A Study of Class Number of Real Quadratic and Cubic Fields

DEBOPAM CHAKRABORTY

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781039, INDIA

JUNE 2016

A Study of Class Number of Real Quadratic and Cubic Fields

By

Debopam Chakraborty

Department of Mathematics

Submitted in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Guwahati
Guwahati - 781039, India

June 2016

To

My Parents

Certificate

This is to certify that the thesis entitled *A Study of Class Number of Real Quadratic and Cubic Fields* submitted by *Mr. Debopam Chakraborty* to the Indian Institute of Technology Guwahati, for the award of the Degree of Doctor of Philosophy, is a record of the original bona fide research work carried out by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Guwahati
June 2016

Prof. Anupam Saikia
Supervisor

Acknowledgements

I could complete this thesis with the assistance of various people, whom I would like to thank here.

First and foremost, I would like to thank my supervisor Prof. Anupam Saikia. I am grateful for his encouragement, advice and patience during my research. His love and passion for the subject has been a strong motivation for me throughout my research tenure. Whenever in doubt, I have always looked up to him for inspiration. I would like to thank him for carefully reading my thesis, providing useful feedback and posing interesting questions.

I want to convey my sincere thanks to the doctoral committee of members Dr. Bhaba Kumar Sarma, Dr. K. V. Krishna and Dr. P. A. S. Sree Krishna for reviewing my research work periodically and giving valuable suggestions for the improvements of the same. I sincerely acknowledge Indian Institute of Technology Guwahati for providing me various facilities necessary to carry out my research. I am most grateful to Ministry of Human and Resource Development, Government of India, for providing me financial assistance for the completion of my thesis work. I thank all the technical staff of the department for their assistance in various ways during my research period.

My hearty thanks to all other faculty members of Mathematics department. I specially thank Dr. K. V. Srikanth as I have been deeply inspired by him during my course-work as well as many times after that.

I wish to thank all my friends for their love and encouragement during this period. I owe my thanks to Kaushik, Murali, Kalyan, Barun, Himadri, Arnab, Santu, Nabakanta, Mandar, Chitralekha, Jhuma, Dishari, Saloni, Swarup, Nasim, Abhishek, Anirban, Subhadeep, Shamik, Shyam, Riju, Gopal, Somnath and many others with whom I have shared some of my best moments of my life.

I am deeply indebted to Gayatri for the constant support and inspiration she has been in my life from the day I have started my journey as a research scholar.

Finally, it is not possible for me to adequately express my gratitude towards my parents for everything they have done for me from the very first day of my life. I am grateful for their unconditional love which surrounds me and gives me the strength at every moment of my life.

Abstract

The primary goal of the thesis is to study class number of the ring of integers of a number field and related arithmetical properties.

The first part of the thesis provides a solution to a classical problem posed by Dirichlet in *"Une propriété des formes quadratiques a déterminant positif"*. Dirichlet asked whether exist infinitely many real quadratic fields with 1 as relative class number. It has been shown in the thesis that $\mathbb{Q}(\sqrt{m})$ will always have 1 as relative class number for the conductor 3, whenever m is a prime of the form 3 (mod 4). The thesis also provides a necessary and sufficient condition for a real quadratic field to have relative class number 1. Moreover, the thesis contains significant generalization of the continued fraction approach of A. Furness and E. A. Parker towards relative class number. Using this approach, the thesis also shows the existence of another infinite family of real quadratic fields with relative class number 1 with an odd prime dividing the discriminant as conductor.

The thesis also shows a simple relation between the fundamental unit of a real cubic field and its class number. It shows that the fundamental unit of a real cubic field must satisfy certain congruences if the class number is not divisible by 3. As a consequence of the methods employed, one can obtain classes of real cubic fields of

the form $\mathbb{Q}(\sqrt[3]{m})$ which have class number not divisible by 3. The latter is in agreement with a classical result of F. Gerth stated in terms of the discriminant of the cubic fields. The approach also yields an elementary proof for certain congruence properties satisfied by the fundamental unit of a real quadratic field of odd class number which were recently proved by Z. Zhe and Q. Yue.

The final part of the thesis gives a construction for an unramified quadratic extension of a biquadratic field from a non-torsion point on a suitable elliptic curve. Using the duplication formula, this result also extends the construction for an infinite family of biquadratic fields starting from a non-torsion point on the curve. In particular, every field of this biquadratic family has even class number.

Contents

1

Introduction

The main theme of the thesis is class number of the ring of integers in a number field and related arithmetical properties. A number field is a finite extension of the field of rational numbers $\mathbb{Q}$, and the integral closure of the rational integers in the number field is called its ring of integers. A detailed definition of ideal class group of a number field is given in the next chapter. The order of the ideal class group is defined to be the class number of the number field. Loosely speaking, the class number of a number field describes the deviation of its ring of integers from being a principal ideal domain, or equivalently in this context, a unique factorization domain. The idea of ideal class group had appeared in the theory of quadratic forms even before the term 'ideal' was properly defined. The importance of class group

became more prominent when mathematicians such as Kummer worked towards the solution of the Fermat's Last Theorem and observed that the main hindrance is the failure of unique factorization in the ring of integers of an arbitrary number field.

Gauss was the first to formalize the definition of class group for quadratic number fields. Using the language of binary quadratic forms, Gauss proved in *Disquisitiones Arithmeticae* (Gauss [1966]) that the class number $h(d)$ of quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ is finite. For $d < 0$, he conjectured that

$$h(d) \to \infty \text{ as } d \to -\infty,$$

a result first proved by Heilbronn (Heilbronn [1934]). The *Disquisitiones* also contains tables of binary quadratic forms with small class number which can be viewed as tables of imaginary quadratic fields of small class number. Gauss conjectured that his tables were complete. The problem of finding an effective algorithm to determine all imaginary quadratic fields with a given class number h is known as the Gauss class number h problem. The important milestones in this problem was obtained by Heegner (Heegner [1952]), Stark (Stark et al. [1967], Stark [1971] & Stark [1972]) and Baker (Baker [1971]). The general Gauss class number problem was solved completely by Goldfeld-Gross-Zagier (Goldfeld [1976], Goldfeld [1985], Gross and Zagier [1986]). The last and final conjecture of this famous book is known as class number one problem for real quadratic fields. Gauss conjectured that there are infinitely many real quadratic fields with class number one. In contrast to the conjectures about imaginary quadratic fields described above, this conjecture is still open.

Motivated by Gauss' class number one problem, many people started asking similar questions regarding real quadratic fields, and in some cases number fields with higher degrees. In (Dirichlet [1856]), Dirichlet gave some applications of a formula for the ratio of the class number of a quadratic integral domain in a real field to

the class number of the whole integral domain consisting of all algebraic integers in that field, with the principal objective of showing that this ratio takes many values (such as 1) infinitely often. That ratio is known as the relative class number of a number field. Recently Amanda Furness and E. A. Parker proved the existence of a particular class of real quadratic fields with relative class number 1 (Furness and Parker [2012]).

Several mathematicians have also studied ideal class group of a number field by using arithmetic tools from elliptic curve and the fundamental unit of a number field. T. Honda used elliptic curves to construct infinitely many quadratic fields (both real and imaginary) with class number divisible by 3 (Honda [1960], Honda [1968]). A. Sato gave a geometric interpretation of Honda's work and also extended his results for 5 and 7 (Sato et al. [2011]). R. Soleng gave a construction of quadratic fields from the points of an elliptic curve such that a subgroup of the ideal class group becomes isomorphic to the torsion group of the curve. Soleng's work also gives a divisibility criteria for the class number of those number fields (Soleng [1994]). In (Lemmermeyer [2013]), points on an elliptic curve have been used to discuss the parity of the class number of certain pure cubic fields. In recent work of Z. Zhang and Q. Yue (Zhang and Yue [2014]), the parity of the class number of a real quadratic field has been related to congruence properties satisfied by its fundamental unit.

The first part of the thesis gives affirmative answers to the question posed by Dirichlet on relative class number of real quadratic fields as mentioned above (see Dirichlet [1856]). We also provide a list of congruence properties satisfied by the fundamental unit of a cubic field whose class number is not divisible by 3. Moreover, we give a simpler proof for the main results in (Zhang and Yue [2014]) for real quadratic fields. Motivated by the results mentioned in the previous paragraph relating class number of number fields and points on an elliptic curve, we give an explicit construction of

an unramified quadratic extension of a biquadratic field from a non-torsion point of an elliptic curve. After presenting the necessary preliminaries in Chapter 2, the main results of the thesis have been organized in the following chapters as follows.

Chapter 3 : Relative class number and continued fractions
Chapter 4 : Real quadratic fields with relative class number 1
Chapter 5 : Fundamental unit and the class number
Chapter 6 : A construction for unramified quadratic extension

Chapter 2 contains the fundamental ingredients needed for the latter chapters. It contains the relevant definitions and results that are to be used throughout the thesis. The first part of the chapter briefly discusses the preliminaries concerning class number and class group of a number field. The second part of that chapter briefly covers the basic notions associated with an elliptic curves.

Chapter 3 explores relative class number of real quadratic fields using continued fractions. In (Furness and Parker [2012]), the relative class number of $\mathbb{Q}(\sqrt{m})$ was investigated using continued fraction in the special case when it has a diagonal form. In Chapter 3, we extend that result and show that there exists a conductor f of relative class number 1 whenever the continued fraction of $\sqrt{m}$ is non-diagonal of period 4 or 5. We further show that there exists an infinite family of real quadratic fields with relative class number 1 with an odd prime dividing the discriminant as conductor. In particular, it gives an affirmative answer to Dirichlet's question on relative class number. We also show there will be infinitely many real quadratic fields with any power of 2 as relative class number if there are infinitely many Mersenne primes. The content of Chapter 3 has been published in (Chakraborty and Saikia [2015]).

Chapter 4 contains a a characterization of real quadratic fields with relative class number 1 through an elementary approach considering the cases when the fundamental unit has norm 1 and norm -1 separately. When the fundamental unit has norm -1, we further show that if d is a quadratic non-residue modulo a Mersenne prime f then the conductor f has relative class number 1. We also show that if the fundamental unit has norm -1 and f is a sufficiently large Sophie Germain prime of the first kind such that d is a quadratic residue modulo $2f+1$, then the conductor $2f+1$ has relative class number 1. The results of this chapter have been published in (Chakraborty and Saikia [2014]).

In Chapter 5, we examine congruence relations satisfied by the fundamental unit of a pure cubic field with a power integral basis and relate them to the class number of the number field. As one of the consequences, we show that all real cubic fields $\mathbb{Q}(\sqrt[3]{m})$ where m is an integer congruent to 2, 4, 5 or 7 modulo 9 have class number divisible by 3. Our approach also yields in an elementary way the congruence relations for the fundamental unit of a real quadratic field of odd class number obtained earlier by Z. Zhang and Q. Yue in (Zhang and Yue [2014]). These results have been published in (Chakraborty and Saikia [2016a]).

The results in Chapter 6 are inspired by the work of R. Soleng, A. Sato and most notably F. Lemmermeyer. We give a construction for everywhere unramified quadratic extensions of an infinite family of biquadratic fields by using a non-torsion point on a suitable elliptic curve. In particular, each biquadratic field in the infinite family will have even class number. The extensions are constructed such that their relative discriminant becomes an ideal square and consequently any prime ideal above an odd prime remains unramified. Then the crucial step is to show that any prime above 2 cannot ramify in the constructed quadratic extension. The results of this chapter have been communicated (Chakraborty and Saikia [2016b]).

2 Background

This chapter describes certain basic notions concerning ideal class groups of number fields which will be used through the thesis. It also includes the basic theory of elliptic curves needed for the later part of the thesis.

2.1 Class number and the fundamental units of a number field

We start this section with notion of algebraic numbers and some of their properties. All the topics mentioned in this section can be found in (Stewart and Tall [2015]).

Definition 2.1.1. A complex number α is said to be *algebraic* if it satisfies a non-zero polynomial with coefficients in $\mathbb{Q}$.

The set of algebraic numbers A is a subfield of the complex field $\mathbb{C}$. The degree $[A : \mathbb{Q}]$ is not finite.

Definition 2.1.2. A *number field* is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}]$ is finite.

The following result is often useful for computations on number fields.

Result 2.1.3. *If K is a number field then $K = \mathbb{Q}(\theta)$ for some algebraic number θ. The choice of θ is not unique.*

Example 2.1.4. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$.

If $K = \mathbb{Q}(\theta)$ is a number field then there exist several distinct embeddings (i.e., injective ring homomorphisms) $\sigma : K \to \mathbb{C}$. For instance, $K = \mathbb{Q}(i)$ has two such embeddings, one that fixes i and the other one that takes i to $-i$.
The following theorem describes the different types of monomorphisms a number field may have.

Theorem 2.1.5. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct embeddings $\sigma_i : K \longrightarrow \mathbb{C}$ $(i = 1, 2, ..., n)$. The element $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$.*

The following is the definition of discriminant of a number field which comes from considering a number field as vector space over $\mathbb{Q}$.

Definition 2.1.6. Let $K = \mathbb{Q}(\theta)$ is a number field of degree n, let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a basis of K (as a vector space over $\mathbb{Q}$). The *discriminant* of this basis is defined to be

$$\Delta[\alpha_1, ..., \alpha_n] = \{det[\sigma_i(\alpha_j)]\}^2$$

.

It can easily be proved that the discriminant of any basis for $K = \mathbb{Q}(\theta)$ is rational and non-zero. If all K-conjugates of θ are real, then the discriminant of any basis is positive.

Definition 2.1.7. A complex number θ is said to be an *algebraic integer* if there is a monic polynomial $p(t)$ with integer coefficient such that $p(\theta) = 0$.

Using the following result it can be proved that the ring of algebraic integers, denoted by B is a subring of A, the field of algebraic numbers.

Result 2.1.8. *A complex number θ is and algebraic integer if and only if the additive group generated by all powers $1, \theta, \theta^2, ...$ is finitely generated.*

For any number field K, $\mathcal{O}_K = K \cap B$ is said to be the ring of integers of K. Because it can easily be proved that for any $\alpha \in K$, there always exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_K$, the following results follows as a corollary.

Result 2.1.9. *If K is a number field then $K = \mathbb{Q}(\theta)$ for an algebraic integer θ.*

The ring $\mathcal{O}_K$ of integers of K is an abelian group under addition. A $\mathbb{Z}$-basis for $(\mathcal{O}_K, +)$ is called an integral basis for K (or $\mathcal{O}_K$). If it exists, the order of the integral basis of a number field is same as the order of the $\mathbb{Q}$-basis of that field. The following theorem asserts the existence of integral basis for each number field.

Theorem 2.1.10. *Every number field K possesses an integral basis, and the additive group of $\mathcal{O}_K$ is free abelian of rank n equal to the degree of K.*

Definition 2.1.11. Let K be a number field of degree n and let $\sigma_1, ..., \sigma_n$ be the embeddings $K \longrightarrow \mathbb{C}$. Then for any $\alpha \in K$, the *norm* is defined as

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

and *trace*

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

The following result describes the structure of the ring of integers of a quadratic number field $\mathbb{Q}(\sqrt{d})$.

Theorem 2.1.12. *Let d be a square-free rational integer. Then the integers of $\mathbb{Q}(\sqrt{d})$ are:*

$$\mathbb{Z}[\sqrt{d}], \text{ if } d \not\equiv 1(\ mod\ 4),$$

$$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \text{ if } d \equiv 1(\ mod\ 4).$$

From the above theorem the following result follows immediately.

Result 2.1.13. *If $d \not\equiv 1$ (mod 4) then $\mathbb{Q}(\sqrt{d})$ has an integral basis of the form $\{1, \sqrt{d}\}$ and discriminant $4d$.*
If $d \equiv 1$ (mod 4) then $\mathbb{Q}(\sqrt{d})$ has an integral basis of the form $\{1, \frac{1+\sqrt{d}}{2}\}$ and discriminant d.

As mentioned in the previous section and as also can be seen from the factorization of 6 in $\mathbb{Z}[\sqrt{-5}]$, we know that unique factorization does not hold for the elements of a ring of integer of a number field but the following few results assert that unique factorization does hold for ideals in the ring of integers of number field. We first briefly describe fractional ideals. The idea of the definition comes from the fact that every ideal in $\mathcal{O}_K$ for a number field K can be seen as (finitely generated) $\mathcal{O}_K$-submodule of $\mathcal{O}_K$.

Definition 2.1.14. A finitely generated $\mathcal{O}_K$-submodule γ of K is called a *fractional ideal* of $\mathcal{O}_K$. Equivalently, an $\mathcal{O}_K$-submodule γ of K is called a *fractional ideal* of $\mathcal{O}_K$ if there exists some non-zero $c \in \mathcal{O}_K$, such that $c\gamma \subseteq \mathcal{O}_K$.

While the ideals in $\mathcal{O}_K$ clearly form a semigroup with the whole ring as identity, the existence of an inverse fails for all other ideals. One of the main motivations behind defining fractional ideals is to enlarge the set of ideals in a way so that each ideal becomes invertible in the enlarged set. The following theorem asserts that group

structures can indeed be defined on the set of fractional ideals of a ring of integer of a number field.

Theorem 2.1.15. *The non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication. Moreover, every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

The above theorem implies that the prime factorization in $\mathcal{O}_K$ is unique if all the ideals of $\mathcal{O}_K$ are principal. In order to measure how far prime factorization fails in $\mathcal{O}_K$ or equivalently, how far ideals of $\mathcal{O}_K$ are from being principal ideals, we define the following.

Definition 2.1.16. Let $\mathcal{F}$ be the group of fractional ideals under the multiplication. The set of principal fractional ideals $\mathcal{P}$ is a subgroup of $\mathcal{F}$. The *class group* of $\mathcal{O}_K$ is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The *class number* $h = h(\mathcal{O}_K)$ is defined to be the order of $\mathcal{H}$.

Result 2.1.17. *Using lattice theory and Minkowski's bound it can be proved that the class number $h = h(\mathcal{O}_K)$ of a number field is always finite.*

A finitely generated abelian group A is isomorphic to $A_{tors} \oplus \mathbb{Z}^t$ for some integer t where A_{tors} is the finite subgroup of torsion elements of A (i.e. of elements of finite order). The number t is uniquely determined by A, and is called the rank of A. The following theorem explicitly describes the structure of the unit group of a number field.

Theorem 2.1.18. *The group of units in a number field K is finitely generated of rank $r + s - 1$ where r denotes the number of real embeddings of K and $2s$ denotes the number of non-real complex embeddings.*

Example 2.1.19. For example for a real quadratic field, the rank is $2 + 0 - 1 = 1$ and for an imaginary quadratic field it is $0 + 1 - 1 = 0$.

Definition 2.1.20. A set of units $\{u_1, ..., u_{r+s-1}\}$ is called a *fundamental system of units* if it forms a basis for the group of units modulo torsion.

It follows that the group of units of a real quadratic or real cubic number field is of rank 1. The free part of the group of units in such a field has a unique generator which is bigger than 1. That unit is called the fundamental unit. The fundamental unit is a key ingredient of our work to be described later.

2.2 Elliptic curves

In this section we briefly describe the fundamentals of elliptic curves needed for the later chapters. Throughout this section we denote by K a perfect field, $\bar{K}$ a fixed algebraic closure of K, $G_{\bar{K}/K}$ the Galois group of $\bar{K}/K$. All the results mentioned here can be found in (Silverman [1986]). We start with the definition of affine and projective space over which elliptic curve is to be defined.

Definition 2.2.1. *Affine n-space* (over K) is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, ..., x_n) : x_i \in \bar{K}\}.$$

Similarly, the set of *K-rational points of* $\mathbb{A}^n$ is the set $\mathbb{A}^n(K) = \{P = (x_1, ..., x_n) \in \mathbb{A}^n : x_i \in K\}$. Assuming $\bar{K}[x]$ is a polynomial ring in n variables we give the definition of an affine algebraic set as following.

Definition 2.2.2. For each ideal $I \subset \bar{K}[x]$, the following subset of $\mathbb{A}^n$ can be associated,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

An *(affine) algebraic set* is any set of the form V_I. If V is an algebraic set, the ideal of V is given by

$$I(V) = \{f \in \bar{K}[x] : f(P) = 0 \text{ for all } P \in V\}.$$

By Hilbert basis theorem, all the ideals in $\bar{K}[x]$ and $K[x]$ are finitely generated. For an algebraic set V, an ideal $I(V/K)$ is defined to be

$$I(V/K) = \{f \in K[x] : f(P) = 0 \text{ for all } P \in V\} = I(V) \cap K[x].$$

Then V *is said to be defined over* K if and only if

$$I(V) = I(V/K)\bar{K}[x].$$

Definition 2.2.3. An affine algebraic set V is said to be an *(affine) variety* if $I(V)$ is a prime ideal in $\bar{K}[x]$.

If V is defined over K, it is not enough to check that $I(V/K)$ is a prime ideal in $K[x]$ for V to be an affine variety as indicated by the example of the ideal $(x_1^2 - 2x_2^2)$ in $\mathbb{Q}[x_1, x_2]$.

Definition 2.2.4. Let V is a variety defined over K. then the *affine coordinate ring* of V/K is defined by

$$K[V] = \frac{K[x]}{I(V/K)}.$$

The ring $K[V]$ is an integral domain. Its quotient field is denoted by $K(V)$ and is called the *function field* of V/K. Similarly $\bar{K}[V]$ and $\bar{K}(V)$ can also be defined.

Definition 2.2.5. Let V be a variety. The *dimension* of V, denoted by $\dim(V)$, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Example 2.2.6. The dimension of $\mathbb{A}^n$ is n, since $\bar{K}(\mathbb{A}^n) = \bar{K}(x_1, ..., x_n)$.

When studying a geometric object, it is natural to be interested about the "smoothness" of the object. The following definition clarifies that concept for varieties.

Definition 2.2.7. Let V be a variety, $P \in V$, and $f_1, ..., f_m \in \bar{K}[x]$ a set of generators for $I(V)$. Then V is *nonsingular (or smooth)* at P if the $m \times n$ matrix

$$\left(\frac{\delta f_i}{\delta x_j}(P)\right)_{1 \le i \le m, 1 \le j \le n}$$

has rank $n - \dim(V)$. If V is nonsingular at every point, then V is said to be nonsingular (or smooth).

Another characterization of smoothness, in terms of the functions on the variety V, is as follows.

Result 2.2.8. *Let V be a variety and for each point $P \in V$, an ideal M_P of $\bar{K}[V]$ is defined to be as follows;*

$$M_P = \{f \in \bar{K}[V] : f(P) = 0\}.$$

Then a point $P \in V$ is nonsingular if and only if

$$dim_{\bar{K}} M_P/M_P^2 = dimV.$$

Definition 2.2.9. The local ring of V at P, denoted by $\bar{K}[V]_P$, is the *localization* of $\bar{K}[V]$ at M_P. In other words,

$$\bar{K}[V]_P = \{F \in \bar{K}(V) : F = f/g \text{ for some } f, g \in \bar{K}[V] \text{ with } g(P) \neq 0\}.$$

If $F = f/g \in \bar{K}[V]_P$, then $F(P) = f(P)/g(P)$ is well defined. The functions in $\bar{K}[V]_P$ are said to be *regular (or defined)* at P.

Next we define projective space which loosely speaking is the addition of "points of infinity" to the affine space.

Definition 2.2.10. *Projective n-space* (over K), denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$, is the set of all $(n+1)$-tuples

$$(x_0, ..., x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

if there exists a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class

$$\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \bar{K}^*\}$$

is denoted by $[x_0, ..., x_n]$ and the individual $x_0, ..., x_n$ are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n$. The set of K-rational points in $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(K) = \{[x_0, ...x_n] \in \mathbb{P}^n : \text{ all } x_i \in K\}.$$

Before define projective algebraic set a definition for the well defined functions (independent of choice of homogeneous coordinates) on a projective space is needed.

Definition 2.2.11. A polynomial $f \in \bar{K}[x] = \bar{K}[x_0, .., x_n]$ is *homogeneous* of degree d if

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n) \text{ for all } \lambda \in \bar{K}.$$

An ideal $I \subset \bar{K}[x]$ is said to be homogeneous if it is generated by homogeneous polynomials.

Just like affine space, to each homogeneous ideal I a subset of $\mathbb{P}^n$ can be associated by the following set

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}$$

The definition of projective algebraic set now as follows;

Definition 2.2.12. A *(projective) algebraic set* is any set of the form V_I for a homogeneous ideal I. If V is a projective algebraic set, the (homogeneous) ideal of V, denoted by $I(V)$, is the ideal of $\bar{K}[x]$ generated by

$$\{f \in \bar{K}[x] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

V is said to be *defined over* K, denoted by V/K, if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[x]$. If $V$is defined over K, then the set of K-rational points of V is the set

$$V(K) = V \cap \mathbb{P}^n(K).$$

A projective algebraic set is called a *(projective) variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{K}[x]$.

It can be easily seen that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. Using the fact we give the analogues of dimension and smoothness as defined in the case of affine space.

Definition 2.2.13. Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. Then the *dimension* of V is defined as the dimension of $V \cap \mathbb{A}^n$.

Definition 2.2.14. Let V be a projective variety, let $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is *nonsingular* (or smooth) at P if $V \cap \mathbb{A}^n$ is non-singular at P.

The local ring of V at P, denoted by $\bar{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P. A function $F \in \bar{K}(V)$ is *regular (or defined)* at P if it is in $\bar{K}[V]_P$.

In the context of elliptic curves, a curve means a projective variety of dimension one. The following will be a few definitions which will be needed to define an elliptic curve.

Definition 2.2.15. The *divisor group* of a curve C, denoted by $\text{Div}\,(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \text{Div}\,(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The degree of D is defined by

$$\deg\,(D) = \sum_{P \in C} n_P.$$

Example 2.2.16. Suppose C is a smooth curve and $f \in \bar{K}(C)^*$. Then $\text{div}(f)$ is a divisor associated to f defined by

$$\text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P).$$

Definition 2.2.17. A divisor $D \in \text{Div}(C)$ is said to be *principal* if it has the form $D = \text{div}(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are equivalent, written $D_1 \sim D_2$ if $D_1 - D_2$ is principal.

The *divisor class group (or Picard group)* denoted by $\text{Pic}(C)$, is the quotient of $\text{Div}(C)$ by its subgroup of principal divisors.

Definition 2.2.18. Let C be a curve. The *space of (meromorphic) differential forms on* C, denoted by Ω_C, is the $\bar{K}$-vector space generated by the symbols of dx for $x \in \bar{K}(C)$, subject to the usual relations:

$$\text{(i) } d(x+y) = dx + dy \text{ for all x, y} \in \bar{K}(C).$$

$$\text{(ii) } d(xy) = xdy + ydx \text{ for all x, y } \in \bar{K}(C).$$

$$\text{(iii) } da = 0 \text{ for all } a \in \bar{K}.$$

Definition 2.2.19. Let $\omega \in \Omega_C$. The *divisor associated to* ω is

$$\text{div } (\omega) = \sum_{P \in C} \text{ord }_P(\omega)(P) \in \text{ Div } (C).$$

Definition 2.2.20. The *canonical divisor class* on C is the image in $\text{Pic}(C)$ of $\text{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$.

We can put a partial order on $\text{Div}(C)$ by the following way.

Definition 2.2.21. A divisor $D = \sum_{P \in C} n_P(P)$ is *positive*, denoted by $D \geq 0$ if $n_P \geq 0$ for every $P \in C$. Similarly for any two divisors D_1, D_2, $D_1 \geq D_2$ implies that $D_1 - D_2$ is positive.

By the following definition we will be able to associate a divisor $D \in \text{ Div}(C)$ to a set of function in $\bar{K}(C)^*$.

Definition 2.2.22. Let $D \in \text{ Div}(C)$. We associate to D the set of functions

$$Ł(D) = \{f \in \bar{K}(C)^* : \text{ div}(f) \geq -D\} \cup \{0\}.$$

The set $Ł(D)$ is a finite-dimensional $\bar{K}$-vector space, and its dimension is denoted by $\ell(D)$.

The following is the celebrated Riemann-Roch theorem that also defines the genus of a curve.

Theorem 2.2.23. *Let C be a smooth curve and let K_C be a canonical divisor on C. Then there is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in Div(C)$,*

$$\ell(D) - \ell(K_C - D) = deg\ D - g + 1.$$

Elliptic curves are curves of genus one with a specified base point. The following theorem shows that every elliptic curve can be written as a locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at ∞.

Theorem 2.2.24. *Let E be an elliptic curve defined over K.*
(a) There exists functions $x, y \in K(E)$ such that the map

$$\phi : E \to \mathbb{P}^2, \qquad \phi = [x, y, 1],$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = x^3 + a_2x^2 + a_4X + a_6$$

with coefficients $a_1, ..., a_6 \in K$ and satisfying $\phi(\bigcirc) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E.

(b) Conversely, every smooth cubic curve C given by a Weierstrass equation as in (a) is an elliptic curve defined over K with the base point $\bigcirc = [0, 1, 0]$.

The following composition law for an elliptic curve E is often referred to as the known as "Geometric group law". It can be proved that this geometric group law coincides with the "algebraic group law" originating from the Picard group of the curve.

Result 2.2.25. *Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and $\bigcirc$. Then L' intersects E at $R, \bigcirc$, and a third point. The third point is denoted by $P \oplus Q$.*

The addition of two points on an elliptic curve E given by a Weierstrass equation can be described in terms of their co-ordinates as follows.

Result 2.2.26. *Let E be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(a) Let $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

(b) Now suppose $P_3 = P_1 + P_2$ with $P_i = (x_i, y_i)$ for all $I = 1, 2, 3$. Let $y = \lambda x + \nu$ denote the chord through P_1 and P_2 when these two points are distinct, and the tangent to E if $P_1 = P_2$. Then the coordinates of the point $P_3 = P_1 + P_2$ are given by

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

We conclude this section with the "Mordell-Weil Theorem" which is one of the most important results concerning elliptic curves. It describes the group structure for the K-rational points on an elliptic curve for any number field K.

Theorem 2.2.27. *Let K be an number field and E be an elliptic curve defined over K. Then the set of K-rational points $E(K)$ form a finitely generated abelian group.*

3

Relative Class Number and Continued Fractions

A. Furness and E.A. Parker (Furness and Parker [2012]) investigated relative class number of a real quadratic field $\mathbb{Q}(\sqrt{m})$ by considering the continued fraction representation of $\sqrt{m}$. They proved the existence of a conductor f for a real quadratic field $\mathbb{Q}(\sqrt{m})$ such that the relative class number $H_d(f)$ is one whenever $\sqrt{m}$ has a diagonal continued fraction representation. In this chapter, we extend their approach to real quadratic fields $\mathbb{Q}(\sqrt{m})$ where $\sqrt{m}$ has a non-diagonal representation of period 4 and 5. We further show the existence of an infinite family of real quadratic fields of relative class number 1, which answers a classical question of Dirichlet.

3.1 Introduction

A real quadratic field K is of the form $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ for some square-free natural number m. The discriminant d of K is m if $m \equiv 1 \bmod 4$, otherwise $d = 4m$. The ring $\mathcal{O}_K$ of integers of K is $\{a + b\frac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z}\}$ in the former case, and in the latter case, $\mathcal{O}_K = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. By Dirichlet's Unit Theorem, the units of $\mathcal{O}_K$ are given by $\pm\xi_m^i$ $(i \in \mathbb{Z})$ where ξ_m is called the fundamental unit. The relative class number of K for a conductor f is the ratio $H_d(f)$ of the class numbers of $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ and $\mathcal{O}_K$. Dirichlet obtained a nice formula for the relative class number (see Cohn [1962]).

Result 3.1.1. ***(Dirichlet [1856])*** *Let $\theta(f)$ be the smallest positive integer such that $\xi_m^{\theta(f)} \in \mathcal{O}_f$ and $\psi(f) = f\prod_{q|f}\left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right)$, where $\left(\frac{d}{q}\right)$ denotes the "Kronecker residue symbol" of d modulo a prime q. Then the relative class number for conductor f is given by*

$$H_d(f) = \frac{\psi(f)}{\theta(f)}. \tag{3.1}$$

The Kronecker residue symbol $\left(\frac{d}{q}\right)$ is the same as the Legendre symbol when q is an odd prime. For $q = 2$ and d odd, $\left(\frac{d}{q}\right)$ is 1 if $d \equiv \pm 1 \bmod 8$ and -1 if $d \equiv \pm 3 \bmod 8$. $\theta(f)$ always divides $\psi(f)$ as the relative class number is always an integer (see Cohn [1962]). We will always write the fundamental unit of $\mathcal{O}_K$ as

$$\xi_m = \alpha_0 + \beta_0\sqrt{m}, \qquad 2\alpha_0,\ 2\beta_0 \in \mathbb{Z}.$$

It is well-known that $\xi_m^3 \in \mathbb{Z}[\sqrt{m}]$ and when $m \not\equiv 5 \bmod 8$, α_0 and β_0 are integers (Mollin [1995]). For the rest of the chapter, we will use the following notation:

$$\tilde{\beta_0} = \beta_0,\ \tilde{\alpha_0} = \alpha_0 \ \text{ if } \xi_m \in \mathbb{Z}[\sqrt{m}], \quad \tilde{\beta_0} = 2\beta_0,\ \tilde{\alpha_0} = 2\alpha_0 \ \text{ if } \xi_m \notin \mathbb{Z}[\sqrt{m}].$$

If $\tilde{\beta_0}$ is divisible by a prime q, then $\theta(q) = 1$. When the square-free integer m does not divide $\tilde{\beta_0}$, there exists a prime q dividing m such that $\tilde{\beta_0}$ is not divisible by q. Taking $f = q$ in Dirichlet's formula, we find that $\psi(q) = q$ and $\theta(q) \neq 1$ is a factor

of $\psi(q)$. Hence $\theta(q) = \psi(q) = q$, and $H_d(q) = 1$. Throughout this chapter we will use this approach to find out real quadratic fields with relative class number one.

3.2 Continued fraction approach

When m is a square-free positive integer, we know that its continued fraction is periodic of the form (Niven et al. [2008])

$$n + \cfrac{1}{a_1 + \cfrac{1}{\cdots + \cfrac{1}{a_r + \cfrac{1}{2n + \cfrac{1}{a_1 + \cdots}}}}}, \quad \text{where } n = [\sqrt{m}], \;\; a_i = a_{r+1-i}.$$

We denote it as

$$\sqrt{m} = \langle n, \overline{a_1, a_2, ..., a_r, 2n} \rangle.$$

Let $x = \langle \overline{a_1, a_2, ..., a_r, 2n} \rangle$. Then, $m = \langle n, x \rangle = n + x^{-1}$. The i-th convergent of the continued fraction of x is defined to be as

$$\frac{h_i}{k_i} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{i+1}}}}.$$

The following recurrence relations are satisfied by h_i and k_i:

$$\begin{gathered} h_0 = a_1, \;\; k_0 = 1, \;\; h_1 = 1 + a_1 a_2, \;\; k_1 = a_2, \\ h_i = a_i h_{i-1} + h_{i-2}, \qquad k_i = a_i k_{i-1} + k_{i-2}, \\ h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}. \end{gathered} \tag{3.2}$$

It is well known that $nh_{r-1} + h_{r-2} + h_{r-1}\sqrt{m}$ is the fundamental unit ξ_m of $\mathbb{Q}(\sqrt{m})$ except in the case $m \equiv 5 \pmod 8$, when it equals ξ_m^3 (Mollin [1995]). Hence h_{r-1} is always a multiple of $\tilde{\beta}_0$. If $m > h_{r-1}$ then $m > \tilde{\beta}_0$ and there is a prime factor p of m which does not divide $\tilde{\beta}_0$ and then by Dirichlet's formula, p is a conductor of relative class number $H_d(p) = 1$ as in that case $\theta(p) = \psi(p) = p$. In this section, we will prove that if $\sqrt{m}$ has period 4 or 5, then m does not divide h_{r-1}, and hence $\tilde{\beta}_0$. We begin by the following lemma, which completely generalizes an analogue in (Furness and Parker [2012]) for the diagonal case $\sqrt{m} = \langle n, \overline{a, \cdots, a, 2n} \rangle$.

Lemma 3.2.1. *$m = n^2 + \frac{k_r}{h_{r-1}}$, and in particular, h_{r-1} divides k_r*

Proof: Note that $\sqrt{m} =< n, x >= n + x^{-1}$ where

$$x = \langle \overline{a_1, a_2, ..., a_r, 2n} \rangle, \quad x = \frac{h_{r+1}}{k_{r+1}} = \frac{xh_r + h_{r-1}}{xk_r + k_{r-1}} \implies x^{-2}(h_{r-1}) + x^{-1}(h_r - k_{r-1}) - k_r = 0.$$

We use Euler's formula (Davenport [1999]) for the partial quotients h_i and k_i of x, and using the fact that $a_i = a_{r+1-i}$ we obtain

$$k_{r-1} = [a_2, a_3, ..., a_r] = [a_r, a_{r-1}, ..., a_2] = [a_1, a_2, ..., a_{r-1}] = h_{r-2}. \tag{3.3}$$

On substituting in the quadratic equation and solving for x^{-1}, we obtain

$$\begin{aligned} & x^{-2}(h_{r-1}) + x(h_r - h_{r-2}) - k_r = 0 \\ \Rightarrow & x^{-2}(h_{r-1}) + x(2nh_{r-1}) - k_r = 0 \\ \Rightarrow & x^{-1} = -n + \sqrt{n^2 + \frac{k_r}{h_{r-1}}}, \quad \text{as } x > 0. \end{aligned}$$

Hence, $\sqrt{m} = n + x^{-1} = \sqrt{n^2 + \frac{k_r}{h_{r-1}}} \implies m = n^2 + \frac{k_r}{h_{r-1}}$. □

Next, we obtain a bound on the coefficients appearing in the continued fraction of $\sqrt{m}$. We will later need this bound in the proof of theorem 3.2.3 and 3.2.4.

Proposition 3.2.2. *Let $\sqrt{m} = \langle n; \overline{a, b, \cdots} \rangle$ be a continued fraction of period at least 3. Then $ab < 2n$.*

Proof: Let $[\sqrt{m}] = n$ so that $m = n^2 + t, \ \ t \leq 2n$. Then

$$\sqrt{m} = n + \sqrt{m} - n = n + \frac{1}{\frac{\sqrt{m}+n}{m-n^2}} = n + \frac{1}{\frac{2n+(\sqrt{m}-n)}{t}}, \qquad 0 < \sqrt{m} - n < 1.$$

Now, the next coefficient a in the continued fraction of $\sqrt{m}$ is given by

$$2n = ta + r_1, \ \ 0 < r_1 < t. \tag{3.4}$$

$r_1 = 0$ would imply that $\sqrt{m}$ has continued fraction $\langle n; \overline{a, 2n} \rangle$ of period 2. Now,

$$\sqrt{m} = n + \frac{1}{\frac{ta+(\sqrt{m}-(n-r_1))}{t}} = n + \frac{1}{a + \frac{1}{\frac{t(\sqrt{m}+(n-r_1))}{m-(n-r_1)^2}}}.$$

Now, the last denominator is

$$m - (n - r_1)^2 = (m - n^2) + 2nr_1 - r_1^2 = t + (ta + r_1)r_1 - r_1^2 = t(1 + ar_1),$$

and the numerator is

$$t(\sqrt{m} + (n - r_1)) = t(2n - r_1 + \sqrt{m} - n).$$

Now, the next coefficient b in the continued fraction of $\sqrt{m}$ is given by

$$2n - r_1 = (1 + ar_1)b + r_2, \quad 0 \leq r_2 < 1 + ar_1. \tag{3.5}$$

As $r_1 \geq 1$, we deduce from the last equality that $2n > ab$. □

3.2.1 When $\sqrt{m}$ is a continued fraction of period 4

Here we show the existence of a prime divisor p of m that does not divide $\tilde{\beta}_0$, so that the relative class number for p is 1. As m is square-free, it is enough to show that m does not divide h_{r-1} where r is the period of the continued fraction for $\sqrt{m}$.

Theorem 3.2.3. ***(Chakraborty and Saikia [2015])*** *If* $\sqrt{m} = \langle n, \overline{a, b, a, 2n} \rangle$, *then* m *does not divide* h_2.

Proof: We have $r = 3$ and

$$h_{r-1} = [a, b, a] = a^2b + 2a, \quad h_{r-2} = [a, b] = ab + 1 = k_{r-1}, \quad k_{r-2} = [b] = b.$$

By (3.2), we have

$$h_{r-1}k_{r-2} - k_{r-1}h_{r-2} = (-1)^{r-1} \implies k_{r-1}^2 \equiv (-1)^{r-1} \pmod{h_{r-1}}. \tag{3.6}$$

By lemma (3.2.1),

$2nk_{r-1} + k_{r-2} = k_r \equiv 0 \ (\text{ mod } h_{r-1})$

$\Rightarrow 2n \equiv 2nk_{r-1}^2 \equiv -k_{r-1}k_{r-2} \equiv -ab^2 - b \ (\text{ mod } h_{r-1})$

$\Rightarrow 2na \equiv -a^2b^2 - ab \equiv ab \ (\text{ mod } h_{r-1})$

$\Rightarrow 2na = l(h_{r-1}) + ab$, where $l \in \mathbb{N}$ as $2n > b$ by proposition 3.2.2

$\Rightarrow 2n = l(ab+2) + b \geq ab + b + 2$

$\Rightarrow 4n^2 > (ab+b+2)^2 = a^2b^2 + 4ab + 4 + 2ab^2 + 4b + b^2 > 4a^2b + 8a = 4h_{r-1}$ for $b > 3$

$\Rightarrow m > n^2 > h_{r-1}$ for $b > 3$

When $b = 1$, $h_{r-1} = \langle a, 1, a\rangle = a^2 + 2 \leq (n-1)^2 + 2 < n^2 < m$, as $a \leq n-1$. Here we are using the fact that in $2n = ta + r_1$ (3.4), t is at least 2 as otherwise,

$$m = n^2 + t = n^2 + 1 \implies \sqrt{m} = \langle n, \overline{2n}\rangle \text{ (of period 1).}$$

When $b = 2$, $h_{r-1} = \langle a, 2, a\rangle = 2a^2 + 2a < 2m$ just like the above case. Now, if m divides h_{r-1}, then that means $h_{r-1} = m$. But then $m = h_{r-1} = 2a(a+1)$ will not be square free as 4 divides $2a(a+1)$.

When $b = 3$ we use (3.5) to obtain

$$t = \frac{2n - r_1}{a} > \frac{2n - (r_1 + r_2)}{1 + ar_1} = b.$$

Here, $b = 3$ implies $t \geq 4$. Therefore,

$$a = \frac{2n - r_1}{t} \leq \frac{2n-1}{4} = \frac{n}{2} - \frac{1}{4} \implies a \leq \frac{n-1}{2}$$

as a is an integer. Now,

$$h_{r-1} = 3a^2 + 2a \leq \frac{3}{4}(n-1)^2 + (n-1) \leq n^2 < m$$

unless $n = 1$, but then $\sqrt{m} = \sqrt{2}$ or $\sqrt{3}$ is of period strictly less than 3. $\square$

3.2.2 When $\sqrt{m}$ is a continued fraction of period 5

The existence of a conductor of relative class number 1 can be proved by the following approach.

Theorem 3.2.4. ***(Chakraborty and Saikia [2015])*** *If* $\sqrt{m} = \langle n, \overline{a, b, b, a, 2n}\rangle$, *then* $m > h_3$.

Proof: Recall that $\sqrt{m} = \sqrt{n^2 + \frac{k_r}{h_{r-1}}}$ when $\sqrt{m} = \langle n, \overline{a_1, a_2, ..., a_r}\rangle$ where, $a_i = a_{r+1-i}$, and $\frac{h_i}{k_i}$ denotes the i-th convergent. Here, $r = 4$. Now,

$$h_{r-1} = h_3 = [a, b, b, a] = (ab+1)^2 + a^2, \quad k_{r-2} = [b, b] = b^2 + 1,$$
$$h_{r-2} = [a, b, b] = ab^2 + a + b = k_{r-1}.$$
$$k_{r-1}^2 \equiv (-1)^{r-1} = -1 \pmod{h_{r-1}} \text{ (as in 3.6).}$$

Now,

$$k_r = 2nk_{r-1} + k_{r-2} \equiv 0 \pmod{h_{r-1}}, \text{ by lemma 3.2.1}$$
$$\implies 2n \equiv -2nk_{r-1}^2 \equiv k_{r-1}k_{r-2} \equiv (ab^2 + a + b)(b^2 + 1) \pmod{h_{r-1}}$$
$$\Rightarrow 2na \equiv (a^2b^2 + a^2 + ab)(b^2 + 1) \equiv -(ab+1)(b^2+1) \pmod{h_{r-1}}$$
$$\Rightarrow 2na(ab+1) \equiv -(ab+1)^2(b^2+1) \equiv a^2(b^2+1) \pmod{h_{r-1}}$$
$$\Rightarrow 2n(ab+1) \equiv a(b^2+1) \pmod{h_{r-1}} \text{ as } gcd(a, h_{r-1}) = 1$$
$$\implies 2n(ab+1) = lh_{r-1} + a(b^2+1) = l((ab+1)^2 + a^2) + a(b^2+1).$$

By proposition 3.2.2, $2n > ab$ and hence l must be a positive integer. We now claim that l must be even from parity considerations in the last equality. When a is even or a, b both are odd, h_{r-1} is odd and hence l must be even. If a is odd and b is even, h_{r-1} is even but $a(b^2+1)$ is odd which is ruled out by the equality

$2n(ab+1) = lh_{r-1} + a(b^2+1)$ mentioned above. Now

$$\begin{aligned}
&2n(ab+1) = l.h_{r-1} + a(b^2+1) \geq 2\big((ab+1)^2 + a^2\big) + a(b^2+1) \\
\Rightarrow &2n \geq 2(ab+1) + \frac{2a^2 + a(b^2+1)}{ab+1}. \\
\Rightarrow &4n^2 \geq 4(ab+1)^2 + 4(2a^2 + a(b^2+1)) + \Big(\frac{2a^2 + a(b^2+1)}{ab+1}\Big)^2 \\
\Rightarrow &4n^2 > 4(ab+1)^2 + 4a^2 = 4.h_{r-1}. \\
\Rightarrow &m > n^2 > h_{r-1}. \qquad \square
\end{aligned}$$

Thus there exists prime f such that f divides m but does not divide h_{r-1} as m is square-free. Hence $H_d(f)$ is 1 by the formula of Dirichlet. Thus we can ascertain the existence of a conductor of relative class number 1 for a real quadratic field $\mathbb{Q}(\sqrt{m})$ when $\sqrt{m}$ is represented by a continued fraction of period 4 or 5 (as well as for all diagonal numbers as proved in (Furness and Parker [2012])). The following result as already mentioned also comes out in the proof.

Corollary 3.2.5. *There does not exist square free positive integer m such that $\sqrt{m} = \langle n, \overline{a, b, b, a, 2n}\rangle$ and a is odd and b is even.*

3.3 Affirmative answer to Dirichlet's question

In this section we give a construction for an infinite family real quadratic fields of relative class number 1. Thus, it gives an affirmative answer to the classical question of Dirichlet on existence of infinitely many real quadratic fields of relative class number 1.

Theorem 3.3.1. *There exists infinitely many square-free product m of two consecutive integers such that $\mathbb{Q}(\sqrt{m})$ has relative class number 1 for a suitable prime conductor p dividing m.*

Proof: If m is a square-free integer of the form $n^2 + n$ then it follows that $\sqrt{m} = \langle n, \overline{2, 2n}\rangle$. Here, $h_{r-1} = 2$. Now, $m = n^2 + n$ must have an odd prime factor p

for $n > 1$ as m is the product of two consecutive integers. Since p does not divide $2 = h_{r-1}$, we must have $H_d(p) = 1$.

Next, we show that there exist infinitely many n such that $m = n^2 + n$ is square-free. Let N be a sufficiently large natural number. If we sieve out all the integers between $2kN + 1$ to $(2k+2)N$ which are divisible by squares of some prime, we will be left with more than N square-free integers as

$$\sum \frac{1}{p^2} < 0.4522474200 \cdots < \frac{1}{2}$$

(see Finch [2003]). Thus, at least two of those square-free integers will be consecutive. Hence there exist infinitely many square free positive integers of the from $m = n^2 + n$. For each such m, $\mathbb{Q}(\sqrt{m})$ has relative class number 1 for any odd prime divisor of m as the conductor. □

3.4 Mersenne primes and relative class number

We conclude the chapter by relating Mersenne primes to relative class number of a real quadratic field.

Theorem 3.4.1. *If there are infinitely many Mersenne primes, then there exist infinitely many real quadratic fields with any given power of* 2 *as relative class number.*

Proof: Suppose $m > 6$ is an integer which is twice a Mersenne prime. In other words, let $m = 2(2^p - 1)$ where $p = 2k - 1$ is a prime. Then, m is square free and we have

$$m = (2^k)^2 - 2 = (n+1)^2 - 2, \qquad \sqrt{m} = \langle n, \overline{1, n-1, 1, 2n} \rangle, \qquad h_{r-1} = n + 1 = 2^k.$$

As $\xi_m \in 2^i \mathcal{O}_K$ for all $0 \leq i \leq k$, $\theta(2^i) = 1$. Now,

$$\psi(2^i) = 2^i \Big(1 - \Big(\frac{d}{p}\Big)\frac{1}{p}\Big)\Big(1 - \Big(\frac{d}{2}\Big)\frac{1}{2}\Big) = 2^i.$$

Therefore $H_d(2^i) = 2^i$. If we assume that the number of Mersenne primes is infinite, there will be infinitely many primes of the form $2^{2k-1} - 1$, and hence we can demonstrate infinitely many real quadratic fields with any power of 2 as relative class number. $\square$

4

Real Quadratic Fields with Relative Class Number 1

Motivated by Gauss' class number one problem for real quadratic fields in *Disquisitiones Arithmeticae* (Gauss [1966]), Dirichlet (Dirichlet [1856]) posed the question whether there exist infinitely many real quadratic fields with relative class number one. Though Dirichlet could not find an answer to it, he obtained a very useful formula for the relative class number of a number field in terms of the fundamental unit. We have already introduced the notion of relative class number and the formula of Dirichlet in the previous chapter (3.1). A. Furness and E.A. Parker provided a partial answer to Dirichlet's question in (Furness and Parker [2012]) for those real

quadratic fields $\mathbb{Q}(\sqrt{m})$ where $\sqrt{m}$ has a special continued fraction representation (Furness and Parker [2012]) which we have generalized in the previous chapter. In this chapter, we give a necessary and sufficient condition for a real quadratic field to have relative class umber one for some conductor. We also prove that $\mathbb{Q}(\sqrt{m})$ will always have 1 as relative class number for the conductor 3, whenever m is a prime of the form 3 (mod 4). It is to be noted R.A. Mollin (Mollin [2013]) also has shown the existence of infinitely many real quadratic fields of class number 1, but our approach is completely different and moreover we provide a characterization.
We use the same notations as in the previous chapter. In particular, we continue to write the fundamental unit of $\mathcal{O}_K$ as

$$\xi_m = \alpha_0 + \beta_0\sqrt{m}, \qquad 2\alpha_0,\ 2\beta_0 \in \mathbb{Z}.$$

It is well-known that $\xi_m^3 \in \mathbb{Z}[\sqrt{m}]$, and when $m \not\equiv 5 \pmod 8$ α_0 and β_0 are integers (Mollin [1995]). For the rest of this chapter, we continue to use the following notation:

$$\tilde{\beta_0} = \beta_0,\ \tilde{\alpha_0} = \alpha_0 \ \text{ if } \xi_m \in \mathbb{Z}[\sqrt{m}], \quad \tilde{\beta_0} = 2\beta_0,\ \tilde{\alpha_0} = 2\alpha_0 \ \text{ if } \xi_m \notin \mathbb{Z}[\sqrt{m}].$$

We first restate Dirichlet's formula (3.1) here, as it plays a key role in this chapter.

Result 4.0.2. ***(Dirichlet [1856])*** *Let $\theta(f)$ be the smallest positive integer such that $\xi_m^{\theta(f)} \in \mathcal{O}_f$ and $\psi(f) = f\prod_{q|f}\left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right)$, where $\left(\frac{d}{q}\right)$ denotes the "Kronecker residue symbol" of d modulo a prime q. Then the relative class number for conductor f is given by*

$$H_d(f) = \frac{\psi(f)}{\theta(f)}. \tag{4.1}$$

Now if we consider $m = 1817$ and $f = 2$. As $1817 \equiv 1 \bmod 8$, we find that $H_d(2) = 1$. But m divides $\tilde{\beta_0}$ in this case (see Stephens and Williams [1988]). Hence, non-divisibility of $\tilde{\beta_0}$ by m is only a sufficient condition for existence of f such that $H_d(f) = 1$ but it is not a necessary condition. Throughout this chapter,

we will mostly consider prime conductors $f = p$, and try to determine the smallest exponent $\theta(p)$ that takes the fundamental unit ξ_m of $\mathbb{Q}(\sqrt{m})$ into the order $\mathcal{O}_p$ of conductor p.

4.1 Powers of ξ_m in $\mathcal{O}_p$

The fundamental unit $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ has norm either 1 or -1, and accordingly, we have $\xi_m^{-1} = \alpha_0 - \beta_0\sqrt{m}$ or $\xi_m^{-1} = -(\alpha_0 - \beta_0\sqrt{m})$. In the following two sections we assume that ξ_m has norm 1. The result of the next two propositions will be used later in this chapter to prove the main theorem.

Proposition 4.1.1. *If ξ_m has norm 1, then $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$ for any odd prime p not dividing m.*

In fact, we obtain the following sharper result.

Proposition 4.1.2. *Let p be an odd prime not dividing m. If 2^s divides $p - \left(\frac{d}{p}\right)$ and $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2^{s-1}}} \equiv 1 \pmod{p}$ then $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2^s}} \in \mathcal{O}_p$.*

We prove the above propositions by considering congruence. The main idea of the proof lies in the following lemma.

Lemma 4.1.3. *$\xi_m^{p-\left(\frac{d}{p}\right)} \equiv 1 \pmod{p}$ for any odd prime p not dividing m.*

Proof: We have modulo $p\mathcal{O}_K$

$$\xi_m^p \equiv \alpha_0^p + \beta_0^p m^{\frac{p-1}{2}}\sqrt{m} \equiv \alpha_0 + \left(\frac{m}{p}\right)\beta_0\sqrt{m} = (\alpha_0 + \beta_0\sqrt{m})^{\left(\frac{m}{p}\right)} = \xi_m^{\left(\frac{m}{p}\right)}.$$

As ξ_m is a unit and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right)$, it follows that $\xi_m^{p-\left(\frac{d}{p}\right)} \equiv 1 \bmod p\mathcal{O}_K$. $\square$

Proof of proposition (4.1.1): Let $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} = \alpha_1 + \beta_1\sqrt{m}$. Then $\xi_m^{-\frac{p-\left(\frac{d}{p}\right)}{2}} = \alpha_1 - \beta_1\sqrt{m}$. Now,

$$2\beta_1\sqrt{m} = \xi_m^{-\frac{p-\left(\frac{d}{p}\right)}{2}}\left(\xi_m^{p-\left(\frac{d}{p}\right)} - 1\right) \in p\mathcal{O}_K.$$

When $\left(\frac{m}{p}\right) = -1$, $p\mathcal{O}_K$ is a prime ideal. As m is not divisible by p, $\sqrt{m}$ does not belong to $p\mathcal{O}_K$. Therefore, $2\beta_1 \in p\mathbb{Z}$. This implies $\beta_1 \in p\mathbb{Z}$ as p is odd. Hence,

$$\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} = \alpha_1 + \beta_1\sqrt{m} \in \mathbb{Z} + p\mathcal{O}_K = \mathcal{O}_p.$$

When $\left(\frac{m}{p}\right) = 1$, $p\mathcal{O}_K$ splits as a product $\wp_1\wp_2$ of two prime ideals. As m is not divisible by p, $\sqrt{m} \notin \wp_i$ and therefore, $2\beta_1 \in \wp_i$, $(i = 1,\ 2)$. Therefore, $2\beta_1 \in p\mathbb{Z}$, and $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$ in this case too. □

Proof of proposition (4.1.2): Let $p - \left(\frac{d}{p}\right) = l2^s$ and $\xi_m^l = \alpha_l + \beta_l\sqrt{m}$. Then $\xi_m^{2l} = ({\alpha_l}^2 + m{\beta_l}^2) + (2\alpha_l\beta_l)\sqrt{m}$. From $(\xi_m^{2l} - 1) \in p\mathcal{O}_K$ we conclude that $4({\alpha_l}^2 + m{\beta_l}^2 - 1)$ and $4\alpha_l\beta_l$ are in $p\mathbb{Z}$, noting that α_l and β_l can be half integers when $m \equiv 5 \bmod 8$. If p divides $2\beta_l$ we are done with our proof. If not, then p must divide $2\alpha_l$ from the second condition. But p also divides $4({\alpha_l}^2 + m{\beta_l}^2 - 1)$. Hence $4m{\beta_l}^2 \equiv 4 \bmod p$. On the other hand, ξ_m^l has norm 1 as ξ_m has norm 1. Therefore $4({\alpha_l}^2 - m{\beta_l}^2) = 4$ and $4m{\beta_l}^2 \equiv -4 \bmod p$. This means p divides 8 which is a contradiction. Therefore we have our desired result. □

4.2 Fundamental unit of norm -1

In this section we assume that the fundamental unit $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ of $\mathbb{Q}(\sqrt{m})$ has norm -1, and obtain information about the relative class number for odd prime conductors that do not divide m. We prove that if d is a quadratic non-residue modulo a Mersenne prime f, then the conductor f has relative class number 1. We also show that if f is Sophie Germain prime such that d is a quadratic residue modulo $2f + 1$, then the conductor $2f + 1$ has relative class number 1. Note that we now have $\xi_m^{-1} = -(\alpha_0 - \beta_0\sqrt{m})$. We start with the following lemma.

Lemma 4.2.1. ${\xi_m}^{p-\left(\frac{d}{p}\right)} \equiv \left(\frac{d}{p}\right)$ *(mod p) for any odd prime p not dividing m.*

Proof:

$$\xi_m^p \equiv \alpha_0^p + \beta_0^p m^{\frac{p-1}{2}}\sqrt{m} \equiv \alpha_0 \pm \beta_0\sqrt{m} \equiv \left(\frac{d}{p}\right)\xi_m^{\left(\frac{d}{p}\right)} \bmod p\mathcal{O}_K,$$

As ξ_m is a unit in $\mathcal{O}_K$, the lemma follows. $\square$

Proposition 4.2.2. *If p is an odd prime not dividing m then $p \equiv 1$ mod 4 if and only if $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$.*

Proof: We can assume that the fundamental units $\xi_m \in \mathbb{Z}[\sqrt{m}]$, as the argument is similar for the case $2\xi_m \in \mathbb{Z}[\sqrt{m}\,]$ for an odd prime p. First assume that $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$. Now $\xi_m^{\frac{p-1}{2}} = \alpha_1 + \beta_1\sqrt{m}$ has norm 1 as $\frac{p-1}{2}$ is even, so its inverse is $\xi_m^{-\frac{p-1}{2}} = \alpha_1 - \beta_1\sqrt{m}$. By lemma (4.2.1)

$$2\beta_1\sqrt{m} = \xi_m^{\frac{p-1}{2}} - \xi_m^{-\frac{p-1}{2}} = \xi_m^{-\frac{p-1}{2}}(\xi_m^{p-1} - 1) \in p\mathcal{O}_K.$$

From $2\beta_1\sqrt{m} \in p\mathcal{O}_K$ it follows that $2m\beta_1 = \sqrt{m}\cdot 2\beta_1\sqrt{m} \in p\mathcal{O}_K$. Hence, $2m\beta_1 \in p\mathbb{Z}$, so $p \mid \beta_1$, since $2m$ is invertible modulo p.

Now let $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$, so $p\mathcal{O}_K$ is a prime ideal. Now $\xi_m^{\frac{p+1}{2}} = \alpha_2 + \beta_2\sqrt{m}$ has norm -1 as $\frac{p+1}{2}$ is odd, so $\alpha_2^2 - m\beta_2^2 = -1$. By lemma (4.2.1)

$$\xi_m^{p+1} + 1 = \left(\xi_m^{\frac{p+1}{2}}\right)^2 + 1 \in p\mathcal{O}_K \implies \alpha_2^2 + m\beta_2^2 + 1 + 2\alpha_2\beta_2\sqrt{m} \in p\mathcal{O}_K.$$

If p does not divide β_2 then p divides α_2 and $m\beta_2^2 = 1 + \alpha_2^2 \equiv 1 \bmod p$ contradicts $\left(\frac{m}{p}\right) = -1$. Hence, $p \mid \beta_2$ and $\xi_m^{\frac{p+1}{2}} \in \mathcal{O}_p$.

We now assume that $p \equiv 3 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$ so that $\xi_m^{p+1} \equiv -1 \bmod p\mathcal{O}_K$ (from 4.2.1). Now $\xi_m^{\frac{p+1}{2}} = \alpha_2 + \beta_2\sqrt{m}$ has norm 1 as $\frac{p+1}{2}$ is even, so $\alpha_2^2 - m\beta_2^2 = 1$. If $\xi_m^{\frac{p+1}{2}} \in \mathcal{O}_p$, then

$$p \mid \beta_2 \implies -1 \equiv \xi_m^{p+1} \equiv \alpha_2^2 \equiv 1 \bmod p\mathcal{O}_K \implies p = 2.$$

Next we assume that $p \equiv 3 \bmod 4$ and $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = 1$ so that $\xi_m^{p-1} \equiv 1 \bmod p\mathcal{O}_K$. Now $\xi_m^{\frac{p-1}{2}} = \alpha_2 + \beta_2\sqrt{m}$ has norm -1 as $\frac{p-1}{2}$ is odd, so $\alpha_2^2 - m\beta_2^2 = -1$. Now

$\xi_m^{p-1} = \alpha_2^2 + m\beta_2^2 + 2\alpha_2\beta_2\sqrt{m} \equiv 1 \bmod p\mathcal{O}_K$, so p divides $2\alpha_2\beta_2$. If $\xi_m^{\frac{p-1}{2}} \in \mathcal{O}_p$ then

$$p \mid \beta_2 \implies 1 \equiv \xi_m^{p-1} \equiv \alpha_2^2 \equiv -1 \bmod p\mathcal{O}_K \implies p = 2. \qquad \square$$

Now we get the following corollaries.

Corollary 4.2.3. *(i) If $p \equiv 1$ mod 4 is an odd prime not dividing m, then the relative class number for conductor p is not* 1.
(ii) If $p \equiv 3$ mod 4 is an odd prime not dividing m, then the relative class number for conductor p is odd.

Proof: If $p \equiv 1 \bmod 4$ not dividing m, then 4.2.2 implies that $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$. So, $\theta(p) \leq \frac{p-\left(\frac{d}{p}\right)}{2} = \frac{\psi(p)}{2}$. And hence $H_d(p) = \frac{\psi(p)}{\theta(p)} \geq 2$ always.
For the proof of the second part of the above corollary, we notice that whenever the relative class number of a real quadratic field $\mathbb{Q}(\sqrt{m})$ is even for some prime conductor p, then $\theta(p)$ will always divide $\frac{p-\left(\frac{d}{p}\right)}{2}$ as

$$\frac{\psi(p)}{\theta(p)} = \frac{p-\left(\frac{d}{p}\right)}{\theta(p)} = 2k \text{ for some integer k .}$$

So if $p \equiv 3 \bmod 4$ and the relative class number of $\mathbb{Q}(\sqrt{m})$ is even for the conductor p, then $\theta(p)$ divides $\frac{p-\left(\frac{d}{p}\right)}{2}$. But this implies that $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$ and hence $p \equiv 1 \bmod 4$ as well, a contradiction. Hence the relative class number will always be odd for primes $p \equiv 3 \bmod 4$. $\square$

Proposition 4.2.4. *When $\mathbb{Q}(\sqrt{m})$ has fundamental unit of norm -1 the relative class number for conductor* 3 *must be* 1.

Proof: If the fundamental unit of $\mathbb{Q}(\sqrt{m})$ has norm -1 then -1 will be a quadratic residue modulo any odd prime dividing d. Hence only odd primes dividing m must be of the form $4k+1$. In particular, 3 can not divide m, and $\psi(3) = 2$ or 4. By the second part of the above corollary, $H_d(3)$ is odd. The only odd factor of 2 or 4 is 1, hence $H_d(3) = 1$. $\square$

Corollary 4.2.5. *There are infinitely many real quadratic fields of relative class number* 1 *for the conductor* 3.

Proof: If m is a prime which is congruent to 1 mod 4, it is an easy exercise to show that the fundamental unit of $\mathbb{Q}(\sqrt{m})$ has norm -1. By Dirichlet's theorem on primes in arithmetic progression, there are infinitely many such primes m. Hence the corollary follows from proposition (4.2.4). $\square$.

Proposition 4.2.6. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field with fundamental unit ξ_m of norm -1. If d is a quadratic non-residue modulo a Mersenne prime f, then the relative class number for conductor f is* 1.

Proof: Let $\xi_m = \alpha_0 + \beta_0\sqrt{m}$. Suppose there exists a Mersenne prime $f = 2^p - 1$ for some prime p such that $\left(\frac{d}{f}\right) = -1$. Now,

$$\psi(f) = f\Big(1 - \Big(\frac{d}{f}\Big)\frac{1}{f}\Big) = 1 + f = 2^p.$$

By corollary (4.2.3), $H_d(f)$ is an odd divisor of 2^p, hence it must be 1. $\square$

A prime f is said to be a "Sophie Germain prime of the first kind" if $2f + 1$ is also a prime. We deduce the following result.

Proposition 4.2.7. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field with fundamental unit ξ_m of norm -1. If d is a quadratic residue modulo $2f + 1$ where f is sufficiently large Sophie Germain prime of the first kind then the relative class number for the conductor $2f + 1$ is* 1.

Proof: Let $\xi_m = \alpha_0 + \sqrt{m}\beta_0$. Suppose f is Sophie Germain prime such that d is a quadratic residue modulo the prime $2f + 1$ and $2f + 1$ does not divide $\tilde{\alpha_0}\tilde{\beta_0}$. Then,

$$\psi(2f + 1) = (2f + 1)\Big(1 - \Big(\frac{d}{2f + 1}\Big)\frac{1}{2f + 1}\Big) = 2f.$$

Now, $2f+1$ does not divide $2m\tilde{\alpha_0}\tilde{\beta_0}$ implies $\phi(f) \neq 2$. By proposition (4.2.2),

$$2f+1 \equiv 3 \pmod 4 \Rightarrow \theta(f) \neq f \Rightarrow \theta(f) = 2f.$$

Therefore,

$$H_d(2f+1) = \frac{\psi(2f+1)}{\theta(2f+1)} = 1. \qquad \square$$

The following corollary follows directly form the previous two propositions.

Corollary 4.2.8. *Suppose $\mathbb{Q}(\sqrt{m})$ has only finitely many prime conductors of relative class number 1. Then*
(i) there are only finitely many Mersenne primes with d as quadratic non-residue.
(ii) there are only finitely many Sophie Germain primes of the first kind with d as quadratic residue.

4.3 A criterion for non-existence of conductor of relative class number 1

The main result of this section is the following criterion for non-existence of a conductor f for which the relative class number of $\mathbb{Q}(\sqrt{m})$ is 1. As before, we have $\xi_m = \alpha_0 + \beta_0\sqrt{m}$ as the fundamental unit and d is the discriminant of $\mathbb{Q}(\sqrt{m})$. We notice that ξ_m must have norm 1 as in proposition (4.2.4) we already saw that $H_d(3) = 1$ for all $\mathbb{Q}(\sqrt{m})$, when the fundamental unit of $\mathbb{Q}(\sqrt{m})$ has norm -1.

Theorem 4.3.1. ***(Chakraborty and Saikia [2014])*** *There does not exist any conductor f for which the relative class number of $\mathbb{Q}(\sqrt{m})$ is 1 if and only if*
(i) m divides $\tilde{\beta_0}$ and
(ii) if m is odd then $m \neq 1 \bmod 8$ and $\tilde{\beta_0}$ is an even integer.

Proof: We first prove the sufficiency. If p is an odd prime dividing m, then p divides $\tilde{\beta_0}$. Then $\xi_m \in \mathcal{O}_p$ and $\theta(p) = 1$. But

$$\psi(p) = p\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) = p > 1.$$

If p is an odd prime not dividing m then by proposition (4.1.1) we have $\xi_m^{\frac{p-\left(\frac{d}{p}\right)}{2}} \in \mathcal{O}_p$. Therefore, $\theta(p) \leq \frac{p-\left(\frac{d}{p}\right)}{2}$. Now by the formula (4.1) of Dirichlet,

$$\psi(p) = p\Big(1 - \Big(\frac{d}{p}\Big)\frac{1}{p}\Big) \implies H_d(p) = \frac{\psi(p)}{\theta(p)} \geq 2.$$

The only remaining prime is $p = 2$ when m is odd. Under the given conditions, $\psi(2) = 2(1 - \left(\frac{d}{2}\right)\frac{1}{2}) = 3$ or 2 (when $d \equiv -3 \bmod 8$), and $\theta(2) = 1$ as $\tilde{\beta}_0$ is even. Therefore, $H_d(2) > 1$. For any non-prime conductor f, our theorem follows from the fact that $H_d(g)$ divides $H_d(f)$ if g divides f (see Cohn [1962]).

Conversely, suppose there does not exist any f with $H_d(f) = 1$. Any prime q that divides m but does not divide $\tilde{\beta}_0$ will give $H_d(q) = \frac{\psi(q)}{\theta(q)} = 1$. Hence m must divide $\tilde{\beta}_0$. Also, $H_d(2) \neq 1$ implies that

$$\psi(2) = 2\left(1 - \left(\frac{d}{2}\right)\frac{1}{2}\right) = 2 \text{ or } 3,$$

and hence m must be of the form $m \not\equiv 1 \bmod 8$ if m is odd. In that case, $\theta(2) = 1$ and hence $\tilde{\beta}_0$ must be an even integer. $\square$

We end this chapter with the following example which agrees with Theorem 4.3.1.

Example: Consider $m = 46$. It is well known that $\beta_0 = 3588$ (Davenport [1999]) which is divisible by 46. Hence $\mathbb{Q}(\sqrt{46})$ does not have relative class number 1 for any conductor.

5

Fundamental Unit and the Class Number

5.1 Introduction

Dirichlet's unit theorem asserts that the group of units in the ring of integers of a pure cubic or real quadratic field is of rank one, and the smallest unit > 1 is referred to as the fundamental unit. In this chapter, we consider a pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$ with a power integral basis where m denotes a natural number. It is well-known that $\mathbb{Q}(\sqrt[3]{m})$ has a power integral basis if and only if m is square-free and $m \not\equiv \pm 1$ modulo 9 (see Lemmermeyer [2013]). Let $\xi_m = x + yt + zt^2$, where $t = \sqrt[3]{m} \in \mathbb{R}$, be the fundamental unit of K. In this chapter we investigate divisibility and congruence properties of x, y and z with respect to the prime 3 and

relate it to the class number of $\mathbb{Q}(\sqrt[3]{m})$, which we denote by h_m. As a consequence, we deduce the following results, the first of which agrees with an old result of Gerth (Gerth et al. [1976]) in a simpler way.

Theorem 5.1.1. ***(Chakraborty and Saikia [2016a])*** *Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with a power integral basis (i.e., m square-free natural number and $m \not\equiv \pm 1 \mod 9$). If 3 does not divide h_m, then m must be either p or $3p$ for some prime p.*

It follows from the above theorem that for any square-free composite number $m \equiv 2, 4, 5$ or $7 \pmod 9$, the class number of $\mathbb{Q}(\sqrt[3]{m})$ is divisible by 3. When $m = 3p$ is a square-free integer for some prime p and 3 does not divide h_m, we show that the fundamental unit satisfies the congruences given in the theorem below.

Theorem 5.1.2. ***(Chakraborty and Saikia [2016a])*** *Suppose $m = 3p$ where p is any prime other than 3. Let $\xi_m = x + yt + zt^2$ be the fundamental unit of the field $K = \mathbb{Q}(t)$ ($t = \sqrt[3]{m}$). If 3 does not divide h_m then $x^2 \equiv 1 \mod 27p$ and $y \equiv z \equiv 0 \mod 3$.*

For the case $m = p \not\equiv \pm 1 \mod 9$ where p is prime, we have the analogous relations given by theorem 5.2.8 and more precisely, by propositions 5.2.6 and 5.2.7.

Our approach is to exploit the ramified primes in the extension. We apply the same approach to study congruence relations satisfied by the fundamental unit of a real quadratic field of odd class number. An immediate consequence of our approach is the classically well-known result that a real quadratic field with discriminant having more than or equal to three prime factors has even class number (see corollary 5.3.2). If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field of odd class number, then it is well-known that d has to be of the form $d = p$, $d = 2p$ or $d = p_1p_2$ where p_1, p_2 are primes congruent to 3 modulo 4. Let $\xi_d = x + y\sqrt{d}$ be the fundamental unit of K. Using our approach, we can prove in an elementary way the following congruences which were given in (Zhang and Yue [2014]).

Theorem 5.1.3. ***(Chakraborty and Saikia [2016a])*** *Let $\xi_d = x + y\sqrt{d} > 1$ be the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$ of odd class number. Then*
1. *If $d = p$ with $p \equiv 3 \mod 4$, then $x \equiv 0 \mod 2$. More precisely, if $p \equiv 3 \mod 8$, then $x \equiv 2 \mod 4$ and if $p \equiv 7 \mod 8$ then $x \equiv 0 \mod 4$.*
2. *If $d = 2p$ with $p \equiv 3 \mod 4$, then $y \equiv 0 \mod 2$ and $x + y \equiv 3 \mod 4$.*
3. *If $d = p_1p_2$ with $p_1 \equiv p_2 \equiv 3 \mod 4$, then $x \equiv 3 \mod 4$ and $y \equiv 0 \mod 4$.*

In the third part of the above theorem when $d = p_1p_2 \equiv 5 \mod 8$, we know that $\xi_d^3 \in \mathbb{Z}[\sqrt{d}]$ but we may not have $\xi_d \in \mathbb{Z}[\sqrt{d}]$. In that case, the congruences are satisfied by x and y where $x + y\sqrt{d} = \xi_d^3$.

5.2 Fundamental Unit of real cubic fields with class number not divisible by 3

In this section, K denotes a pure cubic field $\mathbb{Q}(\sqrt[3]{m})$ of class number not divisible by 3. We first observe that the norm of the fundamental unit ξ_m is the product $(x + yt + zt^2)(x + \zeta_3 yt + \zeta_3^2 zt^2)(x + \zeta_3^2 yt + \zeta_3 zt^2)$ where the first factor is ξ_m itself, which is bigger than 1 and the next two factors are complex conjugates of one another. Therefore, the product must be positive and we have

$$Norm_{K/\mathbb{Q}}(\xi_m) = x^3 + my^3 + m^2z^3 - 3mxyz = 1. \tag{5.1}$$

We first observe certain divisibility relations between ξ_m and ξ_m^2 in the following lemma.

Lemma 5.2.1. *Suppose $K = \mathbb{Q}(\sqrt[3]{m})$ is a pure cubic field where m is not a multiple of 3. Also suppose $\xi_m = x + yt + zt^2 \in \mathbb{Z}[t]$ denotes the fundamental unit of K and $\xi_m^2 = x_1 + y_1t + z_1t^2$. Then 3 divides y, z if and only if 3 divides y_1, z_1.*

Proof. We have

$$\begin{aligned} x_1 + y_1 t + z_1 t^2 = (x + yt + zt^2)^2 \Rightarrow x_1 = x^2 + 2myz, \\ y_1 = mz^2 + 2xy, \qquad z_1 = y^2 + 2xz. \end{aligned} \tag{5.2}$$

If 3 divides $y,\ z$, it is clear from the above expressions that 3 divides $y_1,\ z_1$. Now suppose 3 divides $y_1 = mz^2 + 2xy$ and $z_1 = y^2 + 2xz$. If 3 divides x as well, then 3 has to divide both y and z since $3 \nmid m$. Then 3 would divide each of x, y, z, which leads to a contradiction by (5.1). Therefore 3 does not divide x, and hence $x^2 \equiv 1 \mod 3$. Now we consider the norm of ξ_m^2 to obtain

$$Norm_{K/\mathbb{Q}}(\xi_m^2) = x_1^3 + my_1^3 + m^2 z_1^3 - 3mx_1 y_1 z_1 = 1. \tag{5.3}$$

As $3 \mid y_1$ and $3 \mid z_1$, we find that $x_1^3 \equiv 1 \mod 3$. Therefore,

$$x^2 + 2myz = x_1 \equiv x_1^3 \equiv 1 \mod 3 \Rightarrow 1 + 2myz \equiv 1 \mod 3.$$

So 3 must divide $2myz$ and hence yz as $3 \nmid m$. Using $3 \mid y_1$ or $3 \mid z_1$ in (5.2), it is now easy to conclude that $3 \mid yz$ implies $3 \mid y$ and $3 \mid z$. □

The next lemma follows from the assumption that 3 does not divide the class number of $\mathbb{Q}(\sqrt[3]{m})$. We will use this result throughout this chapter.

Lemma 5.2.2. *Let $q \neq m$ be a prime that ramifies in $K = \mathbb{Q}(\sqrt[3]{m})$. If $3 \nmid h_m$ then either ξ_m or ξ_m^2 can be written as $\frac{\alpha^3}{q}$ for some $\alpha \in K$.*

Proof. As q ramifies in K, we have $q\mathcal{O}_K = \wp^3$ where $\wp$ is a prime ideal in the ring $\mathcal{O}_K$ of integers in K. Thus $\wp$ gives an element of order dividing 3 in the class group of K. As the class number is not divisible by 3, $\wp$ must be principal. In other words, there exists an element $\alpha \in \mathcal{O}_K$ such that $\wp = \alpha\mathcal{O}_K$. Therefore, $q\mathcal{O}_K = \wp^3 = \alpha^3\mathcal{O}_K$, and there is a unit u in $\mathcal{O}_K$ such that $uq = \alpha^3$. We know that $u = \pm\xi_m^j$ for some integer j. If $3 \mid j$, it would imply that either $\sqrt[3]{q} \in K$ or $\sqrt[3]{-q} \in K$ which leads to a contradiction as $q \neq m$. Hence the unit u can be taken as ξ_m^j for either $j = 1$ or $j = 2$ by modifying the element α suitably, and the lemma follows. □

Now we are in a position to prove the following lemma, which is a crucial step in our proof of theorem 5.1.1

Lemma 5.2.3. *Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with a power integral basis (i.e., m is square-free and $m \neq \pm 1 \bmod 9$). If the class number of K is not divisible by 3, then m is either a prime or a multiple of 3.*

Proof. Suppose m is not a prime. We want to show that m must be a multiple of 3. Let $\xi_m = x + yt + zt^2$ $(t = \sqrt[3]{m})$ be the fundamental unit of K. As the class number of K is assumed to be coprime to 3, lemma 5.2.2 is applicable for such m with ramified primes 3 and p. We have $\xi_m^i = \frac{\beta^3}{p}$, $\xi_m^j = \frac{\alpha^3}{3}$ where $i, j \in \{1, 2\}$. We may assume that both $i = j = 1$. For all the other three cases, the following argument still works because of lemma 5.2.1.

Substituting $\beta = a_1 + b_1 t + c_1 t^2$ in $\xi_m = \frac{\beta^3}{p}$, we find that

$$\begin{aligned} p(x + yt + zt^2) = (a_1^3 + mb_1^3 + m^2c_1^3 + 6ma_1b_1c_1) + \\ 3t(a_1^2b_1 + mb_1^2c_1 + ma_1c_1^2) + 3t^2(a_1b_1^2 + a_1^2c_1 + mb_1c_1^2). \end{aligned} \tag{5.4}$$

As $p \neq 3$, it follows that y and z are divisible by 3.

Now we substitute $\alpha = a + bt + ct^2$ in $\xi_m = \frac{\alpha^3}{3}$ and obtain

$$\begin{aligned} x = \frac{a^3 + mb^3 + m^2c^3 + 6mabc}{3}, \qquad y = a^2b + mb^2c + mac^2, \\ z = ab^2 + a^2c + mbc^2. \end{aligned} \tag{5.5}$$

Then 3 divides $(a^2b + mb^2c + mac^2)$ and $(ab^2 + a^2c + mbc^2)$, consequently 3 divides $(a^3 - mb^3)c$. Suppose 3 divides c, then from the expression of y, we can say that 3 divides either a or b. Then from the expression of x and using the fact that $x \in \mathbb{Z}$, we can say 3 divides each of a, b, c as 3 does not divide m. But then, 9 divides $a^3 + mb^3 + m^2c^3 + 6mabc$ and hence 3 divides x along with y and z. Then the norm of the unit ξ_m would be divisible by 3, which is a contradiction. Therefore 3 divides $a^3 - mb^3$.

If $m \equiv 1 \pmod 3$, then $a^3 - mb^3 \equiv 0 \pmod 3$ implies that $a \equiv b \pmod 3$ and also from the expression of x, we can say that $(2a^3 + c^3) \equiv 0 \pmod 3$ and hence $a \equiv c \equiv b \pmod 3$. So now using the fact that if $a \equiv b \pmod 3$ then $a^3 \equiv b^3 \pmod 9$, we can say that $(a^3 + mb^3 + m^2c^3 + 6mabc) \equiv a^3(m^2 + 7m + 1) \equiv 0 \pmod 9$ which in turn implies that x is divisible by 3, again contradiction as y and z are divisible by 3.

Suppose $m \equiv 2 \pmod 3$. Using the same procedure as above we get $a \equiv c \equiv -b \pmod 3$. So, $(a^3 + mb^3 + m^2c^3 + 6mabc) \equiv a^3(m^2 - 7m + 1) \equiv 0 \pmod 9$ always when $m \equiv 2 \pmod 3$ and hence x is again divisible by 3, a contradiction. Therefore $m \equiv 0 \bmod 3$. □

The following corollary is immediate from the above lemma.

Corollary 5.2.4. *For any composite number $m \equiv 2, 4, 5$ or 7 (mod 9), the class number of $\mathbb{Q}(\sqrt[3]{m})$ is divisible by 3.*

Now we prove theorem 5.1.1 with the help of lemma 5.2.3. Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a field with a power integral basis having class number coprime to 3. Suppose m is not a prime. By lemma 5.2.3, m must be divisible by 3. We want to show that $m = 3p$ for some prime p. Suppose m is divisible by two distinct primes p and q other than 3. Then, 3, p and q all ramify in K, and so does $3p$. By lemma 5.2.2 there exist $\alpha,\ \beta \in K$ such that either $\frac{\alpha^3}{3} = \frac{\beta^3}{3p}$ or $(\frac{\alpha^3}{3})^2 = \frac{\beta^3}{3p}$ or $\frac{\alpha^3}{3} = (\frac{\beta^3}{3p})^2$. But these identities imply that a cube root of p or $9p$ belongs to $\mathbb{Q}(\sqrt[3]{m})$, which is not possible as $m \neq p, 9p$. Hence the only possibility is $m = 3p$ where p is a prime.

□

We now discuss some congruence relations for the fundamental unit of $K = \mathbb{Q}(t)$, where $t = \sqrt[3]{m}$ and m is a prime $p \not\equiv \pm 1 \bmod 9$ or $m = 3p$ for any prime $p \neq 3$. We begin by considering $m = 3p$ where p is a prime and prove theorem 5.1.2.

Proof of theorem 5.1.2: By lemma 5.2.2, we know that ξ_m^j can be expressed as $\frac{\alpha^3}{3}$ and as $\frac{\beta^3}{p}$ for some $j \in \{1,2\}$ and $\alpha,\ \beta \in K$. If $\xi_m = \frac{\beta^3}{p}$, then $y \equiv z \equiv 0 \pmod 3$ follows directly from (5.4). If $\xi_m^2 = \frac{\beta^3}{p}$, then $y_1 \equiv z_1 \equiv 0 \pmod 3$ follows similarly. Using (5.2), we now have $y_1 = 3pz^2 + 2xy \Rightarrow xy \equiv 0 \pmod 3$.

If $x \equiv 0 \pmod 3$ then from 5.2 we have $x_1 \equiv y_1 \equiv z_1 \equiv 0 \pmod 3$, a contradiction from the norm equation (5.3) of ξ_m^2. Hence 3 divides y. Now $z_1 \equiv 0 \pmod 3$ implies 3 divides z and hence we again get $y \equiv z \equiv 0 \pmod 3$.

Putting $\alpha = a + bt + ct^2$ in $\xi_m^j = \frac{\alpha^3}{3}$ and taking norm, we obtain

$$\begin{aligned} Norm_{K/\mathbb{Q}}(\alpha)^3 &= 3^3 Norm_{K/\mathbb{Q}}(\xi_m^j) \\ \Rightarrow Norm_{K/\mathbb{Q}}(\alpha) &= a^3 + mb^3 + m^2c^3 - 3mabc = 3. \end{aligned} \tag{5.6}$$

By (5.5), either x or x_1 is $\frac{a^3+mb^3+m^2c^3+6mabc}{3}$ which equals $\frac{3+9mabc}{3}$ by (5.6). As m is divisible by 3, 3 must divide a. Hence either x or x_1 is $1 + 3mabc$. As $m = 3p$, we have either x or x_1 is congruent to 1 (mod $27p$). But $x_1 = x^2 + 2myz \equiv x^2$ (mod $27p$) because $m = 3p$ and $y \equiv z \equiv 0 \pmod 3$. □

Corollary 5.2.5. *If the fundamental unit $\xi_m = x + yt + zt^2$ of $\mathbb{Q}(t)$, ($t = \sqrt[3]{3p}$ where p is a prime other than 3) is such that $3 \nmid y$ or $3 \nmid z$ or $27p \nmid (x^2 - 1)$ then the class number of K is divisible by 3.*

Now we consider the necessary congruence relations satisfied by the fundamental unit of $K = \mathbb{Q}(\sqrt[3]{p})$ when the class number is not divisible by 3. We assume that p is a prime $\not\equiv \pm 1$ mod 9 so that K has a power integral basis, and $p \neq 3$ so that both 3 and p ramifies in K. Note that lemma 5.2.2 is applicable with $q = 3$.

Proposition 5.2.6. *Let $\xi_m = x + yt + zt^2$ be the fundamental unit of $K = \mathbb{Q}(\sqrt[3]{p})$ where p is a prime $\equiv 4$ or 7 mod 9. If $3 \nmid h_p$ then $x^2 \equiv 1$ mod $3p$ and one of the following must hold:*
(i) $x \equiv 1$ mod 3 and $y + z \equiv 0$ mod 3. (ii) $x \equiv 2 \equiv y$ mod 3, $z \equiv 0$ mod 3. (iii) $x \equiv 2 \equiv z$ mod 3 and $y \equiv 0$ mod 3.

Proof. By lemma 5.2.2, we have either $\xi_m = \frac{\alpha^3}{3}$ or $\xi_m^2 = \frac{\alpha^3}{3}$.

In the case $\xi_m = \frac{\alpha^3}{3}$, we substitute $\alpha = a + bt + ct^2$ and using (5.5) and then (5.1) we obtain

$$x = \frac{a^3 + mb^3 + m^2c^3 + 6mabc}{3} = \frac{Norm_{K/\mathbb{Q}}(\alpha) + 9mabc}{3} = \frac{3 + 9pabc}{3} \tag{5.7}$$
$$\Rightarrow x \equiv 1 \bmod 3p.$$

As in (5.6), $Norm_{K/\mathbb{Q}}(\alpha) = 3$ and hence $a^3 + pb^3 + p^2c^3 - 3apbc \equiv 0 \pmod 3$. Since $p \equiv 1 \pmod 3$, we get $a^3 + b^3 + c^3 \equiv 0 \pmod 3$. Hence $a \equiv b \equiv c \pmod 3$ or 3 divides exactly one of a, b, c and the other two are non equivalent mod 3. In the first case, we find using (5.5) that $y = a^2b + pb^2c + pac^2 \equiv a^3 + b^3 + c^3 \equiv 0 \bmod 3$. Similarly $z = ab^2 + a^2c + pbc^2 \equiv 0 \bmod 3$. In the second case, it can be easily seen that $y \equiv -z \not\equiv 0 \bmod 3$.

If $\xi_m^2 = \frac{\alpha^3}{3}$, then (5.2), (5.5) and (5.7) imply that

$$x_1 = x^2 + 2pyz = 1 + 3pabc, \qquad y_1 = pz^2 + 2xy = a^2b + pb^2c + pac^2,$$
$$z_1 = y^2 + 2xz = ab^2 + a^2c + pbc^2. \tag{5.8}$$

As $p \equiv 1 \bmod 3$, just as above we have $y_1 \equiv z_1 \equiv 0 \pmod 3$ or $y_1 \equiv -z_1 \not\equiv 0 \pmod 3$. In the former case, lemma 5.2.1 implies that $y \equiv z \equiv 0 \bmod 3$ and $x^2 \equiv 1 \bmod 3p$. Considering the norm of ξ_m modulo 3 , we find that $x^3 \equiv 1 \bmod 3$. By (5.8) we also have $x^2 \equiv 1 \bmod 3$, so $x \equiv 1 \bmod 3$.

Now suppose $y_1 \equiv -z_1 \not\equiv 0 \bmod 3$. Then $3 \nmid x$, otherwise $z^2 \equiv y_1 \equiv -z_1 \equiv -y^2 \bmod 3$ leads to a contradiction. Hence $x^2 \equiv 1 \bmod 3$, and by (5.8) we have $yz \equiv 0 \bmod 3$ giving $x^2 \equiv 1 \bmod 3p$. Now, either $y \equiv 0 \bmod 3$ or $z \equiv 0 \bmod 3$, but both can not hold in view of lemma 5.2.1. Let $y \equiv 0 \bmod 3$. Considering the norm of ξ_m mod 3, we find $x^3 + z^3 \equiv 1 \bmod 3$. Therefore, $x + z \equiv 1 \bmod 3$. Now $y_1 + z_1 \equiv 0 \bmod 3$ gives $z + 2x \equiv 0 \bmod 3$, i.e., $x \equiv z \bmod 3$. Consequently, $x \equiv z \equiv 2 \bmod 3$. The case $z \equiv 0 \not\equiv y \bmod 3$ is similar. □

For the other primes p such that $\mathbb{Q}(\sqrt[3]{p})$ has power integral basis, we have $p \equiv 2, 5 \bmod 9$ and we get the following analogues statement as in proposition 5.2.6.

Proposition 5.2.7. *Let $\xi_m = x + yt + zt^2$ be the fundamental unit of $K = \mathbb{Q}(\sqrt[3]{p})$ where p is a prime $\equiv 2$ or 5 mod 9. If $3 \nmid h_p$ then $x^2 \equiv 1$ mod $3p$ and one of the following must hold:*

(i) $x \equiv 1$ *mod* 3 *and* $y - z \equiv 0$ *mod* 3.

(ii) $x \equiv 2 \equiv -y$ *mod* 3, $z \equiv 0$ *mod* 3.

(iii) $x \equiv 2 \equiv z$ *mod* 3 *and* $y \equiv 0$ *mod* 3.

Proof. By lemma 5.2.2, we again have either $\xi_m = \frac{\alpha^3}{3}$ or $\xi_m^2 = \frac{\alpha^3}{3}$.

As in the previous proposition, when $\xi_m = \frac{\alpha^3}{3}$, we substitute $\alpha = a + bt + ct^2$ and using (5.5) and then (5.1) we obtain

$$x = \frac{a^3 + mb^3 + m^2c^3 + 6mabc}{3} = \frac{Norm_{K/\mathbb{Q}}(\alpha) + 9mabc}{3} = \frac{3 + 9pabc}{3} \tag{5.9}$$
$$\Rightarrow x \equiv 1 \bmod 3p.$$

As in (5.6), $Norm_{K/\mathbb{Q}}(\alpha) = 3$ and hence $a^3 + pb^3 + p^2c^3 - 3apbc \equiv 0 \pmod 3$. Since $p \equiv 2 \pmod 3$, we get $a^3 + 2b^3 + c^3 \equiv 0 \pmod 3$. Hence $a \equiv -b \equiv c \pmod 3$ or 3 divides exactly one of a, c and the other two are equivalent mod 3 or 3 divides b and $a \equiv -c$ mod 3. In the first case, we find using (5.5) that $y = a^2b + pb^2c + pac^2 \equiv -(a^3 + 2b^3 + c^3) \equiv 0 \bmod 3$. Similarly $z = ab^2 + a^2c + pbc^2 \equiv 0 \bmod 3$. In the second and third cases, it can be easily seen that $y \equiv z \not\equiv 0 \bmod 3$.

If $\xi_m^2 = \frac{\alpha^3}{3}$, then (5.2), (5.5) and (5.9) imply that

$$x_1 = x^2 + 2pyz = 1 + 3pabc, \qquad y_1 = pz^2 + 2xy = a^2b + pb^2c + pac^2,$$
$$z_1 = y^2 + 2xz = ab^2 + a^2c + pbc^2. \tag{5.10}$$

As $p \equiv 2 \bmod 3$, just as above we have $y_1 \equiv z_1 \equiv 0 \pmod 3$ or $y_1 \equiv z_1 \not\equiv 0 \pmod 3$. In the former case, lemma 5.2.1 implies that $y \equiv z \equiv 0 \bmod 3$ and $x^2 \equiv 1 \bmod 3p$. Considering the norm of ξ_m modulo 3 , we find that $x^3 \equiv 1 \bmod 3$. By (5.10) we also have $x^2 \equiv 1 \bmod 3$, so $x \equiv 1 \bmod 3$.

Now suppose $y_1 \equiv z_1 \not\equiv 0 \bmod 3$. Then $3 \nmid x$, otherwise $-z^2 \equiv y_1 \equiv z_1 \equiv y^2 \bmod 3$ leads to a contradiction as it would then demand 3 to divide each of x, y and z

and hence ξ_m. Hence $x^2 \equiv 1 \bmod 3$, and by (5.10) we have $yz \equiv 0 \bmod 3$ giving $x^2 \equiv 1 \bmod 3p$. Now, either $y \equiv 0 \bmod 3$ or $z \equiv 0 \bmod 3$, but both can not hold in view of lemma 5.2.1. Suppose $y \equiv 0 \bmod 3$. Considering the norm of $\xi_m \bmod 3$, we find $x^3 + z^3 \equiv 1 \bmod 3$. Therefore, $x + z \equiv 1 \bmod 3$. Now $y_1 - z_1 \equiv 0 \bmod 3$ gives $2(z^2 - xz) \equiv 0 \bmod 3$, i.e., $x \equiv z \bmod 3$. Consequently, $x \equiv z \equiv 2 \bmod 3$. The case $z \equiv 0 \not\equiv y \bmod 3$ is similar and results into $x \equiv 2 \equiv -y \bmod 3$. And hence the proof follows.

□

The following theorem now follows directly from the previous two propositions.

Theorem 5.2.8. *Let $\xi_m = x + yt + zt^2$ be the fundamental unit of $K = \mathbb{Q}(\sqrt[3]{p})$ where p is a prime $\not\equiv \pm 1$ mod 9. Suppose $3 \nmid h_p$. Then $x^2 \equiv 1$ mod $3p$ and one of the following must hold.*

(i) $x \equiv 2$ mod 3, and 3 divides either y or z but not both.

(ii) $x \equiv 1$ mod 3 and $3 \mid (y + z)$ if $p \equiv 1$ mod 3; $3 \mid (y - z)$ if $p \equiv 2$ mod 3.

5.3 Real quadratic fields with odd class number

In this section we apply our approach to obtain congruence relations for the fundamental unit of a real quadratic field of odd class number. These relations were shown in (Zhang and Yue [2014]). Our approach yields the same congruences in an elementary way. First we state an obvious analogue of lemma 5.2.2 for the real quadratic case.

Lemma 5.3.1. *Let $\xi_d = x + y\sqrt{d} > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$.*

1. If $d = p$ or $2p$ where p is a prime congruent to 3 mod 4, then $2\xi_d = {u_d}^2$ for some $u_d \in \mathcal{O}_K$.

2. If $d = p_1p_2$, where p_1 and p_2 are two distinct primes congruent to $\equiv 3$ mod 4, then $p_1\xi_d = {u_d}^2$ for some $u_d \in \mathcal{O}_K$.

The following result is classically known, but we can also deduce it from the second relation in lemma 5.3.1.

Corollary 5.3.2. *If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field with discriminant having at least three prime factors then the class number of K is even.*

Proof. Suppose $K = \mathbb{Q}(\sqrt{d})$ is the real quadratic field under question. The given condition implies that at least 3 distinct rational primes p, q and r ramify in K. Hence both p and pq ramify in K, but none of them is a square in K. If ξ_d denotes the fundamental unit of K and the class number of K is not divisible by 2, then we can write $\xi_d = \frac{\alpha^2}{p} = \frac{\beta^2}{pq}$ by lemma 5.3.1. Then $\sqrt{q} \in K$, a contradiction. □

We conclude by showing that the congruence relations stated in theorem 5.1.3 follow directly from lemma 5.3.1.

Proof of theorem 5.1.3: Let us first consider the cases $d = p$ or $d = 2p$ where p is a prime congruent to 3 mod 4. By considering the norm of the fundamental unit $\xi_d = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, we have $x^2 - dy^2 = \pm 1$. By lemma 5.3.1, $2\xi_d = {u_d}^2$ for some $u_d = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Hence, $2x = a^2 + db^2$ and $y = ab \in \mathbb{Z}$.

When $d = p \equiv 3 \bmod 4$, we have $2x \equiv a^2 + 3b^2 \bmod 4$, so a and b have same parity. But if both a, b are even then x and y are even as well, contradicting parity in the norm equation $x^2 - dy^2 = \pm 1$. Hence both a and b are odd, so $a^2 \equiv b^2 \equiv 1 \bmod 8$. When $p \equiv 3 \bmod 8$, we further have $2x \equiv a^2 + 3b^2 \equiv 4 \bmod 8$. When $p \equiv 7 \bmod 8$, we have $2x \equiv a^2 + 7b^2 \equiv 8 \bmod 8$, giving $x \equiv 0 \bmod 4$.

When $d = 2p$ with $p \equiv 3 \bmod 4$, then $2x \equiv a^2 + 2b^2 \bmod 4$, hence a must be even, say $a = 2a_1$. Then $y = 2a_1 b$ is even, hence x must be odd. We have $2x = 4a_1^2 + 2pb^2$, hence $x = 2a_1^2 + pb^2$, where b must be odd. Now $x + y \equiv 2a_1^2 + 3b^2 + 2a_1 b = 2a_1(a_1 + b) + 3b^2$. As b is odd, either a_1 is even or $a_1 + b$ is even. Therefore, $x + y \equiv 3 \bmod 4$.

Finally $d = p_1 p_2$ where p_1 and p_2 are two distinct primes congruent to 3 mod 4. When $d \equiv 1 \bmod 8$, we still have $\xi_d = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, and $\mathcal{O}_K = \{\frac{a}{2} + \frac{b}{2}\sqrt{d} \mid$

$a, b \in \mathbb{Z}, a \equiv b \bmod 2\}$. By applying lemma 5.3.1 with the ramified prime p_1, we get $p_1(x + y\sqrt{d}) = (\frac{a}{2} + \frac{b}{2}\sqrt{d})^2$, which gives $4p_1x = a^2 + db^2$ and $4p_1y = 2ab$ for integers $a, b \in \mathbb{Z}$ of same parity. As $y \in \mathbb{Z}$, one of a or b must be even, hence both are even, say $a = 2a_1, b = 2b_1$ and y itself is even. Now $p_1x = a_1^2 + db_1^2 \Rightarrow 3x \equiv a_1^2 + b_1^2$. As y is even, x must be odd. So a_1 and b_1 have different parity and $a_1^2 + db_1^2 \equiv 1 \bmod 4$. Consequently, $3x \equiv 1 \bmod 4 \Rightarrow x \equiv 3 \bmod 4$, and $3y \equiv 2a_1b_1 \equiv 0 \bmod 4$ so that $4 \mid y$. When $d = p_1p_2 \equiv 5 \bmod 8$, we view the second relation in lemma 5.3.1 as $p\xi_d^3 = \alpha^2\xi_d^2 = \beta^2 = (\frac{a}{2} + \frac{b}{2}\sqrt{d})^2$ for some $\beta \in \mathcal{O}_K$, where a and b are integers of same parity. Letting $\xi_d^3 = x + y\sqrt{d}$ we then proceed as before to obtain $4p_1x = a^2 + db^2$, $4p_1y = 2ab$ and similarly conclude that $x \equiv 3 \bmod 4$ and $y \equiv 0 \bmod 4$. □

5.4 Examples

We illustrate our results with the following lists. We use the computation in (Wada [1970]) for the fundamental unit of purely cubic fields, and use SAGE (Stein [2014]) for the computation of the class number. The list in Table 1 below shows that if $m = p \not\equiv \pm 1 \bmod 9$ or $m = 3p$ where p is a prime, then the class number h_m of $K = \mathbb{Q}(\sqrt[3]{m})$ must be divisible by 3 as stated in theorem 5.1.3.

Table 5.1: $m \neq p, 3p$, $m \not\equiv \pm 1 \bmod 9$ & m square-free

m	14	22	30	34	38	42	58	60	65
h_m	3	3	3	3	3	3	3	3	18
m	66	74	77	78	85	86	92	94	95
h_m	6	3	3	9	3	3	3	3	3

Next, we consider examples for theorem 5.1.2 where $m = 3p$ is square-free. In Table 2 we give a list of integers m for which the fundamental unit $\xi_m = x + yt + zt^2$ does

not satisfy the congruences in theorem 5.1.2, so that h_m must be divisible by 3.

Table 5.2: $m = 3p$, where $p \neq 3$ is a prime

m	$x^2 \bmod 27$	$x^2 \bmod p$	$y \bmod 3$	$z \bmod 3$	h_m
21	$1705^2 \not\equiv 1$	$1705^2 \not\equiv 1$	$618 \equiv 0$	$224 \equiv 0$	3
39	$529^2 \not\equiv 1$	$529^2 \not\equiv 1$	$156 \equiv 0$	$46 \not\equiv 0$	6
57	$1460968^2 \not\equiv 1$	$1460968^2 \equiv 1$	$379620 \equiv 0$	$98641 \not\equiv 0$	6

Then in Table 3 we consider examples for theorem 5.1.2 where $m = 3p$ is square-free and $3 \nmid h_m$. We verify that the fundamental unit $\xi_m = x + yt + zt^2$ indeed satisfies the congruences in the theorem 5.1.2.

Table 5.3: $m = 3p$, where $p \neq 3$ is a prime and $3 \nmid h_m$

m	h_m	$x^2 \bmod 27$	$x^2 \bmod p$	$y \bmod 3$	$z \bmod 3$
6	1	$109^2 \equiv 1$	$109 \equiv 1$	$60 \equiv 0$	$33 \equiv 0$
15	2	$5401^2 \equiv 1$	$5401 \equiv 1$	$2190 \equiv 0$	$888 \equiv 0$
33	1	$152706740741292 \equiv 1$	$15270674074129^2 \equiv 1$	$4760876269140 \equiv 0$	$1484279131362 \equiv 0$

Finally we consider examples for proposition 5.2.7 where $m = p \equiv 2$ or 5 mod 9 and $3 \nmid h_m$ in the Table 4 below. We verify that when h_m is not divisible by 3, the fundamental unit $\xi_m = x + yt + zt^2$ of norm 1 satisfies the congruences in theorem 5.2.8, or more precisely, in proposition 5.2.7.

Table 5.4: $m = p$ where p is a prime $\equiv 2$ or $5 \bmod 9$

m	h_m	$x \bmod 3$	$x^2 \bmod 3p$	$y \bmod 3$	$z \bmod 3$
2	1	$1 \equiv 1$	$1 \equiv 1$	$1 \equiv 1$	$1 \equiv 1$
5	1	$41 \equiv 2$	$41^2 \equiv 1$	$24 \equiv 0$	$14 \equiv 2$
11	2	$89 \equiv 2$	$89^2 \equiv 1$	$40 \equiv 1$	$18 \equiv 0$
23	1	$2166673601 \equiv 2$	$2166673601^2 \equiv 1$	$761875860 \equiv 0$	$267901370 \equiv 2$

6

A Construction for Unramified Quadratic Extension

6.1 Introduction

As we stated earlier, the class group of a number field K measures how far its ring of integers is from having unique factorization into irreducible elements. While the class group is defined as the quotient of the group of all fractional ideals of K by the subgroups of principal fractional ideals, it can also be viewed as the Galois group of the maximal unramified abelian extension of K by class field theory.

Soleng (Soleng [1994]) gave a construction of families of quadratic number fields

from an elliptic curve having ideal class group isomorphic to the torsion group of the curve. A. Sato constructed quadratic number fields with class number divisible by 5 from elliptic curves in (Sato et al. [2011]). Lemmermeyer (Lemmermeyer [2013]) showed a method for constructing unramified quadratic extension of cubic fields using points on suitable elliptic curves. Drawing our inspiration from (Lemmermeyer [2013]), we explicitly construct a quadratic unramified extension for each biquadratic field in an infinite family which originates from a non-torsion rational point on a suitably chosen elliptic curve.

The genus field of $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ has been discussed in detail by Ouyang Yi and Zhang Zhe (Ouyang and Zhang [2014]), Sunghan Bae and Qin Yue (Bae and Yue [2011]) and Qin Yue (Yue [2010]) when at least one of a and b is a prime of the form 1 *mod* 4. Our results give quadratic unramified extension of infinitely many biquadratic fields $\mathbb{Q}(\sqrt{r}, \sqrt{m})$ where, if m is suitably chosen, both r and m will be composite or none of r and m will be a prime congruent to 1 mod 4. In 6.3.2, we apply our construction for infinitely many biquadratic fields $\mathbb{Q}(\sqrt{r_i}, \sqrt{3})$ where r_i's are square-free composite numbers. As a consequence, we in fact get an alternative and constructive proof for existence of infinitely many biquadratic fields of even class number Our main result can be stated as follows.

Theorem 6.1.1. ***(Chakraborty and Saikia [2016b])***

Let $m \neq 0, 1$ be a square-free integer which is divisible by 3 if it is positive. Let $P_0 = \left(\frac{r_0}{t_0^2}, \frac{s_0}{t_0^3}\right)$ be any non-torsion point of the elliptic curve $y^2 = x^3 + m$ such that r_0 is odd and non-square. Let $\left(\frac{r_i}{t_i^2}, \frac{s_i}{t_i^3}\right) = 2^i P_0$ for each natural number i. Then the biquadratic field $K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{m})$ has an everywhere unramified quadratic extension $K_i(\sqrt{\beta_i})$, where β_i is either $\pm(s_i + t_i^3\sqrt{m})$ or $3(s_i + t_i^3\sqrt{m})$.

We will identify the precise form of β_i later (see (6.8)). When r_0 is a square and t_0 is even, our construction gives an unramified extension of the quadratic field $\mathbb{Q}(\sqrt{m})$ but for the extension to be non-trivial we need to add an additional condition, for example, $0 < s < m$ (6.3.3). In order to prove theorem 6.1.1, we carefully associate

a non-torsion point P with a suitable element β in a biquadratic field K. We show that β generates the square of a fractional ideal. Then the extension $K(\sqrt{\beta})/K$ is unramified at all finite primes other than those lying above 2. If we can choose $\beta \equiv 1$ modulo 4, then the primes above 2 are also unramified in $K(\sqrt{\beta})/K$. Finally we consider the infinite primes and show that $K(\sqrt{\beta})/K$ is a quadratic extension which is unramified everywhere. These steps will be completed in §2. In §3, we show that the biquadratic fields K_i obtained from the multiples 2^iP_0 of the initial non-torsion point P_0 are all distinct for distinct values $i = 1,\ 2,\ \cdots$.

6.2 Unramified quadratic extension from a non-torsion point

We fix the following notation for the rest of the chapter. For any square-free integer $m \neq 0, 1$, we consider the elliptic curve

$$E_m : \qquad y^2 = x^3 + m. \tag{6.1}$$

By P we denote an arbitrary non-torsion rational point on E_m. Clearly, P can be written as $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ where r, s and t are integers with $gcd(r, t) = 1 = gcd(s, t)$. We may take s and t to be positive as we can replace P by its inverse $-P$ on E_m. On substitution, we find that

$$s^2 = r^3 + mt^6. \tag{6.2}$$

If s is not coprime to m then by (6.2) any common prime factor p will also divide r and hence m will be divisible by p^2. Therefore $gcd(s, m) = 1$. Similarly $gcd(r, m) = 1$.

Lemma 6.2.1. *Consider the duplication formula for the point $P = (\frac{r}{t^2}, \frac{s}{t^3})$ on $y^2 = x^3 + m$:*

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(9r^3 - 8s^2)}{(2st)^2}, \frac{27r^6 - 36r^3s^2 + 8s^4}{(2st)^3}\right) \tag{6.3}$$

Suppose m is square-free and r is odd. If $3 \nmid s$, the fractions on the right hand side of (6.3) are already in their reduced form. When $s = 3s'$ the fractions on the right hand side above reduces to

$$\left(\frac{r(2P)}{t(2P)^2}, \frac{s(2P)}{t(2P)^3}\right) = 2P = \left(\frac{r(r^3 - 8s'^2)}{(2s't)^2}, \frac{r^6 - 12r^3s'^2 + 24s'^4}{(2s't)^3}\right). \tag{6.4}$$

Proof: As m is square-free, it is clear from (6.2) that r and s are coprime, else the square of their common divisor will divide m. From the duplication formula (6.3) it is clear that the numerator $r(9r^3 - 8s^2)$ of $x(2P)$ is odd as r is odd. Now if p is a common prime divisor of t and the numerator $r(9r^3 - 8s^2)$ of $x(2P)$, then p divides $9r^3 - 8s^2$ as r and t are coprime. But $s^2 = r^3 + mt^6$ implies p also divides $r^3 - s^2$, and hence p divides $9r^3 - 8s^2 - 8(r^3 - s^2) = r^3$ which contradicts the fact that r and t are coprime. If p is a prime divisor of s and the numerator of $x(2P)$, then p has to divide $9r^3 - 8s^2$ as r and s are coprime. Then, p has to divide $9r^3$ and hence 9 as p can not divide both r and s. So the only possibility for a common prime divisor of of the numerator and the denominator of $x(2P)$ is $p = 3$ and in that case 3 divides s.

The y-coordinate $27r^6 - 36r^3s^2 + 8s^4$ of $2P$ in (6.3) is odd as r is odd. If p is a common prime divisor of t and $27r^6 - 36r^3s^2 + 8s^4$, then p also divides $r^3 - s^2$ from (6.2). Hence p divides $27r^6 - 36r^3s^2 + 8s^4 - 27r^3(r^3 - s^2) + 9s^2(r^3 - s^2) = -s^4$, which contradicts the fact that s and t are coprime. If p is a common prime divisor of s and $27r^6 - 36r^3s^2 + 8s^4$ then p must divide $27r^6$. But r and s are coprime, so $p = 3$ can be the only common prime divisor of the numerator and the denominator of $y(2P)$, and in that case 3 divides s.

Therefore, when $3 \nmid s$ the fractions on the right hand side of (6.3) are in their reduced form. If $s = 3s'$, then we can cancel 3^2 for the $x(2P)$ and 3^3 for the $y(2P)$ and obtain the reduced form give in (6.4). □

From the duplication formula, it is also clear that if $r(P)$ is odd, $t(2P)$ must be even and hence $s(2P)$ must be odd. Hence from now on, we assume $t = t(P)$ to

be even and $s = s(P)$ is odd without any further loss of generality. We make the following assumption on the co-ordinates of the point $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$.

Assumption 6.2.2. *(i) r is odd (ii) r is a non-square (iii) t is even.*

It can be seen from the duplication formula that if $r = r(P)$ is odd, so is $r(2P)$. If r is a non-square and $gcd(r, s) = 1$, then $r(2P)$ is also a non-square. Thus our assumption 6.2.2 holds for $2P$ if it does for P.

If we allow r to be a square, then our construction gives an unramified quadratic extension of the quadratic field $\mathbb{Q}(\sqrt{m})$ under an additional condition $(0 < s < m)$. We illustrate this point in example (6.3.3) later.

For such a point P satisfying our assumption 6.2.2, we associate a biquadratic extension K and an element α as follows:

$$K = \mathbb{Q}(\sqrt{r}, \sqrt{m}), \qquad \alpha = s + \sqrt{m}t^3 \in K. \tag{6.5}$$

As t is even, we note that

$$\alpha \equiv s \text{ modulo } 4. \tag{6.6}$$

The following lemma is crucial for the proof of the main theorem.

Lemma 6.2.3. *Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a non-torsion point of the elliptic curve E_m satisfying our assumption 6.2.2 with t even. Then α and its conjugate $\bar{\alpha}$ over $\mathbb{Q}(\sqrt{r})$ generate coprime ideals in the ring $\mathcal{O}_K$ of integers in K. Moreover, there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $\langle\alpha\rangle := \alpha\mathcal{O}_K = \mathfrak{a}^2$.*

Proof: Note that we have

$$N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) = \alpha\bar{\alpha} = (s + \sqrt{m}t^3)(s - \sqrt{m}t^3) = s^2 - mt^6 = r^3. \tag{6.7}$$

Now, suppose there exists some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\mathfrak{p}$ appears in the prime factorization of both the ideals $\langle\alpha\rangle$ and $\langle\bar{\alpha}\rangle$. Then $\alpha + \bar{\alpha} = 2s \in \mathfrak{p}$. But $r^3 = N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) \in \langle\alpha\rangle \subset \mathfrak{p}$ and r is odd under our assumption 6.2.2. Therefore, $2 \notin \mathfrak{p}$

and we must have $s \in \mathfrak{p}$. Similarly, $2\sqrt{m}t^3 = \alpha - \bar{\alpha} \in \mathfrak{p}$ implies either $t \in \mathfrak{p}$ or $m \in \mathfrak{p}$. Hence either both s and t belong to $\mathfrak{p}$ or both s and m belongs to $\mathfrak{p}$. But then it will contradict the fact that s is coprime to both m and t. Hence α and $\bar{\alpha}$ generate coprime ideals in $\mathcal{O}_K$.

Now $\alpha.\bar{\alpha} = N_{K/\mathbb{Q}(\sqrt{r})}(\alpha) = (r\sqrt{r})^2$ implies $\langle\alpha\rangle = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$ in $\mathcal{O}_K$. □

For our subsequent argument, we need m to be divisible by 3 when $m > 0$ and $s \equiv 3$ modulo 4. We can deduce a corollary of the above lemma in the case when the integer m is a positive multiple of 3. The corollary will be needed in §3 for showing that at each stage of duplication of a non-torsion point we indeed get a unramified quadratic extension of a biquadratic field.

Corollary 6.2.4. *With the same notation as in the previous lemma, the element* $3\alpha = 3(s + \sqrt{m}t^3)$ *generates the square of an ideal in the ring of integers of* $K = \mathbb{Q}(\sqrt{m}, \sqrt{r})$ *if* m *is divisible by* 3.

Proof: If 3 divides the square-free integer m, then 3 generates the square of a prime ideal in $\mathbb{Q}(\sqrt{m})$, and hence it generates the square of an ideal in $\mathbb{Q}(\sqrt{m}, \sqrt{r})$. As α generates the square of some ideal by the previous lemma, the corollary follows. □

For the biquadratic extension $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ associated with the non-torsion point P, we want to construct a quadratic extension unramified at all finite as well as infinite primes of K. We consider the extension

$$K(\sqrt{\beta}), \qquad \text{where } \beta = \begin{cases} \alpha \text{ if } s \equiv 1 \text{ modulo } 4 \\ -\alpha \text{ if } s \equiv 3 \text{ modulo } 4 \text{ and } m < 0 \\ 3\alpha \text{ if } s \equiv 3 \text{ modulo } 4 \text{ and } m > 0. \end{cases} \tag{6.8}$$

Observe that $\beta \equiv 1$ modulo 4 in view of (6.6). We first deal with the finite primes.

Lemma 6.2.5. *The extension* $K(\sqrt{\beta})$ *over* $K = \mathbb{Q}(\sqrt{r}, \sqrt{m})$ *is quadratic and unramified at all finite primes.*

Proof: First we prove that $K(\sqrt{\beta})$ is indeed a quadratic extension of K. Let us show it explicitly for $\beta = \alpha$. The cases $\beta = -\alpha$ or 3α are analogous. If possible, first assume that $\sqrt{\alpha} = a + b\sqrt{m}$ where $a, b \in \mathbb{Q}$. By comparing coefficients of $\sqrt{m}$, we get $a^2 + mb^2 = s$ and $2ab = t^3$. Hence,

$$r^3 = s^2 - mt^6 = (a^2 + mb^2)^2 - 4a^2b^2m = (a^2 - mb^2)^2$$

implies that r is a square, which is a contradiction. Now consider $\sqrt{\alpha} = a + \sqrt{m}b$ where at least one of a and b is in $\mathbb{Q}(\sqrt{r}) - \mathbb{Q}$, say $a = u + v\sqrt{r}$ where $u,\ 0 \neq v \in \mathbb{Q}$. Comparing coefficients of $\sqrt{m}$ in $\mathbb{Q}(\sqrt{r})$, we still obtain $2ab = t^3$ which means that b must be a rational multiple of the conjugate of a, i.e., $b = k\bar{a} = k(u - v\sqrt{r})$ for some $k \in \mathbb{Q}$. Then,

$$a^2 + mb^2 = s \implies 2uv\sqrt{r}(1 - mk^2) = 0.$$

But $1 - mk^2 \neq 0$ as m is a square-free integer and k is a rational number. If $u = 0$ then $2ab = t^3$ will force $r = 1$. Therefore we can conclude that $\mathbb{Q}(\sqrt{r}, \sqrt{\alpha})$ is indeed a quadratic extension of K.

As $\beta \equiv 1 \bmod (4)$, any prime over 2 in K is unramified in $K(\sqrt{\beta})/K$. By lemma 6.2.3 and corollary 6.2.4, we know that $\langle\beta\rangle = \mathfrak{a}^2$, hence no other finite primes can ramify in this extension. □

Now we consider whether the infinite primes can ramify in $K(\sqrt{\beta})/K$.

Lemma 6.2.6. *The infinite primes do not ramify in* $K(\sqrt{\beta})/K$.

Proof: If $m < 0$ then the infinite prime already ramifies in the extension $K = \mathbb{Q}(\sqrt{m}, \sqrt{r})$ over $\mathbb{Q}$. If $m > 0$, then $\alpha = s + \sqrt{m}t^3 > 0$ as s and t are positive integers and $\sqrt{\beta}$ is real. □

Thus, in this section we have explicitly constructed an everywhere unramified quadratic extension of a biquadratic field that we associate with a non-torsion rational point on the elliptic curve E_m where the co-ordinates of the point satisfy certain mild conditions. Note that we need m to be divisible by 3 only in the case when

$s \equiv 3$ modulo 4. As long as we have $s \equiv 1$ modulo 4 for the point $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ that satisfies our assumption 6.2.2, the field $\mathbb{Q}(\sqrt{m}, \sqrt{s + \sqrt{m}t^3})$ becomes an unramified quadratic extension of $\mathbb{Q}(\sqrt{m}, \sqrt{r})$.

6.3 The Construction for an Infinite Family

In this section we show that we can start with a non-torsion point P_0 and repeat the procedure of the previous section for each multiple $P_i = 2^i(P_0) = \left(\frac{r_i}{t_i^2}, \frac{s_i}{t_i^3}\right)$. It follows from the duplication formula (6.4) that if s_{i-1} is divisible by 3, then $s_i \equiv 1$ modulo 4, and otherwise $s_i \equiv 3$ modulo 4 from (6.3). Just as in (6.5), we associate with P_i a biquadratic extensions K_i and element α_i in K_i:

$$K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{m}), \qquad \alpha_i = s_i + \sqrt{m}t_i^3 \in K_i. \tag{6.9}$$

We obtain an everywhere unramified quadratic extension $K(\beta_i)$ (where $\beta_i = \pm\alpha_i$ or $3\alpha_i$ as in (6.8)). We now show that the biquadratic fields K_i's are all distinct as i varies over natural numbers.

Lemma 6.3.1. *Suppose the initial non-torsion point P_0 on E_m is such that*
(a) r_0 is square-free and t_0 is even.
(b) If $r_0 \equiv 1$ mod (4), then r_0 has a prime factor $p \not\equiv 1, 3$ mod (8).
Then the extensions $\mathbb{Q}(\sqrt{r_i})$ are distinct for distinct values of i.

Proof: First assume that $3 \nmid s_{i-1}$. From the duplication formula (6.3), we have $r_i = r_{i-1}(9r_{i-1}^3 - 8s_{i-1}^2)$. Hence is follows that r_i is odd for all i if r_0 is odd. As $gcd(r_{i-1}, s_{i-1}) = 1$, hence $gcd(r_{i-1}, 9r_{i-1}^3 - 8s_{i-1}^2) = 1$, and hence r_i is not a square if r_{i-1} is not a square. Moreover, if $r_0 \equiv 3$ mod 4 then $9r_0^3 - 8s_0^2 \equiv 3$ modulo 4 and hence is not a square. Now suppose $r_0 \not\equiv 3$ mod 4. If $9r_0^3 - 8s_0^2$ is a square then -2 will be a quadratic residue for any p dividing r_0 and hence r_0 will only have prime factor congruent to 1 or 3 modulo 8, contradicting our assumption (b). As r_i is a multiple of r_0, this argument ensures that $9r_i^3 - 8s_i^2$ is never a square. r_i is

obtained form r_{i-1} by multiplying with a coprime integers, So new prime factors of odd exponent get introduced at each step when we pass from r_i to r_{i+1} and the result follows.

When $3 \mid s_{i-1}$, the same argument works by replacing $(9r^3 - 8s^2)$ with $(r^3 - 8s'^2)$ where $s' = \frac{s}{3}$ as in (6.4). □

Example 6.3.2. Suppose we choose our curve to be $y^2 = x^3 + 3$. Now assuming $P_0 = (1, 2)$ we find that $2P_0$ is $\left(\frac{-23}{16}, \frac{11}{64}\right)$. From the duplication formula (6.3) we find that $2^2P_0 = (\frac{2540833}{88^2}, \frac{4050085583}{88^3})$, and hence using our results we can conclude that $\mathbb{Q}(\sqrt{2540833}, \sqrt{3}, \sqrt{\beta})$ is an unramified quadratic extension of $\mathbb{Q}(\sqrt{2540833}, \sqrt{3})$, where $\beta = 4050085583 + 88^3\sqrt{3}$.

From the duplication formula (6.3) we see that $23 \not\equiv 1, 3 \pmod 8$ is always a divisor of the numerator of the x-coordinate of 2^iP_0 for $i > 0$. We can conclude that the infinite family of biquadratic fields $K_i = \mathbb{Q}(\sqrt{r_i}, \sqrt{3})$ obtained from the rational points 2^iP_0 of the elliptic curve $y^2 = x^3 + 3$ has an unramified abelian quadratic extension given by $K_i(\sqrt{\beta_i})$ for each $i > 0$. □

Next we consider examples of $(\frac{r}{t^2}, \frac{s}{t^3})$ on $y^2 = x^3 + m$ where r is a square but $0 < s < m$. Then by our construction, $L = \mathbb{Q}(\sqrt{m}, \sqrt{s + t^3\sqrt{m}})$ is unramified over $K = \mathbb{Q}(\sqrt{m}$, and if $0 < s < m$ then $s + t^3\sqrt{m}$ can not be a square in K so that L is a quadratic unramified extension of K. □

Example 6.3.3. Considering the point $(\frac{3^2}{4}, \frac{133}{8})$ on $y^2 = x^3 + 265$, we find that $133 < 265$ and hence $\mathbb{Q}(\sqrt{265}, \sqrt{133 + 8\sqrt{265}})$ is a quadratic unramified extension of $\mathbb{Q}(\sqrt{265})$. □

7

Future Work

The main focus of our recent work is related to the theme of Chapter 6. We have been studying the relation between the point on an elliptic curve and the class number of the number field generated by that point.

In (Vaughan [1984]), T. P. Vaughan gave a definition of semi-cube. With the help of semi-cube she gave a necessary and sufficient condition for a quadratic field $\mathbb{Q}(\sqrt{m})$ to have an abelian unramified cubic extension. As a consequence, she obtained a characterization for the field $\mathbb{Q}(\sqrt{m})$ to have class number divisible by 3. Keeping her work in mind, we are trying to relate divisibility of the class number of a real quadratic field by 3 to existence of a point of infinite order on a suitable elliptic curve.

For any totally real number field k and for any prime number p, the Iwasawa invariants $\lambda_p(k)$ and $\mu_p(k)$ capture the growth of the p-part of the class number as we go along the tower of fields in the cyclotomic $\mathbb{Z}_p$-extension of k. While the invariant $\mu_p(k)$ is shown to be 0 for any abelian extension k of $\mathbb{Q}$, Greenberg conjectured that Iwasawa invariant $\lambda_p(k)$ vanishes when k is totally real (Greenberg [1976]). The vanishing of these invariants implies that the p-part of the class number stabilizes eventually as we go along the tower of fields in the cyclotomic $\mathbb{Z}_p$-extension of k. For a totally real number field k of finite degree and a real cyclic extension K/k of degree p, a necessary and sufficient condition has been given for vanishing of $\lambda_p(K)$(Fukuda et al. [1997]). Inspired by that result, we are working towards a construction of an infinite family of bi-quadratic fields with λ_2-invariant zero. Furthermore, we are trying to obtain certain easily verifiable consequences of Greenberg's conjecture in terms of the coordinates of points on a suitable elliptic curve.

Bibliography

Bae, S. and Yue, Q.: 2011, Hilbert genus fields of real biquadratic fields, *The Ramanujan Journal* **24**(2), 161–181.

Baker, A.: 1971, Imaginary quadratic fields with class number 2, *Annals of mathematics* pp. 139–152.

Chakraborty, D. and Saikia, A.: 2014, Another look at real quadratic fields of relative class number 1, *Acta Arithmetica* **163**(4), 371–377.

Chakraborty, D. and Saikia, A.: 2015, On relative class number and continued fractions, *Bull. Korean Math. Soc* **52**(5), 1559–1568.

Chakraborty, D. and Saikia, A.: 2016a, Congruence relations for the fundamental unit of a pure cubic field and its class number, *Journal of Number Theory* **166**, 76–84.

Chakraborty, D. and Saikia, A.: 2016b, An explicit construction for unramified quadratic extension of bi-quadratic fields, *Submitted* .

Cohn, H.: 1962, A numerical study of the relative class numbers of real quadratic integral domains, *Mathematics of Computation* **16**(78), 127–140.

Davenport, H.: 1999, *The higher arithmetic: An introduction to the theory of numbers*, Cambridge University Press.

Dirichlet, L.: 1856, Une propriété des formes quadratiques a déterminant positif, *J. de Math. Pure. Appl* **2**, 76–79.

Finch, S. R.: 2003, *Mathematical constants*, Cambridge university press.

Fukuda, T., Komatsu, K., Ozaki, M., Hisao, T. et al.: 1997, On iwasawa λ_p-invariants of relative real cyclic extensions of degree p, *Tokyo Journal of Mathematics* **20**(2), 475–480.

Furness, A. and Parker, A. E.: 2012, On Dirichlet's conjecture on relative class number one, *Journal of Number Theory* **132**(7), 1398–1403.

Gauss, C. F.: 1966, *Disquisitiones arithmeticae*, Vol. 157, Yale University Press.

Gerth, F. et al.: 1976, Cubic fields whose class numbers are not divisible by 3, *Illinois Journal of Mathematics* **20**(3), 486–493.

Goldfeld, D.: 1985, Gauss class number problem for imaginary quadratic fields, *Bulletin of the American Mathematical Society* **13**(1), 23–37.

Goldfeld, D. M.: 1976, The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer, *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze* **3**(4), 623–663.

Greenberg, R.: 1976, On the iwasawa invariants of totally real number fields, *American Journal of Mathematics* **98**(1), 263–284.

Gross, B. H. and Zagier, D. B.: 1986, Heegner points and derivatives ofl-series, *Inventiones mathematicae* **84**(2), 225–320.

Heegner, K.: 1952, Diophantische analysis und modulfunktionen, *Mathematische Zeitschrift* **56**(3), 227–253.

Heilbronn, H.: 1934, On the class-number in imaginary quadratic fields, *The Quarterly Journal of Mathematics* (1), 150–160.

Honda, T.: 1960, Isogenies, rational points and section points of group varieties, *Japanese journal of mathematics: transactions and abstracts*, Vol. 30, The Mathematical Society of Japan, pp. 84–101.

Honda, T.: 1968, On real quadratic fields whose class numbers are multiples of 3, *J. reine angew. Math* **233**(1), 101–102.

Lemmermeyer, F.: 2013, Why is the class number of $\mathbb{Q}(\sqrt{11})$ even?, *Mathematica Bohemica* **138**(2), 149–163.

Mollin, R. A.: 1995, *Quadratics*, Vol. 2, CRC Press.

Mollin, R. A.: 2013, Proof of relative class number one for almost all real quadratic fields and a counterexample for the rest, *Gen* **17**(2), 81–90.

Niven, I., Zuckerman, H. S. and Montgomery, H. L.: 2008, *An introduction to the theory of numbers*, John Wiley & Sons.

Ouyang, Y. and Zhang, Z.: 2014, Hilbert genus fields of biquadratic fields, *Science China Mathematics* **57**(10), 2111–2122.

Sato, A. et al.: 2011, On the class numbers of certain number fields obtained from points on elliptic curves iii, *Osaka Journal of Mathematics* **48**(3), 809–826.

Silverman, J. H.: 1986, *The arithmetic of elliptic curves*, Springer-Verlag.

Soleng, R.: 1994, Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields, *Journal of Number Theory* **46**(2), 214–229.

Stark, H.: 1971, A transcendence theorem for class-number problems, *Annals of mathematics* pp. 153–173.

Stark, H.: 1972, A transcendence theorem for class-number problems (ii), *Annals of Mathematics* pp. 174–209.

Stark, H. M. et al.: 1967, A complete determination of the complex quadratic fields of class-number one., *The Michigan Mathematical Journal* **14**(1), 1–27.

Stein, W.: 2014, Sage mathematics software 6. 2.

Stephens, A. and Williams, H.: 1988, Some computational results on a problem concerning powerful numbers, *Mathematics of Computation* **50**(182), 619–632.

Stewart, I. and Tall, D.: 2015, *Algebraic number theory and Fermat's last theorem*, CRC Press.

Vaughan, T. P.: 1984, The construction of unramified abelian cubic extensions of a quadratic field, *Acta Arithmetica* **44**(4), 379–387.

Wada, H.: 1970, A table of fundamental units of purely cubic fields, *Proc. Jpn. Math. Soc.* **46**, 1135–1140.

Yue, Q.: 2010, Genus fields of real biquadratic fields, *The Ramanujan Journal* **21**(1), 17–25.

Zhang, Z. and Yue, Q.: 2014, Fundamental units of real quadratic fields of odd class number, *Journal of Number Theory* **137**, 122–129.