SOME PROBLEMS IN IDEAL CLASS GROUPS AND RELATED TOPICS

By

JAITRA CHATTOPADHYAY

MATH08201504003

Harish-Chandra Research Institute, Prayagraj

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

December, 2019

Homi Bhabha National Institute[1]

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Jaitra Chattopadhyay entitled "Some Problems in Ideal Class Groups and Related Topics" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman – Prof. B. Ramakrishnan	**Date:** 9/3/2020
Guide / Convener – Prof. R. Thangadurai	**Date:** 09/03/2020
Examiner – Prof. Anupam Saikia	**Date:** 09/03/2020
Member 1- Prof. Kalyan Chakraborty	**Date:** 09/03/2020
Member 2- Prof. D. Surya Ramana	**Date:** 09/03/2020
Member 3- Prof. Ratnakumar P. K.	**Date:** 09/03/2020

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I/~~We~~ hereby certify that I/~~we~~ have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 09.03.2020

Place: Prayagraj

Prof. R. Thangadurai
Guide

[1] This page is to be included only for final submission after successful completion of viva voce.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

JAITRA CHATTOPADHYAY

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Jaitra Chattopadhyay

JAITRA CHATTOPADHYAY

List of Publications arising from the thesis

Journal

1. "A short note on the divisibility of class numbers of real quadratic fields," Jaitra Chattopadhyay, *J. Ramanujan Math. Soc*, **2019**, *34*, 389-392.

2. "Biquadratic fields having a non-principal Euclidean ideal class," Jaitra Chattopadhyay and Subramani Muthukrishnan, *J. Number Theory*, **2019,** *204*, 99-112.

Chapters in books and lectures notes

1. "Distribution of residues modulo p using the Dirichlet class number formula," Jaitra Chattopadhyay, Bidisha Roy, Subha Sarkar and R. Thangadurai, *Class Groups of Number Fields and Related Topics (Springer Nature)*, **2020**, 97-107.

Others

1. "On the simultaneous divisibility of class numbers of triples of imaginary quadratic fields," Jaitra Chattopadhyay and Subramani Muthukrishnan, Communicated.

Conferences

1. Presented a talk "On the divisibility of class numbers of quadratic fields" in the International conference on Number Theory at IISER Trivandrum, March, 2019.

2. Presented a talk "Biquadratic fields having a non-principal Euclidean ideal class" in the 5th mini Symposium of the Roman Number Theory Association at Universitá Roma Tre, Rome, Italy, April, 2019.

Jaitra Chattopadhyay

JAITRA CHATTOPADHYAY

Dedicated to
MY PARENTS

and
MY TEACHERS

ACKNOWLEDGEMENTS

First and foremost, I am indebted to my parents for their unceasing love and support for the past twenty seven and half years that put me where I stand today. There were moments of joy that I shared with you and there were lows when the only persons in the world were you whom I could turn to. Those hour-long interactions with my father over phone gave me a new perspective of Mathematics as well as of life. It was impossible for me to get through this journey if you were not there for me. Although words cannot describe what you mean to me but still... a big THANK YOU!!

I express my deepest and profound respect towards my supervisor Prof. R. Thangadurai for nearly everything that happened to me in my PhD days. Academically, I spent most of the time with him and that developed a solid rapport between us. He introduced me the ABC of mathematical research and then carefully guided me through every challenges in the formative years of my research career. Whenever things were not moving as per my expectation, he was the one to have given me the encouragement and confidence that I needed. Thank you very much, Sir, for having faith in me and I am sure I shall be able to live up to your expectation in the coming years.

I am grateful to the members of my Doctoral Committee, Prof. B. Ramakrishnan, Prof. D. S. Ramana, Prof. K. Chakraborty and Prof. P. K. Ratnakumar for their kind support during these years.

I consider myself immensely fortunate that I came in touch with Bhargab Mj and Vinay Mj in RKM Vidyamandira. Their teachings and the philosophy of life played a very crucial role in shaping my personality before I came into pursuing research. Time and again, I visited Vidyamandira and met them in person. I cherish all the love, affection and blessings they have poured on me.

I take this opportunity to thank all my collaborators Thanga Sir, Subramani anna, Veekesh bhaaiya, Pranendu da, Bidisha, Subha and Anand for the wonderful experiences we had while working together. We confronted the ups and downs throughout the completion of our respective projects and it would have been much more difficult to cope up with the frustration unless you were not there to extend your helping hands.

There was a time in the fourth year of my PhD when I was facing a very tough time. Emotionally, I was almost shattered and was about to go in depression. I am lucky to have a friend like Nilanjan who stood by me at that time and

patiently listened to me. There are not many people in the world whom I can call my “friend" but certainly, you deserve to be called one.

Special mentions are due to my batchmates Bidisha, Deba, Subha and Lalit. With four of you, I had countless memories during these years. I feel very fortunate to have you as my colleagues. Without you, my stay at HRI would not have become so much memorable. Thank you very much for being there beside me throughout the journey.

I sincerely thank all the administrative staffs of HRI for their kind support at various stages.

I thank all the mess workers (particularly Mewalal ji and Premkant Bhaaiya) of HRI and the room cleaning staffs (particularly Sanjay bhaaiya). The entire HRI family has been immensely supportive towards me and I am grateful for that.

There are several others who have played a major role behind the completion of my PhD. It is quite impossible to mention all of them here. But I gratefully acknowledge that and convey my heartfelt gratitude and thanks to all of you.

Contents

Summary

This thesis deals with problems on the divisibility of class numbers of quadratic fields, an application of Dirichlet's class number formula and the existence of Euclidean ideal class in certain bi-quadratic fields.

In 2003, Byeon and Koh provided an infinite family of real quadratic fields with class number divisible by 3. In the first problem, we made use of their family to find a lower bound for the number of real quadratic fields with class number divisible by 3 and the discriminant having m distinct prime factors, for a fixed but arbitrary positive integer m.

In 2018, Iizuka proved the existence of an infinite family of tuples of imaginary quadratic fields of the form $\{\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+1})\}$ with $D \in \mathbb{Z}$ and the class numbers being divisible by 3. In the second problem, using the techniques from class field theory, we have extended Iizuka's result for triples of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+1})$ and $\mathbb{Q}(\sqrt{D+k^2})$.

The problem of distribution of quadratic residues and non-residues modulo an odd prime number p is very interesting. In the third problem, we have used the Dirichlet's class number formula for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ to study the distribution of residues and non-residues in some particular subintervals of $[1, p-1]$.

In 1979, Lenstra generalized the notion of Euclidean algorithm in number fields and introduced the Euclidean ideal class. He also proved that if a number field K has an Euclidean ideal class, then the ideal class group Cl_K of K is cyclic. He also proved the converse under the validity of the Extended Riemann Hypothesis (ERH). Recently, Hsu proved the existence of non-principal Euclidean ideal classes in a family of bi-quadratic fields. We have extended Hsu's family and provided a much larger family of number fields of class number 2 having a non-principal Euclidean ideal class.

CHAPTER 1

Divisibility of class numbers of quadratic fields

In this chapter, we define the ideal class group of a number field and give the fundamental results concerning the divisibility properties of the class numbers of quadratic fields. Then we give the proof of the main result, which has been published in [8].

1.1 Definitions and basic results

The results of this section can be found in [13].

Definition 1.1.1 *A subfield K of $\mathbb{C}$ is said to be an algebraic number field (or simply, number field) if the degree $[K : \mathbb{Q}]$ is finite. The integral closure of $\mathbb{Z}$ in K is called the ring of integers of K and is denoted by $\mathcal{O}_K$.*

Remark 1.1.1 *Since $\mathbb{Q}$ is a field of characteristic 0, the primitive element the-*

orem for $\mathbb{Q}$ asserts that there exists an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

Let $n \geq 1$ be an integer and let K be a number field with $[K : \mathbb{Q}] = n$. It is a well-known result in algebraic number theory that $\mathcal{O}_K$ is a Dedekind domain. In other words, $\mathcal{O}_K$ is Noetherian, integrally closed and every non-zero prime ideal is maximal. Moreover, every non-zero ideal in $\mathcal{O}_K$ can be uniquely expressed as a product of prime ideals.

Definition 1.1.2 *A set $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_K$ is said to be an integral basis of K if every $\alpha \in \mathcal{O}_K$ can be uniquely expressed as $\alpha = \sum_{i=1}^{n} c_i \alpha_i$ with $c_i \in \mathbb{Z}$. Equivalently, $\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i$ as a $\mathbb{Z}$-module.*

Proposition 1.1.1 *An integral basis of K always exists. Consequently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

Remark 1.1.2 *For a square-free integer d, consider the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then it is well-known that*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z} \oplus \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

as a $\mathbb{Z}$-module.

Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$ with minimal polynomial f. Then f is an irreducible polynomial over $\mathbb{Q}$ of degree n. For a field homomorphism $\phi : K \to \mathbb{C}$, $\phi(\alpha)$ is also a root of f. Since $\mathbb{Q}$ is a field of characteristic 0, K is a separable extension of $\mathbb{Q}$ and hence $\phi(\alpha)$ has precisely n distinct choices. Therefore, there are n distinct embeddings, say $\sigma_1, \ldots, \sigma_{n-1}$ and σ_n, of K into $\mathbb{C}$. We say that K is a *Galois extension* of $\mathbb{Q}$ if all the roots of f lie in K. In that case, $\sigma_i(K) = K$ for all $i \in \{1, \ldots, n\}$ and the set $G = \{\sigma_1, \ldots, \sigma_n\}$ forms a group under the

law of composition of functions. We call G the *Galois group* of $K/\mathbb{Q}$ and is sometimes referred to as $Gal(K/\mathbb{Q})$.

We define the discriminant of K as follows.

Definition 1.1.3 *Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of K and let $\sigma_1, \ldots, \sigma_{n-1}$ and σ_n be all the distinct embeddings of K into $\mathbb{C}$. Then the discriminant of K, denoted by d_K, is defined by $d_K = det[\sigma_i(\alpha_j)]^2$.*

Remark 1.1.3 *Given two integral bases $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ of K, it can be shown that $det[\sigma_i(\alpha_j)]^2 = det[\sigma_i(\beta_j)]^2$. This makes the definition of d_K unambiguous. It is a well-known fact that for any positive real number X, the number of $K/\mathbb{Q}$ of degree n such that $d_K \leq X$ is finite.*

Remark 1.1.4 *For a square-free integer d, consider the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Then*

$$d_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Now, we describe the splitting of prime ideals in an extension of number fields. Let L be a number field containing K and let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Then there exist integers $g \geq 1$, $e_1, \ldots, e_g \geq 0$ and prime ideals $\wp_1, \ldots, \wp_g$ in $\mathcal{O}_L$ such that

$$\mathfrak{p}\mathcal{O}_L = \wp_1^{e_1} \ldots \wp_g^{e_g}.$$

The integer e_i is called the *ramification index* of $\wp_i$ over $\mathfrak{p}$. The prime ideal $\mathfrak{p}$ is said to be *unramified* in L (or $\mathcal{O}_L$) if $e_1 = \cdots = e_g = 1$.

Since $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains, $\mathfrak{p}$ and $\wp_i$ are maximal ideals in $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Thus $\mathcal{O}_L/\wp_i$ is a finite field containing the field $\mathcal{O}_K/\mathfrak{p}$. The degree $[\mathcal{O}_L/\wp_i : \mathcal{O}_K/\mathfrak{p}]$ is called the *residual degree* of $\wp_i$ over $\mathfrak{p}$ and is often

denoted by f_i. Moreover, the relation $[L : K] = \sum_{i=1}^{g} e_i f_i$ holds. If, in particular, L is a Galois extension over K, then all the ramification indices and residual degrees are equal.

We define a fractional ideal of K as follows.

Definition 1.1.4 *Let K be a number field and let M be an $\mathcal{O}_K$-module contained in K. Then M is said to be a fractional ideal of K if there exists a non-zero element $c \in \mathcal{O}_K$ such that $cM = \{cm : m \in M\} \subseteq \mathcal{O}_K$.*

Equivalently, the set of fractional ideals is the free abelian group generated by the set of prime ideals of $\mathcal{O}_K$. In this group, the set of principal fractional ideals forms a subgroup. We denote the group of fractional ideals of K by $\mathcal{F}(K)$ and the subgroup of principal fractional ideals by $\mathcal{P}(K)$.

Definition 1.1.5 *The quotient group $\mathcal{F}(K)/\mathcal{P}(K)$ is called the ideal class group (or, class group) of K and is denoted by Cl_K.*

It is known by Minkowski Theory that for any number field K, the class group Cl_K of K is a finite abelian group. The order of this group is known as the *class number* of K and is commonly denoted by h_K.

Proposition 1.1.2 *For a number field K, $\mathcal{O}_K$ is a principal ideal domain (in short, PID) if and only if $h_K = 1$.*

Proof. Suppose that $\mathcal{O}_K$ is a PID. Let M be a non-zero fractional ideal of K. Then by definition of a fractional ideal, there exists a non-zero element $c \in \mathcal{O}_K$ such that $cM \subseteq \mathcal{O}_K$. Since M is an $\mathcal{O}_K$-module, cM is an ideal in $\mathcal{O}_K$. By our assumption, $\mathcal{O}_K$ is a PID and hence $cM = \langle \beta \rangle$ for some $\beta \in \mathcal{O}_K$. Therefore, $M = \langle c^{-1}\beta \rangle$, which is principal. Since M is an arbitrary fractional ideal, we conclude that all the fractional ideals of K are principal. In other words, $\mathcal{F}(K) = \mathcal{P}(K)$ and hence $h_K = 1$.

Conversely, suppose that $h_K = 1$ and let I be a non-zero ideal in $\mathcal{O}_K$. Then I is an $\mathcal{O}_K$-module and therefore a fractional ideal of K. Now, $h_K = 1$ implies that I is a principal fractional ideal and hence $I = \langle \gamma \rangle$ for some $\gamma \in K$. Since $I \subseteq \mathcal{O}_K$, we have $\gamma \in \mathcal{O}_K$. As I is arbitrary, it follows that $\mathcal{O}_K$ is a PID. □

For a number field K, the non-zero prime ideals are usually called *finite primes*. A *real infinite prime* of K is an embedding $\sigma : K \to \mathbb{R}$ and a *complex infinite prime* is a pair of complex conjugate embeddings $\tau, \overline{\tau} : K \to \mathbb{C}$ with $\tau \neq \overline{\tau}$. Now, let L be a number field such that $K \subseteq L$. We say that an infinite prime σ of K is *ramified* in L if σ is real but it has an extension to L which is non-real. Otherwise, σ is said to be *unramified* in L. The extension L/K is called *unramified* if all the finite as well as the infinite primes of K are unramified in L.

Before going to the next section, we define the notion of an abelian as well as a cyclic extension of K and thereafter we introduce the Hilbert class field.

Definition 1.1.6 *Let L/K be an extension of number fields. We say that L is an abelian extension of K if L/K is Galois and the Galois group $Gal(L/K)$ is abelian. The extension L/K is said to be a cyclic extension if L/K is Galois and the Galois group $Gal(L/K)$ is cyclic.*

Proposition 1.1.3 *Let K be a number field. Then there exists a unique maximal abelian, unramified extension field $H(K)$ of K. It also satisfies the following isomorphism of groups*

$$Gal(H(K)/K) \simeq Cl_K.$$

Definition 1.1.7 *The number field $H(K)$ in Proposition 1.1.3 is said to be the Hilbert class field of K.*

From Proposition 1.1.3, the following proposition readily follows.

Proposition 1.1.4 *Let L be a Galois extension over a number field K with Galois group G. Assume that G is abelian and L/K is unramified. Then $[L : K] \mid h_K$.*

Proof. Since L is an unramified and abelian extension of K, it is contained in the Hilbert class field $H(K)$ of K. That is, $K \subseteq L \subseteq H(K)$. Thus $[L : K]$ divides $[H(K) : K]$. Now, by Proposition 1.1.3, we have $[H(K) : K] = |Gal(H(K)/K)| = h_K$. Hence $[L : K] \mid h_K$. □

1.2 Recent developments and main result

By Proposition 1.1.2, we know that $h_K = 1$ is equivalent to the fact that $\mathcal{O}_K$ is a PID. Since it is desirable to work in a ring which is a PID, it is useful to have information about K for which $h_K = 1$. Gauss raised the question for a complete characterization of imaginary quadratic fields of class number 1. Heegner [20], Baker [3] and Stark [48] resolved this problem and proved the following theorem.

Theorem 1.2.1 *Let $d > 0$ be a square-free integer. Then the quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 precisely for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.*

In 1934, Heilbronn [21] proved that given any integer $m \geq 1$, there exist only finitely many imaginary quadratic fields, each having class number m. However, the analogous question for real quadratic fields still remains unsolved. This is popularly known as the "Gauss class number 1 problem" and is stated as follows.

Conjecture 1.2.2 *There exist infinitely many real quadratic fields of class number 1.*

In the light of Conjecture 1.2.2, it is very difficult to characterize number fields of a given class number. Hence we address the following weaker question about the divisibility of class numbers of number fields.

Question 1.2.3 *Given an integer $n \geq 1$, do there exist infinitely many number fields having class number divisible by n?*

Since, in this chapter, we intend to discuss the class number divisibility problem only for quadratic fields, we furnish some of the relevant results associated to quadratic fields. Nagell [42], Ankeny and Chowla [1] and later many others answered Question 1.2.3 affirmatively for imaginary quadratic fields and proved the following.

Theorem 1.2.4 *([1] and [42]) Let $n \geq 2$ be an integer. Then there exist infinitely many imaginary quadratic fields K with $n \mid h_K$.*

Later, Weinberger [50], Yamamoto [52] and several other mathematicians proved the same divisibility result for real quadratic fields as follows.

Theorem 1.2.5 *([50] and [52]) Let $n \geq 2$ be an integer. Then there exist infinitely many real quadratic fields K with $n \mid h_K$.*

We note that Theorem 1.2.4 and 1.2.5 are of qualitative nature. In the literature, quantitative questions related to this have also been addressed. For that, we introduce the following sets. For an integer $g \geq 2$ and a large positive real number X, let

$$N_g^+(X) = \#\{K = \mathbb{Q}(\sqrt{d}) : d > 0 \text{ is square-free, } |d_K| \leq X \text{ and } g \mid h_K\}$$

and

$$N_g^-(X) = \#\{K = \mathbb{Q}(\sqrt{d}) : d < 0 \text{ is square-free, } |d_K| \leq X \text{ and } g \mid h_K\}.$$

Then one can naturally ask about the growth of $N_g^+(X)$ and $N_g^+(X)$ as $X \to \infty$. It is widely believed that for each integer $g \geq 2$, there exist positive constants

C_g^+ and C_g^- such that $N_g^+(X) \sim C_g^+ X$ and $N_g^-(X) \sim C_g^- X$. Here the symbol " $\sim$ " indicates that $\lim_{X\to\infty} \frac{N_g^+(X)}{X} = C_g^+$ and $\lim_{X\to\infty} \frac{N_g^-(X)}{X} = C_g^-$.

We first study the case $g = 2$ for imaginary quadratic fields. For that, we need to use the prime number theorem along with the following theorem that follows from Gauss's theory of genera. The proofs can be found in [2] and [13].

Theorem 1.2.6 *(Prime number theorem) For a positive real number X, let $\pi(X) = \{p \leq X : p \text{ is prime}\}$. Then $\lim_{X\to\infty} \frac{\pi(X)\log X}{X} = 1$.*

Theorem 1.2.7 *(Gauss) Let $d \geq 2$ be a square-free integer and let $p_1, \ldots, p_{t-1}$ and p_t be the distinct prime divisors of d. Let $K_1 = \mathbb{Q}(\sqrt{d})$ and $K_2 = \mathbb{Q}(\sqrt{-d})$. Then $2^{t-2} \mid h_{K_1}$ and $2^{t-1} \mid h_{K_2}$.*

Theorem 1.2.8 *Following the same notations defined above, we have $C_2^- = \frac{6}{\pi^2}$.*

Proof. For a natural number n, let $\omega(n)$ denote the number of distinct prime divisors of n. Now, for a large positive real number X, let

$$A(X) = \{n \in \mathbb{N} : n \leq X \text{ and } n \text{ is square-free}\}$$

and

$$A_2(X) = \{n \in A(X) : \omega(n) \geq 2\}.$$

Then clearly, $A(X) \setminus A_2(X) = \{n \in \mathbb{N} : n \leq X \text{ and } n \text{ is prime }\} = \pi(X)$. Consequently, $A(X) = A_2(X) \cup \pi(X)$ and $A_2(X) \cap \pi(X) = \emptyset$.

It is a well-known theorem (cf. [2]) in analytic number theory that $\lim_{X\to\infty} \frac{A(X)}{X}$ exists and equals $\frac{6}{\pi^2}$. Also, from Theorem 1.2.6, we get $\lim_{X\to\infty} \frac{\pi(X)}{X} = 0$. There-

fore, we have

$$\lim_{X\to\infty}\frac{A_2(X)}{X}=\lim_{X\to\infty}\frac{A_2(X)}{X}+\lim_{X\to\infty}\frac{\pi(X)}{X}=\lim_{X\to\infty}\frac{A(X)}{X}=\frac{6}{\pi^2}. \tag{1.1}$$

Now, let $d\in A_2$ and let $K=\mathbb{Q}(\sqrt{-d})$. Then by Theorem 1.2.7, we have $2\mid h_K$. It follows from (1.1) that almost all square-free integers n satisfies $\omega(n)\geq 2$ and therefore we obtain $C_2^-=\dfrac{6}{\pi^2}$. □

The growth results of $N_g^+(X)$ and $N_g^-(X)$ are not so regular for integers $g\geq 3$. In fact, when g is an odd prime number, there is a famous conjecture by Cohen and Lenstra [12] regarding the values of C_g^+ and C_g^-. We state this as follows.

Conjecture 1.2.9 *(Cohen-Lenstra heuristics) Let $p\geq 3$ be an odd prime number. Then*

$$C_p^-=\frac{6}{\pi^2}\left(1-\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)\right) \tag{1.2}$$

and

$$C_p^+=\frac{6}{\pi^2}\left(1-\prod_{i=2}^{\infty}\left(1-\frac{1}{p^i}\right)\right). \tag{1.3}$$

Even though the precise values of C_p^+ and C_p^- are unknown for any integer $g\geq 3$, some lower bounds of $N_p^+(X)$ and $N_p^-(X)$ are known due to the works of Byeon [5], Murty [44] and Soundararajan [47]. Before providing their results, we recall the following standard notations.

Notations. Let $\mathcal{S}\subseteq\mathbb{R}_{>0}$ be a non-empty, infinite set and let f and g be two real-valued functions on $\mathcal{S}$ with $g(s)>0$ for all $s\in\mathcal{S}$. We say that $f\ll g$ (respectively, $g\gg f$) if there is an absolute constant $C>0$ such that $|f(s)|\leq Cg(s)$ (respectively, $g(s)\geq C|f(s)|$) for all $s\in\mathcal{S}$. Sometimes we use the notation $f=O(g)$ to mean $f\ll g$. We write $f\asymp g$ if both $f\ll g$ and

$g \ll f$ hold simultaneously. Also, by $f = o(g)$, we mean $\frac{f(s)}{g(s)} \to 0$ as $s \to \infty$.

Now we state the results concerning the lower bounds of $N_p^+(X)$ and $N_p^-(X)$ as follows.

Theorem 1.2.10 *[5]* $N_5^+(X) \gg X^{\frac{1}{2}}$ *and* $N_7^+(X) \gg X^{\frac{1}{2}}$.

Theorem 1.2.11 *[44] Let* $g \geq 3$ *be an integer and* $\epsilon > 0$ *be a real number. Then we have*

$$N_g^-(X) \gg X^{\frac{1}{2}+\frac{1}{g}}$$

and

$$N_g^+(X) \gg \begin{cases} X^{\frac{1}{2g}-\epsilon} & \text{if } g \text{ is odd}, \\ X^{\frac{1}{2g}-\epsilon} & \text{if } g \equiv 2 \pmod 4, \\ X^{\frac{1}{4g}-\epsilon} & \text{if } g \equiv 0 \pmod 4. \end{cases}$$

Later, Soundararajan [47] improved the lower bound in Theorem 1.2.11 for imaginary quadratic fields as follows.

Theorem 1.2.12 *[47] For an even integer* $g \geq 4$ *and any* $\epsilon > 0$, *we have*

$$N_g^-(X) \gg \begin{cases} X^{\frac{1}{2}+\frac{2}{g}-\epsilon} & \text{if } g \equiv 0 \pmod 4, \\ X^{\frac{1}{2}+\frac{3}{2g+2}-\epsilon} & \text{if } g \equiv 2 \pmod 4. \end{cases}$$

For any integer $g \geq 3$, since $2g \mid h_K$ implies $g \mid h_K$, we get $N_g^-(X) \geq N_{2g}^-(X)$. Therefore, by Theorem 1.2.12, we obtain the following theorem.

Theorem 1.2.13 *[47] For an odd integer* $g \geq 3$ *and any* $\epsilon > 0$, *we have*

$$N_g^-(X) \gg X^{\frac{1}{2}+\frac{3}{4g+2}-\epsilon}.$$

Now, we state the main result of this chapter.

Theorem 1.2.14 *[8] Let $\ell \geq 1$ be an integer and let $p_1, \ldots, p_{\ell+1}$ and $p_{\ell+2}$ be distinct prime numbers with $p_i \geq 5$ for all $i \in \{1, \ldots, \ell+2\}$. For a positive real number X, let*

$$N_{3,\ell}(X) = \#\{K = \mathbb{Q}(\sqrt{d}) : d > 0 \text{ is square-free, } d_K \leq X, p_1 \ldots p_{\ell+2} \mid d_K \text{ and } 3 \mid h_K\}.$$

Then for all sufficiently large real numbers X, we have $N_{3,\ell}(X) \gg X^{\frac{7}{8}}$.

Theorem 1.2.14 and Theorem 1.2.7 immediately give the following corollary.

Corollary 1.2.15 *For a positive integer ℓ and for all sufficiently large positive real numbers X, we have*

$$N^{+}_{2^{\ell}.3}(X) \gg X^{\frac{7}{8}}.$$

1.3 Preliminaries

Kishi and Miyake [32] characterized the quadratic fields K with class number divisible by 3 as follows.

Lemma 1.3.1 *[32] Let u and w be integers such that $\gcd(u, w) = 1$ and $d = 4uw^3 - 27u^2$ is not a perfect square in $\mathbb{Z}$. Let $g(T) = T^3 - uwT - u^2 \in \mathbb{Z}[T]$. Suppose that one of the following conditions holds:*

(i) $3 \nmid w$,

(ii) $3 \mid w, uw \not\equiv 3 \pmod 9$, *and* $u \equiv w \pm 1 \pmod 9$,

(iii) $3 \mid w, uw \equiv 3 \pmod 9$, *and* $u \equiv w \pm 1 \pmod{27}$.

If $g(T)$ is irreducible over $\mathbb{Q}$, then the roots of the polynomial $g(T)$ generate an unramified cyclic cubic extension F over $K := \mathbb{Q}(\sqrt{d})$ (which, in turn, by Proposition 1.1.3 implies that $3 \mid h_K$).

Conversely, suppose K is a quadratic field over $\mathbb{Q}$ with $3 \mid h_K$. If F is an unramified cyclic cubic extension over K, then F is obtained by adjoining the roots of $g(T)$ (as defined above) with K for some suitable choices of u and w.

Using Lemma 1.3.1, Byeon and Koh [6] constructed a family of quadratic fields, each having class number divisible by 3. More precisely, they proved the following.

Lemma 1.3.2 *[6] Let m and n be two positive integers with $\gcd(m, n) = 1$, $m \equiv 1 \pmod{18}$ and $n \equiv 1 \pmod{54}$. Let $f(T) = T^3 - 3mT - 2n \in \mathbb{Z}[T]$. If f is irreducible over $\mathbb{Q}$, then the class number of the quadratic field $\mathbb{Q}(\sqrt{3(m^3 - n^2)})$ is divisible by 3.*

We state some results regarding the number of square-free integer solutions of a Diophantine equation which are proved in [47].

Lemma 1.3.3 *[47] Let X be a large positive real number and let $T = X^{\frac{1}{16}}$. Also, let $M = \frac{T^{\frac{2}{3}} X^{\frac{1}{3}}}{2}$ and $N = \frac{TX^{\frac{1}{2}}}{2^4}$. Let $N_1(X)$ stand for the number of triples (m, n, t) of positive integers satisfying $m^3 - n^2 = t^2 d$ with $d \leq X$, $T < t \leq 2T$, $M < m \leq 2M$, $N < n \leq 2N$, $\gcd(m, t) = \gcd(m, n) = \gcd(t, 6) = 1$, $m \equiv 1 \pmod{18}$ and $n \equiv 2 \pmod{18}$ and $p^2 \nmid d$ for all prime numbers $p \leq \log X$. Then*

$$N_1(X) \asymp \frac{MN}{T} + o(MX^{\frac{1}{3}} T^{\frac{2}{3}}).$$

Lemma 1.3.4 *[47] For a non-zero integer ℓ and for a fixed natural number m, let $\rho_m(\ell)$ denote the number of solutions to the congruence $n^2 \equiv m^3 \pmod{\ell}$. Then*

(i) ρ_m *is a multiplicative function.*

(ii) Assume m, M, n, N, t, T *and* d *as in Lemma 1.3.3. Then*

$$\sum_{\substack{M\le m\le 2M\\ m\equiv 1 \pmod{18}}} \sum_{\substack{T\le t\le 2T\\ \gcd(t,6m)=1}} \rho_m(t^2) \asymp MT.$$

Lemma 1.3.5 *Let* m *and* n *be integers such that* $m \equiv 19 \pmod{18\cdot 6}$ *and* $n \equiv 55 \pmod{54\cdot 6}$. *Then* 4 *and* 243 *do not divide* $m^3 - n^2$.

Proof. By $m \equiv 19 \pmod{18\cdot 6}$ and $n \equiv 55 \pmod{54\cdot 6}$, we conclude that $m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$. Hence $m^3 - n^2 \equiv 2 \pmod 4$ which shows that $4 \nmid (m^3 - n^2)$.

Again, from $m \equiv 19 \pmod{18\cdot 6}$ and $n \equiv 55 \pmod{54\cdot 6}$, we get $m \equiv 19 \pmod{27}$ and $n \equiv 55 \pmod{81}$. Therefore, $m \equiv 27a + 19 \pmod{243}$ and $n \equiv 81b + 55 \pmod{243}$ for some $0 \le a \le 8$ and $0 \le b \le 2$. If $m^3 - n^2 \equiv 0 \pmod{243}$, then we have

$$\begin{aligned} 0 \equiv m^3 - n^2 &\equiv (27a+19)^3 - (81b+55)^2 \pmod{243}\\ &\equiv 189 + 81(361a - 110b) \pmod{243}\\ &\equiv 3^3\cdot 7 + 3^4(118a - 110b) \pmod{243} \end{aligned}$$

which implies that $7 + 3(118a - 110b) \equiv 0 \pmod 9$. Since the right hand side is $0 \pmod 3$ but the left hand side is $1 \pmod 3$, this is impossible for any choice of integers a and b. This proves the lemma. □

For a large positive real number X, our aim is to find a lower bound for the number of real quadratic fields of the form $\mathbb{Q}(\sqrt{3(m^3-n^2)})$ and discriminant $\le X$, where m and n are positive integers belonging to certain arithmetic progressions. Then by using Lemma 1.3.2, we get a lower bound for the number of

such real quadratic fields K with $d_K \leq X$ and $h_K \equiv 0 \pmod 3$. In order to do that, we first define the quantities $N_2(X), N_3(X), R'(X), N'(X)$ and $N(X)$ as follows.

For a large positive real number X, let $T = X^{\frac{1}{16}}$, $M = \frac{T^{\frac{2}{3}}X^{\frac{1}{3}}}{2}$, $N = \frac{TX^{\frac{1}{2}}}{2^4}$ and $Z = \frac{X^{\frac{1}{3}}(\log X)^{\frac{2}{3}}}{T^{\frac{1}{3}}}$. Let $N_2(X)$ (respectively, $N_3(X)$) denote the number of triples (m, n, t) of positive integers such that the equation

$$m^3 - n^2 = 27t^2d \tag{1.4}$$

holds with $d \leq X$, $T < t \leq 2T, M < m \leq 2M, N < n \leq 2N, gcd(m, t) = gcd(m, n) = gcd(t, 6) = 1, m \equiv 19 \pmod{18\cdot 6}, n \equiv 55 \pmod{54\cdot 6}$ and $p^2 \mid d$ for at least one p with $\log X < p \leq Z$ (respectively, $p > Z$). Let $R'(X)$ denote the number of triples (m, n, t) of positive integers satisfying the equation (1.4) with m, M, n, N, t, T and d as above and $p^2 \nmid d$ for all prime numbers $p \leq \log X$. Also, let $N'(X)$ denote the number of triples (m, n, t) of positive integers in the above range satisfying equation (1.4) and d is square-free. Lastly, let $N(X)$ denote the number of positive square-free integers $d \leq X$ with at least one integer solution to the equation (1.4) with m, M, n, N, t, T and d as above. Towards the end of this section, we prove that $N(X) \gg X^{\frac{7}{8}}$.

The next lemma is obtained by a slight modification in the arguments given by Soundararajan in [47] and was used in [6]. Since the proof is not available as such, except quoted, we give a proof for the sake of completeness.

Lemma 1.3.6 *With $N_2(X)$ defined as above, we have*

$$N_2(X) \ll \frac{MN}{T(\log X)^2} + o(MX^{\frac{1}{3}}T^{\frac{2}{3}}).$$

Proof. Let m and t be fixed integers in the given range and let

$$N_2'(X) = \sum_{\log X \le p \le Z} \sum_{\substack{N \le n \le 2N \\ n \equiv 55 \pmod{54\cdot 6} \\ n^2 \equiv m^3 \pmod{27t^2p^2}}} 1. \tag{1.5}$$

We split the above sum into intervals of size $54 \cdot 6 \cdot t^2p^2$ to get

$$\sum_{\substack{N \le n \le 2N \\ n \equiv 55 \pmod{54\cdot 6} \\ n^2 \equiv m^3 \pmod{27t^2p^2}}} 1 = \frac{N}{54 \cdot 6} \cdot \frac{\rho_m(27t^2p^2)}{t^2p^2} + O(\rho_m(27t^2)).$$

Using $\rho_m(27p^2) = O(1)$, the equation (1.5) becomes

$$N_2'(X) \ll \sum_{\log X \le p \le Z} \left(\frac{N \cdot \rho_m(27t^2p^2)}{t^2p^2} + O(\rho_m(27t^2)) \right). \tag{1.6}$$

Now, we have $\rho_m(27t^2p^2) \le \rho_m(t^2) \cdot \rho_m(27p^2)$. Also, using $t > T$, the bound for $N_2'(X)$ in (1.6) becomes

$$N_2'(X) \ll \frac{N}{T^2} \cdot \frac{\rho_m(t^2)}{(\log X)^2} + o\left(\frac{X^{\frac{1}{3}} \rho_m(t^2)}{T^{\frac{1}{3}}} \right).$$

Consequently, using Lemma 1.3.4, we obtain

$$N_2(X) = \sum_{\substack{M \le m \le 2M \\ m \equiv 19 \pmod{18\cdot 6}}} \sum_{\substack{T \le t \le 2T \\ \gcd(t, 6m) = 1}} N_2'(X) \ll \frac{MN}{T(\log X)^2} + o(MX^{\frac{1}{3}}T^{\frac{2}{3}}).$$

□

The proof of the next lemma follows *ad verbatim* along the same line of argument given in [47] and thus we omit it.

Lemma 1.3.7 *We have*

$$N_3(X) = o(MX^{\frac{1}{3}}T^{\frac{2}{3}}).$$

Lemma 1.3.8 *[6] We have*

$$R'(X) \asymp \frac{MN}{T} + o(MX^{\frac{1}{3}}T^{\frac{2}{3}}) \gg X^{\frac{7}{8}}.$$

Proof. By the hypotheses, $m \equiv 1 \pmod{18}$ and hence by Lemma 1.3.4,

$$\sum_{\substack{M\le m\le 2M\\ m\equiv 1 \pmod{18}}} \sum_{\substack{T\le t\le 2T\\ \gcd(t,6m)=1}} \rho_m(t^2) \asymp MT$$

holds.

Let m and t be fixed integers in the given range. Then by Lemma 1.3.5, for any $n \equiv 55 \pmod{54\cdot 6}$, we have $4 \nmid \frac{m^3-n^2}{27t^2}$ and $9 \nmid \frac{m^3-n^2}{27t^2}$. Let $P = \prod_{5\le p\le \log X} p$. For a fixed m and t in the given range, let $R(X)$ denote the number of integers n with $N \le n \le 2N$, $n \equiv 55 \pmod{54\cdot 6}$, $\gcd(m,n) = 1$ and $p^2 \nmid \frac{m^3-n^2}{27t^2}$ for all prime number $p \le \log X$. Then

$$\begin{aligned} R(X) &= \sum_{\substack{N\le n\le 2N\\ \gcd(m,n)=1\\ n\equiv 55 \pmod{54\cdot 6}\\ n^2\equiv m^3 \pmod{27t^2}}} \sum_{l^2\mid \gcd(\frac{m^3-n^2}{27t^2}, P^2)} \mu(l) \\ &= \sum_{\substack{l\mid P\\ \gcd(l,m)=1}} \mu(l) \sum_{\substack{N\le n\le 2N\\ n\equiv 55 \pmod{54\cdot 6}\\ n^2\equiv m^3 \pmod{27l^2t^2}}} 1 \\ &= \sum_{\substack{l\mid P\\ \gcd(l,m)=1}} \mu(l)\left(\frac{N}{54\cdot 6}\cdot\frac{\rho_m(27t^2l^2)}{t^2l^2} + O(X^{\epsilon})\right) (\text{by definition of } \rho_m(27l^2t^2)\ ) \end{aligned}$$

$$= \frac{N\rho_m(27t^2)}{54\cdot 6\cdot t^2}\sum_{\substack{l|P\\ \gcd(l,m)=1}}\frac{\mu(l)}{l^2}\rho_m\left(\frac{l}{\gcd(t,l)}\right)+O(X^\epsilon) \qquad \text{(Since}$$

$$\gcd\left(27t^2,\frac{l}{\gcd(t,l)}\right)=1)$$

$$= \frac{N\rho_m(27t^2)}{54\cdot 6\cdot t^2}\prod_{\substack{p|P\\ p\nmid m}}\left(1-\frac{\rho_m(\frac{p}{\gcd(t,p)})}{p^2}\right)+O(X^\epsilon)$$

$$\asymp \frac{N}{T^2}\rho_m(t^2)+O(X^\epsilon).$$

Now, using Lemma 1.3.4, if we sum over all m and t satisfying the hypotheses, then we obtain

$$\begin{aligned} R'(X) &\asymp \frac{N}{T^2}\sum_{\substack{M\le m\le 2M\\ m\equiv 1 \pmod{18}}}\sum_{\substack{T\le t\le 2T\\ \gcd(t,6m)=1}}\rho_m(t^2)+O(MTX^\epsilon)\\ &\asymp \frac{N}{T^2}\cdot MT+O(MTX^\epsilon)\\ &\asymp \frac{MN}{T}+o(MX^{\frac{1}{3}}T^{\frac{2}{3}})\gg X^{\frac{7}{8}}. \end{aligned}$$

□

Remark 1.3.1 *The proofs of Lemma 1.3.6 and Lemma 1.3.8 reveal that the same estimates hold irrespective of the congruence class of n modulo $54\cdot 6$.*

Lemma 1.3.9 *We have*

$$N'(X)\gg X^{\frac{7}{8}}.$$

Proof. We have $N'(X)=R'(X)-(N_2(X)+N_3(X))$. Now, by using Lemma 1.3.6, Lemma 1.3.7 and Lemma 1.3.8 and using the bounds for $R'(X)$, $N_2(X)$ and $N_3(X)$, we get $N'(X)\gg X^{\frac{7}{8}}$. □

Before we prove the lower bound for $N(X)$, we quote the following lemma, whose proof follows the exact same line of argument as given in [47].

Lemma 1.3.10 *[47] For a positive square-free integer $d \leq X$, let $N'(d)$ be the number of triples (m, n, t) of positive integers with $T < t \leq 2T, M < m \leq 2M, N < n \leq 2N, gcd(m, t) = gcd(m, n) = gcd(t, 6) = 1, m \equiv 19 \pmod{18 \cdot 6}, n \equiv 55 \pmod{54 \cdot 6}$ and $m^3 - n^2 = 27t^2d$. Then*

$$\sum_{d \leq X} N'(d)(N'(d) - 1) \ll T^{\frac{10}{3}} X^{\frac{2}{3}+\epsilon}.$$

Remark 1.3.2 *Note that, in our notations, we have $\sum_{d \leq X} N'(d) = N'(X)$.*

Lemma 1.3.11 *We have*

$$N(X) \gg X^{\frac{7}{8}}.$$

Proof. By definition, $N(X)$ denotes the number of square-free positive integers $d \leq X$ for which the equation $m^3 - n^2 = 27t^2d$ admits a solution. We define a characteristic function as follows.

$$N(d) = \begin{cases} 1 & \text{if } 0 \leq d \leq X \text{ is square-free and } m^3 - n^2 = 27t^2d \text{ has a solution,} \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, $\sum_{d \leq X} N(d) = N(X)$. Also, for a square-free positive integer $d \leq X$, we have $N(d) = 0$ if and only if $N'(d) = 0$.

Therefore, using the Cauchy-Schwarz inequality, we have

$$\left(\sum_{d \leq X} (N'(d) \cdot N(d)) \right)^2 \leq \left(\sum_{d \leq X} N'(d)^2 \right) \cdot \left(\sum_{d \leq X} N(d)^2 \right).$$

Since for any square-free d, we have $N(d) = 0$ or 1, we get $\sum_{d \leq X} N(d) = \sum_{d \leq X} N(d)^2 =$

$N(X)$ and hence we obtain

$$\left(\sum_{d\leq X} N'(d)\right)^2 \leq \left(\sum_{d\leq X} N'(d)^2\right)\cdot(N(X))\,.$$

That is, $N(X) \geq \left(\sum_{d\leq X} N'(d)\right)^2 \cdot \left(\sum_{d\leq X} N'(d)^2\right)^{-1}$. Now, from Lemma 1.3.10, we get

$$\sum_{d\leq X} N'(d)^2 = N'(X) + \sum_{d\leq X} N'(d)(N'(d)-1).$$

Therefore, by using Lemma 1.3.9 and Lemma 1.3.10, we get $N(X) \gg X^{\frac{7}{8}}$. □

The next lemma is proved in [7].

Lemma 1.3.12 *[7] Let M and N be two positive real numbers. Let*

$$\mathcal{S} = \big\{f(T) = T^3 + mT + n \in \mathbb{Z}[T] \ : \ |m| \leq M, |n| \leq N, f(T) \text{ is irreducible over } \mathbb{Q} \text{ and } D(f) = -(4m^3+27n^2) \text{ is not a perfect square}\big\}$$

be a subset of $\mathbb{Z}[T]$. Then $\#\mathcal{S} \gg MN$.

1.4 Proof of Theorem 1.2.14

Let $\ell \geq 1$ be an integer and let $p_1, \ldots, p_{\ell+2}$ be distinct prime numbers with $p_i \geq 5$ for each i. For each $i \in \{1, \ldots, \ell+2\}$, we choose integers a_i and b_i such that $3a_i - 2b_i \not\equiv 0 \pmod{p_i}$. Now we consider the following set of simultaneous congruences:

$$\begin{aligned} X &\equiv 19 \pmod{18\cdot 6} \\ X &\equiv 1 + a_1 p_1 \pmod{p_1^2} \\ &\vdots \end{aligned}$$

$$X \equiv 1 + a_{\ell+2}p_{\ell+2} \pmod{p_{\ell+2}^2}.$$

Since each $p_i \geq 5$, the modulii are pairwise relatively prime. Hence by the Chinese remainder theorem, there exists a unique integer $m \pmod{18 \cdot 6\prod_{i=1}^{\ell+2} p_i^2}$ satisfying the above set of congruences. In other words, the number of such integers $m \leq X$ is $((1+o(1))\, X/\left(18 \cdot 6\prod_{i=1}^{l+2} p_i^2\right)$ as $X \to \infty$. We denote by $M_1(X)$ the set of all such integers $m \leq X$.

Similarly, we consider the following set of congruences.

$$\begin{aligned} X &\equiv 55 \pmod{54 \cdot 6} \\ X &\equiv 1 + b_1 p_1 \pmod{p_1^2} \\ &\vdots \\ X &\equiv 1 + b_{\ell+2}p_{\ell+2} \pmod{p_{\ell+2}^2}. \end{aligned}$$

Again the Chinese remainder theorem implies that the number of integers $n \leq X$ satisfying the above set of congruences is $((1+o(1))\, X/\left(54 \cdot 6\prod_{i=1}^{\ell+2} p_i^2\right)$ integers $n \leq X$ as $X \to \infty$. Let $M_2(X)$ stand for all such integers $n \leq X$.

Now, let X be a large positive real number and let $T = X^{\frac{1}{16}}$, $M = \frac{T^{\frac{2}{3}}X^{\frac{1}{3}}}{2}$ and $N = \frac{TX^{\frac{1}{2}}}{2^4}$. Let $M(X)$ be the number of square-free positive integers $d \leq X$ with at least one solution to the equation

$$m^3 - n^2 = 27t^2 d, \tag{1.7}$$

where $T < t \leq 2T$, $M < m \leq 2M$, $N < n \leq 2N$, $\gcd(m,t) = \gcd(m,n) = \gcd(t,6) = 1$, $m \in M_1(X)$ and $n \in M_2(X)$. Therefore, by Lemma 1.3.11, we get $M(X) \gg X^{7/8}$.

Now, for each $i \in \{1, \ldots, \ell+2\}$, for integers $m \in M_1(X)$ and $n \in M_2(X)$,

we have

$$m^3-n^2=(a_ip_i+1)^3-(b_ip_i+1)^2\equiv 3a_ip_i+1-2b_ip_i-1\equiv p_i(3a_i-2b_i) \pmod{p_i^2} \tag{1.8}$$

By the choice of the integers a_i and b_i, we have $m^3-n^2\equiv 0 \pmod{p_i}$ but $m^3-n^2\not\equiv 0 \pmod{p_i^2}$, for each $i\in\{1,\dots,\ell+2\}$. Therefore, each p_i divides the square-free part of $m^3-n^2=27t^2d$, which is $3d$. Since $p_i\geq 5$, we conclude that $p_i\mid d$. Hence $p_1\dots p_{\ell+2}\mid d$ for all such d satisfying (1.7).

For a square-free integer d satisfying (1.7), let $K=\mathbb{Q}(\sqrt{d})$. Then by Lemma 1.3.12, the number of polynomials $f(T)=T^3-3mT-2n\in\mathbb{Z}[T]$ with (m,n,t) satisfying (1.7) is $\gg X^{\frac{7}{8}}$. For such a polynomial f, the discriminant $D(f)$ is $-(-3m)^3-27(-2n)^2=2^2\cdot 3^3\cdot(m^3-n^2)$ and hence

$$\mathbb{Q}(\sqrt{D(f)})=\mathbb{Q}(\sqrt{3(m^3-n^2)})=\mathbb{Q}(\sqrt{3\cdot 27t^2d})=\mathbb{Q}(\sqrt{d}).$$

By Lemma 1.3.2, the class number of $\mathbb{Q}(\sqrt{d})$ is divisible by 3. Hence, the number real quadratic fields $K=\mathbb{Q}(\sqrt{d})$ with $|d_K|\leq X$, $p_1\dots p_{\ell+2}\mid d_K$ and $3\mid h_K$ is $\gg X^{\frac{7}{8}}$. In other words, $N_{3,\ell}(X)\gg X^{\frac{7}{8}}$ and this completes the proof. □

CHAPTER 2

Simultaneous divisibility of class numbers of triples of imaginary quadratic fields

For a cube-free integer $k \geq 1$ *with* $k \equiv 1 \pmod 9$ *and* $\gcd(k, 7 \cdot 571) = 1$, *we prove the existence of infinitely many triples of imaginary quadratic fields* $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1})$ *and* $\mathbb{Q}(\sqrt{d+k^2})$ *with* $d \in \mathbb{Z}$ *such that the class number of each of them is divisible by* 3.

2.1 Introduction

In Chapter 1, we dealt with the problem of the divisibility of class numbers of real quadratic fields. It is equally interesting to consider multiple quadratic fields and study the divisibility properties of their class numbers.

For a prime number p, we begin with the p-rank of a finite abelian group.

Definition 2.1.1 *[28] Let G be a finite abelian group, written additively, and let p be a prime number. Then G/pG is a finite-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$ and the dimension is called the p-rank of G.*

Remark 2.1.1 *The p-rank of a finite abelian group G is often denoted by $rk_p(G)$.*

For a given number field K, one of the most important finite abelian groups associated to K is the ideal class group Cl_K. Hence it is useful to study the p-ranks of Cl_K. From Definition 2.1.1, it immediately follows that if $rk_p(Cl_K) \geq 1$, then $p \mid h_K$.

Number theorists have studied $rk_p(Cl_K)$ for some particular prime p. When $p = 3$, Scholz [45] proved a *reflection principle* for the 3-ranks of the class groups of quadratic fields as follows.

Theorem 2.1.1 *[45] Let $d > 1$ be a square-free integer. Let r and s be the 3-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$, respectively. Then*

$$r \leq s \leq r + 1.$$

From Theorem 2.1.1, we can see that if 3 divides $h_{\mathbb{Q}(\sqrt{d})}$, then 3 also divides $h_{\mathbb{Q}(\sqrt{-3d})}$.

Now, for a square-free integer $d > 1$, let r' be the 3-rank of the real quadratic field $\mathbb{Q}(\sqrt{3d})$ and let s' be the 3-rank of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3d}) = \mathbb{Q}(\sqrt{-d})$. Then from Theorem 2.1.1, we get that $r' \leq s' \leq r' + 1$. In [31], Kishi characterized all quadratic fields for which $s' = r' + 1$ as follows.

Theorem 2.1.2 *[31] Let $d > 1$ be a square-free integer with $3 \nmid d$. Let r' and s' be the 3-ranks of the quadratic fields $\mathbb{Q}(\sqrt{3d})$ and $\mathbb{Q}(\sqrt{-3 \cdot 3d}) = \mathbb{Q}(\sqrt{-d})$, respectively. Then the following statements are equivalent.*

(a) $s' = r' + 1$.

(b) *There does not exist a cubic field K satisfying the following three conditions:*

  (i) *$K/\mathbb{Q}$ is not Galois.*

  (ii) *The Galois closure $\overline{K}$ of K contains $\mathbb{Q}(\sqrt{-d})$ and $\overline{K}/\mathbb{Q}(\sqrt{-d})$ is a cyclic cubic extension which is unramified at all rational primes $q \neq 3$.*

  (iii) *The discriminant D_K of K is divisible by 3^4 but not by 3^5.*

(c) *There exists a cubic field L satisfying the following three conditions:*

  (i) *L is not Galois over $\mathbb{Q}$.*

  (ii) *The Galois closure $\overline{L}$ of L contains $\mathbb{Q}(\sqrt{3d})$ and $\overline{L}/\mathbb{Q}(\sqrt{3d})$ is a cyclic cubic extension which is unramified at all rational primes $q \neq 3$.*

  (iii) *The discriminant D_L of L is divisible by 3^3 but not by 3^4.*

(d) *There does not exist a triple $(u, v, m) \in \mathbb{Z}^3$ with $uvm \neq 0$ satisfying the following three conditions:*

  (i) $3v^2d = u^2 - 4m^3$.

  (ii) $\gcd(u, m) = 1$.

  (iii) $m \equiv 1 \pmod 3$ *and* $u^2 \equiv 1, 7 \pmod 9$.

(e) *There exists a triple $(u, v, m) \in \mathbb{Z}^3$ with $uvm \neq 0$ satisfying the following three conditions:*

  (i) $-v^2d = u^2 - 4m^3$.

  (ii) $\gcd(u, m) = 1$.

  (iii) *One of the following six conditions holds:*

    (1) $3 \mid m$ *and* $u^2 \equiv 4, 7 \pmod 9$.

(2) $3 \nmid m$ *and* $u \equiv 3, 6 \pmod 9$.

(3) $m \equiv 2 \pmod 3$ *and* $u^2 \equiv 1, 4 \pmod 9$.

(4) $m \equiv 1 \pmod 9$ *and* $u^2 \equiv 13, 22 \pmod{27}$.

(5) $m \equiv 4 \pmod 9$ *and* $u^2 \equiv 4, 22 \pmod{27}$.

(6) $m \equiv 7 \pmod 9$ *and* $u^2 \equiv 4, 13 \pmod{27}$.

We observe that, Theorem 1.2.5 and Theorem 2.1.1 imply the following theorem.

Theorem 2.1.3 *There exist infinitely many pairs of quadratic fields* $\mathbb{Q}(\sqrt{d})$ *and* $\mathbb{Q}(\sqrt{-3d})$ *such that*

$$3 \mid h_{\mathbb{Q}(\sqrt{d})} \qquad \text{and} \qquad 3 \mid h_{\mathbb{Q}(\sqrt{-3d})}.$$

In the light of Theorem 2.1.3, it is natural to ask the following question.

Question 2.1.4 *Let* $n \geq 2$ *be an integer. Find all integers* m *such that there exist infinitely many pairs of quadratic fields* $\mathbb{Q}(\sqrt{d})$ *and* $\mathbb{Q}(\sqrt{md})$ *with*

$$n \mid h_{\mathbb{Q}(\sqrt{d})} \qquad \text{and} \qquad n \mid h_{\mathbb{Q}(\sqrt{md})}.$$

Komatsu addressed Question 2.1.4 for $n = 3$ in [33] and proved the following theorem.

Theorem 2.1.5 *[33] Let* m *be a non-zero integer. Then there exist infinitely many distinct pairs of quadratic fields* $\mathbb{Q}(\sqrt{d})$ *and* $\mathbb{Q}(\sqrt{md})$*, with* $d > 0$*, such that* $3 \mid h_{\mathbb{Q}(\sqrt{d})}$ *and* $3 \mid h_{\mathbb{Q}(\sqrt{md})}$.

Note that, in Theorem 2.1.5, either both $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$ are real or one is real and the other is imaginary, according as $m > 0$ or $m < 0$. Komatsu

extended Theorem 2.1.5 to the pairs of imaginary quadratic fields with class numbers divisible by any integer $n \geq 2$ and proved the following theorem.

Theorem 2.1.6 *[34] Let $m \geq 2$ and $n \geq 2$ be integers. Then there exist infinitely many pairs of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{md})$ such that $n \mid h_{\mathbb{Q}(\sqrt{d})}$ and $n \mid h_{\mathbb{Q}(\sqrt{md})}$.*

Remark 2.1.2 *It is worthwhile to note that Theorem 2.1.6 answers affirmatively Question 2.1.4 for imaginary quadratic fields and for all integers $m \geq 2$.*

Now, we consider a slight variant of Question 2.1.4 as follows.

Question 2.1.7 *Let $m \geq 1$ and $n \geq 2$ be integers. Do there exist infinitely many pairs of quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d+m})$ such that $n \mid h_{\mathbb{Q}(\sqrt{d})}$ and $n \mid h_{\mathbb{Q}(\sqrt{d+m})}$?*

In [26], Iizuka, Konomi and Nakano addressed Question 2.1.7 for $n = 3, 5$ and 7 and proved the following theorem.

Theorem 2.1.8 *[26] Let $n \in \{3, 5, 7\}$ and let m_1, m_2, n_1 and n_2 be rational numbers with $m_1 m_2 \neq 0$. Then there exist infinitely many pairs of quadratic fields $K_1 = \mathbb{Q}(\sqrt{m_1 d + n_1})$ and $K_2 = \mathbb{Q}(\sqrt{m_2 d + n_2})$ with $d \in \mathbb{Q}$ such that $n \mid h_{K_1}$ and $n \mid h_{K_2}$.*

Remark 2.1.3 *In Theorem 2.1.8, the crucial hypothesis is $d \in \mathbb{Q}$. It is easy to see that if $n_1 = n_2 = 0$, then we can take $d \in \mathbb{Z}$. But if either $n_1 \neq 0$ or $n_2 \neq 0$, then Theorem 2.1.8 does not necessarily hold for $d \in \mathbb{Z}$. However, d can be chosen to be an integer for some particular values of m_1, m_2, n_1, n_2 and n.*

In [38], Louboutin proved that for an odd integer $n \geq 3$ and an integer $U \geq 2$, the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{1 - 4U^n})$ is divisible by n. Also, by Theorem 1.2.4, it follows that there are infinitely many imaginary

quadratic fields $\mathbb{Q}(\sqrt{-U}) = \mathbb{Q}(\sqrt{-4U^n})$ whose class numbers are divisible by n. In other words, by taking $d = -4U^n$, we conclude that there are infinitely many tuples of imaginary quadratic fields $\{\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1})\}$ with $d \in \mathbb{Z}$ such that $n \mid h_{\mathbb{Q}(\sqrt{d})}$ and $n \mid h_{\mathbb{Q}(\sqrt{d+1})}$. Motivated by this, Iizuka formulated the following conjecture in [24].

Conjecture 2.1.9 *[24] Let $m \geq 1$ be an integer and let $\ell \geq 3$ be a prime number. Then there exist infinitely many tuples $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+m})$ of quadratic fields with $d \in \mathbb{Z}$ such that ℓ divides the class numbers of all them.*

2.2 Statement of main theorem

In this chapter, we address a weaker version of Conjecture 2.1.9 for triples of imaginary quadratic fields and for $\ell = 3$. The precise statement of our main theorem of this chapter is as follows.

Theorem 2.2.1 *[11] Let $k \geq 1$ be a cube-free integer such that $k \equiv 1 \pmod 9$ and $\gcd(k, 7 \cdot 571) = 1$. Then there exist infinitely many triples of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1})$ and $\mathbb{Q}(\sqrt{d+k^2})$ with $d \in \mathbb{Z}$ such that 3 divides $h_{\mathbb{Q}(\sqrt{d})}$, $h_{\mathbb{Q}(\sqrt{d+1})}$ and $h_{\mathbb{Q}(\sqrt{d+k^2})}$.*

2.3 Preliminaries

We recall a few basic definitions and facts from algebraic number theory.

Definition 2.3.1 *[28] Let K be a field. A function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is said to be a valuation on K if the following conditions hold.*

1. *$|x| = 0$ if and only if $x = 0$.*
2. *$|xy| = |x| \cdot |y|$ for all $x, y \in K$.*

3. *(Triangle inequality)* $|x+y| \leq |x| + |y|$ *for all* $x, y \in K$.

A valuation $|\cdot|$ on a field K is called *trivial* if $|x| = 1$ holds for all $x \neq 0$. Otherwise, it is called a *non-trivial* valuation. Two non-trivial valuations $|\cdot|_1$ and $|\cdot|_2$ are said to be *equivalent*, if the following holds true.

$$|x|_1 < 1 \text{ if and only if } |x|_2 < 1 \text{ for all } x \in K.$$

Definition 2.3.2 *[28] Let K be a field and let $|\cdot|$ be a non-trivial valuation on K. Then $|\cdot|$ is said to be non-archimedean if*

$$|x+y| \leq \max\{|x|, |y|\} \qquad \text{for all } x, y \in K.$$

A valuation on K is called *archimedean* if it is not equivalent to any non-archimedean valuation on K.

Now, let us take K to be a number field with ring of integers $\mathcal{O}_K$. For a non-zero element $x \in K$ and a non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, let $v_{\mathfrak{p}}(x)$ denote the power of $\mathfrak{p}$ appearing in the factorization of the fractional ideal $x\mathcal{O}_K$ into product of prime ideals. Therefore, we have

$$x\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

Proposition 2.3.1 *[28] Let K be a number field and let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Let c be a real number with $0 < c < 1$. Then the map $|\cdot|_{\mathfrak{p}} : K \to \mathbb{R}_{\geq 0}$*

defined by

$$|x|_{\mathfrak{p}} = \begin{cases} c^{v_{\mathfrak{p}}(x)}, & \text{if } x \neq 0, \\ 0, & \text{otherwise .} \end{cases}$$

is a non-archimedean valuation on K.

Definition 2.3.3 *Let K be a number field and let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Let c be a real number with $0 < c < 1$. Then the valuation $|\cdot|_{\mathfrak{p}}$ in Proposition 2.3.1 is called the $\mathfrak{p}$-adic valuation on K.*

For a number field K of degree n, let $\sigma_1, \ldots, \sigma_{n-1}$ and σ_n be all the embeddings of K into $\mathbb{C}$. Let $|\cdot|$ be the usual absolute value on $\mathbb{R}$. It is a well-known fact that for each $i \in \{1, \ldots, n\}$, the map $x \mapsto |\sigma_i(x)|$ defines an archimedean valuation on K. Moreover, it is well-known that these valuations on K are pairwise inequivalent and any archimedean valuation on K is equivalent to the valuation induced by σ_i for some i.

Theorem 2.3.2 *(Ostrowski's theorem) [28] Let K be a number field of degree n and let $\sigma_1, \ldots, \sigma_{n-1}$ and σ_n be all the embeddings of K into $\mathbb{C}$. Let $|\cdot|$ be a non-trivial valuation on K. Then either $|\cdot|$ is equivalent to the valuation induced by σ_i for some $i \in \{1, \ldots, n\}$ or is equivalent to the $\mathfrak{p}$-adic valuation for some non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.*

Next, we define the *S-integers* in a number field as follows.

Definition 2.3.4 *[46] For a number field K, let S be a finite set of valuations on K, containing all the archimedean valuations. Then*

$$R_S = \{\alpha \in K : v(\alpha) \geq 0 \text{ for all } v \notin S\}$$

is called the set of S-integers.

Lemma 2.3.3 *For $K = \mathbb{Q}$ and $S = \{|\cdot|\}$, we have $R_S = \mathbb{Z}$.*

Proof. By the definition of S-integers, we have

$$\begin{aligned} R_S &= \{\alpha \in K : v(\alpha) \geq 0 \text{ for all } v \notin S\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : v_p\left(\frac{a}{b}\right) \geq 0 \text{ for all prime number } p\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b \text{ for all prime number } p\right\} \\ &= \mathbb{Z}. \end{aligned}$$

□

The next theorem is one of the fundamental theorems in the theory of algebraic curves.

Proposition 2.3.4 *(Siegel's theorem, [46]) Let K be a number field and let S be a finite set of valuations on K, containing all the archimedean valuations. Let $f(X) \in K[X]$ be a polynomial of degree $d \geq 3$ with distinct roots in the algebraic closure $\overline{K}$ of K. Then the equation $y^2 = f(x)$ has only finitely many solutions $x, y \in R_S$.*

We apply this result to prove that the discriminants of certain irreducible cubic polynomials are not perfect squares.

We now list some results concerning the ramification of primes in cubic fields. We begin with the following lemma which is merely stated in [32] without a proof. For the sake of completeness, we provide a proof here.

Lemma 2.3.5 *[32] Let $f(X) \in \mathbb{Z}[X]$ be a cubic irreducible polynomial and let E be the splitting field of f over $\mathbb{Q}$. Assume that the discriminant $D(f)$ is not a perfect square and let $F = \mathbb{Q}(\sqrt{D(f)})$. For a prime number p, let $\wp_F$ be a prime ideal in $\mathcal{O}_F$ lying above p. Let α be a root of f and let $K = \mathbb{Q}(\alpha)$. Then $\wp_F$ is ramified in E if and only if p is totally ramified in K.*

Proof. Since $D(f)$ is not a perfect square, we have $F = \mathbb{Q}(\sqrt{D(f)})$ is a quadratic extension of $\mathbb{Q}$ and $Gal(E/\mathbb{Q}) \simeq S_3$. Let $\wp_E$ be a prime ideal in $\mathcal{O}_E$ lying above $\wp_F$ and let $\wp_K = \wp_E \cap K$.

Consider the following diagram of number fields.

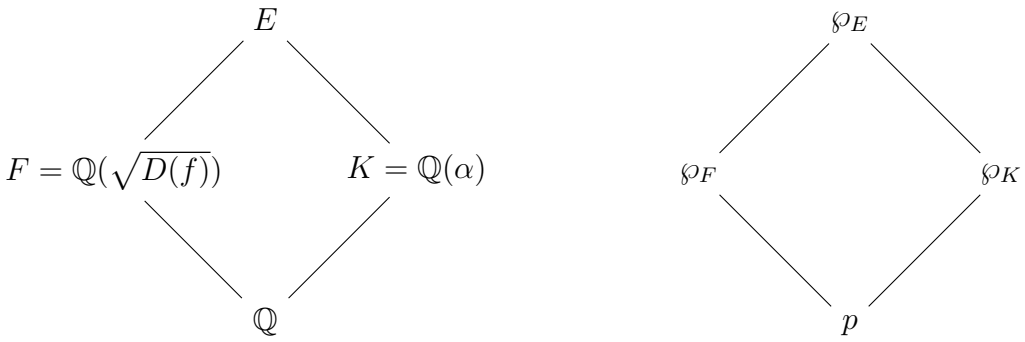


Fig 1. Diagram showing ramification of primes.

Suppose that $\wp_F$ is ramified in E. That is, the ramification index $e(\wp_E|\wp_F) > 1$. Since E is a Galois extension of F of degree 3, we get

$$3 = e(\wp_E|\wp_F) \cdot f(\wp_E|\wp_F) \cdot g, \tag{2.1}$$

where $f(\wp_E|\wp_F)$ is the inertial degree and g is the number of prime ideals in $\mathcal{O}_E$ lying above $\wp_F$. As $e(\wp_E|\wp_F) > 1$, from equation (2.1) we conclude that $e(\wp_E|\wp_F) = 3$. Using the multiplicativity of the ramification indices, we have

$$e(\wp_E|p) = e(\wp_E|\wp_F) \cdot e(\wp_F|p) = 3 \cdot e(\wp_F|p) = e(\wp_E|\wp_K) \cdot e(\wp_K|p). \tag{2.2}$$

From equation (2.2), we get that 3 divides $e(\wp_E|\wp_K) \cdot e(\wp_K|p)$. Since $e(\wp_E|\wp_K) \leq [E : K] = 2$, we have either 3 divides $2 \cdot e(\wp_K|p)$ or 3 divides $e(\wp_K|p)$. Thus we conclude that $3 \mid e(\wp_K|p) \leq [K : \mathbb{Q}] = 3$ and therefore, $e(\wp_K|p) = 3$. Hence p is totally ramified in K.

Conversely, we assume that p is totally ramified in K. We prove that the ramification index $e(\wp_E|\wp_F) > 1$. If not, then $e(\wp_E|\wp_F) = 1$ and

$$e(\wp_E|p) = e(\wp_E|\wp_F) \cdot e(\wp_F|p) = e(\wp_F|p) \leq [F : \mathbb{Q}] = 2. \tag{2.3}$$

Since p is totally ramified in K, from (2.3), we get

$$3 = e(\wp_K|p) \leq e(\wp_E|p) \leq 2,$$

which is a contradiction. Hence $\wp_F$ is ramified in E and this completes the proof of the lemma. □

In Chapter 1, we defined *infinite primes* in a number field. We recall the *ramification* of an infinite prime in a finite extension of a number field.

Definition 2.3.5 *[13] Let L/K be an extension of number fields and let σ be an infinite prime of K. Then σ is said to be ramified in L, if σ is real but it has an extension to L which is complex. If σ is not ramified, then it is said to be unramified in L.*

For an extension of number fields L/K, by the above definition, it follows at once that a complex infinite prime of K is always unramified in L. Moreover, if L is a totally real number field, then any infinite prime of K is unramified in L.

Lemma 2.3.6 *Let $f(X) \in \mathbb{Z}[X]$ be a cubic irreducible polynomial and let E be the splitting field of f over $\mathbb{Q}$. Assume that $D(f)$ is not a perfect square and let $F = \mathbb{Q}(\sqrt{D(f)})$. Then any infinite prime of F is unramified in E.*

Proof. Since the discriminant $D(f)$ of f is not a perfect square, we have $[F : \mathbb{Q}] = 2$ and $Gal(E/\mathbb{Q}) \simeq S_3$. Let σ be an infinite prime of F.

Case 1. $D(f) < 0$. In this case, F is an imaginary quadratic field. Therefore, any extension of σ to E is complex. Thus σ is unramified in E.

Case 2. $D(f) > 0$. That is, F is a real quadratic field. Since f is a polynomial of degree 3, it has a real root, say α. Then the number field $K = \mathbb{Q}(\alpha)$ is contained in $\mathbb{R}$. Since $F \subseteq E$ and $K \subseteq E$, we have $FK \subseteq E$. On the other hand, since $[F : \mathbb{Q}] = 2$ and $[K : \mathbb{Q}] = 3$, we have $[FK : \mathbb{Q}] = 6 = [E : \mathbb{Q}]$. Thus $E = FK \subseteq \mathbb{R}$. Since E is a Galois extension of $\mathbb{Q}$ with $E \subseteq \mathbb{R}$, we conclude that E is totally real. Hence σ is unramified in E. This completes the proof of the lemma. □

For a prime number p and a non-zero integer n, let $v_p(n)$ stand for the unique integer m such that $p^m \mid n$ but $p^{m+1} \nmid n$. The following lemma is a consequence of a theorem in [37] and is presented in [32] as follows.

Lemma 2.3.7 *[32] Let $f(X) = X^3 - aX - b \in \mathbb{Z}[X]$ be an irreducible polynomial over $\mathbb{Q}$ such that for every prime number p, either $v_p(a) < 2$ or $v_p(b) < 3$ holds. Suppose that the discriminant $D(f)$ of f is not a perfect square and let $F = \mathbb{Q}(\sqrt{D(f)})$. Let α be a root of f and let $K = \mathbb{Q}(\alpha)$. Let E be the splitting field of f over $\mathbb{Q}$ and let q be a prime number. Then the following assertions hold.*

(a) If $q \neq 3$, then q is totally ramified in K if and only if $1 \leq v_q(b) \leq v_q(a)$.

(b) The prime 3 is totally ramified in K if and only if one of the following conditions holds.

(i) $1 \leq v_3(a) \leq v_3(b)$,

(ii) $3 \mid a, a \not\equiv 3 \pmod 9, 3 \nmid b$ *and* $b^2 \not\equiv a + 1 \pmod 9$,

(iii) $a \equiv 3 \pmod 9, 3 \nmid b$ *and* $b^2 \not\equiv a + 1 \pmod{27}$.

Proposition 2.3.8 *Let t be an integer with $t \not\equiv 0 \pmod 3$. Then the class number of the quadratic field $\mathbb{Q}(\sqrt{3t(3888t^2+108t+1)})$ is divisible by 3.*

Proof. For an integer t with $t \not\equiv 0 \pmod 3$, let $F = \mathbb{Q}(\sqrt{3t(3888t^2+108t+1)})$. We first prove that F is indeed a quadratic field. For that, we need to prove that $3t(3888t^2+108t+1)$ is not a perfect square. If possible, suppose that $3t(3888t^2+108t+1) = m^2$ for some integer m. Then $3 \mid m$ and hence $9 \mid m^2$. Consequently, $3 \mid t(3888t^2+108t+1)$. Since $\gcd(3, 3888t^2+108t+1) = 1$, we get $3 \mid t$, which contradicts our hypothesis that $t \not\equiv 0 \pmod 3$. Thus F is a quadratic field.

Now, we consider the polynomial $f(X) = X^3 - 3\cdot(108t+1)X - 2 \in \mathbb{Z}[X]$.

Claim. f is irreducible over $\mathbb{Q}$.

If f is reducible over $\mathbb{Q}$, then it must have a linear factor and hence a rational root, say $\frac{a}{b}$ with $\gcd(a,b) = 1$. From the equation $f(\frac{a}{b}) = 0$, we get

$$a^3 - 3\cdot(108t+1)ab^2 - 2b^3 = 0. \tag{2.4}$$

From equation (2.4), we get $a \mid 2b^3$ and $b \mid a^3$. Since $\gcd(a,b) = 1$, we have $b = \pm 1$ and $a = \pm 1, \pm 2$. Therefore, $\frac{a}{b} = \pm 1, \pm 2$.

Case 1. $\frac{a}{b} = 1$. Then $f(1) = 0$ implies $3\cdot(108t+1) = -1$, which is not possible for any $t \in \mathbb{Z}$.

Case 2. $\frac{a}{b} = -1$. Then $f(-1) = 0$ implies $3\cdot(108t+1) = 3$. This, in turn, implies that $t = 0$, which is impossible since $t \not\equiv 0 \pmod 3$.

Case 3. $\frac{a}{b} = 2$. Then $f(2) = 0$ implies $6\cdot(108t+1) = 6$. This, in turn, implies that $t = 0$, which is impossible since $t \not\equiv 0 \pmod 3$.

Case 4. $\frac{a}{b} = -2$. Then $f(-2) = 0$ implies $6\cdot(108t+1) = 10$ which is impossible for any $t \in \mathbb{Z}$.

Therefore, f is an irreducible polynomial over $\mathbb{Q}$ and this proves the claim.

Let E be the splitting field of f over $\mathbb{Q}$. Then we see that

$$D(f) = -4 \cdot [-3 \cdot (108t+1)]^3 - 27 \cdot (-2)^2 = 2^2 \cdot 3^5 \cdot t \cdot (3888t^2 + 108t + 1).$$

Let α be a root of f and let $K = \mathbb{Q}(\alpha)$. Then K is a cubic extension of $\mathbb{Q}$. Also, let p be a prime number. Then by Lemma 2.3.7, we see that p is not totally ramified in F. Hence by Lemma 2.3.5, it follows that every non-zero finite prime of F is unramified in E. Also, by Lemma 2.3.6, we get the infinite primes of F are also unramified in E. Therefore, E is an unramified extension of F of degree 3. Thus by Proposition 1.1.3, we get 3 divides the class number of F. In other words, the class number of the quadratic field $\mathbb{Q}(\sqrt{3t(3888t^2 + 108t + 1)})$ is divisible by 3. □

In the next proposition, we provide another family of imaginary quadratic fields with class number divisible by 3.

Proposition 2.3.9 *Let $t \geq 1$ be an integer. Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{1 - 2916t^3})$ is divisible by 3.*

Proof. We first prove that $F = \mathbb{Q}(\sqrt{1 - 2916t^3})$ is indeed a quadratic field. For that, we need to prove $1 - 2916t^3$ is not a perfect square. If $1 - 2916t^3 = -m^2$ for some integer m, then we have $m^2 \equiv -1 \pmod 3$, which is a contradiction to the fact that any square is congruent to either 0 or 1 $\pmod 3$. Thus, F is a quadratic field.

Consider the polynomial $f(X) = X^3 - 27tX - 1 \in \mathbb{Z}[X]$. If f is reducible over $\mathbb{Q}$, then it must have a linear factor and hence a rational root, say $\frac{a}{b}$ with $\gcd(a, b) = 1$. Then $f(\frac{a}{b}) = 0$ implies that

$$a^3 - 27tab^2 - b^3 = 0. \tag{2.5}$$

From equation (2.5), we have $a \mid b^3$ and $b \mid a^3$. Since $\gcd(a,b) = 1$, we conclude that $\frac{a}{b} = \pm 1$.

Case 1. $\frac{a}{b} = 1$. Then $f(1) = 0$ implies $27t = 0$ which is impossible since $t \geq 1$.

Case 2. $\frac{a}{b} = -1$. Then $f(-1) = 0$ implies $27t = 2$ which is also impossible for any positive integer t.

Hence f is an irreducible polynomial over $\mathbb{Q}$.

Now, we consider the discriminant $D(f) = -4 \cdot (-27t)^3 - 27(-1)^2 = 27 \cdot (2916t^3 - 1)$. Therefore, $\mathbb{Q}(\sqrt{D(f)}) = \mathbb{Q}(\sqrt{3 \cdot (2916t^3 - 1)})$. Since $\gcd(3, 2916t^3 - 1) = 1$, the integer $3 \cdot (2916t^3 - 1)$ is not a perfect square and consequently, $\mathbb{Q}(\sqrt{D(f)})$ is a quadratic field.

Let α be a root of f and let $K = \mathbb{Q}(\alpha)$. Let E be the splitting field of f over $\mathbb{Q}$. Then by Lemma 2.3.5 and Lemma 2.3.6, we get E is a cubic and unramified extension of the real quadratic field $\mathbb{Q}(\sqrt{3 \cdot (2916t^3 - 1)})$. Thus by Proposition 1.1.3, it follows that 3 divides the class number of the real quadratic field $\mathbb{Q}(\sqrt{3 \cdot (2916t^3 - 1)})$. By using Theorem 2.1.1, we conclude that the class number of the imaginary quadratic field

$$F = \mathbb{Q}(\sqrt{-3 \cdot 3 \cdot (2916t^3 - 1)}) = \mathbb{Q}(\sqrt{1 - 2916t^3})$$

is divisible by 3. □

2.4 Proof of Theorem 2.2.1

Let $k \geq 1$ be a cube-free integer such that $k \equiv 1 \pmod 9$ and $\gcd(k, 7 \cdot 571) = 1$. For an integer $t \geq 1$, we consider the polynomial

$$f_t(X) = X^3 - 27tX - k \in \mathbb{Z}[X].$$

If for some integer t, the polynomial f_t is reducible over $\mathbb{Q}$, then it must have a linear factor and hence a rational root, say $\frac{a}{b}$ with $\gcd(a,b)=1$. Using $f_t(\frac{a}{b})=0$, we get

$$a^3 - 27tab^2 - kb^3 = 0. \tag{2.6}$$

From (2.6), we immediately see that $a \mid kb^3$ and $b \mid a^3$. Using $\gcd(a,b)=1$, we get that $b=\pm 1$ and $a \mid k$. Therefore, $\frac{a}{b}$ is an integer and is a divisor of k. Thus $\frac{a}{b}$ has at most finitely many choices and thus f_t is reducible over $\mathbb{Q}$ for at most finitely many values of $t \in \mathbb{N}$. Let $t_0 \in \mathbb{Z}$ be an integer such that f_t is irreducible for all integers $t > |t_0|$.

Next, we consider the discriminant $D(f_t) = 27 \cdot (2916t^3 - k^2)$ of f_t. We note that $D(f_t)$ is a polynomial in t and since $k \neq 0$, we conclude that $D(f_t)$ has distinct roots in $\overline{\mathbb{Q}}$. Therefore, by Lemma 2.3.4, we get that $D(f_t)$ is a perfect square for only finitely many integers t. Let $t_0' \in \mathbb{Z}$ be such that $D(f_t)$ is not a perfect square for all integers $t > |t_0'|$. We set $T = \max\{|t_0|, |t_0'|\} + 1$.

Now, we consider the following simultaneous congruences.

$$\begin{cases} x \equiv 2 \pmod 9; \\ x \equiv 1 \pmod k. \end{cases} \tag{2.7}$$

By our hypothesis, we have $k \equiv 1 \pmod 9$ and hence $\gcd(k,9)=1$. Therefore, by the Chinese remainder theorem, there exists a unique solution $x_0 \pmod{9k}$ of the simultaneous congruence (2.7).

Let

$$\mathcal{M} = \{n \in \mathbb{Z} : n \equiv x_0 \pmod{9k} \text{ and } n > \max\{T, k\}\}.$$

For $n \in \mathcal{M}$, we have

$$27 \cdot n \cdot (3888n^2 + 108n + 1) \equiv 3^3 \cdot 7 \cdot 571 \not\equiv 0 \pmod k. \tag{2.8}$$

Now, for $n \in \mathcal{M}$, let $t_n = n \cdot (3888n^2+108n+1)$. We consider the polynomial $f_{t_n}(X) = X^3 - 27 \cdot n \cdot (3888n^2 + 108n + 1)X - k \in \mathbb{Z}[X]$. Since $t_n > T$, we have that f_{t_n} is irreducible over $\mathbb{Q}$ and the discriminant $D(f_{t_n})$ is not a perfect square. Now, using (2.8), Lemma 2.3.5, Lemma 2.3.6 and Lemma 2.3.7, we conclude that the splitting field E of f_{t_n} over $\mathbb{Q}$ is an unramified extension over $\mathbb{Q}(\sqrt{D(f_{t_n})})$. Thus by Proposition 1.1.3, it follows that 3 divides the class number of $\mathbb{Q}(\sqrt{D(f_{t_n})})$.

We note that, $\mathbb{Q}(\sqrt{D(f_{t_n})}) = \mathbb{Q}(\sqrt{27 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{3 \cdot (2916t_n^3 - k^2)})$ is a real quadratic field. Consequently, using Theorem 2.1.1, we get 3 divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3 \cdot (2916t_n^3 - k^2)}) = \mathbb{Q}(\sqrt{k^2 - 2916t_n^3})$.

Also, by Proposition 2.3.8, we get that the class number of the real quadratic field $\mathbb{Q}(\sqrt{3t_n})$ is divisible by 3. Again from Theorem 2.1.1, we obtain that 3 divides the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3 \cdot 3t_n}) = \mathbb{Q}(\sqrt{-t_n})$. Using the fact that $\mathbb{Q}(\sqrt{-2916t_n^3}) = \mathbb{Q}(\sqrt{-t_n})$ and Proposition 2.3.9, we conclude that 3 divides the class numbers of $\mathbb{Q}(\sqrt{-2916t_n^3})$, $\mathbb{Q}(\sqrt{-2916t_n^3 + 1})$ and $\mathbb{Q}(\sqrt{-2916t_n^3 + k^2})$.

Finally, we only need to prove that

$$\mathcal{Q} = \{\mathbb{Q}(\sqrt{-t_n}) : n \in \mathcal{M}\} \tag{2.9}$$

is infinite. We use the standard argument using the ramification of primes in quadratic fields.

If possible, suppose that $\mathcal{Q}$ is a finite set. Let D be the product of the discriminants of the quadratic fields in the finite set $\mathcal{Q}$. Therefore, a prime number ℓ is ramified in some $\mathbb{Q}(\sqrt{-t_n}) \in \mathcal{Q}$ if and only if $\ell \mid D$. By Dirichlet's theorem for primes in arithmetic progressions, there exist infinitely many prime

numbers $p \equiv x_0 \pmod{9k}$. That is, there are infinitely many primes in $\mathcal{M}$. We choose a prime number $q \in \mathcal{M}$ such that $q \nmid D$. Then q is unramified in $\mathbb{Q}(\sqrt{-t_n})$ for every $n \in \mathcal{M}$, which contradicts the fact that q is ramified in $\mathbb{Q}(\sqrt{-q \cdot (3888q^2 + 108q + 1)}) = \mathbb{Q}(\sqrt{-t_q}) \in \mathcal{Q}$. Hence the family $\mathcal{Q}$ is infinite. This completes the proof of Theorem 2.2.1. □

CHAPTER 3

Distribution of quadratic residues and non-residues using Dirichlet's class number formula

For an odd prime number $p \geq 3$, we consider the quadratic residues and non-residues modulo p in $\{1, 2, \ldots, p-1\}$ that are divisible by 2, 3 and 4. We study their distribution using Dirichlet's class number formula for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

3.1 Introduction and basic results

Let us fix an odd prime number p. We begin with the definition of a *quadratic residue* modulo p.

Definition 3.1.1 *[27] An element $a \in \{1, \ldots, p-1\}$ is said to be a quadratic*

residue $\pmod p$ *if there is an integer* b *such that*

$$b^2 \equiv a \pmod p.$$

In other words, an integer a with $p \nmid a$ is a quadratic residue $\pmod p$ if and only if the polynomial $f(X) = X^2 - a$ has a root in the field $\mathbb{Z}/p\mathbb{Z}$. If a is not a quadratic residue $\pmod p$, then it is called a *quadratic non-residue*. Next, we introduce the *Legendre symbol* as follows.

Definition 3.1.2 *[27] Let* a *be an integer. Then the Legendre symbol* $\left(\frac{\cdot}{p}\right)$ *is defined by the following.*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue} \pmod p, \\ -1, & \text{if } a \text{ is a quadratic non-residue} \pmod p, \\ 0, & \text{if } p \mid a. \end{cases}$$

For an integer m, we denote by $\overline{m}$ the residue of $m \pmod p$. The next proposition provides some basic properties of the Legendre symbol.

Proposition 3.1.1 *[27] For integers* a *and* b*, the following statements hold.*

(i) If $a \equiv b \pmod p$*, then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

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

Proof. (i) Suppose $a \equiv b \pmod p$. If $p \mid a$, then also $p \mid b$ and in that case, we have $\left(\frac{a}{p}\right) = 0 = \left(\frac{b}{p}\right)$.

Now, we assume that $p \nmid ab$. If $a \equiv c^2 \pmod p$ for some integer c, then $b \equiv a \equiv c^2 \pmod p$ and hence $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$.

Finally, if a is a quadratic non-residue $\pmod p$, then $a \not\equiv c^2 \pmod p$ for any integer c. Since $a \equiv b \pmod p$, we have $b \not\equiv c^2 \pmod p$ for any integer c. Therefore, $\left(\frac{a}{p}\right) = -1 = \left(\frac{b}{p}\right)$.

(*ii*) If $p \mid a$, then $a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod p$.

We assume that $p \nmid a$. If $\left(\frac{a}{p}\right) = 1$, then $a \equiv c^2 \pmod p$ for some integer c and hence $a^{\frac{p-1}{2}} \equiv (c^2)^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \pmod p$.

Now, suppose that $\left(\frac{a}{p}\right) = -1$. Let $\overline{g}$ be a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. That is, $g^{p-1} \equiv 1 \pmod p$ and $g^m \not\equiv 1 \pmod p$ for any integer $m < p-1$. Since $p \nmid a$, we have $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ and $a \equiv g^k \pmod p$ for some integer k. Since a is a quadratic non-residue $\pmod p$, the integer k is odd. Using $g^{p-1} \equiv 1 \pmod p$, we get

$$g^{p-1} - 1 \equiv \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Since $\overline{g}$ generates $(\mathbb{Z}/p\mathbb{Z})^*$, we conclude that $g^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod p$ and hence $g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$. Consequently, we get

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

Thus in all the above cases, we get $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

(*iii*) Using $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ for any integer a, we get

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p. \tag{3.1}$$

Since for any integer n, we have $\left(\frac{n}{p}\right) = 0$ or 1 or -1, we conclude from (3.1)

that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. This completes the proof of the proposition. □

Remark 3.1.1 *From (iii) of Proposition 3.1.1, it follows that the map* $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ *defines a group homomorphism.*

Next, we define the *Jacobi symbol* and the *Kronecker symbol*, that are generalizations of the Legendre symbol as follows.

Definition 3.1.3 *[15] Let $a \in \mathbb{Z}$ and let Q be a positive odd integer. Let $Q = \prod_{j=1}^{t} q_j^{e_j}$ be the prime factorization of Q. Then the Jacobi symbol is defined by*

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{t} \left(\frac{a}{q_j}\right)^{e_j}.$$

Definition 3.1.4 *[15] Let $a \in \mathbb{Z}$ and let $n = 2^m n_1$ be an integer with n_1 odd. Then the Kronecker symbol is defined as follows.*

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } 2 \mid a, \\ 1, & \text{if } a \equiv \pm 1 \pmod 8, \\ -1, & \text{if } a \equiv \pm 3 \pmod 8. \end{cases}$$

$$\left(\frac{a}{-1}\right) = \begin{cases} -1, & \text{if } a < 0, \\ 1, & \text{if } a > 0. \end{cases}$$

and

$$\left(\frac{a}{n}\right) = \left(\frac{a}{2}\right)^m \cdot \left(\frac{a}{n_1}\right).$$

The next proposition provides the number of quadratic residues $\pmod p$.

Proposition 3.1.2 *[27] Let p be an odd prime number. Then there are exactly $\frac{p-1}{2}$ quadratic residues* $\pmod p$.

Proof. Let g be a primitive root $\pmod p$. That is, $\overline{g}$ is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Then the $\frac{p-1}{2}$ elements $g^2, g^4, \ldots, g^{p-1}$ are clearly quadratic residues $\pmod p$. By Proposition 3.1.1, an element $a \in \{1, \ldots, p-1\}$ is a quadratic residue $\pmod p$ if and only if a is a root of the polynomial $f(X) = X^{\frac{p-1}{2}} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the polynomial f can have at most $\frac{p-1}{2}$ roots in $\mathbb{Z}/p\mathbb{Z}$. The elements $g^2, g^4, \ldots, g^{p-1}$ are distinct roots of f and hence f has precisely $\frac{p-1}{2}$ roots $\pmod p$. Thus there are exactly $\frac{p-1}{2}$ quadratic residues $\pmod p$. □

Before stating the law of *quadratic reciprocity*, let us characterize the prime numbers p for which -1 and 2 are quadratic residues.

Proposition 3.1.3 *[27] The integer -1 is a quadratic residue $\pmod p$ if and only if $p \equiv 1 \pmod 4$.*

Proof. Suppose that -1 is a quadratic residue $\pmod p$. Then there exists an integer b such that $b^2 \equiv -1 \pmod p$. Therefore, $b^4 \equiv 1 \pmod p$ and hence the element $\overline{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ has order 4. Thus 4 divides the order of the group $(\mathbb{Z}/p\mathbb{Z})^*$. That is, $p \equiv 1 \pmod 4$.

Conversely, assume that $p \equiv 1 \pmod 4$. Then $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$ which is divisible by 4. Consequently, there exists an element $\overline{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ of order 4. Therefore, $b^4 \equiv 1 \pmod 4$ but $b^2 \not\equiv 1 \pmod 4$. That is, $b^2 \equiv -1 \pmod 4$. Hence -1 is a quadratic residue $\pmod p$. □

Proposition 3.1.4 *[15] The integer 2 is a quadratic residue $\pmod p$ if and only if $p \equiv 1$ or $7 \pmod 8$.*

Proof. Let i stand for $\sqrt{-1}$. Then for an odd prime number p, we have

$$(1+i)^p = \sum_{r=0}^{p} \binom{p}{r} i^r.$$

Since $p \mid \binom{p}{r}$ for all $r \in \{1, \ldots, p-1\}$, we get $(1+i)^p \equiv 1 + i^p \pmod{p\mathbb{Z}[i]}$. On the other hand, we have

$$\begin{aligned}(1+i)^p &= (1+i)\cdot(1+i)^{p-1} \\ &= (1+i)\cdot(2i)^{\frac{p-1}{2}} \\ &= i^{\frac{p-1}{2}}\cdot(1+i)\cdot 2^{\frac{p-1}{2}}.\end{aligned}$$

Therefore, we get

$$i^{\frac{p-1}{2}}\cdot(1+i)\cdot 2^{\frac{p-1}{2}} \equiv 1 + i^p \pmod{p\mathbb{Z}[i]}. \tag{3.2}$$

Case 1. $p \equiv 1 \pmod 8$.

Then $i^p = i$ and $i^{\frac{p-1}{2}} = 1$. Therefore, from the equation (3.2), we get

$$1 + i \equiv (1+i)\cdot 2^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]}. \tag{3.3}$$

Since p is an odd prime number, we have $\gcd(p, 1+i) = 1$ in the ring $\mathbb{Z}[i]$. Thus, equation (3.3) becomes $2^{\frac{p-1}{2}} \equiv 1 \pmod{p\mathbb{Z}[i]}$. Therefore, there exist integers a and b such that

$$2^{\frac{p-1}{2}} - 1 = p(a+bi).$$

That is, $2^{\frac{p-1}{2}} - 1 - pa - bi = 0$. Since $\{1, i\}$ is a $\mathbb{Q}$-linearly independent set, we conclude that $2^{\frac{p-1}{2}} - 1 = pa$ and $b = 0$. Hence $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ and using (ii) of Proposition 3.1.1, we conclude that $\left(\dfrac{2}{p}\right) = 1$.

Case 2. $p \equiv 7 \pmod 8$.

Then $i^p = -i$ and $i^{\frac{p-1}{2}} = -i$. Then equation (3.2) becomes

$$1 - i \equiv -i\cdot(1+i)\cdot 2^{\frac{p-1}{2}} \equiv (1-i)\cdot 2^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]}. \tag{3.4}$$

Since p is an odd prime number, we have $\gcd(p, 1-i) = 1$ in $\mathbb{Z}[i]$. Thus, equation (3.4) becomes $2^{\frac{p-1}{2}} \equiv 1 \pmod{p\mathbb{Z}[i]}$. Hence $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and using (ii) of Proposition 3.1.1, we conclude that $\left(\frac{2}{p}\right) = 1$.

Case 3. $p \equiv 3 \pmod 8$.

Then $i^p = -i$ and $i^{\frac{p-1}{2}} = i$. Then equation (3.2) becomes

$$1 - i \equiv i \cdot (1+i) \cdot 2^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]}. \tag{3.5}$$

Writing $1-i$ as $-i(1+i)$ and from (3.5), we get $2^{\frac{p-1}{2}} \equiv -1 \pmod{p\mathbb{Z}[i]}$. Thus, equation (3.5) becomes $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence using (ii) of Proposition 3.1.1, we conclude that $\left(\frac{2}{p}\right) = -1$.

Case 4. $p \equiv 5 \pmod 8$.

Then $i^p = i$ and $i^{\frac{p-1}{2}} = -1$. Then equation (3.2) becomes

$$1 + i \equiv -1 \cdot (1+i) \cdot 2^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]}$$

and hence $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence using (ii) of Proposition 3.1.1, we conclude that $\left(\frac{2}{p}\right) = -1$. □

Now, we state one of the most celebrated theorems in number theory, namely, the law of *quadratic reciprocity*. This provides a relation between the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for two distinct odd prime numbers p and q. The precise statement is as follows.

Theorem 3.1.5 *(Quadratic reciprocity) [27] Let p and q be two distinct odd prime numbers. Then the following holds.*

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

3.2 Motivation and history

From Proposition 3.1.2, it follows that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0. \tag{3.6}$$

In other words, the number of quadratic residues in $\{1, \ldots, p-1\}$ is same as the number of quadratic non-residues. Equation (3.6) motivated number theorists to consider the distribution of residues and non-residues over different subintervals of $[1, p-1]$. We list a few results along this direction in the following.

Proposition 3.2.1 *[4] Let p be a prime number with $p \equiv 1 \pmod 4$. Then*

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 0.$$

Proof. Since $p \equiv 1 \pmod 4$, by Proposition 3.1.3, we get that -1 is a square $(\text{mod } p)$. That is, $-1 \equiv b^2 \pmod p$ for some integer b. Therefore, for an integer a, using Proposition 3.1.1, we get

$$\left(\frac{a}{p}\right) = \left(\frac{b^2 a}{p}\right) = \left(\frac{-a}{p}\right). \tag{3.7}$$

Thus, equation (3.6) and equation (3.7) together imply

$$0 = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 2 \cdot \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

Hence $\displaystyle\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 0$ and this completes the proof of the proposition. □

Proposition 3.2.2 *[4] Let p be a prime number with $p \equiv 3 \pmod 4$. Let q be an integer such that $\gcd(p, q) = 1$.*

(i) If $\left(\frac{q}{p}\right) = 1$ *, then*

$$\sum_{m=1}^{[\frac{q}{2}]} \sum_{\frac{(2m-1)p}{2q} < n < \frac{mp}{q}} \left(\frac{n}{p}\right) = 0.$$

(ii) If $\left(\frac{q}{p}\right) = -1$ *, then*

$$\sum_{m=0}^{[\frac{q-1}{2}]} \sum_{\frac{mp}{q} < n < \frac{(2m+1)p}{2q}} \left(\frac{n}{p}\right) = 0.$$

As an application of Proposition 3.2.2, we obtain results similar to Proposition 3.2.1 as follows.

Proposition 3.2.3 *[4] Let p be an odd prime number.*

(i) If $p \equiv 3 \pmod 8$*, then* $\sum_{0<n<\frac{p}{4}} \left(\frac{n}{p}\right) = 0.$

(ii) If $p \equiv 7 \pmod 8$*, then* $\sum_{\frac{p}{4}<n<\frac{p}{2}} \left(\frac{n}{p}\right) = 0.$

(iii) If $p \equiv 11 \pmod{12}$*, then* $\sum_{\frac{p}{6}<n<\frac{p}{3}} \left(\frac{n}{p}\right) = 0.$

Proof. (i) Since $p \equiv 3 \pmod 8$, by Proposition 3.1.4, we have $\left(\frac{2}{p}\right) = -1$. Therefore, by (ii) of Proposition 3.2.2, we have $\sum_{0<n<\frac{p}{4}} \left(\frac{n}{p}\right) = 0.$

(ii) Since $p \equiv 7 \pmod 8$, by Proposition 3.1.4, we have $\left(\frac{2}{p}\right) = 1$. Therefore, by (i) of Proposition 3.2.2, we have $\sum_{\frac{p}{4}<n<\frac{p}{2}} \left(\frac{n}{p}\right) = 0.$

(*iii*) Since $p \equiv 11 \pmod{12}$, we have $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$. Therefore, by Theorem 3.1.5, we get

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

Thus for $q = 3$ in Proposition 3.2.2, we obtain $\sum_{\frac{p}{6}<n<\frac{p}{3}} \left(\frac{n}{p}\right) = 0.$ □

Proposition 3.2.3 shows that for primes in some particular arithmetic progressions, the number of quadratic residues and non-residues are equal in certain sub-intervals of $[1, p-1]$. Now, we consider certain arithmetic progressions in $[1, p-1]$ and ask the following natural question.

Question 3.2.4 *Let p be an odd prime number and let k be an integer with $1 \leq k \leq p-1$. Let*

$$\mathcal{S}_k = \{a \in \{1, 2, \ldots, p-1\} : a \equiv 0 \pmod k\}.$$

Then how many quadratic residues (respectively, non-residues) belong to $\mathcal{S}_k$?

In the literature, there are some results addressing Question 3.2.4 (cf. [29], [30] and [35]). Before we proceed further, we fix some notations as follows. Let $Q(p, \mathcal{S}_k)$ (respectively, $N(p, \mathcal{S}_k)$) stand for the number of quadratic residues (respectively, quadratic non-residues) $\pmod p$ in the set $\mathcal{S}_k$. In a subsequent section, using standard techniques in analytic number theory, we prove the following formula for $Q(p, \mathcal{S}_k)$.

$$Q(p, \mathcal{S}_k) = \frac{p-1}{2k} + O(\sqrt{p}\log p). \tag{3.8}$$

Using standard techniques, we cannot determine whether $Q(p, \mathcal{S}_k) > N(p, \mathcal{S}_k)$ or $Q(p, \mathcal{S}_k) < N(p, \mathcal{S}_k)$ for some primes p. We answer this question for $k = 2, 3$

and 4 using Dirichlet's class number formula for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

3.3 Statements of main theorems

Theorem 3.3.1 *[9] Let p be an odd prime number. If $p \equiv 3 \pmod 4$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$Q(p, \mathcal{S}_2) - \frac{p-1}{4} \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

If $p \equiv 1 \pmod 4$, then we have

$$Q(p, \mathcal{S}_2) = \frac{p-1}{4}.$$

Corollary 3.3.2 *[9] Let p be an odd prime number and let $\mathcal{O}$ be the set of all odd integers in $[1, p-1]$. If $R = N(p, \mathcal{S}_2)$ or $R = Q(p, \mathcal{O})$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$\frac{p-1}{4} - R \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 3 \pmod 4.$$

If $p \equiv 1 \pmod 4$, then we have

$$R = \frac{p-1}{4}.$$

Theorem 3.3.3 *[9] Let p be an odd prime number. If $p \equiv 1$ or $11 \pmod{12}$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$Q(p, \mathcal{S}_3) - \frac{p-1}{6} \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

Corollary 3.3.4 *[9] Let p be an odd prime number. If $p \equiv 1$ or $11 \pmod{12}$, then for any ϵ with $0 < \epsilon < \frac{1}{2}$, we have*

$$\frac{p-1}{6} - N(p, \mathcal{S}_3) \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

Theorem 3.3.5 *[9] Let p be an odd prime. If $p \equiv 3 \pmod{8}$, then we have*

$$Q(p, \mathcal{S}_4) = \frac{1}{2}\left[\frac{p-1}{4}\right].$$

Also, for any $0 < \epsilon < \frac{1}{2}$, we have

$$Q(p, \mathcal{S}_4) - \frac{p-1}{8} \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 1 \pmod{4},$$

and

$$Q(p, \mathcal{S}_4) - \frac{1}{2}\left[\frac{p-1}{4}\right] \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 7 \pmod{8}.$$

Corollary 3.3.6 *[9] Let p be an odd prime number. If $p \equiv 3 \pmod{8}$, then we have*

$$N(p, \mathcal{S}_4) = \frac{1}{2}\left[\frac{p-1}{4}\right].$$

Also, for any $0 < \epsilon < \frac{1}{2}$, we have

$$\frac{p-1}{8} - N(p, \mathcal{S}_4) \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 1 \pmod{4},$$

and

$$\frac{1}{2}\left[\frac{p-1}{4}\right] - N(p, \mathcal{S}_4) \gg_\epsilon p^{\frac{1}{2}-\epsilon}, \text{ if } p \equiv 7 \pmod{8}.$$

Using Theorems 3.3.1 and 3.3.5, we conclude the following.

Corollary 3.3.7 *[9] Let p be an odd prime number with $p \equiv 3 \pmod{8}$. Then*

for any ϵ *with* $0 < \epsilon < \frac{1}{2}$, *we have*

$$Q(p, \mathcal{S}_2 \backslash \mathcal{S}_4) - \frac{1}{2}\left\lfloor \frac{p-1}{4} \right\rfloor \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

3.4 Preliminaries

We begin with the basic fact concerning *Dirichlet's L-function*. For that, we define the *Dirichlet character* as follows.

Definition 3.4.1 *[28] Let* $q \geq 2$ *be an integer. A group homomorphism* $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ *is called a Dirichlet character modulo* q. *The integer* q *is often called the modulus of the Dirichlet character.*

Remark 3.4.1 *If* χ *is the trivial group homomorphism, then it is called the principal Dirichlet character modulo* q. *We denote the principal Dirichlet character by* χ_0. *Given a Dirichlet character* χ, *we can think of it as a function from* $\mathbb{Z}$ *to* $\mathbb{C}$ *defined by*

$$\chi(k) = \begin{cases} \chi(\overline{k}), & \text{if } \gcd(k,q) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Definition 3.4.2 *[28] Let* $q \geq 2$ *be an integer and let* χ *be a Dirichlet character modulo* q. *Then the Dirichlet series*

$$L(s,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}, \qquad \text{for } s \in \mathbb{C}$$

is called the Dirichlet L-function associated to χ.

If χ is a non-principal Dirichlet character, then the associated Dirichlet L-function $L(s,\chi)$ is analytic in the half plane $\{s \in \mathbb{C} : Re(s) > 0\}$. Moreover, for

all complex numbers s with $Re(s) > 1$, the Dirichlet L-function $L(s, \chi)$ admits the *Euler product* expansion

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{3.9}$$

For the rest of the discussion, we assume that all the Dirichlet characters χ are *quadratic*. That is, $\chi^2 = \chi_0$.

For a non-trivial character χ, by (3.9), we conclude that $L(s, \chi) \neq 0$ for all complex numbers s with $Re(s) > 1$. In particular, $L(s, \chi) > 0$ for all real number s with $s > 1$. Since $L(s, \chi)$ is a continuous function in the half plane $\{s \in \mathbb{C} : Re(s) > 1\}$, we get that $L(1, \chi) \geq 0$. It is a well-known theorem in analytic number theory that $L(1, \chi) \neq 0$. Thus we obtain $L(1, \chi) > 0$. The following theorem due to Landau and Siegel provides a lower bound of $L(1, \chi)$ in terms of the modulus of the Dirichlet character.

Theorem 3.4.1 *(cf. [41]) Let $q \geq 2$ be an integer and let χ be a non-trivial quadratic character modulo q. Then for each $\epsilon > 0$, there exists a constant $C(\epsilon) > 0$ such that*

$$L(1, \chi) > \frac{C(\epsilon)}{q^\epsilon}.$$

For an odd prime number p, let χ_p stand for the Legendre symbol $\left(\frac{\cdot}{p}\right)$. By Proposition 3.1.1, it follows that χ_p is a quadratic character. We also define a character χ_4 by

$$\chi_4(k) = \begin{cases} (-1)^{(k-1)/2}; & \text{if } k \text{ is odd,} \\ 0; & \text{otherwise.} \end{cases}$$

We can also define the Dirichlet character χ_{4p} by setting $\chi_{4p}(k) = \chi_4(k) \cdot \chi_p(k)$. Again, we define the Dirichlet character χ_{3p} by setting $\chi_{3p}(k) = \chi_3(k) \cdot \chi_p(k)$. It immediately follows that both χ_{3p} and χ_{4p} are non-trivial, real quadratic

Dirichlet characters.

Now, we state the following important lemma, which will be crucially used in the proof of our main theorems.

Lemma 3.4.2 *(See Page 151, Theorem 7.2 and 7.4 in [51]) Let $p > 3$ be an odd prime number. For a real number $\ell \geq 1$, we define*

$$S(1, \ell) = \sum_{1 \leq m < \ell} \chi_p(m). \tag{3.10}$$

Then the following hold.

(i) For a prime number p with $p \equiv 3 \pmod 4$, we have

$$S\left(1, \frac{p}{2}\right) = \frac{\sqrt{p}}{\pi} \left(2 - \chi_p(2)\right) L(1, \chi_p),$$

where $L(1, \chi_p)$ is the Dirichlet L-function; Also, we have

$$S\left(1, \frac{p}{3}\right) = \frac{\sqrt{p}}{2\pi} (3 - \chi_p(3)) L(1, \chi_p).$$

(ii) For a prime number p with $p \equiv 1 \pmod 4$, we have

$$S\left(1, \frac{p}{3}\right) = \frac{\sqrt{3p}}{2\pi} L(1, \chi_{3p});$$

Also, we have

$$S\left(1, \frac{p}{4}\right) = \frac{\sqrt{p}}{\pi} L(1, \chi_{4p}).$$

Remark 3.4.2 *To prove Lemma 3.4.2, the main tool is to use the Dirichlet's class number formula for imaginary quadratic fields which states that for an imaginary quadratic field K with discriminant d_K and class number h_K, we*

have

$$L(1,\chi)=\frac{2\pi h_K}{w\cdot\sqrt{|d_K|}},$$

where w is the number of roots of unity in K and $\chi(\cdot)=\left(\frac{d_K}{\cdot}\right)$ is the Kronecker symbol.

Now, we state the famous *Pölya-Vinogradov* inequality as follows.

Theorem 3.4.3 *[2] Let p be an odd prime number and let χ be a non-principal Dirichlet character modulo p. Then, for any integers M and N with $0\leq M<N\leq p-1$, we have*

$$\left|\sum_{m=M}^{N}\chi(m)\right|\leq\sqrt{p}\log p.$$

The next lemma provides the characteristic functions for quadratic residues and non-residues.

Lemma 3.4.4 *[9] Let p be an odd prime number and let*

$$f(x)=\frac{1}{2}\left(1+\left(\frac{x}{p}\right)\right)\ \textit{for all}\ \overline{x}\in(\mathbb{Z}/p\mathbb{Z})^* \tag{3.11}$$

and

$$g(x)=\frac{1}{2}\left(1-\left(\frac{x}{p}\right)\right)\ \textit{for all}\ \overline{x}\in(\mathbb{Z}/p\mathbb{Z})^* \tag{3.12}$$

Then, we have

$$f(x)=\begin{cases}1; & \textit{if } x \textit{ is a quadratic residue} \pmod p,\\ 0; & \textit{otherwise.}\end{cases}$$

and

$$g(x)=\begin{cases}1; & \textit{if } x \textit{ is a quadratic nonresidue} \pmod p,\\ 0; & \textit{otherwise.}\end{cases}$$

Proof. If x is a quadratic residue $\pmod p$, then $\left(\frac{x}{p}\right) = 1$ and hence $f(x) = 1$. Otherwise, if x is a quadratic non-residue $\pmod p$, then $\left(\frac{x}{p}\right) = -1$ and hence $f(x) = 0$. Therefore, f is indeed a characteristic function for the quadratic residues $\pmod p$. Similarly, we can show that g is a characteristic function for the quadratic non-residues $\pmod p$. □

Now, we give a proof of the formula (3.8) in the following proposition.

Proposition 3.4.5 *[9] Let $k \geq 1$ be an integer and let p be an odd prime number. Let $\mathcal{S}_k = kI$, where $I = \{1, 2, \ldots, [\frac{p-1}{k}]\}$. Then*

$$Q(p, \mathcal{S}_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + \frac{1}{2}\left(\frac{k}{p}\right)\sum_{m=1}^{[\frac{p-1}{k}]}\left(\frac{m}{p}\right) \tag{3.13}$$

and hence

$$Q(p, \mathcal{S}_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + O(\sqrt{p}\log p).$$

Moreover, the same expression holds for $N(p, \mathcal{S}_k)$.

Proof. We define a function ψ_k by setting

$$\psi_k(m) = \begin{cases} 1; & \text{if } m \in \mathcal{S}_k, \\ 0; & \text{if } m \notin \mathcal{S}_k. \end{cases}$$

Now, by Lemma 3.4.4, we have

$$\begin{aligned} Q(p, \mathcal{S}_k) &= \sum_{m \in S_k} f(m) = \sum_{m=1}^{p-1} \psi_k(m) f(m) \\ &= \frac{1}{2}\sum_{m=1}^{p-1} \psi_k(m)\left(1 + \left(\frac{m}{p}\right)\right) \\ &= \frac{1}{2}\left[\frac{p-1}{k}\right] + \frac{1}{2}\left(\frac{k}{p}\right)\sum_{m=1}^{[\frac{p-1}{k}]}\left(\frac{m}{p}\right). \end{aligned}$$

This proves (3.13). By Theorem 3.4.3, we have $\sum_{m=1}^{[\frac{p-1}{k}]} \left(\frac{m}{p}\right) = O(\sqrt{p}\log p)$. Consequently, using (3.13), we conclude that

$$Q(p, \mathcal{S}_k) = \frac{1}{2}\left[\frac{p-1}{k}\right] + O(\sqrt{p}\log p).$$

Similarly, working with the characteristic function g for quadratic non-residues (mod p) in place of f, we get the same formula for $N(p, \mathcal{S}_k)$. □

3.5 Proof of Theorem 3.3.1

Let p be a given odd prime. We want to estimate the quantity $Q(p, \mathcal{S}_2)$. Therefore, by (3.13), we get

$$Q(p, \mathcal{S}_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{1}{2}\left(\frac{2}{p}\right)\sum_{n=1}^{(p-1)/2}\left(\frac{n}{p}\right). \tag{3.14}$$

Case 1. $p \equiv 1 \pmod 4$.

Then by Lemma 3.2.3, we have $\sum_{n=1}^{(p-1)/2}\left(\frac{n}{p}\right) = 0$ and therefore, equation (3.14) boils down to

$$Q(p, \mathcal{S}_2) = \frac{p-1}{4},$$

which is as desired.

Case 2. $p \equiv 3 \pmod 8$.

By Lemma 3.4.2 and by (3.14), we get

$$Q(p, \mathcal{S}_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{\sqrt{p}}{\pi}\left(2 - \chi_p(2)\right) L(1, \chi_p).$$

Since $p \equiv 3 \pmod 8$, by Proposition 3.1.4, we have $\left(\frac{2}{p}\right) = -1$. Therefore, we

obtain

$$Q(p, \mathcal{S}_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + 3\frac{\sqrt{p}}{\pi}L(1, \chi_p).$$

Let ϵ be any real number such that $0 < \epsilon < \frac{1}{2}$. Then by Theorem 3.4.1, we get

$$Q(p, \mathcal{S}_2) - \frac{1}{2}\left[\frac{p-1}{2}\right] = 3\frac{\sqrt{p}}{\pi}L(1, \chi_p) \gg_\epsilon p^{\frac{1}{2}-\epsilon},$$

as required.

Case 3. $p \equiv 7 \pmod 8$.

Since $p \equiv 7 \pmod 8$, we know by Proposition 3.1.4 that $\left(\frac{2}{p}\right) = 1$. Therefore, by Lemma 3.4.2 and by (3.14), we get

$$Q(p, \mathcal{S}_2) = \frac{1}{2}\left[\frac{p-1}{2}\right] + \frac{\sqrt{p}}{\pi}L(1, \chi_p).$$

Let ϵ be a real number with $0 < \epsilon < \frac{1}{2}$. Then by Theorem 3.4.1, we get

$$Q(p, \mathcal{S}_2) - \frac{1}{2}\left[\frac{p-1}{2}\right] \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

This completes the proof of the theorem. □

3.6 Proof of Theorem 3.3.3

For a given prime number p, we want to estimate $Q(p, \mathcal{S}_3)$. By equation (3.13), we get

$$Q(p, \mathcal{S}_3) = \frac{1}{2}\left[\frac{p-1}{3}\right] + \left(\frac{3}{p}\right)\sum_{n=1}^{(p-1)/3}\left(\frac{n}{p}\right). \tag{3.15}$$

Case 1. $p \equiv 1 \pmod{12}$.

In this case, we have $\left(\frac{3}{p}\right) = 1$. By (3.15) and by Lemma 3.4.2, we get

$$\begin{aligned} Q(p, \mathcal{S}_3) - \frac{1}{2}\left(\frac{p-1}{3}\right) &= \frac{1}{2}\frac{\sqrt{3p}}{2\pi} L(1, \chi_3\chi_p) \\ &\geq \frac{\sqrt{3p}}{4\pi}\frac{C(\epsilon)}{(3p)^{\epsilon}} \gg_{\epsilon} p^{\frac{1}{2}-\epsilon}, \end{aligned}$$

for any given $0 < \epsilon < \frac{1}{2}$ in Theorem 3.4.1.

Case 2. $p \equiv 11 \pmod{12}$.

In this case, we have, $\left(\frac{3}{p}\right) = 1$. By (3.15) and by Lemma 3.4.2, we get

$$\begin{aligned} Q(p, \mathcal{S}_3) &= \frac{1}{2}\left[\frac{p-1}{3}\right] + \frac{1}{2}\frac{\sqrt{3p}}{2\pi}(3 - \chi_p(3))L(1, \chi_p) \\ &= \frac{1}{2}\left[\frac{p-1}{3}\right] + \frac{1}{2}\frac{\sqrt{3p}}{2\pi}(3-1)L(1, \chi_p) \\ &= \frac{1}{2}\left[\frac{p-1}{3}\right] + \frac{\sqrt{3p}}{2\pi}L(1, \chi_p). \end{aligned}$$

Hence for any ϵ with $0 < \epsilon < \frac{1}{2}$, using Theorem 3.4.1, we get

$$Q(p, \mathcal{S}_3) - \frac{1}{2}\left[\frac{p-1}{3}\right] = \frac{\sqrt{3p}}{2\pi}L(1, \chi_p) \gg_{\epsilon} p^{\frac{1}{2}-\epsilon}.$$

This completes the proof of the theorem. □

3.7 Proof of theorem 3.3.5

Let p be a given odd prime number. We want to estimate $Q(p, \mathcal{S}_4)$. Using equation (3.13), we note that

$$Q(p, \mathcal{S}_4) = \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\left(\frac{4}{p}\right)\sum_{m=1}^{(p-1)/4}\left(\frac{m}{p}\right) = \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\sum_{m=1}^{(p-1)/4}\left(\frac{m}{p}\right). \tag{3.16}$$

Case 1. $p \equiv 1 \pmod 4$.

Now, by applying Lemma 3.4.2 in (3.16), we get

$$Q(p, \mathcal{S}_4) = \frac{1}{2}\left(\frac{p-1}{4}\right) + \frac{1}{2}\frac{\sqrt{p}}{\pi}L(1, \chi_4\chi_p).$$

Hence for a real number ϵ with $0 < \epsilon < \frac{1}{2}$, by Theorem 3.4.1, we get

$$Q(p, \mathcal{S}_4) - \frac{p-1}{8} \gg_\epsilon p^{\frac{1}{2}-\epsilon}.$$

Case 2. $p \equiv 3 \pmod 8$.

In this case, by applying (i) of Lemma 3.2.3, we get

$$Q(p, \mathcal{S}_4) = \frac{1}{2}\left[\frac{p-1}{4}\right].$$

Case 3. $p \equiv 7 \pmod 8$.

We observe that by (ii) of Lemma 3.2.3, we have

$$\sum_{\frac{p-1}{4} < m < \frac{p-1}{2}} \left(\frac{m}{p}\right) = 0.$$

Therefore, we can rewrite equation (3.16) as follows.

$$\begin{aligned} Q(p, \mathcal{S}_4) &= \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\sum_{1 \le m \le (p-1)/4}\left(\frac{m}{p}\right) + \frac{1}{2}\sum_{(p-1)/4 \le m \le (p-1)/2}\left(\frac{m}{p}\right) \\ &= \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\sum_{m=1}^{\frac{p-1}{2}}\left(\frac{m}{p}\right). \end{aligned}$$

Now, by using Lemma 3.4.2, we get

$$Q(p, \mathcal{S}_4) = \frac{1}{2}\left[\frac{p-1}{4}\right] + \frac{1}{2}\frac{\sqrt{p}}{\pi}L(1, \chi_p).$$

Hence for a real number ϵ with $0 < \epsilon < \frac{1}{2}$, from Theorem 3.4.1, we get

$$Q(p, \mathcal{S}_4) - \frac{1}{2}\left[\frac{p-1}{4}\right] \gg p^{\frac{1}{2}-\epsilon}.$$

This completes the proof of the theorem. □

CHAPTER 4

Euclidean ideal class in certain bi-quadratic fields

In this chapter, following [36], we define the notion of an Euclidean ideal class in a number field K and prove the existence of a non-principal Euclidean ideal class in a family (possibly infinite) of bi-quadratic number fields. The main results of this chapter have been published in [10].

4.1 Introduction

Let R be an integral domain. A function $\phi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ is said to be an *Euclidean function* if for any two elements a and b in R with $b \neq 0$, there exist q and r in R such that

$$a = bq + r, \text{ with either } r = 0 \text{ or } \phi(r) < \phi(b).$$

Definition 4.1.1 *An integral domain R is called an Euclidean domain if there exists an Euclidean function on R.*

Example 4.1.1 The ring $\mathbb{Z}$ is a familiar example of an Euclidean domain, where the usual absolute value $|\cdot|$ plays the role of an Euclidean function. Also, the ring $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ is an Euclidean domain with respect to the Euclidean function $\phi(a + bi) = a^2 + b^2 = |a + ib|$.

Proposition 4.1.1 *[27] Let R be an Euclidean domain with respect to an Euclidean function ϕ. Then R is a PID.*

Proof. Let I be a non-zero ideal in R. Since $\mathbb{N}$ is well-ordered, there exists $b \in I$ such that $\phi(b) \leq \phi(b')$ for all $b' \in I$. Let a be a non-zero element of I. Since R is an Euclidean domain with respect to ϕ, there exist q and r in R such that $a = bq + r$. Now if $r \neq 0$, then $\phi(r) = \phi(a - bq) < \phi(b)$. Since I is an ideal and a and b in I, we conclude that $r = a - bq \in I$. This contradicts the fact that $\phi(b) \leq \phi(b')$ for all $b' \in I$ as $\phi(r) < \phi(b)$. Consequently, $r = 0$ and thus $a = bq$. Since a is an arbitrary element of I, we conclude that $I \subseteq \langle b \rangle$. The inclusion $\langle b \rangle \subseteq I$ is evident because $b \in I$. Hence $I = \langle b \rangle$. Since I is an arbitrary ideal in R, we conclude that every ideal in R is principal and thus R is a PID. □

Remark 4.1.1 *Suppose that for a number field K, the ring of integers $\mathcal{O}_K$ is an Euclidean domain. Then by Proposition 4.1.1, we conclude that the class number h_K of K is 1.*

Let K be a number field of degree $n \geq 1$ and let $\mathcal{O}_K$ be its ring of integers. Let $\sigma_1, \ldots, \sigma_{n-1}$ and σ_n be all the embeddings of K into $\mathbb{C}$. Then for an element $\alpha \in \mathcal{O}_K$, we define its *norm* by the equation

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

It is clear that norm is a multiplicative function, that is, $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

Proposition 4.1.2 *[27] Let K be a number field and let $\alpha \in \mathcal{O}_K$. Then $N(\alpha) \in \mathbb{Z}$.*

Proof. If $\alpha = 0$, then $N(\alpha) = 0 \in \mathbb{Z}$. We assume that $\alpha \neq 0 \in \mathcal{O}_K$ and let $f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Then α is of degree d over $\mathbb{Q}$ and therefore, d divides n. Moreover, $f(\sigma_i(\alpha)) = 0$ for all $i \in \{1, \ldots, n\}$. Thus we have

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = ((-1)^d a_0)^{\frac{n}{d}} = (-1)^n a_0^{\frac{n}{d}}$$

which is an integer. □

Remark 4.1.2 *By Proposition 4.1.2, we see that N is a map from $\mathcal{O}_K$ to $\mathbb{Z}$. Since K is the field of fraction of $\mathcal{O}_K$, we can extend the norm map from K to $\mathbb{Q}$ by the formula $N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}$ for α and $\beta \in \mathcal{O}_K$ with $\beta \neq 0$.*

Having defined the norm map, it is interesting to investigate when the ring $\mathcal{O}_K$ is an Euclidean domain with respect to the absolute value of the norm map. For the sake of convenience, we denote $|N(x)|$ by $\mathrm{Nm}(x)$ for all $x \in K$.

Definition 4.1.2 *[40] A number field K is said to be norm-Euclidean if the ring of integers $\mathcal{O}_K$ is an Euclidean domain with respect to the function* Nm.

The following basic proposition (cf. [27]) provides an equivalent criterion for K to be norm-Euclidean.

Proposition 4.1.3 *Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Then K is norm-Euclidean if and only if for any $x \in K \setminus \{0\}$, there exists $\alpha \in \mathcal{O}_K$ such that $\mathrm{Nm}(x - \alpha) < 1$.*

Proof. Suppose that K is norm-Euclidean and let x be a non-zero element in K. Let $x = \frac{a}{b}$ with a and $b \in \mathcal{O}_K \setminus \{0\}$. Since K is norm-Euclidean, there exist q and $r \in \mathcal{O}_K$ such that $a = bq + r$ and either $r = 0$ or $\mathrm{Nm}(r) < \mathrm{Nm}(b)$. If $r = 0$, then we have $x = \frac{a}{b} = q \in \mathcal{O}_K$ and hence we can take $\alpha = q$ so that $\mathrm{Nm}(x - \alpha) = 0 < 1$. Otherwise,

$$\mathrm{Nm}(x - q) = \mathrm{Nm}\left(\frac{a}{b} - q\right) = \mathrm{Nm}\left(\frac{a - bq}{b}\right) = \mathrm{Nm}\left(\frac{r}{b}\right) = \frac{\mathrm{Nm}(r)}{\mathrm{Nm}(b)} < 1$$

and hence we can take $\alpha = q$.

Conversely, suppose that for any $x \in K \setminus \{0\}$, there exists $\alpha \in \mathcal{O}_K$ such that $\mathrm{Nm}(x - \alpha) < 1$. Let a and b be two non-zero elements of $\mathcal{O}_K$. Then, by hypothesis, there exist $q \in \mathcal{O}_K$ such that $\mathrm{Nm}\left(\frac{a}{b} - q\right) < 1$. By setting $r = a - bq$ and using the multiplicativity of Nm, we obtain $a = bq + r$ with either $r = 0$ or $\mathrm{Nm}(r) < \mathrm{Nm}(b)$. In other words, K is norm-Euclidean. □

4.2 Euclidean ideal class

In 1979, H. W. Lenstra [36] extended the notion of a norm-Euclidean number field to ideals. Since $\mathrm{Nm}(\mathcal{O}_K) = 1$, he replaced 1 by $\mathrm{Nm}(I) = N(I)$ and defined the *norm-Euclidean* ideal as follows.

Definition 4.2.1 *[36] Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. A non-zero ideal I in $\mathcal{O}_K$ is said to be norm-Euclidean if for any $x \in K \setminus \{0\}$, there exists $\alpha \in I$ such that $\mathrm{Nm}(x - \alpha) < N(I)$, where $N(I)$ stands for the cardinality of the finite set $\mathcal{O}_K/I$.*

Remark 4.2.1 *Note that, if we take $I = \mathcal{O}_K$, then Definition 4.1.2 and Definition 4.2.1 coincide.*

Lenstra [36] generalized Definition 4.2.1 further for any Dedekind domain and coined the notion of an *Euclidean ideal* as follows.

Definition 4.2.2 *[36] Let R be a Dedekind domain. Let $\mathbb{I}$ be the set of all fractional ideals containing R and let W be a well-ordered set. A fractional ideal C of R is said to be an Euclidean ideal if there exists a function $\psi : \mathbb{I} \to W$ such that for any $J \in \mathbb{I}$ and any $x \in JC \setminus C$, there exists some $y \in C$ satisfying*

$$\psi((x-y)^{-1}JC) < \psi(J). \tag{4.1}$$

Remark 4.2.2 *Note that, if we take $R = \mathcal{O}_K$, $C = I$, $\psi = \mathrm{Nm}^{-1}$ and J any fractional ideal containing R, then $JC = JI = K$ and equation (4.1) becomes*

$$\mathrm{Nm}(x-y) < \mathrm{Nm}(I),$$

which implies that I is a norm-Euclidean ideal. Hence Definition 4.2.2 is indeed a generalization of Definition 4.2.1.

Proposition 4.2.1 *[36] Let K be a number field and let C be a non-zero fractional ideal of K. If C is an Euclidean ideal, then C' is also an Euclidean ideal for any C' in the ideal class $[C]$ in Cl_K.*

Proof. Since $C' \in [C]$, there exists $\delta \in K \setminus \{0\}$ such that $C' = \delta \cdot C$. Let J be a fractional ideal containing $\mathcal{O}_K$ and let x' be an element of $JC' \setminus C'$. Then $x' = \delta \cdot x$ for some $x \in JC \setminus C$. Since C is an Euclidean ideal, there exists a function $\psi : \mathbb{I} \to W$ and an element $y \in C$ satisfying $\psi((x-y)^{-1}JC) < \psi(J)$.

Since $C' = \delta \cdot C$ and $y \in C$, we have $y' = \delta \cdot y \in \delta \cdot C = C'$. Hence

$$\psi((x'-y')^{-1}JC') = \psi((\delta \cdot x - \delta \cdot y)^{-1}J\delta \cdot C) = \psi((x-y)^{-1}JC) < \psi(J).$$

Thus, C' is also an Euclidean ideal. Since C' is an arbitrary element in $[C]$, we conclude that every fractional ideal in the ideal class $[C]$ is Euclidean. □

Proposition 4.2.1 enables us to unambiguously define an *Euclidean ideal class* as follows.

Definition 4.2.3 *An ideal class $[C]$ in Cl_K is said to be an Euclidean ideal class, if C is an Euclidean ideal.*

One of the important consequences of the existence of an Euclidean ideal class in a number field K is that Cl_K is a cyclic group. More precisely, Lenstra [36] proved the following theorem.

Theorem 4.2.2 *[36] Let K be a number field and let C be a non-zero fractional ideal. Assume that $[C]$ is an Euclidean ideal class. Then the class group Cl_K is cyclic. Moreover, $[C]$ generates Cl_K.*

However, the converse of Theorem 4.2.2 is false. Indeed, Lenstra [36] proved that even though the class group of the quadratic field $\mathbb{Q}(\sqrt{-d})$ for $d = 19$, 23, 31, 35, 39, 43, 47 is cyclic, it has no Euclidean ideal class. Therefore, it is natural to ask for the classification of the number fields for which the converse of Theorem 4.2.2 holds. Lenstra [36] proved the converse of Theorem 4.2.2 for a large class of number fields, under the assumption of the *Extended Riemann hypothesis* (abbreviated as ERH). Before stating his result, we briefly recall ERH and *Dirichlet unit theorem* as follows.

For a number field K, we consider the following Dirichlet series

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s},$$

where the sum runs over all the ideals in $\mathcal{O}_K$. Then $\zeta_K(s)$ defines an analytic function in the region $\{s \in \mathbb{C} : Re(s) > 1\}$ and is called the *Dedekind zeta*

function of K. It can be analytically continued to a meromorphic function with a simple pole at $s = 1$.

Conjecture 4.2.3 *(**Extended Riemann hypothesis**) Let K be a number field with the associated Dedekind zeta function ζ_K. Let $s = \sigma + it \in \mathbb{C}$ with $\sigma > 0$ be such that $\zeta_K(s) = 0$. Then $\sigma = \frac{1}{2}$.*

Theorem 4.2.4 *(**Dirichlet unit theorem**) (see [15]) Let K be a number field of degree $n \geq 1$ with r_1 real and r_2 pairs of complex embeddings. Then the multiplicative group $\mathcal{O}_K^*$ is a finitely generated abelian group of rank $r = r_1 + r_2 - 1$.*

Now, we state the result of Lenstra as follows.

Theorem 4.2.5 *[36] Let K be a number field with $rank(\mathcal{O}_K^*) \geq 1$. Then, the ideal class group Cl_K is cyclic if and only if K has an Euclidean ideal class, provided ERH is true.*

In other words, under ERH, the converse of Theorem 4.2.2 holds for all number fields other than $\mathbb{Q}$ and the imaginary quadratic fields.

4.3 Recent developments

Quantitative results related to Euclidean ideal class are of special interest to number theorists. In [17], Graves proved a growth result for certain number fields without the assumption of ERH. More precisely, she proved the following theorem.

Theorem 4.3.1 *[17] Let K be a number field with $|\mathcal{O}_K^*| = \infty$ and let C be a*

non-zero ideal in $\mathcal{O}_K$. *Suppose that the ideal class* $[C]$ *generates* Cl_K *and*

$$|\{\textit{prime ideal } \wp \subset \mathcal{O}_K : N(\wp) \leq x, [\wp] = [C], \pi_\wp \textit{ is onto }\}| \gg \frac{x}{(\log x)^2},$$

where $\pi_\wp : \mathcal{O}_K^* \to (\mathcal{O}_K/\wp)^*$ *is the canonical map. Then* $[C]$ *is an Euclidean ideal class.*

Using Theorem 4.3.1, Graves and Murty [18] unconditionally proved the converse of Theorem 4.2.2 for a large family of number fields.

Theorem 4.3.2 *[18] Let* K *be a number field with* $K/\mathbb{Q}$ *Galois and* Cl_K *cyclic. Let* $H(K)$ *be the Hilbert class field of* K. *Assume that* $H(K)$ *is Galois over* $\mathbb{Q}$ *with the Galois group* $Gal(H(K)/\mathbb{Q})$ *abelian. If rank* $(\mathcal{O}_K^*) \geq 4$, *then*

$$Cl_K = \langle [C] \rangle \textit{ if and only if } [C] \textit{ is an Euclidean ideal class .}$$

We observe that one of the most crucial hypotheses in Theorem 4.3.2 is $rank(\mathcal{O}_K^*) \geq 4$. In [16], Graves gave the first example of a number field K with $rank(\mathcal{O}_K^*) = 3$ such that K has a non-principal Euclidean ideal class.

Theorem 4.3.3 *[16] The number field* $\mathbb{Q}(\sqrt{2}, \sqrt{35})$ *has a non-principal Euclidean ideal class.*

Later, Hsu [23] provided a family of quartic number fields, each having a non-principal Euclidean ideal class. More precisely, she proved the following theorems.

Theorem 4.3.4 *[23] Let* q, k *and* $r \geq 29$ *be distinct prime numbers with* $q \equiv k \equiv r \equiv 1 \pmod 4$. *Let* $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ *and assume that* $h_K = 2$. *Then* K *has a non-principal Euclidean ideal class.*

Theorem 4.3.5 *[23] Let $q, k \geq 17$ be distinct prime numbers with $q \equiv k \equiv 1 \pmod 4$. Let $b > 0$ be an integer such that $b \equiv 0 \pmod 4$ and $k - b^2 > 0$ is a perfect square. Consider the number field $K = \mathbb{Q}\left(\sqrt{q(k + b\sqrt{k})}\right)$. If $h_K = 2$, then K has a non-principal Euclidean ideal class.*

Remark 4.3.1 *$h_K = 2$ is equivalent to the fact that $Cl_K \simeq \mathbb{Z}/2\mathbb{Z}$. In other words, Cl_K is cyclic. Thus Theorem 4.3.4 and Theorem 4.3.5 affirmatively answers the converse of Theorem 4.2.2 for a certain family of quartic fields. In [23], Hsu also conjectured that the families considered in Theorem 4.3.4 and Theorem 4.3.5 are both infinite.*

4.4 Statements of our main theorems

Our results extend the family of number fields considered in Theorem 4.3.3 and Theorem 4.3.4. More precisely, the statements of our main theorems are as follows.

Theorem 4.4.1 *[10] Let $q \geq 3, k \geq 5$ and $r \geq 5$ be distinct prime numbers with $q \equiv 3 \pmod 4$ and $k \equiv r \equiv 1 \pmod 4$. Consider the bi-quadratic field $K_1 = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$. If $h_{K_1} = 2$, then K_1 has a non-principal Euclidean ideal class.*

Theorem 4.4.2 *[10] Let $p \geq 5$ and $q \geq 5$ be two distinct prime numbers with $p \equiv q \equiv 1 \pmod 4$. Consider the bi-quadratic field $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$. If $h_{K_2} = 2$, then K_2 has a non-principal Euclidean ideal class.*

By combining Theorem 4.3.4 and Theorem 4.4.1, we have a larger family of bi-quadratic fields with an Euclidean ideal class as follows.

Theorem 4.4.3 *[10] Let $p \geq 2, q \geq 5$ and $r \geq 5$ be distinct prime numbers*

with $q \equiv r \equiv 1 \pmod 4$. *Consider the bi-quadratic field* $K = \mathbb{Q}(\sqrt{p}, \sqrt{qr})$. *If* $h_K = 2$, *then* K *has a non-principal Euclidean ideal class.*

In the end of this chapter, we provide a list of bi-quadratic fields with class number 2 which have an Euclidean ideal class.

4.5 Preliminaries

To prove Theorem 4.4.1 and Theorem 4.4.2, we need to compute the *conductor* and the Hilbert class field of K_1 and K_2. To define the conductor, we start with the *Kronecker-Weber theorem.*

Theorem 4.5.1 *[13] Let* K *be a finite abelian extension of* $\mathbb{Q}$ *with Galois group* $Gal(K/\mathbb{Q})$. *Then* $K \subseteq \mathbb{Q}(\zeta_m)$ *for some integer* $m \geq 1$, *where* ζ_m *is a primitive* m^{th} *root of unity.*

Definition 4.5.1 *[13] Let* K *be a finite abelian extension of* $\mathbb{Q}$. *Then the least positive integer* m *such that* $K \subseteq \mathbb{Q}(\zeta_m)$ *is called the conductor of* K.

For the rest of this chapter, we denote the conductor of a number field K by $\mathfrak{f}(K)$. The following well-known proposition provides us the conductor of certain quadratic fields and can be found in [40].

Proposition 4.5.2 *[40] Let* p *be an odd prime number and let* $K = \mathbb{Q}(\sqrt{p})$. *Then*

$$\mathfrak{f}(K) = \begin{cases} p & ; \text{ if } p \equiv 1 \pmod 4, \\ 4p & ; \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

Also, the conductor of $\mathbb{Q}(\sqrt{2})$ *is* 8.

Now, we recall some standard results from algebraic number theory.

Lemma 4.5.3 *[13] Let K_1 and K_2 be number fields and let $L = K_1K_2$ be the compositum. Let p be a prime number. If p is unramified in both K_1 and K_2, then p is unramified in L.*

Earlier, we had defined the Hilbert class field of a number field K as the maximal, abelian, unramfied extension of K. We provide another equivalent formulation of $H(K)$ as follows.

Proposition 4.5.4 *[13] Let K be a number field. Then the Hilbert class field $H(K)$ of K is the unique maximal, abelian extension of K such that precisely the principal prime ideals of $\mathcal{O}_K$ split completely in $\mathcal{O}_{H(K)}$.*

Proposition 4.5.5 *[13] Let $K \subseteq L$ be number fields such that L/K Galois with Galois group G. Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$ which is unramified in L and let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then there is a unique element $\sigma \in G$ such that for all $\alpha \in \mathcal{O}_L$, we have*

$$\sigma(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}.$$

Proposition 4.5.5 enables us to define the *Artin symbol*.

Definition 4.5.2 *[13] The unique element σ in Proposition 4.5.5 is called the Artin symbol and is usually denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$.*

Suppose $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are all the prime ideals in $\mathcal{O}_L$ lying above $\mathfrak{p}$. For any $\tau \in G$, it is easy to see that

$$\left(\frac{L/K}{\tau(\mathfrak{P}_i)}\right) = \tau \left(\frac{L/K}{\mathfrak{P}_i}\right) \tau^{-1} \text{ for all } i \in \{1, \ldots, g\}.$$

Also, it is a well-known fact that G acts transitively on $\{\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g\}$ and hence the set $\left\{\left(\frac{L/K}{\mathfrak{P}_i}\right) : i = 1, 2, \ldots, g\right\}$ is a conjugacy class in G. Thus by

$\left(\frac{L/K}{\mathfrak{p}}\right)$, we unambiguously denote this conjugacy class.

Now, we define the *Dirichlet density* of a set of prime ideals in $\mathcal{O}_K$ as follows.

Definition 4.5.3 *[13] Let K be a number field and let $\mathcal{S}$ be a set of prime ideals in $\mathcal{O}_K$. The Dirichlet density of the set $\mathcal{S}$ is defined to be*

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

provided the limit exists.

Remark 4.5.1 *From Definition 4.5.3, we immediately see that if $\delta(\mathcal{S}) > 0$, then $\mathcal{S}$ is an infinite set.*

Next, we state one of the most important theorems in number theory, namely, the *Chebotarev density theorem.*

Theorem 4.5.6 *(**Chebotarev density theorem**) [13] Let L/K be a finite Galois extension of number fields with Galois group G and let $\mathcal{C}$ be a conjugacy class in G. Then the Dirichlet density of the set*

$$\left\{ \text{prime ideal } \mathfrak{p} \text{ in } \mathcal{O}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C} \right\}$$

exists and equals $\frac{|\mathcal{C}|}{[L:K]}$.

In order to compute the conductors of the required bi-quadratic fields, we need the following basic lemmas.

Lemma 4.5.7 *[10] Let L/K be a finite extension of number fields. Assume that L is an abelian extension of $\mathbb{Q}$. Then $\mathfrak{f}(K)$ divides $\mathfrak{f}(L)$.*

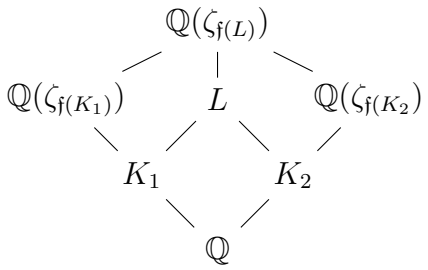
Proof. Since L is an abelian extension of $\mathbb{Q}$ and $K \subseteq L$, using the fundamental theorem of Galois theory, we see that K is also a Galois extension of $\mathbb{Q}$ with $Gal(K/\mathbb{Q}) \simeq Gal(L/\mathbb{Q})/Gal(L/K)$. Therefore, K is an abelian extension of $\mathbb{Q}$ and hence both $\mathfrak{f}(K)$ and $\mathfrak{f}(L)$ are well-defined. Now, since $K \subseteq L$, using Theorem 4.5.1, we have $K \subseteq L \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(L)})$. Also, by Definition 4.5.1, $\mathfrak{f}(K)$ is the smallest positive integer such that $K \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(K)})$. Thus we get

$$K \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(K)}) \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(L)}).$$

Since both $\zeta_{\mathfrak{f}(K)}$ and $\zeta_{\mathfrak{f}(L)}$ are primitive roots of unity and $\mathbb{Q}(\zeta_{\mathfrak{f}(K)}) \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(L)})$, we conclude that $\mathfrak{f}(K)$ divides $\mathfrak{f}(L)$. □

Lemma 4.5.8 *Let L be a finite abelian extension of $\mathbb{Q}$. Suppose that K_1 and K_2 are two subfields of L such that $L = K_1K_2$. Then $\mathfrak{f}(L) = \text{lcm } \{\mathfrak{f}(K_1)), \mathfrak{f}(K_2))\}$.*

Proof. We consider the following tower of number fields.



(Fig. 1)

Since $L/\mathbb{Q}$ is abelian and K_1 and K_2 are subfields of L, we see that $\mathfrak{f}(K_1)$, $\mathfrak{f}(K_2)$ and $\mathfrak{f}(L)$ are well-defined. By Lemma 4.5.7, $\mathfrak{f}(K_1)$ divides $\mathfrak{f}(L)$ and $\mathfrak{f}(K_2)$ divides $\mathfrak{f}(L)$. Consequently, lcm $\{\mathfrak{f}(K_1), \mathfrak{f}(K_2)\}$ divides $\mathfrak{f}(L)$.

On the other hand, using the fact $L = K_1K_2$, we obtain

$$L = K_1K_2 \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(K_1)})\mathbb{Q}(\zeta_{\mathfrak{f}(K_2)}) = \mathbb{Q}(\zeta_{\text{ lcm}\{\mathfrak{f}(K_1),\mathfrak{f}(K_2\}}).$$

By the definition of the conductor, we have $L \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}(L)}) \subseteq \mathbb{Q}(\zeta_{\text{lcm}(\mathfrak{f}(K_1),\mathfrak{f}(K_2))})$. Therefore, $\mathfrak{f}(L)$ divides $\text{lcm}(\mathfrak{f}(K_1, \mathfrak{f}(K_2))$ and hence $\mathfrak{f}(L) = \text{lcm}\ \{\mathfrak{f}(K_1), \mathfrak{f}(K_2)\}$.

□

Now, we compute the conductors of a certain family of bi-quadratic fields.

Lemma 4.5.9 *Let q, k and r be prime numbers such that $q \equiv 3 \pmod 4$ and $k \equiv r \equiv 1 \pmod 4$. Then the conductor $\mathfrak{f}(K)$ of $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ is $4qkr$.*

Proof. Let $K_1 = \mathbb{Q}(\sqrt{q})$, $K_2 = \mathbb{Q}(\sqrt{kr})$, $K_3 = \mathbb{Q}(\sqrt{k})$ and $K_4 = \mathbb{Q}(\sqrt{r})$. By Proposition 4.5.2, we have $\mathfrak{f}(K_1) = 4q$, $\mathfrak{f}(K_3) = k$ and $\mathfrak{f}(K_4) = r$. Since $K_2 \subseteq K_3K_4 \subseteq \mathbb{Q}(\zeta_k)\mathbb{Q}(\zeta_r) = \mathbb{Q}(\zeta_{kr})$, using Lemma 4.5.7, we get $\mathfrak{f}(K_2) \mid kr$. This implies that $\mathfrak{f}(K_2) = k$ or r or kr. As $k \equiv 1 \pmod 4$ and $r \equiv 1 \pmod 4$ are distinct prime numbers, the only quadratic subfields of $\mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\zeta_r)$ are $\mathbb{Q}(\sqrt{k})$ and $\mathbb{Q}(\sqrt{r})$, respectively. Hence $\mathfrak{f}(K_2) = kr$.

Now, since $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr}) = K_1K_2$, using Lemma 4.5.8, we conclude that

$$\mathfrak{f}(K) = \text{lcm}\{\mathfrak{f}(K_1), \mathfrak{f}(K_2)\} = \text{lcm}\{4q, kr\} = 4qkr.$$

□

Lemma 4.5.10 *Let p and q be two prime numbers with $p \equiv q \equiv 1 \pmod 4$. Then the conductor $\mathfrak{f}(K)$ of $K = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$ is $8pq$.*

Proof. Let $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt{pq})$. By Proposition 4.5.2, we have $\mathfrak{f}(K_1) = 8$. Also, by similar arguments used in the proof of Lemma 4.5.9, we obtain $\mathfrak{f}(K_2) = pq$. Thus we get

$$\mathfrak{f}(K) = \text{lcm}\{\mathfrak{f}(K_1), \mathfrak{f}(K_2)\} = \text{lcm}\{8, pq\} = 8pq.$$

□

Remark 4.5.2 *It is worthwhile to note that the map $\pi_{\wp}$ in Theorem 4.3.1 is not always surjective for any number field K. For instance, if $K = \mathbb{Q}$ and $\wp = 5\mathbb{Z}$, the map $\pi_{\wp} : \mathbb{Z}^* \to (\mathbb{Z}/5\mathbb{Z})^*$ is not onto. We denote an onto map by the symbol "$\twoheadrightarrow$".*

In view of Remark 4.5.2, it is useful to have conditions on the number field K for which $\pi_{\wp}$ is onto. The following theorem, mentioned in [16], deals with this property.

Theorem 4.5.11 *[16] Let K be a totally real number field with conductor $\mathfrak{f}(K)$ and let $\{e_1, e_2, e_3\}$ be a multiplicatively independent set contained in $\mathcal{O}_K^*$. If $l = lcm\{16, \mathfrak{f}(K)\}$, and if $gcd(u, l) = gcd(\frac{u-1}{2}, l) = 1$ for some integer u, then*

$$\left|\left\{\substack{primes\ \wp\subseteq\mathcal{O}_K \\ of\ degree\ one} : N(\wp) \equiv u \ (mod\ l), N(\wp) \leq x, \langle -1, e_i\rangle \twoheadrightarrow (\mathcal{O}_K/\wp)^*\right\}\right| \gg \frac{x}{(\log x)^2},$$

for some $i \in \{1, 2, 3\}$.

Remark 4.5.3 *We immediately see that, whenever the canonical map $\langle -1, e_i\rangle \twoheadrightarrow (\mathcal{O}_K/\wp)^*$ is surjective, the map $\pi_{\wp}$ is also surjective. Using this observation, we make use of the growth result in Theorem 4.5.11 to prove our main theorems.*

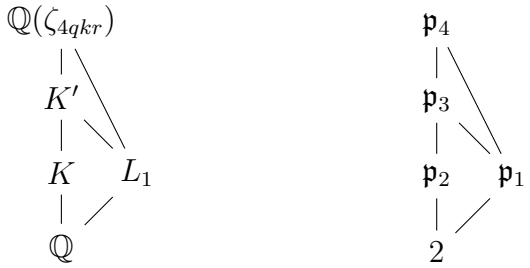
Next, we compute the Hilbert class fields of bi-quadratic fields of our interest.

Lemma 4.5.12 *Let $q \geq 3, k \geq 5$ and $r \geq 5$ be prime numbers with $q \equiv 3 \pmod 4$ and $k \equiv r \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$. If $h_K = 2$, then the Hilbert class field $H(K)$ of K is $\mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$.*

Proof. Let $K' = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$, $K_1 = \mathbb{Q}(\sqrt{q})$, $K_2 = \mathbb{Q}(\sqrt{k})$, $K_3 = \mathbb{Q}(\sqrt{r})$ and $L_1 = \mathbb{Q}(\sqrt{k}, \sqrt{r})$. Since $L_1 = K_2K_3$, using Lemma 4.5.8, we get $\mathfrak{f}(L_1) = \text{lcm}\{\mathfrak{f}(K_2), \mathfrak{f}(K_3)\} = \text{lcm}\{k, r\} = kr$. Again, using $K' = K_1L_1$ and Lemma

4.5.8, we have $\mathfrak{f}(K') = \operatorname{lcm}\{\mathfrak{f}(K_1), \mathfrak{f}(L_1)\} = 4qkr$. Thus K and K' have the same conductor.

By our hypothesis, $h_K = 2$ and therefore, $H(K)$ is a quadratic extension of K. Since K' is also a quadratic extension of K, we conclude that $H(K) = K'$, provided K'/K is unramified. Since $\mathbb{Q} \subsetneq K \subsetneq K' \subsetneq \mathbb{Q}(\zeta_{4qkr})$, the prime ideals in $\mathcal{O}_K$ lying above $2, q, k$ and r may ramify in K'. We first prove that 2 is unramified in K'/K. For that, we consider the following diagram.



(Fig. 2)

Let $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_4$ be primes in $\mathcal{O}_{L_1}$, $\mathcal{O}_K$, $\mathcal{O}_{K'}$ and $\mathbb{Z}[\zeta_{4qkr}]$ respectively, all lying above 2. Since $k \equiv r \equiv 1 \pmod 4$, the prime 2 is unramified in $\mathbb{Q}(\sqrt{k})$ and $\mathbb{Q}(\sqrt{r})$ and hence in the compositum field L_1. In other words, the ramification index $e(\mathfrak{p}_1|2) = 1$. Since $q \equiv 3 \pmod 4$, the prime 2 is ramified in $\mathbb{Q}(\sqrt{q})$. As $\mathbb{Q}(\sqrt{q}) \subseteq K \subseteq K'$, we have $e(\mathfrak{p}_2|2) > 1$ and $e(\mathfrak{p}_3|2) > 1$. Thus from the multiplicativity of the ramification indices, we get,

$$1 < e(\mathfrak{p}_3|2) = e(\mathfrak{p}_3|\mathfrak{p}_1)e(\mathfrak{p}_1|2) \leq 2 \cdot 1.$$

Thus, $e(\mathfrak{p}_3|2) = 2$ and $e(\mathfrak{p}_2|2) = 2$. Consequently, $e(\mathfrak{p}_3|\mathfrak{p}_2) = \frac{e(\mathfrak{p}_3|2)}{e(\mathfrak{p}_2|2)} = 1$. That is, $\mathfrak{p}_3$ is unramified over $\mathfrak{p}_2$.

We immediately see that by replacing the prime 2 by the prime q, the same argument given above yields that q is unramified for K'/K. Similarly, by replacing L_1 with $L_2 = \mathbb{Q}(\sqrt{q}, \sqrt{r})$ and $L_3 = \mathbb{Q}(\sqrt{k}, \sqrt{q})$, we obtain the unram-

ifiedness of the primes k and r, respectively. Therefore, all the prime ideals in $\mathcal{O}_K$ lying above the rational primes $2, q, k$ and r are unramified in K'. Since q, k and r are all positive integers, the infinite primes are also unramified. Hence, $H(K) = K' = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$. □

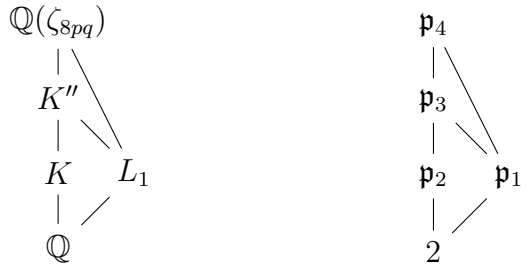
Lemma 4.5.13 *Let $p \geq 5$ and $q \geq 5$ be two prime numbers with $p \equiv q \equiv 1 \pmod 4$. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$. If $h_K = 2$, then the Hilbert class field $H(K)$ of K is $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$.*

Proof. Let $K'' = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$, $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{p})$, $K_3 = \mathbb{Q}(\sqrt{q})$ and $L_1 = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Since $L_1 = K_2K_3$, by using Lemma 4.5.8, we have $\mathfrak{f}(L_1) = \operatorname{lcm}\{\mathfrak{f}(K_2), \mathfrak{f}(K_3)\} = \operatorname{lcm}\{p, q\} = pq$. Since $\mathfrak{f}(K_1) = 8$ and $K'' = K_1L_1$, using Lemma 4.5.8, we conclude that $\mathfrak{f}(K'') = \operatorname{lcm}\{\mathfrak{f}(K_1), \mathfrak{f}(L_1)\} = \operatorname{lcm}\{8, pq\} = 8pq$. Thus the conductors of K and K'' are equal.

Claim. K'' is an unramified extension of K.

Since $\mathbb{Q} \subsetneq K \subsetneq K'' \subsetneq \mathbb{Q}(\zeta_{8pq})$, it is enough to prove that the primes lying above $2, p$ and q in K are unramified in K''. In the following, we provide a detailed proof of the fact that 2 is unramified in K''/K. The argument is essentially same for the primes p and q and therefore we omit it.

Consider the following diagram.



(Fig. 3)

Let $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_4$ be primes in $\mathcal{O}_{L_1}$, $\mathcal{O}_K$, $\mathcal{O}_{K''}$ and $\mathbb{Z}[\zeta_{8pq}]$ respectively, all lying above 2. Since $p \equiv q \equiv 1 \pmod 4$, the prime 2 is unramified in K_2

and K_3. By Lemma 4.5.3, the prime 2 is unramified in L_1. In other words, the ramification index $e(\mathfrak{p}_1|2) = 1$. On the other hand, since 2 is ramified in $\mathbb{Q}(\sqrt{2})$, it is also ramified in K. That is, $e(\mathfrak{p}_2|2) = 2$. Hence we get

$$2 = e(\mathfrak{p}_2|2) \leq e(\mathfrak{p}_3|2) = e(\mathfrak{p}_3|\mathfrak{p}_1) \cdot e(\mathfrak{p}_1|2) = e(\mathfrak{p}_3|\mathfrak{p}_1) \leq [K'' : L_1] = 2. \quad (4.2)$$

Therefore, equality holds throughout in (4.2) and consequently, $e(\mathfrak{p}_3|2) = 2$. Hence $e(\mathfrak{p}_3|\mathfrak{p}_2) = \frac{e(\mathfrak{p}_3|2)}{e(\mathfrak{p}_2|2)} = 1$. Thus 2 is unramified in K''/K.

Since p and q are positive integers, the infinite primes of K are also unramified in K''. This proves the claim.

Since K'' is a quadratic, unramified extension of K, we have $K'' \subseteq H(K)$. As $h_K = 2$, we have $[H(K) : K] = 2$ and therefore, we can conclude that $K'' = H(K)$. Thus the Hilbert class field $H(K)$ of K is $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$. □

4.6 Proof of Theorem 4.4.1

For prime numbers $q \geq 3$, $k \geq 5$ and $r \geq 5$ with $q \equiv 3 \pmod 4$ and $k \equiv r \equiv 1 \pmod 4$, let $K_1 = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ be the bi-quadratic field. By Lemma 4.5.9 and Lemma 4.5.12, we have $\mathfrak{f}(K_1) = 4qkr$ and $H(K_1) = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$. Also, since q, k and r are all positive, the number field K_1 is totally real with 4 real embeddings. Therefore, $\text{rank}(\mathcal{O}_{K_1}^*) = 3$ and hence there exist 3 multiplicatively independent elements in $(\mathcal{O}_{K_1}^*)$.

For a prime number p, let $\mathfrak{p}$ and $\wp$ be the prime ideals in $\mathcal{O}_{K_1}$ and $\mathcal{O}_{H(K_1)}$, respectively, lying above p.

Claim 1. There exists an integer u such that for all prime numbers p with $p \equiv u \pmod{4qkr}$, we have $f(\mathfrak{p}|p) = 1$ and $f(\wp|p) = 2$.

To prove the claim, let $\left(\frac{p}{K_1/\mathbb{Q}}\right)$ and $\left(\frac{p}{H(K_1)/\mathbb{Q}}\right)$ be the Artin symbols of the prime p in the number field K_1 and $H(K_1)$, respectively. We consider the

following two sets of prime numbers in $\mathbb{Z}$.

$$X_{K_1} = \left\{ p : p \text{ is prime and } \left(\frac{p}{K_1/\mathbb{Q}} \right) = 1 \right\},$$

and

$$X_{H(K_1)} = \left\{ p : p \text{ is prime and } \left(\frac{p}{H(K_1)/\mathbb{Q}} \right) = 1 \right\}.$$

In other words, X_{K_1} (respectively, $X_{H(K_1)}$) consists of all the prime numbers that split completely in K_1 (respectively, $H(K_1)$). Since $K_1 \subseteq H(K_1)$ and the ramification indices and residual degrees are multiplicative, it immediately follows that if a prime p splits completely in $H(K_1)$, then it splits completely in K_1. That is, $X_{H(K_1)} \subseteq X_{K_1}$.

Now, since both $Gal(K_1/\mathbb{Q})$ and $Gal(H(K_1)/\mathbb{Q})$ are abelian, every conjugacy class is singleton. In particular, the identity element constitutes a conjugacy class. Therefore, by Theorem 4.5.6, the Dirichlet densities of the sets X_{K_1} and $X_{H(K_1)}$ are $\frac{1}{4}$ and $\frac{1}{8}$, respectively. Since $X_{H(K_1)} \subseteq X_{K_1}$, the Dirichlet density of the set $X_{K_1} \setminus X_{H(K_1)}$ is $\frac{1}{4} - \frac{1}{8} = \frac{1}{8}$. In other words, $X_{K_1} \setminus X_{H(K_1)}$ is an infinite set. We choose a prime number $u \in X_{K_1} \setminus X_{H(K_1)}$. Then any prime lying above u has residual degree 1 in K_1 and 2 in $H(K_1)$. Since both K_1 and $H(K_1)$ are abelian extensions of $\mathbb{Q}$ with conductor $4qkr$, we conclude that for any prime number p with $p \equiv u \pmod{4qkr}$, we have $f(\mathfrak{p}|p) = 1$ and $f(\wp|p) = 2$. This proves the claim.

Now, we study the set $X_{K_1} \setminus X_{H(K_1)}$ more closely as follows.

Claim 2. $X_{K_1} \setminus X_{H(K_1)} = \left\{ p : p \text{ is prime and } \left(\frac{q}{p} \right) = 1 \text{ and } \left(\frac{k}{p} \right) = \left(\frac{r}{p} \right) = -1 \right\}$, where $\left(\frac{\cdot}{p} \right)$ is the Legendre symbol.

To prove the claim, let $p \in X_{K_1} \setminus X_{H(K_1)}$. Then p splits completely in K_1 but not in $H(K_1)$. We note that, p splits completely in $K_1 = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ if and only if p splits completely in both $\mathbb{Q}(\sqrt{q})$ and in $\mathbb{Q}(\sqrt{kr})$. In other words, p

splits completely in $K_1 = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ if and only if $\left(\frac{q}{p}\right) = 1$ and $\left(\frac{kr}{p}\right) = 1$. On the other hand, p does not split completely in $H(K_1) = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$ if and only if p does not split completely in one of the fields $\mathbb{Q}(\sqrt{q})$ or $\mathbb{Q}(\sqrt{k})$ or $\mathbb{Q}(\sqrt{r})$. Thus, we get

$$\left(\frac{q}{p}\right) = 1, \left(\frac{k}{p}\right) = -1 \text{ and } \left(\frac{r}{p}\right) = -1.$$

Conversely, let p be a prime number such that $\left(\frac{q}{p}\right) = 1, \left(\frac{k}{p}\right) = -1$ and $\left(\frac{r}{p}\right) = -1$. Then p splits completely in $\mathbb{Q}(\sqrt{q})$. Also, since $\left(\frac{kr}{p}\right) = 1$, we have that p also splits completely in $\mathbb{Q}(\sqrt{kr})$. Thus p splits completely in $K_1 = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ but not in $H(K_1) = \mathbb{Q}(\sqrt{q}, \sqrt{k}, \sqrt{r})$. That is $p \in X_{K_1} \setminus X_{H(K_1)}$ and this proves the claim.

Let $l = \text{lcm}\{16, \mathfrak{f}(K_1)\} = \text{lcm}\{16, 4qkr\} = 16qkr$. To apply Theorem 4.5.11, we need to find an integer u satisfying the properties in Claim 1 along with

$$(i) \ \gcd(u, 16qkr) = 1, \tag{4.3}$$

and

$$(ii) \ \gcd\left(\frac{u-1}{2}, 16qkr\right) = 1. \tag{4.4}$$

We note that the condition (ii) above is equivalent to the following simultaneous congruences.

$$\begin{cases} u \not\equiv 1 \pmod{q}, \\ u \not\equiv 1 \pmod{r}, \\ u \not\equiv 1 \pmod{k}, \\ u \not\equiv 1 \pmod{4}. \end{cases}$$

In other words, it is enough to find an element $w \in X_{K_1} \setminus X_{H(K_1)}$ satisfying (4.3)

and (4.4). For that, we choose prime numbers $p_1 < q$, $p_2 < k$ and $p_3 < r$ such that

$$\left(\frac{p_1}{q}\right) = -1, \left(\frac{p_2}{k}\right) = -1 \text{ and } \left(\frac{p_3}{r}\right) = -1.$$

Next, we consider the following set of congruence.

$$\begin{cases} u \not\equiv 1 \pmod{q}; \\ u \not\equiv 1 \pmod{r}; \\ u \not\equiv 1 \pmod{k}; \\ u \not\equiv 1 \pmod{4}. \end{cases}$$

Since q, k and r are distinct odd prime numbers, the modulii in the above set of congruences are pairwise relatively prime. Therefore, by the Chinese remainder theorem, there exist a unique solution x_0 modulo $4qkr$. Also, since $\gcd(x_0, 4qkr) = 1$, by Dirichlet's theorem for primes in arithmetic progressions, there exists infinitely many prime numbers $w \equiv x_0 \pmod{4qkr}$. We pick one such prime w. Then it follows that w satisfies (4.3) and (4.4). It only remains to prove that $w \in X_{K_1} \setminus X_{H(K_1)}$. For that, using the law of quadratic reciprocity, we get

$$\left(\frac{q}{w}\right) = \left(\frac{w}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{w-1}{2}} = -\left(\frac{w}{q}\right) = -\left(\frac{p_1}{q}\right) = 1,$$

$$\left(\frac{k}{w}\right) = \left(\frac{w}{k}\right)(-1)^{\frac{k-1}{2}\cdot\frac{w-1}{2}} = \left(\frac{w}{k}\right) = \left(\frac{p_2}{k}\right) = -1$$

and

$$\left(\frac{r}{w}\right) = \left(\frac{w}{r}\right)(-1)^{\frac{r-1}{2}\cdot\frac{w-1}{2}} = \left(\frac{w}{r}\right) = \left(\frac{p_3}{r}\right) = -1.$$

Thus, by using Claim 2, we get that $w \in X_{K_1} \setminus X_{H(K_1)}$.

Let $\mathfrak{p}$ and $\wp$ be prime ideals in $\mathcal{O}_{K_1}$ and $\mathcal{O}_{H(K_1)}$, respectively, lying above w. Since $w \in X_{K_1} \setminus X_{H(K_1)}$, we conclude that $\mathfrak{p}$ does not split completely in

$H(K_1)$. Consequently, using Proposition 4.5.4, we get that $\mathfrak{p}$ is not a principal ideal. Since $h_{K_1} = 2$ and $\mathfrak{p}$ is non-principal, we get that $\langle[\mathfrak{p}]\rangle = Cl_{K_1}$. Hence by Theorem 4.3.1, we conclude that $[\mathfrak{p}]$ is a non-principal Euclidean ideal class. □

4.7 Proof of Theorem 4.4.2

For prime numbers $p \geq 5$ and $q \geq 5$ with $p \equiv q \equiv 1 \pmod 4$, let $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$ be the bi-quadratic field. By Lemma 4.5.10 and Lemma 4.5.13, we have $\mathfrak{f}(K_2) = 8pq$ and $H(K_2) = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$. Also, since p and q are positive, the number field K_2 is totally real with 4 real embeddings. Therefore, $\text{rank}(\mathcal{O}_{K_2}^*) = 3$ and hence there exist 3 multiplicatively independent elements in $(\mathcal{O}_{K_2}^*)$.

Let us define the following sets.

$$X_{K_2} = \left\{\ell : \ell \text{ is prime and } \left(\frac{\ell}{K_2/\mathbb{Q}}\right) = 1\right\},$$

and

$$X_{H(K_2)} = \left\{\ell : \ell \text{ is prime and } \left(\frac{\ell}{H(K_2)/\mathbb{Q}}\right) = 1\right\}.$$

Claim 3. $X_{K_2} \backslash X_{H(K_2)} = \left\{\ell : \ell \text{ is prime and } \left(\frac{2}{\ell}\right) = 1 \text{ and } \left(\frac{p}{\ell}\right) = \left(\frac{q}{\ell}\right) = -1\right\}$.

To see this, let $\ell \in X_{K_2} \setminus X_{H(K_2)}$. Then ℓ splits completely in K_2 but not in $H(K_2)$. Now, ℓ splits completely in $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$ if and only if ℓ splits completely in both $\mathbb{Q}(\sqrt{2})$ and in $\mathbb{Q}(\sqrt{pq})$. That is, $\left(\frac{2}{\ell}\right) = 1$ and $\left(\frac{pq}{\ell}\right) = 1$. On the other hand, ℓ does not split completely in $H(K_2) = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q})$ if and only if ℓ does not split completely in one of the fields $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{q})$. Thus we have

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

Conversely, let ℓ be a prime number such that $\left(\frac{2}{\ell}\right) = 1$ and $\left(\frac{p}{\ell}\right) = \left(\frac{q}{\ell}\right) = -1$. Then we have $\left(\frac{pq}{\ell}\right) = 1$. Consequently, ℓ splits completely in $\mathbb{Q}(\sqrt{2})$ and in $\mathbb{Q}(\sqrt{pq})$ and hence in K_2. But since $\left(\frac{p}{\ell}\right) = \left(\frac{q}{\ell}\right) = -1$, we get that ℓ does not split completely in $H(K_2)$. Therefore, $\ell \in X_{K_2} \setminus X_{H(K_2)}$. This completes the proof of Claim 3.

Now, let $l = \operatorname{lcm}\{16, \mathfrak{f}(K_2)\} = \operatorname{lcm}\{16, 8pq\} = 16pq$. We need to find an integer u such that the following two conditions hold.

$$\gcd(u, 16pq) = 1 \tag{4.5}$$

and

$$\gcd\left(\frac{u-1}{2}, 16pq\right) = 1. \tag{4.6}$$

We note that equation (4.6) is equivalent to the following equivalent conditions.

$$\begin{cases} u \not\equiv 1 \pmod{p}; \\ u \not\equiv 1 \pmod{q}; \\ u \not\equiv 1 \pmod{4}. \end{cases}$$

Now, we choose prime numbers p_1 and p_2 such that

$$p_1 < p, p_2 < q \text{ and } \left(\frac{p_1}{p}\right) = \left(\frac{p_2}{q}\right) = -1$$

and consider the following set of congruence.

$$\begin{cases} x \equiv p_1 \pmod{p}; \\ x \equiv p_2 \pmod{q}; \\ x \equiv 7 \pmod{8}. \end{cases} \tag{4.7}$$

Since p and q are distinct odd prime numbers, the modulii in (4.7) are pair-

wise relatively prime. Therefore, by the Chinese remainder theorem, there exists a unique solution x_0 modulo $8pq$. Since $\gcd(x_0, 8pq) = 1$, by Dirichlet's theorem for primes in arithmetic progressions, there exist infinitely many prime numbers $w \equiv x_0 \pmod{8pq}$. For such a prime number w, using the law of quadratic reciprocity and the fact that $p \equiv q \equiv 1 \pmod 4$, we get

$$\left(\frac{p}{w}\right) = \left(\frac{w}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{w-1}{2}} = \left(\frac{w}{p}\right) = \left(\frac{x_0}{p}\right) = \left(\frac{p_1}{p}\right) = -1,$$

and

$$\left(\frac{q}{w}\right) = \left(\frac{w}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{w-1}{2}} = \left(\frac{w}{q}\right) = \left(\frac{x_0}{q}\right) = \left(\frac{p_2}{p}\right) = -1.$$

Let $\mathfrak{p}$ and $\wp$ be prime ideals in $\mathcal{O}_{K_2}$ and $\mathcal{O}_{H(K_2)}$, respectively, lying above w. Since $w \in X_{K_2} \setminus X_{H(K_2)}$, we conclude that $\mathfrak{p}$ does not split completely in $H(K_2)$. Consequently, using Proposition 4.5.4, we get that $\mathfrak{p}$ is not a principal ideal. Since $h_{K_2} = 2$ and $\mathfrak{p}$ is non-principal, we get that $\langle[\mathfrak{p}]\rangle = Cl_{K_2}$. Hence by Theorem 4.3.1, we conclude that $[\mathfrak{p}]$ is a non-principal Euclidean ideal class. This completes the proof of Theorem 4.4.2. □

In the statements of Theorem 4.4.1 and Theorem 4.4.2, the crucial hypotheses were $h_{K_1} = h_{K_2} = 2$. It is therefore natural to ask the following question.

Question 4.7.1 *Are there any bi-quadratic fields of the form $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$, where $q = 2$ or a prime number with $q \equiv 3 \pmod 4$ and k and r are prime numbers with $k \equiv r \equiv 1 \pmod 4$ such that $h_K = 2$?*

Our computation provides an affirmative answer to Question 4.7.1 as there are plenty of quartic fields of the form $K = \mathbb{Q}(\sqrt{q}, \sqrt{kr})$ with class number 2. We list some of them of our interest together with their class numbers. We have computed the class numbers of the fields using Sage program.

(q,k,r)	h_K	(q,k,r)	h_K	(q,k,r)	h_K	(q,k,r)	h_K
(3, 5, 13)	2	(3, 5, 17)	2	(3, 5, 37)	2	(3, 5, 113)	2
(3, 13, 5)	2	(3, 13, 89)	2	(3, 13, 137)	2	(3, 13, 197)	2
(3, 17, 5)	2	(3, 17, 29)	2	(3, 17, 37)	2	(3, 17, 61)	2
(3, 17, 109)	2	(3, 17, 181)	2	(3, 17, 197)	2	(3, 29, 17)	2
(3, 29, 37)	2	(3, 29, 41)	2	(3, 29, 61)	2	(3, 29, 113)	2

$(2,k,r)$	h_K	$(2,k,r)$	h_K	$(2,k,r)$	h_K	$(2,k,r)$	h_K
(2, 5, 17)	2	(2, 5, 37)	2	(2, 5, 61)	2	(2, 5, 97)	2
(2, 5, 149)	2	(2, 5, 173)	2	(2, 5, 193)	2	(2, 13, 29)	2
(2, 13, 37)	2	(2, 13, 73)	2	(2, 13, 89)	2	(2, 13, 97)	2
(2, 13, 109)	2	(2, 13, 157)	2	(2, 13, 193)	2	(2, 13, 197)	2
(2, 17, 5)	2	(2, 17, 29)	2	(2, 17, 37)	2	(2, 17, 61)	2
(2, 17, 181)	2	(2, 17, 197)	2	(2, 29, 13)	2	(2, 29, 17)	2
(2, 29, 53)	2	(2, 29, 61)	2	(2, 29, 73)	2	(2, 29, 89)	2

Bibliography

[1] N. Ankeny and S. Chowla, *On the divisibility of the class numbers of quadratic fields*, Pacific J. Math., **5** (1955), 321-324.

[2] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York (1984).

[3] A. Baker, Linear forms in the logarithms of algebraic numbers, Mathematika, **13** (1966), 204âĂŞ216.

[4] B. C. Berndt and S. Chowla, *Zero sums of the Legendre symbol*, Nordisk Mat. Tidskr., **22** (1974), 5-8.

[5] D. Byeon, *Real quadratic fields with class number divisible by* 5 *or* 7, Manuscripta Math., **120** (2006) (2) 211-215.

[6] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by* 3, Manuscripta Math., **111** (2003), 261-263.

[7] K. Chakraborty and M. Ram Murty, *On the number of real quadratic fields with class number divisible by* 3, Proc. Amer. Math. Soc., **131** (2002), 41-44.

[8] J. Chattopadhyay, *A short note on the divisibility of class numbers of real quadratic fields*, J. Ramanujan Math. Soc., **34** (2019), 389-392.

[9] J. Chattopadhyay, B. Roy, S. Sarkar and R. Thangadurai, *Distribution of residues modulo p using the Dirichlet's class number formula*, Class Groups of Number Fields and Related Topics, *Springer Nature* (2020), 97-107.

[10] J. Chattopadhyay and M. Subramani, *Biquadratic fields having a non-principal Euclidean ideal class*, J. Number Theory, **204** (2019), 99-112.

[11] J. Chattopadhyay and M. Subramani, *On the simultaneous divisibility of class numbers of triples of imaginary quadratic fields*, Preprint.

[12] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Springer Lect. Notes Math., **1068** (1984), 33-62.

[13] D. A. Cox, *Primes of the Form x^2+ny^2 : Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York (1989).

[14] H. Davenort and H. Heilbronn, *On the density of discriminants of cubic fields,* Proc. Royal Soc. A, **322** (1971), 405-420.

[15] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, Berlin, 2nd edition, (2005).

[16] H. Graves, $\mathbb{Q}(\sqrt{2}, \sqrt{35})$ *has a non-principal Euclidean ideal*, Int. J. Number Theory, **7** (2011), 2269-2271.

[17] H. Graves, *Growth results and Euclidean ideals*, J. Number Theory, **133** (2013), 2756-2769.

[18] H. Graves and M. Ram Murty, *A family of number fields with unit rank at least 4 that has Euclidean ideals*, Proc. Amer. Math. Soc., **141** (2013), 2979-2990.

[19] M. Harper and M. Ram Murty, *Euclidean rings of algebraic integers*, Canad. J. Math., **56** (2004), 71-76.

[20] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z., **56** (1952), 227-253.

[21] H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math., **5** (1934), 150-160.

[22] T. Honda, *On real quadratic fields whose class numbers are multiples of* 3, J.Reine Angew. Math, **223** (1968), 101-102.

[23] C. Hsu, *Two classes of number fields with a non-principal Euclidean ideal*, Int. J. Number Theory, **12** (2016), 1123-1136.

[24] Y. Iizuka, *On the class number divisibility of pairs of imaginary quadratic fields*, J. Number Theory, **184** (2018), 122-127.

[25] Y. Iizuka, Y. Konomi and S. Nakano, *On the class number divisibility of pairs of quadratic fields obtained from points on elliptic curves*, J. Math. Soc. Japan, **68** (2016), 899-915.

[26] Y. Iizuka, Y. Konomi and S. Nakano, *An application of the arithmetic of elliptic curves to the class number problem for quadratic fields*, preprint.

[27] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York (1990).

[28] G.J. Janusz, *Algebraic Number Fields*, Pure and Applied Mathematics, **55**, Academic Press, New York-London, (1973).

[29] W. Johnson and K. J. Mitchell, *Symmetries for sums of the Legendre symbol,* Pacific J. Math., **59** (1977), 117-124.

[30] B. Karaivanov and T. S. Vassilev, *On certain sums involving the Legendre symbol,* Integers, **16** (2016) A14.

[31] Y. Kishi, *On the* 3*-rank of the ideal class group of quadratic fields*, Kodai Math. J., **36** (2013), 275-283.

[32] Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three,* J. Number Theory, **80** (2000), 209-217.

[33] T. Komatsu, *An infinite family of pairs of quadratic fields* $\mathbb{Q}(\sqrt{D})$ *and* $\mathbb{Q}(\sqrt{mD})$ *whose class numbers are both divisible by* 3, Acta Arith., **104** (2002), 129-136.

[34] T. Komatsu, *An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order*, Int. J. Number Theory, **13** (2017), 253-260.

[35] A. Laradji, M. Mignotte and N. Tzanakis, *Elementary trigonometric sums related to quadratic residues,* Elem. Math., **67** (2012) 51-60.

[36] H. W. Lenstra, *Euclidean ideal classes*, Astérisque, **61** (1979), 121-131.

[37] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc., **87** (1983), 579-585.

[38] S. R. Louboutin, *On the divisibility of the class number of imaginary quadratic number fields*, Proc. Amer. Math. Soc., **137** (2009), 4025-4028.

[39] F. Luca, *A note on the divisibility of class numbers of real quadratic fields,* C. R. Math. Acad. Sci. Soc. R. Can, **25** (2003), 71-75.

[40] D.A. Marcus, *Number Fields,* Springer-Verlag, New York, (1977).

[41] H. Montgomery, R. Vaughan, *Multiplicative Number Theory I. Classical Theory.*, Cambridge University Press, Cambridge, (2007).

[42] T. Nagell, *Uber die Klassenzahl imaginar quadratischer Zahkorper,* Abh. Math. Seminar Univ. Hamburg, **1** (1922), 140-150.

[43] W. Narkiewicz, *Units in residue classes*, Arch. Math., **51** (1988), 238-241.

[44] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in Number theory (University Park, PA, (1997) Math. Appl., **467** *Kluwer Acad. Publ., Dordrecht*, (1999), 229-239.

[45] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math., **166** (1932), 201-203.

[46] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., **106**, Springer-Verlag, New York (1986).

[47] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc., **61** (2000), 681-690.

[48] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J., **14** (1967), 1-27.

[49] P. J. Weinberger, *On Euclidean rings of algebraic integers*, Analytic Number Theory, Proceedings of Symposia in Pure Mathematics, **Vol. 24** (American Mathematical Society, Providence, RI, 1973), 321-332.

[50] P. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory, **5** (1973), 237-241.

[51] S. Wright, *Quadratic residues and non-residues: Selected topics,* arXiv:1408.0235v7, (2016).

[52] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields,* Osaka J. Math., **7** (1970), 57-76.

[53] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory, **97** (2002), 35-44.