GROWTH RATE OF CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

WILLIAM ZHANG

ABSTRACT: This paper presents a review of the results on the growth rate of class number of imaginary quadratic fields. We first develop the theory of binary quadratic forms and algebraic number fields, and explore how the class number is represented in each of these contexts. We then review Dirichlet's class number formula. This background in turn allows us to outline the historical development of the works on the lower bound for the class number of imaginary quadratic fields, from Gauss' class number one problem to Siegel's theorem and then the Goldfeld-Gross-Zagier theorem, the first general result with an effective constant.

1. Introduction

In 1772 Euler [Eul72] discovered that

$$x^2 - x + 41 \text{ is a prime for all integers } x \in \{1, 2, \cdots, 40\}.$$

Similarly, Legendre observed in 1798 that

$$x^2 + x + 41 \text{ is a prime for all } x \in \{0, 1, 2, \cdots, 39\}.$$

A century later, in 1912, Rabinovitch [Rab13] would present the following general result for quadratics of this form:

Theorem 1.1. *(Rabinovitch) $D < 0, D \equiv 1 (mod\ 4)$,*

$$x^2 - x + \frac{1 + |D|}{4} \text{ is a prime for all } x \in \{1, 2, \cdots, \frac{|D| - 3}{4}\},$$

if and only if every integer of the field $Q(\sqrt{D})$ has unique factorization into product of primes.

Ayoub and Chowla [AC81] showed that a similar theorem holds for $x^2 + x + \frac{1+|D|}{4}$. It is known that $Q(\sqrt{-163})$ has the unique factorization property, which accounts for the polynomial property above. In fact, this makes -163 one of the nine Heegner numbers that have the same property. These Heegner number quadratics, which evaluate to prime numbers for many consecutive integer values of x, are some of the earliest examples related to what is now known as Gauss' class number one problem.

Finding all of the Heegner numbers is a special case of Gauss' class number problem, which Gauss first described in his book *Disquisitiones Arithmeticae* [Gau01]. Written in 1798, *Disquisitiones* is one of the most influential texts in the history of algebraic number theory. The book consolidates the work of Gauss' predecessors, such as Euler, Lagrange, and Legendre, and presents interesting questions that still attract attention from mathematicians over two centuries later. This paper seeks to give an overview of the class number problem for imaginary quadratic fields with particular focus on its lower bound. However, to rigorously discuss this issue, we must first define some terms.

Date: July 17, 2023.

The rest of the paper is organized as follows. Section 2 discusses the theory of binary quadratic forms, as described in Cox [Cox22]. The notion of equivalence between forms allows us to define the class number. The main result of this section is that the class number is finite and positive. This section also states Gauss' class number problem and one of its special cases, the Gauss class number one problem. Section 3 introduces the concepts necessary to present the class number problem in an algebraic number theoretical approach. Section 4 presents Dirichlet's class number formula with a rough sketch of analytical proof [LD39] and its generalization. Section 5 covers Siegel's theorem [Sie35] with a short proof by Goldfeld [Gol74] plus description of the initial solutions to the Gauss class number problem. Section 6 reviews the Goldfeld-Gross-Zagier theorem [Gol85], which, in contrast to Siegel's, provides an effective constant that can be utilized to limit the number of candidates for consideration when classifying imaginary quadratic fields with a given class number. Section 7 gives a brief on the up-to-date classification results of imaginary quadratic fields with class number ≤ 100, most notably the work by Watkins [Wat04]. Section 8 summarizes the main results and points out potential future work on the growth rate of the class number of imaginary quadratic fields, with a theoretical upper bound under the Generalized Riemann Hypothesis.

2. Binary Quadratic Forms

2.1. **Definition, Equivalence, and Definiteness.** In *Disquisitiones Arithmeticae*, Gauss also deals with generalized binary quadratic forms, which have the the form

$$ax^2 + bxy + cy^2 \text{ for } a, b, c \in Z.$$

The discriminant of the form is $d = b^2 - 4ac$, analagous to the standard single variable quadratic. We will focus mainly on forms with negative discriminants, so we assume both $a, c \neq 0$. In particular, we are interested in fundamental discriminants, where $d \equiv 1(mod\ 4)$ is square-free or $d = 4n$ where $n \equiv 2, 3(mod\ 4)$ is square-free. For the remainder of this section, we let $f(x, y)$ denote the form $ax^2 + bxy + cy^2$. The study of binary quadratic forms began with Lagrange, as treated in his 1773- 1775 work *Recherchesd'Arithmetique* [DL73], in the context of determining when an integer m can be represented by some form $f(x, y)$ for some integer x and y. The theory from *Recherches* was further developed by Gauss to whom most of the terminology is due, although many of the concepts were inspired by Lagrange. For further discussion of the origin of the study of binary quadratic forms and the more general theory, see the work by Cox [Cox22] or Ribenboim [Rib06].

A form $f(x, y)$ is called primitive when $gcd(a, b, c) = 1$. Since any form is an integer multiple of a primitive form, it is sufficient to concern ourselves exclusively with primitive forms. We also restrict our attention to positive-definite forms, which are those for which $f(x, y) \geq 0$ for all (x, y). Similarly, a form is negative-definite if $f(x, y) \leq 0$ for all (x, y) and indefinite if neither positive- nor negative-definite.

Two forms $f(x, y)$ and $g(x', y')$ are called equivalent if there is a matrix in

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \middle| p, q, r, s \in \mathbb{Z} \text{ such that } ps - qr = 1 \right\}$$

such that

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

It is clear that the equivalence of forms is an equivalence relation: the group action of $SL_2(\mathbb{Z})$ on the set of forms as given above partitions the set into classes according to equivalence. Following Gauss, we say that two equivalent forms are in the same class, denoted by $f(x,y) \sim g(x,y)$.

It is clear that the form $f(x,y)$ can be written in matrix form as

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

We denote the matrix by F:

$$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Clearly, the discriminant

$$d = -4 \cdot \det(F), \tag{1}$$

where $\det(F)$ is the determinant of F. It is well known that $f(x,y)$ is positive or negative definite if and only if F is positive or negative definite, respectively.

If $g(x',y') = Ax'^2 + Bx'y' + Cy'^2$ has matrix G and is equivalent to $f(x,y)$ via

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}),$$

then

$$f(x,y) = g(x',y') = \begin{pmatrix} x' & y' \end{pmatrix} G \begin{pmatrix} x' \\ y' \end{pmatrix} = \left(M \begin{pmatrix} x \\ y \end{pmatrix} \right)^T G \left(M \begin{pmatrix} x \\ y \end{pmatrix} \right) = \begin{pmatrix} x & y \end{pmatrix} (M^T G M) \begin{pmatrix} x \\ y \end{pmatrix},$$

which implies

$$F = M^T G M,$$

from which in turn we get

$$\det(F) = \det(M^T) \cdot \det(G) \cdot \det(M) = 1 \cdot \det(G) \cdot 1 = \det(G).$$

Therefore, we have the following

Proposition 2.1. *Any two equivalent forms $f(x,y) \sim g(x,y)$ have the same discriminant.*

We can see that the converse of this proposition is not necessarily true. For example, consider $d = -20$ and the forms $g(x',y') = x'^2 + 5y'^2$ and $f(x,y) = 2x^2 + 2xy + 3y^2$. We claim these forms are not equivalent. Using methods from the proof of Proposition 2.1 above, with $(a,b,c) = (2,2,3)$ and $(A,B,C) = (1,0,5)$, suppose we have a matrix M as given above. But then a little algebra gives

$$\begin{aligned} 2 = a &= Ap^2 + Bpr + Cr^2 = p^2 + 5r^2, \\ 2 = b &= 2(Apq + Crs) + B(ps + qr) = 2(pq + 5rs), \\ 3 = c &= Aq^2 + Bqs + Cs^2 = q^2 + 5s^2, \end{aligned}$$

and this is impossible for $p,q,r,s \in Z$ as the first equation necessitates $r = 0$, but then p would not be an integer.

To examine the special case of Gauss' class number problem that we are interested in, *i.e.*, that of imaginary quadratic fields, we restrict our attention to positive-definite forms with negative discriminant, so $d < 0$. The sign of the discriminant strongly restricts the behavior of the form.

Proposition 2.2. *Let $f(x, y)$ be a form with discriminant $b^2 - 4ac < 0$. Then $f(x, y)$ is either positive- or negative-definite, as determined by the sign of a.*

This follows directly from 1 and $d < 0$ as F is a 2×2 matrix, and so the only main diagonal sub-matrices are the first element (a) and the entire matrix.

From this point on, we take a to be positive (and so $c > 0$ as well), which provides an especially nice notion of a reduced form. A form $f(x, y)$ is reduced if $|b| \leq a \leq c$ and $b \geq 0$ if either $a = |b|$ or $a = c$. It follows that every primitive, positive-definite form is equivalent to a canonical unique reduced form [Cox22]. As a complement to the more classically-styled proof of Cox in [Cox22], Goldfeld [Gol85] gives a discussion of this result. In particular, for a form $f(x, y)$ with discriminant d, we get an associated complex number $\omega = \frac{-b+\sqrt{d}}{2a}$. A form is thus reduced precisely when ω is in the fundamental domain of the modular group $SL_2(Z)$.

2.2. **Class Number.**

Definition 2.1. The class number, denoted $h(d)$, is the number of nonequivalent forms $f(x, y)$ with discriminant $d = b^2 - 4ac$.

Determining $h(d)$ for a given d can be a challenge in and of itself, although the task is made much easier via computer programs. Note that $-d = 4ac - b^2 \geq 3a^2$, and so we can bound the coefficients by $|b| \leq a \leq \sqrt{\frac{-d}{3}}$. This implies that there are only finitely many reduced forms for a given discriminant since a and b are bounded by $|d|$ and c is uniquely determined by a, b, d, and thus the number of equivalence classes is also finite.

Furthermore, since $d \equiv b^2 \equiv 0$ or $1 \pmod 4$, the following provides at least one binary quadratic form of discriminant d for any valid d, called the *principal form*:

$$\begin{cases} x^2 - \frac{1}{4}dy^2 & \text{if } d \equiv 0 \pmod 4 \\ x^2 + xy - \frac{1}{4}(d-1)y^2 & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{2}$$

Hence $h(d)$ is a positive integer, and together we get the following theorem.

Theorem 2.1. *[Cox22] For fixed d, the number $h(d)$ of primitive, positive-definite forms of discriminant d is finite and positive. Further, $h(d)$ is equal to the number of reduced forms of discriminant d.*

Remarkably, Gauss conjectured the same fact in *Disquisitiones*. Without knowing what a group is, Gauss proves that the classes of forms with a given discriminant form a finite group under composition as the group operation [Cox22]. This group is known as the form class group and denoted $C(d)$, and the order of $C(d)$ is clearly the class number $h(d)$.

2.3. **Gauss Class Number Problem.**

In the *Disquisitiones Arithmeticae* (1801) [Gau01], Gauss conjectured

1. $h(d) = 1$ for $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ and no others for $d < -163$, known as **Gauss' class number one problem**.
2. $\lim_{d \to -\infty} h(d) = \infty$
3. There are infinitely many real quadratic fields with class number one.

This set off a race of more than 200 years of finding an effective algorithm to determine all imaginary quadratic fields with a given class number h, known as the **Gauss class number problem**. The Gauss class number problem is especially intriguing, because if such an effective algorithm did not exist, then the associated Dirichlet L–function would have to have a real zero, and the Generalized Riemann Hypothesis would necessarily be false.

To highlight the difficulty of the problem, the third part of the Gauss class number problem concerns the real quadratic fields, which are not covered in this paper, and is still an open question today!

2.4. **Automorphs on Binary Quadratic Forms.** For describing Dirichlet's class number formula in Section 4, we also need to look at the automorphs on the forms of a given d, namely, $SL_2(\mathbb{Z})$ transformations that keep a form unchanged - not just equivalent. There are always two trivial automorphs, namely, the identity $x = x', y = y'$ and the negative identity $x = -x', y = -y'$. If $d < 0$, there are in general no others, except for when $d = -3$ or -4. In both these cases there is only one class of forms, represented by the principal form 2.1. If $d = -3$, the principal form is $x^2 + xy + y^2$, and this has the additional automorphs $x = -y', y = x' + y'$, and $x = x' + y', y = -x'$ and their negatives. If $d = -4$, the principal form is $x^2 + y^2$, and this has the additional automorph $x = y', y = -x'$ and its negative. We denote by w the number of automorphs, so that

$$w(d) = \begin{cases} 2 & \text{if } d < -4 \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3 \end{cases} \tag{3}$$

(Another interpretation for w is that it is the number of roots of unity in the quadratic field of discriminant d.)

3. Connection to Algebraic Number Theory

In this section, we introduce the fundamental algebraic number field concepts necessary for establishing the class number in that regard.

3.1. **Basics.**

Definition 3.1. Let E be a field, and $F \subseteq E$ be a subfield of E. That is, F is a subset of E and is a field with respect to E's operations.

Then, the dimension of F considered as a vector space over E is called the degree of extension of F over E and is denoted by $[F : E]$. The degree of extension can be finite or infinite: $[\mathbb{C} : \mathbb{R}] = 2$, but $[\mathbb{R} : \mathbb{Q}] = \infty$

Definition 3.2. An algebraic element α of a field K satisfies that α is a root of some polynomial in $\mathbb{Q}[x]$.

Definition 3.3. An Algebraic Extension K of $\mathbb{Q}$ satisfies that $\forall\ \alpha \in K$, α is an algebraic element of $\mathbb{Q}$. K may be a finite or infinite extension.

Definition 3.4. Let $\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n$ be complex numbers. The smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and all of $\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n$ is denoted by $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n)$, which is said to be obtained by adjoining $\mathbb{Q}$ with $\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n$. Such a field always exists and it is the intersection of all subfields of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha_1, \alpha_2, \alpha_3 \ldots \alpha_n$.

Definition 3.5. A cyclotomic field is a number field obtained by adjoining a complex root of unity to $\mathbb{Q}$.

Definition 3.6. An algebraic integer is any complex number that is a root of a monic polynomial, meaning a polynomial with leading coefficient 1, with coefficients in $\mathbb{Z}$.

Definition 3.7. The ring of algebraic integers $\mathcal{O}_K$ in an algebraic field K is the set of all algebraic integers in K. This set is guaranteed to be a ring.

Definition 3.8. A quadratic field is an algebraic number field of degree two over $\mathbb{Q}$. Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$, where d is a square free integer other than 0 and 1. If $d > 0$, $\mathbb{Q}(\sqrt{d})$ is a real quadratic field, and if $d < 0$ it is an imaginary quadratic field or complex quadratic field.

3.2. **Ideals.** Note: since the only rings necessary to consider are commutative, we will assume every ring considered in the following sections to be commutative.

Definition 3.9. Let $(R, +, \cdot)$ be a commutative ring. $I \subseteq R$ is called an ideal of R if $(I, +)$ is a subgroup of $(R, +)$ and $\forall r \in R$ and $x \in I$, $rx \in I$.

Notation: $I \triangleleft R$ means that I is an ideal of R. Ideals $I \neq R$ are called proper ideals.

Multiplication of Ideals

Let I and J be two ideals of a ring R. Then, the product IJ is the smallest ideal containing all the products of elements of I with elements of J.

Notation : Let $a_1, a_2, \ldots a_n$ be elements of a commutative ring R. The smallest ideal that contains these elements is denoted by $(a_1, a_2 \ldots a_n)$.

Example. If $I = (a_1, b_1), J = (a_2, b_2)$ are two ideals, then $IJ = (a_1a_2, a_1b_2, a_2b_1, b_1b_2)$.

For a numerical example, consider $I = (2, 1 + \sqrt{-17})$ in $\mathbb{Z}[\sqrt{-17}]$. From the above formula, $I^2 = (4, 2(1+\sqrt{-17}), 2(1+\sqrt{-17}), (1+\sqrt{-17})^2) = (4, 2(1+\sqrt{-17}), (1+\sqrt{-17})^2) = (4, 2(1+\sqrt{-17}), (-16+2\sqrt{-17}))$. The three generators $4, 2(1+\sqrt{-17}), (-16+2\sqrt{-17})$ of I^2 are all multiples of 2, so

$$I^2 \subseteq (2).$$

Note also that

$$2 = 4 \cdot 5 - 2(1+\sqrt{-17}) + (-16+2\sqrt{-17}),$$
$$2\sqrt{-17} = 4 \cdot -5 + 2 \cdot 2(1+\sqrt{-17}) - (-16+2\sqrt{-17})$$

So, $2, 2\sqrt{-17} \in I^2$ since they can be written as a linear combination of generators of I^2 with coefficients from $\mathbb{Z}[\sqrt{-17}]$. Thus, we can also conclude

$$(2) \subseteq I^2.$$

So, $I^2 = (2)$.

Definition 3.10. A prime ideal P of an integral domain D is a proper ideal that satisfies $\forall a, b \in D$, $ab \in P \implies a \in P$ or $b \in P$.

Definition 3.11. The maximal ideal I of a ring R satisfies that for all ideals J of R, $I \subseteq J \subseteq R \implies I = J or J = R$.

Proposition 3.1. *If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z}$. So, $\mathfrak{p}$ contains a unique prime p.*

This is because $\mathfrak{p} \cap \mathbb{Q}$ is a prime ideal in $\mathbb{Z}$.

Proposition 3.2. *Every prime ideal $\mathcal{O}_K$ is a maximal ideal of $\mathcal{O}_K$.*

Proposition 3.3. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ then for ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}_K$ such that $p \subset \mathfrak{ab}$,*

$$\mathfrak{p} \supset \mathfrak{a} \text{ or } \mathfrak{p} \supset \mathfrak{b}.$$

Theorem 3.1. *Let K be an algebraic number field. Then, every proper ideal $\mathbb{O}_k$ is uniquely expressible as a product of prime ideals up to order.*

Definition 3.12. Let D be an integral domain, and K be the quotient field of D. Any nonempty subset A of K that satisfies the following three properties is called a fractional ideal of D.

(1) A is closed under addition.
(2) $\alpha \in A, r \in D \implies r\alpha \in A$
(3) There exists a nonzero $\gamma \in D$ such that $\gamma A \subseteq D$

A fractional ideal A of D can be expressed as $A = \frac{1}{\gamma} I$ for some $\gamma \neq 0, \gamma \in D$ and I is an ordinary ideal of D.

Theorem 3.2. *The set of fractional ideals of an algebraic number field K form an Abelian group under multiplication.*

Definition 3.13. The norm I of a nonzero proper ideal is defined as

$$N(I) = |\mathcal{O}_K / I| = [\mathcal{O}_K : I]$$

The norm when I is the zero ideal is defined to be zero.

Proposition 3.4. *If J is an ideal in $\mathcal{O}_K$, then $N(J) = |\mathcal{O}_K / J|$ is finite.*

Proposition 3.5. *For an ideal J, if the norm $N(J)$ is a prime number, J is a prime ideal.*

Definition 3.14. Let K be an algebraic number field.

An embedding of K into $\mathbb{C}$ is a homomorphism from K to $\mathbb{C}$. K is generated by a single algebraic element, say θ. Let $\deg \theta = n$, meaning θ has n algebraic conjugates $\theta_1, \theta_2, \ldots \theta_n$ including θ itself.

Every embedding $\sigma : K \to \mathbb{C}$ is an isomorphism from K onto $\sigma(K)$. This embedding is completely determined just by the value of $\sigma(\theta)$, so there are n possible embeddings.

Definition 3.15. Let K be an algebraic number field and $\sigma_1, \sigma_2, \ldots \sigma_n$ be all of the n embeddings of K into $\mathbb{C}$. If $\alpha \in K$, $N_{K/\mathbb{Q}}\alpha$ is defined by

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Corollary 3.2.1. *In the caze of a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, there are exactly two embeddings σ_1 and σ_2 of K into $\mathbb{C}$, given by $\sigma_1(\sqrt{d}) = \sqrt{d}$ and $\sigma_2(\sqrt{d}) = -\sqrt{d}$.*

If $\alpha = a + b\sqrt{d}$, then

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = \alpha\overline{\alpha},$$

where $\sigma_2(\alpha) = \overline{\alpha}$.

So, $N(a + b\sqrt{d}) = a^2 - db^2$.

For example, $N(3) = 3^2 = 9$, while $N(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2 = 1$.

Definition 3.16. A principal ideal is an ideal I in ring R generated by a single element a of R. Like before, we represent this by $I = (a)$.

Since (a) is generated by a single element, $I = \{ra : r \in R\}$.

Proposition 3.6. *Principal fractional ideals form a group under multiplication, and this group is a subgroup of the group of fractional ideals.*

3.3. **Domain.**

Definition 3.17. An integral domain is a nonzero commutative ring where the product of any two nonzero elements is nonzero. In other words, there are no zero divisors.

Definition 3.18. An element u of an integral domain D is said to be a unit if there exists some element u^{-1} usch that $uu^{-1} = 1$

Definition 3.19. An irreducible element of an integral domain is anonzero element that is not invertible and is not the product of two non invertible elements.

Definition 3.20. An element p is said to be a prime element of an integral domain D if $p \neq 0$, p is not a unit, and if $p|ab$, then either $p|a$ or $p|b$ for $a, b \in D$.

Unique Factorization Domain

Definition 3.21. Two elements a and b in an integral domain D are called associated if $b = au$, where $u \in D$ is a unit. Then, $a = bu^{-1}$.

Example. In $\mathbb{Z}$, for every integer $n \in \mathbb{Z}$, n and $-n$ are associated elements.

Definition 3.22. An integral domain D is called a Unique Factorization Domain, or UFD, if every nonzero, nonunit element $a \in D$ can be expressed uniquely as a product of irreducible elements up to ordering.

For example, $\mathbb{Z}$ is a unique factorization domain, and this fact is known as the fundamental theorem of algebra.

Definition 3.23. A principal ideal domain, or PID, is an integral domain in which every ideal is principal (generated by a single element).

Proposition 3.7. *Suppose that a principal ideal domain R is not a field. Then an ideal $I = (p)$ is maximal if and only if p is an irreducible element.*

Proposition 3.8. *In every PID, the ascending chain of ideals*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \dots$$

stabilizes, meaning $(a_n) = (a_m)$ for all $n \geq m$ starting at some m. This is called the ascending chain condition on principal ideals.

Corollary 3.2.2. *Let R be a PID ring. Then every nonzero nonunit element a is divisible by an irreducible element.*

Corollary 3.2.3. *An element in a PID is prime iff it is irreducible.*

Corollary 3.2.4. *Every nonzero, nonunit element in a PID is a product of irreducible elements.*

Theorem 3.3. *Every PID is a UFD.*

***Note**: The converse of this theorem is not true.*

3.4. **Integral Basis.**

Definition 3.24. A set of algebraic integers $\alpha_1, \alpha_2, \ldots \alpha_s \in K$ is an integral basis of $\mathcal{O}_K$ if every algebraic integer $\gamma \in K$ can be written uniquely as $\gamma = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_s\alpha_s$, where $b_1, b_2, \ldots b_s \in \mathbb{Z}$.

An integral basis of $\mathcal{O}_K$ is an integral basis of K.

Definition 3.25. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements of K. Their discriminant is defined by

$$\begin{vmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}^2$$

This discriminant is nonzero iff $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$.

Theorem 3.4. *Every number field has an integral basis.*

Theorem 3.5. *Let K be a quadratic field $\mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \pmod 4$, then an integral basis of K is $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$, and otherwise it is $\{1, \sqrt{d}\}$.*

Definition 3.26. An Abelian group G is called a free Abelian group with rank n if there exist n elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in G such that $G = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \ldots + \mathbb{Z}\alpha_n$ and every element p of G can be expressed with a unique linear combination of the form $p = m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n$, with $m_i \in \mathbb{Z}$ for all $i = 1, 2, \ldots, n$.

Theorem 3.6. *Let $[K : \mathbb{Q}] = n$ and J be a nonzero ideal of $\mathbb{O}_K$. Then J has an integral basis of n elements.*

Lemma 3.7. *Let J be a nonzero ideal of $\mathbb{O}_K$. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_n$ is an integral basis of $\mathbb{O}_K$. Then for every $i, 1 \leq i \leq n$, there is a positive integer m_i such that $m_i\alpha_i \in J$.*

Lemma 3.8. *Let J be a nonzero ideal of $\mathbb{O}_K$. Then, J has an integral basis with n elements of the form*

$$\beta_1 = m_1\alpha_1 + c_{1,2}\alpha_2 + \ldots + c_{1,n}\alpha_n$$

$$\beta_2 = m_2\alpha_2 + c_{2,3}\alpha_3 + \ldots + c_{2,n}\alpha_n,$$

$$\ldots$$

$$\beta_n = m_n\alpha_n,$$

where all $c_{i,j}$ are integers and $m_1, m_2, \ldots, m_n$ are positive integers.

Lemma 3.9. *We have $|\mathcal{O}_K| = m_1m_2 \ldots m_n$, where $m_1, m_2, \ldots m_n$ are the same as those in the previous lemma.*

Theorem 3.10. *Let $J \neq 0$ be an ideal of $\mathcal{O}_K$. Then, $N(J) = |\mathcal{O}_K/J| = \sqrt{\frac{\delta(\beta_1\beta_2 \ldots \beta_n)}{\delta(\alpha_1\alpha_2 \ldots \alpha_n)}}$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an integral basis of $\mathbb{O}_K$, and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is an integral basis of J.*

3.5. **Examples of Calculation of Integral Basis of Ideals and Their norms.**

Proposition 3.9. *If α is a generator of an ideal J, then $N_{\frac{\mathbb{Q}(\alpha)}{\mathbb{Q}}}(\alpha)$ is in J.*

Corollary 3.10.1. *If $J = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, then $d = \gcd\left(N_{\frac{\mathbb{Q}(\alpha_1)}{\mathbb{Q}}}, N_{\frac{\mathbb{Q}(\alpha_2)}{\mathbb{Q}}}, \ldots, N_{\frac{\mathbb{Q}(\alpha_k)}{\mathbb{Q}}}\right) \in J$.*

So, if $d = 1$, then $J = \mathcal{O}_K and N(J) = 1$. The integral basis of J in this case is just the integral basis of $\mathcal{O}_K$.

Definition 3.27. If a is an element of the ring of integers $\mathcal{O}_F$ of an algebraic number field F, a is called a unit if there exists a nonzero element $b \in \mathcal{O}_F$ such that $ab = 1$. $\mathcal{O}_F$ may have an infinite number of units.

Theorem 3.11. *Let K be an algebraic number field of degree n. Let r be the number of real embeddings of K into $\mathbb{C}$ and $2s$ the number of complex embeddings of K. Dirichlet's unit theorem states that $\mathbb{O}_K$ contains $r + s - 1$ units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}$ such that each unit of $\mathcal{O}_K$ can be expressed uniquely in the form $\rho\varepsilon_1^{n_1}\varepsilon_2^{n_2}\ldots\varepsilon_{r+s-1}^{n_{r+s-1}}$, where ρ is a root of unity in $\mathcal{O}_K$ and $n_1, n_2, \ldots n_{r+s-1}$ are integers.*

3.6. **Units in Quadratic Number Fields.** To describe all units in quadratic number fields $K = \mathbb{Q}(\sqrt{d})$, we use Dirichlet's Unit Theorem.

When $d > 0$, K is a real quadratic field with $r = 2, s = 0, r + s - 1 = 1$. So, for a primitive root of unity $\zeta \in K$, $\varepsilon = \zeta^n\eta^k = \pm\eta^k$, as $\zeta = -1$ is the only real primitive root of unity in $\mathcal{O}_K$. So, every real quadratic field has infinitely many units, and the unit η is called the fundamental unit of $\mathcal{O}_K$.

3.7. **Fundamental Unit.**

Theorem 3.12. *Let $d > 1$ be a squarefree integer, and $K = \mathbb{Q}(\sqrt{d})$.*

1. *Then, the smallest unit $\eta > 1$ exists in $\mathcal{O}_K$.*
2. *Every unit of $\mathcal{O}_K$ is of the form $u = \pm\eta^n$ with $n \in \mathbb{Z}$.*

Definition 3.28. Let $d > 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Then, the unit $\eta > 1$ described in the preceding theorem is called the fundamental unit of K.

3.8. **Ideal Class Groups.** An ideal class group is the quotient group of the group of fractional ideals of the integers with the subgroup of principal ideals.

Definition 3.29. Let K be an algebraic number field of degree of n. Let $\{\eta_1, \eta_2, \ldots, \eta_n\}$ be an integral basis for K. Then, $D(\eta_1, \eta_2, \ldots, \eta_n)$ is called the discriminant of K and denoted by $d(K)$.

Theorem 3.13. *Let K be a quadratic number field, and d be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{d})$. Then, $d(K) = 4d$ if $d \not\equiv 1 \pmod 4$ and $d(K) = d$ if $d \equiv 1 \pmod 4$.*

Definition 3.30. The ideal class group of the algebraic number field K is the quotient group $\frac{J_K}{P_K}$, where J_K is the group of fractional ideals of the ring of integers K, and P_K is the subgroup of principal ideals in J_K, $\frac{J_K}{P_K}$ is denoted by $H(K)$.

Theorem 3.14. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n = r + 2s$, where θ has r real conjugates and s pairs of nonreal complex conjugates. Let A be an integral or fractional ideal of $\mathcal{O}_K$. Then there exists an element α, α in$A, \alpha \neq 0$, such that*

$$|N(\alpha) \leq \left(\frac{2}{\pi}\right)^s N(A)\sqrt{|d(K)|}.$$

This result's proof also invokes the following lemmas:

Lemma 3.15. *Let $S(\mathbb{R}^n)$ be a centrally symmetric convex body of volume $V(S) \geq 2^n$. Then, S contains a nonzero lattice point.*

Lemma 3.16. *Let $A = [a_{j,k}]_{n\times n}$ be a complex matrix such that $a_{j,k} \in \mathbb{R}$ for $j = 1, 2, \ldots, r$ and $k = 1, 2, \ldots, n$, and*

$$a_{j+sk} = \overline{a}_{j,k} for j = r + 1, r + 2, \ldots r + s; k = 1, 2, \ldots, n.$$

Suppose that positive real numbers $\delta_1, \delta_2, \ldots, \delta_n$ satisfy the following conditions

$$\delta_1\delta_2 \ldots \delta_n \geq \left(\frac{2}{\pi}\right)^s |\det(a_{j,k})|$$

and

$$\delta_j = \delta_{j+s}, j = r + 1, r + 2, \ldots, r + s$$

Then, the system of linear equations

$$\left|\sum_{k=1}^{n} a_{j,k}y_k\right| \leq \delta_j, j = 1, 2, \ldots, n.$$

Theorem 3.17. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n = r + 2s$, where θ has r real conjugates and s pairs of nonreal complex conjugates. Let A be an integral or fractional ideal of $\mathcal{O}_K$. Then there exists an element α, α in$A, \alpha \neq 0$ such that*

$$|N(\alpha) \leq \left(\frac{2}{\pi}\right)^s N(A)\sqrt{|d(K)|}.$$

3.9. **Correspondence between Form Classes and Ideal Classes.** Given a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $d = b^2 - 4ac < 0$, consider the *fractional ideal* $< a, \frac{-b+\sqrt{d}}{2} >$ generated over $\mathcal{O}_K$.

It can be shown that equivalent fractional ideals of the ideal generated from $f(x, y)$ this way correspond to equivalent forms of $f(x, y)$. Thus there is a one-to-one correspondence between the equivalent classes of binary quadratic forms $f(x, y)$ and the ideal classes. Therefore, the ideal class group has order $h(d)$.

When $h(d) = 1$, every fractional ideal in $\mathbb{Q}(\sqrt{d})$ is principal, thus $\mathcal{O}_K$ a principal ideal domain (PID), and the algebraic integers of $\mathbb{Q}(\sqrt{d})$ have unique factorizations. This is why Theorem 1.1 holds for $D = -163$ because $h(-163) = 1$.

4. Dirichlet's Class Number Formula

Dirichlet's class number formula, in its simplest and most striking form, was conjectured by Jacobi in 1832 and proved in full by Dirichlet in 1839. Before we cover Dirichlet's class number formula, we need to introduce some basic concepts: Legendre and Kronecker symbols, Dirichlet character, and Dirichlet L-function.

4.1. **Legendre and Kronecker Symbols.**

Definition 4.1. Legendre Symbol: Let a be an integer and p be a prime. We define Legendre symbol as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \not\equiv 0 \text{ and } a \text{ is a quadratic residue} \pmod{p} \\ -1, & \text{if } a \text{ is not a quadratic residue} \pmod{p} \\ 0, & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

Properties of the Legendre symbol: Suppose p and q are two odd primes, and a and b are integers not divisble by p, the following properties for Legendre symbol hold:

(1) Periodic: if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) Multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
(3) $\left(\frac{a^2}{p}\right) = 1$
(4) $\left(\frac{1}{p}\right) = 1$
(5) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$
(6) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
(7) Quadratic reciprocity law: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Example: $\left(\frac{385}{97}\right) = \left(\frac{5\cdot 7\cdot 11}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{7}{97}\right)\left(\frac{11}{97}\right)$ by multiplicity. Applying quadratic reciprocity and periodicity, $\left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{97-1}{2}}\left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1$ (the last equality is because 2 is $\not\equiv 0$ and not a quadratic residue $\pmod{5}$). Similarly, $\left(\frac{7}{97}\right) = \left(\frac{97}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = 1(-1) = -1$. Likewise, $\left(\frac{11}{97}\right) = 1$. Therefore, $\left(\frac{385}{97}\right) = (-1)(-1)1 = 1$.

Definition 4.2. Kronecker symbol: Let n be a non-zero integer, with prime factorization $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$, where u is a unit (± 1). Let a be an integer. Define the Kronecker symbol $\left(\frac{a}{n}\right)$ recursively as

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

For odd p_i, the number $\left(\frac{a}{p_i}\right)$ is simply the usual Legendre symbol. When $p_i = 2$, we define $\left(\frac{a}{2}\right)$ by

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

For $u = 1$, $\left(\frac{a}{1}\right) = 1$. For $u = -1$, we define as

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

For $n = 0$, it is defined as

$$\left(\frac{a}{0}\right) = \begin{cases} 1, & \text{if } a = \pm 1 \\ 0, & \text{otherwise} \end{cases}$$

Here are some basic properties of the Kronecker symbol:

(1) $\left(\frac{a}{n}\right) = \pm 1$ if $\gcd(a, n) = 1$, otherwise $\left(\frac{a}{n}\right) = 0$.
(2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ unless $n = -1$, one of a, b is zero and the other one is negative.
(3) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ unless $a = -1$, one of m, n is zero and the other one has odd part congruent to 3mod4.
(4) For $n > 0$, we have $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ whenever $a \equiv b \bmod \begin{cases} 4n, & n \equiv 2 \pmod 4, \\ n & \text{otherwise.} \end{cases}$. If additionally a, b have the same sign, the same also holds for $n < 0$.
(5) For $a \not\equiv 3 \pmod 4$, $a \neq 0$, we have $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ whenever $m \equiv n \bmod \begin{cases} 4|a|, & a \equiv 2 \pmod 4, \\ |a| & \text{otherwise.} \end{cases}$

Kronecker symbol generalizes the Jacobi symbol and satisfies its own quadratic reciprocity law.

Example: Applying Property 3 and Legendre symbols, we get $\left(\frac{2}{21}\right) = \left(\frac{2}{3\cdot 7}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = (-1)1 = -1$.

4.2. **Dirichlet Character.** When Euler proved (1748) that there are infinitely many primes, he used the so-called Euler product

$$\sum_{1}^{\infty} \frac{1}{n} = \prod_{p \ prime} \sum_{k=0}^{\infty} \frac{1}{p^k} = \prod_{p \ prime} (1 - \frac{1}{p})^{-1}.$$

The first equality is because each integer n has a unique prime factorization that corresponds to a unique term in the product expansion of the second expression. When Dirichlet proved that there are infinitely many primes in the arithmetic progression

$$a, a + q, a + 2q, \cdots, \text{where } (a, q) = 1,$$

similar product $\prod_{p \equiv a \pmod q} (1 - \frac{1}{p})^{-1}$ could not be directly used as there is no known equality like the harmonic series. Dirichlet remedied the problem with the *Dirichlet character*.

Definition 4.3. Dirichlet Character: A complex-valued arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character of modulus m (where m is a positive integer) if for all integers a and b:

(1) $\chi(ab) = \chi(a)\chi(b)$; that is, χ is completely multiplicative.
(2) $\chi(a) \begin{cases} = 0 & \text{if } \gcd(a, m) > 1 \\ \neq 0 & \text{if } \gcd(a, m) = 1. \end{cases}$
(3) $\chi(a + m) = \chi(a)$; that is, χ is periodic with period m.

The simplest possible character, called the principal character, usually denoted χ_0, exists for all moduli: $\chi_0(a) = \begin{cases} 0 & \text{if } \gcd(a, m) > 1 \\ 1 & \text{if } \gcd(a, m) = 1. \end{cases}$. Real-valued characters are just Kronecker symbols

4.3. **Dirichlet L-function.** With a character χ, Dirichlet defined the L-function:

Definition 4.4.

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p\ prime} \sum_{k=0}^{\infty} \frac{(\chi(p))^k}{(p^s)^k} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} (Re(s) > 1)$$

As with the Euler product, the second equality is because a character is multiplicative and each integer n has a unique prime factorization that corresponds to a unique term in the product expansion of the third expression.

4.4. **Dirichlet Class Number Formula.**

Theorem 4.1. *(Dirichlet's class number formula) [LD39] Let $d < 0$ be a fundamental discriminant and χ be the* $\pmod d$ *Kronecker symbol* $(\chi(m) = \left(\frac{d}{m}\right))$. *Then*

$$h(d) = \frac{w(d)\sqrt{|d|}}{2\pi} L(1,\chi), \tag{4}$$

$$L(1,\chi) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|-1} m \left(\frac{d}{m}\right). \tag{5}$$

Combining the two formulas above gives the following explicit finite sum of Kronecker symbols for $h(d)$ with $d < 0$:

$$h(d) = -\frac{w(d)}{2|d|} \sum_{m=1}^{|d|-1} m \left(\frac{d}{m}\right),$$

known as the Dirichlet class number formula.

Examples

(1) $d = -3, w(d) = 6, h(d) = -\frac{6}{2\cdot 3}\sum_{m=1}^{2} m\left(\frac{-3}{m}\right) = -1(1\left(\frac{-3}{1}\right) + 2\left(\frac{-3}{2}\right)) = -1(1\cdot 1 + 2\cdot(-1)) = -1(-1) = 1$. Therefore, the algebraic integers of $\mathbb{Q}(\sqrt{-3})$ form a PID, and its integers have unique factorizations.

(2) For $\mathbb{Q}(\sqrt{-5})$, the fundamental discriminant $d = -20$ ($-5 \equiv 3 \pmod 4$), and similarly $h(-20) = 2$, so the algebraic integers of $\mathbb{Q}(\sqrt{-5})$ do not form a PID, and its integers may have multiple factorizations. For example, $6 = 2\cdot 3 = (1+\sqrt{5})(1-\sqrt{-5})$.

4.5. **Sketch Proof of the Dirichlet Class Number Formula.** We follow [Dav13] for a sketch proof of Dirichlet's formula. There are two stages in Dirichlet's proof. In the first stage, the class number of quadratic forms of given (fundamental) discriminant d is related to the value of $L(1,\chi)$, where χ is the real primitive character denoted by the Kronecker symbol. This relation immediately implies that $L(1,\chi) > 0$. In the second stage, the value of $L(1,\chi)$ is expressed in terms of a finite sum, which is achievable with quadratic fields.

We first turn to the question of the total number of representations of a positive integer n by a representative set of forms of given (fundamental) discriminant d. This question was answered (implicitly, at least) in the classical theory of quadratic forms, developed by Lagrange and further by Gauss. When $d < 0$, so that the forms are positive definite, the

number of representations of n by any form is finite, which can be seen through elementary completing the square technique:

$$n = ax^2 + bxy + cy^2 = a(x + \frac{b}{2a}y)^2 + \frac{4ac - b^2}{4a}y^2$$

with all coefficients positive, which implies that both y and $x + \frac{b}{2a}y$ are bounded by $\sqrt{n}$, thus there are only finite number of solutions for x, y. We denote by $R(n)$ the total number of representations by the various forms of a representative set. The basic result of the theory of quadratic forms is as follows:

Theorem 4.2. *If $n > 0$ and $(n, d) = 1$, then*

$$R(n) = w(d) \sum_{m|n} \left(\frac{d}{m}\right), \tag{6}$$

where w is given by 3 for $d < 0$.

Expressing $R(n)$ in terms of the number of solutions of the congruence $z^2 \equiv d \pmod{4n}$, and then evaluating this number in terms of quadratic character symbols. The basic idea in the first stage of Dirichlet's work is to determine, from the above expression for $R(n)$, the average value of $R(n)$ as n varies. It is convenient (and it suffices for the purpose in view) to limit oneself to values of n that are relatively prime to d. We have

$$\begin{aligned}\frac{1}{w} \sum_{\substack{n=1 \\ (n,m)=1}} R(n) &= \sum_{\substack{m_1 m_2 \le N \\ (m_1 m_2, d)=1}} \left(\frac{d}{m_1}\right) \\ &= \sum_{m_1 \le \sqrt{N}} \left(\frac{d}{m_1}\right) \sum_{\substack{m_2 \le \frac{N}{m_1} \\ (m_2,d)=1}} 1 + \sum_{\substack{m_2 < \sqrt{N} \\ (m_2,d)=1}} \sum_{\sqrt{N} < m_1 \le \frac{N}{m_2}} \left(\frac{d}{m_1}\right),\end{aligned}$$

since the first sum comprises all pairs m_1, m_2 for which $m_1 \le \sqrt{N}$ and the second sum all pairs for which $m_1 > \sqrt{N}$. The first inner sum is

$$\frac{N}{m_1}\frac{\phi(|d|)}{|d|} + O[\phi(|d|)].$$

so the first double sum is

$$N\frac{\phi(|d|)}{|d|} \sum_{m_1 \le \sqrt{N}} \frac{1}{m_1}\left(\frac{d}{m_1}\right) + O(\sqrt{N}),$$

for fixed d and arbitrarily large N. Since $\left(\frac{d}{m_1}\right)$ is a non-principal character to the modulus $|d|$, the sum of its values as m_1 varies over any range is bounded. Hence the second double sum is $O(\sqrt{N})$. Thus

$$\frac{1}{w} \sum_{\substack{n=1 \\ (n,m)=1}} R(n) = N\frac{\phi(|d|)}{|d|} \sum_{m \le \sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right) + O(\sqrt{N}).$$

We can extend the sum over N to infinity, and the remainder is estimated by

$$\sum_{m>\sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right) = O(\sqrt{N})$$

on using partial summation. This again contributes an error $O(\sqrt{N})$ in the above asymptotic expression. In particular, we conclude that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n) = w\frac{\phi(|d|)}{|d|} \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{d}{m}\right). \tag{7}$$

Since $\frac{\phi(|d|)}{|d|}$ measures the density of the integers n for which $(n,d)=1$, we can express the result in the form: The average with respect to n of $R(n)$ is $wL(1,\chi)$, where $\chi(m) = \left(\frac{d}{m}\right)$. The next step is to evaluate the average of $R(n)$ from its original definition. Let $R(n,f)$ denote the number of representations of n by a particular form f of discriminant d. Then

$$R(n) = \sum_{f} R(n,f), \tag{8}$$

where the summation is over a representative set of forms (with $a>0$), so that the number of terms in the sum is $h(d)$. We shall now evaluate

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n,f),$$

and it will turn out to be independent of f. Comparison of the two limits will give the relation between $h(d)$ and $L(1,\chi)$. In the case of $d<0$. Then

$$\sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n,f)$$

is the number of pairs of integers x, y satisfying

$$0 < ax^2+bxy+cy^2 \le N,\ (ax^2+bxy+cy^2, d) = 1.$$

The second condition limits x, y to certain pairs of residue classes $\pmod{|d|}$, and it is easily proved that the number of these pairs is $|d|\phi(|d|)$. Hence it suffices to consider the number of pairs of integers x, y satisfying

$$ax^2+bxy+cy^2 \le N,\ x \equiv x_0, y \equiv y_0 \pmod{|d|}.$$

The first inequality expresses that the point (x,y) is in an ellipse with center at the origin, and as $N\to\infty$ this ellipse expands uniformly.

The area of the ellipse is

$$\frac{2\pi}{\sqrt{4ac-b^2}}N = \frac{2\pi}{\sqrt{|d|}}N.$$

Intuition suggests-and a rigorous proof is easily given by dividing the plane into squares of side length $|d|$-that the number of points is asymptotic to

$$\frac{1}{|d|^2}\frac{2\pi}{\sqrt{|d|}}N \text{ as } N\to\infty.$$

We have to multiply this by $|d|\phi(|d|)$ to allow for the various possibilities for x_0, y_0. Thus the conclusion is that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n,f) = \frac{1}{|d|^2} \frac{2\pi}{\sqrt{|d|}}.$$

This combined with 7 and 8 gives

$$h(d) = \frac{w\sqrt{|d|}}{2\pi} L(1,\chi) \text{ for } d < 0. \tag{9}$$

This completes the first stage of the work 4, and, as we said earlier, the result 9 render visible the fact that $L(1,\chi) > 0$. There remains the question of expressing $L(1,\chi)$ by means of a finite sum. For that, we need to evaluate a slight extension of Gauss' sum. This takes the form

$$\sum_{m=1}^{|d|} \left(\frac{d}{m}\right) e(\frac{mn}{|d|}) = \left(\frac{d}{n}\right) i\sqrt{|d|} \text{ for } d < 0,$$

which, when combined with 9, gives

$$L(1,\chi) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|} m \left(\frac{d}{m}\right) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|-1} m \left(\frac{d}{m}\right) \text{ for } d < 0. \tag{10}$$

The last equality is due to $\left(\frac{d}{|d|}\right) = 0$ for any d with $|d| > 1$ because $d \equiv 0 \pmod{p}$ for any prime factor p of $|d|$. This completes the proof for the second part 5 of the Dirichlet's class number formula.

4.6. **The General Class Number Formula.** To briefly introduce the general class number formula, we first define the following symbols:

K is an extension field over the rational field Q with $[K : Q] = n = r_1 + 2r_2$, where r_1 denotes the number of real and complex embeddings of K, and $2r_2$ is the number of complex embeddings of K. $\zeta_K(s)$ is the Dedekind zeta function of K. h_K is the ideal class number, the number of elements in the ideal class group of K. Reg_K is the regulator of K. w_K is the number of roots of unity contained in K. D_K is the discriminant of the algebraic extension K/Q. With these defined, we have:

Theorem 4.3. *(Class Number Formula) [NN74] $\zeta_K(s)$ converges absolutely for $Re(s) > 1$ and extends to a meromorphic function defined for all complex s with only one simple pole at $s = 1$, with residue*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}}.$$

The finite limit is called the class number. This is the most general class number formula. In particular cases, for example when K is a cyclotomic extension of Q or an imaginary quadratic field as covered above, there are particular and more refined class number formulas.

5. Siegel's Theorem

In 1934, Heilbronn [Hei34] proved part of the Gauss class number conjecture:

$$\lim_{d\to-\infty} h(d) = \infty.$$

Heilbronn proved this under the assumption of falsity of the Generalized Riemann Hypothesis while Hecke (1918) did it under the opposite assumption, thus proving it unconditionally. Unfortunately, this method of proof was not effective, since if the Generalized Riemann Hypothesis were false, the constant D_M for whenever $d < D_M < 0$, there is $h(d) > M$ for a given $M > 0$ would depend on an unknown zero of $L(s,\chi)$ located off the line $Re(s) = \frac{1}{2}$. This presumably nonexistent zero is now known as Siegel's zero.

In 1935, Siegel proved the following beautiful result about the growth rate of $h(d)$.

Theorem 5.1. *(Siegel) [Sie35] Let $Q(\sqrt{-d})$, $d > 0$ be a quadratic field, and h(d) denote its class number. For every $\epsilon > 0$, we have*

$$h(d) > C_\epsilon d^{\frac{1}{2}-\epsilon}$$

for some constant $C_\epsilon > 0$.

Lemma 5.2. *Let χ be any real primitive Dirichlet character (mod q), then for every $\epsilon > 0$, $L(1,\chi) > \frac{C(\epsilon)}{q^\epsilon}$ where $C(\epsilon)$ is an ineffective constant [Sie35]. In particular, $L(1,\chi) >> q^{\frac{1}{2}}$, which is a consequence of Dirichlet's class number formula.*

Proof. We present the following short proof for 5.1 from Goldfeld [Gol74]:
Let

$$f(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2) \tag{11}$$

be a zeta function of a bi-quadratic field and let $\lambda = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)$ be the residue at $s = 1$.

Lemma 5.3. *For every $\epsilon > 0$, there exists χ_1 (mod q_1) and $1-\epsilon < \beta < 1$ such that $f(\beta) \le 0$ independent of what χ_2 (mod q_2) may be.*

This must be true since if there are no real zeros in $[1-\epsilon, 1]$ for any $L(s,\chi)$ then $f(\beta) < 0$ if $1-\epsilon < \beta < 1$, since $\zeta(\beta) < 0$. On the other hand, if such real zeros do exist, let β be such a zero and χ_1 be the corresponding character so that $f(\beta) = 0$ independent of χ_2.

It now follows that

$$\begin{aligned} 1 &<< \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f(s+\beta)\frac{x^s}{s(s+1)(s+2)(s+3)(s+4)}ds \\ &= \lambda\frac{x^{1-\beta}}{\prod_{k=1}^{5}(k-\beta)} + \frac{f(\beta)}{4!} + O\left(\frac{(q_1q_2)^{1+\epsilon}x^{-\beta}}{1-\beta}\right) \end{aligned}$$

upon shifting the line of integration to $\sigma = -\beta$. But $f(\beta) \le 0$ by 5.3, and therefore

$$1 << \lambda\frac{x^{1-\beta}}{1-\beta}$$

if $(q_1q_2)^{2+\epsilon} << x$ since $\lambda >> \frac{1}{q_1q_2}$. Consequently, since

$$\lambda << L(1,\chi_2)\log(q_1q_2)\log(q_1)$$

we get

$$L(1,\chi_2) > C \cdot q_2^{-(2+\epsilon)(1-\beta)} log(q_2)^{-1}$$

where constant $C > 0$ depends only on χ_1, and therefore only on ϵ. This proves Siegel's theorem if $(2+\epsilon)(1-\beta) < \frac{1}{2}\epsilon$ and q_2 sufficiently large. □

For a short analytical proof, see Eastermann (1948) [Est48].

Siegel's theorem gives a landmark result on the lower bound of the class number with respect to the magnitude of the discriminant. However, it has an *ineffective* constant C_ϵ in that, given ϵ, there is no way of computing a constant value that makes the inequality hold even though it exists.

Therefore, even with these results and the Dirichlet class number formula, we were still far from solving even the Gauss class number one problem.

Tazuzawa (1952) [Tat52] proved that Siegel's theorem is true with an effectively computable constant for all discriminants $d < 0$, except for at most one.

The first important milestones were obtained by Heegner (1952) [Hee52] , Stark (1967) [Sta67] , Baker (1971) [Bak71] , and Stark (1972) [Sta72], whose work led to the solution of the class number one and two problems.

6. Goldfeld-Gross-Zagier Theorem

The general Gauss class number problem was finally solved completely, at least theoretically, by Goldfeld–Gross–Zagier (Goldfeld (1975) [Gol76] and (1985) [Gol85], Gross and Zagier (1985) [GZ85]) in 1985. Their results combined to reduce the problem of finding all the $d < 0$'s with given $h(d)$ to a finite amount of computation in applying the Dirichlet class number formula.

Theorem 6.1. *(Goldfeld-Gross-Zagier) For every $\epsilon > 0$ there exists an effective computable constant $c > 0$ such that $h(d) > c(\log(|d|)^{1-\epsilon}$.*

This theorem followed from Goldfeld's result in 1975 that if the Hasse-Weil L-function $L_E(s)$ associated with an elliptic curve E over $\mathbb{Q}$ has a triple zero at $s = 1$, then the theorem holds and Gross-Zagier's result in 1985 that such L-function does indeed have a triple zero at $s = 1$.

Even though the Goldfeld-Gross-Zagier theorem reduces the order of magnitude of the lower bound on the class number from almost $|d|^{\frac{1}{2}}$ to less than $\log(|d|)$, it gives an *effective* constant, which can be computed given ϵ.

Its *effectiveness* can be seen in that it can be utilized to limit the possible $d's$ to a finite number of choices, given a fixed class number.

7. The Current State

Oesterlé in 1985 solved the class number 3 problem after improving the result by Goldfeld-Gross-Zagier to the following theorem.

Theorem 7.1. *(Oesterlé) [Oes88] For $(d, 5077) = 1$,*

$$h(d) > \frac{1}{55}\log(|d|) \prod_{p|d, p\neq|d|} \left(1 - \frac{\lfloor 2\sqrt{p}\rfloor}{p+1}\right).$$

Arno (1992) [Arn92] solved the class number four problem, and subsequently, work with Robinson and Wheeler (1998) [ARW98], and work of Wagner (1996) [Wag96] gave a solution to Gauss' class number problem for class numbers 5,6,7 and odd class numbers ≤ 23.

Watkins (2004) [Wat04] obtained the complete list of all imaginary quadratic fields with class number ≤ 100. He adapted the Goldfeld-Oesterlé approach of using an elliptic curve L-function with an order 3 zero at the central critical point to instead using Dirichlet L-functions with low-height zeros near the real line, reducing the computational sieving by about 99.9% and enabling him to complete the computation within seven months.

8. Conclusion and Discussion

The Gauss class number problem has been one of the main drivers in mathematical research for over 200 years in number theory, with wide connection to algebra and analysis, etc. Significant results such as Siegel's theorem and Goldfeld-Gross-Zagier theorem have been proven. Even though $h(d)$ grows approximately in the order of $|d|^{\frac{1}{2}}$ by Siegel's theorem, its constant is uncomputable thus ineffective. The Goldfeld-Gross-Zagier theorem gives a growth rate of approximately $\log(|d|)$ with a computable thus effective constant. Complete lists of imaginary quadratic fields with class number ≤ 100 have been identified by Watkins.

For future work, theoretically, it would be interesting to investigate whether the order of growth can be increased from log with an effective constant and/or whether the effective constant of the lower bound can be increased. It would also be interesting to find efficient algorithm, with or without theoretical advancement, for computing the d's for $h(d) > 100$.

It is worth noting that the Generalized Riemann Hypothesis implies that the class number $h(d)$ is at least

$$(1 + o(1))\frac{\pi}{12e^{\gamma}}\frac{\sqrt{|d|}}{\log\log|d|}$$

by Littlewood (1928) [Lit28] (Paley (1932) [Pal32] has shown that this is best possible except for a factor of two). In other words, if the Generalized Riemann Hypothesis were true, then the best possible growth rate of the class number of imaginary quadratic fields with an effective constant is $\frac{\sqrt{|d|}}{\log\log|d|}$.

9. Acknowledgement

I would like to thank Dr. Simon Rubinstein-Salzedo for suggesting the topic, offering his valuable advice, and teaching us how to do independent mathematical research at Euler Circle, including writing papers and slides in Latex. I would also like to thank my teaching assistant Kishan Jani for providing valuable advice, references, and feedback. Lastly, I would like to thank all the guest speakers for their expert presentations and my classmates at Euler Circle for their fellowship and sharing. I learned a great deal from all of them.

References

[AC81] Raymond G Ayoub and Saravadaman Chowla. On euler's polynomial. *Journal of Number Theory*, 13(4):443–445, 1981.

[Arn92] Steven Arno. The imaginary quadratic fields of class number 4. *Acta Arithmetica*, 60(4):321–334, 1992.

[ARW98] Steven Arno, M Robinson, and Ferrell Wheeler. Imaginary quadratic fields with small odd class number. *Acta Arithmetica*, 83(4):295–330, 1998.

[Bak71] Alan Baker. Imaginary quadratic fields with class number 2. *Annals of mathematics*, 94(1):139–152, 1971.

[Cox22] David A Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions*, volume 387. American Mathematical Soc., 2022.

[Dav13] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[DL73] Joseph Louis De Lagrange. Recherches d'arithmétique. *Nouveaux Mémoires de l'Académie de Berlin*, 1773.

[Est48] Th Estermann. On dirichlet's l functions. *Journal of the London Mathematical Society*, 1(4):275–279, 1948.

[Eul72] L. Euler. Mém de berlin, année 1722, 36. *Comm. Arith.*, 1(584), 1772.

[Gau01] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. in commissis apud Gerh. Fleischer, jun., 1801.

[Gol74] Dorian M Goldfeld. A simple proof of siegel's theorem. *Proceedings of the National Academy of Sciences*, 71(4):1055–1055, 1974.

[Gol76] Dorian M Goldfeld. 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, 1976.

[Gol85] Dorian Goldfeld. Gauss' class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, 13(1):23–37, 1985.

[GZ85] Benedict Gross and Don Zagier. Heegner points and derivatives of l-series. 1985.

[Hee52] Kurt Heegner. Diophantische analysis und modulfunktionen. *Mathematische Zeitschrift*, 56(3):227–253, 1952.

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, (1):150–160, 1934.

[LD39] G Lejeune Dirichlet. Recherches sur diverses applications de l'analyse infinitesimale à la théorie des nombres. 1839.

[Lit28] John E Littlewood. On the class-number of the corpus p (- k). *Proceedings of the London Mathematical Society*, 2(1):358–372, 1928.

[NN74] Władysław Narkiewicz and Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers*, volume 57. Springer, 1974.

[Oes88] Joseph Oesterlé. Le problème de gauss sur le nombre de classes. *Enseign. Math*, 34(1-2):43–67, 1988.

[Pal32] REAC Paley. A theorem on characters. *Journal of the London Mathematical Society*, 1(1):28–32, 1932.

[Rab13] Georg Rabinowitsch. Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern*. 1913.

[Rib06] Paulo Ribenboim. *My numbers, my friends: Popular lectures on number theory*. Springer Science & Business Media, 2006.

[Sie35] Carl Siegel. Über die classenzahl quadratischer zahlkörper. *Acta Arithmetica*, 1(1):83–86, 1935.

[Sta67] Harold M Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, 14(1):1–27, 1967.

[Sta72] Harold Mead Stark. A transcendence theorem for class-number problems (ii). *Annals of Mathematics*, 96(1):174–209, 1972.

[Tat52] Tikao Tatuzawa. On a theorem of siegel. In *Japanese journal of mathematics: transactions and abstracts*, volume 21, pages 163–178. The Mathematical Society of Japan, 1952.

[Wag96] Christian Wagner. Class number 5, 6 and 7. *Mathematics of computation*, 65(214):785–800, 1996.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Mathematics of Computation*, 73(246):907–938, 2004.