The Class Number Formula for Quadratic Fields and Related Results

Roy Zhao

January 31, 2016

Contents

1 Acknowledgements

I would like to thank my advisor Professor Richard Pink for his helpful discussions with me on this subject matter throughout the semester, and his extremely helpful comments on drafts of this paper. I would also like to thank Professor Chris Skinner for helping me choose this subject matter and for reading through this paper. Finally, I would like to thank Princeton University and ETH Zurich for providing me the amazing opportunity to spend an exchange semester in Zurich, Switzerland.

2 Notation

$\lvert X\rvert$	The cardinality of a finite set X
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$	The natural numbers (not including 0), the integers, and rationals
$\mathbb{Q}[\sqrt{D}]$	The field $\{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$
$\mathcal{O}_D$	The ring of integers in $\mathbb{Q}[\sqrt{D}]$
$\mathcal{O}_D^\times$	The set of units in the ring $\mathcal{O}_D$, namely all elements which have an inverse
η	The fundamental unit of a real ring of integers. It satisfies $\eta > 1$.
h	The class number of a quadratic field
$\mathfrak{a}, \mathfrak{b}$	Ideals of a ring
$\mathfrak{p}$	Prime ideals of a ring
$\mathscr{I}$, $\mathscr{J}$	Fractional ideals of an integral domain
$\mathbf{A}, \mathbf{B}$	Ideal classes in the ideal class group

3 Introduction

This paper is an expository piece into the ideal properties of quadratic field extensions $K/\mathbb{Q}$. The arithmetic of K is reviewed and exciting and important results are stated for the unique factorization of ideals in the ring of integers of K, and the ideal class group of K. The main result is the class number formula for real and imaginary quadratic fields. Afterwards, some related propositions and theorems are presented about the Dedekind ζ-function and Dirichlet L-series for a field. Due to wanting to keep the length of this piece short, only the main results are proven in depth, but references to proofs are given to the other main propositions and theorems.

The arithmetic of quadratic fields has a very rich history with Euler using the unique prime factorization of certain quadratic fields to find integer points on elliptic curves [4]. For example, to find lattice points $(x, y) \in \mathbb{Z}^2$ satisfying $y^3 = x^2 + 2$, Euler factorized the right side as $(x+\sqrt{-2})(x-\sqrt{-2})$. Since there is unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$, and $x+\sqrt{-2}, x-\sqrt{-2}$ are relatively prime, Euler determined that there must exist integers $a, b \in \mathbb{Z}$ such that

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 \quad \text{and} \quad x - \sqrt{2} = (a - b\sqrt{-2})^3.$$

But not all quadratic fields possess unique prime factorization, such as $\mathbb{Z}[\sqrt{-5}]$ where

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It was Dedekind who was able to remedy this by proving that there is unique prime factorization of ideals in all of these rings. Based on the work of Kummer in cyclotomic fields, Dedekind developed the theory of the ideal class group for quadratic field extensions, as well as a generalization of it to all finite field extensions [4]. The cardinality of the ideal class group is a rough measurement for how far the field is from being a principal ideal domain, and hence possessing unique prime factorization of its elements. Dedekind showed that this group is finite. So a natural question to ask would be "what is the asymptotic behavior of these class numbers and how quickly do they grow?" This resulted in several conjectures by Gauss [4]. Gauss conjectured that the class number went to ∞ as the discriminant of a field went to $-\infty$, and this was originally proven by Heilbronn in 1934 with him showing that there are only a finite number of discriminants with a given class number [3]. Gauss also conjectured that there are infinitely many real quadratic fields with class number 1, which is still an open problem.

Modern work on this problem relies on the connection between the class number and the Dedekind ζ-function [3]. Dedekind proved that his generalization of the ζ-function has a meromorphic extension to the complex plane with a simple pole as $s = 1$, and the residue at $s = 1$ depends on the class number of the field. This relationship between the residue at $s = 1$ and the class number of the field is known as the class number formula. Recent attempts at tackling Gauss's second conjecture have relied on this connection by attempting to find asymptotic minimum bounds for this residue [3].

As mentioned before, Dedekind extended the notion of class number to extensions of higher order and extended the ζ-function to these fields as well. The connection between the ζ-function and the class number exists as well in higher dimensions and this is crucial to the work done in the relatively new branch of class field theory [4]. In this paper, we only deal with the quadratic case but encourage the motivated reader to read Sivek [9] for a proof of the general class number formula. The ideas used in the proof are an extension of the ones as used in our proof of the class number formula in two degrees.

4 Concepts Needed

We assume the reader has basic knowledge rings, ideals, and prime ideals. First, we quickly review relevant concepts the reader should also be knowledgeable about.

4.1 The Kronecker Symbol

Refer to Chapter 1.1 of Trifković [11] for proofs.

Definition 4.1. Let $p \in \mathbb{N}$ be an odd prime number and $a \in \mathbb{Z}$, then we define the **Legendre symbol** as:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a non zero square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}.$$

Proposition 4.2. *Let $a, b \in \mathbb{Z}$ and $p \in \mathbb{N}$ be an odd prime number. Then these are some properties of the Legendre symbol:*

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

$$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases},$$

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

Definition 4.3. A generalization of the Legendre symbol to get rid of the constraint of p being an odd prime is the **Kronecker symbol**. Let $a \in \mathbb{Z}$ and $0 \neq n \in \mathbb{Z}$. Then let $n = up_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of n where $u = \pm 1$, the p_i are distinct prime numbers, and $e_i \in \mathbb{N}$ for all $i \in [1, k]$. Then define the **Kronecker symbol** as:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

where $\left(\frac{a}{p_i}\right)$ is equal to the Legendre symbol if p_i is odd and define:

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

Proposition 4.4. *The Kronecker symbol is multiplicative in both variables. Namely if $a, b, m, n \in \mathbb{Z}$ and $mn \neq 0$, then*

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \quad \text{and} \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

4.2 Lattices

Please refer to Chapter 4 of Cohn [1] for proofs.

Definition 4.5. A **lattice** $\Lambda \subset \mathbb{R}^n$ is an additive subgroup of the form $\Lambda = \sum_{i=1}^{n} \mathbb{Z}v_i$, generated by n linearly independent vectors $v_1, \ldots, v_n$. Any such generating set $\{v_1, \ldots, v_n\}$ is called a **basis** of Λ.

Proposition 4.6. *For any lattice $\Lambda \subset \mathbb{R}^n$, we have* $\inf\{|x| : x \in \Lambda \backslash \{0\}\} > 0$.

Definition 4.7. The **discriminant** of a lattice Λ is the volume of the parallelotope defined by a basis set $\{v_1, \ldots, v_n\}$.

Proposition 4.8. *The discriminant of a lattice Λ is independent of the basis set.*

5 Review about Quadratic Extensions

5.1 Ring of Integers

Refer to Chapter 4 of Trifković [11] for proofs.

Proposition 5.1. *All quadratic extensions $K/\mathbb{Q}$ are of the form $K = \mathbb{Q}[\sqrt{D}]$ where $D \in \mathbb{Z}$ is chosen to be square free. Then $D \neq 0, 1$ and D is unique. We call K an **imaginary quadratic field** if $D < 0$ and a **real quadratic field** if $D > 0$.*

Definition 5.2. An element $x \in K$ of an extension $K/\mathbb{Q}$ is said to be **integral** if and only if it is a root of a monic polynomial with integer coefficients. This means there exist $n \in \mathbb{N}, a_i \in \mathbb{Z}$ such that

$$x^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0.$$

Definition 5.3. The **ring of integers** in an extension $K/\mathbb{Q}$ is the set of all elements in K which are integral.

Proposition 5.4. *The ring of integers in $K = \mathbb{Q}[\sqrt{D}]$ is $\mathbb{Z}[\delta]$ where*

$$\delta = \begin{cases} \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \\ \dfrac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \end{cases}.$$

5.2 Norm in Quadratic Fields

Refer to chapter 4 of Trifković [11] for proofs.

Definition 5.5. For any $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$, with $a, b \in \mathbb{Q}$, the **conjugate** of α is the element $\bar{\alpha} := a - b\sqrt{D}$.

Definition 5.6. The **norm** of an element $\alpha \in \mathbb{Q}[\sqrt{D}]$ is $N(\alpha) := \alpha\bar{\alpha} \in \mathbb{Q}$.

Proposition 5.7. *The norm is a multiplicative function.*

Definition 5.8. The **discriminant** of a field $K = \mathbb{Q}[\sqrt{D}]$ is defined to be $D_K := (\delta - \bar{\delta})^2$.

Proposition 5.9. *The discriminant of the field $\mathbb{Q}[\sqrt{D}]$ is*

$$D_K = \begin{cases} 4D & \text{if } D \not\equiv 1 \pmod 4 \\ D & \text{if } D \equiv 1 \pmod 4 \end{cases}.$$

Remark 5.10. The field $\mathbb{Q}[\sqrt{D}]$ is the same as $\mathbb{Q}[\sqrt{D_K}]$. From now on, any mention of D will denote the discriminant, D_K, and the ring of integers in this quadratic field will be denoted $\mathcal{O}_D$. Also if $2 \nmid D$, then D is square free. If $2 \mid D$, then $4 \mid D$ and $D/4$ is square free and $D/4 \equiv 2$ or $3 \pmod 4$.

5.3 The Group of Units

Refer to Chapter 6 of Cohn [1] for proofs.

Theorem 5.11. *If $D < 0$, then the group of units in $\mathcal{O}_D$, denoted by $\mathcal{O}_D^\times$, is finite and*

$$|\mathcal{O}_D^\times| = \begin{cases} 4 & \text{if } D = -4 \\ 6 & \text{if } D = -3 \\ 2 & \text{otherwise} \end{cases}.$$

Theorem-Definition 5.12. *If $D > 0$, there exists an $\eta \in \mathcal{O}_D$ with $|\eta| \neq 1$ such that all units are of the form $\pm\eta^n$ where $n \in \mathbb{Z}$. For standardization, we choose η out of the set $\{\pm\eta, \pm\eta^{-1}\}$ such that $\eta > 1$ and call this the* ***fundamental unit****.*

Corollary 5.13. *We call two elements $a, b \in \mathcal{O}_D$* ***associates*** *if there exists a unit $u \in \mathcal{O}_D^\times$ such that $a = bu$. For any $0 \neq a \in \mathcal{O}_D$ with $D > 0$, there exists a unique associate of a such that $b > 0$ and $1 \leq |b/\bar{b}| < \eta^2$. This number is called the* ***primary associate****.*

6 Unique Factorization of Ideals

6.1 Containment Implies Division

Proposition 6.1. *The ring $\mathcal{O}_D$ can be embedded as a two-dimensional lattice into a plane.*

Proof. If $D < 0$, there is a natural embedding into the complex plane by viewing $a+b\sqrt{D}$ as $a+ib\sqrt{|D|}$. This is a lattice generated by 1 and δ. If $D > 0$, then there is a natural embedding into $\mathbb{R}^2$ by sending $a + b\sqrt{D}$ to $(a + b\sqrt{D}, a - b\sqrt{D})$ which again is generated as a lattice by the image of 1 and δ. □

Corollary 6.2. *For each nonzero ideal $\mathfrak{a} \subset \mathcal{O}_D$, there exist $\alpha, \beta \in \mathcal{O}_D$ such that $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$.*

Proof. Ideals are additive subgroups of $\mathcal{O}_D$, and since $\mathcal{O}_D$ is isomorphic to $\mathbb{Z}^2$ through its embedding, each ideal is isomorphic to a subgroup of $\mathbb{Z}^2$. Since $\mathcal{O}_D$ can be embedded as a lattice, every ideal must be a sublattice and hence have rank $0, 1$, or 2. Let $\mathfrak{a} \subset \mathcal{O}_D$ be a nonzero ideal, then there exists a nonzero $\alpha \in \mathfrak{a}$ and $\alpha\delta \in \mathfrak{a}$ as well. But $\alpha, \alpha\delta$ are linearly independent since $\alpha \neq 0$ and hence $\mathfrak{a}$ is a sublattice of rank 2. □

Proposition 6.3. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be an ideal and denote by $\bar{\mathfrak{a}}$ the ideal generated by the conjugates of all elements in $\mathfrak{a}$. Then there exists $\alpha \in \mathcal{O}_D : \mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$.*

Proof. Please refer to Chapter 4.6 of Trifković [11] for proof. □

Proposition 6.4. *Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_D$ be two ideals, then $\mathfrak{a} \supset \mathfrak{b}$ if and only if there exists an ideal $\mathfrak{c} \subset \mathcal{O}_D$ such that $\mathfrak{ac} = \mathfrak{b}$.*

Proof. For the reverse direction $\mathfrak{c} \subset \mathcal{O}_D$ and thus $\mathfrak{b} = \mathfrak{ac} \subset \mathfrak{a}\mathcal{O}_D = \mathfrak{a}$.

For the forward direction, if $\mathfrak{a} = 0$ then $\mathfrak{b} = 0$ and we can simply choose $\mathfrak{c} = (1)$. So now assume that $\mathfrak{a} \neq 0$. By Proposition 6.3, there exists an $\alpha \in \mathcal{O}_D$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ and hence $(\alpha) \supset \bar{\mathfrak{a}}\mathfrak{b}$. Therefore each element in $\bar{\mathfrak{a}}\mathfrak{b}$ can be written as αx for some $x \in \mathcal{O}_D$. This means that if we define $\mathfrak{c} := \{\beta \in \mathcal{O}_D : \alpha\beta \in \bar{\mathfrak{a}}\mathfrak{b}\}$, then $\alpha\mathfrak{c} = \bar{\mathfrak{a}}\mathfrak{b}$. So multiplying by $\mathfrak{a}$ gives $\alpha\mathfrak{ac} = (\alpha)\mathfrak{b}$ and since $\mathfrak{a} \neq 0$, we know that $\alpha \neq 0$ and hence $\mathfrak{ac} = \{\beta \in \mathcal{O}_D : \alpha\beta \in \alpha\mathfrak{ac}\} = \{\beta \in \mathcal{O}_D : \alpha\beta \in \alpha\mathfrak{b}\} = \mathfrak{b}$. □

6.2 Unique Factorization

Theorem 6.5 (Unique factorization)**.** *Any nonzero ideal $\mathfrak{a} \in \mathcal{O}_D$ has a unique decomposition into prime ideals, that is there exist distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and positive integers $e_1, \ldots, e_k$ such that*

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i},$$

and this decomposition is unique up to reordering.

Proof. The first step is showing there is a unique decomposition into indecomposable ideals by using the previous proposition. Then the second step is to show that all indecomposable ideals are prime ideals. Please refer to Chapter 7.8 in Cohn [1] for the details. □

6.3 Identifying Prime Ideals

Please refer to Chapter 4.9 of Trifković [11] for proofs.

Proposition 6.6. *Every nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_D$ contains a unique prime number $p \in \mathbb{N}$.*

Proposition 6.7. *Let $p \in \mathbb{N}$ be a prime number. The prime factorization of (p) in $\mathcal{O}_D$ is one of the following three forms*

$$\begin{cases} (p) = \mathfrak{p}_1 & \text{in this case } p \text{ is said to be } \textbf{\textit{inert}}. \\ (p) = \mathfrak{p}_1\mathfrak{p}_2 & \text{in this case } p \text{ is said to be } \textbf{\textit{split}}. \\ (p) = \mathfrak{p}_1^2 & \text{in this case } p \text{ is said to be } \textbf{\textit{ramified}}. \end{cases}$$

All nonzero prime ideals in $\mathcal{O}_D$ arise in one of these three ways.

Proposition 6.8. *Let $p \in \mathbb{N}$ be a prime number, then the decomposition of (p) in $\mathcal{O}_D$ depends on $\left(\frac{D}{p}\right)$ by*

$$\left(\frac{D}{p}\right) = \begin{cases} -1 & \text{if } p \text{ is inert in } \mathcal{O}_D \\ 0 & \text{if } p \text{ is ramified in } \mathcal{O}_D \\ 1 & \text{if } p \text{ is split in } \mathcal{O}_D \end{cases}.$$

Corollary 6.9. *Only finitely many prime numbers $p \in \mathbb{N}$ are ramified in $\mathcal{O}_D$.*

7 Ideal Class Group

7.1 Ideal Norm

For proofs of the following two propositions, please refer to Chapter 4.6 in Trifković [11].

Proposition 7.1. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be any nonzero ideal. Then $\mathcal{O}_D/\mathfrak{a}$ is a finite ring.*

Definition 7.2. The **norm** of an ideal $\mathfrak{a}$ is $N(\mathfrak{a}) := |\mathcal{O}_D/\mathfrak{a}|$

Proposition 7.3. *The ideal norm is multiplicative.*

Please refer to Chapter 8.1 in Cohn [1] for proofs.

Proposition 7.4. *For any $0 \neq \alpha \in \mathcal{O}_D$, we have $|N(\alpha)| = N((\alpha))$.*

Corollary 7.5. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be a nonzero ideal. Then $\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))$.*

Proposition 7.6. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be a nonzero ideal. By Corollary 6.2, there exist $\alpha, \beta \in \mathcal{O}_D$ such that $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$. Then $N(\mathfrak{a}) = \left|\dfrac{\alpha\bar{\beta} - \beta\bar{\alpha}}{\sqrt{D}}\right|$.*

Proof. Please refer to Chapter 4.10 in Cohn [1] for the proof. □

7.2 Fractional Ideals

Definition 7.7. A **fractional ideal** of $\mathcal{O}_D$ is a non-empty subset $\mathscr{I} \subset \mathbb{Q}[\sqrt{D}]$ which is closed under addition, multiplication by $\mathcal{O}_D$, and such that there exists an $x \in \mathcal{O}_D$ so that $x\mathscr{I}$ is a nonzero ideal of $\mathcal{O}_D$.

Remark 7.8. The usual ideals of $\mathcal{O}_D$ also satisfy the definition of a fractional ideal (with $x = 1$). They are called integral ideals of $\mathcal{O}_D$.

Proposition 7.9. *The set of nonzero fractional ideals of $\mathcal{O}_D$ forms an abelian group under multiplication.*

Proof. Multiplication is clearly commutative, the unit ideal (1) acts as the identity, and for any fractional ideal $\mathscr{I}$, there exists a nonzero $x \in \mathcal{O}_D$ such that $x\mathscr{I}$ is an ideal and hence by Corollary 7.5

$$\mathscr{I} \cdot \frac{x}{N(x\mathscr{I})}\overline{(x\mathscr{I})} = (1).$$

So every fractional ideal has an inverse. □

Definition 7.10. A fractional ideal of the form $\mathcal{O}_D \cdot x$ for some $x \in K^\times$ is called **principal**.

7.3 Ideal Class Group

Definition 7.11. Let I be the group of all nonzero fractional ideals of $\mathcal{O}_D$. Let P be the set of all nonzero principal fractional ideals of $\mathcal{O}_D$. The subset P can easily be verified to be a subgroup of I. The quotient group I/P is called the **ideal class group** of the field $\mathbb{Q}[\sqrt{D}]$. The ideal class group is a quotient group of an abelian group and hence abelian itself.

7.4 Minkowski Bound

Please refer to Trifković [11] Chapter 5.2 and 5.3 for proofs of the following two statements.

Theorem 7.12 (Minkowski)**.** *Let $\Lambda \subset \mathbb{R}^2$ be a lattice and $S \subset \mathbb{R}^2$ be a subset that is centrally symmetric around 0, convex, and measurable. Then if the area of S is greater than 4 times the discriminant of Λ, there exists a nonzero point in $S \cap \Lambda$.*

Proposition 7.13. *Each ideal class contains an ideal with norm at most $\mathfrak{M}_K$ with:*

$$\mathfrak{M}_K = \sqrt{|D|} \cdot \begin{cases} \frac{2}{\pi} & \text{if } D < 0 \\ \frac{1}{2} & \text{if } D > 0 \end{cases}$$

7.5 Finiteness of the Ideal Class Group

Lemma 7.14. *For each $B \in \mathbb{N}$, there are only finitely many ideals with norm B.*

Proof. Please refer to Cohn [1] Chapter 7.4 for proof. □

Theorem 7.15. *The ideal class group is finite.*

Proof. As a consequence of the previous lemma, there are only finitely many ideals with norm at most $\mathfrak{M}_K$. By Proposition 7.13, it follows that there are a finite number of ideal classes. □

Definition 7.16. The ideal class number of a field is the order of the ideal class group and is denoted h.

7.6 Examples of Calculating the Ideal Class Group

When trying to manually calculate the ideal class number, we can use the Minkowski bound and unique prime factorization to simplify our search. Since every ideal has a prime factorization, the prime ideals generate the ideal class group. Then by Proposition 7.13, we only need look at prime ideals with norm less than $\mathfrak{M}_K$.

Example 7.17. The field $\mathbb{Q}[\sqrt{-5}]$ has ideal class number 2.

Proof. We know $-5 \equiv 3 \pmod 4$ and hence the discriminant is $4 \cdot (-5) = -20$ and $O_{-20} = \mathbb{Z}[\sqrt{-5}]$. By Proposition 7.13, each ideal class contains an ideal of norm at most $\frac{2}{\pi}\sqrt{20} \approx 2.8$. Then we also know that $\left(\frac{-20}{2}\right) = 0$ and hence (2) is ramified in $\mathcal{O}_{-20}$ and so there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_{-20}$ with norm 2. There are no elements of $\mathcal{O}_{-20}$ with norm 2 since $x^2 + 5y^2 = 2$ has no solutions with $x, y \in \mathbb{Z}$. Therefore $\mathfrak{p}$ is not principal.

Since every ideal class contains an ideal with norm at most 2.8 and prime ideals generate the ideal class group, the ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is generated by $\mathfrak{p}$. Since $\mathfrak{p}$ is not principal but $\mathfrak{p}^2 = (2)$ is principal, $\mathfrak{p}$ has order 2 and hence the ideal class group consists of two ideal classes. Therefore the ideal class number is 2. □

8 The Class Number Formula for Quadratic Extensions

8.1 Ideal Density

Proposition 8.1. *Let $\gamma(t) : [0, 1] \to \mathbb{R}^2$ be a piecewise smooth convex non-intersecting curve in the plane with $\gamma(0) = \gamma(1)$. Let $A(\gamma)$ denote the area of the region encapsulated by γ and let $N(\gamma)$ denote the number of lattice points that lie on or inside γ. Finally for any $0 < t \in \mathbb{R}$, let $t\gamma : [0, 1] \to \mathbb{R}^2$ be the curve which is a dilation of γ by a factor of t. Then $N(t\gamma) = A(\gamma)t^2 + O(t)$ as $t \to \infty$.*

Proof. We will use a result found in Section 4 of Garbett [2], and please refer to it for a proof. It tells us that if R is a bounded convex region, then $N(t\gamma) \leq A(\gamma)t^2 + O(|t\gamma|)$, where $|t\gamma|$ denotes the length of the curve. But this is simply $O(t)$. Hence $N(t\gamma) \leq A(\gamma)t^2 + O(t)$.

To get a lower bound on $N(t\gamma)$, let A_t denote the closed region with boundary $t\gamma$, let P_t denote the convex hull of the set of lattice points which lie in A_t, and let R_t be the region consisting of all points in the interior of A_t which lie at least a distance of $\sqrt{2}$ away from boundary. We claim R_t lies complete within P_t. For any point in R_t, it must lie in a unit square and since its distance to any of the corners in the unit square is less than $\sqrt{2}$, all four corners must lie inside A_t and hence all four corners must lie within P_t and so the point is in P_t as well.

Now using Pick's Theorem for convex polygons found in Section 4 of Garbett [2], we know $N(t\gamma) \geq A(P_t) \geq A(R_t)$. But since γ is a convex curve, we know that the area of the difference between region R_t and A_t must be less than $\sqrt{2}|t\gamma|$. So $A(R_t) \geq A(A_t) - \sqrt{2}|t\gamma| = A(\gamma)t^2 + O(t)$. Combining this with the previous result, we have $N(t\gamma) = A(\gamma)t^2 + O(t)$. □

8.1.1 Ideal Density in Imaginary Quadratic Fields

Proposition 8.2. *Let $D < 0$. For all $T \in \mathbb{N}$, let $F(T)$ be the number of ideals in $\mathcal{O}_D$ with $0 < N(\mathfrak{a}) \leq T$. Then*

$$\lim_{T\to\infty} \frac{F(T)}{T} = \frac{2\pi h}{w\sqrt{|D|}},$$

where h is the size of the ideal class group and $w = |\mathcal{O}_D^\times|$.

Proof. For any ideal class $\mathbf{A}$ and $T \in \mathbb{N}$, define $F(\mathbf{A}, T)$ to be the number of ideals in the ideal class $\mathbf{A}$ with $0 < N(\mathfrak{a}) \leq T$. Also, for any ideal $\mathfrak{a} \subset \mathcal{O}_D$, let $G(\mathfrak{a}, T)$ denote the number of elements $\alpha \in \mathfrak{a}$ with $0 < N(\alpha) \leq T$. Now take any $\mathfrak{a} \in \mathbf{A}^{-1}$. We claim that $F(\mathbf{A}, T) = \frac{1}{w}G(\mathfrak{a}, TN(\mathfrak{a}))$. To see this, if $\mathfrak{b} \in \mathbf{A}$ with $N(\mathfrak{b}) \leq T$, then since $\mathfrak{a} \in \mathbf{A}^{-1}$, their product must be a principal ideal and hence there exists an $0 \neq \alpha \in \mathcal{O}_D$ such that $\mathfrak{ab} = (\alpha)$. Taking norms, $N((\alpha)) = N(\alpha) = N(\mathfrak{a})N(\mathfrak{b}) \leq TN(\mathfrak{a})$.

On the other hand, if $\alpha \in \mathfrak{a}$ and $0 < N(\alpha) \leq TN(\mathfrak{a})$, then by Proposition 6.4, there exists an ideal $\mathfrak{b} \subset \mathcal{O}_D$ such that $\mathfrak{ab} = (\alpha)$. But since (α) is a principal ideal, we know that $\mathfrak{b} \in \mathbf{A}^{-1}$ and $N(\mathfrak{a})N(\mathfrak{b}) = N(\alpha) \leq TN(\mathfrak{a})$ so $N(\mathfrak{b}) \leq T$. Hence there is a one to one correspondence between ideals which are counted in $F(\mathbf{A}, T)$ and principal ideals which are counted in $G(\mathfrak{a}, TN(\mathfrak{a}))$. But now if $(\alpha) = (\beta) \neq (0)$, then $N(\alpha) = N(\beta)$ and so α, β must be associates. So for each $(\alpha) \subset \mathfrak{a}$, there are a total of w different elements $\beta \in \mathfrak{a} : (\beta) = (\alpha)$ and hence $F(\mathbf{A}, T) = \frac{1}{w} G(\mathfrak{a}, TN(\mathfrak{a}))$, proving the claim.

By Proposition 6.2, we know that there exist $a, b \in \mathfrak{a}$ with $\mathfrak{a} = a\mathbb{Z} + b\mathbb{Z}$ and so each $\alpha \in \mathfrak{a}$ can be written as $ax + by$ with $x, y \in \mathbb{Z}$. Then $N(\alpha) = (ax + by) \cdot (\bar{a}x + \bar{b}y) = a\bar{a}x^2 + (a\bar{b} + b\bar{a})xy + b\bar{b}y^2 \geq 0$. Hence $G(\mathfrak{a}, TN(\mathfrak{a}))$ has a geometric interpretation: It is the number of lattice points (x, y) which satisfy the inequality for an ellipse:

$$a\bar{a}x^2 + (a\bar{b} + b\bar{a})xy + b\bar{b}y^2 \leq TN(\mathfrak{a}).$$

But by Proposition 8.1, we know that as $T \to \infty$, the number of lattice points contained in the ellipse is equal to the area with error of magnitude $O(\sqrt{TN(\mathfrak{a})}) = O(\sqrt{T})$. The area of the ellipse is

$$\frac{2\pi TN(\mathfrak{a})}{(4a\bar{a}b\bar{b} - (a\bar{b} + b\bar{a})^2)^{1/2}} = \frac{2\pi TN(\mathfrak{a})}{(-(a\bar{b} - b\bar{a})^2)^{1/2}} \overset{7.6}{=} \frac{2\pi TN(\mathfrak{a})}{\sqrt{|D|N(\mathfrak{a})^2}} = \frac{2\pi T}{\sqrt{|D|}}.$$

Therefore

$$\lim_{T\to\infty} \frac{F(\mathbf{A}, T)}{T} = \lim_{T\to\infty} \frac{G(\mathfrak{a}, T\mathfrak{a})}{wT} \overset{8.1}{=} \lim_{T\to\infty} \frac{\frac{2\pi T}{\sqrt{|D|}} + O(\sqrt{T})}{wT} = \frac{2\pi}{w\sqrt{|D|}}.$$

Since this holds for any ideal class $\mathbf{A}$, we have

$$\lim_{T\to\infty} \frac{F(T)}{T} = \lim_{T\to\infty} \frac{\sum_{\mathbf{A}} F(\mathbf{A}, T)}{T} = \frac{2\pi h}{w\sqrt{|D|}}.$$

□

8.1.2 Ideal Density in Real Quadratic Fields

Proposition 8.3. *Let $D > 0$. Then for all $T \in \mathbb{N}$ denoting $F(T)$ to be the number of ideals in $\mathcal{O}_D$ with $0 < N(\mathfrak{a}) \leq T$, we have*

$$\lim_{T\to\infty} \frac{F(T)}{T} = \frac{2h \ln \eta}{\sqrt{D}},$$

where η is the fundamental unit.

Proof. As in the previous proof, for each ideal class $\mathbf{A}$ and number $T \in \mathbb{N}$, define $F(\mathbf{A}, T)$ as the number of ideals in the ideal class $\mathbf{A}$ with $0 < N(\mathfrak{a}) \leq T$. For an ideal $\mathfrak{a} \subset \mathcal{O}_D$ and $T \in \mathbb{N}$, we cannot use the same definition of $G(\mathfrak{a}, T)$ as before since the norm of an integer is not necessarily non negative and there are an infinite number of units and hence every integer has an infinite number of associates. Using Corollary 5.13, we instead define $G(\mathfrak{a}, T)$ as the number of primary associates, α, contained in $\mathfrak{a}$ with $|N(\alpha)| \leq T$. Since every nonzero element of $\mathcal{O}_D$ has a unique primary associate, the argument used in the proof of the previous proposition gives us $F(\mathbf{A}, T) = G(\mathfrak{a}, TN(\mathfrak{a}))$.

By Corollary 6.2, there exist $a, b \in \mathfrak{a}$ such that $\mathfrak{a} = a\mathbb{Z} + b\mathbb{Z}$. For each $\alpha \in \mathfrak{a}$, there exist $x, y \in \mathbb{Z}$ such that $\alpha = ax + by$. The geometric interpretation of $G(\mathfrak{a}, TN(\mathfrak{a}))$ is then the number of lattice points $(x, y) \in \mathbb{Z}^2$ with $0 < |N(ax + by)| \leq TN(\mathfrak{a})$. Since α must be a primary associate, in addition

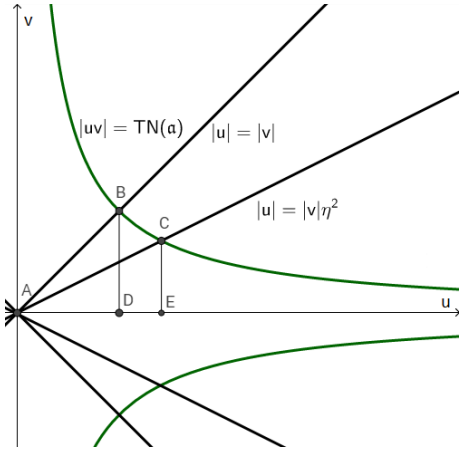

Figure 1

$1 \leq \left|\dfrac{ax+by}{\bar{a}x+\bar{b}y}\right| < \eta^2$ and $ax+by>0$. For any $x, y \in \mathbb{R}$, let R denote the region defined by the following five inequalities:

$$\begin{gathered} 0 < |N(ax+by)| \leq TN(\mathfrak{a}) \\ 1 \leq \left|\frac{ax+by}{\bar{a}x+\bar{b}y}\right| < \eta^2 \\ ax+by>0 \end{gathered} \quad . \tag{1}$$

By Proposition 8.1, the number of lattice points in R is equal to the area of R with error of magnitude $O(\sqrt{T})$. We are able to use Proposition 8.1 because we claim the region R is the difference of two convex bounded regions, both of which satisfy the conditions of the proposition. Admit the claim for now. Then letting $A(R)$ denote the area of region R, we know $G(\mathfrak{a}, TN(\mathfrak{a})) = A(R) + O(\sqrt{T})$.

To simplify the calculation of the area, we can perform a change of variables with $u = ax+by$ and $v = \bar{a}x+\bar{b}y$. In (u,v)-coordinates the region R is now defined by the following inequalities:

$$\begin{gathered} 0 < |uv| \leq TN(\mathfrak{a}) \\ 1 \leq \left|\frac{u}{v}\right| < \eta^2 \\ u>0 \end{gathered} \quad . \tag{2}$$

The region R in (u,v)-coordinates is depicted by sector ABC and its reflection across the u-axis in Figure 1. First we briefly pause to justify our claim that we can use Proposition 8.1. Sector ABC is the difference between triangle ABC and the convex region BC. Since our transformation from (x,y)-coordinates to (u,v)-coordinates was a linear transformation, convex regions are preserved under this mapping and hence the preimage of sector ABC in (x,y)-coordinates satisfies the result of the proposition. The same argument applies to the reflection of sector ABC across the u-axis. Since region R is the disjoint union of these two regions, our claim is proven.

Now, we return to calculating the area of region R in (u,v)-coordinates. Due to symmetry, the area of this region is twice the area of sector ABC. To calculate this area, we first take the integral of $|uv| = TN(\mathfrak{a})$ from $u = D$ to $u = E$ to get the area of region $BCED$, add the area of $\triangle ABD$, then subtract the area of $\triangle ACE$. This area is

$$2\left[\underbrace{\int_{\sqrt{TN(\mathfrak{a})}}^{\eta\sqrt{TN(\mathfrak{a})}} \frac{TN(\mathfrak{a})}{u}du}_{BCED} + \underbrace{\frac{TN(\mathfrak{a})}{2}}_{\triangle ABD} - \underbrace{\frac{TN(\mathfrak{a})}{2}}_{\triangle ACE}\right] = 2TN(\mathfrak{a})\ln u\Big|_{\sqrt{TN(\mathfrak{a})}}^{\eta\sqrt{TN(\mathfrak{a})}} = 2TN(\mathfrak{a})\ln\eta.$$

The area of R in (x, y)-coordinates is equal to the area of R in (u, v)-coordinates multiplied by the absolute value of the Jacobian. The absolute value of the Jacobian is

$$\left|\begin{matrix}\frac{\partial x}{\partial u} & \frac{\partial x}{\partial v}\\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v}\end{matrix}\right| = \left|\begin{matrix}\frac{\bar{b}}{a\bar{b}-\bar{a}b} & \frac{-b}{a\bar{b}-b\bar{a}}\\ \frac{-\bar{a}}{a\bar{b}-\bar{a}b} & \frac{a}{a\bar{b}-b\bar{a}}\end{matrix}\right| = \left|\frac{a\bar{b}-b\bar{a}}{(a\bar{b}-b\bar{a})^2}\right| = \frac{1}{N(\mathfrak{a})\sqrt{D}}.$$

Hence the area of region R in (x, y)-coordinates is $\dfrac{2TN(\mathfrak{a})\ln\eta}{N(\mathfrak{a})\sqrt{D}} = \dfrac{2T\ln\eta}{\sqrt{D}}$. Therefore

$$\lim_{T\to\infty}\frac{F(\mathbf{A},T)}{T} = \lim_{T\to\infty}\frac{G(\mathfrak{a},TN(\mathfrak{a}))}{T} \overset{8.1}{=} \lim_{T\to\infty}\frac{\frac{2T\ln\eta}{\sqrt{D}}+O(\sqrt{T})}{T} = \frac{2\ln\eta}{\sqrt{D}}.$$

Since this holds for every ideal class $\mathbf{A}$, we conclude

$$\lim_{T\to\infty}\frac{F(T)}{T} = \lim_{T\to\infty}\frac{\sum_{\mathbf{A}}F(\mathbf{A},T)}{T} = \frac{2h\ln\eta}{\sqrt{D}}.$$

□

Definition 8.4. The **Dirichlet structure constant** is

$$\kappa := \begin{cases}\dfrac{2\pi}{w\sqrt{|D|}} & \text{if } D<0\\ \dfrac{2\ln\eta}{\sqrt{d}} & \text{if } D>0\end{cases}.$$

Then in both cases, the ideal density of the field is

$$\lim_{T\to\infty}\frac{F(T)}{T} = h\kappa.$$

8.2 The Zeta Function and L-Series

Definition 8.5. The **Riemann ζ-function** is defined for all $s > 1$ by the series

$$\zeta(s) := \sum_{n=1}^{\infty}\frac{1}{n^s}$$

Theorem 8.6 (Euler Product)**.** *The above series converges absolutely for all $s > 1$, and $\zeta(s)$ can be written as an infinite product*

$$\zeta(s) = \prod_{p\in\mathbb{N}}\left(1-\frac{1}{p^s}\right)^{-1},$$

where the product is taken over all prime numbers $p \in \mathbb{N}$.

Proof. Refer to Chapter 8 of Stein [10] for a proof. □

Theorem 8.7. *The ζ-function has a meromorphic extension to the whole complex plane with a simple pole at $z = 1$ and no other poles. The residue of the ζ-function at 1 is 1. Namely:*

$$\lim_{s\to 1^+}(s-1)\zeta(s) = 1$$

Proof. Refer to Rubin [7] for a proof. □

Definition 8.8. The **Dedekind ζ-function** for $\mathbb{Q}[\sqrt{D}]$ is defined for all $s > 1$ by the series:

$$\zeta(s; D) := \sum \frac{1}{N(\mathfrak{a})^s},$$

where the sum is taken over all nonzero ideals $\mathfrak{a} \subset \mathcal{O}_D$.

Definition 8.9. The **Dedekind L-series** for $\mathbb{Q}[\sqrt{D}]$ is defined for all $s > 1$ by the series:

$$L(s; D) := \sum_{n=1}^{\infty} \frac{\left(\frac{D}{n}\right)}{n^s}.$$

Proposition 8.10. *The Dedekind ζ-function converges absolutely for $s > 1$ and $\zeta(s; D) = \zeta(s)L(s; D)$ for all $s > 1$.*

Proof. We start with the L-series. We know that for all $n \in \mathbb{N}$, the Kronecker symbol is $-1, 0$, or 1 and so $\left|\left(\frac{D}{n}\right)\right| \leq 1$. Hence $L(s; D)$ converges absolutely for all $s > 1$. Next note that since the Kronecker symbol is multiplicative, for $s > 1$ we can rewrite the L-series in Euler product form so that

$$L(s; D) = \prod_{p \in \mathbb{N}} \left(1 - \frac{\left(\frac{D}{p}\right)}{p^s}\right)^{-1} = \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{D}{q}\right)=-1} \left(1 + \frac{1}{q^s}\right)^{-1} \prod_{\left(\frac{D}{r}\right)=0} 1,$$

where p, q, r are all prime numbers.

Then we can perform the same splitting of the Euler product for the Riemann ζ-function to get

$$\begin{aligned}\zeta(s)L(s; D) &= \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\left(\frac{D}{q}\right)=-1} \left(1 + \frac{1}{q^s}\right)^{-1} \left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\left(\frac{D}{r}\right)=0} \left(1 - \frac{1}{r^s}\right)^{-1} \\ &= \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\left(\frac{D}{q}\right)=-1} \left(1 - \frac{1}{q^{2s}}\right)^{-1} \prod_{\left(\frac{D}{r}\right)=0} \left(1 - \frac{1}{r^s}\right)^{-1}.\end{aligned}$$

But by Proposition 6.7, if $\left(\frac{D}{p}\right) = 1$, then p is split and there exist distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_D$ such that $\mathfrak{p}_1\mathfrak{p}_2 = (p)$. Taking the norm gives $N(\mathfrak{p}_1\mathfrak{p}_2) = N(\mathfrak{p}_1)N(\mathfrak{p}_2) = N((p)) = p\bar{p} = p^2$. But both ideals are prime and hence $N(\mathfrak{p}_i) \neq 1$ for $i = 1, 2$. Therefore $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.

If $\left(\frac{D}{q}\right) = -1$, then q is inert and $\mathfrak{q} = (q)$ is a prime ideal so $N(\mathfrak{q}) = N((q)) = q\bar{q} = q^2$.

Finally if $\left(\frac{D}{r}\right) = 0$, then r is ramified and there exists a prime ideal $\mathfrak{r} \subset \mathcal{O}_D$ such that $\mathfrak{r}^2 = (r)$. Therefore $N(\mathfrak{r}) = r$. Using these facts, we can rewrite the Euler product in term of ideal norms so

$$\zeta(s)L(s; D) = \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{1}{N(\mathfrak{p}_1)^s}\right)^{-1} \left(1 - \frac{1}{N(\mathfrak{p}_2)^s}\right)^{-1} \prod_{\left(\frac{D}{q}\right)=-1} \left(1 - \frac{1}{N(\mathfrak{q})^s}\right)^{-1} \prod_{\left(\frac{D}{r}\right)=0} \left(1 - \frac{1}{N(\mathfrak{r})^s}\right)^{-1}.$$

But since every prime ideal in $\mathcal{O}_D$ must arise in one of the three cases in Proposition 6.7, every prime ideal in $\mathcal{O}_D$ appears exactly once in the above product. Therefore we can simplify to

$$\zeta(s)L(s; D) = \prod_{\mathfrak{p} \subset \mathcal{O}_D} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

But we claim that this is $\zeta(s; D)$. Every ideal $\mathfrak{a} \subset \mathcal{O}_D$ has an unique prime ideal factorization and we know that $\zeta(s)L(s; D)$ converges absolutely for all $s > 1$, and hence by the same argument as Theorem 8.6, for all $s > 1$, we have

$$\zeta(s)L(s; D) = \prod_{\mathfrak{p} \subset \mathcal{O}_D} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{\mathfrak{a} \subset \mathcal{O}_D} \frac{1}{N(\mathfrak{a})^s} = \zeta(s; D).$$

□

8.3 The Class Number Formula

Lemma 8.11. *For $n \in \mathbb{N}$ and $s > 1$, we have*

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

Proof. We have

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = \int_n^{n+1} \frac{s}{x^{s+1}} dx \leq \int_n^{n+1} \frac{s}{n^{s+1}} dx = \frac{s}{n^{s+1}},$$

because $\frac{1}{x^{s+1}} \leq \frac{1}{n^{s+1}}$ for all $x \geq n$. Then

$$\frac{s}{n^{s+1}} - \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right] = \int_n^{n+1} \left(\frac{s}{n^{s+1}} - \frac{s}{x^{s+1}}\right) dx \leq s \int_n^{n+1} \left(\frac{1}{n^{s+1}} - \frac{1}{(n+1)^{s+1}}\right) dx \leq \frac{s(s+1)}{n^{s+2}},$$

by applying the first result to $\frac{1}{n^{s+1}} - \frac{1}{(n+1)^{s+1}}$. □

Theorem 8.12 (Class Number Formula)**.** *The Dedekind ζ-function has a meromorphic extension to $\mathbb{C}$ with a simple pole at $s = 1$ and no other poles. Moreover,*

$$\lim_{s \to 1^+} (s-1)\zeta(s; D) = L(1; D) = h\kappa,$$

where h, κ are defined as above.

Proof. Please refer to Overholt[6] for a proof of the meromorphic continuation of the Dedekind ζ-function.

By the Proposition 8.10, we know that $\zeta(s; D)$ converges absolutely for all $s > 1$, and hence we can rearrange the terms. We know that the $N(\mathfrak{a}) \in \mathbb{N}$ and hence

$$\zeta(s; D) = \sum_{\mathfrak{a} \subset \mathcal{O}_D} \frac{1}{N(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \sum_{N(\mathfrak{a})=n} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{F(n) - F(n-1)}{n^s},$$

where $F(T)$ is the number of ideals $\mathfrak{a} \subset \mathcal{O}_D$ such that $0 < N(\mathfrak{a}) \leq T$. Then $F(0) = 0$ and rearranging some more gives

$$\sum_{n=1}^{\infty} \frac{F(n) - F(n-1)}{n^s} = \sum_{n=1}^{\infty} F(n) \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right] \overset{8.11}{=} \epsilon(s) + \sum_{n=1}^{\infty} F(n) \frac{s}{n^{s+1}} = \epsilon(s) + s \sum_{n=1}^{\infty} \frac{F(n)}{n} \frac{1}{n^s},$$

where

$$|\epsilon(s)| \overset{8.11}{\leq} s(s+1) \sum_{n=1}^{\infty} \frac{1}{n} \frac{F(n)}{n} \frac{1}{n^s}.$$

Then from the proof of Propositions 8.2 and 8.3, we know that $\frac{F(n)}{n} = h\kappa + O(1/\sqrt{n})$. Therefore

$$|\epsilon(s)| \leq s(s+1) \sum_{n=1}^{\infty} \frac{h\kappa + O(1/\sqrt{n})}{n^{s+1}},$$

and the right term is bounded as $s \to 1$. Hence as $s \to 1^+$, we have

$$\lim_{s \to 1^+} (s-1)\epsilon(s) = 0.$$

Similarly, the expression $s \sum_{n=1}^{\infty} \frac{O(1/\sqrt{n})}{n^s}$ remains bounded as $s \to 1^+$ and hence

$$\lim_{s \to 1^+} (s-1)\zeta(s; D) = \lim_{s \to 1^+} (s-1)\epsilon(s) + s(s-1) \sum_{n=1}^{\infty} \frac{h\kappa + O(1/\sqrt{n})}{n^s} = 0 + \lim_{s \to 1^+} h\kappa(s-1) \sum_{n=1}^{\infty} \frac{1}{n^s} \overset{8.7}{=} h\kappa.$$

□

8.4 Value of the Kronecker Symbol

Theorem 8.13. *Let p_i denote the ith prime number. Then the series*

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

diverges.

Proof. See Stein[10] Chapter 8 for a proof. □

Lemma 8.14. *For any $\epsilon \in \mathbb{R}$ with $|\epsilon| \leq \frac{1}{2}$, we have $\ln(1+\epsilon) = \epsilon + E(\epsilon)$ where $|E(\epsilon)| \leq \epsilon^2$.*

Proof. See Stein[10] Chapter 8 Lemma 1.8 for a proof. □

Proposition 8.15. *The series*

$$\sum_{i=1}^{\infty} \frac{\left(\frac{D}{p_i}\right)}{p_i}$$

converges.

Proof. For $s > 1$, we can rewrite the L-series in Euler product form so that:

$$L(s;D) = \prod_{i=1}^{\infty} \left(1 - \frac{\left(\frac{D}{p_i}\right)}{p_i^s}\right)^{-1}.$$

We can take the logarithm of both sides so that

$$\ln L(s;D) = -\sum_{i=1}^{\infty} \ln\left(1 - \frac{\left(\frac{D}{p_i}\right)}{p_i}\right),$$

and since $p_i \geq 2$ for all $i \in \mathbb{N}$, Lemma 8.14 gives us

$$\ln L(s;D) = -\sum_{i=1}^{\infty} \left[-\frac{\left(\frac{D}{p_i}\right)}{p_i^s} + E\left(\frac{\left(\frac{D}{p_i}\right)}{p_i^s}\right)\right].$$

Since

$$0 \leq \left|\sum_{i=1}^{\infty} E\left(\frac{\left(\frac{D}{p_i}\right)}{p_i^s}\right)\right| \leq \sum_{i=1}^{\infty} \left|E\left(\frac{\left(\frac{D}{p_i}\right)}{p_i^s}\right)\right| \leq \sum_{i=1}^{\infty} \frac{\left(\frac{D}{p_i}\right)^2}{p_i^{2s}} \leq \sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6},$$

the left most sum converges to some number $C \in \mathbb{R}$. Thus

$$\ln L(s;D) = O(1) + \sum_{i=1}^{\infty} \frac{\left(\frac{D}{p_i}\right)}{p_i^s}.$$

But as $s \to 1^+$, Theorem 8.12 tells us that $L(s;D) \to h\kappa > 0$. Therefore the logarithm of the L-series must remain bounded as s tends towards 1 and hence

$$\sum_{i=1}^{\infty} \frac{\left(\frac{D}{p_i}\right)}{p_i}$$

remains bounded and so the series converges. □

Corollary 8.16. *There are infinitely many prime numbers, such that* $\left(\frac{D}{p}\right) = 1$*, and there are infinitely many prime numbers such that* $\left(\frac{D}{p}\right) = -1$*.*

Proof. Assume for the sake of contradiction that there were only finitely many prime numbers such that $\left(\frac{D}{p}\right) = 1$. By Corollary 6.9, there are only finitely many prime numbers such that $\left(\frac{D}{p}\right) = 0$. Since the series

$$\sum_{i=1}^{\infty} \frac{\left(\frac{D}{p_i}\right)}{p_i}$$

converges, adding a finite number of terms gives us that the series

$$\sum_{i=1}^{\infty} \frac{-1}{p_i}$$

converges, which is a contradiction to Theorem 8.13. Therefore there are infinitely many prime numbers such that $\left(\frac{D}{p}\right) = 1$.

The proof that there are infinitely many prime numbers with $\left(\frac{D}{p}\right) = -1$ follows the same line of arguments. □

Definition 8.17. Let P denote the set of all prime numbers and $A \subset P$ be any subset. Then the limit

$$\lim_{s \to 1^+} \frac{\sum_{p \in A} p^{-s}}{\sum_{p \in P} p^{-s}},$$

if it exists, is called the **Dirichlet density** of A.

Theorem 8.18. *Let* $P_1(D)$ *denote the set of prime numbers such that* $\left(\frac{D}{p}\right) = 1$*, let* $P_{-1}(D)$ *denote the set of prime numbers with* $\left(\frac{D}{p}\right) = -1$*. Then the Dirichlet densities of* $P_1(D)$ *and* $P_{-1}(D)$ *are both* $\frac{1}{2}$*.*

Proof. See Serre [8] Chapter 6 for a proof. □

Definition 8.19. Let $A \subset P$ be any subset. For each $n \in \mathbb{N}$, denote $A_n = \{p \in A : p \leq n\}$ and similarly $P_n = \{p \in P : p \leq n\}$. Then the limit

$$\lim_{n \to \infty} \frac{|A_n|}{|P_n|},$$

if it exists, is called the **natural density** of A.

Theorem 8.20. *The natural densities of* $P_1(D)$ *and* $P_{-1}(D)$ *are both* $\frac{1}{2}$*.*

Proof. See Serre [8] Chapter 6 for a proof. □

Theorem 8.21. *Let* $A \subset P$ *be any subset. If the natural density of* A *exists, then the Dirichlet density of* A *exists as well, and is equal to the natural density of* A*.*

Proof. See Jun [5] Section 4 for a proof. □

Remark 8.22. The converse is not necessarily true.

In order to visualize the asymptotic behavior of $\pi(x), \pi_1(x)$, and $\pi_{-1}(x)$, we wrote a program to calculate those values for large values of x. Using $D = -20$ as before, the values are displayed in the table below. The Python script can be found in the appendix.

x	10^5	$5 \cdot 10^5$	10^6	$5 \cdot 10^6$	10^7
$\pi(x)$	9592	41538	78498	348513	664579
$\pi_1(x)$	4773	20743	39140	174170	332142
$\pi_{-1}(x)$	4817	20793	39356	174341	332435

8.5 Uniqueness of the Field

Proposition 8.23. *Let $D, D' \in \mathbb{Z}$ be discriminants of quadratic fields. If $\left(\frac{D}{n}\right) = \left(\frac{D'}{n}\right)$ for all $n \in \mathbb{N}$, then $D = D'$.*

Proof. First we note that for all prime numbers $p \in \mathbb{N}$, we have

$$p \mid D \iff \left(\frac{D}{p}\right) = 0 \iff \left(\frac{D'}{p}\right) = 0 \iff p \mid D',$$

so D and D' have the same prime factors. We know that since D and D' are discriminants of quadratic fields, by Remark 5.10, if p is an odd prime number, then $p^2 \nmid D$. Combining this with the fact that D and D' have the same prime factors, for each odd prime number p, the same power of p divides both D and D'. Now we claim that the same power of 2 divides both D and D' as well. If $\left(\frac{D}{2}\right) \neq 0$ then no positive powers of 2 divide either D, D'. If $\left(\frac{D}{2}\right) = 0$, then $2 \mid D$ and by Remark 5.10, we have $4 \mid D$ and $D/4, D'/4 \in \mathbb{Z}$ are both square free with residue 2 or 3 (mod 4). Suppose for the sake of contradiction that $D/4 \equiv 2 \pmod 4$ and $D'/4 \equiv 3 \pmod 4$. Then since D and D' have the same odd prime factors and for each odd prime factor, the same power divides both D and D', we must have $D = \pm 2D'$. First suppose that $D = 2D'$. We know 8 is the discriminant of the field $\mathbb{Q}[\sqrt{2}]$ and by Corollary 8.16, there are infinitely many prime numbers such that $\left(\frac{8}{p}\right) = -1$. Only finitely many of these divide D, so choose p such that $p \nmid D$ and $\left(\frac{8}{p}\right) = -1$. Then $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)$ and so

$$\left(\frac{D}{p}\right) = \left(\frac{2D'}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{D'}{p}\right) = -\left(\frac{D}{p}\right).$$

Hence $\left(\frac{D}{p}\right) = 0$ but $p \nmid D$ which is a contradiction. Now suppose that $D = -2D'$. We know -8 is the discriminant of the field $\mathbb{Q}[\sqrt{-2}]$ and by Corollary 8.16, there exist infinitely many prime numbers such that $\left(\frac{-8}{p}\right) = -1$. Choosing one such that $p \nmid D$, we get

$$\left(\frac{D}{p}\right) = \left(\frac{-2D'}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{D'}{p}\right) = -\left(\frac{D}{p}\right).$$

Hence $\left(\frac{D}{p}\right) = 0$ which again is a contradiction. Therefore $D/4 \equiv D'/4 \equiv 2 \pmod 4$ or $D/4 \equiv D'/4 \equiv 3 \pmod 4$.

Therefore for each prime number, the same power divides both D and D' and hence $|D| = |D'|$. So we need to show that D and D' have the same sign. Suppose for the sake of contradiction that $D = -D'$. We know -4 is the discriminant of $\mathbb{Q}[\sqrt{-1}]$. So by Corollary 8.16, there exist infinitely many prime numbers such that $\left(\frac{-4}{p}\right) = -1$. Choose one which does not divide D. Then $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right)$ and

$$\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right) = \left(\frac{-D}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{D}{p}\right) = -\left(\frac{D}{p}\right).$$

But $\left(\frac{D}{p}\right) \neq 0$ which is a contradiction. Therefore $D = D'$. □

Proposition 8.24. *Let $(a_n)_{n\in\mathbb{N}}$ be a bounded sequence in $\mathbb{R}$. If there exists an $c \in \mathbb{R}$ such that:*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = 0$$

for all $s > c$, then $a_n = 0$ for all $n \in \mathbb{N}$.

Proof. Suppose for the sake of contradiction that there exists an $n \in \mathbb{N}$ such that $a_n \neq 0$. Then let N denote the smallest such index. Then

$$\left|\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right| = \left|\sum_{n=N}^{\infty} \frac{a_n}{n^s}\right| \geq \frac{|a_N|}{N^s} - \sum_{n=N+1}^{\infty} \frac{M}{n^s}.$$

But $\frac{1}{n^s} \leq \int_{n-1}^{n} \frac{1}{x^s} dx$ for any $n > 1$ and $s > 1$ and hence

$$\left|\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right| \geq \frac{|a_N|}{N^s} - M \sum_{n=N+1}^{\infty} \int_{n-1}^{n} \frac{1}{n^s} ds = \frac{|a_N|}{N^s} - M \int_{N}^{\infty} \frac{1}{x^s} dx = \frac{|a_N|}{N^s} - \frac{M}{(s-1)N^{s-1}}.$$

for all $s > \max(1, c)$ and hence let $s_0 = \dfrac{MNt}{|a_N|} + 1$ where $t \in \mathbb{N}$ is chosen such that $t > 1$ and $s_0 > \max(1, c)$. Then since $s_0 > 1$, we have that

$$\left|\sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}}\right| \geq \frac{|a_N|}{N^{s_0}} - \frac{M}{(s_0-1)N^{s_0-1}} = \frac{|a_N|}{N^{s_0}} - \frac{|a_N|M}{MNtN^{s_0-1}} = \frac{|a_N|}{N^{s_0}} \left[1 - \frac{1}{t}\right] > 0.$$

But since $s_0 > c$, by assumption $|\sum_{n=1}^{\infty} a_n n^{-s_0}| = 0$ and hence this is a contradiction. Therefore $a_n = 0$ for all $n \in \mathbb{N}$. □

Corollary 8.25 (Uniqueness of the Field)**.** *If $D, D' \in \mathbb{Z}$ are determinants of quadratic fields, and $L(s; D) = L(s; D')$ for all $s > 1$, then $D = D'$.*

Proof. Let $a_n = \left(\frac{D}{n}\right) - \left(\frac{D'}{n}\right)$ which is bounded in magnitude by 2. Then we know that $\sum_{n=1}^{\infty} a_n n^{-s} = L(s; D) - L(s; D') = 0$ for all $s > 1$. By the previous proposition, we know $a_n = 0$ for all $n \in \mathbb{N}$ and hence $\left(\frac{D}{n}\right) = \left(\frac{D'}{n}\right)$ for all $n \in \mathbb{N}$. Therefore by Proposition 8.23, we have $D = D'$. □

Corollary 8.26. *If $\zeta(s; D) = \zeta(s; D')$ for all $s > 1$, then $D = D'$.*

Proof. We know that $\zeta(s; D) = \zeta(s)L(s; D)$ and $\zeta(s) \neq 0$ for all $s > 1$. Hence we can divide by $\zeta(s)$ to get $L(s; D) = L(s; D')$ for all $s > 1$ and the previous Corollary tells us $D = D'$. □

9 Appendix

```
import math

def leg(a, p):
        return mod(a, (p - 1)/2, p)

def prime(p):
        if x == 2 or x == 3 or x == 5 or x == 7:
                return True
```

```
        if x % 2 == 0 or x % 3 == 0 or x % 5 == 0 or x % 7 == 0:
                return False
        for i in range(2, int(math.sqrt(x)/6) + 2):
                if x % (6 * i - 1) == 0 or x % (6 * i + 1) == 0:
                        return False
        return True

def run(x):
        numP = 0
        numP1 = 0
        numP0 = 0
        for i in range(2, x):
                if prime(i):
                        numP = numP + 1
                        if leg(-20, i) == 1:
                                numP1 = numP1 + 1
                        elif 20 % p == 0:
                                numP0 = numP0 + 1
        print numP, numP1, numP - numP1 - numP0
```

References

[1] Cohn, H. *Advanced Number Theory.* General Publishing Company, Ltd., 1962.

[2] Garbett, J. Lattice point geometry: Pick's theorem and minkowski's theorem.

[3] Goldfeld, D. Gauss class number problem for imaginary quadratic fields.

[4] Goldman, J. R. *The Queen of Mathematics.* A K Peters, Ltd., 1998.

[5] Jun, H. K. The density of primes of the form $a + km$.

[6] Overholt, M. *A Course in Analytic Number Theory.* American Mathematical Society, 2014.

[7] Rubin, F. Riemann's first proof of the analytic continuation of $\zeta(s)$ and $L(s, \chi)$.

[8] Serre, J.-P. *A Course in Arithmetic.* Springer-Verlag New York Inc., 1973.

[9] Sivek, G. The analytic class number formula.

[10] Stein, E. M. *Fourier Analysis.* Princeton University Press, 2003.

[11] Trifković, M. *Algebraic Theory of Quadratic Numbers.* Springer-Verlag New York, 2013.