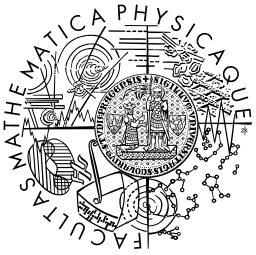

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁRSKA PRÁCA

Kristína Mišlanová

Matica Legendrových symbolov

Katedra algebry

Vedúci bakalárskej práce:	Mgr. Vítězslav Kala, Ph.D.
Študijný program:	Matematika
Študijný odbor:	Obecná matematika

Praha 2019

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

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

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

Chcela by som poďakovať svojmu vedúcemu Víťovi za skvelý výber témy, pomoc pri písaní práce, všetky cenné pripomienky a najmä za ochotu a čas strávený konzultáciami.

Názov práce: Matica Legendrových symbolov

Autor: Kristína Mišlanová

Katedra: Katedra algebry

Vedúci bakalárskej práce: Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: V tejto práci sa na začiatku budeme zaoberať charakterizáciou matíc kvadratických zvyškov príslušných k množine prvočiniteľov, ktorých jednotlivé prvky odpovedajú Legendrovým symbolom. Neskôr sa presunieme k maticiam kubických zvyškov, kde sú Legendrove symboly nahradené kubickými mocninnými symbolmi. Táto práca vychádza z článku [2], ktorého autori D. S. Dummit, E. P. Dummit a H. Kisilevsky zaviedli pojem týchto matíc pre primárne prvočinitele a dokázali niekoľko ich základných vlastností, predovšetkým charakterizovali blokový tvar týchto matíc. V práci sa pokúsime o zhrnutie príslušnej teórie spolu s výsledkami článku a následne o rozšírenie týchto výsledkov aj na komplikovanejšie prípady matíc, ktoré odpovedajú voľbe neprimárnych prvočiniteľov.

Kľúčové slová: znamienkové matice, Legendrov symbol, matice kvadratických zvyškov, kubický mocninný symbol, matice kubických zvyškov

Title: Matrix of Legendre symbols

Author: Kristína Mišlanová

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: In this thesis, we initially deal with the characterization of quadratic residue matrices associated to a set of prime elements, whose elements correspond to the Legendre symbols. Then we move to the cubic residue matrices, where the Legendre symbols are being replaced by cubic residue symbols. This work is based on the article [2] by D. S. Dummit, E. P. Dummit and H. Kisilevsky, who introduced the concept of these matrices for primary primes to prove several of their basic properties, in particular to characterize the block form of these matrices. In the work we summarize the relevant theory and the results of this article and then extend these results to the more complicated case of matrices that correspond to nonprimary prime elements.

Keywords: sign matrices, Legendre symbol, quadratic residue matrices, cubic residue symbol, cubic residue matrices

Obsah

Úvod

Legendrov symbol by sme dnes už kľudne mohli zaradiť medzi základné pojmy z teórie čísel. Dá sa pomocou neho úsporne zapísať a skúmať fakt, či číslo je alebo nie je kvadratickým zvyškom modulo konkrétne prvočíslo. Existuje veľmi prirodzený spôsob akým nejakej množine prvočísel priradiť maticu, ktorej prvky sú Legendrove symboly jednotlivých dvojíc týchto prvočísel. Tieto matice vyzerajú byť prirodzeným elementárnym objektom na skúmanie, avšak ako autori David S. Dummit, Evan P. Dummit a Hershy Kisilevsky článku [2] z roku 2016 tvrdia, nemajú žiadnu vedomosť o tom, že by sa tieto matice niekedy predtým vyskytli v literatúre. O týchto maticiach, budeme ďalej podobne ako v článku, hovoriť ako o maticiach kvadratických zvyškov.

Naskytajú sa preto otázky, či táto trieda matíc má nejaké spoločné vlastnosti? Existuje spôsob ako z ľubovoľnej matice zistiť, či je, alebo nie je maticou kvadratických zvyškov? Práve v tomto vyššie spomínanom článku [2], z ktorého budeme v celej práci vychádzať, sa autori vydali na cestu skúmania a charakterizácie týchto matíc. Ukázali, že matice kvadratických zvyškov majú veľmi špecifický blokový tvar, ktorý plynie z vlastností Legendrovho symbolu a zákonu kvadratickej reciprocity. Rovnako ukázali, že tento tvar je nielen nutnou, ale dokonca postačujúcou podmienkou na to, aby matica bola maticou kvadratických zvyškov. Okrem toho v článku uvádzajú veľmi peknú charakterizáciu, ako pomocou prvkov na hlavnej diagonále druhej mocniny ľubovoľnej matice zistiť, či je, alebo nie je maticou kvadratických zvyškov. V ďalších častiach článku sa autori presúvajú ku charakterizácií matíc kubických a kvartických zvyškov, ktorých jednotlivé prvky sú kubické alebo kvartické mocninné symboly, istá zovšeobecnená verzia Legendrových symbolov.

Jedným zo zámerov tejto práce bolo podrobnejšie spísať teóriu a vlastnosti Legendrových, kubických a kvartických mocninných symbolov, ktoré sa v článku automaticky využívajú a priniesť tak nad jednotlivé charakterizácie väčší nadhľad. Ďalší zámer súvisí s tým, že jednotlivé matice či už kvadratických alebo kubických zvyškov boli v článku [2] zadefinované a charakterizované iba pre primárne prvočinitele. Na konci článku však autori spomínajú možnosť rozšíriť túto teóriu aj na definície, ktoré pripúšťajú neprimárne prvočinitele. Dodávajú však, že túto triedu matíc považujú za ťažšie charakterizovateľnú. Ďalším a oveľa dôležitejším zámerom tejto práce bol práve pokus o spomínané rozšírenie v čo najväčšej podobe.

V práci teda môžeme nájsť podrobnú blokovú charakterizáciu pre rozšírené matice kvadratických aj kubických zvyškov. Ide o moje vlastné výsledky spolu s dôkazmi, ktoré sa nevyskytujú nikde publikované, aspoň pokiaľ je mi známe. Jednotlivé dôkazy boli inšpirované práve dôkazmi v článku [2], aj keď ide o značne náročnejšie rozšírenie problému.

V prvej kapitole zadefinujeme a krátko zhrnieme základné vlastnosti Legendrových symbolov.

V druhej kapitole sa presunieme ku charakterizácií matíc kvadratických zvyškov. Najprv v nej zavedieme tento pojem a potom v krátkosti zrhnieme a na príklade ukážeme výsledky z článku [2]. Následne prichádza vlastná charakterizácia rozšírených matíc kvadratických zvyškov aj na neprimárne prvočinitele spolu s kľúčovým dôkazom.

V kapitole číslo tri zhrnieme vlastnosti okruhu $\mathbb{Z}[\omega]$, v ktorom budeme ďalej pracovať a pokúsime sa vybudovať potrebnú teóriu k exaktnej definícií kubického mocninného symbolu. Teóriu v tejto časti čerpám predovšetkým z knihy K.Irelanda a M.Rosena [3]. Niektoré ďalšie časti sú z knihy [5], ktorú napísali M.R.Murty a J.Esmonde. Po zavedení kubického mocninného symbolu prejdeme k niekoľkým jeho základným vlastnostiam a vysvetlíme pojem primárneho prvočiniteľa a jeho voľby.

Štvrtá kapitola slúži opäť na charakterizáciu, tentokrát ale matíc kubických zvyškov. V úvode uvedieme definíciu a výsledky z článku, a následne prejdeme k rozšíreniu definície a novej vlastnej charakterizácií. K tejto charakterizácií budeme potrebovať dôsledok 4.5, ktorý plynie z Čebotarevovej vety. Tento dôsledok uvedieme v texte bez dôkazu len so stručným komentárom, keďže je nad rámec tejto práce.

V poslednej piatej kapitole už len stručne zhrnieme teóriu potrebnú k zadefinovaniu matíc kvartických zvyškov a výsledky charakterizačnej vety z článku [2], keďže ide o veľmi podobný prípad, akým sú matice kubických zvyškov.

1. Legendrov symbol

1.1 Vlastnosti Legendrových symbolov

V tejto kapitole uvedieme definíciu Legendrovho symbolu a niekoľko základných tvrdení bez dôkazov popisujúcich jeho vlastnosti, ktoré sú potrebné pre zvyšok práce. Dôkazy všetkých tvrdení sa dajú nájsť napríklad v skriptách A. Drápala k predmetu Teorie čísel a RSA [1, Kapitola 3].

Definícia 1.1 (kvadratický zvyšok)**.** *Nech $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Potom a je* kvadratický zvyšok *modulo n, ak existuje $b \in \mathbb{Z}$ také, že $a \equiv b^2 \mod n$. V opačnom prípade nazývame a* kvadratický nezvyšok *modulo n.*

Definícia 1.2 (Legendrov symbol)**.** *Nech p je nepárne prvočíslo, $a \in \mathbb{Z}$. Potom definujeme* Legendrov symbol $\left(\frac{a}{p}\right)$ *nasledovne:*

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

Veta 1.3 (Eulerovo kritérium)**.** *Nech p je nepárne prvočíslo. Potom pre všetky $a \in \mathbb{Z}$ platí*

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

Eulerovo kritérium nám ponúklo nový pohľad na prácu s Legendrovými symbolmi, a priamo z neho plynú dve nasledujúce základné vlastnosti.

Tvrdenie 1.4 (multiplikativita Legendrovho symbolu)**.** *Nech p je nepárne prvočíslo, $a, b \in \mathbb{Z}$. Potom platí*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Tvrdenie 1.5. *Nech p je nepárne prvočíslo. Potom platí*

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

Teda -1 je kvadratický zvyšok modulo p ak $p = 4k+1$ a kvadratický nezvyšok ak $p = 4k+3$ pre nejaké $k \in \mathbb{N}$.

Nakoniec uvedieme kľúčovú vetu pre nasledujúcu kapitolu práce, ktorá nám umožní podrobnejšie skúmať vlastnosti matíc Legendrových symbolov.

Veta 1.6 (zákon kvadratickej reciprocity)**.** *Nech p, q sú rôzne nepárne prvočísla. Potom platí nasledujúci vzťah*

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

2. Matice kvadratických zvyškov

2.1 Znamienkové matice a matice kvadratických zvyškov

Definícia 2.1 (znamienková matica)**.** *Štvorcovú maticu $n \times n$ nazveme* znamienkovou maticou *ak všetky jej prvky na hlavnej diagonále sú rovné* 0 *a všetky ostatné prvky sú rovné* ± 1.

Všetkých znamienkových matíc typu $n \times n$ je až 2^{n^2-n}. V takejto matici máme totiž n^2 prvkov, z čoho n prvkov na hlavnej diagonále je nutne rovných 0. Pre každý zo zvyšných $n^2 - n$ prvkov máme dve možnosti a nezávisle volíme jeho hodnotu ako 1 alebo -1. Z veľkého množstva znamienkových matíc sa ďalej budeme zaoberať iba tými, ktoré sú tvorené Legendrovými symbolmi pre istú množinu prvočiniteľov $p_1, p_2, \ldots, p_n$.

Definícia 2.2 (matica kvadratických zvyškov)**.** *Nech $p_1, p_2, \ldots p_n$ sú navzájom rôzne nepárne prvočinitele v obore celých čísel, navyše pre všetky $1 \leq i, j \leq n$ platí $p_i \neq -p_j$. Potom* matica kvadratických zvyškov *prislúchajúca k $p_1, p_2, \ldots p_n$ je matica $n \times n$, ktorá má na pozícii (i,j) Legendrov symbol $\left(\frac{p_i}{|p_j|}\right)$.*

Poznámka. V obore celých čísel je zaužívanejšie pomenovanie prvočíslo. Pojem prvočiniteľ sme použili práve preto, lebo v definícii chceme pri voľbe $p_1, p_2, \ldots, p_n$ pripustiť prvočísla, ale aj k nim asociované záporné prvočísla.

V článku [2] Dummit, Dummit a Kisilevsky používali zúženú definíciu matíc kvadratických zvyškov práve len na prvočísla. Vychádzajúc z tohto článku sa v práci pokúsime rozšíriť túto teóriu na väčšiu triedu matíc, ktorú považovali za ťažšie charakterizovateľnú. Rozšírenú triedu matíc získame práve povolením aj asociovaných prvočiniteľov v podobe záporných prvočísel.

Z definície môžeme priamo vidieť, že každá matica kvadratických zvyškov je iba špeciálnym prípadom znamienkovej matice. Na hlavnej diagonále sa nám na pozícii (i,i) vyskytne prvok $\left(\frac{p_i}{|p_i|}\right)$, ktorý je vždy rovný 0, keďže $|p_i|$ delí p_i. Zároveň na všetkých pozíciach (i,j) pre $i \neq j$ bude Legendrov symbol $\left(\frac{p_i}{|p_j|}\right)$, ktorý nadobúda hodnoty ± 1, keďže z definície plynie, že jednotlivé $p_1, p_2, \ldots, p_n$ sú navzájom nesúdeliteľné. Nesúdeliteľnosť máme zabezpečenú tým, že ide o prvočinitele, ktoré sú všetky navzájom rôzne a navyše platí $p_i \neq -p_j$ pre všetky $1 \leq i, j \leq n$.

Uvedieme konkrétny príklad, ako môže vyzerať matica kvadratických zvyškov.

Príklad. Nech $n = 5$ a zvolené prvočinitele p_1, p_2, p_3, p_4, p_5 sú v poradí 19, 17, 5, -13, -3. Potom príslušná matica kvadratických zvyškov má tvar:

$$\begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \end{array} \begin{array}{c} \begin{array}{ccccc} p_1 & p_2 & p_3 & p_4 & p_5 \end{array} \\ \begin{pmatrix} \left(\frac{19}{19}\right) & \left(\frac{19}{17}\right) & \left(\frac{19}{5}\right) & \left(\frac{19}{13}\right) & \left(\frac{19}{3}\right) \\ \left(\frac{17}{19}\right) & \left(\frac{17}{17}\right) & \left(\frac{17}{5}\right) & \left(\frac{17}{13}\right) & \left(\frac{17}{3}\right) \\ \left(\frac{5}{19}\right) & \left(\frac{5}{17}\right) & \left(\frac{5}{5}\right) & \left(\frac{5}{13}\right) & \left(\frac{5}{3}\right) \\ \left(\frac{-13}{19}\right) & \left(\frac{-13}{17}\right) & \left(\frac{-13}{5}\right) & \left(\frac{-13}{13}\right) & \left(\frac{-13}{3}\right) \\ \left(\frac{-3}{19}\right) & \left(\frac{-3}{17}\right) & \left(\frac{-3}{5}\right) & \left(\frac{-3}{13}\right) & \left(\frac{-3}{3}\right) \end{pmatrix} \end{array} = \begin{pmatrix} 0 & 1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 1 & -1 \\ 1 & -1 & 0 & -1 & -1 \\ 1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 \end{pmatrix}.$$

2.2 Invariantnosť pri konjugovaní permutačnou maticou

Vlastnosť byť maticou kvadratických zvyškov je invariantná na konjugovanie permutačnou maticou. Ak je M matica kvadratických zvyškov odpovedajúca v poradí prvočiniteľom $p_1, p_2, \ldots, p_n$, tak potom pre každú permutačnú maticu P rozmerov $n \times n$ platí, že aj matica PMP^{-1} je matica kvadratických zvyškov odpovedajúca rovnakej množine prvočiniteľov, ibaže usporiadaných v inom poradí.

Rovnako pre ľubovoľnú permutáciu $p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}$ poradia prvočiniteľov $p_1, p_2, \ldots, p_n$ vieme nájsť permutačnú maticu P tak, aby PMP^{-1} bola matica kvadratických zvyškov odpovedajúca v poradí prvočiniteľom $p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(n)}$.

Preto si pri skúmaní matíc kvadratických zvyškov môžeme pre množinu prvočiniteľov $p_1, p_2, \ldots, p_n$ zvoliť ako zástupcu jednu konkrétnu maticu na základe nejakého vhodného poradia týchto prvočiniteľov, ktorou sa budeme zaoberať. Zvyšné matice kvadratických zvyškov odpovedajúce tejto množine prvočiniteľov získame konjugovaním tohto zástupcu s permutačnými maticami.

2.3 Blokový tvar matice kvadratických zvyškov

Ďalej sa budeme zaoberať už iba znamienkovými maticami, ktoré odpovedajú maticiam kvadratických zvyškov. Dummit, Dummit a Kisilevsky zhrnuli charakterizáciu matíc kvadratických zvyškov v nasledujúcej vete, ktorú v tomto znení uviedli v článku [2, Theorem 1]. Pripomíname, že definícia v článku sa nezhoduje s definíciou 2.2, pretože pripúšťa ako prvočinitele iba kladné prvočísla.

Veta 2.3. *Nech M je znamienková matica $n \times n$. Potom sú nasledujúce tvrdenia ekvivalentné:*

a) Existuje $s \in \mathbb{N}$, $1 \leq s \leq n$ také, že matica M môže byť konjugovaná permutačnou maticou na blokovú maticu tvaru:

$$\left(\begin{array}{c|c} A & B \\ \hline B^T & S \end{array}\right),$$

kde A je $s \times s$ antisymetrická znamienková matica, S je $(n-s) \times (n-s)$ symetrická znamienková matica, B je $s \times (n-s)$ matica, ktorej všetky prvky sú ± 1 a B^T značí transponovanú maticu B.

b) Matica M je matica kvadratických zvyškov prislúchajúca rôznym nepárnym prvočíslam $p_1, p_2, \ldots, p_n$.

c) Existuje $s \in \mathbb{N}$, $1 \leq s \leq n$ také, že na hlavnej diagonále M^2 je s prvkov tvaru $n+1-2s$ a $n-s$ prvkov tvaru $n-1$.

Poznámka. Formulácia ekvivalencií nám nielenže popisuje ako matice kvadratických zvyškov vyzerajú, ale dáva nám aj návod, ako z ľubovoľnej znamienkovej matice zistiť, či je alebo nie je maticou kvadratických zvyškov. Jedna z možností je konjugovať maticu permutačnými maticami a zisťovať, či je vo vyššie popísanom blokovom tvare.

Druhá možnosť je maticu umocniť a pozrieť sa na prvky na hlavnej diagonále. Jediná možnosť, kedy by boli prvky $n-1$ a $n+1-2s$ nerozoznateľné, je prípad ak $s=1$. Ak sú teda všetky prvky na hlavnej diagonále rovnaké a rovné $n-1$, tak vieme, že $s=1$ (keďže možnosť $s=0$ je vo vete vylúčená). Inak vieme zistiť koľko prvkov na diagonále je tvaru $n-1$. Z tohto počtu vieme určiť hodnotu s a následne overiť, či zvyšných prvkov je práve s a ich hodnota je $n+1-2s$.

Príklad. Ak ostaneme pri zúženej definícii matíc kvadratických zvyškov a za prvočinitele zvolíme $p_1=3$, $p_2=5$, $p_3=7$, tak máme:

$$M=\begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}, \qquad M^2=\begin{pmatrix} 0 & 1 & 1 \\ -1 & 2 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

Na hlavnej diagonále M^2 sú prvky 0, 0, 2. Hodnota $n-1$ je 2, čiže ak má byť $n-s=3-s$ prvkov tvaru $n-1$, tak potom $s=2$. Zvyšné dva prvky majú mať hodnotu $n+1-2s=3+1-2\cdot 2=0$, čo platí. Zároveň existuje permutačná matica P taká, že matica PMP^{-1} je v požadovanom blokovom tvare:

$$PMP^{-1}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}=\left(\begin{array}{cc|c} 0 & -1 & -1 \\ 1 & 0 & -1 \\ \hline -1 & -1 & 0 \end{array}\right).$$

Ak si však vezmeme ľubovoľnú znamienkovú maticu:

$$M=\begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \qquad M^2=\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & -2 \end{pmatrix}.$$

V tomto prípade vidíme, že matica M^2 nemá na diagonále žiaden prvok tvaru $n-1=2$. To by muselo znamenať, že $s=n$ a nemá byť na diagonále žiaden takýto prvok. V takomto prípade by však museli byť všetky tri prvky na diagonále tvaru $n+1-2s$, a teda rovnaké. To sa tiež nestalo, čiže daná matica nie je maticou kvadratických zvyškov.

Hlavným cieľom práce bude skúmať matice kvadratických zvyškov podľa našej novej definície rozšírenej na všetky prvočinitele v $\mathbb{Z}$. V tejto časti ukážeme, že aj pre tieto matice platí, že musia byť v špecifickom blokovom tvare a naopak, že pre matice v takomto tvare už vždy skonštruujeme príslušné prvočinitele. Ide teda o ekvivalent tvrdení a), b) z vety 2.3.

Pred našou hlavnou vetou si ešte bez dôkazu uvedieme dve známe vety z teórie čísel, ktoré budeme potrebovať v nasledujúcom dôkaze. Dôkaz Čínskej zvyškovej vety môžeme nájsť napríklad v knihe [3, Chapter 3, §4, Theorem 1] a Dirichletovu vetu o prvočíslach v aritmetických postupnostiach nájdeme v knihe [6, Chapter 6].

Veta 2.4 (Čínska zvyšková veta)**.** *Nech $m_1, m_2, \ldots, m_n$ sú po dvoch nesúdeliteľné prirodzené čísla väčšie ako 1 a $a_1, a_2, \ldots, a_n$ sú ľubovoľné celé čísla. Potom vždy existuje riešenie x sústavy kongruencií:*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n. \end{aligned}$$

Pričom každé dve riešenia sú navzájom kongruentné modulo $M = m_1 m_2 \ldots m_n$.

Veta 2.5 (Dirichletova veta o prvočíslach v aritmetických postupnostiach)**.** *Pre každé dve nesúdeliteľné čísla $a, m \in \mathbb{N}$ aritmetická postupnosť $a, a+m, a+2m, \ldots$ obsahuje nekonečne veľa prvočísel.*

Poznámka. Dirichletova veta o prvočíslach v aritmetických postupnostiach nám hovorí, že pre nesúdeliteľné čísla $a, m \in \mathbb{N}$ existuje nekonečne mnoho prvočísel kongruentných a modulo m. Čo je význam, v ktorom ju neskôr použijeme.

Teraz už máme všetky nástroje potrebné na podrobný dôkaz hlavnej vety o blokovom tvare matíc kvadratických zvyškov. Jedná sa zároveň o dôkaz všeobecnejšej verzie časti vety 2.3 z článku [2], ktorým je inšpirovaný.

Veta 2.6 (blokový tvar matice kvadratických zvyškov)**.** *Nech M je znamienková matica $n \times n$. Potom sú nasledujúce tvrdenia ekvivalentné:*

a) Matica M je matica kvadratických zvyškov pre množinu nepárnych prvočiniteľov $p_1, p_2, \ldots, p_n$, kde pre všetky $1 \leq i, j \leq n$ také, že $i \neq j$ platí $p_i \nmid p_j$.

b) Existujú $k, l, m \in \mathbb{N}_0$ také, že platí $0 \leq k \leq l \leq m \leq n$ a matica M môže byť konjugovaná vhodne zvolenou permutačnou maticou na blokovú maticu tvaru:

$$N = \left(\begin{array}{c|c|c|c} A_1 & B & C & D \\ \hline B^T & S_1 & E & F \\ \hline -C^T & E^T & S_2 & G \\ \hline D^T & F^T & -G^T & A_2 \end{array}\right),$$

kde pre jednotlivé bloky platí:

- *A_1 je antisymetrická znamienková matica s rozmermi $k \times k$*
- *S_1 je symetrická znamienková matica s rozmermi $(l-k) \times (l-k)$*
- *S_2 je symetrická znamienková matica s rozmermi $(m-l) \times (m-l)$*
- *A_2 je antisymetrická znamienková matica s rozmermi $(n-m) \times (n-m)$*
- *B je matica s rozmermi $k \times (l-k)$ s prvkami rovnými ± 1*
- *C je matica s rozmermi $k \times (m-l)$ s prvkami rovnými ± 1*
- *D je matica s rozmermi $k \times (n-m)$ s prvkami rovnými ± 1*
- *E je matica s rozmermi $(l-k) \times (m-l)$ s prvkami rovnými ± 1*
- *F je matica s rozmermi $(l-k) \times (n-m)$ s prvkami rovnými ± 1*
- *G je matica s rozmermi $(m-l) \times (n-m)$ s prvkami rovnými ± 1.*

Dôkaz. $a) \Rightarrow b)$ Máme maticu M, ktorá je maticou kvadratických zvyškov pre prvočinitele $p_1, p_2, \ldots, p_n$. Z definície ide o nepárne prvočinitele, a teda pre všetky $1 \leq i \leq n$ platí, že $p_i \equiv 1 \mod 4$ alebo $p_i \equiv 3 \mod 4$. Príslušné prvočinitele môžeme teda zoradiť tak, aby platilo:

- $p_1, p_2, \ldots, p_k$ sú kladné a kongruentné 3 modulo 4,
- $p_{k+1}, p_{k+2}, \ldots, p_l$ sú kladné a kongruentné 1 modulo 4,
- $p_{l+1}, p_{l+2}, \ldots, p_m$ sú záporné a kongruentné 3 modulo 4,
- $p_{m+1}, p_{m+2}, \ldots, p_n$ sú záporné a kongruentné 1 modulo 4.

Získali sme tak hľadané $k, l, m \in \mathbb{N}_0$, pre ktoré platí $0 \leq k \leq l \leq m \leq n$. Je možné, že v niektorej z možností (prípadne aj viacerých) sa nenachádzal žiadny prvočiniteľ, čo odpovedá tomu, že medzi príslušnými neznámymi nastala rovnosť.

Podľa sekcie 2.2 vieme nájsť permutačnú maticu, ktorou keď konjugujeme maticu M, tak získame maticu N, ktorá je maticou kvadratických zvyškov pre naše nové poradie prvočiniteľov $p_1, p_2, \ldots, p_n$.

Rozdelíme si maticu N na blokovú maticu 4×4 a jednotlivé bloky označíme číslami 1 až 16 podľa nasledujúcej schémy:

	$p_1 \ldots p_k$	$p_{k+1} \ldots p_l$	$p_{l+1} \ldots p_m$	$p_{m+1} \ldots p_n$
p_1 $\vdots$ p_k	1	2	3	4
p_{k+1} $\vdots$ p_l	5	6	7	8
p_{l+1} $\vdots$ p_m	9	10	11	12
p_{m+1} $\vdots$ p_n	13	14	15	16

.

Rozmery jednotlivých blokov odpovedajú rozmerom v časti $b)$, ktorú chceme dokázať. Ukážeme, že majú aj požadované vlastnosti, čiže N je hľadaná matica.

Označme $N = (n_{i,j})$. Na hlavnej diagonále N sa vždy nachádza prvok $n_{i,i} = \left(\frac{p_i}{|p_i|}\right) = 0$. Mimo hlavnej diagonály, pre $i \neq j$ platí, že $n_{i,j} = \left(\frac{p_i}{|p_j|}\right) = \pm 1$, keďže sa jedná o Legendrov symbol a p_i a p_j sú nesúdeliteľné. Odtiaľ plynie, že bloky $1, 6, 11$ a 16 sú znamienkové matice a zvyšné bloky majú všetky prvky rovné ± 1.

Teraz sa pozrieme na jednotlivé bloky a na to, v akom vzťahu sú prvky na pozícií (i,j) a (j,i) pre $i \neq j$. Vieme, že $n_{i,j} = \left(\frac{p_i}{|p_j|}\right) = \pm 1$ a $n_{j,i} = \left(\frac{p_j}{|p_i|}\right) = \pm 1$. Vyčíslime hodnotu $n_{i,j} \cdot n_{j,i}$. Ak bude súčin rovný -1, tak to znamená, že činitele museli mať opačné znamienko a platí nutne $n_{i,j} = -n_{j,i}$. Naopak, ak bude súčin rovný 1, tak činitele mali rovnaké znamienko a platí $n_{i,j} = n_{j,i}$.

Blok 1

Prvky v tomto bloku sú $n_{i,j}$ pre $1 \leq i \leq k$ a $1 \leq j \leq k$. Pre ľubovoľný prvok $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$, pre $i \neq j$, potom platí $p_i \equiv 3 \mod 4$, $p_j \equiv 3 \mod 4$ a zároveň $p_i, p_j > 0$. Môžeme písať $p_i = 4x+3$ a $p_j = 4y+3$ pre $x, y \in \mathbb{N}_0$. Ich súčin vieme vyjadriť pomocou zákonu kvadratickej reciprocity (veta 1.6) nasledovne:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}} = (-1)^{\frac{4x+3-1}{2}\frac{4y+3-1}{2}}$$
$$= (-1)^{(2x+1)(2y+1)} = -1$$

Odtiaľ plynie $n_{i,j} = -n_{j,i}$ pre všetky $1 \leq i \leq k$, $1 \leq j \leq k$. Čo znamená, že blok 1 je antisymetrická znamienková matica. Môžeme ju označiť A_1.

Blok 6

Pre prvky $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ v bloku platí $k+1 \leq i \leq l$ a $k+1 \leq j \leq l$, z čoho plynie $p_i \equiv 1 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i, p_j > 0$. Môžeme písať $p_i = 4x+1$ a $p_j = 4y+1$ pre $x, y \in \mathbb{N}_0$. Súčin v prípade ak $i \neq j$:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = (-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}} = (-1)^{\frac{4x+1-1}{2}\frac{4y+1-1}{2}} = (-1)^{(2x)(2y)} = 1$$

Odkiaľ $n_{i,j} = n_{j,i}$ pre všetky $k+1 \leq i \leq l$ a $k+1 \leq j \leq l$. Blok 6 je symetrická znamienková matica, môžeme ju označiť S_1.

Blok 11

Pre prvky $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ v bloku platí $l+1 \leq i \leq m$ a $l+1 \leq j \leq m$, teda máme $p_i \equiv 3 \mod 4$, $p_j \equiv 3 \mod 4$ a $p_i, p_j < 0$. Položme $p_i = 4x+3$ a $p_j = 4y+3$ pre $x, y \in \mathbb{Z}$. Keďže $p_i, p_j < 0$, tak označme $q_i = -p_i$ a $q_j = -p_j$. Potom $q_i, q_j > 0$. V súčine pre $i \neq j$ využijeme multiplikativitu (1.4) a vyjadrenie $\left(\frac{-1}{p}\right)$ (1.5):

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{-q_i}{q_j}\right)\left(\frac{-q_j}{q_i}\right) = \left(\frac{-1}{q_j}\right)\left(\frac{-1}{q_i}\right)\left(\frac{q_i}{q_j}\right)\left(\frac{q_j}{q_i}\right)$$
$$= (-1)^{\frac{q_j-1}{2}}(-1)^{\frac{q_i-1}{2}}(-1)^{\frac{q_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{-(4y+3)-1}{2}+\frac{-(4x+3)-1}{2}+\frac{-(4x+3)-1}{2}\frac{-(4y+3)-1}{2}}$$
$$= (-1)^{-2y-2-2x-2+(-2x-2)(-2y-2)} = (-1)^{4xy+2x+2y} = 1$$

Odkiaľ $n_{i,j} = n_{j,i}$ pre všetky $l+1 \leq i \leq m$ a $l+1 \leq j \leq m$. Blok 11 je symetrická znamienková matica, môžeme ju označiť S_2.

Blok 16

Pre prvky $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ v tomto bloku platí $m+1 \leq i \leq n$ a $m+1 \leq j \leq n$, teda $p_i \equiv 1 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i, p_j < 0$. Môžeme písať $p_i = 4x+1$ a $p_j = 4y+1$ pre $x, y \in \mathbb{Z}$. Označme $q_i = -p_i$ a $q_j = -p_j$, potom $q_i, q_j > 0$. Súčin pre $i \neq j$:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{-q_i}{q_j}\right)\left(\frac{-q_j}{q_i}\right) = \left(\frac{-1}{q_j}\right)\left(\frac{-1}{q_i}\right)\left(\frac{q_i}{q_j}\right)\left(\frac{q_j}{q_i}\right)$$
$$= (-1)^{\frac{q_j-1}{2}}(-1)^{\frac{q_i-1}{2}}(-1)^{\frac{q_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{-(4y+1)-1}{2}+\frac{-(4x+1)-1}{2}+\frac{-(4x+1)-1}{2}\frac{-(4y+1)-1}{2}}$$
$$= (-1)^{-2y-1-2x-1+(-2x-1)(-2y-1)} = (-1)^{4xy-1} = -1$$

Odkiaľ $n_{i,j} = -n_{j,i}$ pre všetky $m+1 \leq i \leq n$ a $m+1 \leq j \leq n$. Blok 16 je antisymetrická znamienková matica, môžeme ju označiť A_2.

Blok 2 a 5

Prvky v bloku 2 sú $n_{i,j}$ pre $1 \leq i \leq k$ a $k+1 \leq j \leq l$. Pre ľubovoľný prvok $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ z bloku 2 potom platí $p_i \equiv 3 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i, p_j > 0$. Môžeme písať $p_i = 4x+3$ a $p_j = 4y+1$ pre $x, y \in \mathbb{N}_0$. Každý prvok $n_{i,j}$ z bloku 2 má svoj prvok s prehodenými súradnicami $n_{j,i}$ v bloku 5. Ich súčinom pomocou zákonu kvadratickej reciprocity (veta 1.6) zistíme vzťah medzi blokmi 2 a 5 v matici N:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}} = (-1)^{\frac{4x+3-1}{2}\frac{4y+1-1}{2}}$$
$$= (-1)^{(2x+1)(2y)} = (-1)^{4xy+2y} = 1$$

Odtiaľ plynie $n_{i,j} = n_{j,i}$ pre všetky $1 \leq i \leq k$, $k+1 \leq j \leq l$. Čo znamená, že blok 5 je transponovaný blok 2, pričom všetky prvky sú rovné ± 1. Môžeme blok 2 označiť ako B, potom blok 5 je B^T.

Blok 3 a 9

Prvky v bloku 3 sú $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ pre $1 \leq i \leq k$ a $l+1 \leq j \leq m$. Potom platí $p_i \equiv 3 \mod 4$, $p_j \equiv 3 \mod 4$ a zároveň $p_i > 0, p_j < 0$. Môžeme písať $p_i = 4x+3$ a $p_j = 4y+3$ pre $x, y \in \mathbb{Z}$. Označme $q_j = -p_j$, $q_j > 0$. Pre každý prvok $n_{i,j}$ z bloku 3 je $n_{j,i}$ v bloku 9. Ich súčin:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{q_j}\right)\left(\frac{-q_j}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$
$$= (-1)^{\frac{p_i-1}{2}}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{(4x+3)-1}{2}+\frac{(4x+3)-1}{2}\frac{-(4y+3)-1}{2}}$$
$$= (-1)^{2x+1+(2x+1)(-2y-2)} = (-1)^{-4xy-2x-2y-1} = -1$$

Odtiaľ plynie $n_{i,j} = -n_{j,i}$ pre všetky $1 \leq i \leq k$, $l+1 \leq j \leq m$. Čo znamená, že blok 9 je transponovaný blok 3 s opačnými znamienkami, pričom všetky prvky sú rovné ± 1. Môžeme blok 3 označiť ako C, potom blok 9 je $-C^T$.

Blok 4 a 13

Prvky v bloku 4 sú $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ pre $1 \leq i \leq k$ a $m+1 \leq j \leq n$. Potom platí $p_i \equiv 3 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i > 0, p_j < 0$. Môžeme písať $p_i = 4x+3$ a $p_j = 4y+1$ pre $x, y \in \mathbb{Z}$. Označme $q_j = -p_j$, $q_j > 0$. Pre každý prvok $n_{i,j}$ z bloku 4 je $n_{j,i}$ v bloku 13. Ich súčin:

$$n_{i,j} \cdot n_{j,i} = \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{q_j}\right)\left(\frac{-q_j}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$
$$= (-1)^{\frac{p_i-1}{2}}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{(4x+3)-1}{2}+\frac{(4x+3)-1}{2}\frac{-(4y+1)-1}{2}}$$
$$= (-1)^{2x+1+(2x+1)(-2y-1)} = (-1)^{-4xy-2y} = 1$$

Odtiaľ plynie $n_{i,j} = n_{j,i}$ pre všetky $1 \leq i \leq k$, $m+1 \leq j \leq n$. Čo znamená, že blok 13 je transponovaný blok 4, pričom všetky prvky sú rovné ± 1. Môžeme blok 4 označiť ako D, potom blok 13 je D^T.

Blok 7 a 10

Prvky v bloku 7 sú $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ pre $k+1 \leq i \leq l$ a $l+1 \leq j \leq m$. Potom platí $p_i \equiv 1 \mod 4$, $p_j \equiv 3 \mod 4$ a zároveň $p_i > 0, p_j < 0$. Môžeme písať $p_i = 4x+1$ a $p_j = 4y+3$ pre $x, y \in \mathbb{Z}$. Označme $q_j = -p_j$, $q_j > 0$. Pre každý prvok $n_{i,j}$ z bloku 7 je $n_{j,i}$ v bloku 10. Ich súčin:

$$\begin{aligned} n_{i,j} \cdot n_{j,i} &= \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{q_j}\right)\left(\frac{-q_j}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \\ &= (-1)^{\frac{p_i-1}{2}}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{(4x+1)-1}{2}+\frac{(4x+1)-1}{2}\frac{-(4y+3)-1}{2}} \\ &= (-1)^{2x+(2x)(-2y-2)} = (-1)^{-4xy-2x} = 1 \end{aligned}$$

Odtiaľ plynie $n_{i,j} = n_{j,i}$ pre všetky $k+1 \leq i \leq l$, $l+1 \leq j \leq m$. Čo znamená, že blok 10 je transponovaný blok 7, pričom všetky prvky sú rovné ± 1. Môžeme blok 7 označiť ako E, potom blok 10 je E^T.

Blok 8 a 14

Prvky v bloku 8 sú $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ pre $k+1 \leq i \leq l$ a $m+1 \leq j \leq n$. Potom platí $p_i \equiv 1 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i > 0, p_j < 0$. Môžeme písať $p_i = 4x+1$ a $p_j = 4y+1$ pre $x, y \in \mathbb{Z}$. Označme $q_j = -p_j$, $q_j > 0$. Pre každý prvok $n_{i,j}$ z bloku 8 je $n_{j,i}$ v bloku 14. Ich súčin:

$$\begin{aligned} n_{i,j} \cdot n_{j,i} &= \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{p_i}{q_j}\right)\left(\frac{-q_j}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \\ &= (-1)^{\frac{p_i-1}{2}}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{(4x+1)-1}{2}+\frac{(4x+1)-1}{2}\frac{-(4y+1)-1}{2}} \\ &= (-1)^{2x+(2x)(-2y-1)} = (-1)^{-4xy} = 1 \end{aligned}$$

Odtiaľ plynie $n_{i,j} = n_{j,i}$ pre všetky $k+1 \leq i \leq l$, $m+1 \leq j \leq n$. Čo znamená, že blok 14 je transponovaný blok 8, pričom všetky prvky sú rovné ± 1. Môžeme blok 8 označiť ako F, potom blok 14 je F^T.

Blok 12 a 15

Prvky v bloku 12 sú $n_{i,j} = \left(\frac{p_i}{|p_j|}\right)$ pre $l+1 \leq i \leq m$ a $m+1 \leq j \leq n$. Potom platí $p_i \equiv 3 \mod 4$, $p_j \equiv 1 \mod 4$ a zároveň $p_i, p_j < 0$. Môžeme písať $p_i = 4x+3$ a $p_j = 4y+1$ pre $x, y \in \mathbb{Z}$. Označme $q_i = -p_i$, $q_j = -p_j$ potom q_i,$q_j > 0$. Pre každý prvok $n_{i,j}$ z bloku 12 je $n_{j,i}$ v bloku 15. Ich súčin:

$$\begin{aligned} n_{i,j} \cdot n_{j,i} &= \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \left(\frac{-q_i}{q_j}\right)\left(\frac{-q_j}{q_i}\right) = \left(\frac{-1}{q_j}\right)\left(\frac{-1}{q_i}\right)\left(\frac{q_i}{q_j}\right)\left(\frac{q_j}{q_i}\right) \\ &= (-1)^{\frac{q_j-1}{2}}(-1)^{\frac{q_i-1}{2}}(-1)^{\frac{q_i-1}{2}\frac{q_j-1}{2}} = (-1)^{\frac{-(4y+1)-1}{2}+\frac{-(4x+3)-1}{2}+\frac{-(4x+3)-1}{2}\frac{-(4y+1)-1}{2}} \\ &= (-1)^{-2y-1-2x-2+(-2x-2)(-2y-1)} = (-1)^{4xy+2y-1} = -1 \end{aligned}$$

Odtiaľ plynie $n_{i,j} = -n_{j,i}$ pre všetky $l+1 \leq i \leq m$, $m+1 \leq j \leq n$. Čo znamená, že blok 15 je transponovaný blok 12 s opačnými znamienkami, pričom všetky prvky sú rovné ± 1. Môžeme blok 12 označiť ako G, potom blok 15 je $-G^T$.

Ukázali sme, že N je bloková matica tvaru:

$$\begin{array}{c|c|c|c|c} & p_1 \dots p_k & p_{k+1} \dots p_l & p_{l+1} \dots p_m & p_{m+1} \dots p_n \\ \hline p_1 \\ \vdots \\ p_k & A_1 & B & C & D \\ \hline p_{k+1} \\ \vdots \\ p_l & B^T & S_1 & E & F \\ \hline p_{l+1} \\ \vdots \\ p_m & -C^T & E^T & S_2 & G \\ \hline p_{m+1} \\ \vdots \\ p_n & D^T & F^T & -G^T & A_2 \end{array}.$$

$b) \Rightarrow a)$ Nech M je matica, ktorá sa dá konjugovať vhodne zvolenou permutačnou maticou na blokovú maticu $N = (n_{i,j})$, ktorá spĺňa podmienky tvrdenia $b)$. Ukážeme, že daná matica N je maticou kvadratických zvyškov pre nejaké prvočinitele $p_1, p_2, \dots, p_n$. Podľa sekcie 2.2 potom plynie, že aj M je maticou kvadratických zvyškov pre rovnakú množinu prvočiniteľov $p_1, p_2, \dots, p_n$, len v prepermutovanom poradí.

Induktívne skonštruujeme prvočinitele $p_1, p_2, \dots, p_n$, pre ktoré je N maticou kvadratických zvyškov. Budeme požadovať, aby v závislosti na k, l, m a n platili nasledujúce podmienky:

- $p_1, p_2, \dots, p_k$ sú kladné a kongruentné 3 modulo 4
- $p_{k+1}, p_{k+2}, \dots, p_l$ sú kladné a kongruentné 1 modulo 4
- $p_{l+1}, p_{l+2}, \dots, p_m$ sú záporné a kongruentné 3 modulo 4
- $p_{m+1}, p_{m+2}, \dots, p_n$ sú záporné a kongruentné 1 modulo 4.

V prvom kroku volíme prvočiniteľ p_1 ľubovoľne tak, aby spĺňal nasledujúcu podmienku:

- ak $k > 0$ potom $p_1 \equiv 3 \mod 4$ a $p_1 > 0$,
- ak $k = 0$ a zároveň $l > 0$ potom $p_1 \equiv 1 \mod 4$ a $p_1 > 0$,
- ak $k = l = 0$ a zároveň $m > 0$ potom $p_1 \equiv 3 \mod 4$ a $p_1 < 0$,
- ak $k = l = m = 0$ potom $p_1 \equiv 1 \mod 4$ a $p_1 < 0$.

Z indukčného predpokladu majme prvočinitele $p_1, p_2, \dots, p_s$. Pričom p_i podľa veľkosti indexu i spĺňa to, či má byť kladný, respektíve záporný, a aký zvyšok má mať modulo 4, podľa vyššie uvedených kategórií. Navyše pre všetky $1 \leq i, j \leq s$ platí $\left(\frac{p_i}{|p_j|}\right) = n_{i,j}$.

Teraz skonštruujeme prvočiniteľ p_{s+1} tak, aby pre všetky $1 \leq i, j \leq s$ platilo $\left(\frac{p_i}{|p_{s+1}|}\right) = n_{i,s+1}$ a $\left(\frac{p_{s+1}}{|p_j|}\right) = n_{s+1,j}$.

$$\begin{array}{c} \\ p_1 \\ p_2 \\ \vdots \\ p_s \\ p_{s+1} \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccccc} p_1 & p_2 & \dots & p_s & p_{s+1} & \dots \end{array} \\ \begin{pmatrix} 0 & n_{1,2} & \dots & n_{1,s} & n_{1,s+1} & \\ n_{2,1} & 0 & \dots & n_{2,s} & n_{2,s+1} & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ n_{s,1} & n_{s,2} & \dots & 0 & n_{s,s+1} & \\ n_{s+1,1} & n_{s+1,2} & \dots & n_{s+1,s} & 0 & \\ & & & & & \end{pmatrix} \end{array}$$

Pre všetky $1 \leq j \leq s$ ľubovoľne zvolíme nenulový prvok u_j modulo $|p_j|$ tak, aby platilo $\left(\frac{u_j}{|p_j|}\right) = n_{s+1,j}$.

Teraz si rozoberieme niekoľko prípadov podľa hodnoty indexu s:

- Ak $s < k$, tak hľadáme prvočiniteľ $p_{s+1} > 0$ a $p_{s+1} \equiv 3 \mod 4$. Označme $a = 3$.
- Ak $k \leq s < l$, tak hľadáme prvočiniteľ $p_{s+1} > 0$ a $p_{s+1} \equiv 1 \mod 4$. Označme $a = 1$.
- Ak $l \leq s < m$, tak hľadáme prvočiniteľ $p_{s+1} < 0$ a $p_{s+1} \equiv 3 \mod 4$. Položíme $q_{s+1} = -p_{s+1}$ a našu úlohu preformulujeme tak, že hľadáme prvočiniteľ $q_{s+1} > 0$ a $q_{s+1} \equiv -p_{s+1} \equiv -3 \equiv 1 \mod 4$. Označme $a = 1$.
- Ak $m \leq s$, tak hľadáme prvočiniteľ $p_{s+1} < 0$ a $p_{s+1} \equiv 1 \mod 4$. Položíme $q_{s+1} = -p_{s+1}$ a našu úlohu preformulujeme tak, že hľadáme prvočiniteľ $q_{s+1} > 0$ a $q_{s+1} \equiv -p_{s+1} \equiv -1 \equiv 3 \mod 4$. Označme $a = 3$.

Prvočinitele $|p_1|, |p_2|, \dots, |p_s|$ a 4 sú všetky navzájom rôzne a po dvoch nesúdeliteľné prirodzené čísla, takže podľa Čínskej zvyškovej vety (veta 2.4) existuje riešenie x sústavy kongruencií:

$$\begin{aligned} x &\equiv u_1 \mod |p_1| \\ x &\equiv u_2 \mod |p_2| \\ &\vdots \\ x &\equiv u_s \mod |p_s| \\ x &\equiv a \mod 4. \end{aligned}$$

Našli sme prirodzené číslo x, ktoré pre všetky $1 \leq j \leq s$ spĺňa $\left(\frac{x}{|p_j|}\right) = n_{s+1,j}$. A navyše, z Čínskej zvyškovej vety vieme, že x je so všetkými ostatnými riešeniami sústavy kongruentné modulo $|4p_1p_2 \dots p_s|$.

Úlohu sme si vyššie preformulovali tak, že hľadáme kladný prvočiniteľ p_{s+1}, respektíve q_{s+1}. Pre jednoduchosť značenia budeme teda ďalej písať, že hľadáme kladné prvočíslo p rôzne od $|p_1|, |p_2|, \dots |p_s|$. Budeme od neho požadovať, aby $p \equiv x \mod |4p_1p_2 \dots p_s|$. Potom pre všetky $1 \leq j \leq s$ dostaneme $\left(\frac{p}{|p_j|}\right) = n_{s+1,j}$, keďže by išlo o iné riešenie danej sústavy kongruencií. Posledným krokom konštrukcie ostáva ukázať, že vždy vieme takéto p nájsť.

Existenciu prvočísla p ukážeme pomocou Dirichletovej vety o prvočíslach v aritmetických postupnostiach (veta 2.5). Overíme predpoklad vety, že x a $|4p_1p_2\dots p_s|$ sú nesúdeliteľné čísla. To plynie z toho, že máme $\left(\frac{u_j}{|p_j|}\right) = n_{s+1,j} \neq 0$, čiže $|p_j|$ nedelí u_j. To znamená $NSD(u_j, |p_j|) = 1$ pre všetky $1 \leq j \leq s$. Takže ak $x \equiv u_j \mod |p_j|$, tak hneď dostávame $NSD(x, |p_j|) = 1$. Rovnako máme vďaka poslednej kongruencii v sústave aj $NSD(x, 4) = 1$. A teda dokopy platí, že x a $|4p_1p_2\dots p_s|$ sú nesúdeliteľné.

Keď už máme overené predpoklady, tak z Dirichletovej vety o prvočíslach plynie, že existuje nekonečne veľa prvočísel kongruentných x modulo $|4p_1p_2\dots p_s|$. Keďže ich existuje nekonečne veľa, tak určite vieme vybrať spomedzi nich také p, aby bolo rôzne od $|p_1|, |p_2|, \dots |p_s|$ a položiť $p_{s+1} = p$ prípadne $q_{s+1} = p$.

Vytvorili sme tak celú konštrukciu prvočiniteľa p_{s+1}, pre ktorý pre všetky $1 \leq j \leq s$ platí $\left(\frac{p_{s+1}}{|p_j|}\right) = n_{s+1,j}$. Vďaka podmienkam, ktoré sme si kládli na prvočinitele v závislosti na veľkostiach blokov a výpočtom v prvej implikácií platí, že Legendrove symboly $\left(\frac{p_{s+1}}{|p_j|}\right)$ a $\left(\frac{p_j}{|p_{s+1}|}\right)$ sú v rovnakom vzťahu ako prvky $n_{s+1,j}$ a $n_{j,s+1}$ vďaka blokovému tvaru matice N. Platí teda aj pre všetky $1 \leq i \leq s$, že $\left(\frac{p_i}{|p_{s+1}|}\right) = n_{i,s+1}$. Prvočiniteľ p_{s+1} tak spĺňa všetky požadované podmienky.

□

Príklad. Matica kvadratických zvyškov, ktorú sme si uviedli ako príklad na začiatku, odpovedala prvočiniteľom $p_1 = 19, p_2 = 17, p_3 = 5, p_4 = -13$ a $p_5 = -3$. Podľa konštrukcie v dôkaze vieme podľa zvyškov modulo 4 a toho, či sú prvočinitele kladné alebo záporné určiť, že $k = 1, l = 3, m = 4$ a $n = 5$. Z čoho priamo plynú rozmery jednotlivých blokov, ktoré keď v matici vyznačíme, tak vidíme, že spĺňajú podmienky symetrickosti respektíve antisymetrickosti z tvrdenia.

$$\left(\begin{array}{c|cc|cc} 0 & 1 & 1 & -1 & 1 \\ \hline 1 & 0 & -1 & 1 & -1 \\ 1 & -1 & 0 & -1 & -1 \\ \hline 1 & 1 & -1 & 0 & -1 \\ \hline 1 & -1 & -1 & 1 & 0 \end{array}\right) = \left(\begin{array}{c|c|c|c} A_1 & B & C & D \\ \hline B^T & S_1 & E & F \\ \hline -C^T & E^T & S_2 & G \\ \hline D^T & F^T & -G^T & A_2 \end{array}\right)$$

Daná charakterizačná veta nám slúži aj k tomu, že ak dostaneme ľubovoľnú znamienkovú maticu, tak vieme určiť, či sa jedná o maticu kvadratických zvyškov alebo nie. Stačí danú maticu iba konjugovať všetkými permutačnými maticami daného rozmeru a zistiť, či v nejakom prípade výsledná matica má požadovaný blokový tvar. V prípade, že je odpoveď kladná, tak nám dôkaz dokonca dáva aj nejaký návod, ako skonštruovať množinu prvočiniteľov, ktorým môže odpovedať.

2.4 Hlavná diagonála druhej mocniny matice kvadratických zvyškov

Ak je M matica kvadratických zvyškov, tak potom vieme odvodiť vzťah pre prvky nachádzajúce sa na hlavnej diagonále matice M^2, ktorý v tejto časti popíšeme nasledujúcou vetou. Ide o rozšírenie jednej z implikácií vo vete 2.3 z článku [2].

Veta 2.7. *Nech M je matica kvadratických zvyškov pre prvočinitele $p_1, p_2, \ldots, p_n$. Potom existujú $k, l, m \in \mathbb{N}_0$ také, že $0 \leq k \leq l \leq m \leq n$ a matica M^2 má na hlavnej diagonále:*

- *k prvkov tvaru $2l + 2k - 2m + n + 1$,*
- *$l - k$ prvkov tvaru $n - 1$,*
- *$m - l$ prvkov tvaru $2m - 2k - n - 1$,*
- *$n - m$ prvkov tvaru $2l - n + 1$.*

Dôkaz. Nech M je matica kvadratických zvyškov pre $p_1, p_2, \ldots, p_n$. Podľa vety 2.6 ju vieme permutačnou maticou konjugovať na maticu N v popísanom blokovom tvare.

Matica N^2 bude mať na diagonále rovnaké prvky ako matica M^2, ibaže v inom poradí. Môžeme teda kľudne pracovať ďalej s maticou N^2.

Prvok na diagonále N^2 sa dá vyjadriť ako:

$$(N^2)_{i,i} = \sum_{j=1}^{n} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = \sum_{j=1}^{k} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) + \sum_{j=k+1}^{l} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) + \sum_{j=l+1}^{m} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) + \sum_{j=m+1}^{n} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = X + Y + Z + W,$$

kde X, Y, Z a W predstavuje označenie jednotlivých súm v tomto poradí.

Presnú hodnotu jednotlivých súčinov $\left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = n_{i,j} \cdot n_{j,i} = \pm 1$ alebo 0 vieme vyjadriť podľa toho, v akých blokoch matice N sa jednotlivé činitele nachádzajú. Rozdelíme si teda určovanie hodnoty $(N^2)_{i,i}$ na štyri prípady podľa i.

Pre $1 \leq i \leq k$:

- Oba činitele $n_{i,j} = \left(\frac{p_i}{|p_j|}\right), n_{j,i} = \left(\frac{p_j}{|p_i|}\right)$ v jednom člene sumy X sa nachádzajú podľa indexov v bloku A_1, ktorým je antisymetrická matica, a teda platí $n_{i,j} = -n_{j,i}$. Z čoho máme pre $i \neq j$ vzťah $n_{i,j} \cdot n_{j,i} = -1$. Zároveň sa v sume X bude vyskytovať člen $\left(\frac{p_i}{|p_i|}\right)\left(\frac{p_i}{|p_i|}\right) = 0$. Platí preto:

$$X = \sum_{j=1}^{k} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = k \cdot (-1) + 1 = -k + 1.$$

- V jednom člene sumy Y sa bude vždy jeden z činiteľov nachádzať v bloku B a druhý v B^T. Platí preto vzťah $n_{i,j} = n_{j,i}$, čiže $n_{i,j} \cdot n_{j,i} = 1$. Odtiaľ:

$$Y = \sum_{j=k+1}^{l} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = (l - k) \cdot 1 = l - k.$$

- V jednom člene sumy Z sa bude vždy jeden z činiteľov nachádzať v bloku C a druhý v $-C^T$. Platí preto vzťah $n_{i,j} = -n_{j,i}$, čiže $n_{i,j} \cdot n_{j,i} = -1$. Odtiaľ:

$$Z = \sum_{j=l+1}^{m} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = (m - l) \cdot (-1) = l - m.$$

- V jednom člene sumy W sa bude vždy jeden z činiteľov nachádzať v bloku D a druhý v D^T. Platí preto vzťah $n_{i,j} = n_{j,i}$, čiže $n_{i,j} \cdot n_{j,i} = 1$. Odtiaľ:

$$W = \sum_{j=m+1}^{n} \left(\frac{p_i}{|p_j|}\right)\left(\frac{p_j}{|p_i|}\right) = (n-m)\cdot 1 = n-m.$$

Dokopy potom pre $1 \leq i \leq k$ máme:

$$\begin{aligned}(N^2)_{i,i} &= X + Y + Z + W = (-k+1) + (l-k) + (l-m) + (n-m)\\ &= 2l - 2k - 2m + n + 1.\end{aligned}$$

Pre všetky $1 \leq i \leq k$ platí, že $(N^2)_{i,i} = 2l - 2k - 2m + n + 1$. Čo je práve k prvkov na diagonále N^2 rovných $2l - 2k - 2m + n + 1$.

Vo zvyšných troch prípadoch budeme postupovať úplne analogicky. Všetky členy $n_{i,j} \cdot n_{j,i}$, pre $i \neq j$, každej zo súm X, Y, Z a W vždy nadobudnú rovnakú hodnotu 1 alebo -1, keďže budú vždy prislúchať rovnakým blokom matice N. Každá zo súm X, Y, Z a W teda vo všetkých prípadoch nadobudne hodnotu v tvare *počet členov* $\cdot\, 1$ alebo *počet členov* $\cdot\, (-1)$ poprípade ešte ± 1 za jediný nulový člen keď $i = j$. Uvedieme teda iba skrátené výpočty.

Pre $k+1 \leq i \leq l$:
Členy sumy X odpovedajú blokom B, B^T, sumy Y bloku S_1, sumy Z blokom E, E^T a sumy W blokom F, F^T. Potom platí:

$$\begin{aligned}(N^2)_{i,i} &= X + Y + Z + W = k\cdot 1 + (l-k)\cdot 1 - 1 + (m-l)\cdot 1 + (n-m)\cdot 1\\ &= n - 1.\end{aligned}$$

Matica N^2 má na hlavnej diagonále $l-k$ prvkov tvaru $n-1$.

Pre $l+1 \leq i \leq m$:
Členy sumy X odpovedajú blokom $C, -C^T$, sumy Y blokom E, E^T, sumy Z bloku S_2 a sumy W blokom $G, -G^T$. Potom platí:

$$\begin{aligned}(N^2)_{i,i} &= X + Y + Z + W = k\cdot(-1) + (l-k)\cdot 1 + (m-l)\cdot 1 - 1 +\\ &\quad + (n-m)\cdot(-1) = 2m - 2k - n - 1.\end{aligned}$$

Matica N^2 má na hlavnej diagonále $m-l$ prvkov tvaru $2m - 2k - n - 1$.

Pre $m+1 \leq i \leq n$:
Členy sumy X odpovedajú blokom D, D^T, sumy Y blokom F,F^T, sumy Z blokom $G, -G^T$ a sumy W bloku A_2. Potom platí:

$$\begin{aligned}(N^2)_{i,i} &= X + Y + Z + W = k\cdot 1 + (l-k)\cdot 1 + (m-l)\cdot(-1) +\\ &\quad + (n-m)\cdot(-1) + 1 = 2l - n + 1.\end{aligned}$$

Matica N^2 má na hlavnej diagonále $n-m$ prvkov tvaru $2l - n + 1$.

Tým sme ukázali, že matica N^2 má na hlavnej diagonále práve prvky spomínané v znení vety.

□

3. Okruh $\mathbb{Z}[\omega]$ a kubický mocninný symbol

3.1 Cyklotomické znamienkové matice

V druhej kapitole sme vychádzali z pojmu znamienkových matíc, ktorých diagonálne prvky boli rovné 0 a prvky mimo hlavnej diagonály ± 1. Prirodzená otázka, ktorá sa ponúka je, či sa dá daná skupina matíc nejako zovšeobecniť a následne aj problém matíc kvadratických zvyškov, ktorý sme rozoberali. Odpoveďou je priamo nasledujúca definícia cyklotomických znamienkových matíc.

Definícia 3.1 (m-té odmocniny z 1)**.** *Nech $m \in \mathbb{N}$, potom m-tá* odmocnina z 1 *je komplexné číslo α také, že $\alpha^m = 1$.*

Poznámka. Množina všetkých m-tých odmocnín z 1 má vždy m prvkov tvaru $U_m = \{e^{2k\pi i/m} \mid k = 0, 1, \ldots, m-1\}$.

Definícia 3.2 (cyklotomická znamienková matica pre m-té odmocniny z 1)**.** *Štvorcovú maticu $n \times n$ nazveme* cyklotomickou znamienkovou maticou pre m-té odmocniny z 1*, ak všetky jej prvky na hlavnej diagonále sú rovné 0 a všetky ostatné prvky mimo hlavnej diagonály sú m-té odmocniny z 1.*

Poznámka. Ide o zovšeobecnenie znamienkových matíc, ktoré odpovedajú cyklotomickým zmanienkovým maticiam pre $m = 2$, keďže prvky mimo hlavnej diagonály boli ± 1, čo sú práve druhé odmocniny z 1.

Vychádzajúc z rovnakých definícii ako Dummit, Dummit a Kisilevsky v článku [2] sa aj my budeme ďalej zaoberať len cyklotomickými maticami nízkych stupňov.

Definícia 3.3 (kubická znamienková matica, kvartická znamienková matica)**.** *Cyklotomická znamienková matica pre m-té odmocniny z 1 sa pre $m = 3$ nazýva* kubická znamienková matica *a pre $m = 4$* kvartická znamienková matica*.*

3.2 Okruh Eisensteinových celých čísel $\mathbb{Z}[\omega]$

Pre $m = 3$ pri skúmaní kubických znamienkových matíc je prirodzené uvažovať ako pole[1] $\mathbb{Q}(\sqrt{-3})$. V skutočnosti budeme pracovať v okruhu celistvých prvkov tohto poľa, teda v $\mathbb{Z}[\omega]$, kde $\omega = \frac{-1+\sqrt{-3}}{2}$. Prvky tohto okruhu sú komplexné čísla tvaru $a + b\omega$, kde $a, b \in \mathbb{Z}$. Okruh $\mathbb{Z}[\omega]$ sa nazýva aj Eisensteinove celé čísla.

V tejto podkapitole si najprv uvedieme niektoré zo základných vlastností okruhu $\mathbb{Z}[\omega]$, ako napríklad charakterizáciu jednotiek a prvočiniteľov.

Definícia 3.4 (norma)**.** *Nech $\alpha \in \mathbb{Z}[\omega]$ a platí $\alpha = a + b\omega$, pre $a, b \in \mathbb{Z}$. Potom* normu *prvku α definujeme vzťahom $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$.*

[1] V češtine sa namiesto výrazu pole využíva pomenovanie těleso.

Tvrdenie 3.5 (jednotky v $\mathbb{Z}[\omega]$)**.** *Prvok $\alpha \in \mathbb{Z}[\omega]$ je jednotkou tohoto okruhu práve vtedy, keď $N\alpha = 1$.*

Dôkaz nájdeme v knihe [3, Proposition 9.1.1] od K. Irelanda a M. Rosena.

Poznámka. Z charakterizácie uvedenej v poslednom tvrdení vyplýva, že jednotky v $\mathbb{Z}[\omega]$ sú práve prvky $1, -1, \omega, -\omega, \omega^2$ a $-\omega^2$.

Tvrdenie 3.6 (klasifikácia prvočiniteľov v $\mathbb{Z}[\omega]$)**.** *Nech p je prvočíslo v $\mathbb{Z}$. Potom platí:*

- *Ak $p = 3$, potom $1 - \omega$ je prvočiniteľ v $\mathbb{Z}[\omega]$ a platí $3 = -\omega^2(1-\omega)^2$.*
- *Ak $p \equiv 2 \mod 3$, potom p je prvočiniteľ v $\mathbb{Z}[\omega]$.*
- *Ak $p \equiv 1 \mod 3$, potom $p = \pi\overline{\pi}$, kde π je prvočiniteľ v $\mathbb{Z}[\omega]$.*

Dôkaz nájdeme v knihe [3, Proposition 9.1.4.].

Poznámka. Môžeme si všimnúť normu prvočiniteľov v jednotlivých prípadoch:

- Ak $p = 3$, potom $N(1-\omega) = 3$.
- Ak $p \equiv 2 \mod 3$, p prvočiniteľ. Potom $Np = p^2$ a odtiaľ $Np \equiv 1 \mod 3$.
- Ak $p \equiv 1 \mod 3$, $p = \pi\overline{\pi}$. Potom $p^2 = Np = N\pi N\overline{\pi}$ a keďže sa jedná o netriviálny rozklad, tak prvočiniteľ π má nutne normu $N\pi = p$. Odtiaľ máme $N\pi \equiv 1 \mod 3$.

3.3 Kubický mocninný symbol

Nato, aby sme mohli zadefinovať obdobu matíc kvadratických zvyškov v $\mathbb{Z}[\omega]$, potrebujeme ekvivalent Legendrovho symbolu, ktorým bude kubický mocninný symbol. Začneme tvrdeniami, ktoré nám následne zaručia jeho korektnú definíciu.

Tvrdenie 3.7. *Nech π je prvočiniteľ v $\mathbb{Z}[\omega]$. Potom $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ je konečné pole s $N\pi$ prvkami.*

Dôkaz nájdeme v [3, Proposition 9.2.1.].

Z čoho vyplýva, že multiplikatívna grupa $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ má rád $N\pi - 1$. Vďaka tomu máme v $\mathbb{Z}[\omega]$ analógiu Malej Fermatovej vety, ktorú si sformulujeme v nasledujúcom tvrdení a môžme ju nájsť v [3, Proposition 9.3.1.].

Tvrdenie 3.8. *Nech $\alpha \in \mathbb{Z}[\omega]$ a π je prvočiniteľ v $\mathbb{Z}[\omega]$ taký, že $\pi \nmid \alpha$. Potom platí:*

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

Podľa poznámky pod vetou o klasifikácii prvočiniteľov v $\mathbb{Z}[\omega]$ (tvrdenie 3.6) vidíme, že pre všetky prvočinitele π v $\mathbb{Z}[\omega]$ okrem $1-\omega$ platí, že $N\pi \equiv 1 \mod 3$. Ak teda pridáme predpoklad $N\pi \neq 3$, tak platí $3 \mid N\pi - 1$.

Tvrdenie 3.9. *Nech $\alpha \in \mathbb{Z}[\omega]$ a π je prvočiniteľ v $\mathbb{Z}[\omega]$ taký, že $N\pi \neq 3$ a zároveň $\pi \nmid \alpha$. Potom existuje jednoznačne určené $m = 0, 1$ alebo 2 také, že platí:*

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

Dôkaz nájdeme v [3, Proposition 9.3.2.].

Vďaka tvrdeniu 3.9 teraz už môžeme korektne zadefinovať kubický mocninný symbol.

Definícia 3.10 (kubický mocninný symbol)**.** *Nech $\alpha \in \mathbb{Z}[\omega]$ a π je prvočiniteľ v $\mathbb{Z}[\omega]$ taký, že $N\pi \neq 3$. Potom definujeme* kubický mocninný symbol *nasledovne:*

$$\left(\frac{\alpha}{\pi}\right)_3 \begin{cases} = 0 & \text{ak } \pi \mid \alpha, \\ \equiv \alpha^{\frac{N\pi-1}{3}} \mod \pi & \text{kde } \left(\frac{\alpha}{\pi}\right)_3 \text{ nadobúda hodnoty } 1, \omega \text{ alebo } \omega^2 \text{ ak } \pi \nmid \alpha. \end{cases}$$

Poznámka. Prvky $1, \omega$ a ω^2 sú všetko tretie odmocniny z 1, keďže platí $\omega^3 = 1$. Kubický mocninný symbol teda nadobúda iba hodnoty, ktoré odpovedajú tretím odmocninám z 1.

Uvedieme si niekoľko vlastností kubických mocninných symbolov, ktoré využijeme pri počítaní s nimi. Zhrnieme ich v jednej vete, pričom dôkazy k nim sa dajú nájsť v [3, Proposition 9.3.3., 9.3.4.].

Tvrdenie 3.11. *Nech $\alpha, \beta \in \mathbb{Z}[\omega]$, π je prvočiniteľ v $\mathbb{Z}[\omega]$. Potom platí:*

a) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *práve vtedy, ak existuje $x \neq 0$ také, že $x^3 \equiv \alpha \mod \pi$.*

b) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

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

Aj vďaka týmto vlastnostiam vieme odvodiť hodnoty kubických mocninných symbolov pre jednotky v $\mathbb{Z}[\omega]$. Zhrnieme a dokážeme si ich v nasledujúcom tvrdení.

Tvrdenie 3.12. *Nech π je prvočiniteľ v $\mathbb{Z}[\omega]$, $N\pi \neq 3$. Potom platí:*

a) $\left(\frac{1}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 = 1$.

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

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

Dôkaz. *a*) Plynie priamo z tvrdenia 3.11 a). Vieme zvoliť x rovné 1 respektíve -1, tak aby platila požadovaná kongruencia $x^3 \equiv \pm 1 \mod \pi$.

b) Rovnosť medzi symbolmi plynie priamo z výpočtu $\left(\frac{-\omega}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 \left(\frac{\omega}{\pi}\right)_3 = 1 \cdot \left(\frac{\omega}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3$ využívajúc vlastnosť multiplikativity z tvrdenia 3.11 a výsledku a).

Ukázali sme už, že $N\pi \equiv 1 \mod 3$, odtiaľ vidíme $N\pi \equiv 1, 4$ alebo $7 \mod 9$. Následne už len dosadíme hodnoty do definície kubického mocninného symbolu $\left(\frac{\omega}{\pi}\right)_3 \equiv \omega^{\frac{N\pi-1}{3}} \mod \pi$. Napríklad pre prípad ak $N\pi \equiv 4 \mod 9$, tak máme $\left(\frac{\omega}{\pi}\right)_3 \equiv \omega^{\frac{9k+4-1}{3}} \equiv \omega^{3k+1} \equiv (\omega^3)^k \cdot \omega \equiv 1 \cdot \omega \equiv \omega \mod \pi$. Takže máme $\left(\frac{\omega}{\pi}\right)_3 = \omega$ pre $N\pi \equiv 4 \mod 9$. Zvyšné dva prípady analogicky.

c) Rovnosť medzi príslušnými kubickými mocninnými symbolmi pre $-\omega^2$ a ω^2 dostávame analogicky ako v b). Následne z tvrdenia 3.11 c) máme rovnosť $\left(\frac{\omega^2}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3^2$, čiže jednotlivé hodnoty priamo odvodíme z b).

□

3.4 Primárny prvočiniteľ a kubická reciprocita

Definícia 3.13 (primárny prvočiniteľ)**.** *Nech π je prvočiniteľ v $\mathbb{Z}[\omega]$. Potom povieme, že π je* primárny prvočiniteľ *ak platí $\pi \equiv 2 \mod 3$.*

Poznámka. Ak $\pi = p$, kde p je prvočíslo v $\mathbb{Z}$, tak potom je π vždy primárnym prvočiniteľom, keďže platí $p \equiv 2 \mod 3$ (tvrdenie 3.6). V prípade, že $\pi = a + b\omega$, tak nám daná podmienka hovorí, že musí platiť $a \equiv 2 \mod 3$ a zároveň $b \equiv 0 \mod 3$.

Poznámka. Podotkneme len, že definícia primárneho prvočiniteľa sa líši od tej, ktorú využívali Dummit, Dummit a Kisilevsky v článku [2], ktorí považovali za primárny prvočiniteľ $\pi \equiv 1 \mod 3$. Nečiní to však žiaden zásadný rozdiel, keďže ide iba o prenásobenie 2. Našu definíciu môžeme odôvodniť tým, že chceme aby prvočísla zo $\mathbb{Z}$, ktoré ostanú prvočiniteľmi, boli priamo primárnymi.

V $\mathbb{Z}[\omega]$ máme 6 jednotiek, čo znamená, že každý nenulový prvok v $\mathbb{Z}[\omega]$ je asociovaný so 6 prvkami. Dôvod, prečo zavádzame pojem ako primárny prvočiniteľ je práve ten, aby sme sa vyhli tejto nejasnosti. Nasledujúca veta nám dokonca zaručuje jednoznačnosť výberu primárneho prvočiniteľa.

Veta 3.14 (jednoznačnosť primárneho prvočiniteľa)**.** *Nech π je prvočiniteľ v $\mathbb{Z}[\omega]$, $N\pi \neq 3$. Potom medzi prvkami asociovanými s π existuje práve jeden primárny prvočiniteľ.*

Dôkaz. Chceme zistiť počet tried modulo 3 v $\mathbb{Z}[\omega]$. Do úvahy pripadá 9 tried s reprezentantmi $0, 1, 2, 0+\omega, 1+\omega, 2+\omega, 0+2\omega, 1+2\omega, 2+2\omega$.

Nato, aby niektoré dva z týchto prvkov boli v rovnakej triede musí platiť, že 3 delí ich rozdiel. Ich rozdiel vieme zapísať ako $a + b\omega$, kde ale a, b nadobúdajú hodnoty $0, \pm 1$ alebo ± 2, nikdy nie sú však obe rovné 0 zároveň.

Platí, že prirodzené číslo $n \mid (a+b\omega)$ práve vtedy, keď $n \mid a$ a $n \mid b$. Takže nato, aby 3 delila rozdiel $a + b\omega$, by muselo platiť $a = b = 0$, čo je ale spor. Ukázali sme, že prvky $0, 1, 2, 0+\omega, 1+\omega, 2+\omega, 0+2\omega, 1+2\omega, 2+2\omega$ sú každý v inej triede.

Náš prvočiniteľ π patrí do niektorej z týchto deviatich rozkladových tried. Ukážeme, že nemôže patriť do rovnakej triedy ako $0, 2+\omega$ alebo $1+2\omega$.

Sporom, nech π patrí do rovnakej triedy ako $1+2\omega$, potom $\pi \equiv 1+2\omega \mod 3$. Keďže $\sqrt{-3}$ delí 3 v $\mathbb{Z}[\omega]$, tak z toho plynie, že $\pi \equiv 1+2\omega \mod \sqrt{-3}$. Lenže $1+2\omega = 1+(-1+\sqrt{-3}) = \sqrt{-3}$, čiže $\pi \equiv 0 \mod \sqrt{-3}$. Takže máme $\sqrt{-3}$ delí π. Keďže je však π prvočiniteľ, tak potom nutne $\sqrt{-3} \| \pi$. To je ale spor s predpokladom $N\pi \neq 3$. Úplne analogicky postupujeme aj vo zvyšných dvoch prípadoch.

Prvočiniteľ π patrí do jednej zo zvyšných 6 rozkladových tried s reprezentantmi $1, 2, 0+\omega, 1+\omega, 0+2\omega, 2+2\omega$. Ukážeme, že v každej z tried leží práve jedna jednotka okruhu $\mathbb{Z}[\omega]$. To, že v každej triede leží práve jedna jednotka, dostávame z nasledujúcich výpočtov a podobného argumentu ako vyššie, že 3 nedelí rozdiel žiadnych dvoch z nich.

- trieda $[1]$ obsahuje 1
- trieda $[2]$ obsahuje -1, pretože platí $2 \equiv -1 \mod 3$
- trieda $[\omega]$ obsahuje ω
- trieda $[1+\omega]$ obsahuje $-\omega^2$, pretože platí $1+\omega = 1+\frac{-1+\sqrt{-3}}{2} = \frac{1+\sqrt{-3}}{2} = -\omega^2$
- trieda $[2\omega]$ obsahuje $-\omega$, pretože platí $2\omega \equiv -\omega \mod 3$
- trieda $[2+2\omega]$ obsahuje ω^2, pretože platí $2+2\omega \equiv -1-\omega \equiv \omega^2 \mod 3$

Takže π patrí do jednej z tried $[1], [-1], [\omega], [-\omega], [\omega^2], [-\omega^2]$. Existuje teda jednoznačne určená jednotka ε v $\mathbb{Z}[\omega]$ taká, že platí $\pi \equiv \varepsilon \mod 3$. To je ekvivalentné $\pi \cdot \varepsilon^{-1} \equiv 1 \mod 3$, odkiaľ po prenásobení -1 dostávame $\pi(-\varepsilon^{-1}) \equiv 2 \mod 3$. Keďže $-\varepsilon^{-1}$ je opäť jednotka v $\mathbb{Z}[\omega]$, tak sme našli jednoznačne určený asociovaný prvočiniteľ $\pi(-\varepsilon^{-1})$ s prvočiniteľom π, ktorý je primárny.

□

Pre kubické mocninné symboly existuje v $\mathbb{Z}[\omega]$ ekvivalent zákonu kvadratickej reciprocity, ktorá platila v $\mathbb{Z}$ pre Legendrove symboly. Ide o zákon kubickej reciprocity, ktorý už aktuálne s pomocou pojmu primárneho prvočiniteľa môžeme sformulovať.

Veta 3.15 (zákon kubickej reciprocity)**.** *Nech π_1, π_2 sú primárne prvočinitele v $\mathbb{Z}[\omega]$, $N\pi_1 \neq 3$, $N\pi_2 \neq 3$. Potom platí vzťah:*

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

M. R. Murty a J. Esmonde sformulovali dôkaz v knihe [5, Theorem 9.1.16.].

4. Matice kubických zvyškov

4.1 Primárne matice kubických zvyškov

V tejto chvíli už máme vybudovanú potrebnú teóriu, aby sme mohli zadefinovať špeciálnu triedu kubických znamienkových matíc, ktoré budeme nazývať primárnymi maticami kubických zvyškov. Vychádzame z podobnej definície ako v článku [2].

Definícia 4.1 (primárna matica kubických zvyškov)**.** *Nech $\pi_1, \pi_2, \ldots, \pi_n$ sú prvočinitele v $\mathbb{Z}[\omega]$, pre všetky $1 \leq i \leq n$ platí $N\pi_i \neq 3$. Navyše pre všetky $i \neq j$ platí $\pi_i \nmid \pi_j$. Označme $\sigma_1, \sigma_2, \ldots, \sigma_n$ postupne primárne prvočinitele k $\pi_1, \pi_2, \ldots, \pi_n$. Potom* primárna matica kubických zvyškov *je matica $n \times n$, ktorá má na pozícii (i,j) kubický mocninný symbol $\left(\frac{\sigma_i}{\sigma_j}\right)_3$.*

Poznámka. V článku [2] nazývajú tieto matice priamo maticami kubických zvyškov, my sme si dovolili pozmeniť názov na primárne matice kubických zvyškov, keďže ich ďalej budeme chcieť ešte zovšeobecniť a zredukovať podmienku primárnych prvočiniteľov. Ďalej pracujeme priamo s prvočiniteľmi a k nim asociovanými primárnymi prvočiniteľmi, kým v článku sa hovorí o prvoideáloch a ich generátoroch, respektíve primárnych generátoroch.

Obdobne, ako pri maticiach kvadratických zvyškov, sa Dummit, Dummit a Kisilevsky v článku [2] zaoberali charakterizáciou blokového tvaru týchto matíc. Dokázali, že v tomto prípade je tento problém dokonca jednoduchší, pretože ide o symetrickú maticu. Nasledujúca veta je z článku [2, Theorem 2].

Veta 4.2. *Nech M je $n \times n$ kubická znamienková matica. Potom sú nasledujúce tvrdenia ekvivalentné:*

a) Matica M je primárna matica kubických zvyškov pre prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$ také, že pre všetky $1 \leq i \leq n$ platí $N\pi_i \neq 3$ a zároveň pre všetky $1 \leq i,j \leq n$, $i \neq j$ platí $\pi_i \nmid \pi_j$.

b) Matica M je symetrická.

To, že primárna matica kubických zvyškov je symetrická matica, je vidieť priamo zo zákona kubickej reciprocity.

4.2 Matice kubických zvyškov

Už pri maticiach kvadratických zvyškov sme rozšírili definíciu z primárnych prvočiniteľov (kladné prvočísla) aj na neprimárne prvočinitele (asociované záporné prvočísla). Teraz sa pri maticiach kubických zvyškov pokúsime o podobný krok povolením aj neprimárnych prvočiniteľov hore v kubickom mocninnom symbole.

Definícia 4.3 (matica kubických zvyškov)**.** *Nech $\pi_1, \pi_2, \ldots, \pi_n$ sú prvočinitele v $\mathbb{Z}[\omega]$, pre všetky $1 \leq i \leq n$ platí $N\pi_i \neq 3$. Navyše pre všetky $i \neq j$ platí $\pi_i \nmid \pi_j$. Označme $\sigma_1, \sigma_2, \ldots, \sigma_n$ postupne primárne prvočinitele k $\pi_1, \pi_2, \ldots, \pi_n$. Potom* matica kubických zvyškov *je matica $n \times n$, ktorá má na pozícii (i,j) kubický mocninný symbol $\left(\frac{\pi_i}{\sigma_j}\right)_3$.*

Keď sme pri maticiach kvadratických zvyškov chceli rozšíriť teóriu o blokovom tvare matice, tak sme sa vo výpočtoch museli vysporiadať s Legendrovými symbolmi tvaru $\left(\frac{-q_i}{q_j}\right)$. Tie sme pomocou multiplikativity rozdelili na súčin dvoch Legendrových symbolov $\left(\frac{-1}{q_j}\right)\left(\frac{q_i}{q_j}\right)$ a zvlášť vyčíslili symbol pre -1 a zvyšok výrazu previedli na prípad zákona kvadratickej reciprocity spolu s ďalším činiteľom.

O podobný prístup sa pokúsime aj pri rozšírení teórie na matice kubických zvyškov, ktoré majú hore v kubickom mocninnom symbole povolený ľubovoľný prvočiniteľ. Keďže však zákon kubickej reciprocity máme iba pre primárne prvočinitele, tak opäť budeme potrebovať upraviť symbol $\left(\frac{\pi_i}{\sigma_j}\right)_3$ pomocou vlastnosti multiplikativity na súčin $\left(\frac{\varepsilon}{\sigma_j}\right)_3\left(\frac{\sigma_i}{\sigma_j}\right)_3$, pričom platí, že σ_i je asociovaný primárny prvočiniteľ a získali sme ho ako $\pi_i = \varepsilon\sigma_i$. Rovno odtiaľ však už vidno, že na to, aby sme vo výrazoch vedeli takéto kubické mocninné symboly vyčísľovať, budeme musieť poznať voľbu jednotky, pomocou ktorej získame primárny prvočiniteľ a na samotnú hodnotu symbolu $\left(\frac{\varepsilon}{\sigma_j}\right)_3$ podľa vety 3.12 aj normu prvočiniteľa σ_j modulo 9. Pôjde teda až o blokovú maticu 9×9, ako neskôr vysvetlíme v dôkaze. Na zvýšenie prehľadnosti zavedieme nasledujúce značenie.

Značenie. Ukážeme to na príklade pre $n = 3$. Majme blokovú kubickú znamienkovú maticu 3×3 bloky, pričom bloky na hlavnej diagonále sú štvorcové matice ľubovoľných rozmerov. Všetky bloky pod hlavnou diagonálou odpovedajú prislúchajúcim transponovaným blokom nad hlavnou diagonálou, prenásobeným nejakou kladnou jednotkou zo $\mathbb{Z}[\omega]$. Matica je teda v nasledujúcom tvare, kde $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{1, \omega, \omega^2\}$:

$$\left(\begin{array}{c|c|c} & A & B \\ \hline \varepsilon_1 A^T & & C \\ \hline \varepsilon_2 B^T & \varepsilon_3 C^T & \end{array}\right).$$

Takúto maticu budeme v ďalšom texte pre prehľadnosť zapisovať iba pomocou daných jednotiek.

$$\left(\begin{array}{c|c|c} & & \\ \hline \varepsilon_1 & & \\ \hline \varepsilon_2 & \varepsilon_3 & \end{array}\right).$$

Rovnako budeme zapisovať aj blokové matice $n \times n$ blokov pre ľubovoľné n.

4.3 Blokový tvar matice kubických zvyškov

Na začiatok uvedieme klasickú Čebotarevovu vetu o hustote v znení podľa článku [4, Theorem 3.1] od autora H. Lenstry. Vysvetlenie jednotlivých pojmov a presnejšie detaily nebudeme uvádzať, dajú sa nájsť práve v tomto článku [4].

Veta 4.4 (Čebotarev)**.** *Nech $K \subset L$ je Galoisovo rozšírenie polí, ďalej nech $C \subset G = Gal(L/K)$ je uzavretá na konjugovanie. Potom*

$$\{\mathfrak{p} : \mathfrak{p} \text{ prvoideál v } \mathcal{O}_K,\ \mathfrak{p} \nmid \Delta_{L/K},\ \sigma_\mathfrak{p} \in C\}$$

má hustotu $\#C/\#G$. Pričom $\Delta_{L/K}$ značí diskriminant a $\sigma_\mathfrak{p}$ je Frobeniov automorfizmus prislúchajúci prvku $\mathfrak{p}$.

Hustota $\#C/\#G$ vo vete 4.4 predstavuje limitu pre $x \to \infty$ pomeru počtu prvoideálov s normou menšou ako x, ktoré spĺňajú predpísané podmienky a počtu všetkých prvoideálov v $\mathcal{O}_K$ s normou menšou ako x. Danú vetu teda môžeme chápať aj tak, že hustota $\#C/\#G > 0$ implikuje existenciu nekonečne mnoho prvoideálov, ktoré spĺňajú predpísané vlastnosti. Daná veta nám poskytuje obdobu Dirichletovej vety o prvočíslach v aritmetických postupnostiach z druhej kapitoly.

Veta 4.5. *Nech $\pi_1, \pi_2, \ldots, \pi_n$ sú rôzne neasociované prvočinitele zo $\mathbb{Z}[\omega]$ také, že $N\pi_i \neq 3$ pre všetky $1 \leq i \leq n$. Majme predpísané hodnoty $\left(\frac{\pi_i}{\pi}\right)_3$ pre všetky $1 \leq i \leq n$ a hodnotu $N\pi \mod 9 \in \{1, 4, 7\}$. Potom existuje nekonečne mnoho prvočiniteľov π v $\mathbb{Z}[\omega]$ takých, že spĺňajú tieto predpísané podmienky a navyše platí $\pi \equiv 2 \mod 3$.*

Veta 4.5 plynie z vety 4.4 ak vezmeme za $K = \mathbb{Q}(\sqrt{-3})$, v ktorom pri maticiach kubických zvyškov pracujeme a ktoré sme spomínali na začiatku kapitoly 3. A ako rozšírenie vezmeme $L = K(\zeta_9, \sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \ldots, \sqrt[3]{\pi_n})$. Vďaka rozšíreniu o tretie odmocniny zabezpečíme podmienky pre vyššie spomínané kubické mocninné symboly a pridaním ζ_9 podmienku pre normu. Podrobné odvodenie tejto vety je však rozsahom nad rámec tejto práce, a preto ju uvádzame bez dôkazu.

Veta 4.6 (blokový tvar matice kubických zvyškov)**.** *Nech M je kubická znamienková matica $n \times n$. Potom sú nasledujúce tvrdenia ekvivalentné:*

a) Matica M je matica kubických zvyškov pre prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$, kde pre všetky $1 \leq i \leq n$ platí $N\pi_i \neq 3$. Navyše pre všetky $i \neq j$ platí $\pi_i \nmid \pi_j$.

b) Matica M môže byť konjugovaná vhodne zvolenou permutačnou maticou na blokovú maticu tvaru:

$$N = \left(\begin{array}{c|c|c|c|c|c|c|c|c} S_1 & & & & & & & & \\ \hline 1 & S_2 & & & & & & & \\ \hline 1 & 1 & S_3 & & & & & & \\ \hline 1 & \omega^2 & \omega & S_4 & & & & & \\ \hline 1 & \omega^2 & \omega & \omega & S_5 & & & & \\ \hline 1 & \omega^2 & \omega & \omega^2 & \omega & S_6 & & & \\ \hline 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & S_7 & & \\ \hline 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & S_8 & \\ \hline 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & S_9 \end{array}\right),$$

pričom využívame značenie zavedené na konci sekcie 4.2. Bloky $S_1, S_2, \ldots, S_9$ sú symetrické kubické znamienkové matice.

Dôkaz. *a) $\Rightarrow$ b)* M matica kubických zvyškov pre prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$. Ku každému z nich máme prislúchajúci primárny prvočiniteľ $\sigma_1, \sigma_2, \ldots, \sigma_n$. Pričom $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ značia jednotky v $\mathbb{Z}[\omega]$, pomocou ktorých vznikli asociované primárne prvočinitele. Pre všetky $1 \leq i \leq n$ teda platí $\pi_i = \varepsilon_i\sigma_i$. Pričom prvočiniteľ π_i a asociovaný primárny prvočiniteľ σ_i majú rovnakú normu, keďže $N\pi_i = N(\varepsilon_i\sigma_i) = N\varepsilon_i N\sigma_i = 1 \cdot N\sigma_i = N\sigma_i$.

Prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$ vieme preusporiadať podľa toho, aká jednotka sa vyskytla vo výraze $\pi_i = \varepsilon_i \sigma_i$ a podľa zvyšku $N\pi_i$ modulo 9, ktorý, ako sme už ukázali, môže byť rovný $1, 4$ alebo 7. Prepermutujeme ich tak, aby platilo:

- $\pi_1, \pi_2, \ldots, \pi_a$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{a+1}, \pi_{a+2}, \ldots, \pi_b$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{b+1}, \pi_{b+2}, \ldots, \pi_c$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{c+1}, \pi_{c+2}, \ldots, \pi_d$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{d+1}, \pi_{d+2}, \ldots, \pi_e$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{e+1}, \pi_{e+2}, \ldots, \pi_f$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{f+1}, \pi_{f+2}, \ldots, \pi_g$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 7 \mod 9$
- $\pi_{g+1}, \pi_{g+2}, \ldots, \pi_h$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 7 \mod 9$
- $\pi_{h+1}, \pi_{h+2}, \ldots, \pi_n$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 7 \mod 9$

Ukážeme, že matica $N = (n_{i,j})$, ktorá vznikne konjugovaním permutačnou maticou z matice M a je maticou kubických zvyškov pre naše nové poradie prvočiniteľov je už v požadovanom blokovom tvare. Veľkosti jednotlivých blokov sú obdobne ako v dôkaze 2.6 určené veľkosťami vyššie uvedených skupín prvočiniteľov, teda blok S_1 má rozmer $a \times a$, blok S_2 rozmer $(b-a) \times (b-a)$ a tak ďalej až blok S_9 má rozmer $(n-h) \times (n-h)$.

Pozrieme sa na vzťah v akom sú prvok $n_{i,j}$ a prvok $n_{j,i}$. Z toho už budeme vedieť odvodiť vlastnosti jednotlivých blokov. Využitím multiplikativity kubického mocninného symbolu (veta 3.11), vzťahu $\pi_i = \varepsilon_i \sigma_i$ a zákonu kubickej reciprocity pre primárne prvočinitele (veta 3.15) dostávame:

$$n_{j,i} = \left(\frac{\pi_j}{\sigma_i}\right)_3 = \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\sigma_j}{\sigma_i}\right)_3 = \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\sigma_i}{\sigma_j}\right)_3 = \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\varepsilon_i^{-1}}{\sigma_j}\right)_3 \left(\frac{\pi_i}{\sigma_j}\right)_3 =$$
$$= \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\varepsilon_i^{-1}}{\sigma_j}\right)_3 n_{i,j}.$$

Nebudeme už podrobne prevádzať výpočty pre jednotlivé bloky, ide totiž iba o dosadenie do vzorca:

$$n_{j,i} = \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\varepsilon_i^{-1}}{\sigma_j}\right)_3 n_{i,j}.$$

Pričom jednotlivé jednotky ε_i a ε_j získame podľa toho, v ktorom bloku sa prvky $n_{i,j}, n_{j,i}$ nachádzajú. V tvrdení 3.12 sme opísali hodnoty jednotlivých kubických mocninných symbolov, ktoré majú hore niektorú z jednotiek zo $\mathbb{Z}[\omega]$. Ukázali sme, že táto hodnota závisí iba od toho, do ktorej z troch skupín ± 1 alebo $\pm\omega$ alebo $\pm\omega^2$ jednotka spadá, prípadne aký zvyšok má $N\sigma_i$ a $N\sigma_j$ modulo 9. Všetky tieto informácie sú však v rámci jedného bloku rovnaké vzhľadom na to, ako sme si jednotlivé bloky zadefinovali.

Bloky pod hlavnou diagonálou teda odpovedajú príslušným transponovaným blokom nad hlavnou diagonálou, ktoré sú navyše prenásobené jednotkou určenou vzťahom $\left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\varepsilon_i^{-1}}{\sigma_j}\right)_3$ pre i, j z daných blokov. Podrobným výpočtom by sme sa dopracovali k blokovému tvaru uvedenému v tvrdení b).

$b) \Rightarrow a)$ Máme blokovú maticu N, o ktorej ukážeme, že je maticou kubických zvyškov. Potom nutne aj pôvodná matica M je matica kubických zvyškov. Induktívne skonštruujeme pvočinitele $\pi_1, \pi_2, \ldots, \pi_n$.

V tejto implikácií máme naopak z blokového tvaru predpísané veľkosti jednotlivých blokov matice. Na základe toho budeme pri konštrukcii prvočiniteľov požadovať, aby platila predpísaná hodnota pre ich normu modulo 9 a jednotka, pre ktorú platí $\pi_i = \varepsilon_i \sigma_i$, kde σ_i je primárny prvočiniteľ k π_i, Budeme požadovať:

- $\pi_1, \pi_2, \ldots, \pi_a$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{a+1}, \pi_{a+2}, \ldots, \pi_b$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{b+1}, \pi_{b+2}, \ldots, \pi_c$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 1 \mod 9$
- $\pi_{c+1}, \pi_{c+2}, \ldots, \pi_d$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{d+1}, \pi_{d+2}, \ldots, \pi_e$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{e+1}, \pi_{e+2}, \ldots, \pi_f$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 4 \mod 9$
- $\pi_{f+1}, \pi_{f+2}, \ldots, \pi_g$ jednotka $\varepsilon_i = \pm 1$ a $N\pi_i \equiv 7 \mod 9$
- $\pi_{g+1}, \pi_{g+2}, \ldots, \pi_h$ jednotka $\varepsilon_i = \pm\omega$ a $N\pi_i \equiv 7 \mod 9$
- $\pi_{h+1}, \pi_{h+2}, \ldots, \pi_n$ jednotka $\varepsilon_i = \pm\omega^2$ a $N\pi_i \equiv 7 \mod 9$

Kde veľkosť prvej skupiny je rovná rozmeru štvorcového bloku S_1 a tak ďalej až veľkosť poslednej skupiny prvočiniteľov je rovná rozmeru bloku S_9.

V prvom kroku volíme ľubovoľný prvočiniteľ π_1 tak, aby spĺňal vyššie spomínané podmienky, teda aby spadal do prvej neprázdnej z vyššie popísaných skupín. Na základe vety 4.5 vieme takéhoto prvočiniteľa vždy zvoliť, aj keď podmienky sú teraz kladené len na normu a primárnosť prvočiniteľa. Následne ho môžeme prenásobiť vhodnou jednotkou, čo nebude mať žiaden vplyv na hodnotu normy.

Ďalej z indukčného predpokladu majme $\pi_1, \pi_2, \ldots, \pi_s$ také, že podľa indexu spadajú do správnych skupín a $\sigma_1, \sigma_2, \ldots, \sigma_s$ sú primárne prvočinitele s nimi asociované. Navyše pre všetky $1 \leq i, j \leq s$ platí, že $n_{i,j} = \left(\frac{\pi_i}{\sigma_j}\right)_3$.

Chceme skonštruovať prvočiniteľ π_{s+1}. Podľa veľkosti indexu s máme predpísanú hodnotu $N\pi_{s+1}$ modulo 9, označme ju x, a hodnotu jednotky ε_{s+1} tak, aby platilo $\pi_{s+1} = \varepsilon_{s+1}\sigma_{s+1}$, kde σ_{s+1} je primárny prvočiniteľ. Navyše v matici N máme predpísané hodnoty kubických mocninných symbolov pre všetky $1 \leq i, j \leq s$, teda ako musí vyzerať $\left(\frac{\pi_i}{\sigma_{s+1}}\right)_3 = n_{i,s+1}$ a $\left(\frac{\pi_{s+1}}{\sigma_j}\right)_3 = n_{s+1,j}$.

Podmienky na kubické mocninné symboly nám stačí obmedziť na tie popisujúce $(s+1)$-vý stĺpec matice, teda aby platilo $\left(\frac{\pi_i}{\sigma_{s+1}}\right)_3 = n_{i,s+1}$ pre všetky $1 \leq i \leq s$. Je to z toho dôvodu, že medzi symbolmi $\left(\frac{\pi_i}{\sigma_{s+1}}\right)_3, \left(\frac{\pi_{s+1}}{\sigma_i}\right)_3$ je jasne predpísaný vzťah z dôkazu prvej implikácie, ktorý ale vďaka blokovému tvaru matice vieme, že bude splnený.

Namiesto toho, aby sme hľadali prvočiniteľ π_{s+1}, budeme rovno hľadať primárny prvočiniteľ σ_{s+1} a potom položíme $\pi_{s+1} = \varepsilon_{s+1}\sigma_{s+1}$. Podmienku určujúcu jednotke sme teda vyriešili. Pozrieme sa ako nám to pozmení ostatné podmienky. Platí $N\sigma_{s+1} = N\pi_{s+1}$, takže požiadavka na normu ostáva nezmenená. Rovnako v požiadavkách na kubické mocninné symboly už priamo figuroval iba primárny prvočiniteľ σ_{s+1}.

Máme teda na σ_{s+1} nasledujúce požiadavky:

$$\begin{aligned} N\sigma_{s+1} &\equiv x && \mod 9 \\ \sigma_{s+1} &\equiv 2 && \mod 3 \\ \left(\frac{\pi_1}{\sigma_{s+1}}\right)_3 &= n_{1,s+1} \\ &\vdots \\ \left(\frac{\pi_s}{\sigma_{s+1}}\right)_3 &= n_{s,s+1} \end{aligned}$$

Podľa vety 4.5 ale existuje nekonečne mnoho rôznych prvočiniteľov v $\mathbb{Z}[\omega]$ takých, aby tieto podmienky spĺňali. Položíme σ_{s+1} rovné takému z nich, aby následne pre $\pi_{s+1} = \varepsilon_{s+1}\sigma_{s+1}$ platilo, že $\pi_{s+1} \nmid \pi_i$ pre všetky $1 \leq i \leq s$.

□

Charakterizovali sme blokový tvar matice kubických zvyškov pre ľubovoľnú voľbu prvočiniteľov. Môžeme si všimnúť, že ak by sme prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$ obmedzili len na tie, ktorých norma je kongruentná 1 modulo 9, tak by sme dostali symetrickú maticu ako pri vete 4.2 o primárnych maticiach kubických zvyškov. Ide totiž o podmaticu z predchádzajúcej vety:

$$N = \left(\begin{array}{c|c|c} S_1 & & \\ \hline 1 & S_2 & \\ \hline 1 & 1 & S_3 \end{array}\right).$$

Dôvod je ten, že všetky kubické mocninné symboly sa pre prvočiniteľ π taký, že $N\pi \equiv 1 \mod 9$ rovnajú $\left(\frac{1}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 = \left(\frac{\omega}{\pi}\right)_3 = \left(\frac{-\omega}{\pi}\right)_3 = \left(\frac{\omega^2}{\pi}\right)_3 = \left(\frac{-\omega^2}{\pi}\right)_3 = 1$. Pre všetky vzťahy v predchádzajúcej vete teda platí $n_{j,i} = \left(\frac{\varepsilon_j}{\sigma_i}\right)_3 \left(\frac{\varepsilon_i^{-1}}{\sigma_j}\right)_3 n_{i,j} = n_{i,j}$.

5. Matice kvartických zvyškov

Prípad matíc kvartických zvyškov je veľmi podobný maticiam kubických zvyškov. V tejto kapitole teda iba zhrnieme základné definície, ktoré vedú k pojmu matíc kvartických zvyškov a výsledky z článku [2]. Teória vychádza predovšetkým z knihy [3] a samotného článku [2].

5.1 Okruh Gaussových celých čísel $\mathbb{Z}[i]$

Pre $m = 4$ pri kvartických znamienkových maticiach uvažujeme pole $\mathbb{Q}(i)$. Pracovať budeme v okruhu celistvých prvkov, ktoré predstavujú Gaussove celé čísla $\mathbb{Z}[i]$, kde $i = \sqrt{-1}$. Prvky $\mathbb{Z}[i]$ sú komplexné čísla tvaru $a + bi$, kde $a, b \in \mathbb{Z}$.

Definícia 5.1 (norma)**.** *Nech $\alpha \in \mathbb{Z}[i]$ a platí $\alpha = a + bi$, pre $a, b \in \mathbb{Z}$. Potom* normu *prvku α definujeme vzťahom $N\alpha = \alpha\overline{\alpha} = a^2 + b^2$.*

Tvrdenie 5.2 (jednotky v $\mathbb{Z}[i]$)**.** *Prvok $\alpha \in \mathbb{Z}[i]$ je jednotkou tohto okruhu práve vtedy, keď $N\alpha = 1$. Jednotku sú tým pádom v $\mathbb{Z}[i]$ prvky $\pm 1, \pm i$.*

Tvrdenie 5.3 (klasifikácia prvočiniteľov v $\mathbb{Z}[i]$)**.** *Nech p je prvočíslo v $\mathbb{Z}$. Potom platí:*

- *Ak $p = 2$, potom $1 + i$ je prvočiniteľ v $\mathbb{Z}[i]$ a platí $2 = -i(1 + i)^2$.*
- *Ak $p \equiv 3 \mod 4$, potom p je prvočiniteľ v $\mathbb{Z}[i]$.*
- *Ak $p \equiv 1 \mod 4$, potom $p = \pi\overline{\pi}$, kde π je prvočiniteľ v $\mathbb{Z}[i]$.*

5.2 Kvartický mocninný symbol

Tvrdenie 5.4. *Nech π je prvočiniteľ v $\mathbb{Z}[i]$. Potom $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ je konečné pole s $N\pi$ prvkami.*

Z toho obdobne vyplýva, že multiplikatívna grupa $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ má rád $N\pi - 1$. Vďaka čomu máme v $\mathbb{Z}[i]$ opäť analógiu Malej Fermatovej vety.

Tvrdenie 5.5. *Nech $\alpha \in \mathbb{Z}[i]$ a π je prvočiniteľ v $\mathbb{Z}[i]$ taký, že $\pi \nmid \alpha$. Potom platí:*

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

Tvrdenie 5.6. *Nech $\alpha \in \mathbb{Z}[i]$ a π je prvočiniteľ v $\mathbb{Z}[i]$ taký, že $N\pi \neq 2$ a zároveň $\pi \nmid \alpha$. Potom existuje jednoznačne určené $m = 0, 1, 2$ alebo 3 také, že platí:*

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

Posledné tvrdenie nám dáva možnosť exaktne zadefinovať kvartický mocninný symbol.

Definícia 5.7 (kvartický mocninný symbol)**.** *Nech $\alpha \in \mathbb{Z}[i]$ a π je prvočiniteľ v $\mathbb{Z}[i]$ taký, že $N\pi \neq 2$. Potom definujeme* kvartický mocninný symbol *nasledovne:*

$$\left(\frac{\alpha}{\pi}\right)_4 \begin{cases} = 0 & \text{ak } \pi \mid \alpha, \\ \equiv \alpha^{\frac{N\pi-1}{4}} \mod \pi & \text{kde } \left(\frac{\alpha}{\pi}\right)_4 \text{ nadobúda hodnoty } \pm 1 \text{ alebo } \pm i \text{ ak } \pi \nmid \alpha. \end{cases}$$

5.3 Primárny prvočiniteľ a kvartická reciprocita

Definícia 5.8 (primárny prvočiniteľ). *Nech π je prvočiniteľ v $\mathbb{Z}[i]$. Potom povieme, že π je* primárny prvočiniteľ *ak platí $\pi \equiv 1 \mod 2(1+i)$.*

Poznámka. Prvok $\pi = a + bi$ je primárny ak $a \equiv 1 \mod 4$ a $b \equiv 0 \mod 4$ alebo $a \equiv 3 \mod 4$ a $b \equiv 2 \mod 4$.

V $\mathbb{Z}[i]$ máme 4 jednotky, teda každý nenulový prvok v $\mathbb{Z}[i]$ je asociovaný so 4 prvkami.

Veta 5.9 (jednoznačnosť primárneho prvočiniteľa). *Nech π je prvočiniteľ v $\mathbb{Z}[i]$, $N\pi \neq 2$. Potom medzi prvkami asociovanými s π existuje práve jeden primárny prvočiniteľ.*

Pre kvartické mocninné symboly máme v $\mathbb{Z}[i]$ opäť ekvivalent kvadratickej reciprocity, ktorá platila v $\mathbb{Z}$ pre Legendrove symboly a ktorá umožňuje skúmať blokový tvar matíc kvartických zvyškov.

Veta 5.10 (zákon kvartickej reciprocity). *Nech π_1, π_2 sú primárne prvočinitele v $\mathbb{Z}[i]$, $N\pi_1 \neq 2$, $N\pi_2 \neq 2$. Potom platí vzťah:*

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

5.4 Matice kvartických zvyškov

Definíciu matíc kvartických zvyškov uvádzame ako v článku [2].

Definícia 5.11 (matica kvartických zvyškov). *Nech $\pi_1, \pi_2, \ldots, \pi_n$ sú prvočinitele v $\mathbb{Z}[i]$, pre všetky $1 \leq j \leq n$ platí $N\pi_j \neq 2$. Navyše pre všetky $j \neq k$ platí $\pi_j \nmid \pi_k$. Označme $\sigma_1, \sigma_2, \ldots, \sigma_n$ postupne primárne prvočinitele k $\pi_1, \pi_2, \ldots, \pi_n$. Potom* matica kubických zvyškov *je matica $n \times n$, ktorá má na pozícii (j,k) kvartický mocninný symbol $\left(\frac{\sigma_j}{\sigma_k}\right)_4$.*

Na záver sformulujeme charakterizačnú vetu pre matice kvartických zvyškov z článku [2, Theorem 3].

Veta 5.12. *Nech M je kvartická znamienková matica $n \times n$. Potom nasledujúce tvrdenia sú ekvivalentné:*

a) Existuje $s \in \mathbb{N}$, $1 \leq s \leq n$ také, že matica M môže byť konjugovaná permutačnou maticou na blokovú maticu tvaru:

$$\left(\begin{array}{c|c} A & B \\ \hline B^T & S \end{array}\right),$$

kde blok A je $s \times s$ antisymetrická kvartická znamienková matica, blok S je $(n-s) \times (n-s)$ symetrická kvartická znamienková matica a B je $s \times (n-s)$ matica, ktorej všetky prvky sú ± 1 alebo $\pm i$.

b) Matica M je matica kvartických zvyškov pre prvočinitele $\pi_1, \pi_2, \ldots, \pi_n$, kde pre všetky $1 \leq i \leq n$ platí $N\pi_i \neq 2$. Navyše pre všetky $i \neq j$ platí $\pi_i \nmid \pi_j$.

c) Ak $M = (m_{j,k})$, potom $m_{j,k} = \pm m_{k,j}$ pre všetky $1 \leq j, k \leq n$ a existuje $s \in \mathbb{N}$, $1 \leq s \leq n$ také, že na hlavnej diagonále $M\overline{M}$ je s prvkov tvaru $n + 1 - 2s$ a $n - s$ prvkov tvaru $n - 1$.

Záver

V práci sme vychádzali z článku [2], ktorého autormi sú Dummit, Dummit, Kisilevsky. Článok sa zaoberal charakterizáciou špecifických tried cyklotomických znamienkových matíc, konkrétne matíc kvadratických, kubických a kvartických zvyškov. Hlavným obsahom sa stala predovšetkým charakterizácia v podobe popisu blokového tvaru týchto matíc. V nasledujúcej tabuľke na zhrnutie uvádzame výsledky autorov článku, ktoré sme v plnom znení uviedli vo vetách 2.3, 4.2 a 5.12.

	Trieda matíc	Okruh	Blokový tvar matice
$m = 2$	Matice kvadratických zvyškov	$\mathbb{Z}$	$\left(\begin{array}{c\|c} A & B \\ \hline B^T & S \end{array}\right)$
$m = 3$	Matice kubických zvyškov	$\mathbb{Z}[\omega]$	symetrická matica
$m = 4$	Matice kvartických zvyškov	$\mathbb{Z}[i]$	$\left(\begin{array}{c\|c} A & B \\ \hline B^T & S \end{array}\right)$

Cieľom tejto práce bolo rozšíriť charakterizáciu na väčšiu triedu týchto matíc, ktorá vznikla povolením aj neprimárnych prvočiniteľov v ich definíciách. Toto rozšírenie viedlo k zložitejšiemu problému a blokovým maticiam s väčšími počtami blokov. Konkrétne vlastné výsledky zhrnieme v nasledujúcej tabuľke. Jedná sa o vety 2.6 a 4.6. V prípade $m = 3$ využijeme pre maticu značenie zo sekcie 4.2.

	Trieda matíc	Okruh	Blokový tvar matice
$m = 2$	Matice kvadratických zvyškov	$\mathbb{Z}$	$\left(\begin{array}{c\|c\|c\|c} A_1 & B & C & D \\ \hline B^T & S_1 & E & F \\ \hline -C^T & E^T & S_2 & G \\ \hline D^T & F^T & -G^T & A_2 \end{array}\right)$
$m = 3$	Matice kubických zvyškov	$\mathbb{Z}[\omega]$	$\left(\begin{array}{c\|c\|c\|c\|c\|c\|c\|c\|c} S_1 & & & & & & & & \\ \hline 1 & S_2 & & & & & & & \\ \hline 1 & 1 & S_3 & & & & & & \\ \hline 1 & \omega^2 & \omega & S_4 & & & & & \\ \hline 1 & \omega^2 & \omega & \omega & S_5 & & & & \\ \hline 1 & \omega^2 & \omega & \omega^2 & \omega & S_6 & & & \\ \hline 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & S_7 & & \\ \hline 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & S_8 & \\ \hline 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & S_9 \end{array}\right)$

Podobné rozšírenie blokovej charakterizácie by bolo možné aj pre prípad matíc kvartických zvyškov, ktorému sme sa už v práci nevenovali. Z odvodenej teórie je však možné pozorovať, že by principiálne išlo o podobný problém ako pri maticiach kubických zvyškov.

Okrem blokového tvaru sa autori článku pri maticiach kvadratických zvyškov venujú aj ďalšej charakterizácií týchto matíc. Ide o ekvivalentné tvrdenie popisujúce matice kvadratických zvyškov pomocou tvaru prvkov na hlavnej diagonále ich druhej mocniny, ktoré bolo súčasťou vety 2.3.

V tejto práci sa nám podarilo dokázať, že aj rozšírené matice kvadratických zvyškov už podobný popis spĺňajú, čo sme zhrnuli vo vete 2.7. Rozšírenie charakterizácie o opačnú implikáciu, kedy by popis prvkov na hlavnej diagonále druhej mocniny matice slúžil už ako postačujúca podmienka, však ostáva naďalej otvorený.

Zoznam použitej literatúry

[1] A. Drápal. Teorie čísel a RSA [online]. `http://www.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf`.

[2] D. S. Dummit, E. P. Dummit, and H. Kisilevsky. Characterizations of quadratic, cubic, and quartic residue matrices. *J. Number Theory*, 168:167–179, 2016.

[3] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[4] H. Lenstra. The Chebotarev Density Theorem [online]. `http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf`.

[5] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory*, volume 190 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2005.

[6] J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.