2x \rfloor - 2 \lfloor x \rfloor = \begin{cases} 0, & \text{jestliže } 0 \leq \{x\} < \frac{1}{2} \\ 1, & \text{jestliže } \frac{1}{2} \leq \{x\} . \end{cases}$$

Důkaz: Pro číslo x platí $2x = 2 \lfloor x \rfloor + 2 \{x\}$, kde $0 \leq \{x\} < 1$.

Jestliže $0 \leq \{x\} < \frac{1}{2}$, tak $2 \{x\} < 1$ a tedy $\lfloor 2x \rfloor = 2 \lfloor x \rfloor$. Dostaneme tak první možnost $\lfloor 2x \rfloor - 2 \lfloor x \rfloor = 0$.

Jestliže $\frac{1}{2} \leq \{x\} < 1$, tak $1 \leq 2 \{x\} < 2$. Odtud dostaneme $\lfloor 2x \rfloor = 2 \lfloor x \rfloor + 1$ a tedy $\lfloor 2x \rfloor - 2 \lfloor x \rfloor = 1$. □

Redukovaný systém zbytků

Definice 1.21 Množinu celých čísel $\{a_1, \ldots, a_n\}$ nazveme *úplný systém zbytků modulo n*, platí-li $\overline{a}_i \neq \overline{a}_j$ pro $i \neq j$.

Definice 1.22 Množinu čísel $\left\{a_1, \ldots, a_{\phi(n)}\right\}$ nazveme *redukovaný systém zbytků modulo n*, je-li množina $\left\{\overline{a}_1, \ldots, \overline{a}_{\phi(n)}\right\}$ množinou všech nedělitelů nuly v $\mathbb{Z}_n$.

Malá Fermatova věta

Věta 1.3 *Nechť p je prvočíslo. Potom pro všechna přirozená čísla a platí*

$$a^p \equiv a \,(mod\ p)\,.$$

Je-li navíc $(a, p) = 1$, *platí*

$$a^{p-1} \equiv 1 \,(mod\ p)\,.$$

Důkaz: Viz [1, str. 33]. □

2 Obory integrity $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}[\omega]$

Několik důležitých vlastností prvočísel lze odvodit při studiu dělitelnosti ve speciálních oborech integrity. Takovými jsou obory integrity $\mathbb{Z}[\mathrm{i}]$ a $\mathbb{Z}[\omega]$ celých algebraických čísel v tělesech $\mathbb{Q}[\mathrm{i}]$ a $\mathbb{Q}[\omega]$. Symbolem i se rozumí imaginární jednotka $\mathrm{i} = \sqrt{-1}$ a symbolem ω rozumíme primitivní třetí odmocninu z jedné $\omega = \frac{-1+\sqrt{-3}}{2}$. Obor integrity $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i}; a, b \in \mathbb{Z}\}$ se nazývá *obor integrity Gaussových celých čísel.*

Definice 2.1 Normou v oboru integrity $\mathbb{Z}[\mathrm{i}]$ budeme nazývat zobrazení

$$N : \mathbb{Z}[\mathrm{i}] \to \mathbb{N} \cup \{0\},$$

které je pro libovolný prvek $\alpha = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, kde $a, b \in \mathbb{Z}$, dané předpisem $N(\alpha) = a^2 + b^2 = \alpha \cdot \overline{\alpha}$, kde $\overline{\alpha} = a - b\mathrm{i}$ je číslo komplexně sdružené k číslu α.

Poznámka 2.1 *Snadno lze ukázat, že norma v $\mathbb{Z}[\mathrm{i}]$ je multiplikativní. Tedy $N(\alpha) \cdot N(\beta) = N(\alpha \cdot \beta)$. Jednotky dělení v $\mathbb{Z}[\mathrm{i}]$ jsou právě ty prvky α, pro něž je $N(\alpha) = 1$, tj. jsou to prvky $\pm 1, \pm\mathrm{i}$.*

Věta 2.1 *$\mathbb{Z}[\mathrm{i}]$ je eukleidovský obor integrity s normou N.*
Důkaz: Potřebujeme dokázat, že pro libovolná dvě čísla $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$, kde $\beta \neq 0$, existují čísla $\gamma, \delta \in \mathbb{Z}[\mathrm{i}]$ taková, že

$$\alpha = \gamma\beta + \delta, \ \textit{kde } \delta \neq 0 \textit{ nebo } N(\delta) < N(\beta).$$

Upravíme podíl $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} = r + s\mathrm{i}$, kde $r, s \in \mathbb{Q}$. Zde jsme využili vlastností $\overline{\beta} \in \mathbb{Z}[\mathrm{i}]$ a $N(\beta) = \beta\overline{\beta}$. Existují tedy čísla $m, n \in \mathbb{Z}$ taková, že $|r - m| \leq \frac{1}{2}$ a $|s - n| \leq \frac{1}{2}$. Víme, že $\mathbb{Z}[\mathrm{i}]$ je obor integrity a jeho podílovým tělesem je těleso $\mathbb{Q}[i] = \{a + b\mathrm{i} | a, b \in \mathbb{Q}\}$. Formálně vzato jde o těleso zlomků $\frac{a+b\mathrm{i}}{c+d\mathrm{i}}$, kde $a, b, c, d \in \mathbb{Z}$. Tento zlomek lze upravit na tvar $\frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\mathrm{i}$. Odtud je vidět, že norma v tělese $\mathbb{Q}[i]$ je definována jako rozšíření normy z oboru $\mathbb{Z}[\mathrm{i}]$. Tedy, že norma podílu je rovna podílu norem. Jestliže položíme $\gamma = m + n\mathrm{i}$, můžeme potom psát $N\left(\frac{\alpha}{\beta} - \gamma\right) = N((r - m) + \mathrm{i}(s - n)) = (r - m)^2 + (s - n)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$.

Pro číslo $\delta = \alpha - \gamma\beta$ díky multiplikativnosti normy v tělese komplexních čísel platí $N(\delta) = N(\alpha - \gamma\beta) = N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)\, N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta)$. □

Podívejme se podrobněji na obor integrity $\mathbb{Z}[\omega]$. Kořeny polynomu $x^3 - 1 = 0$ jsou $x_1 = 1, x_2 = \frac{-1+\sqrt{-3}}{2}$ a $x_3 = \frac{-1-\sqrt{-3}}{2}$. Označíme $\omega = \frac{-1+\sqrt{-3}}{2}$. Pro libovolné $k \in \mathbb{Z}$ platí $\omega^{3k} = 1, \omega^{3k+1} = \omega$ a $\omega^{3k+2} = \omega^2$. Všimněme si dále, že $1 + \omega + \omega^2 = 0$ a že $\overline{\omega} = \omega^2 = -1 - \omega$.

Podobně, jako jsme v úvodu kapitoly zavedli množinu Gaussových celých čísel, můžeme zavést množinu $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$. Tato množina je uzavřená

na sčítání a násobení a je zřejmé, že neutrálním prvkem vzhledem k násobení je číslo 1 a opačným prvkem k číslu $a+b\omega$ je číslo $-a-b\omega$. Jedná se tedy o okruh. Tato množina je také uzavřená vzhledem ke komplexní sdruženosti svých prvků. Označíme-li $\alpha = a+b\omega$, tak potom $\overline{\alpha} = a+b\overline{\omega} = a+b\omega^2 = a+b(-1-\omega) = (a-b)-b\omega \in \mathbb{Z}[\omega]$.

Definice 2.2 Normou v oboru integrity $\mathbb{Z}[\omega]$ budeme nazývat zobrazení

$$N : \mathbb{Z}[\omega] \to \mathbb{N} \cup \{0\},$$

které je pro libovolný prvek $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, kde $a, b \in \mathbb{Z}$, dané předpisem $N(\alpha) = \alpha \cdot \overline{\alpha}$.

Poznámka 2.2 *Chceme-li odvodit vztah pro výpočet normy prvků z množiny* $\mathbb{Z}[\omega]$*, stačí přímé dosazení do vztahu* $N(\alpha) = \alpha \cdot \overline{\alpha}$*. Dostaneme potom:*

$$\alpha \cdot \overline{\alpha} = (a+b\omega)\cdot(a-b-b\omega) = a^2 - ab + b^2\left(-\omega-\omega^2\right).$$

Víme, že platí $1 = -\omega - \omega^2$ *a odtud již plyne, že norma prvku* $\alpha = a+b\omega$ *je určena vztahem* $N(\alpha) = a^2 - ab + b^2$*.*

Věta 2.2 $\mathbb{Z}[\omega]$ *je eukleidovský obor integrity s normou* N*.*
Důkaz: Analogicky jako pro obor integrity $\mathbb{Z}[\mathrm{i}]$ dokážeme, že pro libovolná dvě čísla $\alpha, \beta \in \mathbb{Z}[\omega]$, kde $\beta \neq 0$, existují čísla $\gamma, \delta \in \mathbb{Z}[\omega]$ taková, že

$$\alpha = \gamma\beta + \delta, \ \textit{kde } \delta \neq 0 \textit{ nebo } N(\delta) < N(\beta).$$

Upravíme podíl $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} = r+s\omega$, kde $r, s \in \mathbb{Q}$. Existují čísla m, n taková, že $|r-m| \leq \frac{1}{2}$ a $|s-n| \leq \frac{1}{2}$. Víme, že $\mathbb{Z}[\omega]$ je obor integrity a jeho podílovým tělesem je těleso $\mathbb{Q}[\omega] = \{a+b\omega \mid a, b \in \mathbb{Q}\}$. Norma je v tělese $\mathbb{Q}[\omega]$ definována podobným způsobem jako v oboru integrity $\mathbb{Z}[\omega]$. Jestliže položíme $\gamma = m+n\omega$, můžeme potom psát

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N\left((r-m) + \omega(s-n)\right) =$$

$$(r-m)^2 - (r-m)(s-n) + (s-n)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1.$$

Pro číslo $\delta = \alpha - \gamma\beta$ díky multiplikativnosti norem v $\mathbb{Q}[\omega]$ platí

$$N(\delta) = N(\alpha - \gamma\beta) = N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)\, N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta).$$

□

Důsledek 2.1 *$\mathbb{Z}[\omega]$ je obor integrity s jednoznačným rozkladem. Libovolný nenulový prvek $\alpha \in \mathbb{Z}[\omega]$, který není jednotkou, lze zapsat jako součin konečného počtu ireducibilních prvků ze $\mathbb{Z}[\omega]$.*

Tvrzení 2.1 *Prvek $\alpha \in \mathbb{Z}[\omega]$ je jednotkou oboru integrity $\mathbb{Z}[\omega]$ právě tehdy, když $N(\alpha) = 1$.*
Důkaz: „$\Rightarrow$“ Jestliže α je jednotka v $\mathbb{Z}[\omega]$, potom existuje $\beta \in \mathbb{Z}[\omega]$ takové, že $\alpha\beta = 1$. Dále platí, že $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. Obě normy $N(\alpha), N(\beta)$ jsou tedy rovny jedné.
„$\Leftarrow$“ Platí, že $N(\alpha) = \alpha\overline{\alpha} = 1$. Prvek $\overline{\alpha}$ je tedy inverzní k prvku α a ten je jednotkou v $\mathbb{Z}[\omega]$. □

Poznámka 2.3 *Chceme-li nalézt všechny jednotky množiny $\mathbb{Z}[\omega]$, zjistíme, že to již není tak zřejmé, jako tomu bylo v oboru integrity $\mathbb{Z}[\mathrm{i}]$.*

Příklad 2.1 *Najděte všechny jednotky v oboru integrity $\mathbb{Z}[\omega]$.*

Řešení: Aby prvek $\alpha = a + b\omega$ byl jednotkou v $\mathbb{Z}[\omega]$ musí platit rovnost $a^2 - ab + b^2 = 1$. Tuto rovnost vynásobíme čtyřmi a upravíme

$$4a^2 - 4ab + 4b^2 = 4$$

$$(2a - b)^2 + 3b^2 = 4$$

Je vidět, že pro koeficient b musí platit podmínka $|b| \leq 1$. Dostaneme tedy následující možnosti:

(1) $b = 1$, $2a - b = \pm 1$ a tyto koeficienty odpovídají číslu $1 + \omega$ a ω

(2) $b = -1$, $2a - b = \pm 1$ a tyto koeficienty odpovídají číslu $-\omega$ a $-1 - \omega$

(3) $b = 0$, $2a - b = \pm 2$ a tyto koeficienty odpovídají číslu 1 a -1

Využitím rovnosti $\omega^2 = -1 - \omega$ a $-\omega^2 = 1 + \omega$ jsme dokázali, že všechny jednotky v oboru integrity $\mathbb{Z}[\omega]$ jsou tvaru $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

3 Kvadratický zákon vzájemnosti

V této kapitole se budeme zabývat řešitelností kongruenčních rovnic tvaru $x^2 \equiv a\,(mod\ p)$, pro nějaké prvočíslo p. K rozhodnutí o řešitelnosti těchto rovnic zavedeme tzv. *Legendreův symbol* a *kvadratický zákon vzájemnosti*. Tyto pojmy budeme potřebovat i v následujících kapitolách, k důkazům některých vět.

Definice 3.1 Mějme $m \in \mathbb{N}$ a $a \in \mathbb{Z}$ taková, že $(a, m) = 1$. Číslo a nazveme *kvadratickým zbytkem modulo m*, má-li kongruence $x^2 \equiv a\,(mod\ m)$ řešení. Tedy existuje-li $x \in \mathbb{Z}$ takové, že $x^2 \equiv a\,(mod\ m)$. Pokud žádné takové celé číslo x neexistuje, řekneme, že a je *kvadratickým nezbytkem modulo m*.

Věta 3.1 *Nechť p je liché prvočíslo. V redukované soustavě zbytků modulo p je stejný počet kvadratických zbytků jako nezbytků.*
Důkaz: Uvažujme redukovaný systém zbytků modulo p, tedy množinu čísel $\left\{\pm 1, \pm 2, \cdots, \pm\frac{p-1}{2}\right\}$. Umocněním těchto prvků na druhou dostaneme množinu kvadratických zbytků modulo p, a to $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$. Musíme ukázat, že to jsou právě všechny kvadratické zbytky.
Předpokládejme, že dvě z těchto čísel jsou kongruentní modulo p. Např. pro $1 \leq k < l \leq \frac{p-1}{2}$ platí

$$k^2 \equiv l^2\,(mod\ p)\,.$$

Potom platí $p \mid (k+l)\cdot(l-k)$, což vzhledem k p dává

$$p \mid (k+l) \quad \text{nebo} \quad p \mid (l-k)\,.$$

Vzhledem k nerovnosti $1 \leq k < l \leq \frac{p-1}{2}$ není možné aby nastal ani jeden předchozí případ. Proto jsme našli všechny kvadratické zbytky a můžeme říci, že počet kvadratických zbytků modulo p je roven $\frac{p-1}{2}$ a zároveň je to také počet kvadratických nezbytků modulo p. □

Příklad 3.1 Určete všechny kvadratické zbytky a nezbytky modulo 19.

Řešení: Libovolné nenulové řešení kongruence $x^2 \equiv a\,(mod\ 19)$ je kongruentní s jedním z čísel ± 1, ± 2, ± 3, ± 4, ± 5, ± 6, ± 7, ± 8, ± 9. Po umocnění na druhou dostaneme postupně čísla 1, 4, 9, 16, 25, 36, 49, 64 a 81. Vydělíme je modulo 19 a obdržíme množinu všech kvadratických zbytků 1, 4, 9, 16, 6, 17, 11, 7 a 5. Množina všech kvadratických nezbytků modulo 19 obsahuje čísla 2, 3, 8, 10, 12, 13, 14, 15, 18.

Definice 3.2 Pro liché prvočíslo $p \in \mathbb{Z}$ a číslo $a \in \mathbb{Z}$ definujeme *Legendreův symbol* $\left(\frac{a}{p}\right)$ následovně:

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

Věta 3.2 *Nechť p je liché prvočíslo, $a, b \in \mathbb{Z}$. Pak platí:*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \,(mod\ p)\,,$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right),$
3. *je-li* $a \equiv b \,(mod\ p)$, *pak* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$

Důkaz:

1. Pokud $p \mid a$ je tvrzení zřejmé.
Podívejme se na případ, kdy $p \nmid a$. Podle malé Fermatovy věty platí $a^{p-1} \equiv 1 \,(mod\ p)$, tedy

$$\left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \,(mod\ p)\,.$$

Protože $\mathbb{Z}_p$ je těleso, platí buď

$$a^{\frac{p-1}{2}} \equiv 1 \,(mod\ p) \quad \text{nebo} \quad a^{\frac{p-1}{2}} \equiv -1 \,(mod\ p)\,.$$

Zároveň tedy

$$a^{\frac{p-1}{2}} + 1 \not\equiv a^{\frac{p-1}{2}} - 1 \,(mod\ p)\,,$$

neboť pro liché prvočíslo p platí $-1 \not\equiv 1 \,(mod\ p)$. Je-li a kvadratický zbytek, pak existuje $x \in \mathbb{Z}, (x, p) = 1$, takové že $a \equiv x^2 \,(mod\ p)$ a dále

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

Kvadratických zbytků je stejně jako kvadratických nezbytků, a to právě $\frac{p-1}{2}$. Rovnice $a^{\frac{p-1}{2}} \equiv 1 \,(mod\ p)$ má pro neznámou a právě $\frac{p-1}{2}$ řešení. Zároveň této rovnici nevyhovuje žádný kvadratický nezbytek. Ty splňují rovnici $a^{\frac{p-1}{2}} \equiv -1 \,(mod\ p)$.

2. Použijeme první část této věty:

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

Obě strany nabývají pouze hodnot ± 1 a $1 \not\equiv -1 \,(mod\ p)$. Můžeme tak od kongruence přejít k rovnosti.

3. Jestliže $a \equiv b \,(mod\ p)$, pak kongruence $x^2 \equiv a \,(mod\ p)$ je řešitelná právě tehdy, když je řešitelná kongruence $x^2 \equiv b \,(mod\ p)$.

□

Věta 3.3 *Pro liché prvočíslo p platí:*

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

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

Důkaz:

1. Podle věty 3.1 (1) platí

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

Obě strany kongruence nabývají hodnot ± 1. Vzhledem k tomu, že $1 \not\equiv -1\,(mod\ p)$ můžeme místo kongruence psát přímo rovnost.
Ještě můžeme doplnit, že první možnost nastane pro prvočísla $p \equiv 1\,(mod\ 4)$ a druhá možnost pro prvočísla $p \equiv 3\,(mod\ 4)$.

2. Nechť p je liché prvočíslo. Budeme chtít ukázat, že 2 je kvadratický zbytek pro prvočísla ve tvaru $8k \pm 1$ a kvadratický nezbytek pro prvočísla ve tvaru $8k \pm 3$.

Uvažujme následující kongruence:

$$\begin{aligned}
p - 1 &\equiv 1\,(-1)^1 \,(mod\ p)\\
2 &\equiv 2\,(-1)^2 \,(mod\ p)\\
p - 3 &\equiv 3\,(-1)^3 \,(mod\ p)\\
4 &\equiv 4\,(-1)^4 \,(mod\ p)\\
p - 5 &\equiv 5\,(-1)^5 \,(mod\ p)\\
&\vdots\\
q &\equiv \frac{p-1}{2}\,(-1)^{\frac{p-1}{2}} \,(mod\ p)
\end{aligned}$$

kde číslo q je rovno buď $p - \frac{p-1}{2}$ nebo $\frac{p-1}{2}$.

Vynásobením těchto kongruencí dostaneme

$$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)!\,(-1)^{1+2+3+\ldots+\frac{p-1}{2}} \,(mod\ p)\,.$$

Součet $1 + 2 + 3 + \ldots + \frac{p-1}{2}$ je roven zlomku $\frac{p^2-1}{8}$ a součin $2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$ je roven číslu $2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$. Po úpravě poslední kongruence dostaneme

$$2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\,(-1)^{\frac{p^2-1}{8}} \,(mod\ p)\,.$$

Podle věty 3.1 (1) dále platí

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

Když budeme uvažovat číslo $p = 8k \pm 1$, tak můžeme exponent z poslední kongruence upravit $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$. Dostaneme sudé číslo a 2 proto bude kvadratický zbytek modulo p. Pokud budeme uvažovat $p = 8k \pm 3$, dostaneme $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k+8}{8} = 8k^2 \pm 2k + 1$. To je jistě liché číslo a v tomto případě bude 2 kvadratickým nezbytkem modulo p. □

Příklad 3.2 Je dána rovnice paraboly $443y = x^2 - 152$. Zjistěte, jestli na grafu této kuželosečky leží body s celočíselnými souřadnicemi (tzv. mřížové body roviny).

Řešení: Body, které leží na grafu dané funkce, musí vyhovovat její rovnici. Tzn., že hledané body existují, jestliže je řešitelná kongruenční rovnice $x^2 \equiv 152\,(mod\ 443)$. Již víme, že tato rovnice bude mít řešení, jestliže bude hodnota příslušného Legendreova symbolu rovna jedné. Chceme tedy určit hodnotu $\left(\frac{152}{443}\right)$. Jednoduše vypočítáme, že

$$\left(\frac{152}{443}\right) = \left(\frac{2}{443}\right)^3 \cdot \left(\frac{19}{443}\right).$$

Určíme hodnotu symbolu $\left(\frac{2}{443}\right)$

$$\left(\frac{2}{443}\right) = (-1)\,\frac{443^2 - 1}{8} = (-1)^{24531} = -1.$$

Dále

$$\left(\frac{19}{443}\right) = \left(\frac{443}{19}\right)(-1)^{9\cdot 221} = -\left(\frac{443}{19}\right).$$

Určíme stejným způsobem hodnotu symbolu $\left(\frac{443}{19}\right)$

$$\left(\frac{443}{19}\right) = \left(\frac{6}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{3}{19}\right).$$

Symbol $\left(\frac{2}{19}\right)$ má hodnotu

$$\left(\frac{2}{19}\right) = (-1)^{45} = -1.$$

$$\left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Celkově dostaneme

$$\left(\frac{152}{443}\right) = (-1)^3 \cdot (-1)\,(-1)\,(-1) = 1.$$

Rovnice řešitelná je a proto existují mřížové body paraboly $443y = x^2 - 152$. Pro zajímavost můžeme ještě doplnit, že jsou to body $[174; 68]\,, [269; 163]$.

3.1 Gaussovo lemma

Na závěr této kapitoly ukážeme se jeden z mnoha důkazů kvadratického zákona vzájemnosti. Budeme k tomu ale nejprve potřebovat následující lemma.

Lemma 3.1 ***Gaussovo lemma*** *Nechť p je liché prvočíslo takové, že $p \nmid a$. Dále, nechť m je počet čísel z množiny $\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$, jejichž zbytek po dělení p je větší než $\frac{p}{2}$. Potom platí*

$$\left(\frac{a}{p}\right) = (-1)^m .$$

Důkaz: Označme $S = a \cdot 2a \cdot 3a \cdot \ldots \cdot \frac{p-1}{2}a$. Tento součin je roven číslu

$$S = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

Dále si uvědomme, že každé z čísel ka, kde $k = 1, 2, \ldots, \frac{p-1}{2}$ se dá vyjádřit ve tvaru $sp + z$, kde z je některý z prvků redukovaného systému zbytků modulo p. Prvek z bude nabývat záporné hodnoty pro ty čísla, pro která bude zbytek po dělení p větší než $\frac{p}{2}$. Tedy právě m čísel. Dále žádná dvě čísla ka nejsou kongruentní modulo p a stejně tak neplatí $k_1 a \equiv -k_2 a \,(mod\ p)$, pro $k_1 \neq k_2$.

Platí tedy, že mezi čísly ka jsou všechna čísla $1, 2, \ldots, \frac{p-1}{2}$ a z nich je m záporných a zbytek je kladných. Dostaneme tedy

$$S \equiv (-1)^m \left(\frac{p-1}{2}\right)! \,(mod\ p) .$$

Celkově

$$a^{\frac{p-1}{2}} \equiv (-1)^m \,(mod\ p) .$$

□

Věta 3.4 *Pro číslo m z Gauussova lemmatu platí*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor \,(mod\ 2) .$$

Legendreův symbol tedy můžeme psát ve tvaru

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor} ,$$

pro liché a potom ve tvaru

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor} .$$

Důkaz: Budou nás zajímat zbytky čísel ka po dělení prvočíslem p, kde $k = 1, 2, \ldots, \frac{p-1}{2}$. Podle lemmatu 1.1 platí

$$\left\lfloor \frac{2ak}{p} \right\rfloor = \begin{cases} 2\left\lfloor \frac{ak}{p} \right\rfloor, & jestliže\ 0 \leq \left\{ \frac{ak}{p} \right\} < \frac{1}{2}, \\ 2\left\lfloor \frac{ak}{p} \right\rfloor + 1, & jestliže\ \frac{1}{2} \leq \left\{ \frac{ak}{p} \right\}. \end{cases}$$

Odtud plyne, že číslo $\left\lfloor \frac{2ak}{p} \right\rfloor$ je sudé, jestliže $0 \leq \left\{ \frac{ak}{p} \right\} < \frac{1}{2}$, a liché v opačném případě.
Číslo ak můžeme psát také ve tvaru $ak = q_k p + r_k$. Odtud dostaneme $\left\{ \frac{ak}{p} \right\} = \left\{ q_k + \frac{r_k}{p} \right\} = \left\{ \frac{r_k}{p} \right\} = \frac{r_k}{p}$. Pro zlomek $\frac{r_k}{p}$ platí, že $\frac{r_k}{p} \geq \frac{1}{2}$ právě tehdy, když $r_k \geq \frac{p}{2}$.

Číslo m tedy označuje počet těch čísel, pro které je $\left\lfloor \frac{2ak}{p} \right\rfloor$ liché číslo.
Pro liché číslo a platí

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right).$$

Dokázali jsme tedy, že

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)k}{p} \right\rfloor}.$$

Exponent můžeme dále upravit

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)\,k}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \lfloor k \rfloor = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \frac{p^2-1}{8}.$$

Celkem tedy dostaneme

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor} (-1)^{\frac{p^2-1}{8}} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor} \left(\frac{2}{p}\right).$$

Odtud již dostaneme hledanou rovnost

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor}.$$

□

3.2 Důkaz kvadratického zákona vzájemnosti

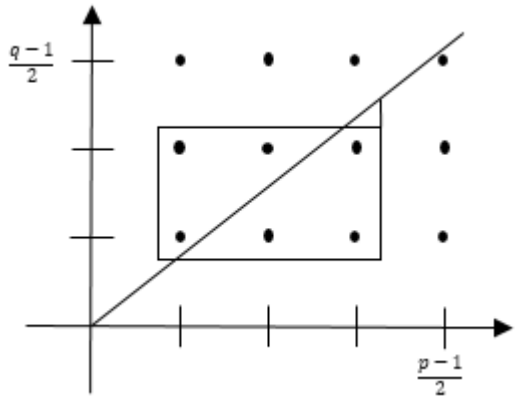
Máme již vše potřebné k tomu, abychom dokázali kvadratický zákon vzájemnosti.

Věta 3.5 Kvadratický zákon vzájemnosti *Nechť p, q jsou různá lichá prvočísla. Pak*

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

Důkaz: Počet všech mřížových bodů $(x, y) \in \mathbb{N} \times \mathbb{N}$ takových, že $1 \leq x \leq \frac{p-1}{2}$ a $1 \leq y \leq \frac{q-1}{2}$ je určitě $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Zkusme teď ke stejnému výsledku dojít jiným způsobem.

Hledané body rozdělíme na dvě skupiny. $S_1 = \{(x, y)\,; qx > py\}$ a $S_2 = \{(x, y)\,; qx < py\}$. Tato situace je znázorněna pro $p = 7, q = 5$ na obrázku 1.



Obrázek 1: p=7, q=5

Počet prvků v množinách S_1 a S_2 můžeme vyjádřit:

$$|S_1| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor,$$

$$|S_2| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Podíváme-li se pozorně na obrázek, který je výše v textu, tak si můžeme všimnout, že počítáme počet mřížových bodů v útvaru, který je složen z obdélníku a malého trojúhelníku. Je-li $p > q$ je tento trojúhelník nad daným obdélníkem. Potřebujeme proto také ukázat, že v tomto trojúhelníku není žádný mřížový bod.

K tomu si stačí uvědomit, že na přímce $y = \frac{q}{p}x$ neleží žádný mřížový bod. Sečtením předchozích rovností, pak dostaneme

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Těchto poznatků využijeme pro vyjádření Legendreových symbolů z předchozí věty a dostaneme

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Celkově tedy

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

□

Příklad 3.3 Zjistěte, zda je řešitelná kongruence $x^2 \equiv 11\,(mod\ 31)$.

Řešení: Určíme hodnotu Legendreova symbolu $\left(\frac{11}{31}\right)$. Můžeme rovnou použít kvadratický zákon vzájemnosti:

$$\left(\frac{11}{31}\right) = \left(\frac{31}{11}\right) \cdot (-1)^{5\cdot 15} = -\left(\frac{31}{11}\right).$$

Podle věty 3.1 platí

$$\left(\frac{31}{11}\right) = \left(\frac{9}{11}\right) = 1.$$

Celkový výsledek je

$$\left(\frac{11}{31}\right) = -1$$

a kongruence $x^2 \equiv 11\,(mod\ 31)$ tedy řešitelná není.

Příklad 3.4 Určete, pro která prvočísla p je řešitelná kongruence $x^2 \equiv 13\,(mod\ p)$.

Řešení: Předpokládejme, že $p \nmid 13$. Kongruence je tedy řešitelná, právě když 13 je kvadratickým zbytkem modulo p, což znamená $\left(\frac{13}{p}\right) = 1$.

Vyšetříme tedy hodnotu Legendreova symbolu $\left(\frac{13}{p}\right)$. Použijeme kvadratický zákon vzájemnosti

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) \cdot (-1)^{\frac{p-1}{2}\cdot\frac{13-1}{2}}.$$

Protože součin $\frac{p-1}{2} \cdot \frac{13-1}{2} = (p-1)\cdot 3$ je číslo sudé, tak můžeme rovnou psát $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. Užitím věty 3.1 (3) dostaneme následující možnosti pro hodnotu symbolu $\left(\frac{p}{13}\right)$.

- $p \equiv 1\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{1}{13}\right) = 1$
- $p \equiv 2\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{169-1}{8}} = -1$.
- $p \equiv 3\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{3}{13}\right)$. Použijeme kvadratický zákon vzájemnosti a větu 3.1 (2, 3) $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) \cdot (-1)^{\frac{13-1}{2} \cdot \frac{3-1}{2}} = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$.
- $p \equiv 4\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{4}{13}\right) = 1$. Použijeme větu 3.1 (2) a dostaneme $\left(\frac{4}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{2}{13}\right) = 1$
- $p \equiv 5\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{5}{13}\right) = 1$. Použijeme kvadratický zákon vzájemnosti a větu 3.1 (2, 3) $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) \cdot (-1)^{\frac{13-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{13}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right) \cdot \left(\frac{2}{5}\right) = -1$
- $p \equiv 6\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{6}{13}\right) = 1$. Použijeme větu 3.1 (2) $\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) = -1$
- $p \equiv 7\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{7}{13}\right) = 1$. Použijeme větu 3.1 $\left(\frac{7}{13}\right) = \left(\frac{-6}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{6}{13}\right) = -1$
- $p \equiv 8\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{8}{13}\right) = 1$. Použijeme větu 3.1 (2) $\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{4}{13}\right) = -1$
- $p \equiv 9\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{9}{13}\right) = 1$. Použijeme větu 3.1 (2) $\left(\frac{9}{13}\right) = \left(\frac{3}{13}\right) \cdot \left(\frac{3}{13}\right) = 1$
- $p \equiv 10\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{10}{13}\right) = 1$. Použijeme větu 3.1 (2) $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right) = 1$
- $p \equiv 11\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{11}{13}\right) = 1$. Použijeme větu 3.1 (2, 3) $\left(\frac{11}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right) = -1$
- $p \equiv 12\,(mod\ 13)$: $\left(\frac{p}{13}\right) = \left(\frac{12}{13}\right) = 1$. Použijeme větu 3.1 (2) $\left(\frac{12}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{6}{13}\right) = 1$

Kongruence je tedy řešitelná pro prvočísla $p \equiv 1, 3, 4, 9, 10, 12\,(mod\ 13)$.

4 Kubický zákon vzájemnosti

V úvodních dvou kapitolách jsme si zavedli potřebný aparát k tomu, abychom se mohli zabývat otázkami řešitelnosti kongruencí vyšších řádů. Tedy řešením rovnic typu $x^n \equiv a\,(mod\ p)$, kde $a, n \in \mathbb{Z}, n > 2$ jsou pevně daná čísla. V této kapitole budeme uvažovat číslo $n = 3$ a dojdeme k tzv. kubickému zákonu vzájemnosti.

Uvedeme vlastnosti prvočinitelů, zavedeme zbytkové třídy okruhu $\mathbb{Z}[\omega]$, poté se dostaneme k pojmu kubický mocninný symbol, který je obdobou Legendreova symbolu v teorii kvadratických zbytků a na závěr kapitoly vyslovíme kubický zákon vzájemnosti.

4.1 Obor integrity $\mathbb{Z}[\omega]$ podrobněji

Základní vlastnosti oboru integrity $\mathbb{Z}[\omega]$ jsme uvedli již v druhé kapitole. Nyní naše znalosti rozšíříme o charakterizaci prvočinitelů v tomto oboru.

Tvrzení 4.1 *Jestliže π je prvočinitel v $\mathbb{Z}[\omega]$, potom existuje prvočíslo p takové, že $N(\pi) = p$ nebo $N(\pi) = p^2$. V případě, že je norma rovna číslu p, tak π není prvkem asociovaným s žádným prvočíslem. V druhém případě, kdy je norma rovna číslu p^2, je prvek π asociovaný s prvočíslem p.*

Důkaz: Mějme π prvočinitele v $\mathbb{Z}[\omega]$. Platí tedy $N(\pi) = \pi\overline{\pi}$. Položme $N(\pi) = n$, kde $n \in N$. Z rovnosti $\pi\overline{\pi} = n$ plyne $\pi \mid n$, dále také víme, že n lze rozložit v $\mathbb{Z}$ jednoznačně (až na pořadí) na součin prvočísel. Dostáváme, že pro nějaké prvočíslo p platí $\pi \mid p$ a tedy $p = \pi\gamma$, kde $\gamma \in \mathbb{Z}[\omega]$. Z multiplikativnosti normy v okruhu $\mathbb{Z}[\omega]$ platí

$$N(\pi)\,N(\gamma) = N(\pi\gamma) = N(p) = p^2$$

Pro normy čísel π a γ máme tři možnosti:

a) $N(\gamma) = 1, N(\pi) = p^2$

b) $N(\gamma) = p, N(\pi) = p$

c) $N(\gamma) = p^2, N(\pi) = 1.$

V prvním případě je γ jednotkou, a tedy π je asociované s p.

Pokud by v druhém případě bylo π asociované s nějakým prvočíslem q, platilo by $\pi = \delta q$, kde δ je jednotka v okruhu $\mathbb{Z}[\omega]$. To by ale znamenalo

$$p = N(\pi) = N(\delta p) = N(\delta)\,N(p) = 1 \cdot N(p) = q^2.$$

Pro žádná dvě prvočísla ovšem nemůže platit rovnost $p = q^2$ a tedy π není asociované s p.

Třetí rovnost nastat nemůže, neboť π není jednotka. □

Tvrzení 4.2 *Jestliže $\pi \in \mathbb{Z}[\omega]$ je prvek, pro který platí $N(\pi) = p$, kde p je prvočíslo, potom je π prvočinitel v $\mathbb{Z}[\omega]$.*
Důkaz: Z předpokladů plyne, že π není jednotka. Předpokládejme tedy, že číslo π je složené a lze jej psát ve tvaru $\pi = \gamma\delta$, kde γ a δ nejsou jednotky v $\mathbb{Z}[\omega]$. Potom platí

$$p = N(\pi) = N(\gamma) N(\delta).$$

Jelikož $N(\gamma)$ i $N(\delta)$ jsou přirozená čísla různá od jedné, dostáváme spor, protože součin dvou přirozených čísel větších než jedna není roven žádnému prvočíslu. Prvek π tedy musí být prvočinitel v $\mathbb{Z}[\omega]$. □

Dokažme nyní tvrzení, pomocí něhož budeme schopni charakterizovat všechny prvočinitele oboru integrity $\mathbb{Z}[\omega]$.

Tvrzení 4.3 *Jsou-li p a q jsou prvočísla, potom platí:*

1. $3 = -\omega^2 (1-\omega)^2$ *a* $1-\omega$ *je prvočinitel v* $\mathbb{Z}[\omega]$.
2. *Jestliže* $p \equiv 1 \,(mod\ 3)$, *potom* $p = \pi\overline{\pi}$, *kde* π *je prvočinitel v* $\mathbb{Z}[\omega]$ *a prvky* π *a* $\overline{\pi}$ *nejsou asociované.*
3. *Jestliže* $q \equiv 2 \,(mod\ 3)$, *potom* q *je prvočinitel v* $\mathbb{Z}[\omega]$.

Libovolný prvočinitel v $\mathbb{Z}[\omega]$ je asociovaný s jedním z prvočinitelů z bodů $1. - 3.$.

Poznámka 4.1 *Toto tvrzení se občas také interpretuje tak, že v prvním případě se prvočíslo tzv. větví, tj. je dělitelné vyšší mocninou nějakého prvočinitele. V druhém případě se říká, že prvočíslo se úplně rozkládá, tj. je součinem dvou různých prvočinitelů. A ve třetím případě se prvočíslo nazývá inertní, tj. je samo prvočinitelem.*

Důkaz:

1. Z definice normy jsme schopni hned vypočítat $N(1-\omega) = 1^2 - 1(-1) + (-1)^2 = 3$.

Z věty 4.2 tedy plyne, že $1-\omega$ je prvočinitel.

Pro důkaz rovnosti $3 = -\omega^2 (1-\omega)^2$ vyjdeme z rovnice $1 + \omega + \omega^2 = 0$. Tuto rovnici vynásobíme $-\omega^2$ a přičteme k ní 3.

$$-\omega^2 - \omega^3 - \omega^4 + 3 = 3$$

Víme, že $\omega^2 = -1 - \omega$ a $\omega^3 = 1$. Rovnost tedy dál upravíme na

$$-\omega^2 + 2\omega^3 - \omega^4 = 3\text{a} - \omega^2\left(1 - 2\omega + \omega^2\right) = 3.$$

To už je hledaný výsledek $-\omega^2 (1-\omega)^2 = 3$.

2. Uvažujme prvočíslo p, pro které platí $p \equiv 1\,(mod\ 3)$ a ukažme, že p je součinem dvou různých prvočinitelů, kteří nejsou spolu asociovaní. Pomocí kvadratického zákona vzájemnosti zjistíme, že -3 je kvadratický zbytek modulo p:

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

Jelikož $p \equiv 1\,(mod\ 3)$ můžeme dál upravovat

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

Z rovnosti $\left(\frac{-3}{p}\right) = 1$ dostáváme, že existuje číslo $a \in \mathbb{Z}$ takové, že $a^2 \equiv -3\,(mod\ p)$. To znamená, že a^2+3 je dělitelné p, tedy existuje číslo $b \in \mathbb{Z}$ splňující $pb = a^2+3$. Zkusme nyní upravit výraz a^2+3.

$$a^2+3 = \left(a+\sqrt{-3}\right)\left(a-\sqrt{-3}\right) = (a+1+2\omega)(a-1-2\omega).$$

Využili jsme rovnost $1+2\omega = 1+2\frac{-1+\sqrt{-3}}{2} = \sqrt{-3}$. Předpokládejme nyní, že π je prvočinitel dělící p. Protože $\pi \mid p$ a $p \mid (a+1+2\omega)(a-1-2\omega)$ tak musí i $\pi \mid (a+1+2\omega)(a-1-2\omega)$. Prvočinitel π musí tedy dělit některého z činitelů součinu $(a+1+2\omega)(a-1-2\omega)$. Tím je dokázáno, že prvočinitelem není číslo asociované s p, protože p nedělí ani $(a+1+2\omega)$ ani $(a-1-2\omega)$. Po vydělení číslem p bychom totiž dostali nějaké komplexní číslo, které neleží v $\mathbb{Z}[\omega]$. Celkem jsme tedy zjistili, že p není prvočinitel.

Když p není prvočinitel, tak se dá rozložit $p = \pi\eta$ a π ani η nejsou jednotky. Z multiplikativnosti normy v $\mathbb{Z}[\omega]$ platí $N(p) = N(\pi)N(\eta) = p^2$. A protože p je prvočíslo, tak jediná možnost jak rozložit p^2 je $p \cdot p$. Dostaneme tedy, že $N(\pi) = p$ a zároveň dle definice je $N(\pi) = \pi\overline{\pi}$ a tím máme hledaný rozklad.

Ukážeme, že π a $\overline{\pi}$ nejsou asociované. Kdyby byly prvky π a $\overline{\pi}$ asociované musel by jeden dělit druhý. Například $\overline{\pi} \mid \pi$. Po vynásobení číslem π dostaneme $\overline{\pi}\pi \mid \pi^2$ a odtud $p \mid \pi^2$. Podíváme se teď podrobněji na jednotlivé případy, které při dělení mohou nastat. Označme $\pi = c+d\omega$, můžeme potom psát $p \mid (c+d\omega)^2$, kde

$$(c+d\omega)^2 = c^2+2cd\omega+d^2\omega^2 = c^2+2cd\omega+d^2(-1-\omega) = c^2-d^2+\omega\left(2cd-d^2\right).$$

Dostáváme odtud, že

$$p \mid \left(c^2-d^2\right) \wedge p \mid d(2c-d)$$

Víme, že $c, d \in \mathbb{Z}$ a p je prvočíslo. Dostáváme tedy následující možnosti:

a) $p \mid (c-d) \wedge p \mid d$, platí tedy, že $p \mid (c-d+d) = c$

b) $p \mid (c-d) \wedge p \mid (2c-d)$, platí tedy, že $p \mid (2c-d-(c-d)) = c$ a $p \mid (c-(c-d)) = d$

c) $p \mid (c+d) \wedge p \mid d$, platí tedy, že $p \mid (c+d-d) = c$

d) $p \mid (c+d) \wedge p \mid (2c-d)$, platí tedy, že $p \mid (2c-d+c+d) = 3c$

První tři možnosti nám ukazují, že $p \mid c$ a zároveň $p \mid d$. Čtvrtá možnost nám dává výsledek $p \mid 3c$ a ten vede buď k závěru, že $p \mid c$ a nebo ke sporu s předpokladem, že $p \equiv 1 \,(mod\ 3)$ jestliže $p \mid 3$. Z výsledků $p \mid c$ a zároveň $p \mid d$ vyplývá, že $p \mid (c + d\omega) = \pi$. Což je ale ve sporu s tím, že $p = \pi\overline{\pi}$. Celkově tedy prvky $\pi, \overline{\pi}$ nejsou asociované.

3. Jestliže $\pi \mid 2$ tak, potom $N(\pi) \neq 1$, protože by π byla jednotka a zároveň musí platit, že $N(\pi) \mid N(2)$. Jelikož $N(2) = 4$ tak dostáváme dvě možnosti.

1. $N(\pi) = 2$
Předpokládejme, že $\pi = a + b\omega$. Víme, že $N(\pi) = a^2 - ab + b^2$. Budeme tedy počítat

$$a^2 - ab + b^2 = 2 \Rightarrow 4a^2 - 4ab + 4b^2 = 8 \Rightarrow (2a+b)^2 + 3b^2 = 8.$$

Tato rovnost ovšem nemá v $\mathbb{Z}$ žádné řešení a dostáváme se tím do sporu.

2. $N(\pi) = 4$
Víme tedy, že $N(\pi) = 4$ a budeme rozkládat dvojku. Existuje $\eta \in \mathbb{Z}[\omega]$ takové, že $\pi \cdot \eta = 2$. Z multiplikativnosti norem víme, že $N(\pi)\,N(\eta) = 4$ a jelikož víme, že $N(\pi) = 4$ tak musí být $N(\eta) = 1$. Zjistili jsme tedy, že η je jednotka a že π je asociované s dvojkou. Celkově jsme dokázali, že až na asociovanost existuje jediný prvočinitel dělicí dvojku, a to dvojka sama.

Obecněji. Mějme libovolné prvočíslo q takové, že $q = 2 \,(mod\ 3)$. Uvažujme prvočinitele $\pi \in \mathbb{Z}[\omega]$, který dělí q. To znamená, že existuje $\eta \in \mathbb{Z}[\omega]$ takové, že $\eta \cdot \pi = q$. Přechodem k normám dostaneme

$$N(\eta)\,N(\pi) = N(q) = q^2$$

Víme, že $N(\pi) \neq 1$ a dostaneme tak dvě následující možnosti

1. $N(\pi) = q$
Předpokládejme, že $\pi = a + b\omega$. Víme, že $N(\pi) = a^2 - ab + b^2$. Budeme tedy počítat

$$a^2 - ab + b^2 = q \Rightarrow 4a^2 - 4ab + 4b^2 = 4q \Rightarrow (2a+b)^2 + 3b^2 = 4q.$$

$$(2a+b)^2 \equiv 4q \equiv 2 \,(mod\ 3).$$

Tato rovnost ovšem nemá v $\mathbb{Z}$ žádné řešení a dostáváme se tím do sporu.

2. $N(\pi) = q^2$
Z tohoto předpokladu ovšem dostáváme, že $N(\eta) = 1$ a tedy, že η je jednotka v $\mathbb{Z}[\omega]$. Dále dostáváme, že π je prvek asociovaný s q a že až na asociovanost existuje jediný prvočinitel dělící číslo q, a to číslo q samo.

□

4.2 Zbytkové třídy okruhu $\mathbb{Z}[\omega]$

V této kapitole se seznámíme s pojmem kongruence na okruhu $\mathbb{Z}[\omega]$. Jestliže $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ a $\gamma \neq 0$ řekneme, že $\alpha \equiv \beta \,(mod\ \gamma)$, pokud $\gamma \mid (\alpha - \beta)$. Tedy říkáme, tak jako v okruhu $\mathbb{Z}$, že α je kongruentní β modulo γ. Obdobně jako v okruhu $\mathbb{Z}$ kongruence faktorizuje okruh $\mathbb{Z}[\omega]$ na okruh zbytkových tříd modulo γ, který značíme $\mathbb{Z}[\omega]/\gamma\mathbb{Z}[\omega]$.

Tvrzení 4.4 *Mějme $\pi \in \mathbb{Z}[\omega]$, který je prvočinitel. Potom $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ je konečné těleso o $N(\pi)$ prvcích.*
Důkaz: Z algebry víme, že každý konečný obor integrity je tělesem. Bude tedy stačit, když se nám podaří ukázat, že $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ je konečný obor integrity, přesněji, že má právě $\mathbb{N}(\pi)$ prvků.

Ukážeme, že $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ neobsahuje dělitele nuly. Mějme $\alpha, \beta \in \mathbb{Z}$, položíme-li $[\alpha]_\pi \cdot [\beta]_\pi = [\alpha\beta]_\pi = [0]_\pi$, potom vidíme, že $\pi \mid \alpha\beta$. Jelikož je π prvočinitel, musí dělit jeden z prvků na pravé straně. Předpokládejme, že je to prvek α. To, že $\pi \mid \alpha$ znamená, že $[\alpha]_\pi = [0]_\pi$ a proto neexistují prvky $\alpha, \beta \in \mathbb{Z}[\omega]$, $[\alpha]_\pi \neq [0]_\pi \neq [\beta]_\pi$, vyhovují rovnosti $[\alpha]_\pi \cdot [\beta]_\pi = [0]_\pi$.

Kolik má tento obor integrity prvků ukážeme tím způsobem, že projdeme postupně všechny možnosti uvedené v tvrzení 4.3.

Nejprve předpokládejme, že $\pi = p$, kde p je prvočíslo kongruentní s dvojkou modulo tři. Dokážeme, že $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] = \left\{[a + b]_p \omega \mid 0 \leq a < p, 0 \leq b < p\right\}$. Mějme $\mu = m + n\omega \in \mathbb{Z}[\omega]$. Čísla m, n a p jsou celá a tedy dle věty o dělení celých čísel se zbytkem platí, že $m = ps + a$, $n = pt + b$, kde $s, t, a, b \in \mathbb{Z}$ a $0 \leq a, b < p$. Po dosazení za m a n dostaneme

$$\mu = ps + a + (pt + b)\,\omega \Rightarrow \mu \equiv a + b\omega \,(mod\ p).$$

Můžeme nyní říci, že libovolný prvek okruhu $\mathbb{Z}[\omega]$ patří do jedné ze zbytkových tříd množiny $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$. Zbývá ukázat, že tato množina má skutečně $N(p) = p^2$ prvků, tedy, že žádné dvě zbytkové třídy spolu nesplývají.

Předpokládejme, že $a + b\omega \equiv a' + b'\omega \,(mod\ p)$, kde $0 \leq a, b, a', b' < p$. Odtud dostáváme, že $p \mid (a - a' + (b - b')\,\omega)$, a proto $\frac{a-a'}{p} + \frac{b-b'}{p}\omega \in \mathbb{Z}[\omega]$, z čehož plyne, že $\frac{a-a'}{p}$ a $\frac{b-b'}{p}$ jsou celá čísla. To je ale možné jen když bude platit $a = a'$ a $b = b'$. Tedy, že $a + b\omega = a' + b'\omega$.

Nyní budeme předpokládat, že $p \equiv 1 \,(mod\ 3)$ a že $p = \pi\overline{\pi} = N(\pi)$, kde π

je prvočinitel v $\mathbb{Z}[\omega]$ a prvky π a $\overline{\pi}$ nejsou asociované. Ukážeme, že, množina $\{0, 1, \cdots, p-1\}$ je množinou čísel, kterými lze reprezentovat libovolnou zbytkovou třídu modulo π. Z toho poté vyplyne, že $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ má $N(\pi) = p$ prvků. Položme $\pi = a + b\omega$ a z definice normy v okruhu vidíme, že $p = a^2 - ab + b^2$ a že $p \nmid b$. Položme dále $\mu = m + n\omega$. Víme, že $p \nmid b$ a budeme-li postupně brát $x = 0, 1, \cdots, p-1$ potom součin xb bude nabývat všech hodnot úplné soustavy zbytků modulo p. Existuje tedy celé číslo c takové, že $cb \equiv n\,(mod\ p)$. Odtud $p \mid (n - cb)$ a proto $\mu - c\pi = m - ca + (n - cb)\,\omega$, tedy $\mu - c\pi \equiv m - ca\,(mod\ p)$. Dále platí, že $\mu \equiv m - ca\,(mod\ \pi)$, protože $\pi \mid p$. Ukázali jsme, že libovolný prvek z množiny $\mathbb{Z}[\omega]$ patří do zbytkové třídy reprezentované nějakým celým číslem modulo π. Mějme nějaké celé číslo l. Podle věty o dělení se zbytkem lze toto číslo psát ve tvaru $l = sp + r$, kde $s, r \in \mathbb{Z}$ a $0 \leq r < p$. Platí tedy, že $l \equiv r\,(mod\ p)$ a jelikož $\pi \mid p$ tak také $l \equiv r\,(mod\ \pi)$. Ukázali jsme tedy, že každý prvek množiny $\mathbb{Z}[\omega]$ je kongruentní s prvkem množiny $\{0, 1, \cdots, p-1\}$ modulo π. Zbývá ukázat, že žádné dvě z těchto tříd nesplývají. Jestliže, $r \equiv r'\,(mod\ \pi)$, kde $r, r' \in \mathbb{Z}$ a $0 \leq r, r' < p$, potom $r - r' = \pi\gamma$ pro nějaké $\gamma \in \mathbb{Z}[\omega]$. Výpočtem norem výrazů na levé a pravé straně rovnosti dostaneme $(r - r')^2 = N(r - r') = N(\pi\gamma) = N(\pi)\,N(\gamma) = pN(\gamma)$. Tedy $p \mid (r - r')^2$ a jelikož je p prvočíslo, tak $p \mid r - r'$. Celkově dostáváme, že $r - r' = 0$, a tedy $r = r'$. Všechny prvky množiny $\{0, 1, \cdots, p-1\}$ jsou tak reprezentanty různých zbytkových tříd tělesa $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

Víme, že libovolný prvočinitel je asociovaný s jedním z uvedených prvočinitelů a můžeme jej tedy zařadit do jednoho z výše popsaných případů. Tím jsme s důkazem hotovi. □

Je-li π prvočinitel, potom multiplikativní grupa tělesa $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ má řád $N(\pi) - 1$ a můžeme vyslovit tvrzení analogické malé Fermatově větě.

Tvrzení 4.5 *Mějme $\alpha \in \mathbb{Z}[\omega]$ a π prvočinitel takový, že $\pi \nmid \alpha$. Potom*

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

Důkaz: Věta je důsledkem Lagrangeovy věty aplikované na multiplikativní grupu $(\mathbb{Z}[\omega]/\pi Z[\omega])^*$. Viz [3, str. 39]. □

Jestliže je norma π různá od tří, tak potom zbytkové třídy v tělese $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ obsahující $1, \omega$ a ω^2 jsou různé. Například pro $\omega \equiv 1\,(mod\ \pi)$ bychom měli, že $\pi \mid (1 - \omega)$ a $1 - \omega$ je prvočinitel, tedy π a $1 - \omega$ jsou asociované. Platí proto, že $N(\pi) = N(1 - \omega) = 3$, což je ale spor. Obdobně by se daly ukázat i zbylé případy.

Platí, že $\langle[\omega]_\pi\rangle = \{[1]_\pi, [\omega]_\pi, [\omega^2]_\pi\}$ je spolu s operací násobení zbytkových tříd cyklická grupa řádu 3. Podle Lagrangeovy věty potom 3 dělí řád multiplikativní grupy $(\mathbb{Z}[\omega]/\pi Z[\omega])^*$, tedy $3 \mid N(\pi) - 1$.

Tvrzení 4.6 *Nechť $\alpha \in \mathbb{Z}[\omega]$ a π je prvočinitel takový, že $N(\pi) \neq 3$ a $\pi \nmid \alpha$. Potom existuje jednoznačně určené číslo m rovno $0, 1$ nebo 2 takové, že*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \,(mod\ \pi).$$

Důkaz: Víme, že $\pi \mid \alpha^{N(\pi)-1}-1$. Dále víme, že $x^3-1 = (x-1)(x-\omega)(x-\omega^2)$ a toho nyní využijeme při úpravě výrazu $\alpha^{N(\pi)-1}-1$.

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

Protože π je prvočinitel, tak musí dělit právě jeden ze tří členů na pravé straně rovnosti. To že dělí právě jeden z daných činitelů plyne z faktu, že kdyby dělilo dva činitele na pravé straně, tak by dělilo i jejich rozdíl. To ale není možné, neboť jsme v předchozích odstavcích ukázali, že prvky $1, \omega$ a ω^2 patří pro $N(\pi) \neq 3$ do různých zbytkových tříd modulo π. □

Nyní můžeme zavést tzv. kubický mocninný symbol.

Definice 4.1 Mějme $\alpha, \pi \in \mathbb{Z}[\omega]$, kde π je prvočinitel takový, že $N(\pi) \neq 3$. Potom definujeme *kubický mocninný symbol* čísla α modulo π následovně:

1. jestliže $\pi \mid \alpha$, klademe $\left(\frac{\alpha}{\pi}\right)_3 = 0$,
2. jestliže $\pi \nmid \alpha$, definujeme $\left(\frac{\alpha}{\pi}\right)_3 \in \{1, \omega, \omega^2\}$ podmínkou $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \,(mod\ \pi)$.

Kubický mocninný symbol hraje v teorii kubického zákona vzájemnosti stejnou roli jako Legendreův symbol v teorii kvadratického zákona vzájemnosti. V následující definici je popsán pojem kubického zbytku.

Definice 4.2 Mějme $\alpha, \gamma \in \mathbb{Z}[\omega]$ taková, že $(\alpha, \gamma) = 1$. Číslo α nazveme *kubickým zbytkem modulo γ*, má-li kongruence $x^3 \equiv \alpha \,(mod\ \gamma)$ řešení v okruhu $\mathbb{Z}[\omega]$. Pokud žádné takové číslo $x \in \mathbb{Z}[\omega]$ neexistuje, řekneme, že α je *kubickým nezbytkem modulo γ*.

Tvrzení 4.7 *Nechť $\alpha \in \mathbb{Z}[\omega]$ a π prvočinitel takový, že $N(\pi) \neq 3$ a $\pi \nmid \alpha$. Potom platí:*

1. $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \,(mod\ \pi)$,
2. $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$,
3. *jestliže $\alpha \equiv \beta \,(mod\ \pi)$, potom* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$,
4. $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *právě tehdy, když kongruence $x^3 \equiv \alpha \,(mod\ \pi)$ je řešitelná v okruhu $\mathbb{Z}[\omega]$ (tj. právě tehdy, když je α kubickým, zbytkem modulo π.)*

Důkaz:

1. Důkaz plyne přímo z definice kubického mocninného symbolu.

2. Podle první části věty platí, že

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

Protože obě strany kongruence nabývají hodnot $0, 1, \omega, \omega^2$ a žádné dva z těchto prvků neleží ve stejné zbytkové třídě modulo π, můžeme místo kongruence psát přímo rovnost.

3. Jestliže $\alpha \equiv \beta\,(mod\ \pi)$, potom $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \equiv \beta^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 (mod\ \pi)$.

4. $\Longrightarrow$ Nechť $\left(\frac{\alpha}{\pi}\right)_3 = 1$. Platí, že $(\mathbb{Z}[\omega]/\pi Z[\omega])^* = \langle\gamma\rangle$ pro nějaké $\gamma \in \mathbb{Z}[\omega]$, pro které $\pi \nmid \gamma$. Pro nějaké $n \in \mathbb{N}$ je $\alpha \equiv \gamma^n\,(mod\ \pi)$ a využitím částí 2. a 3. dostaneme $1 = \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\gamma^n}{\pi}\right)_3 = \left(\frac{\gamma}{\pi}\right)_3^n$. Tato rovnost je splněna buď pro $\left(\frac{\gamma}{\pi}\right)_3 = 1$, nebo jestliže $3 \mid n$. V prvním případě by z definice kubického mocninného symbolu platilo $\gamma^{\frac{N(\pi)-1}{3}} \equiv 1\,(mod\ \pi)$, což však není možné, jelikož je prvek γ generátorem grupy $(\mathbb{Z}[\omega]/\pi Z[\omega])^*$, a musí tedy mít řád roven řádu této grupy, tj. $N(\pi) - 1$. Proto musí nastat druhý případ, kdy $3 \mid n$. Nyní stačí položit $x = \gamma^{\frac{n}{3}}$ a dostaneme řešení dané kongruence.
$\Longleftarrow$ Označme γ řešení kongruence $x^3 \equiv \alpha\,(mod\ \pi)$. Potom platí $\gamma^3 \equiv \alpha\,(mod\ \pi)$ a musí dále platit, že $\pi \nmid \gamma$, protože by v opačném případě platilo $\pi \mid \alpha$. Pomocí částí 2. a 3. dostaneme $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\gamma^3}{\pi}\right)_3 = \left(\frac{\gamma}{\pi}\right)_3^3 = 1$, neboť $1 = 1^3 = \omega^3 = \omega^6$.

□

Následující tvrzení popisuje vlastnosti kubických mocninných symbolů vzhledem ke komplexní sdruženosti.

Tvrzení 4.8 *Nechť $\alpha \in \mathbb{Z}[\omega]$ a π je prvočinitel, pro který $N(\pi) \neq 3$. Pak platí:*

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

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

Důkaz:

1. Z definice kubického mocninného symbolu víme, že $\left(\frac{\alpha}{\pi}\right)_3$ je roven $1, \omega$ nebo ω^2. Z rovnosti $\omega\overline{\omega} = N(\omega) = 1 = \omega^3$ plyne, že $\overline{\omega} = \omega^2, \overline{\omega^2} = \omega = (\omega^2)^2$ a odkud dostáváme, že $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2$. Zbylá část rovnosti plyne z druhé části tvrzení 4.7.

2. Podle tvrzení 4.7 je

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

Abychom ukázali, že $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$ potřebujeme nejprve dokázat, že pokud pro prvky $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ platí $\alpha \equiv \beta \,(mod\ \gamma)$, pak také platí $\overline{\alpha} \equiv \overline{\beta} \,(mod\ \overline{\gamma})$.
Pro libovolná $\mu, \nu \in \mathbb{C}$ platí $\overline{\mu} \cdot \overline{\nu} = \overline{\mu\nu}$ a dále $\overline{\mu} - \overline{\nu} = \overline{\mu - \nu}$. Jestliže platí $\alpha \equiv \beta \,(mod\ \gamma)$, pak $\gamma \mid (\alpha - \beta)$, tedy existuje $\delta \in \mathbb{Z}[\omega]$ takové, že $\alpha - \beta = \delta \cdot \gamma$. Poslední rovnost přepíšeme do tvaru $\overline{\alpha - \beta} = \overline{\delta \cdot \gamma}$ a dále využijeme zmíněné vztahy, abychom celkově dostali $\overline{\alpha} - \overline{\beta} = \overline{\delta} \cdot \overline{\gamma}$. Jelikož $\overline{\delta} \in \mathbb{Z}[\omega]$, platí $\overline{\gamma} \mid \left(\overline{\alpha} - \overline{\beta}\right)$, a tedy $\overline{\alpha} \equiv \overline{\beta} \,(mod\ \overline{\gamma})$.
Odtud dostaneme

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

Protože $N(\pi) = \pi\overline{\pi} = \overline{\overline{\pi}\pi} = N(\overline{\pi})$, dostaneme díky tvrzení 4.7 kongruenci

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

Spojením posledních dvou kongruencí dostaneme $\overline{\left(\frac{\alpha}{\pi}\right)_3} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3 (mod\ \overline{\pi})$. Víme, že obě strany mohou nabývat pouze hodnot $0, 1, \omega$ a ω^2, které leží v různých zbytkových třídách, lze proto kongruenci zaměnit za rovnost.

□

Důsledek 4.1 *Nechť $p \equiv 2 \,(mod\ 3)$ je prvočíslo, $\alpha \in \mathbb{Z}[\omega]$. Pak:*

1. $\left(\frac{\overline{\alpha}}{p}\right)_3 = \left(\frac{\alpha^2}{p}\right)_3$,

2. *pro $n \in \mathbb{Z}$ takové, že $p \nmid n$, platí $\left(\frac{n}{p}\right)_3 = 1$.*

Důkaz:

1. Protože $p = \overline{p}$, dostaneme z předchozích vět

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

2. Protože $n = \overline{n}$, dostaneme z předchozích vět

$$\left(\frac{n}{p}\right)_3 = \left(\frac{\overline{n}}{p}\right)_3 = \overline{\left(\frac{n}{p}\right)_3} = \left(\frac{n}{p}\right)_3^2.$$

Víme, že $p \nmid n$ a protože $\left(\frac{n}{p}\right)_3 \neq 0$, musí platit $\left(\frac{n}{p}\right)_3 = 1$.

□

Díky předchozímu důsledku můžeme říci, že celé číslo n, které je nesoudělné s prvočíslem $p \equiv 2\,(mod\ p)$, je kubickým zbytkem modulo p. Jsou-li tedy p_1, p_2 dvě různá prvočísla taková, že $p_1 \equiv p_2 \equiv 2\,(mod\ 3)$, potom $\left(\frac{p_1}{p_2}\right)_3 = \left(\frac{p_2}{p_1}\right)_3$. Dostali jsme speciální případ kubického zákona vzájemnosti, k jehož obecnější formě se dostaneme v následující kapitole.

4.3 Kubický zákon vzájemnosti

Definice 4.3 Prvočinitel $\pi \in \mathbb{Z}[\omega]$ nazveme *primární*, jestliže $\pi \equiv 2\,(mod\ 3)$.

Jestliže $\pi = a + b\omega$, lze podmínku z definice formulovat jako $a \equiv 2\,(mod\ 3)$ a zároveň $b \equiv 0\,(mod\ 3)$. Můžeme tedy říci, že libovolný prvočíselný prvočinitel je primární. Také si můžeme všimnout, že pokud $\pi = a + b\omega$ je primární prvočinitel, pak také $\overline{\pi} = (a - b) - b\omega$ je primární.

Tvrzení 4.9 *Nechť $\pi \in \mathbb{Z}[\omega]$ je prvočinitel, $p \in \mathbb{Z}$ prvočíslo takové, že $N(\pi) = p \equiv 1\,(mod\ 3)$. Potom je mezi prvky asociovanými s π právě jeden primární prvočinitel.*

Důkaz: Položme $\pi = a + b\omega$. Prvky asociované k π jsou tvaru π, $\omega\pi$, $\omega^2\pi$, $-\pi$, $-\omega\pi$, $-\omega^2\pi$. Celkově se tedy bude jednat o prvky

1. $a + b\omega$,
2. $\omega(a + b\omega) = -b + (a - b)\omega$,
3. $\omega^2(a + b\omega) = (b - a) - a\omega$,
4. $-a - b\omega$,
5. $b + (b - a)\omega$,
6. $(a - b) + a\omega$.

Najdeme mezi těmito prvočiniteli alespoň jeden, který bude primární. Protože $N(\pi) = p = a^2 - ab + b^2 \equiv 1\,(mod\ 3)$ nemůže nastat případ, kdy $3 \mid a$ a zároveň $3 \mid b$. Porovnáním prvků částí 1. a 2. důkazu vidíme, že lze bez újmy na obecnosti předpokládat, že $3 \nmid a$. Dále porovnáním prvků 1. a 4. můžeme dokonce předpokládat, že $a \equiv 2\,(mod\ 3)$. Díky tomu dostáváme $p = a^2 - ab + b^2 \equiv 4 - 2b + b^2\,(mod\ 3) \equiv 1$. Což lze také přepsat ve tvaru $b(b - 2) \equiv 0\,(mod\ 3)$. Celkově můžeme předpokládat, že buď $a \equiv 2\,(mod\ 3) \wedge a \equiv 0\,(mod\ 3)$, nebo $a \equiv 2\,(mod\ 3) \wedge a \equiv 2\,(mod\ 3)$. V prvním případě je primárním prvočinitelem prvek $a + b\omega$, ve druhém prvek $b + (b - a)\omega$.

Pro dokázání jednoznačnosti předpokládejme, že $a + b\omega$ je primární prvočinitel. Jestliže porovnáme první složky prvků 2. a 5. zjistíme, že nemohou být primární. Dále vidíme, že prvek 6. nemůže být primární prvočinitel vzhledem ke koeficientu a ve druhé složce. Tím je tedy věta dokázána. □

Příklad 4.1 Najděte primárního prvočinitele, který je asociovaný s prvočinitelem:

1. $1-2\omega$,
2. $1+4\omega$,
3. $-7-3\omega$.

Řešení:

1. Nejprve ověříme, že $N(1-2\omega)=7$, a proto je prvek $1-2\omega$ dle tvrzení 4.2 prvočinitelem. Asociované prvky k tomuto prvku jsou přitom tvaru

a) $1-2\omega$,

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

c) $\omega^2(1-2\omega)=\omega^2-2\omega^3=(-1-\omega)-2=-3-\omega$,

d) $-1+2\omega$,

e) $-2-3\omega$,

f) $3+\omega$.

Primárním prvočinitelem je prvek $2+3\omega$.

2. Opět zkontrolujeme nejprve platnost tvrzení 4.2 a zjistíme, že $N(1+4\omega)=13$. Asociované prvky budou následující:

a) $1+4\omega$,

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

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

d) $-1-4\omega$,

e) $4+3\omega$,

f) $-3+\omega$.

Primárním prvočinitelem je prvek $-4-3\omega$.

3. Zde je situace jednodušší. Platí, že $N(-7-3\omega)=37$ a zároveň je rovnou splněno $-7\equiv 2\,(mod\ 3)$ a $-3\equiv 0\,(mod\ 3)$. Prvek $-7-3\omega$ je tedy přímo primární prvočinitel.

Příklad 4.2 Jak vypadá těleso $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega]$?

Řešení : Číslo $p=5$ je prvočinitel v $\mathbb{Z}[\omega]$. Víme tedy, že $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega]$ je těleso o $N(p)$ prvcích. V našem případě to bude 25 prvků, které budou vyhovovat kongruenční rovnici $x^3\equiv a+b\omega\,(mod\ 5)$ v $\mathbb{Z}[\omega]$. Všechny tyto prvky jsou v následující tabulce. Pro jednodušší zápis budeme dál ztotožňovat zbytkové třídy s jejich reprezentanty.

0	ω	2ω	3ω	4ω
1	$1+\omega$	$1+2\omega$	$1+3\omega$	$1+4\omega$
2	$2+\omega$	$2+2\omega$	$2+3\omega$	$2+4\omega$
3	$3+\omega$	$3+2\omega$	$3+3\omega$	$3+4\omega$
4	$4+\omega$	$4+2\omega$	$4+3\omega$	$4+4\omega$

Grupa $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ je cyklická grupa řádu 24 a třetí mocniny jejích prvků tvoří její cyklickou podgrupu řádu 8. Zkusíme najít generátor této podgrupy a všechny její prvky. Určeme postupně hodnoty kubických mocninných symbolů pro prvky z tělesa $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega]$.

$$\left(\frac{1}{5}\right)_3 = 1^8 \,(mod\ 5) = 1$$

$$\left(\frac{2}{5}\right)_3 = 2^8 \,(mod\ 5) = 1$$

$$\left(\frac{3}{5}\right)_3 = 3^8 \,(mod\ 5) = 1$$

$$\left(\frac{4}{5}\right)_3 = 4^8 \,(mod\ 5) = 1$$

$$\left(\frac{1+2\omega}{5}\right)_3 = (1+2\omega)^8 = \ldots = 5\omega^2 + 5\omega + 6 = 1$$

$$\left(\frac{2+4\omega}{5}\right)_3 = \left(\frac{2}{5}\right)_3 \left(\frac{1+2\omega}{5}\right)_3 = 1$$

$$\left(\frac{3+\omega}{5}\right)_3 = 1$$

$$\left(\frac{4+3\omega}{5}\right)_3 = 1$$

Vidíme tedy, že hledaná podgrupa má prvky

$$1, 2, 3, 4, 1+2\omega, 2+4\omega, 3+\omega, 4+3\omega$$

a jejím generátorem je prvek $1+2\omega$.

Stejným způsobem bychom mohli určit hodnoty zbylých prvků a dospěli bychom k výsledku že $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega] \simeq \mathbb{Z}_3$. Prvky zobrazující se na 1 jsme již našli. Prvky zobrazující se na ω jsou

$$1+\omega, 4+\omega, 2+2\omega, 3+2\omega, 2+3\omega, 3+3\omega, 1+4\omega, 4+4\omega$$

a prvky zobrazující se na ω^2 jsou

$$\omega, 2\omega, 3\omega, 4\omega, 1+3\omega, 2+\omega, 4+2\omega, 3+4\omega.$$

Tvrzení 4.10 ***Kubický zákon vzájemnosti*** *Nechť $\pi_1, \pi_2 \in \mathbb{Z}[\omega]$ jsou primární prvočinitelé takoví, že $N(\pi_1) \neq N(\pi_2)$. Potom*

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

Důkaz: Důkaz kubického zákona vzájemnosti je k dispozici v několika verzích v literatuře [1, str. 115 - 118]. □

Nyní budeme chtít podrobněji vyšetřit, jak se mění hodnota kubického mocninného symbolu $\left(\frac{\omega}{\pi}\right)_3$ pro všechny jednotky okruhu $\mathbb{Z}[\omega]$ a dále pro prvočinitele $1-\omega$, na něhož nelze aplikovat kubický zákon vzájemnosti.

Předpokládejme, že $N(\pi) \neq 3$. Jak je vidět, tak kongruence $x^3 \equiv 1 \,(mod\ \pi)$ a $x^3 \equiv -1 \,(mod\ \pi)$ jsou řešitelné vždy, neboť stačí položit $x = 1$ případně $x = -1$. Platí tedy $\left(\frac{1}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 = 1$.

Podívejme se ještě na hodnotu $\left(\frac{\omega}{\pi}\right)_3$. Z tvrzení 4.5 můžeme psát $\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{N(\pi)-1}{3}}$. Obě strany kongruence nabývají pouze hodnot $1, \omega, \omega^2$, ležící v různých zbytkových třídách modulo π. Konkrétně platí

$$\left(\frac{\omega}{\pi}\right)_3 = \begin{cases} 1 & N(\pi) \equiv 1 \,(mod\ 9) \\ \omega & ,jestliže\ N(\pi) \equiv 4 \,(mod\ 9). \\ \omega^2 & N(\pi) \equiv 7 \,(mod\ 9) \end{cases}$$

Víme, že platí $\left(\frac{\omega^2}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3^2$ a jsme tedy schopni již určit hodnoty kubického mocninného symbolu modulo π pro všechny zbývající jednotky.

Věta 4.1 *Nechť π je primární prvočinitel, pro který platí $N(\pi) \neq 3$. Položíme-li $\pi = 3m - 1 + 3n\omega$, kde $m, n \in \mathbb{Z}$, pak platí:*

1. $\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n}$
2. $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$

Důkaz: Pokud bychom chtěli číslo π psát v obvyklém tvaru $\pi = a + b\omega$, tak bychom položili $a = 3m - 1$ a $b = 3n$. Tím je číslo π jednoznačně určeno a v souladu s definicí primárního prvočinitele.

1. Podle tvrzení 4.5 platí $\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{N(\pi)-1}{3}}$. Vypočítáme, čemu se rovná exponent na pravé straně rovnosti:

$$\frac{N(\pi)-1}{3} = \frac{N(3m-1+3n\omega)-1}{3} = \frac{(3m-1)^2 - (3m-1)3n + (3n)^2 - 1}{3}$$

$$= \frac{9m^2 - 6m - 9mn + 3n + 9n^2}{3}.$$

Odtud dostaneme

$$\frac{N(\pi)-1}{3} = 3m^2 - 2m - 3mn + n + 3n^2 \equiv m + n \,(mod\ 3)\,.$$

Proto platí $\left(\frac{\omega}{\pi}\right) = \omega^{m+n}$.

2. Důkaz této části věty je poměrně pracný a vzhledem k rozsahu práce jej zde nebudeme uvádět. Lze jej nalézt v knize [1, str. 135].

□

Příklad 4.3 Určete, zda je řešitelná kongruence $x^3 \equiv 11\,(mod\ 17)$.

Řešení : Z předchozího textu víme, že je-li $p \equiv 2\,(mod\ 3)$ je kongruence $x^3 \equiv a\,(mod\ p)$ řešitelná vždy, jestliže a je nesoudělné s p. V našem případě jsou obě podmínky splněny a kongruence je řešitelná.

Ke stejnému výsledku bychom dospěli i pokud bychom chtěli využít malou Fermatovu větu. Platí, že $11^{17-1} = (11^2)^8 = 121^8 \equiv 2^8 = 256 \equiv 1\,(mod\ 17)$.

Příklad 4.4 Určete, zda je řešitelná kongruence $x^3 \equiv 13\,(mod\ 37)$.

Řešení : Protože je $37 \equiv 1\,(mod\ 3)$, lze využitím tvrzení 4.3 najít prvočinitele π, $\overline{\pi}$ takové, že $37 = \pi\overline{\pi}$. Označme $\pi = a + b\omega$. Hledáme tedy řešení rovnice $a^2 - ab + b^2 = 37$. Vynásobením rovnice 4 a úpravou levé strany na čtverec dostaneme ekvivalentní rovnici $(2a-b)^2 + 3b^2 = 148$. Výrazy v této rovnici nabývají pouze kladných hodnot a požadujeme, aby platilo $3 \mid b$. Existuje tedy $c \in \mathbb{Z}$ takové, že $b = 3c$. Můžeme proto rovnici přepsat do tvaru $(2a-3c)^2 + 27c^2 = 148$. Rovnici můžeme řešit v závislosti na hodnotě výrazu c^2. Dostaneme následující možnosti:

1. $c^2 = 0$ a zároveň $(2a-3c)^2 = 148$ což nelze, protože 148 není druhá mocnina žádného celého čísla

2. $c^2 = 1$ a zároveň $(2a-3c)^2 = 121$ odtud dostáváme, že $c = \pm 1$ a zároveň $(2a-3c) = \pm 11$

3. $c^2 = 4$ a zároveň $(2a-3c)^2 = 40$ což nelze, protože 40 není druhá mocnina žádného celého čísla

4. $c^2 \geq 9$ a zároveň $(2a-3c)^2 < 0$ což neplatí pro žádné čísla $a, c \in \mathbb{Z}$.

Vidíme tedy, že jen druhý případ povede k řešení rovnice. Dosazením $c = \pm 1$ do rovnosti $(2a-3c) = \pm 11$, $b = 2c$ dostaneme možnosti $a_1 = -4$, $a_2 = 7$, $b = 3$ a $a_1 = 4$, $a_2 = -7$, $b = -3$. Hledáme primární prvočinitele, takže můžeme použít rovnou koeficienty, které splňují podmínky pro primární prvočinitel a získáme výsledek ve tvaru $\pi_1 = -4 + 3\omega$ a $\pi_2 = -7 - 3\omega$. Snadno se lze přesvědčit, že platí $\overline{\pi}_1 = \pi_2$ a naopak. Tedy $37 = \pi_1 \cdot \overline{\pi}_1$.

Pro výpočet hodnoty kubického mocninného symbolu $\left(\frac{13}{-4+3\omega}\right)_3$ nelze použít kubický zákon vzájemnosti. Budeme-li postupovat stejně jako pro číslo 37, dojdeme k výsledku $(-4-3\omega)(-1+3\omega) = 4-9\omega-9\omega^2 = 4-9\omega-9(-1-\omega) = 13$. Platí tedy, že $13 = (-4-3\omega)(-1+3\omega)$ a dále využitím tvrzení 4.5 (2) a kubického zákona vzájemnosti dostáváme

$$\left(\frac{13}{-4+3\omega}\right)_3 = \left(\frac{-4-3\omega}{-4+3\omega}\right)_3 \cdot \left(\frac{-1+3\omega}{-4+3\omega}\right)_3 = \left(\frac{-4+3\omega}{-4-3\omega}\right)_3 \cdot \left(\frac{-4+3\omega}{-1+3\omega}\right)_3$$

Jelikož $-4+3\omega \equiv 1\,(mod\ -4+3\omega)$ a $-4+3\omega \equiv 3\,(mod\ -1+3\omega)$ platí dle tvrzení 4.5 (3), že

$$\left(\frac{-4+3\omega}{-4-3\omega}\right)_3 \cdot \left(\frac{-4+3\omega}{-1+3\omega}\right)_3 = \left(\frac{1}{-4-3\omega}\right)_3 \cdot \left(\frac{3}{-1+3\omega}\right)_3.$$

Víme, že kongruence $x^3 \equiv 1\,(mod\ \pi)$ je řešitelná pro každé $\pi \in \mathbb{Z}[\omega]$. Proto $\left(\frac{1}{-4-3\omega}\right)_3 = 1$. Využijeme dále vztahu $3 = -\omega^2(1-\omega)^2$ a dostaneme

$$\left(\frac{3}{-1+3\omega}\right)_3 = \left(\frac{-1}{-1+3\omega}\right)_3 \cdot \left(\frac{\omega}{-1+3\omega}\right)_3^2 \cdot \left(\frac{1-\omega}{-1+3\omega}\right)_3^2.$$

Použitím věty 4.1 a vzhledem k tomu, že $\left(\frac{-1}{-1+3\omega}\right)_3 = 1$ dostáváme výsledek

$$\left(\frac{\omega}{-1+3\omega}\right)_3^2 \cdot \left(\frac{1-\omega}{-1+3\omega}\right)_3^2 = \left(\omega^2\right)^2 \cdot \left(\omega^0\right)^2 = \omega \neq 1.$$

Kongruence tedy řešitelná není.

5 Bikvadratický zákon vzájemnosti

V této kapitole si ukážeme, jak pomocí bikvadratického zákona vzájemnosti rozhodovat o řešitelnosti kongruencí typu $x^4 \equiv a\,(mod\ p)$, kde $a \in \mathbb{Z}$ a p je prvočíslo. V několika případech se setkáme s analogickými větami a definicemi jako v předchozí kapitole.

5.1 Obor integrity $\mathbb{Z}[\mathrm{i}]$ podrobněji

Podobně jako v předchozí kapitole se nejprve podíváme na prvočinitele v oboru integrity $\mathbb{Z}[\mathrm{i}]$.

Tvrzení 5.1 *Je-li π je prvočinitel v $\mathbb{Z}[\mathrm{i}]$, potom existuje prvočíslo p takové, že $\pi \mid p$.*
Důkaz: Využijeme definici normy v $\mathbb{Z}[\mathrm{i}]$. Platí $\pi \cdot \overline{\pi} = N(\pi) = n \in \mathbb{N}$, tedy $\pi \mid n$. Víme, že n lze rozložit na součin konečně mnoha prvočísel $n = p_1 \cdot \ldots \cdot p_k$. Jelikož π je prvočinitel, tak bude existovat $i \in \{1, \ldots k\}$ takové, že $\pi \mid p_i$. □

Tvrzení 5.2 *Jestliže pro prvek $\pi \in \mathbb{Z}[\mathrm{i}]$ platí $N(\pi) = p$, kde p je prvočíslo, pak π je prvočinitel v $\mathbb{Z}[\mathrm{i}]$.*
Důkaz: Nechť $\pi = \gamma\delta$. Platí, že $N(\pi) = N(\gamma) \cdot N(\delta)$. Podle předpokladu je $N(\pi)$ rovna prvočíslu p a jedno z čísel $N(\gamma)$, $N(\delta)$ musí být rovno 1 a druhé prvočíslu p. Musí tedy být buď γ nebo δ jednotkou a tedy π je prvočinitel. □

Pomocí následující věty budeme schopni charakterizovat všechny prvočinitele v $\mathbb{Z}[\mathrm{i}]$.

Tvrzení 5.3 *Nechť p je prvočíslo, potom platí:*

(1) *Je-li $p = 2$, potom $2 = -\mathrm{i}(1+\mathrm{i})^2$ a $1+\mathrm{i}$ je prvočinitel v $\mathbb{Z}[\mathrm{i}]$.*

(2) *Jestliže $p \equiv 1\,(mod\ 4)$, potom $p = \pi\overline{\pi}$, kde π je prvočinitel v $\mathbb{Z}[\mathrm{i}]$ a prvky π a $\overline{\pi}$ nejsou asociované.*

(3) *Jestliže $p \equiv 3\,(mod\ 4)$, potom p je prvočinitel v $\mathbb{Z}[\mathrm{i}]$.*

Libovolný prvočinitel v $\mathbb{Z}[\omega]$ je asociovaný s jedním z prvočinitelů z bodů (1) - (3).
Důkaz: Z předchozí věty plyne, že $1+\mathrm{i}$ je prvočinitel v $\mathbb{Z}[\mathrm{i}]$. Snadno vypočítáme, že $-\mathrm{i}(1+\mathrm{i})^2 = -\mathrm{i}\left(1 + 2\mathrm{i} + \mathrm{i}^2\right) = -\mathrm{i} \cdot 2 - \mathrm{i} = 2$.

Předpokládejme nyní, že q není prvočinitel v $\mathbb{Z}[\mathrm{i}]$ a že pro q platí $q \equiv 3\,(mod\ 4)$. Prvek q lze tedy psát ve tvaru $q = \alpha\beta$, kde $N(\alpha) > 1$ a $N(\beta) > 1$. Zároveň platí $q^2 = N(q) = N(\alpha\beta) = N(\alpha)N(\beta)$. Odtud musí být $N(\alpha) = N(\alpha) = q$. Položíme-li $\alpha = a + b\mathrm{i}$, kde $a, b \in \mathbb{Z}$, potom lze psát $q = a^2 + b^2$. Pro součet druhých mocnin libovolných celých čísel platí, že po dělení čtyřmi dávají jeden ze zbytků $0, 1, 2$. Tím ale dostáváme spor s předpokladem $q \equiv 3\,(mod\ 4)$, z

čehož plyne, že q je prvočinitelem v $\mathbb{Z}[\mathrm{i}]$.

Mějme nyní prvočíslo $p \equiv 1\,(mod\ 4)$. Číslo -1 je kvadratickým zbytkem modulo p a existuje tedy číslo $a \in \mathbb{Z}$ takové, že $a^2 \equiv -1\,(mod\ p)$, neboli $p \mid a^2 + 1$. Pokud by p byl prvočinitel v $\mathbb{Z}[\mathrm{i}]$, pak by musel dělit jeden z prvků $a + \mathrm{i}, a - \mathrm{i}$, což neplatí. Prvek p tedy není prvočinitel a lze jej psát ve tvaru $p = \pi\gamma$, kde π, γ nejsou jednotky. Víme, že platí $N(\pi)\,N(\gamma) = N(\pi\gamma) = N(p) = p^2$ a dále $p = N(\pi) = \pi\overline{\pi}$. π je tedy prvočinitel v $\mathbb{Z}[\mathrm{i}]$. Předpokládejme nyní, že prvky $\pi, \overline{\pi}$ jsou asociované. Tedy $\overline{\pi} \mid \pi$ a také $p \mid \pi^2$. Označme $\pi = c + d\mathrm{i}$. Potom platí $p \mid (c + d\mathrm{i})^2 = c^2 + 2cd\mathrm{i} - d^2$. Pro p tedy dostáváme $p \mid (c^2 - d^2)$ a zároveň $p \mid (2cd\mathrm{i})$. Jelikož c, d jsou celá čísla a p je prvočíslo, z druhé podmínky dostaneme následující možnosti:

1. $p \mid 2$, což je zřejmě spor s předpokladem $p \equiv 1\,(mod\ 4)$
2. $p \mid c \wedge p \mid (c^2 - d^2)$, zároveň tedy $p \mid d$
3. $p \mid d \wedge p \mid (c^2 - d^2)$, zároveň tedy $p \mid c$.

Celkově jsme tedy ukázali, že $p \mid c$ a zároveň $p \mid d$, z čehož již plyne, že $p \mid \pi$. To ale není možné, protože by muselo platit $N(p) \mid N(\pi)$, neboli $p^2 \mid p$. Prvky π a $\overline{\pi}$ tedy nemohou být asociované.

Zbývá již jen ukázat, že libovolný prvočinitel oboru $\mathbb{Z}[\mathrm{i}]$ je asociovaný s jedním z výše uvedených prvočinitelů. Nechť nyní π je libovolný prvočinitel. Platí tedy, že π dělí nějaké prvočíslo p. Toto prvočíslo lze dle 1. až 3. rozložit na součin prvočinitelů. Tento rozklad je jednoznačný až na asociovanost. Prvočinitel π tedy musí být asociovaný s jedním z výše uvedených prvočinitelů, vyskytujících se v tomto rozkladu. □

5.2 Bikvadratický mocninný symbol

Nejprve rozšíříme pojem kongruence na okruh Gaussových celých čísel.

Definice 5.1 Pro $\alpha, \beta, \gamma \in \mathbb{Z}[\mathrm{i}]$ značíme $\alpha \equiv \beta\,(mod\ \gamma)$, pokud $\gamma \mid (\alpha - \beta)$. Říkáme, že α je kongruentní β modulo γ.

Poznámka 5.1 Kořenem polynomu $x^2 + 1 = 0$ je číslo i, které je algebraickým celým číslem. Tato čísla tvoří okruh, jehož podokruhem je okruh celých čísel $\mathbb{Z}$. Proto také libovolná lineární kombinace čísel 1 a i je algebraickým celým číslem. Dostaneme tedy uspořádání $\mathbb{Z} < \mathbb{Z}[\mathrm{i}] < \Omega$, kde Ω je okruh algebraických celých čísel. Libovolná kongruence celých čísel je tedy kongruencí v okruhu $\mathbb{Z}[\mathrm{i}]$ a také libovolná kongruence v $\mathbb{Z}[\mathrm{i}]$ je kongruencí v okruhu Ω.

Prvky, které jsou spolu kongruentní modulo γ, můžeme sloučit do zbytkových tříd modulo γ a dostaneme tím okruh $\mathbb{Z}[\mathrm{i}]/\gamma\mathbb{Z}[\mathrm{i}]$. Tento okruh nazýváme *okruh zbytkových tříd modulo* γ.

Věta 5.1 *Nechť $\pi \in \mathbb{Z}[\mathrm{i}]$ je prvočinitel. Potom $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ je konečné těleso o $N(\pi)$ prvcích.*
Důkaz: Důkaz je analogický důkazu tvrzení 4.4. Stačí ukázat, že $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ je obor integrity o $N(\pi)$ prvcích.

Vidíme, že $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ je komutativní okruh bez dělitelů nuly.

Stejně jako v tvrzení 4.4 dokážeme, že pro prvočíselné prvočinitele $\pi = p \equiv 3\,(mod\ 4)$ platí

$$\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}] = \left\{[r+s\mathrm{i}]_p \mid 0 \leq r < p, 0 \leq s < p\right\}.$$

Pokud je naopak π prvočinitel takový, že $\pi\overline{\pi} = N(\pi) = p$ pro nějaké prvočíslo p, potom $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}] = \{[r]_\pi \mid 0 \leq r < p\}$. V obou případech je počet prvků oboru integrity $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ roven číslu $N(\pi)$. □

Jelikož z věty plyne, že multiplikativní grupa tělesa $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ má řád $N(\pi)-1$, můžeme přepsat malou Fermatovu větu následujícím způsobem.

Věta 5.2 *Nechť $\alpha \in \mathbb{Z}[\mathrm{i}]$ a π je prvočinitel takový, že $\pi \nmid \alpha$. Potom*

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

Důkaz: Jedná se o důsledek Lagrangeovy věty (viz lit. [3, str. 39]), který je aplikovaný na grupu $(Z[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}])^*$. □

Poznámka 5.2 *Pokud platí, že $N(\pi) \neq 2$, potom jsou zbytkové třídy v tělese $\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}]$ různé. Tyto třídy jsou reprezentované jednotkami $1, -1, \mathrm{i}, -\mathrm{i}$.*

Protože $\langle[\mathrm{i}]_\pi\rangle = \{[1]_\pi, [-1]_\pi, [\mathrm{i}]_\pi, [-\mathrm{i}]_\pi\}$ spolu s operací násobení zbytkových tříd tvoří cyklickou grupu řádu 4, plyne z Lagrangeovy věty, že 4 dělí řád multiplikativní grupy $(\mathbb{Z}[\mathrm{i}]/\pi\mathbb{Z}[\mathrm{i}])^*$. Tedy $4 \mid N(\pi) - 1$.

Věta 5.3 *Nechť $\alpha \in \mathbb{Z}[\mathrm{i}]$ a π je prvočinitel takový, že $N(\pi) \neq 2, \pi \neq \alpha$. Potom existuje jednoznačně určené číslo $m \in \{0,1,2,3\}$, pro které platí*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv \mathrm{i}^m\,(mod\ \pi).$$

Důkaz: Z předchozí věty víme, že $\pi \mid \alpha^{N(\pi)-1} - 1$. Výraz $\alpha^{N(\pi)-1} - 1$ lze rozložit následujícím způsobem

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

Jelikož π je prvočinitel, tak vzhledem k předchozí poznámce, π dělí právě jeden z činitelů na pravé straně.

□

Předchozí výsledky nám umožní zavést tzv. bikvadratický mocninný symbol. Jde o obdobu Legendreova symbolu v teorii kvadratických zbytků a kubického mocninného symbolu v teorii kubických zbytků.

Definice 5.2 Pro prvky $\alpha, \pi \in \mathbb{Z}[\mathrm{i}]$, kde π je prvočinitel, pro který platí, že $N(\pi) \neq 2$, definujeme *bikvadratický mocninný symbol* modulo π následujícím způsobem:

1. jestliže $\pi \mid \alpha$, klademe $\left(\frac{\alpha}{\pi}\right)_4 = 0$
2. jestliže $\pi \nmid \alpha$, definujeme $\left(\frac{\alpha}{\pi}\right)_4 \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$ podmínkou

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

Zaveďme pojem bikvadratický zbytek v okruhu $\mathbb{Z}[\mathrm{i}]$. Bude se jednat o analogii s kvadratickými zbytky z předchozích kapitol.

Definice 5.3 Nechť $\alpha, \gamma \in \mathbb{Z}[\mathrm{i}]$ a zároveň $(\alpha, \gamma) = 1$. Číslo α nazveme *bikvadratickým zbytkem modulo* γ, má-li kongruence $x^4 \equiv \alpha \,(mod\ \gamma)$ řešení v okruhu $\mathbb{Z}[\mathrm{i}]$. Tedy existuje-li $x \in \mathbb{Z}[\mathrm{i}]$ takové, že $x^4 \equiv \alpha \,(mod\ \gamma)$. Pokud žádné takové číslo neexistuje, řekneme, že α je *bikvadratickým nezbytkem modulo* γ.

Věta 5.4 *Nechť $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ a π je prvočinitel takový, že $N(\pi) \neq 2$,. Potom platí:*

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

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

(3) *je-li* $\alpha \equiv \beta \,(mod\ \pi)$, *potom* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$

(4) *Nechť* $\pi \nmid \alpha$. *Potom* $\left(\frac{\alpha}{\pi}\right)_4 = 1$, *právě když je kongruence* $x^4 \equiv \alpha \,(mod\ \pi)$ *řešitelná v* $\mathbb{Z}[\mathrm{i}]$.

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

Důkaz:

(1) Pokud $\pi \nmid \alpha$ je výsledek zřejmý přímo z definice bikvadratického mocninného symbolu. Jestliže naopak $\pi \mid \alpha$, potom $\pi \mid \alpha^{\frac{N(\pi)-1}{4}}$. Tedy $\alpha^{\frac{N(\pi)-1}{4}} \equiv 0 \,(mod\ \pi)$. Zároveň ale z definice bikvadratického mocninného symbolu platí $\left(\frac{\alpha}{\pi}\right)_4 = 0$.

(2) Využijeme výsledků z části (1).

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

Obě strany kongruence mohou nabývat pouze hodnot $0, 1, -1, \mathrm{i}, -\mathrm{i}$ a můžeme tedy kongruenci nahradit přímo hledanou rovností.

(3) Je-li $\alpha \equiv \beta \,(mod\ \pi)$ pak $\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N(\pi)-1}{4}} \equiv \beta^{\frac{N(\pi)-1}{4}} \equiv \left(\frac{\beta}{\pi}\right)_4 (mod\ \pi)$. Stejně jako v předchozí části důkazu můžeme od kongruence přejít k hledané rovnosti.

(4) „⇒“Nechť $\left(\frac{\alpha}{\pi}\right)_4 = 1$. Multiplikativní grupa tělesa $\mathbb{Z}[\mathrm{i}]\,\pi\mathbb{Z}[\mathrm{i}]$ je cyklická a tedy $\alpha \equiv \gamma^n \,(mod\ \pi)$ pro nějaké $n \in \mathbb{N}$. Využitím předchozích dvou částí věty dostaneme $1 = \left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\gamma^n}{\pi}\right)_4 = \left(\frac{\gamma}{\pi}\right)_4^n$. Tato rovnost je splněná v následujících případech:

a) $\left(\frac{\gamma}{\pi}\right)_4 = 1$, pro libovolné n

b) $\left(\frac{\gamma}{\pi}\right)_4^n = -1$, pro $2 \mid n$

c) $\left(\frac{\gamma}{\pi}\right)_4^n = \pm\mathrm{i}$, pro $4 \mid n$.

Pokud by nastala první nebo druhá možnost, potom by muselo platit $\gamma^{\frac{N(\pi)-1}{2}} \equiv 1 \,(mod\ \pi)$. Protože je ale γ generátor grupy $(\mathbb{Z}[\mathrm{i}]\,\pi\mathbb{Z}[\mathrm{i}])^*$ a má řád roven řádu této grupy, tj. $N(\pi) - 1$, není to možné. Musí tedy platit třetí možnost, podle které $4 \mid n$. Pokud položíme $x = \gamma^{\frac{n}{4}}$ dostaneme řešení dané kongruence.
„⇐“Označme δ řešení kongruence $x^4 \equiv \alpha \,(mod\ \pi)$. Vidíme, že $\pi \nmid \delta$ a pomocí předchozích částí, že $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\delta^4}{\pi}\right)_4 = \left(\frac{\delta}{\pi}\right)_4^4 = 1$.

(5) Využitím první části věty a vlastností komplexně sdružených čísel dostaneme

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} = \overline{\alpha}^{\frac{N(\pi)-1}{4}} \,(mod\ \overline{\pi}).$$

Pro normy čísel π a $\overline{\pi}$ platí, že $N(\pi) = \pi \cdot \overline{\pi} = \overline{\overline{\pi}} \cdot \overline{\pi} = N(\overline{\pi})$. Díky tomu a první části věty můžeme psát

$$\left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 = \overline{\alpha}^{\frac{N(\pi)-1}{4}} \,(mod\ \overline{\pi}).$$

Dostaneme tedy kongruenci $\overline{\left(\frac{\alpha}{\pi}\right)_4} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 mod\ \overline{\pi}$. Ze stejného důvodu jako v předchozích částech důkazu můžeme kongruenci nahradit rovnou hledanou rovností.

□

Věta 5.5 *Nechť $p \equiv 3 \,(mod\ 4)$ je prvočíslo, $a \in \mathbb{Z}$ takové, že $p \nmid a$. Potom*

$$\left(\frac{a}{p}\right)_4 = 1$$

Důkaz: Přímo z definice bikvadratického mocninného symbolu můžeme psát

$$\left(\frac{a}{p}\right)_4 \equiv a^{\frac{p^2-1}{4}} = \left(a^{p-1}\right)^{\frac{p+1}{4}} (mod\ p).$$

Podle malé Fermatovy věty platí

$$\left(a^{p-1}\right)^{\frac{p+1}{4}} \equiv 1^{\frac{p+1}{4}} = 1\,(mod\ p)$$

a dostáváme tak kongruenci

$$\left(\frac{a}{p}\right)_4 \equiv 1\,(mod\ p),$$

kterou můžeme nahradit přímo hledanou rovností. □

Odvodili jsme, že libovolné celé číslo nesoudělné s prvočíslem $p \equiv 3\,(mod\ 4)$ je bikvadratickým zbytkem modulo p a že v tomto případě je kongruence $x^4 \equiv a\,(mod\ p)$ řešitelná v $\mathbb{Z}[\mathrm{i}]$.

5.3 Bikvadratický zákon vzájemnosti

Definice 5.4 Řekneme, že prvočinitel $\pi \in \mathbb{Z}[\mathrm{i}]$ je *primární*, jestliže

$$\pi \equiv 1\,(mod\ 2+2\mathrm{i}).$$

Věta 5.6 *Prvočinitel $\pi = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ je primární, právě tehdy když platí buď $a \equiv 1\,(mod\ 4), b \equiv 0\,(mod\ 4)$, nebo $a \equiv 3\,(mod\ 4), b \equiv 2\,(mod\ 4)$.*
Důkaz: Nechť $\pi = a + b\mathrm{i}$ je prvočinitel v $\mathbb{Z}[\mathrm{i}]$. Aby byl primární, tak musí dle definice platit $2 + 2\mathrm{i} \mid (a-1) + b\mathrm{i}$. Což můžeme upravit

$$\frac{(a-1)+b\mathrm{i}}{2\cdot(1+\mathrm{i})} \cdot \frac{1-\mathrm{i}}{1-\mathrm{i}} = \frac{a+b-1}{4} + \frac{b-a+1}{4}\mathrm{i} \in \mathbb{Z}[\mathrm{i}].$$

Výrazy na pravé straně rovnosti jsou ekvivalentní podmínce $a + b \equiv 1\,(mod\ 4)$ a zároveň $a - b \equiv 1\,(mod\ 4)$. Po sečtení těchto kongruencí dostaneme dvě podmínky pro prvek a. A to $a \equiv 1\,(mod\ 4)$ a $a \equiv 3\,(mod\ 4)$. Dosazením do kongruence $a + b \equiv 1\,(mod\ 4)$ dostaneme hledané podmínky pro prvek b. □

Důsledek 5.1 *Jestliže π je primární prvočinitel v $\mathbb{Z}[\mathrm{i}]$, potom $N(\pi) \neq 2$.*
Důkaz: Pokud je π primární prvočinitel v $\mathbb{Z}[\mathrm{i}]$, potom díky předchozí větě dostaneme $N(\pi) = a^2 + b^2 \equiv 1\,(mod\ 4)$. Proto musí platit, že $N(\pi) \neq 2$. □

Věta 5.7 ***Bikvadratický zákon vzájemnosti*** *Nechť $\pi_1, \pi_2 \in \mathbb{Z}[\mathrm{i}]$ jsou primární prvočinitelé takoví, že $N(\pi_1) \neq N(\pi_2)$. Potom*

$$\left(\frac{\pi_1}{\pi_2}\right)_4 = \left(\frac{\pi_2}{\pi_1}\right)_4 \cdot (-1)^{\frac{N(\pi_1)-1}{4}\frac{N(\pi_2)-1}{4}}.$$

Důkaz: Důkaz této věty uvádět nebudeme, lze jej nalézt v knize [1, str. 123-127]. □

Věta 5.8 *Nechť $\pi = a + b\mathrm{i}$ je primární prvočinitel v $\mathbb{Z}[\mathrm{i}]$. Potom platí:*

1. $\left(\frac{\mathrm{i}}{\pi}\right)_4 = i^{-\frac{a-1}{2}}$
2. $\left(\frac{1+\mathrm{i}}{\pi}\right)_4 = i^{-\frac{a-b-1-b^2}{4}}$.

Důkaz:

1. Podle věty 5.4 je $\left(\frac{\mathrm{i}}{\pi}\right)_4 = i^{\frac{a^2+b^2-1}{4}}$. Vzhledem k možnostem pro hodnoty bikvadratického symbolu nám bude stačit dokázat rovnost $i^{\frac{a^2+b^2-1}{4}} = i^{-\frac{a-1}{2}}$. Tato rovnost bude splněna, právě když

$$\frac{a^2+b^2-1}{4} \equiv -\frac{a-1}{2}\,(mod\ 4).$$

Tuto kongruenci budeme dále upravovat

$$a^2+b^2-1 \equiv -2a+2\,(mod\ 16),$$

$$a^2++2a-3+b^2 \equiv 0\,(mod\ 16),$$

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

Podle věty 5.6 může nyní nastat jedna z následujících možností:

a) $a \equiv 1\,(mod\ 4) \wedge b \equiv 0\,(mod\ 4)$, tedy $(a-1)(a+3) \equiv 0\,(mod\ 16) \wedge b^2 \equiv 0\,(mod\ 16)$. To dává požadovanou kongruenci.

b) $a \equiv 3\,(mod\ 4) \wedge b \equiv 2\,(mod\ 4)$. Položíme-li $a = 4k+3, b = 4l+2$ pro nějaká $k, l \in \mathbb{Z}$ potom po dosazení dostaneme

$$(a-1)(a+3)+b^2 = (4k+2)(4k+6)+(4l+2)^2 = 16k^2+32k+16l^2+16l+16.$$

Tento výraz je zjevně dělitelný 16.

2. Důkaz této části pro náročnost uvádět nebudeme. Lze jej nalézt v knize [1, str. 136].

□

Věta 5.9 *Nechť $\pi = a + b\mathrm{i}$ je primární prvočinitel v $\mathbb{Z}[\mathrm{i}]$. Potom*

$$\left(\frac{2}{\pi}\right)_4 = i^{\frac{ab}{2}}.$$

Důkaz: Platí

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{(-\mathrm{i})(1+\mathrm{i})^2}{\pi}\right)_4 = \left(\frac{-\mathrm{i}}{\pi}\right)_4 \left(\frac{1+\mathrm{i}}{\pi}\right)_4^2.$$

S využitím předchozích poznatků, můžeme psát

$$\left(\frac{-\mathrm{i}}{\pi}\right)_4 = \mathrm{i}^{\frac{a-1}{2}}, \ \left(\frac{1+\mathrm{i}}{\pi}\right)_4^2 = \mathrm{i}^{\frac{a-b-1-b^2}{2}}.$$

Celkem tedy dostaneme

$$\left(\frac{2}{\pi}\right)_4 = \mathrm{i}^{a-1-\frac{b+b^2}{2}}.$$

Nyní potřebujeme ukázat, že $\mathrm{i}^{a-1-\frac{b+b^2}{2}} = \mathrm{i}^{\frac{ab}{2}}$. K tomu využijeme následující tvrzení. Je-li ς primitivní n-tá odmocnina z jedné a $\varsigma^x = \varsigma^y$, potom $x \equiv y\,(mod\ n)$.

Stačí tedy ukázat, že $a - 1 - \frac{b+b^2}{2} \equiv \frac{ab}{2}\,(mod\ 4)$. Neboli $4 \mid a - 1 - \frac{b+b^2}{2} - \frac{ab}{2}$ a $8 \mid 2a - 2 - b(1 + a + b)$. Rozebereme obě možnosti z věty 5.6.

(i) Jestliže $a \equiv 1\,(mod\ 4) \wedge b \equiv 0\,(mod\ 4)$, potom $8 \mid 2a - 2$. Ze vztahů $4 \mid b$ a $2 \mid 1 + a + b$ plyne, že $8 \mid b(1 + a + b)$. Čímž již dostaneme hledaný výsledek.

(ii) Jestliže $a \equiv 3\,(mod\ 4) \wedge b \equiv 2\,(mod\ 4)$, potom $2a - 2 \equiv 4\,(mod\ 8)$ a vztahy $b \equiv 2\,(mod\ 4)$ a $1 + a + b \equiv 2\,(mod\ 4)$ lze vyjádřit ve tvaru $b = 4k + 2$ a $1 + a + b = 4l + 2$, pro $k, l \in \mathbb{Z}$. Tedy $b(1 + a + b) = (4k + 2)(4l + 2) \equiv 4\,(mod\ 8)$. Celkově tedy $2a - 2 - b(1 + a + b) \equiv 0\,(mod\ 8)$. Tím je důkaz hotov.

□

Příklad 5.1 Určete, zda je řešitelná kongruence $x^4 \equiv 11\,(mod\ 31)$.

Řešení: Protože prvočíslo 31 dává zbytek 3 po dělení 4, stačí když určíme, zda je řešitelná kongruence $x^2 \equiv 11\,(mod\ 31)$. Tuto kongruenci jsme již řešili v příkladu 3.2 a dokázali jsme, že řešení nemá. Není tedy řešitelná ani kongruence $x^4 \equiv 11\,(mod\ 31)$.

Příklad 5.2 Určete, zda je řešitelná kongruence $x^4 \equiv 13\,(mod\ 37)$.

Řešení: Prvočíslo $37 \equiv 1\,(mod\ 4)$. Musíme tedy najít primárního prvočinitele $\pi = a + b\mathrm{i}$, takového, aby $N(\pi) = a^2 + b^2 = 37$. Budeme uvažovat koeficienty splňující podmínky $a \equiv 1\,(mod\ 4), b \equiv 0\,(mod\ 4)$, nebo $a \equiv 3\,(mod\ 4), b \equiv 2\,(mod\ 4)$. Nejprve tedy první podmínka:

a) $b = 0$ a $a^2 = 37$

b) $b = \pm 4$ a $a^2 = 21$

c) $\mid b \mid \geq 8$ a $a^2 < 0$

Vidíme, že v tomto případě není možná ani jedna z variant a) - c).
Uvažujme $a \equiv 3\,(mod\ 4), b \equiv 2\,(mod\ 4)$. Pak mohou nastat následující možnosti:

d) $b = \pm 2$ a $a^2 = 33$

e) $b = \pm 6$ a $a^2 = \pm 1$

V tomto případě již najdeme koeficienty a, b vyhovující podmínkám, a to $b = \pm 6$ a $a = -1$. Našli jsme dva primární prvočinitele $-1 + 6\mathrm{i}$ a $-1 - 6\mathrm{i}$. Vybereme si ten první a budeme chtít zjistit hodnotu symbolu $\left(\frac{13}{-1+6\mathrm{i}}\right)_4$.Využijeme bikvadratický zákon vzájemnosti a postupně budeme upravovat

$$\left(\frac{13}{-1+6\mathrm{i}}\right)_4 = \left(\frac{-1+6\mathrm{i}}{13}\right)_4 (-1)^{\frac{168}{4}\frac{36}{4}} = \left(\frac{-1+6\mathrm{i}}{13}\right)_4.$$

Podle věty 5.4 budeme dále upravovat

$$\left(\frac{-1+6\mathrm{i}}{13}\right)_4 = \left(\frac{12+6\mathrm{i}}{13}\right)_4 = \left(\frac{2}{13}\right)_4 \cdot \left(\frac{3}{13}\right)_4 \cdot \left(\frac{2+\mathrm{i}}{13}\right)_4.$$

Jednotlivé symboly jsou rovny

$$\left(\frac{2}{13}\right)_4 = \mathrm{i}^0 = 1, \quad \text{podle věty 5.9}$$

$$\left(\frac{3}{13}\right)_4 = \left(\frac{13}{3}\right)_4 (-1)^{\frac{8}{4}\frac{168}{4}} = \left(\frac{13}{3}\right)_4 = 1, \quad \text{podle věty 5.5.}$$

Zbývá určit hodnotu symbolu $\left(\frac{2+\mathrm{i}}{13}\right)_4$. Protože $2 + \mathrm{i}$ není primární prvočinitel. Musíme postupovat následovně

$$\left(\frac{2+\mathrm{i}}{13}\right)_4 = \left(\frac{-\mathrm{i}}{13}\right)_4 \cdot \left(\frac{-1+2\mathrm{i}}{13}\right)_4.$$

Máme

$$\left(\frac{-\mathrm{i}}{13}\right)_4 = (-1)^6 \cdot \mathrm{i}^{-6} = -1.$$

Dále

$$\left(\frac{-1+2\mathrm{i}}{13}\right)_4 = \left(\frac{13}{-1+2\mathrm{i}}\right)_4 \cdot (-1)^{\frac{4}{4}\frac{168}{4}} = -\left(\frac{13}{-1+2\mathrm{i}}\right)_4$$

Celkově po vynásobení dostaneme

$$\left(\frac{2+\mathrm{i}}{13}\right)_4 = \left(\frac{13}{-1+2\mathrm{i}}\right)_4$$

Číslo 13 lze v $\mathbb{Z}[\mathrm{i}]$ rozložit na součin $13 = (3+2\mathrm{i})(3-2\mathrm{i})$. Musíme určit hodnoty symbolů $\left(\frac{3+2\mathrm{i}}{-1+2\mathrm{i}}\right)_4$ a $\left(\frac{3-2\mathrm{i}}{-1+2\mathrm{i}}\right)_4$.

Platí, že $3+2\mathrm{i} \equiv 4\,(mod\, -1+2\mathrm{i})$ a $3-2\mathrm{i} \equiv 2\,(mod\, -1+2\mathrm{i})$. Tím se nám situace velice zjednoduší a dojdeme k výsledku

$$\left(\frac{4}{-1+2\mathrm{i}}\right)_4 \cdot \left(\frac{2}{-1+2\mathrm{i}}\right)_4 = \mathrm{i}^{-3} = \mathrm{i}.$$

Celkem jsme tedy zjistili, že $\left(\frac{13}{-1+6\mathrm{i}}\right)_4 = \mathrm{i}$ a můžeme proto tvrdit, že kongruence $x^4 \equiv 13\,(mod\ 37)$ řešitelná není.

Závěr

Cílem práce bylo představit teorii zákonů vzájemnosti, a to kvadratického, kubického a bikvadratického. Práce obsahuje všechny potřebné netriviální základy pro snazší pochopení zákonů vzájemnosti. Jak je v textu několikrát zmíněno je mezi jednotlivými zákony určitá analogie. Postupovali jsme od základních pojmů, k formulování kvadratického a kubického zákon vzájemnosti až k bikvadratickému zákonu vzájemnosti. Ke každé zmíněné problematice jsou připojeny ilustrující příklady, pro snazší představu o využitelnosti uvedené teorie.

Naší snahou bylo vytvořit jednotný, ucelený a srozumitelný text, který bude pro zájemce o danou problematiku přínosný.

Literatura

[1] Ireland, K., Rosen, M., *A classical introduction to medern number theory*, 2nd ed., New York, N. Y.: Springer, 1990. xiv, 389 s. ISBN 0-387-97329-X

[2] Halaš, R., *Úvod do teorie čísel*, Olomouc: Univerzita Palackého v Olomouci, Přírodovědecká fakulta. 150 s. ISBN 978-80-244-4068-2

[3] Rosický, J., *Algebra 1*, Druhý dotisk čtvrtého, přepracovaného vydání, Brno: Masarykova univerzita, fakulta přírodovědecká, 2007. 133 s. ISBN 978-80-210-2964-4

[4] Beneš, P., *Zákony reciprocity*, [cit. 2014-06-18]. Diplomová práce. Masarykova univerzita, Přírodovědecká fakulta. Vedoucí práce Radan Kučera. Dostupné z: http://is.muni.cz/th/184497/prif_m/

[5] Lepka, K. *Malá Fermatova věta.* Učební text dostupný z: http://bart.math.muni.cz/ fuchs/ucitel/clanky/1_3_5.pdf