โครงการ

การเรียนการสอนเพื่อเสริมประสบการณ์

ชื่อโครงการ	**ฟังก์ชันตัวหารมอดูลาร์และสัญลักษณ์ส่วนตกค้างกำลังสามและกำลังสี่**
	Modular divisor function and cubic and quartic residue symbols
ชื่อนิสิต	**นายอภินันท์ โพธิ์แก้ว 5933556323**
ภาควิชา	**คณิตศาสตร์และวิทยาการคอมพิวเตอร์**
	สาขาวิชา คณิตศาสตร์
ปีการศึกษา	**2562**

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ฟังก์ชันตัวหารมอดูลาร์และสัญลักษณ์ส่วนตกค้างกำลังสามและกำลังสี่

นายอภินันท์ โพธิ์แก้ว

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

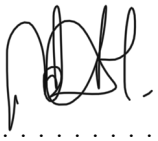
Modular Divisor Functions and Cubic and Quartic Residue Symbols

Mr. Apinan Pokaew

A Project Submitted in Partial Fulfillment of the Requirements
for the Degree of Bachelor of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2019
Copyright of Chulalongkorn University

หัวข้อโครงงาน	ฟังก์ชันตัวหารมอดูลาร์และสัญลักษณ์ส่วนตกค้างกำลังสามและกำลังสี่
โดย	นายอภินันท์ โพธิ์แก้ว รหัสประจำตัว 5933556323
สาขาวิชา	คณิตศาสตร์
อาจารย์ที่ปรึกษาโครงงานหลัก	ศาสตราจารย์ ดร.ยศนันต์ มีมาก

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับโครงงานฉบับนี้เป็นส่วนหนึ่ง ของการศึกษาตามหลักสูตรปริญญาบัณฑิต ในรายวิชา 2301499 โครงงานวิทยาศาสตร์ (Senior Project)



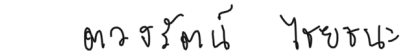
. . . . . หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

(ศาสตราจารย์ ดร.กฤษณะ เนียมมณี)

คณะกรรมการสอบโครงงาน

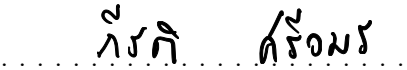
. . . . . อาจารย์ที่ปรึกษาโครงงานหลัก

(ศาสตราจารย์ ดร.ยศนันต์ มีมาก)



. . . . . กรรมการ

(รองศาสตราจารย์ ดร.ตวงรัตน์ ไชยชนะ)



. . . . . กรรมการ

(อาจารย์ ดร.กิรติ ศรีอมร)

อภินันท โพธิ์แก้ว: ฟังก์ชันตัวหารมอดูลาร์และสัญลักษณ์ส่วนตกค้างกำลังสามและกำลังสี่. (MODULAR DIVISOR FUNCTION AND CUBIC AND QUARTIC RESIDUE SYMBOLS)
อ.ที่ปรึกษาโครงงานหลัก: ศ.ดร.ยศนันต์ มีมาก, 32 หน้า.

ในโครงงานนี้ เรานิยามฟังก์ชันตัวหารมอดูลาร์ $\tau(-,\pi)$ เมื่อ π เป็นจำนวนเฉพาะบนริง $\mathbb{Z}[\omega]$ และฟังก์ชันตัวหารมอดูลาร์ $\eta(-,\pi)$ เมื่อ π เป็นจำนวนเฉพาะบนริง $\mathbb{Z}[i]$ พร้อมทั้งศึกษาความสัมพันธ์ระหว่างฟังก์ชันตัวหารมอดูลาร์ดังกล่าวกับการมีผลเฉลยของสมการสมภาค $x^3 \equiv \alpha \mod \pi$ และ $x^4 \equiv \alpha \mod \pi$ ยิ่งกว่านั้นยังศึกษาสมบัติทางเลขคณิตของฟังก์ชันเหล่านี้โดยใช้สัญลักษณ์ส่วนตกค้างกำลังสามและกำลังสี่

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต . . . . . .
สาขาวิชา . คณิตศาสตร์ . ลายมือชื่อ อ.ที่ปรึกษาโครงงานหลัก . . . . . .
ปีการศึกษา . . . . 2562 . . . .

5933556323: MAJOR MATHEMATICS.
KEYWORDS: MODULAR DIVISOR FUNCTION, CUBIC RESIDUE SYMBOLS, QUARTIC RESIDUE SYMBOLS.
APINAN POKAEW: MODULAR DIVISOR FUNCTION AND CUBIC AND QUARTIC RESIDUE SYMBOLS.
ADVISOR: PROF. YOTSANAN MEEMARK, PH.D., 32 PP.

In this project, we define the modular divisor function $\tau(-,\pi)$ where π is a prime in $\mathbb{Z}[\omega]$ and the modular divisor function $\eta(-,\pi)$ where π is a prime in $\mathbb{Z}[i]$. We study the relations between these functions and the existence of solutions of the congruence $x^3 \equiv \alpha \mod \pi$ and $x^4 \equiv \alpha \mod \pi$. Moreover, we determine many arithmetic properties of them using the cubic and quartic residue symbols.

Department . Mathematics and Computer Science . Student's Signature . . . . . .
Field of Study . . Mathematics . . Advisor's Signature . Yotsanan Meemark . . .
Academic Year . . . . . 2019 . . . . .

Acknowledgements

This project could not have been achieved without help from the following important persons.

Firstly, I would like to express my gratitude to Professor Yotsanan Meemark, Ph.D. who is my project advisor for his help and advices. I receive valuable knowledge and experiences throughout working in this project. It is my pleasure to have an opportunity to work with him.

Secondly, I would like to express my thanks to my committee Associate Professor Tuangrat Chaichana, Ph.D. and Kirati Sriamorn, Ph.D. for giving the comments and suggestions.

Finally, I would like to thanks my family and my friends for their support and encouragement.

Apinan Pokaew

contents

Chapter 1
Preliminaries

In this chapter, we collect some elemmentary results in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$. Most of them are taken from Chapter 9 of [3]. The new ones come with a small proof.

1.1 Some Background in $\mathbb{Z}[\omega]$

Let $\omega = (-1+\sqrt{-3})/2$ and $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$. Note that $\omega^2+\omega+1=0$.

Definition 1.1 For $a, b \in \mathbb{Z}$, the **norm** of $a+b\omega$ is $(a+b\omega)(a+b\overline{\omega}) = a^2+b^2-ab \in \mathbb{N}\cup\{0\}$ and is denoted by $N(a+b\omega)$. It follows that $\mathbb{Z}[\omega]$ is a Euclidean domain and the norm map is a valuation map.

Proposition 1.2 $\alpha \in \mathbb{Z}[\omega]$ is a unit if and only if $N\alpha = 1$. The units in $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

Proposition 1.3 If π is a prime in $\mathbb{Z}[\omega]$, then there is a rational prime p such that $N\pi = p$ or p^2. In former case π is not associate to a rational prime, in latter case π is associate to p.

Proposition 1.4 If $\pi \in \mathbb{Z}[\omega]$ is such that $N\pi = p$, a rational prime, then π is a prime in $\mathbb{Z}[\omega]$.

Proposition 1.5 Suppose that p and q are rational primes. If $q \equiv 2 \mod 3$, then q is a prime in $\mathbb{Z}[\omega]$. If $p \equiv 1 \mod 3$, then $p = \pi\overline{\pi}$ where π is prime in $\mathbb{Z}[\omega]$. Finally, $1-\omega$ is a prime in $\mathbb{Z}[\omega]$.

Note that if π is a prime in $\mathbb{Z}[\omega]$ with $N\pi \neq 3$, then $N\pi \equiv 1 \mod 3$.

Proposition 1.6 Let $\pi \in \mathbb{Z}[\omega]$ be a prime. Then $\mathbb{Z}[\omega]/(\pi)$ is a finite field with $N\pi$ elements.

a. If $\pi = q$ is a rational prime congruent $2 \bmod 3$, then $\{a + b\omega : 0 \leq a < q$ and $0 \leq b < q\}$ is a complete set of coset representatives of $\mathbb{Z}[\omega]/(q)$.
b. If $p \equiv 1 \bmod 3$ is a rational prime and $N\pi = p$, then $\{0, 1, \ldots, p-1\}$ is a complete set of coset representatives of $\mathbb{Z}[\omega]/(\pi)$.

Lemma 1.7 Let $\pi \in \mathbb{Z}[\omega]$ be a prime with $N\pi \neq 3$. If $\alpha \in (\mathbb{Z}[\omega]/(\pi))^{\times}$, then $\alpha,\ \alpha\omega$ and $\alpha\omega^2$ are distinct elements in $(\mathbb{Z}[\omega]/(\pi))^{\times}$.

Proof. We will claim that $\omega \not\equiv \pm 1 \bmod \pi$. Since $1 + \omega = -\omega^2$ is a unit, $\pi \nmid (1 + \omega)$. Since $N(1 - \omega) = 1 + 1 + 1 = 3$ and $N\pi \neq 3$, $N\pi \nmid N(1 - \omega)$, so $\pi \nmid (1 - \omega)$. Hence, we have the claim and the desired results easily follow from the claim. □

Definition 1.8 Let π be a prime in $\mathbb{Z}[\omega]$. For $\alpha = a + b\omega$ where $a, b \in \mathbb{Z}$ not both zero, we say that

α is in Q_1 if $a > 0$ and $b \geq 0$

α is in Q_2 if $a \leq 0 \leq b$ or $a < b \leq 0$

α is in Q_3 if $b \leq a \leq 0$ or $b < 0 \leq a$.

Lemma 1.9 Let π be a prime with $N\pi \neq 3$ and $\alpha \in (\mathbb{Z}[\omega]/(\pi))^{\times}$. If α is in Q_1, then $\alpha\omega$ and $\alpha\omega^2$ are in Q_2 and Q_3, respectively. Similarly, if α is in Q_2, then $\alpha\omega$ and $\alpha\omega^2$ are in Q_3 and Q_1, respectively and if α is in Q_3, then $\alpha\omega$ and $\alpha\omega^2$ are in Q_1 and Q_2, respectively.

Proof. Let π be a prime with $N\pi \neq 3$ and $\alpha \in (\mathbb{Z}[\omega]/(\pi))^{\times}$. WLOG, assume that α is in Q_1. Then $\alpha = a + b\omega$ where $a, b \in \mathbb{Z}$, $a > 0$ and $b \geq 0$. Thus $\alpha\omega = (a + b\omega)\omega = -b + (a - b)\omega$ and $\alpha\omega^2 = (a + b\omega)\omega^2 = (-a + b) + (-a)\omega$. If $a \geq b$, then $-a + b \leq 0 \leq a - b$. Hence $\alpha\omega = -b + (a - b)\omega$ and $-b \leq 0 \leq a - b$, so $\alpha\omega$ is in Q_2. Since $\alpha\omega^2 = (-a + b) + (-a)\omega$ and $-a \leq -a + b \leq 0$, $\alpha\omega^2$ is in Q_3. If $a < b$, then $a - b < 0 < -a + b$. Hence $\alpha\omega = -b + (a - b)\omega$ and $-b < a - b \leq 0$, so $\alpha\omega$ is in Q_2. Since $\alpha\omega^2 = (-a + b) + (-a)\omega$ and $-a < 0 \leq -a + b$, $\alpha\omega^2$ is in Q_3. □

Proposition 1.10 If π is a prime in $\mathbb{Z}[\omega]$ with $N\pi \neq 3$, then the complete set of coset representatives of $(\mathbb{Z}[\omega]/(\pi))^{\times}$ is divided equally into $(N\pi - 1)/3$ elements in Q_1, Q_2 and Q_3.

Proof. It follows from Lemmas 1.7 and 1.9. □

1.2 Cubic Residue Symbol

Throughout this section, we let π be a prime in $\mathbb{Z}[\omega]$ with $N\pi \neq 3$. Then the multiplicative group of $(\mathbb{Z}[\omega]/(\pi))^\times$ has order $N\pi - 1$ with $(N\pi - 1)/3$ elements in Q_1.

Proposition 1.11 If $\alpha \in \mathbb{Z}[\omega]$ and $\pi \nmid \alpha$, then $\alpha^{N\pi-1} \equiv 1 \mod \pi$.

Proposition 1.12 If $\alpha \in \mathbb{Z}[\omega]$ and $\pi \nmid \alpha$, then there exists a unique integer $m = 0, 1$ or 2 such that $\alpha^{(N\pi-1)/3} \equiv \omega^m \mod \pi$.

Definition 1.13 Let $\alpha \in \mathbb{Z}[\omega]$. The **cubic residue symbol of** α **modulo** π is given by

a. $(\alpha/\pi)_3 = 0$ if $\pi \mid \alpha$.

b. $(\alpha/\pi)_3 \equiv \alpha^{(N\pi-1)/3} \mod \pi$ if $\pi \nmid \alpha$.

Note that $(\alpha/\pi)_3$ equals to ω, ω^2 or 1.

Proposition 1.14 Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be such that $\pi \nmid \alpha\beta$. Then

a. $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \mod \pi$ is solvable.

b. $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.

c. If $\beta \equiv \alpha \mod \pi$, then $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Proposition 1.15 Let $\alpha \in \mathbb{Z}[\omega]$ be such that $\pi \nmid \alpha$. Then

a. $\overline{(\alpha/\pi)_3} = (\alpha/\pi)_3{}^2 = (\alpha^2/\pi)_3$.

b. $\overline{(\alpha/\pi)_3} = (\overline{\alpha}/\overline{\pi})_3$.

Corollary 1.16 If $\pi = q$ is a rational prime congruent to 2 modulo 3, then $(\overline{\alpha}/q)_3 = (\alpha^2/q)_3$ and $(n/q)_3 = 1$ if n is a rational integer relatively prime to q.

Definition 1.17 If π is prime in $\mathbb{Z}[\omega]$, we say that π is **primary** if $\pi \equiv 2 \mod 3$, i.e., either $\pi = q \equiv 2 \mod 3$ is a rational prime or $\pi = a + b\omega$ with $a \equiv 2 \mod 3$ and $b \equiv 0 \mod 3$, $N\pi = p \equiv 1 \mod 3$.

Proposition 1.18 Suppose that $N\pi = p \equiv 1 \mod 3$. Among the six associates of π exactly one is primary.

Theorem 1.19 (The Law of Cubic Reciprocity). Let α and π be primary primes in $\mathbb{Z}[\omega]$ with $N\alpha, N\pi \neq 3$ and $N\alpha \neq N\pi$. Then

$$(\alpha/\pi)_3 = (\pi/\alpha)_3.$$

Theorem 1.20 (Supplement to the Law of Cubic Reciprocity). Suppose that $N\pi \neq 3$. If π is a primary and write $\pi = a + b\omega$ where $a = 3m - 1$ and $b = 3n$, then

$$(1-\omega/\pi)_3 = \omega^{2m}.$$

1.3 Some Background in $\mathbb{Z}[i]$

Let $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}$.

Definition 1.21 For $a, b \in \mathbb{Z}$, the **norm** of $a + bi$ is $(a + bi)(a + b\bar{i}) = a^2 + b^2$ and is also denoted by $N(a + bi)$. It follows that $\mathbb{Z}[i]$ is a Euclidean domain and the norm map is a valuation map.

Proposition 1.22 $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N\alpha = 1$. The units in $\mathbb{Z}[\omega]$ are $1, -1, i, -i$.

Proposition 1.23 If π is a prime in $\mathbb{Z}[i]$, then there is a rational prime p such that $\pi \mid p$.

Proposition 1.24 If $\alpha \in \mathbb{Z}[i]$ is such that $N\alpha$ is prime, then α is a prime in $\mathbb{Z}[i]$.

Proposition 1.25 $1 + i$ is a prime and $2 = -i(1 + i)^2$ is a prime factorization of 2 in $\mathbb{Z}[i]$.

Proposition 1.26 If $q \equiv 3 \mod 4$ is a prime in $\mathbb{Z}$, then q is a prime considered as an element of $\mathbb{Z}[i]$.

Proposition 1.27 If p is a prime in $\mathbb{Z}$ and $p \equiv 1 \mod 4$, then there is a prime π such that $p = \pi\overline{\pi}$.

Proposition 1.28 Let $\pi \in \mathbb{Z}[i]$ be a prime. Then $\mathbb{Z}[i]/(\pi)$ is a finite field with $N\pi$ elements.

a. If $\pi = q$ is a rational prime congruent $3 \mod 4$, then $\{a + bi : 0 \leq a < q$ and $0 \leq b < q\}$ is a complete set of coset representatives.

b. If $p \equiv 1 \mod 4$ is a rational prime and $N\pi = p$, then $\{0, 1, \ldots, p - 1\}$ is a complete set of coset representatives.

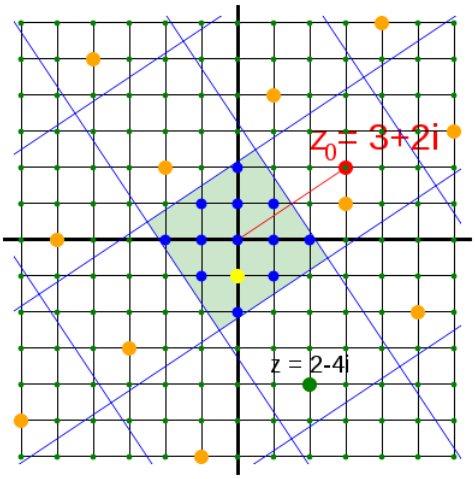
Proposition 1.29 If π is a prime in $\mathbb{Z}[i], N\pi \neq 2$, then the complex plane, whose squares are delimited by the two lines

$$\mathbb{V}_s = \{\pi(s - \tfrac{1}{2} + ix) : x \in \mathbb{R}\} \text{ and } \mathbb{H}_t = \{\pi(x + i(t - \tfrac{1}{2})) : x \in \mathbb{R})\}$$

with s and t integers. They divide the plane in semi-open squares

$$Q_{mn} = \{(s + it)\pi : s \in [m - \tfrac{1}{2}, m + \tfrac{1}{2}), t \in [n - \tfrac{1}{2}, n + \tfrac{1}{2})\}$$

where $m, n \in \mathbb{Z}$. Q_{00} is called **minimal residues class modulo** π and its elements is divided equally into $(N\pi - 1)/4$ elements in the 1st, 2nd, 3rd and 4th quadrants.



Figures 1.1: All 13 residue classes with their minimal residues in the square Q_{00} for the modulus $z_0 = 3 + 2i$ and $z = 2 - 4i \equiv -i \mod 3 + 2i$ is highlighted with yellow dots.

1.4 Quartic Residue Symbol

Throughout this section, we let π be an irreducible element in $\mathbb{Z}[i]$ with $N\pi \neq 2$. Then the multiplicative group of $(\mathbb{Z}[i]/(\pi))^\times$ has order $N\pi - 1$ with $(N\pi - 1)/4$ elements in 1st quadrant.

Proposition 1.30 If $\alpha \in \mathbb{Z}[i]$ and $\pi \nmid \alpha$, then $\alpha^{\mathbb{N}\pi - 1} \equiv 1 \mod \pi$.

Proposition 1.31 If $\alpha \in \mathbb{Z}[i]$ and $\pi \nmid \alpha$, then there exists a unique integer $j = 0, 1, 2$ or 3 such that $\alpha^{(\mathbb{N}\pi-1)/4} \equiv i^j \mod \pi$.

Definition 1.32 Let $\alpha \in \mathbb{Z}[i]$. The **quartic residue symbol of** α **modulo** π is given by

a. $(\alpha/\pi)_4 = 0$ if $\pi \mid \alpha$.

b. $(\alpha/\pi)_4 \equiv \alpha^{(N\pi-1)/4} \mod \pi$ if $\pi \nmid \alpha$.

Note that $(\alpha/\pi)_4$ equals to $i, -1, -i$ or 1.

Proposition 1.33 Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha\beta$.

a. $(\alpha/\pi)_4 = 1$ if and only if $x^4 \equiv \alpha \mod \pi$ is solvable.

b. $(\alpha\beta/\pi)_4 = (\alpha/\pi)_4(\beta/\pi)_4$.

c. If $\beta \equiv \alpha \bmod \pi$, then $(\alpha/\pi)_4 = (\beta/\pi)_4$.

d. $\overline{(\alpha/\pi)_4} = (\overline{\alpha}/\overline{\pi})_4$.

e. If $(\lambda) = (\pi)$, then $(\alpha/\lambda)_4 = (\alpha/\pi)_4$.

Corollary 1.34 Let $\alpha \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha$. Then $(\alpha/\pi)_4 = 1$ or -1 if and only if $x^2 \equiv \alpha \bmod \pi$ is solvable.

Proof. ($\rightarrow$) If $x^2 \equiv \alpha \bmod \pi$ is solvable, then $x^4 \equiv \alpha^2 \bmod \pi$ is also solvable, so $1 = (\alpha^2/\pi)_4 = (\alpha/\pi)_4{}^2$, i.e., $(\alpha/\pi)_4 = 1$ or -1.
($\leftarrow$) If $(\alpha/\pi)_4 = 1$, then $x^4 \equiv \alpha^2 \bmod \pi$ is solvable by Proposition 1.33 (a), so $x^2 \equiv \alpha \bmod \pi$ is also solvable. If $(\alpha/\pi)_4 = -1$, then $(\alpha^2/\pi)_4 = (\alpha/\pi)_4{}^2 = 1$. Thus, $x^4 \equiv \alpha^2 \bmod \pi$ is solvable by Proposition 1.33 (a). Assume that x_0 is a solution of $x^4 \equiv \alpha^2 \bmod \pi$ and ${x_0}^2 \not\equiv \alpha \bmod \pi$. Then ${x_0}^2 \equiv -\alpha \bmod \pi$ implies that $(x_0 i)^2 \equiv \alpha \bmod \pi$. Hence, $x_0 i$ is a solution of $x^2 \equiv \alpha \bmod \pi$. □

Proposition 1.35 Let q be a prime in $\mathbb{Z}$ such that $q \equiv 3 \bmod 4$. Then $(a/q)_4 = 1$ for all $a \in \mathbb{Z}$ with $q \nmid a$.

Definition 1.36 We say that π is **primary** if $\pi \equiv 1 \bmod (1+i)^3$.

Proposition 1.37 If π is irreducible in $\mathbb{Z}[i]$, then $\pi = a + bi$ is primary irreducible if and only if either ($a \equiv 1 \bmod 4$ and $b \equiv 0 \bmod 4$) or ($a \equiv 3 \bmod 4$ and $b \equiv 2 \bmod 4$).

Lemma 1.38 Let $\alpha \in \mathbb{Z}[i]$ be a nonunit element such that $(1+i) \nmid \alpha$. Then there is a unique unit u such that $u\alpha$ is primary.

Lemma 1.39 A primary element can be written as the product of primary primes.

Proposition 1.40 If π is a primary prime, then $(-1/\pi)_4 = (-1)^{(a-1)/2}$ where a is the real part of π.

Definition 1.41 Let $\alpha \in \mathbb{Z}[i]$ be a nonunit element such that $(1+i) \nmid \alpha$, and $\beta \in \mathbb{Z}[i]$. Write $\alpha = \Pi_i \lambda_i$ where λ_i is a prime in $\mathbb{Z}[i]$. If $\gcd(\alpha, \beta) = 1$, we define $(\beta/\alpha)_4$ by

$$(\beta/\alpha)_4 = \Pi_i (\beta/\lambda_i)_4.$$

Proposition 1.42 Let $\alpha \in \mathbb{Z}, \alpha \neq 0$, and $a \in \mathbb{Z}$ be an odd nonunit. If $\gcd(\alpha, a) = 1$, then $(\alpha/a)_4 = 1$.

Proposition 1.43 If $n \neq 1$ is an integer and $n \equiv 1 \mod 4$, then $(i/n)_4 = (-1)^{(n-1)/4}$.

Theorem 1.44 (The Law of Quartic Reciprocity). Let α and π be primary primes in $\mathbb{Z}[i]$ with $N\alpha, N\pi \neq 2$ and $N\alpha \neq N\pi$. Then

$$(\alpha/\pi)_4 = (\pi/\alpha)_4(-1)^{((N\alpha-1)/4)((N\pi-1)/4)}.$$

1.5 Our Objectives

Steiner [2] studied the modular divisor function $\tau(-, p)$ defined by for an odd prime p and an integer a with $p \nmid a$, $\tau(a, p)$ is the number of ordered pairs of integers (x, y) such that

$$0 < x < \tfrac{1}{2}p, 0 < y < \tfrac{1}{2}p, xy \equiv a \mod p$$

He showed that if p is an odd prime and $p \nmid a$, then a is a quadratic residue modulo p if and only if $\tau(a, p)$ is odd. In addition, he used this result to give another proof of the quadratic reciprocity law.

In this project, we define the modular divisor function $\tau(-, \pi)$ where π is a prime in $\mathbb{Z}[\omega]$ and the modular divisor function $\eta(-, \pi)$ where π is a prime in $\mathbb{Z}[i]$. We study the relation between $\tau(\alpha, \pi)$ and the existence of solutions of $x^3 \equiv \alpha \mod \pi$ and the relation between $\eta(\alpha, \pi)$ and the existence of solutions of $x^4 \equiv \alpha \mod \pi$. In addition, we determine many arithmetic properties of them using the cubic and quartic residue symbols. They are presented for $\mathbb{Z}[\omega]$ in Section 2.1 and for $\mathbb{Z}[i]$ in Section 2.2, respectively.

Chapter 2
Results

2.1 Modular Divisor Function $\tau(-,\pi)$ on $\mathbb{Z}[\omega]$

In this section, let π be a prime in $\mathbb{Z}[\omega]$ with $N\pi \neq 3$. We begin by defining the modular divisor function $\tau(-,\pi)$ on $\mathbb{Z}[\omega]$ and study their properties.

Definition 2.1 The **modular divisor function** $\tau(-,\pi)$ on $\mathbb{Z}[\omega]$ is defined by

$$\tau(\alpha,\pi) = \#\{(x,y,z) : x,y,z \in (\mathbb{Z}[\omega]/(\pi))^\times \text{ in } Q_1 \text{ and } xyz \equiv \alpha \mod \pi\}$$

for all $\alpha \in \mathbb{Z}[\omega]$ and $\pi \nmid \alpha$.

Next, we relate $\tau(-,\pi)$ to the cubic residue symbol.

Proposition 2.2 Let $\alpha \in \mathbb{Z}[\omega]$ be such that $\pi \nmid \alpha$. Then

a. $(\alpha/\pi)_3 = 1$ if and only if $\tau(\alpha,\pi) \equiv 1 \mod 3$,

b. $(\alpha/\pi)_3 \neq 1$ if and only if $\tau(\alpha,\pi) \equiv 0 \mod 3$, and

c. $\tau(\alpha,\pi) \not\equiv 2 \mod 3$.

In other words,

a. $x^3 \equiv \alpha \mod \pi$ is solvable if and only if $\tau(\alpha,\pi) \equiv 1 \mod 3$, and

b. $x^3 \equiv \alpha \mod \pi$ is not solvable if and only if $\tau(\alpha,\pi) \equiv 0 \mod 3$.

Proof. If (x,y,z) is a triple counting towards $\tau(\alpha,\pi)$, then permutations of x,y,z in it is also a triple counting towards $\tau(\alpha,\pi)$. It follows that up to a cyclic permutation, there are $6k$ triple for some $k \in \mathbb{N}\cup\{0\}$ where x,y,z are distinct and there are $3l$ for some $l \in \mathbb{N}\cup\{0\}$ where $x = y, x \neq z$ and $y \neq z$. Assume that x_0 is the solution of $x^3 \equiv \alpha \mod \pi$. Then $x_0\omega$ and $x_0\omega^2$ are also solutions. Thus there is exactly one solution in Q_1. Since $(\alpha/\pi)_3 = 1$ if and only if $x^3 \equiv \alpha \mod \pi$ is

solvable, $(\alpha/\pi)_3 = 1$ if and only if $\tau(\alpha,\pi) = 6k+3l+1$ for some $k, l \in \mathbb{N}\cup\{0\}$ and $(\alpha/\pi)_3 \neq 1$ if and only if $\tau(\alpha,\pi) = 6k+3l$ for some $k, l \in \mathbb{N}\cup\{0\}$. In other words, $(\alpha/\pi)_3 = 1$ if and only if $\tau(\alpha,\pi) \equiv 1 \mod 3$ and $(\alpha/\pi)_3 \neq 1$ if and only if $\tau(\alpha,\pi) \equiv 0 \mod 3$. In addition, $\tau(\alpha,\pi) \not\equiv 2 \mod 3$. □

By the cubic reciprocity law, we have the following property.

Proposition 2.3 Let α and π be primary primes in $\mathbb{Z}[\omega]$ with $N\alpha, N\pi \neq 3$ and $N\alpha \neq N\pi$. Then

$$\tau(\alpha,\pi) \equiv \tau(\pi,\alpha) \mod 3.$$

Proof. By Theorem 1.19, we have $(\alpha/\pi)_3 = (\pi/\alpha)_3$, so $\tau(\alpha,\pi) \equiv \tau(\pi,\alpha) \mod 3$ by Proposition 2.2. □

Proposition 2.4 If $\frac{N\pi-1}{3} \equiv 1 \mod 3$, then

a. $(\alpha/\pi)_3 = \omega$ if and only if $\tau(\alpha\omega^2,\pi) \equiv 1 \mod 3$, and

b. $(\alpha/\pi)_3 = \omega^2$ if and only if $\tau(\alpha\omega,\pi) \equiv 1 \mod 3$.

Proof. Suppose that $\frac{N\pi-1}{3} \equiv 1 \mod 3$. Then $(\omega^2/\pi)_3 \equiv (\omega^2)^{\frac{N\pi-1}{3}} \equiv \omega^2 \mod \pi$. Proposition 2.2 and Proposition 1.14 (b) imply that

$$\tau(\alpha\omega^2,\pi) \equiv 1 \mod 3 \Leftrightarrow (\alpha\omega^2/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3(\omega^2/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3 = \omega$$

Since $(\omega/\pi)_3 \equiv \omega^{\frac{N\pi-1}{3}} \equiv \omega \mod \pi$, we also have

$$\tau(\alpha\omega,\pi) \equiv 1 \mod 3 \Leftrightarrow (\alpha\omega/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3(\omega/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3 = \omega^2$$

as desired. □

Proposition 2.5 If $\frac{N\pi-1}{3} \equiv 2 \mod 3$, then

a. $(\alpha/\pi)_3 = \omega$ if and only if $\tau(\alpha\omega,\pi) \equiv 1 \mod 3$, and

b. $(\alpha/\pi)_3 = \omega^2$ if and only if $\tau(\alpha\omega^2,\pi) \equiv 1 \mod 3$.

Proof. Suppose that $\frac{N\pi-1}{3} \equiv 2 \mod 3$. Then $(\omega/\pi)_3 \equiv \omega^{\frac{N\pi-1}{3}} \equiv \omega^2 \mod \pi$ and $(\omega^2/\pi)_3 \equiv (\omega^2)^{\frac{N\pi-1}{3}} \equiv \omega \mod \pi$. Similar to the previous proposition, we obtain

$$\tau(\alpha\omega,\pi) \equiv 1 \mod 3 \Leftrightarrow (\alpha\omega/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3(\omega/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3 = \omega \text{ and}$$
$$\tau(\alpha\omega^2,\pi) \equiv 1 \mod 3 \Leftrightarrow (\alpha\omega^2/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3(\omega^2/\pi)_3 = 1 \Leftrightarrow (\alpha/\pi)_3 = \omega^2.$$

This completes the proof. □

Proposition 2.6 If $\frac{N\pi-1}{3} \equiv 0 \mod 3$, then

$$\tau(\alpha,\pi) \equiv \tau(\alpha\omega,\pi) \equiv \tau(\alpha\omega^2,\pi) \mod 3.$$

Proof. Suppose that $\frac{N\pi-1}{3} \equiv 0 \mod 3$. Then $(\omega/\pi)_3 \equiv \omega^{\frac{N\pi-1}{3}} \equiv 1 \mod \pi$ and $(\omega^2/\pi)_3 \equiv (\omega^2)^{\frac{N\pi-1}{3}} \equiv 1 \mod \pi$. It follows that $(\alpha/\pi)_3 = (\alpha\omega/\pi)_3 = (\alpha\omega^2/\pi)_3$. Hence, $\tau(\alpha,\pi) \equiv \tau(\alpha\omega,\pi) \equiv \tau(\alpha\omega^2,\pi) \mod 3$. □

Arithemetic properties of $\tau(-,\pi)$ are presented below.

Proposition 2.7 If $\alpha,\beta \in \mathbb{Z}[\omega]$ are such that $\pi \nmid \alpha$ and $\pi \nmid \beta$ and $\tau(\alpha,\pi) \equiv 1 \mod 3$, then $\tau(\alpha\beta,\pi) \equiv \tau(\beta,\pi) \mod 3$.

Proof. Suppose that $\alpha,\beta \in \mathbb{Z}[\omega]$ are such that $\pi \nmid \alpha$ and $\pi \nmid \beta$ and $\tau(\alpha,\pi) \equiv 1 \mod 3$. Then $(\alpha/\pi)_3 = 1$, so $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3 = (\beta/\pi)_3$ by Proposition 1.14 (b). If $(\alpha\beta/\pi)_3 = 1 = (\beta/\pi)_3$, then $\tau(\alpha\beta,\pi) \equiv 1 \equiv \tau(\beta,\pi) \mod 3$ by Proposition 2.2 (a). If $(\alpha\beta/\pi)_3 = (\beta/\pi)_3$, $(\alpha\beta/\pi)_3, (\beta/\pi)_3 \neq 1$ then $\tau(\alpha\beta,\pi) \equiv 0 \equiv \tau(\beta,\pi) \mod 3$ by Proposition 2.2 (b). □

Proposition 2.8 If $\alpha,\beta \in \mathbb{Z}[\omega]$ are such that $\pi \nmid \alpha$ and $\pi \nmid \beta$ and $\alpha \equiv \beta \mod \pi$. Then $\tau(\alpha,\pi) \equiv \tau(\beta,\pi) \mod 3$.

Proof. Suppose that $\alpha,\beta \in \mathbb{Z}[\omega]$ and $\alpha \equiv \beta \mod \pi$. By Proposition 1.14 (c), we have $(\alpha/\pi)_3 = (\beta/\pi)_3$. If $(\alpha/\pi)_3 = 1 = (\beta/\pi)_3$, then $\tau(\alpha,\pi) \equiv 1 \equiv \tau(\beta,\pi) \mod 3$ by Proposition 2.2 (a). If $(\alpha/\pi)_3 = (\beta/\pi)_3$ and $(\alpha/\pi)_3, (\beta/\pi)_3 \neq 1$ then $\tau(\alpha,\pi) \equiv 0 \equiv \tau(\beta,\pi) \mod 3$ by Proposition 2.2 (b). □

Proposition 2.9 Let $\alpha \in \mathbb{Z}[\omega]$ be such that $\pi \nmid \alpha$. Then $\tau(\alpha,\pi) \equiv \tau(\overline{\alpha},\overline{\pi}) \equiv \tau(\alpha^2,\pi) \mod 3$.

Proof. Note that $x^3 \equiv \alpha \mod \pi$ is solvable $\Leftrightarrow \overline{x}^3 \equiv \overline{\alpha} \mod \pi$ is solvable. Then $(\alpha/\pi)_3 = 1 \Leftrightarrow (\overline{\alpha}/\overline{\pi})_3 = 1$, so $\tau(\alpha,\pi) \equiv \tau(\overline{\alpha},\overline{\pi}) \mod 3$ by Proposition 2.2. In addition, by Proposition 1.15 (a) and (b), we have $(\overline{\alpha}/\overline{\pi})_3 = \overline{(\alpha,\pi)_3} = (\alpha^2,\pi)_3$. If $(\overline{\alpha}/\overline{\pi})_3 = 1 = (\alpha^2,\pi)_3$, then $\tau(\overline{\alpha},\overline{\pi}) \equiv 1 \equiv \tau(\alpha^2,\pi) \mod 3$ by Proposition 2.2 (a). If $(\overline{\alpha}/\overline{\pi})_3 = (\alpha^2/\pi)_3$, $(\overline{\alpha}/\overline{\pi})_3, (\alpha^2/\pi)_3 \neq 1$, then $\tau(\overline{\alpha}/,\overline{\pi}) \equiv 0 \equiv \tau(\alpha^2,\pi) \mod 3$ by Proposition 2.2 (b). Hence $\tau(\alpha,\pi) \equiv \tau(\overline{\alpha},\overline{\pi}) \equiv \tau(\alpha^2,\pi) \mod 3$. □

Proposition 2.10 If $\pi = q$ is a rational prime congruence to 2 modulo 3 and n is a rational integer relatively prime to q, then $\tau(n, q) \equiv 1 \mod 3$

Proof. By Corollary 1.16, $(n/q)_3 = 1$, so $\tau(n, q) \equiv 1 \mod 3$. □

Next, we assume that $\pi = a + b\omega$ is a primary prime in $\mathbb{Z}[\omega]$. Then $a \equiv 2 \mod 3$ and $b \equiv 0 \mod 3$. Write $\pi = (3m - 1) + 3n\omega$ for some $m, n \in \mathbb{Z}$. Thus, $N\pi = 9m^2 + 9n^2 - 9mn - 6m + 3n + 1$ and $\frac{N\pi-1}{3} = 3m^2 + 3n^2 - 3mn - 2m + n \equiv m + n \mod 3$.

Lemma 2.11 Let π be a primary prime in $\mathbb{Z}[\omega]$. Then

a. If $\pi = q$ is a rational prime congruent to 2 modulo 3, then

$$(\omega/q)_3 = \omega^t \text{ if and only if } q \equiv 3t - 1 \mod 9$$

for all $t \in \{0, 1, 2\}$.

b. If $N\pi = p$ is a rational prime congruent to 1 modulo 3, then

$$(\omega/\pi)_3 = \omega^t \text{ if and only if } (\pi \equiv 3t - 1 - 3n(1 - \omega) \mod 9 \text{ for some } n \in \{0, 1, 2\})$$

for all $t \in \{0, 1, 2\}$.

Proof. a. Suppose that $\pi = q$ is a rational prime congruent to 2 modulo 3 and write $q = 3m - 1$ for some $m \in \mathbb{N}$. Then

$$(\omega/q)_3 \equiv \omega^{\frac{Nq-1}{3}} \equiv \omega^{\frac{q^2-1}{3}} \equiv \omega^{\frac{(3m-1)^2-1}{3}} \equiv \omega^{3m^2-2m} \equiv \omega^m \mod q.$$

Thus, for $t \in \{0, 1, 2\}$, we have $(\omega/q)_3 = \omega^t$ if and only if $\omega^t \equiv \omega^m \mod q$ if and only if $t \equiv m \mod 3$ if and only if $3t \equiv 3m \mod 9$ if and only if $q \equiv 3t - 1 \mod 9$ because $q = 3m - 1$.

b. Suppose that $N\pi = p$ is a rational prime congruent to 1 modulo 3. Since π is primary, write $\pi = a + b\omega = (3m - 1) + 3n\omega$ for some $m, n \in \mathbb{Z}$. Then $N\pi = (3m - 1)^2 - (3m - 1)(3n) + (3n)^2 = 9m^2 - 6m + 1 - 9mn + 3n + 9n^2$ and

$$(\omega/\pi)_3 \equiv \omega^{\frac{N\pi-1}{3}} \equiv \omega^{3m^2-2m-3mn+n+3n^2} \equiv \omega^{m+n} \mod \pi.$$

Thus, for $t \in \{0, 1, 2\}$, we have $(\omega/\pi)_3 = \omega^t$ if and only if $\omega^t \equiv \omega^{m+n} \mod \pi$ if and only if $t \equiv m + n \mod 3$ if and only if $3t - 1 \equiv 3m - 1 + 3n \mod 9$ if and only if $3t - 1 \equiv \pi - 3n\omega + 3n \mod 9$ if and only if $\pi \equiv 3t - 1 - 3n(1 - \omega) \mod 9$. Since we consider modulo 9, $n \in \{0, 1, 2\}$. □

Proposition 2.12 Let π be a primary prime in $\mathbb{Z}[\omega]$. Then

a. If $\pi = q$ is a rational prime congruent to 2 modulo 3, then

i. $\tau(\omega, q) \equiv 1 \mod 3$ if and only if $q \equiv -1 \mod 9$, and

ii. $\tau(\omega, q) \equiv 0 \mod 3$ if and only if $q \equiv 2$ or $5 \mod 9$.

b. If $N\pi = p$ is a rational prime congruent to 1 modulo 3, then

i. $\tau(\omega, \pi) \equiv 1 \mod 3$ if and only if ($\pi \equiv -1 - 3n(1-\omega) \mod 9$) for some $n \in \{0, 1, 2\}$, and

ii. $\tau(\omega, \pi) \equiv 0 \mod 3$ if and only if ($\pi \equiv 2 - 3n(1-\omega)$ or $5 - 3n(1-\omega) \mod 9$ for some $n \in \{0, 1, 2\}$).

Proof. a. Suppose that $\pi = q$ is a rational prime congruent to 2 modulo 3. By Lemma 2.11 (a), we have $(\omega/q)_3 = 1$ if and only if $q \equiv -1 \mod 9$ and $(\omega/q)_3 \neq 1$ if and only if $q \equiv 2$ or $5 \mod 9$. Hence, $\tau(\omega, q) \equiv 1 \mod 3$ if and only if $q \equiv -1 \mod 9$ and $\tau(\omega, q) \equiv 0 \mod 3$ if and only if $q \equiv 2$ or $5 \mod 9$ by Proposition 2.2.
b. Suppose that $N\pi = p$ is a rational prime congruent to 1 modulo 3. By Lemma 2.11 (b), we have $(\omega/\pi)_3 = 1$ if and only if $\pi \equiv -1 - 3n(1-\omega) \mod 9$ and $(\omega/\pi)_3 \neq 1$ if and only if $\pi \equiv 2 - 3n(1-\omega)$ or $5 - 3n(1-\omega) \mod 9$. Hence, $\tau(\omega, p) \equiv 1 \mod 3$ if and only if $\pi \equiv -1 - 3n(1-\omega) \mod 9$ and $\tau(\omega, p) \equiv 0 \mod 3$ if and only if $\pi \equiv 2 - 3n(1-\omega)$ or $5 - 3n(1-\omega) \mod 9$ by Proposition 2.2. □

Lemma 2.13 Let π be a primary prime in $\mathbb{Z}[\omega]$. Then

$(1 - \omega/\pi)_3 = \omega^t$ if and only if ($\pi \equiv -3t - 1 + 3n\omega \mod 9$ for some $n \in \{0, 1, 2\}$)

for all $t \in \{0, 1, 2\}$.

Proof. Suppose that π be a primary prime in $\mathbb{Z}[\omega]$. Write $\pi = (3m - 1) + 3n\omega$ for some $m, n \in \mathbb{Z}$. By Theorem 1.20, we have $(1 - \omega/\pi)_3 = \omega^{2m}$, so $(1 - \omega/\pi)_3 = \omega^t$ if and only if $\omega^t = \omega^{2m}$ if and only if $t \equiv 2m \mod 3$ if and only if $-3t \equiv 3m \mod 9$ if and only if $-3t - 1 \equiv 3m - 1 \mod 9$ if and only if $-3t - 1 + 3n\omega \equiv 3m - 1 + 3n\omega = \pi \mod 9$. Since we consider modulo 9, $n \in \{0, 1, 2\}$. □

Proposition 2.14 Let $\pi = a + b\omega$ be a primary prime in $\mathbb{Z}[\omega]$. Then

a. $\tau(1 - \omega, \pi) \equiv 1 \mod 3$ if and only if ($\pi \equiv -1 + 3n\omega \mod 9$ for some $n \in \{0, 1, 2\}$), and

b. $\tau(1-\omega,\pi) \equiv 0 \mod 3$ if and only if $\pi \equiv 2+3n\omega$ or $5+3n\omega \mod 9$ for some $n \in \{0,1,2\}$.

Proof. By Lemma 2.13, we have $(1-\omega/\pi)_3 = 1$ if and only if $\pi \equiv -1+3n\omega \mod 9$ and $(1-\omega/\pi)_3 \neq 1$ if and only if $\pi \equiv 2+3n\omega+3$ or $5+3n\omega \mod 9$. Therefore, $\tau(1-\omega,\pi) \equiv 1 \mod 3$ if and only if $\pi \equiv -1+3n\omega \mod 9$ and $\tau(1-\omega,\pi) \equiv 0 \mod 3$ if and only if $\pi \equiv 2+3n\omega$ or $5+3n\omega \mod 9$ by Proposition 2.2. □

Lemma 2.15 Let π be a primary prime in $\mathbb{Z}[\omega]$. Then

$(3/\pi)_3 = \omega^t$ if and only if ($\pi \equiv (3m-1)-3t\omega \mod 9$ for some $m \in \{0,1,2\}$)

for all $t \in \{0,1,2\}$.

Proof. Suppose that π be a primary prime in $\mathbb{Z}[\omega]$. Write $\pi = (3m-1)+3n\omega$ for some $m, n \in \mathbb{Z}$. Note that $(1-\omega)^2 = -3\omega$, we have $((1-\omega)/\pi)_3{}^2 = ((1-\omega)^2/\pi)_3$ $= (3/\pi)_3(\omega/\pi)_3(-1/\pi)_3$ by Propositions 1.14 (b) and 1.15 (a). Thus, $(1-\omega/\pi)_3 = (3/\pi)_3{}^2(\omega/\pi)_3{}^2$. By Lemma 2.11 and Theorem 1.20, we have $(\omega/\pi)_3 = \omega^{m+n}$ and $(1-\omega/\pi)_3 = \omega^{2m}$. It follows that $\omega^{2m} = (3/\pi)_3{}^2\omega^{2m+2n}$. Hence $(3/\pi)_3{}^2 = \omega^n$, so $(3/\pi)_3 = \omega^{2n}$. This implies that $(3/\pi)_3 = \omega^t$ if and only if $\omega^t \equiv \omega^{2n} \mod \pi$ if and only if $t \equiv 2n \mod 3$ if and only if $3t\omega \equiv -3n\omega \mod 9$ if and only if $(3m-1)-3t\omega$ $\equiv (3m-1)+3n\omega = \pi \mod 9$. Since we consider modulo 9, $m \in \{0,1,2\}$. □

Proposition 2.16 Let π be a primary prime in $\mathbb{Z}[\omega]$. Then
a. $\tau(3,\pi) \equiv 1 \mod 3$ if and only if $\pi \equiv 3m-1 \mod 9$ and
b. $\tau(3,\pi) \equiv 0 \mod 3$ if and only if $\pi \equiv (3m-1)+3\omega$ or $(3m-1)+6\omega \mod 9$ for some $m \in \{0,1,2\}$.

Proof. By Lemma 2.15, we have $(3/\pi)_3 = 1$ if and only if $\pi \equiv 3m-1 \mod 9$ and $(3/\pi)_3 \neq 1$ if and only if $\pi \equiv (3m-1)+3\omega$ or $(3m-1)+6\omega \mod 9$. Therefore, $\tau(3,\pi) \equiv 1 \mod 3$ if and only if $\pi \equiv 3m-1 \mod 9$ and $\tau(3,\pi) \equiv 0 \mod 3$ if and only if $\pi \equiv (3m-1)+3\omega$ or $(3m-1)+6\omega \mod 9$ by Proposition 2.2. □

2.2 Modular Divisor Function $\eta(-,\pi)$ on $\mathbb{Z}[i]$

Throughtout this section, let π be an irreducible element in $\mathbb{Z}[i]$ with $N\pi \neq 2$.

Definition 2.17 The **modular divisor function** $\eta(-,\pi)$ on $\mathbb{Z}[i]$ is defined by

$$\eta(\alpha,\pi) = \#\{(x,y,z,w) : x,y,z,w \in (\mathbb{Z}[i]/(\pi))^\times \text{ in the 1st quadrant, and } xyzw \equiv \alpha \mod \pi\}$$

for all $\alpha \in \mathbb{Z}[i]$ and $\pi \nmid \alpha$.

Proposition 2.18 Let $\alpha \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha$. Then

a. $(\alpha/\pi)_4 = 1$ if and only if $\eta(\alpha,\pi)$ is odd, and

b. $(\alpha/\pi)_4 \neq 1$ if and only if $\eta(\alpha,\pi)$ is even.

In other words,

a. $x^4 \equiv \alpha \mod \pi$ is solvable if and only if $\eta(\alpha,\pi)$ is odd, and

b. $x^4 \equiv \alpha \mod \pi$ is not solvable if and only if $\eta(\alpha,\pi)$ is even.

Proof. If (x,y,z,w) is a pair counting towards $\eta(\alpha,\pi)$, then permutations of x,y,z,w in it is also a pair counting towards $\eta(\alpha,\pi)$. It follows that there are $24k$ pairs for some $k \in \mathbb{N}\cup\{0\}$ where x,y,z,w are distinct and there are $12l$ pairs for some $l \in \mathbb{N}\cup\{0\}$ where $x = y$ and x,z,w are distinct, $4m$ pairs for some $m \in \mathbb{N}\cup\{0\}$ where $x = y = z$ and $x,y,z \neq w$, $6n$ pairs for some $n \in \mathbb{N}\cup\{0\}$ where $x = y, z = w$ and $x \neq z$. Assume that x_0 is the solution of $x^4 \equiv \alpha \mod \pi$. Then $x_0 i, -x_0$ and $-x_0 i$ are also solutions. Thus, there is exactly one solution in the 1st quadrant. Since $(\alpha/\pi)_4 = 1$ if and only if $x^4 \equiv \alpha \mod \pi$ is solvable, $(\alpha/\pi)_4 = 1$ if and only if $\eta(\alpha,\pi) = 24k + 12l + 4m + 6n + 1$ for some $k,l,m,n \in \mathbb{N}\cup\{0\}$ and $(\alpha/\pi)_4 \neq 1$ if and only if $\eta(\alpha,\pi) = 24k + 12l + 4m + 6n$ for some $k,l,m,n \in \mathbb{N}\cup\{0\}$. In other words, $(\alpha/\pi)_4 = 1$ if and only if $\eta(\alpha,\pi)$ is odd and $(\alpha/\pi)_4 \neq 1$ if and only if $\eta(\alpha,\pi)$ is even. □

Corollary 2.19 Let $\alpha \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha$ and $(\alpha/\pi)_4 = \pm i$. Then $\eta(\alpha,\pi) \equiv 0 \mod 4$.

Proof. Suppose that $\alpha \in \mathbb{Z}[i]$ is such that $\pi \nmid \alpha$ and $(\alpha/\pi)_4 = \pm i$. By Corollary 1.34, we have $x^2 \equiv \alpha \mod \pi$ is not solvable, so $x^4 \equiv \alpha \mod \pi$ and $x^2y^2 \equiv \alpha \mod \pi$ is

not solvable. Thus the pairs (x, x, y, y) and (x, x, x, x) are not counting towards $\eta(\alpha, \pi)$. Hence $\eta(\alpha, \pi) = 24k + 12l + 4m \equiv 0 \mod 4$ for some $k, l, m \in \mathbb{N} \cup \{0\}$. □

From the quartic reciprocity law, we have the following proposition.

Proposition 2.20 Let α and π be primary primes in $\mathbb{Z}[i]$ with $N\alpha, N\pi \neq 2$ and $N\alpha \neq N\pi$. Then

$$\eta(\alpha, \pi) \equiv \eta((-1)^{((N\alpha-1)/4)((N\pi-1)/4)}\pi, \alpha) \mod 2.$$

Proof. By Theorem 1.44, we have $(\alpha/\pi)_4 = (\pi/\alpha)_4(-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\pi-1}{4}}$. If $\frac{N\alpha-1}{4}, \frac{N\pi-1}{4}$ are not both odd integers, then $(\alpha/\pi)_4 = (\pi/\alpha)_4$, so $\eta(\alpha, \pi) \equiv \eta(\pi, \alpha) \mod 2$ by Proposition 2.18. If $\frac{N\alpha-1}{4}, \frac{N\pi-1}{4}$ are both odd integers, then $(\alpha/\pi)_4 = -(\pi/\alpha)_4 = (-1/\alpha)_4(\pi/\alpha)_4 = (-\pi/\alpha)_4$ by Proposition 1.33 (b), so $\eta(\alpha, \pi) \equiv \eta(-\pi, \alpha) \mod 2$ by Proposition 2.18. □

Next, we study arithmetic properties of $\eta(-, \pi)$.

Proposition 2.21 If $\alpha, \beta \in \mathbb{Z}[i]$ are such that $\pi \nmid \alpha$ and $\pi \nmid \beta$ and $\eta(\alpha, \pi)$ is odd, then $\eta(\alpha\beta, \pi) \equiv \eta(\beta, \pi) \mod 2$.

Proof. Suppose that $\alpha, \beta \in \mathbb{Z}[i]$, $\pi \nmid \alpha$, $\pi \nmid \beta$ and $\eta(\alpha, \pi)$ is odd. Then $(\alpha/\pi)_4 = 1$, so $(\alpha\beta/\pi)_4 = (\alpha/\pi)_4(\beta/\pi)_4 = (\beta/\pi)_4$ by Proposition 1.33 (c). If $(\alpha\beta/\pi)_4 = 1 = (\beta/\pi)_1$, then $\eta(\alpha\beta, \pi) \equiv 1 \equiv \eta(\beta, \pi) \mod 2$ by Proposition 2.18 (a). If $(\alpha\beta/\pi)_4 = (\beta/\pi)_4$ and $(\alpha\beta/\pi)_4, (\beta/\pi)_4 \neq 1$ then $\eta(\alpha\beta, \pi) \equiv 0 \equiv \eta(\beta, \pi) \mod 2$ by Proposition 2.18 (b). □

Proposition 2.22 If $\alpha, \beta \in \mathbb{Z}[i]$ are such that $\pi \nmid \alpha$ and $\pi \nmid \beta$ and $\alpha \equiv \beta \mod \pi$, then $\eta(\alpha, \pi) \equiv \eta(\beta, \pi) \mod 2$.

Proof. Suppose that $\alpha, \beta \in \mathbb{Z}[i]$, $\pi \nmid \alpha$, $\pi \nmid \beta$ and $\alpha \equiv \beta \mod \pi$. By Proposition 1.33 (d), we have $(\alpha/\pi)_4 = (\beta/\pi)_4$. If $(\alpha/\pi)_4 = 1 = (\beta/\pi)_4$, then $\eta(\alpha, \pi) \equiv 1 \equiv \eta(\beta, \pi) \mod 2$ by Proposition 2.18 (a). If $(\alpha/\pi)_4 = (\beta/\pi)_4$, $(\alpha/\pi)_4, (\beta/\pi)_4 \neq 1$ then $\eta(\alpha, \pi) \equiv 0 \equiv \eta(\beta, \pi) \mod 2$ by Proposition 2.18 (b). □

Proposition 2.23 Let $\alpha \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha$. Then $\eta(\overline{\alpha}, \overline{\pi}) \equiv \eta(\alpha, \pi) \mod 2$.

Proof. Suppose $\alpha \in \mathbb{Z}[i]$ with $\pi \nmid \alpha$. Note that $x^4 \equiv \alpha \mod \pi$ is solvable $\Leftrightarrow \overline{x}^4 \equiv \overline{\alpha} \mod \pi$ is solvable. Then $(\alpha/\pi)_4 = 1 \Leftrightarrow (\overline{\alpha}/\overline{\pi})_4 = 1$, so $\eta(\alpha, \pi) \equiv \eta(\overline{\alpha}, \overline{\pi}) \mod 2$ by Proposition 2.18. □

Proposition 2.24 Let π and $\lambda \in \mathbb{Z}[i]$ be primes and $(\pi) = (\lambda)$ and $\alpha \in \mathbb{Z}[i]$ with $\pi \nmid \alpha$ and $\lambda \nmid \alpha$. Then $\eta(\alpha, \pi) \equiv \eta(\alpha, \lambda) \mod 2$.

Proof. Suppose that $\pi, \lambda \in \mathbb{Z}[i]$ are primes and $(\pi) = (\lambda)$ and $\alpha \in \mathbb{Z}[i]$ with $\pi \nmid \alpha$ and $\lambda \nmid \alpha$. By Proposition 1.33 (e), we have $(\alpha/\pi)_4 = (\alpha/\lambda)_4$. If $(\alpha/\pi)_4 = 1 = (\alpha/\lambda)_4$, then $\eta(\alpha, \pi) \equiv 1 \equiv \eta(\alpha, \lambda) \mod 2$ by Proposition 2.18 (a). If $(\alpha/\pi)_4 = (\alpha/\lambda)_4$, $(\alpha/\pi)_4, (\alpha/\lambda)_4 \neq 1$ then $\eta(\alpha, \pi) \equiv 0 \equiv \eta(\alpha/, \lambda) \mod 2$ by Proposition 2.18 (b). □

Proposition 2.25 Let $\alpha \in \mathbb{Z}, \alpha \neq 0$, and $a \in \mathbb{Z}$ an odd nonunit element. If $\gcd(\alpha, a) = 1$, then $\eta(\alpha, a)$ is odd.

Proof. Suppose that $\alpha \in \mathbb{Z}[i], \alpha \neq 0$ and $a \in \mathbb{Z}$ is an odd nonunit element and $\gcd(\alpha, a) = 1$. By Proposition 1.42, we have $(\alpha/a)_4 = 1$, so $\eta(a, q)$ is odd by Proposition 2.18 (a). □

Proposition 2.26 Let $\pi = q$ be a rational prime congruent to 3 modulo 4. Then
a. $\eta(i, q)$ is odd if and only if $q = 8k - 1$ for some $m \in \mathbb{Z}$, and
b. $\eta(i, q)$ is even if and only if $q = 8l + 3$ for some $l \in \mathbb{Z}$.

Proof. Suppose that $\pi = q$ is a rational prime congruent to 3 modulo 4. Write $q = 4t - 1$ for some $t \in \mathbb{Z}$. Then $(i/q)_4 \equiv i^{\frac{Nq-1}{4}} \equiv i^{\frac{q^2-1}{4}} \equiv i^{\frac{16t^2-8t}{4}} \equiv i^{4t^2-2t} \equiv i^{2t} \equiv (-1)^t \mod \pi$. Thus, $(i/q)_4 = 1$ if and only if t is even if and only if $q \equiv -1 \mod 8$, so $\eta(i, q)$ is odd if and only if $q = 8k - 1$ for some $k \in \mathbb{Z}$ by Proposition 2.18 (a) and $(i/q)_4 = -1$ if and only if t is odd if and only if $q \equiv 3 \mod 8$, so $\eta(i, q)$ is even if and only if $q = 8l + 3$ for some $l \in \mathbb{Z}$ by Proposition 2.18 (b). □

In what follows, we assume that $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$. Then ($a \equiv 1 \mod 4$ and $b \equiv 0 \mod 4$) or ($a \equiv 3 \mod 4$ and $b \equiv 2 \mod 4$) by Proposition 1.37.

Lemma 2.27 Let $\pi = a + bi$ be a primary prime with $N\pi = p$. Then $a \equiv (-1)^{\frac{p-1}{4}} \mod 4$ and $b \equiv 1 - (-1)^{\frac{p-1}{4}} \mod 4$.

Proof. Suppose that $\pi = a + bi$ be a primary prime with $N\pi = p$.
Case 1. $a \equiv 1 \mod 4$ and $b \equiv 0 \mod 4$. Write $\pi = (4k+1) + 4li$ for some $k, l \in \mathbb{Z}$. We claim that $\frac{p-1}{4}$ is even. Note that $p = N\pi = (4k+1)^2 + (4l)^2 = 16k^2$ $+8k + 1 + 16l^2$, so $\frac{p-1}{4} = 4k^2 + 2k + 4l^2$ is even. Hence, we have the claim.
Case 2. $a \equiv 3 \mod 4$ and $b \equiv 2 \mod 4$. Write $\pi = (4k+3) + (4l+2)i$ for some $k, l \in \mathbb{Z}$. We claim that $\frac{p-1}{4}$ is odd. Note that $p = N\pi = (4k+3)^2 + (4l+2)^2 = 16k^2 + 24k + 9 + 16l^2 + 16l + 4$, so $\frac{p-1}{4} = 4k^2 + 6k + 4l^2 + 4l + 3$ is odd. Hence, we have the claim.

The desired results easily follow from the above two cases. □

Proposition 2.28 Let $\pi = a + bi$ be a primary prime with $N\pi = p$. Then
a. $\eta(i, \pi)$ is odd if and only if $\pi \equiv 1 + 4li \mod 8$ for some $l \in \{0, 1\}$, and
b. $\eta(i, \pi)$ is even if and only if ($\pi \equiv 5 + 4li \mod 8$ or $\pi \equiv 3 + 2i \mod 4$ for some $l \in \{0, 1\}$).

Proof. Suppose that $\pi = a + bi$ is a primary prime with $N\pi = p$.
Case 1. $a \equiv 1 \mod 4$ and $b \equiv 0 \mod 4$. Write $\pi = (4k+1) + 4li$ for some $k, l \in \mathbb{Z}$. Then $N\pi = (4k+1)^2 + (4l)^2 = 16k^2 + 8k + 1 + 16l^2$ and

$$(i/\pi)_4 \equiv i^{\frac{N\pi-1}{4}} = i^{4k^2+2k+4l^2} \equiv i^{2k} = (-1)^k \mod \pi.$$

Thus, for $t \in \{0, 1\}$, we have $(i/\pi)_4 = (-1)^t$ if and only if $(-1)^t \equiv (-1)^k \mod \pi$ if and only if $t \equiv k \mod 2$ if and only if $4t + 1 \equiv 4k + 1 \mod 8$ if and only if $4t + 1 +$ $4li \equiv 4k + 1 + 4li = \pi \mod 8$. Hence, $(i/\pi)_4 = 1$ if and only if $\pi \equiv 1 + 4li \mod 8$, and $(i/\pi)_4 = -1$ if and only if $\pi \equiv 5 + 4li \mod 8$.
Case 2. $a \equiv 3 \mod 4$ and $b \equiv 2 \mod 4$. Write $\pi = (4k+3) + (4l+2)i$ for some $k, l \in \mathbb{Z}$. Then $N\pi = (4k+3)^2 + (4l+2)^2 = 16k^2 + 24k + 9 + 16l^2 + 16l + 4$ and

$$(i/\pi)_4 \equiv i^{\frac{N\pi-1}{4}} = i^{4k^2+6k+4l^2+4l+2} \equiv i^{2k+3} = (-1)^k i \mod \pi.$$

Hence, $(i/\pi)_4 \neq 1$.

The desired results easily follow from the above two cases and Proposition 2.18. □

Proposition 2.29 If p is a rational prime congruent to 1 modulo 4, then $(i/p)_4 = (-1)^{\eta(-1,\pi)+1}$ where π is primary prime with $N\pi = p$.

Proof. Suppose that p is a rational prime congruent to 1 modulo 4. Then there exists a primary prime $\pi = a + bi \in \mathbb{Z}[i]$ such that $N\pi = p$. By Proposition 1.40, we have $(i/p)_4 = (-1)^{\frac{p-1}{4}}$. Thus, $(i/p)_4 = 1$ if and only if $\frac{p-1}{4}$ is even if and only if $a \equiv 1 \mod 4$ and $b \equiv 0 \mod 4$ (by Lemma 2.26) if and only if $\eta(-1, \pi)$ is odd (by Proposition 2.27 (a)), and $(i/p)_4 = -1$ if and only if $\frac{p-1}{4}$ is odd if and only if $a \equiv 3 \mod 4$ and $b \equiv 2 \mod 4$ (by Lemma 2.26) if and only if $\eta(-1, \pi)$ is even (by Proposition 2.27 (b)). Hence $(i/p)_4 = (-1)^{\eta(-1,\pi)+1}$. □

Proposition 2.30 Let π be a primary prime. Then
a. $\eta(-1, \pi)$ is odd if and only if $\pi \equiv 1 \mod 4$, and
b. $\eta(-1, \pi)$ is even if and only if $\pi \equiv 3 + 2i \mod 4$.

Proof. Suppose that π is a primary prime. By Proposition 1.37, we have

$$(-1/\pi)_4 = (-1)^{(a-1)/2}$$

where a is the real part of π. Then $(-1/\pi)_4 = (-1)^t$ if and only if $(-1)^{\frac{a-1}{2}} \equiv (-1)^t \mod \pi$ if and only if $\frac{a-1}{2} \equiv t \mod 2$ if and only if $a \equiv 2t + 1 \mod 4$. Thus, $(-1/\pi)_4 = 1$ if and only if $a \equiv 1 \mod 4$ and $(-1/\pi)_4 = -1$ if and only if $a \equiv 3 \mod 4$. It follows by Proposition 1.37 that $(-1/\pi)_4 = 1$ if and only if $a \equiv 1 \mod 4$ and $b \equiv 0 \mod 4$ if and only if $\pi \equiv 1 \mod 4$ and $(-1/\pi)_4 = -1$ if and only if $\pi \equiv 3 + 2i \mod 4$. Hence $\eta(-1, \pi)$ is odd if and only if $\pi \equiv 1 \mod 4$, and $\eta(-1, \pi)$ is even if and only if $\pi \equiv 3 + 2i \mod 4$ (by Proposition 2.18). □

References

[1] V. Bucaj, Finding factors of factor rings over Eisenstein integers, *Inter. Math. Forum*, Vol. 9, No.31 (2014), 1521–1537.

[2] J. T. Cross, The Euler Φ - function in the Gaussian Integer, *Amer. Math. Monthly*, Vol. 900, No.8 (1983), 518–528.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Springer, New York, 1990.

[4] R. Steiner, Modular divisor functions and quadratic reciprocity, *Amer. Math. Monthly*, Vol. 117, No.5 (2010), 448–451.

[5] Wikipedia.(2019). *Gaussian integer*. [online]. available :https://en.wikipedia.org/wiki/Gaussian_integer?fbclid=IwAR2kSkZiV_i1qqz7iTmKOxakyB2K6JMFL38TVy-qG60YtR07IxSIucsRtxQ [2019, November 15].

The Project Proposal of Course 2301399 Project Proposal

Academic Year 2019

Project Tittle (Thai)	ฟังก์ชันตัวหารมอดูลาร์และกฎภาวะส่วนกลับกำลังสามและกำลังสี
Project Tittle (English)	Modular divisor functions and cubic and quartic reciprocity laws
Project Advisor	Professor Dr. Yotsanan Meemark
By	Mr. Apinan Pokaew ID 5933556323 Mathematics, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University

---

Background and Rationale

For $n \in \mathbb{N}$, we let $\tau(n)$ denote the number of positive divisors of n. It is well known that $\sqrt{n}$ is an integer if and only if $\tau(n)$ is odd. Steiner[2] studied a modular divisor function $\tau(-, p)$ defined by for an odd prime p and an integer a with $p \nmid a$, $\tau(a, p)$ is the number of ordered pairs of integers (x, y) such that

$$0 < x < \tfrac{1}{2}p,\ 0 < y < \tfrac{1}{2}p,\ xy \equiv a \mod p.$$

He showed that if p is an odd prime and $p \nmid a$, then a is a quadratic residue modulo p if and only if $\tau(a, p)$ is odd. In addition, he used this result to give another proof of the quadratic reciprocity law.

Let $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z} \text{ and } \omega^2 + \omega + 1 = 0\}$. For $a, b \in \mathbb{Z}$, the norm of $a + b\omega$ is $(a + b\omega)(a + b\overline{\omega}) = a^2 + b^2 - ab$ and is denoted by $N(a + b\omega)$. It follows that $\mathbb{Z}[\omega]$ is a Euclidean domain and the norm map is a valuation map. Let π be a prime in $\mathbb{Z}[\omega]$ and $\alpha \in \mathbb{Z}[\omega]$. The field $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has order $N\pi$ and the group of units in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has order $N\pi - 1$. Thus, if $\pi \nmid \alpha$, then $\alpha^{N\pi-1} \equiv 1 \mod \pi$.

Moreover, if $N\pi \neq 3$ and $\pi \nmid \alpha$, then there exists a unique integer $m = 0, 1 \text{ or } 2$ such that $\alpha^{(N\pi-1)/3} \equiv \omega^m \mod \pi$. Assume that $N\pi \neq 3$. The cubic residue symbol of α modulo π is given by

$$(\alpha/\pi)_3 = 0 \text{ if } \pi \mid \alpha \text{ and}$$
$$\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \mod \pi, \text{ with } (\alpha/\pi)_3 \text{ equals to } \omega, \omega^2 \text{ or } 1.$$

We note that α is a cubic residue modulo π if and only if $(\alpha/\pi)_3 = 1$. The cubic reciprocity law is stated as follows.

Theorem. [1] *Let π_1 and π_2 be primes in $\mathbb{Z}[\omega]$ with $\pi_1 \equiv 2 \mod 3$ and $\pi_2 \equiv 2 \mod 3$, $N\pi_1, N\pi_2 \neq 3$ and $N\pi_1 \neq N\pi_2$. Then $(\pi_1/\pi_2)_3 = (\pi_2/\pi_1)_3$.*

Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 + 1 = 0\}$. For $a, b \in \mathbb{Z}$, the norm of $a + bi$ is $(a + bi)(a + b\bar{i}) = a^2 + b^2$ and is also denoted by $N(a + bi)$. It follows that $\mathbb{Z}[i]$ is a Euclidean domain and the norm map is a valuation map. Let π be a prime in $\mathbb{Z}[i]$ and $\alpha \in \mathbb{Z}[i]$. The field $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has order $N\pi$ and the group of units in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ has order $N\pi - 1$. Thus, if $\pi \nmid \alpha$, then $\alpha^{N\pi-1} \equiv 1 \mod \pi$. Moreover, if $(\pi) \neq (1 + i)$ and $\pi \nmid \alpha$, then there exists a unique integer $j = 0, 1, 2 \text{ or } 3$ such that $\alpha^{(N\pi-1)/4} \equiv i^j \mod \pi$. Assume that π is an irreducible, $N\pi \neq 2$. The quartic residue symbol of α modulo π is given by

$$(\alpha/\pi)_4 = 0 \text{ if } \pi \mid \alpha \text{ and}$$
$$\alpha^{(N\pi-1)/4} \equiv (\alpha/\pi)_4 \mod \pi, \text{ with } (\alpha/\pi)_4 \text{ equals to } i, \text{-1}, -i \text{ or } 1.$$

We note that α is a quartic residue modulo π if and only if $(\alpha/\pi)_4 = 1$. The quartic reciprocity law is stated as follows.

Theorem. [1] *Let π_1 and π_2 be primes in $\mathbb{Z}[i]$ with $\pi_1 \equiv 1 \mod (1 + i)^3$ and $\pi_2 \equiv 1 \mod (1 + i)^3$ and $N\pi_1 \neq N\pi_2$. Then*
$(\pi_2/\pi_1)_4 = (\pi_1/\pi_2)_4(-1)^{((N\pi_1-1)/4)((N\pi_2-1)/4)}$.

We plan to define modular divisor functions on $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ similar to Steiner's $\tau-$function and use their properties to prove the cubic and quartic reciprocity laws.

Objectives

1. Define and study modular divisor functions on $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ similar to Steiner's $\tau-$function which relate cubic and quartic residues.
2. Use the modular divisor functions to prove the cubic and quartic reciprocity laws.

Project Activities

1. Review quadratic residues, Legendre symbols and the quadratic reciprocity law.
2. Study cubic and quartic residues along with cubic and quartic residue symbols and their reciprocity laws.
3. Study Steiner's work on a modular divisor function and the quadratic reciprocity law.
4. Define and study modular divisor functions on $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ similar to Steiner's $\tau-$function.
5. Prove the cubic and quartic reciprocity laws.
6. write a report.

Duration

Procedue	August 2019 - April 2020								
	Aug.	Sep.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	Apr.
1.Review quadratic residues, Legendre symbols and the quadratic reciprocity law.									
2.Study cubic and quartic residues along with cubic and quartic residue symbols and their reciprocity laws.									
3.Study Steiner's work on a modular divisor function and the quadratic reciprocity law.									
4.Define and study modular divisor functions on $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ similar to Steiner's $\tau-$function.									
5.Prove the cubic and quartic reciprocity laws.									
6.write a report.									

Benefits

1. Learn about cubic and quartic residues and their reciprocity laws.
2. Obtain some relationship between modular divisor functions and cubic and quartic residues.
3. Obtain other proofs of the cubic and quartic reciprocity laws.

Equipments

1. A4 paper and stationary
2. Computer
3. Printer

References

[1] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Springer, New York, 1990.

[2] R. Steiner, Modular divisor functions and quadratic reciprocity, *Amer. Math. Monthly*, Vol. 117, No.5 (2010), 448–451.

Author’s profile

Mr. Apinan Pokaew ID 5933556323
Department of Mathematics and Computer Science,
Faculty of Science, Chulalongkorn University