Class Number One Problems

Elijah Bunnell

April 24, 2009

Contents

Chapter 1

Origin

In 1798 at the age of 21 Carl Friedrich Gauss wrote his classic number theory book *Disquisitiones Arithmeticae*. Three years later it was published, containing many results from previous mathematicians such as Legendre and Euler, along with many of his own contributions. This work covers many different topics including congruences, quadratic reciprocity, cyclotimic fields and quadratic forms of up to 3 variables. In Section IV, Congruences of the Second Degree, Gauss addresses issues dealing with the behavior of binary quadratic forms, in particular, expressions that can be written as

$$ax^2 + 2bxy + cy^2$$

with discriminant defined to be

$$b^2 - ac.$$

At the end of Section IV in articles 303 and 304 Gauss puts forth a few conjectures of interest. Some of these conjectures remain open questions today, more than 200 years after their publication!

1.1 Gauss' Conjectures

In article 303, Gauss presents a table of select negative discriminants of forms which he conjectures to be complete. He classified them by *class*, and *genus* which will be discussed in more detail later. However, in the English translation of *Disquisitiones Arithmeticae*, Clarke notes Gauss' view that, "... rigorous proofs of these observations [of completeness] seem to be very difficult"[Gau66]. Accompanying these conjectures, Clarke translates Gauss as saying,

> Since the tables [of discriminants] have been extended far beyond [the value of 1848] , and since it furnishes no other belonging to these classes, there seems to be no doubt that the preceding series [of class numbers] does in fact terminate, and by analogy it is permissible to extend the same conclusion to any other classifications.[Gau66]

Genus	Classes/Genus	Negative Discriminant
1	**1**	**1,2,3,4,7**
1	3	11,19,23,27,31,43,67,163
1	5	47,79,103,127
1	7	71,151,223,343,463,487
⋮	⋮	⋮
16	1	840,1320,1365,1848

Table 1.1: Gauss' Discriminant Table

In the following article 304, Gauss discusses forms of positive discriminant,

> It is a curious question and it would not be unworthy of a geometer's talent to investigate the law that governs the fact that [discriminants] having one class in a genus become increasingly rare.[Gau66]

As one can imagine, a statement like this from the great Carl Fredrich Gauss is enough to have claimed the interest of many mathematicians throughout the years.

The conjectures from Gauss' table, together with the comments above make up the classical version of the Gauss Class Number Problem. To avoid confusion, it is necessary to point out that Gauss originally stated these conjectures using a less general representation of binary quadratic forms then we currently use. Today we represent these forms as,

$$ax^2 + bxy + cy^2$$

where the discriminant is defined to be

$$d = b^2 - \mathbf{4}ac.$$

In *Disquisitiones Arithmeticae*, Gauss works on forms as stated earlier

$$ax^2 + \mathbf{2}bxy + cy^2.$$

Notice when working with these forms we have a distinct advantage. We are considering the discriminant to be the term beneath the square root in the quadratic formula

$$(2by)^2 - 4acy^2 = 4y^2(b^2 - ac)$$

and since $4y^2$ is a square, we ignore it and work with the simplified

$$d = b^2 - ac.$$

Notice that Gauss was actually going about solving a much simpler problem then is currently considered the Gauss Class Number Problem. This can cause much confusion if not noted, especially for one picking up *Disquisitiones Arithmeticae* for the first time. Notice, Gauss stated that the negative discriminants having only one class are {-1, -2, -3, -4, -7 } whereas today we consider them to be {-3, -4, -7, -8, -11, -19, -43, -67, -163}.

Definition 1. If $d \neq 1$ is a integer such that $d \equiv 1 \pmod 4$ or $d = 4m$ where m is square-free and $m \equiv 2, 3 \pmod 4$, then we call d a *fundamental discriminant*.

Sometimes, we will have a discriminant with a square factor. In these cases we are interested in the non-square factor. If the square free part does not have the form of a discriminant $b^2 - 4ac$ for some a, b, and c, then we are forced to leave the square factor in the discriminant. Otherwise we need to remove the square factor to obtain a fundamental discriminant. As you can see, Gauss' discriminant is four times larger than the modern form of a discriminant. If we multiply Gauss' class number one discriminants by 4 we get {-4, -8, -12, -16, -28}. Now, disregarding the non-fundamental discriminants we are left with -4 and -8, the even discriminants of the quadratic forms $ax^2 + bxy + cy^2$ with class number one. As you can see, the modern version is substantially more involved.

Another curiosity of Gauss' representation of forms is that he never insists on the relative primality of their coefficients. For instance, we currently consider the following forms

$$6x^2 + 4xy + 10y^2 \approx 3x^2 + 2xy + 5y^2$$

to be equivalent, since they differ by a multiple. Instead, Gauss characterizes these forms as having different *orders*. He defines the order of a form to be the greatest common divisor of the coefficients. Specifically, the $\gcd(a, b/2, c)$ so as to maintain the parity of his xy coefficient since his forms are of the form $ax^2 + 2bxy + cy^2$. So Gauss arranges the forms as orders, genera, and classes. In [Cox89], Cox points out that this is reminiscent of the way in which Carl Linnaeus, a noteworthy botanist and zoologist from just before Gauss' time, classified biology. It doesn't seem unlikely that this is the origin of Gauss' terminology.

1.2 Overview

In this paper we examine some of the developments concerning the Gauss class number problems and build a solid understanding of the class number. First we will develop some background knowledge necessary to understand the problem, specifically the theory of quadratic forms and quadratic fields and how the class number is represented in each. The current form of Gauss' conjectures will not be formally stated until this groundwork is set. The class equation will then be thoroughly examined in order to illustrate the connection between the class number and L-functions. It is assumed that the reader has basic knowledge in abstract algebra and complex analysis. The rest of this chapter will be concerned with understanding binary quadratic forms.

1.3 Class of a Binary Quadratic Form

Impressively, Gauss had discovered and proved that binary quadratic forms of a particular negative discriminant act as a group. It is interesting to note that Gauss discovered this relationship before an explicit definition of a group had even been formalized.

Definition 2. A binary quadratic form

$$f(x,y) = ax^2 + bxy + cy^2$$

is called *positive definite* if $f(x,y) \geq 0$ for all (x,y). Similarly $f(x,y)$ is called *negative definite* if $f(x,y) \leq 0$.

Note that if the discriminant of a form is negative, $b^2 - 4ac < 0$, the form is either positive or negative definite, since by a simple square completion we get that

$$ax^2 + bxy + cy^2 = a\left[\left(x + \frac{by}{2a}\right)^2 - (b^2 - 4ac)\left(\frac{y}{2a}\right)^2\right],$$

an expression whose sign is based completely on a. We will only be concerned with positive definite forms, so we require a to be positive.

Definition 3. Two forms $f(x,y)$ and $g(x,y)$ are *equivalent* if $f(x,y) = g(a,b)$ where $(a,b) = L(x,y)$ for $L \in SL(2,\mathbb{Z})$. If L has determinant $+1$ we say f and g are *properly equivalent*. We denote the set of these equivalence classes by $C(d)$.

Now notice, if $f(x,y)$ is of discriminant c and $g(x,y)$ is of discriminant d are two equivalent forms by the transformation $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$, then we can compute a relationship between the discriminants

$$c = (\alpha\delta - \beta\gamma)^2 d.$$

So equivalent forms always have the same discriminant since the determinant of the transformation is $(\alpha\delta - \beta\gamma) = \pm 1$. This is a very important observation since we will be looking at how forms of a particular choice of d behave. For a given discriminant, we will potentially have forms that are not equivalent. The following discriminant will reoccur in examples because its properties are fairly simple, but non-trivial.

Example 1. *Consider the following two forms of discriminant $d = -20$.*

$$x^2 + 5y^2 \tag{1.1}$$

$$2x^2 + 2xy + 3y^2. \tag{1.2}$$

We claim that these two forms are not equivalent. To see this consider the transformation

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2,\mathbb{Z})$$

of x and y for form (1.1). This will result in

$$(5\gamma^2 + \alpha^2)x^2 + (2\alpha\beta + 10\delta\gamma)xy + (5\delta^2 + \beta^2)y^2.$$

Notice these coefficients will not match up with the coefficients of (1.2) as long as $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$.

We will refer to all equivalent forms of a particular discriminant as being in the same equivalence class, or just *class*. This equivalence is an equivalence relation. In fact, our modern term "equivalence class" originates from Gauss' reference to classes of equivalent forms[Cox89]. We will denote the number of such classes for a particular discriminant d by $h(d)$, the *class number* for quadratic forms.

1.4 Group Structure of Quadratic Forms

One of the amazing properties of quadratic forms of discriminant d is that they form a group! The group operation is quite bizzare and arises from the necessity for the discriminant to remain unchanged.

Definition 4. A form $ax^2 + bxy + cy^2$ is a *reduced form* if $|b| \leq a \leq c$, and $b \geq 0$ if either $a = c$ or $|b| = a$.

Theorem 1. *[Cox89] Every primitive positive definite form is properly equivalent to a unique reduced form.*

It is interesting to note Gauss' wording in artical 175,

> If among all the reduced forms of a given [discriminant], we reject one or the other of the pairs of forms which are properly equivalent without being identical, the remaining forms have the following remarkable property: that any form of the [discriminant] will be properly equivalent to one of them and indeed only to one ... [t]hus ... all forms of the same [discriminant] can be distributed into as many classes as there are remaining forms.[Gau66]

Gauss then goes on to establish many other relationships between forms of a given discriminant, and finally comes about to his formulation of a group relationship between classes. The modern formulation is as follows.

Theorem 2. *[Cox89] If $d < 0$, $d = 0, 1 \pmod 4$, $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ such that f and g both are of discriminant d, then*

$$(f * g)(x, y) = aa'x^2 + Bxy + \frac{B^2 - d}{4aa'}y^2$$

where

$$\begin{aligned} 0 < B < 2aa' \\ B \equiv b \pmod{2a} \\ B \equiv b' \pmod{2a'} \\ B^2 \equiv d \pmod{4aa'} \end{aligned}$$

defines an abelian group operation on the set of positive definite quadratic forms $C(d)$ under the equivalence relation noted above. The order of $C(d)$ is the number of classes, denoted $h(d)$.

A quick computation confirms that $f * g$ is also of discriminant d. Our identity elements for a particular d are known as the principal forms which can be represented as either

$$\begin{cases} x^2 - (d/4)y^2 & \text{if } 4|d \\ x^2 + xy + ((1-d)/4)y^2 & \text{if } d = 1 \pmod 4. \end{cases}$$

We call such a form a *principal form*.

Notice that in the hypotheses of Theorem 2, we have $d = 0, 1 \pmod 4$. The reason for this is very simple,

$$\begin{aligned} d &= b^2 - 4ac \\ &\equiv b^2 \pmod 4. \end{aligned}$$

So we have d as a quadratic residue modulo 4, thus $d = 0, 1 \pmod 4$.

Example 2. *In order to illustrate the multiplicative structure on C(d) we look at forms with $d = -20$. Consider $f(x, y) = 2x^2 + 2xy + 3y^2$ and the principal (identity) form, $i(x, y) = x^2 + 5y^2$. We first determine our value for B.*

$$0 < B < 4$$

$$B \equiv 0 \pmod 2$$

At this point $B = 2$. The other two relationships of B are not even needed to find the unique value of B in this case. So we have,

$$\begin{aligned} (f * i)(x, y) &= 2 \cdot 1x^2 + 2xy + \frac{2^2 - (-20)}{4 \cdot 2 \cdot 1} y^2 \\ &= 2x^2 + 2xy + 3y^2 \\ &= f(x, y) \end{aligned}$$

Unfortunately, Gauss' description of this group relation is very long and complicated, taking up multiple sections in his book. As you have seen, the modern formulation is very awkward, even with the benefit of modern language. Gauss also points out in [Gau66] the fact that this group can be written as a direct product of cyclic subgroups!

1.5 Genera of Binary Quadratic Forms

We will not make much use of genus theory in this paper, but will make a few statements about it for completeness. When determining the class of a particular discriminant, we are specifically interested in how the coefficients of the form behave. An alternative, and very natural method of characterization arises from observing how the forms act when evaluated at values of (x, y). For the following, let $U(R)$ be the units of the ring R.

Definition 5. When a form $f(x, y)$ is evaluated at (x_0, y_0) where x_0 and y_0 are relatively prime, we say f *properly represents* the integer $M = f(x_0, y_0)$.

Curiously, the integers f properly represents modulo d will always be elements of the multiplicative group $U(\mathbb{Z}/d\mathbb{Z})$.

Definition 6. Two forms $f(x, y), g(x, y)$ of discriminant d are of the same genus if the values they properly represent over the integers contained in $U(\mathbb{Z}/d\mathbb{Z})$ are the same.

Example 3. *We will again use $d = -20$ which has two classes, represented by 1.1 and 1.2 which are restated below for convenience.*

$$x^2 + 5y^2$$
$$2x^2 + 2xy + 3y^2$$

By evaluating these at various points, you can see that the only elements properly represented in $U(\mathbb{Z}/20\mathbb{Z})$ are $\{1, 9\}$ for 1.1 and $\{3, 7\}$ for 1.2. Notice that for $D = -20$ we have not represented all elements of $U(\mathbb{Z}/20\mathbb{Z})$.

Theorem 3. *[Cox89] The values of the principal form of discriminant d properly represent a subgroup of $U(\mathbb{Z}/d\mathbb{Z})$, and the values properly represented by any other form of the same discriminant will be a coset.*

Notice that this is true in the example, since our principal form 1.1 properly represents $\{1, 9\}$ which is a subgroup of $U(\mathbb{Z}/d\mathbb{Z})$, and $3\{1, 9\} = \{3, 7\}$ is the coset properly represented by 1.2.

Theorem 4. *[Cox89] All genera of forms of discriminant d consist of the same number of classes, and the number of genera is a power of 2.*

Again, you can see this from the example, since there are 2^1 genera. As stated before, these properties are quite interesting, but will have little to do with the remainder of this paper.

Chapter 2

Connection to Quadratic Fields

Many of the tools necessary to understand the Gauss class number problem come about by viewing it in terms of quadratic fields rather than binary quadratic forms. In this chapter we will use some tools from algebra to form an alternate picture of the class number.

2.1 Basics of Quadratic Fields

Definition 7. A *complex quadratic number field* is a field $\mathbb{Q}(\sqrt{d})$ where $d < 0$ is square-free.

We will use these quadratic fields to understand quadratic forms, so in the end we will be particularly interested in d when it is a fundamental discriminant. We are particularly interested in a generalization of the idea of the integers, $\mathbb{Z}$ in $\mathbb{Q}$, to the *algebraic integers*, O_d in $\mathbb{Q}(\sqrt{d})$.

Definition 8. The *minimal polynomial* for an element α over a field R, $f_\alpha(x) \in \mathbb{Z}[x]$ is the unique irreducible monic polynomial such that $f_\alpha(\alpha) = 0$.

Let's first look at some properties of $\mathbb{Z}$ in $\mathbb{Q}$.

Example 4. *Notice that for any element α of $\mathbb{Z}$, its minimal polynomial in $\mathbb{Z}[x]$ will simply be*

$$f_\alpha(x) = x - \alpha.$$

This is clearly an element of $\mathbb{Z}[x]$. Now, suppose that α is an arbitrary element of $\mathbb{Q}$ other than 0, say $\alpha = \frac{\beta}{\gamma}$ where $(\gamma, \beta) = 1$. We will show that if α is a zero of some monic polynomial in $Z[x]$, then α must be an integer. Say α is a zero of the monic polynomial

$$\sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x],$$

with $c_n = 1$. Then we must have

$$0 = \sum_{i=0}^{n} c_i \beta^i \gamma^{n-i},$$

by multiplying both sides by γ^n. We can write this as

$$\beta^n = \gamma\left(-\sum_{i=0}^{n-1} c_i \beta^i \gamma^{n-i-1}\right),$$

so γ must divide β^n since we have gcd(γ, β)=1. We must then have $\gamma|\beta$, and it must be true that $\gamma = 1$. Thus α must be an integer.

Definition 9. For α in $\mathbb{Q}(\sqrt{d})$ let $f_\alpha(x)$ be the minimal polynomial of α over $\mathbb{Q}$, then α is an *algebraic integer* if $f_\alpha(x)$ is an element of $\mathbb{Z}[x]$.

Theorem 5. *[IR90] The algebraic integers, O_d, form a subring of the quadratic field $\mathbb{Q}(\sqrt{d})$.*

Theorem 6. *[IR90] If $d \equiv 2, 3 \pmod 4$ then $O_d = \mathbb{Z}(\sqrt{d})$. If $d \equiv 1 \pmod 4$ then $O_d = \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$*

A necessary tool for understanding the way in which these integers act is a *norm*. We will define our norm,

$$N : \mathbb{Z}(\sqrt{d}) \to \mathbb{Z}$$

by

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

Now, the norm is multiplicative, which will allow us to determine if elements are irreducible. Notice if

$$N(\alpha) = ab$$

with a, b prime, but there does not exist an x such that

$$N(x) = a,$$

then we must not be able to factor α. So α along with all elements of norm ab must be irreducible. Before we put this norm to use, we need to establish some terminology.

Definition 10. A *zero divisor* is an element $a \neq 0$ such that $ab = 0$ for some $b \neq 0$

Definition 11. An *integral domain* is a commutative ring with unity that contains no zero-divisors.

Definition 12. An integral domain in which every ideal is principal, is a *principal ideal domain.*

Definition 13. An integral domain in which each nonzero, non-unit element can be factored uniquely (up to associates) as a finite product of irreducibles, is called a *unique factorization domain*, or UFD.

Notice that $\mathbb{Z}$ behaves rather nicely as a subring of $\mathbb{Q}$ in that it is a UFD. Ideally, we would hope that each O_d could be treated as a UFD. Unfortunately, this is not always the case.

Example 5. *Consider,*

$$Q(\sqrt{-5})$$

which has a ring of integers

$$O_{-5} = \mathbb{Z}[\sqrt{-5}].$$

Notice the element 6 can be factored in two different ways.

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 - \sqrt{-5})(1 + \sqrt{-5}) \end{aligned}$$

Now, any element of O_{-5} will have norm

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

which cannot be 2 or 3. So elements of norm 6 are irreducible, and we have

$$\begin{aligned} N(1 - \sqrt{-5}) &= 6 \\ &= N(1 + \sqrt{-5}). \end{aligned}$$

Also, notice

$$N(2) = 2 \cdot 2$$

and there are no integers c, and f such that

$$c^2 + 5f^2 = 2.$$

So 2 is irreducible since it is of norm 4. Similarly, 3 is irreducible. So factorization into irreducible elements is not necessarily unique.

2.2 The Ideal Class Group

We determined earlier that the class number for quadratic forms was the order of the group $C(d)$. In a similar fashion, we will identify a group structure in quadratic fields using ideals. Notice we have a few ways of to determine which quadratic number fields have algebraic integers that form a UFD.

Theorem 7. *[DF04] If R is a PID, then R is a UFD.*

Theorem 8. *[DF04] If R is a Euclidean Domain, then R is a UFD.*

One additional method for showing that O_d is a PID, and thus a UFD for a particular d is by looking at its ideals under the following equivalence relation.

Definition 14. Let $A, B \subset O_d$ be ideals. We say A and B are *equivalent*, denoted $A \approx B$, if there are nonzero elements, α, β of O_d such that $(\alpha)A = (\beta)B$ where (α) and (β) are the ideals generated by α and β.

Also, we can derive an equivalent and more descriptive way of writing $(\alpha)A = (\beta)B$ by introducing the following definition.

Definition 15. We say $F \subset \mathbb{Q}(\sqrt{d})$ is a *fractional ideal* if there is a non-zero algebraic integer $\beta \in O_d$ such that βF is an ideal of O_d.

This is a very natural idea which allows us to define $\left(\frac{1}{\beta}\right)$ as the fractional ideal such that

$$\beta\left(\frac{1}{\beta}\right) = O_d.$$

Now we can rewrite $(\alpha)A = (\beta)B$ in the form

$$\left(\frac{\alpha}{\beta}\right)A = B.$$

The set of these fractional ideals forms a group under ideal multiplication.

Definition 16. Let F_d be the group of fractional ideals of O_d, and $B_d \subset F_d$ be the subgroup containing all the principal ideals. The ideal class group of $\mathbb{Q}(\sqrt{d})$ is

$$H_d = F_d/B_d.$$

We denote the order of this group by h_d, known as the *class number* for quadratic fields. Notice that O_d acts as the identity element of the class group. Now, if $h_d = 1$ we have $A \approx O_d$ for all ideals $A \subset O_d$. Thus,

$$(\alpha)A = (\beta)O_d = (\beta)$$

giving us that,

$$A = \left(\frac{\beta}{\alpha}\right)$$

So every ideal is principal. This gives us that whenever $h_d = 1, O_d$ is a UFD. We also have the converse, that every O_d that is a UFD is also a PID, and thus $h_d = 1$ by the following Theorem. Recall that the norm of an ideal is defined to be

$$N(A) = |O_d/A|$$

Theorem 9. *If O_d is a UFD then O_d is a PID.*

Proof. Assume O_d is a UFD and A is one if its prime ideals. Clearly $N(A)$ is an integer and thus an element of O_d. Since O_d is a UFD we can factor $N(A) = a_1 \cdot a_2 \cdots a_n$ uniquely. Also, since the a_i are irreducible, they are prime, since O_d is a UFD. So, $(N(A)) = (a_1)\cdot(a_2)\cdots(a_n)$. Notice, if for x in O_d, $N(A)x$ is an element of A by definition of $N(A)$. This gives us that $N(A)$ is an element of A. Thus,

$$\begin{aligned}(a_1)\cdot(a_2)\cdots(a_n) &= (N(A)) \\ &\subset A\end{aligned}$$

Since A is prime we have that $(a_i) \subset A$ for some $i \leq n$, and (a_i) is also prime and thus maximal so $(a_i) = A$. Thus A is principal and O_d is a PID. □

The problem of showing that a particular O_d is a UFD is thus reduced to showing that $h_d = 1$. We will need the following theorem later on.

Theorem 10. *[IR90] Let p be an odd prime. Then in O_d we have,*

$$(p) = \begin{cases} (p) & \text{if } \left(\frac{d}{p}\right) = -1 \\ (p, a+\sqrt{d})(p, a-\sqrt{d}) & \text{if } \left(\frac{d}{p}\right) = 1, a \in \mathbb{Z}, a^2 \equiv d \mod p \\ (p, \sqrt{d})^2 & \text{if } \left(\frac{d}{p}\right) = 0 \end{cases}$$

This allows us to write a multiplicative function for the number of ideals in O_d of norm m which we will denote η_m and discuss in more detail in chapter 3. We will also need to understand the units of O_d.

Theorem 11. *[IR90] The units U_d of O_d are*

$$U_d = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & \text{if } d = -1 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } d = -3 \\ \{\pm 1\} & \text{else} \end{cases}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$.

So in almost all cases, we will have only 2 units and of greater importance, we never have infinite units.

2.3 Modern Gauss Class Number Problem

So far we have looked at binary quadratic forms, and quadratic fields. We saw Gauss' group of quadratic forms of a particular discriminant, $C(d)$, whose order we called $h(d)$. We also looked at the ideals of the ring of integers for quadratic fields, H_d, and noted a group structure with order h_d. In the following theorem we show a striking relationship between these groups.

Theorem 12. *[Cox89] For a fundamental discriminant $d < 0$ the map $\phi : C(d) \to H_d$ defined by*

$$\phi(ax^2 + bxy + cy^2) = \left(a, \frac{-b + \sqrt{b^2 - 4ac}}{2a}\right)$$

is a group isomorphism.

This result is quite fantastic in that it shows $h(d) = h_d$. From here on we will simply refer to the class number as $h(d)$, noting this encompasses both contexts. We can now state a few of the Gauss class number problems in the modern terminology.

Modern Gauss Class Number Problems

1. $\liminf_{d\to-\infty} h(d) = \infty$.
2. For $d < 0$, $h(d) = 1$ if and only if $d \in -3, -4, -7, -8, -11, -19, -43, -67, -163$.
3. For $d < 0$, find all d such that $h(d) = n$ for small n.
4. There are infinitely many $d > 0$ such that $h(d) = 1$.

The first part of Gauss' conjecture was solved by Hans Heilbronn in 1934[Hei34]. Prior to this contribution, Hans was a student at Gottingen where he studied Number Theory under Landau. In 1933, one year before providing the proof, Hitler came to power in Germany. Shortly after, the Civil Service Law was passed. This called for all "non-Aryan civil servants" to be retired, which included Heilbronn. Luckily, the University of Bristol took him in and provided a small salary which allowed him to continue his work. Hans remained at Bristol for 18 months, where he proved that $h(d) \to \infty$ as $d \to -\infty$. He was able to accomplish this by building on the ideas formulated by Deuring, Mordell and Hecke. While at Bristol, Hans began to collaborate with Edward H. Linfoot, one of his Mathematics Lecturers. At this time, nine quadratic fields of class number one were known. Together, Heilbronn and Linfoot were able to show that there could be at most one additional such field.

Chapter 3

Connection to Analytic Number Theory

3.1 The Dirichlet Class Number Formula

In this section we will apply some analytic number theory to gain some insight into the class number of quadratic fields. Our goal will be to expose a connection between an L-function and the class number known as the Dirichlet Class Number Formula. This connection is what allows us to use modern analytic tools to approach Gauss' problems. This will be done by first relating the Riemann zeta function to the Dedekind zeta function through an L-function by examining properties of complex latices and Euler products. Recall the Riemann Zeta function is the complex valued function,

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

If we look at $\zeta(s)$ for real values s, we can see

$$\int_1^{\infty} \frac{dx}{x^s} \leq \zeta(s) \leq 1 + \int_1^{\infty} \frac{dx}{x^s}$$

and so,

$$\frac{1}{s-1} \leq \zeta(s) \leq \frac{s}{s-1}$$

giving that,

$$1 \leq (s-1)\zeta(s) \leq s.$$

So as $s \to 1^+$, we have $(s-1)\zeta(s) \to 1$, giving us that $\zeta(s)$ has a simple pole at 1 with residue of one.

Definition 17. A Dirichlet series is a complex valued function of the form

$$F(s) = \sum_{m=1}^{\infty} f(m)m^{-s}$$

where f is defined over the positive integers (arithmetic).

Definition 18. A Dirichlet character $\chi_d(n)$ is a multiplicative arithmetic function such that $\chi_d(n) = \chi_d(n+d)$ for all n, and if $gcd(n,d) > 1$ then $\chi_d(n) = 0$, otherwise $\chi(n) \neq 0$.

Definition 19. An $L - function$ or $L - series$ is a Dirichlet series defined by

$$L(\chi_d, s) = \sum_{m=1}^{\infty} \chi_d(m) m^{-s}$$

for a Dirichlet character $\chi_d(m)$.

We will be primarily concerned with

$$L_d(s) := \sum_{m=1}^{\infty} \left(\frac{d}{m}\right) m^{-s},$$

whose Euler Product can write as

$$L_d(s) = \prod_p \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$$

where p is prime and $Re(s) > 1$.

We will examine the Dirichlet series with $f(x) = \eta_x$, the number of ideals of O_d of norm x from the end of Section 2.1. Since η_x is the number of ideas, for a particular norm, we know that it must be multiplicative. We will be attempting to relate the $L_d(1)$ to $h(d)$, so from here on we will restrict our variable s to $\mathbb{R}$. For the remainder of this chapter, we frequently borrow results from [Wes04], sometimes without proof if appropriate. First, we look at some partial sums to build up a nice relationship to the class number. Let

$$A_M = \sum_{m=1}^{M} \eta_m$$

As before let $h(d)$ denote the class number of $\mathbb{Q}(\sqrt{d})$. Let w be the number of units in O_d, which are finite from Theorem 11, and let $\eta_m(C)$ be the number of ideals in a class C with norm m. So clearly, we have,

$$\eta_m = \sum \eta_m(C)$$

where we sum over each class of discriminant d. Also, define

$$A_M(C) = \sum_{m=1}^{M} \eta_m(C).$$

Now, lets focus our attention on the class of principal ideals, C_o. Let b_m be the number of elements of O_d with norm m. We know that each element of O_d has w associates, so we can write

$$w\eta_m(C_o) = b_m.$$

Consider

$$B_M := \sum_{m=1}^{M} b_m.$$

Notice,

$$B_M = wA_M(C_o).$$

We will estimate B_M by viewing O_d as a lattice in the complex plane. The following theorem will allow us more leverage from this point.

Theorem 13. *In the complex plane, let $L = \langle \alpha, \beta \rangle$ be a lattice, let D_t be a disk centered at the origin of radius t, and let A be the area of the parallelogram formed by 0, α, β, and $\alpha + \beta$. For all $t \geq 1$, there exists a C such that,*

$$\left| |L \cap D_t| - \frac{\pi t^2}{A} \right| \leq Ct$$

Proof. For a given t, let $\lambda \in L \cap D_t$, and let P_λ be the parallelogram based at λ. Let $l(t) = |L \cap D_t|$, let $d(t) = \#\{\lambda | P_\lambda \subset D_t\}$, and let $s(t) = \#\{\lambda | P_\lambda \cap D_t \neq \emptyset\}$. So,

$$l(t) < d(t) < s(t).$$

In addition,

$$d(t)A \leq \pi t^2,$$

and

$$\pi t^2 \leq s(t)A,$$

since the area of $D_t = \pi t^2$. Now letting δ be the distance along the diagonal of P_0, we get that $P_\lambda \subset D_{t+\delta}$ for any $\lambda \in L \cap D_t$. Thus,

$$l(t) \leq d(t+\delta) \leq \frac{\pi(t+\delta)^2}{A}.$$

Also notice that if $P_\lambda \cap D_{t-\delta} \neq \emptyset$ then we have that $P_\lambda \subset D_t$, so

$$\frac{\pi(t-\lambda)^2}{A} \leq s(t-\lambda) \leq l(t).$$

Thus,

$$\begin{aligned} \left| l(t) - \frac{\pi t^2}{A} \right| &\leq \frac{\pi}{A}(2t\delta + \delta^2) \\ &\leq \frac{\pi}{A}(2t\delta + \delta^2 t) \\ &\leq Ct. \end{aligned}$$

□

To make use of this theorem notice that we can look at B_M as the set of lattice points of norm $N(\alpha) = |\alpha|^2 \leq M$, so that

$$B_M = \{\alpha \in O_d | \, |\alpha| \leq \sqrt{M}\}.$$

Our theorem then gives us that a constant k exists such that

$$\left| B_M - \frac{\pi}{A} M \right| \leq k\sqrt{M}.$$

We can also say that for $wk' = k$

$$\left| A_M(C_o) - \frac{\pi}{Aw} M \right| \leq k'\sqrt{M}.$$

Now, although this is only clear for the class of principal ideas, we can extend it to all classes.

Theorem 14. *For any ideal class C, there exists a constant k such that*

$$\left| A_M(C) - \frac{\pi}{Aw} M \right| \leq k\sqrt{M}.$$

Now this is where the connection to the class number comes in. By summing over all classes of ideals in the algebraic integers, of which there are $h(d)$, we get

$$\left| A_M - \frac{h(d)\pi}{Aw} M \right| \leq k\sqrt{M}.$$

Theorem 15. *For a given prime p,*

$$\sum_{n=0}^{\infty} \frac{\eta_{p^n}}{p^{ns}} = \begin{cases} (1-p^{-s})^{-2} \text{ if } (\frac{d}{p}) = 1 \\ (1-p^{-s})^{-1} \text{ if } (\frac{d}{p}) = 0 \\ (1-p^{-2s})^{-1} \text{ if } (\frac{d}{p}) = -1 \end{cases}$$

where $(\frac{d}{p})$ is the Legendre Symbol.

Proof. First, recall that η_p is precisely the number of ideals of norm p in the ring of integers of $\mathbb{Q}(\sqrt{d})$. In the case where $(\frac{d}{p}) = 1$, we have that any ideal of norm p^j will be of the form $A^i B^{j-i}$ with $0 \leq i \leq j$ where A and B are the prime ideals of norm p (since there are only 2). So we have $\eta_{p^j} = j + 1$. Now notice,

$$\begin{aligned} \sum_{j=0}^{\infty} (j+1)u^j &= \frac{d}{du} u \sum_{j=0}^{\infty} u^j \\ &= \frac{d}{du} \frac{u}{1-u} \\ &= \frac{1}{(1-u)^2} \end{aligned}$$

Substituting $u = \frac{1}{p^s}$ gives us the first case. The other cases follow similarly. □

We will also need the following results and again refer the reader to [Wes04].

Theorem 16. *Let (a_n) be a real sequence. If there exist real numbers c and $r > 0$ such that*

$$\left|\sum_{m=1}^{M} a_m\right| \leq cM^r$$

then the series

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s},$$

converges for all $s > r$.

Theorem 17. *If (a_m) is a multiplicative sequence such that there exists $c > 0$ with $|\sum_{m=1}^{M} a_m| \leq cM$ for all M, then for $s > 1$,*

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = \prod_p \left(\sum \frac{a_{p^j}}{p^j s}\right).$$

Also, if (a_n) is completely multiplicative and $|a_p| \leq p$ for all p, then

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = \prod_p \left(1 - \frac{a_p}{p^s}\right)^{-1}.$$

Now, we can start our discussion of the Dedekind zeta function. This is defined to be the Dirichlet series with arithmetic function η_m, so that we have,

$$\zeta_d(s) = \sum_{m=1}^{\infty} \frac{\eta_m}{m^s}.$$

Notice that from Theorems 15 and 17 we can write this as

$$\zeta_d(s) = \prod_{p,(\frac{d}{p})=1} (1 - p^{-s})^{-2} \prod_{p,(\frac{d}{p})=0} (1 - p^{-s})^{-1} \prod_{p,(\frac{d}{p})=-1} (1 - p^{-2s})^{-1}$$

Theorem 18. *The Dedekind zeta function ζ_d converges for all $s > 1$ and has a simple pole at $s = 1$ with residue $\frac{h\pi}{A\omega}$.*

Proof. From Theorem 14 we can show that

$$|A_M| \leq \left(\frac{h(d)\pi}{Aw} + k\right) \cdot M$$

for $M \geq 1$. Theorem 16 then gives us that $\zeta_d(s)$ converges for $s > 1$. Now we will look at a new Dirichlet series

$$h(s) = \sum_{m=1}^{\infty} \left(\eta_m - \frac{h(d)\pi}{Au}\right) m^{-s}.$$

Notice that

$$\left|\sum_{m=1}^{M}\left(\eta_m - \frac{h(d)\pi}{Aw}\right)\right| = \left|A_M - \frac{h(d)\pi}{Aw}M\right| \leq k\sqrt{M},$$

so it must converge for $s > \frac{1}{2}$ by Theorem 16. By breaking the sum up we get that for $s > 1$,

$$h(s) = \zeta_d(s) - \frac{h(d)\pi}{Aw}\zeta(s).$$

We saw earlier that $\zeta(s)$ has a simple pole at $s = 1$, so as $s \to 1^+$, we see that $\zeta_d(s) \to \infty$. To show that $\zeta_d(s)$ has a simple pole at $s = 1$ with the stated residue, we notice

$$\begin{aligned}\lim_{s\to 1^+}(s-1)\zeta_d(s) &= \lim_{s\to 1^+}(s-1)h(s) + \frac{h(d)\pi}{Au}\lim_{s\to 1^+}(s-1)\zeta(s)\\ &= 0 + \frac{h(d)\pi}{Au}(1)\end{aligned}$$

□

Theorem 19. *For $s > 1, \zeta_d(s) = \zeta(s)L_d(s)$.*

Proof. The most convenient method of approach is to use Euler products. We have,

$$\begin{aligned}\zeta_d(s) &= \prod_{p,(\frac{d}{P})=1}(1-p^{-s})^{-2}\prod_{p,(\frac{d}{p})=0}(1-p^{-s})^{-1}\prod_{p,(\frac{d}{p})=-1}(1-p^{-2s})^{-1}\\ &= \prod_{p}(1-p^{-s})^{-1}\prod_{p,(\frac{d}{p})=1}(1-p^{-s})^{-1}\prod_{p,(\frac{d}{p})=-1}(1+p^{-s})^{-1}\\ &= \prod_{p}(1-p^{-s})^{-1}\prod_{p}(1-(\frac{d}{p})p^{-s})^{-1}\\ &= \zeta(s)L_d(s).\end{aligned}$$

□

We are now able to state the class number equation.

Theorem 20. ***The Class Number Equation***
For square-free d, we have,

$$L_d(1) = \begin{cases}\frac{h(d)\pi}{\sqrt{-d}\cdot u} & \text{if } d \equiv 2,3(4)\\ \frac{2h(d)\pi}{\sqrt{-d}\cdot u} & \text{if } d \equiv 1(4).\end{cases}$$

Proof. First notice we have

$$A = \begin{cases} \sqrt{-d} \text{ if } d \equiv 2, 3(4) \\ \frac{\sqrt{-d}}{2} \text{ if } d \equiv 1(4). \end{cases}$$

Now, consider

$$\begin{aligned} L_d(1) &= \lim_{s \to 1^+} L_d(s) \\ &= \lim_{s \to 1^+} \frac{\zeta_d(s)}{\zeta(s)} \\ &= \lim_{s \to 1^+} \frac{(s-1)\zeta_d(s)}{(s-1)\zeta(s)} \\ &= \frac{h(d)\pi}{A \cdot u} \end{aligned}$$

□

This relationship is fully illustrated here because it is what allows an understanding of progress in the class-number problems. We clearly have the L-series related to the class number in Theorem 20. So now we can begin to incorporate our knowledge of L-series to gain leverage on the class-number. In particular, it illustrates our ability to incorporate the generalized Riemann Hypothesis.

3.2 Divergence of the Class Number

The first complete proof that $\liminf_{d \to -\infty} h(d) = \infty$ was given by Hans Heilbronn in 1934. The proof was based on a rather peculiar usage of the generalized Riemann hypothesis. The generalized Riemann hypothesis is still without proof so it may appear odd that one could prove a theorem using an unknown hypothesis. The Generalized Riemann Hypothesis claims that:

$$\text{All zeros of } L(\chi, s) \text{ have real part } \sigma \leq \tfrac{1}{2}.$$

In order to do this, Heilbronn used a theorem proved by Hecke in 1918 which equivalently states,

Theorem 21. *[Hei34] If $L_d(s) \neq 0$ for $Re(s) > \frac{1}{2}$ then $\lim_{d \to -\infty} h(d) = \infty$.*

Notice that if the generalized Riemann hypothesis is true then $L_d(s)$ will most certainly have no zeros with real part greater than $\frac{1}{2}$. So Hecke's theorem shows that if the generalized Riemann hypothesis is true then the class number goes to infinity as $d \to \infty$. In 1933 Deuring proved a theorem that pointed mathematicians in a strange direction. His theorem is equivalent to the following.

Theorem 22. *[Hei34] If $\zeta(s)$ has at least one zero for $Re(s) > \frac{1}{2}$ then*

$$\liminf_{d\to-\infty} h(d) \geq 2.$$

At this point the picture gains a bit of clarity. Notice Deuring is saying that if the original Riemann hypothesis is *not* true then the class number will at least *begin* to take off. If only this theorem could be strengthened then perhaps the desired property of class numbers would be established. The next contribution was made by Mordell in the same year. In his paper he states,

> I prove a little more than Deuring does, namely, if [$h(d)$ is] a given number, for an infinity of d, then the Riemann hypothesis is true.[Mor34]

Notice that Mordell shows a generalization of Deuring's theorem where the liminf of $h(d)$ increased from 2 to ∞.

The direction of these ideas is so magnificent that they deserve full accentuation and clarification. Notice that first Hecke shows if the generalized Riemann hypothesis is $false$ then we have $\lim_{d\to-\infty} h(d) = \infty$. Then Mordell shows that if the original Riemann hypothesis is *true* then we have $\lim_{d\to-\infty} h(d) = \infty$. If Mordell's theorem could only be strengthened to encompass the *generalized* Riemann hypothesis, the property of class numbers would be established independent of the Riemann hypothesis. As stated earlier, in 1934 Heilbronn puts together the final piece.

Theorem 23. *[Hei34] If there is at least one real character χ of modulus m (principal or not) so that*

$$L(\rho, \chi) = 0$$

with $Re(\rho) > \frac{1}{2}$ then $\lim_{d\to-\infty} h(d) = \infty$.

Throughout his paper, Heilbronn assumes that that there exists some class number H such that $h(d) = H$ for infinitely many d and proceeds to establish a contradiction. His proof relies on a few key lemmas that we will briefly explore[Hei34]. Let σ be the real part of s, and σ_m is such that $\frac{1}{2} < \sigma_m < Re(\rho) < 1$.

Lemma 24. *For $\sigma_m < \sigma < 2, s \neq 1$,*

$$L_0(s)L_2(s) = \zeta(2s)\prod_{p|m}(1-p^{-2s})\sum_a \chi(a)a^{-s} + o(|s| + \frac{1}{|s-1|})$$

as $d \to \infty$, where a runs through the minima of the H forms of discriminant d.

Here the "minima of the H forms of discriminant d" refers to the minimum value obtainable when evaluating a quadratic form at non-zero integer values.

Lemma 25. *If a runs through the minima of the H quadratic forms belonging to d, then if $\sigma \geq \frac{1}{2}$,*

$$|\sum_a \chi(a)a^{-s}| \geq \frac{1}{4}H^2 + o(1),$$

for $d \to -\infty$.

Heilbronn then evaluates the inequality given in the first lemma at the zero of his L-function ρ, and lets $d \to -\infty$:

$$\begin{aligned} 0 &= \lim_{d\to-\infty} L_0(\rho)L_2(\rho) \\ &= \lim_{d\to-\infty} \zeta(2s)\prod_{p|m}(1-p^{-2\rho})\sum_a \chi(a)a^{-\rho} \end{aligned}$$

Now since $\frac{1}{2} < Re(\rho) < 1$, we can say $\zeta(2s)\prod_{p|m}(1-p^{-2\rho}) \neq 0$. This leaves us with

$$\lim_{d\to-\infty}\sum_a \chi(a)a^{-\rho} = 0.$$

This contradicts the second lemma.

So regardless of whether or not the generalized Riemann hypothesis it true, it must follow that $\lim_{d\to-\infty} = \infty$.

An interesting observation of Heilbronn's theorem was made by Chowla during that same year[Cho34]. He discovered that a simple extension of Heilbronn's first lemma frees his proof from relying on Hecke. He noted that evaluating the inequality at $m = 1$ gives us

$$\zeta(s)L_1(s) = \zeta(2s)\sum_a a^{-s} + o(1).$$

Here, $o(1)$ is simply the "little o" function which simply means some value bounded below by 0 and above by a constant. Now for the strip $\frac{2}{3} < s \leq \frac{4}{5}$ we know that $\zeta(s) < 0$ and clearly $\zeta(2s)\sum_a a^{-s} + o(1)$ is positive, so $L_1(s) < 0$. We also know that $L_1(1) > 0$ so there must be some $\frac{4}{5} < s < 1$ such that $L_1(s) = 0$. Now remember, Heilbronn's theorem is shown assuming that $\lim_{d\to-\infty} h(d) \neq \infty$. Thus, if $L_1(s) \neq 0$ then $\lim_{d\to-\infty} h(d) = \infty$, which takes the place of Hecke's theorem.

3.3 Complete Determination of Class-Number One

Although Heilbronn was able to show that there are only finitely many discriminants of class number one, his proof was ineffective. By this we mean that we are unable to determine exactly when or how the class number takes off, only that its liminf does in fact tend toward infinity. So Heilbronn's paper, although important, sheds no light on the problem of determining how many discriminants are of class number 1. It is known that there exists at least 9 discriminants of class number 1[DF04], namely

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$$

.

As we saw in a previous example, one can easily show that a discriminant, such as -5 for example has class number larger than 1 by showing that the associated quadratic field

$Q(\sqrt{-5})$ has elements in its ring of integers $\mathbb{Z}(\sqrt{-5})$ that factor into irreducibles in more than one way. On the flip side, one can also show that a particular discriminant has class number 1 by showing it gives rise a UFD of algebraic integer, as in Chapter 2. Curiously enough, the first person to make significant progress toward proving that this list of 9 discriminants was complete was a high school teacher Kurt Heegner. Heegner's specializations were mathematics and radio engineering, for which he has a handful of patents. In 1952 he claimed to have a proof that no other discriminants of class number 1 exist other than those listed. Unfortunately, his paper was not widely understood, and was considered to be incorrect, or at best incomplete. His argument used modular forms, and was based on showing that a particular 24 degree polynomial had a 6 degree factor over algebraic integers. He uses this to derive a set of Diophantine equations that have solutions for d, when $h(d) = 1$[Sta69] Unfortunately, his approach was not widely understood, and was considered incomplete if not completely wrong. It wasn't until 1967 that this gap was filled by Stark in the first paper of the Journal of Number Theory[Sta69]. Unfortunately, Heegner died only 2 years prior to the completion of this paper, never receiving the true credit that he deserved. In October of 1966, the mathematics journal received the first complete proof of the complete determination of class number 1 (negative) discriminants. In his paper, *Linear Forms in the Logarithms of Algebraic Numbers*[Bak68], A. Baker developed some new ideas in his Theory of Transcendental Numbers by proving the following.

Theorem 26. *There is an effectively computable number*

$$C = C(n, \alpha_1, ..., \alpha_n, \kappa, d) > 0$$

such that for all algebraic numbers $\beta_1, ..., \beta_n$ not all 0, with degrees at most d, we have

$$|\beta_1 log\alpha_1 + ... + \beta_n log\alpha_n| > Ce^{-(logH)^{\kappa}},$$

where H denotes the maximum of the heights of $\beta_1, ..., \beta_n$.

He then notes that,

> [I]t follows from work of Gelfond and Linnik ... that there are only nine imaginary quadratic fields with class number 1.

Interestingly, in November of 1966, one month after Baker's paper was received, the Michigan Mathematics Journal received a completely different proof of this determination by Stark in the paper, *A Complete Determination of the Complex Quadratic Fields of Class-Number One*[Sta67]. In this paper Stark assumes that the class number $h(d) = 1$ and uses two L-functions to derive a set of Diophantine equations in terms of a sufficiently large discriminant d. Stark then shows that these equations are valid for $d \geq 200$, and that this forces a contradiction. Thus if $h(d) = 1$ we must have $d < 200$, completing the proof. It should be pointed out that the Diophantine equations that Stark derives happen to be the same equations that Heegner used in his incomplete paper. Also recall that it was Stark who completed Heegner's proof in a 1967 paper. In his defense, Stark notes that,

> It is frequently stated that my proof and Heegner's proof are the same. The two papers end up with the same Diophantine equations, but I invite anybody to read both papers and then say they give the same proof![Sta07]

Unfortunately, Heeger's paper is written in German, and an English translation is not widely available. Even if Stark's proof happens to have similar elements as Heegner's proof, Stark should receive all the credit due to a major contributor to this field, especially when one consider that he was the first to present a method of fixing Heegner's proof.

Chapter 4

Further Progress

4.1 Post 1970

Some interesting results came after 1970. One interesting theorem,

Theorem 27. *[Gol85](Goldfeld-Gross-Zagier) For every $\epsilon > 0$ there exists an effectively computable $c > 0$ such that*

$$h(d) > c(log|d|)^{1-\epsilon}$$

For the special case $(d, 5077) = 1$ we get $h(d) \geq \frac{1}{5077} log(|d|)$. Notice that this lower bound is *very* low. Even for $h(d) = 1$ we only have that $d < e^{5077}$. In this paper we have only highlighted $h(d) = 1$. There has been much done in recent history dealing with class numbers $h(d) > 1$. The first step was completed by both Baker and Stark when they joined forces. They were able to completed the determination of $h(d) = 2$ in 1971 by using the method of linear independence of logarithms. Oddly, there are exactly 18 complex quadratic fields with $h(d) = 2$, namely

$$\{15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, 427\}$$

(negatives omitted). Also, many other class numbers have been completely determined. In 1985, Oesterle found a complete list for $h(d) = 3$, and by 1998, $h(d) \leq 7$ and odd numbers $h(d) \leq 23$ had been handled. [Wat04] Then in 2003 Watkins was able to find a determination for all $h(d) \leq 100$. [Wat04] Also there has been some progress made by generalizing quadratic fields to CM-fields, and incorporating the Modified Generalized Riemann Hypothesis. [Sta07] It should be noted that the determination of class number 1 real quadratic fields has not yet been solved. In fact, it is still unknown whether or not there are finitely many.

4.2 Conclusion

The story of the Class Number problems is a very interesting progression in the development of mathematics. The roots of these developments stretch clear back to conjectures of the great Carl Frederich Gauss who's challenge concerning class numbers of real quadratic fields,

> It is a curious question and it would not be unworthy of a geometer's talent to investigate the law that governs the fact that discriminants having one class in a genus become increasingly rare.[Gau66]

has yet to be met. On the road to solving these problems, mathematicians have made great displays of cleverness, even forging a tool out of a hypotheses completely independent of the theorem at hand, the Riemann Hypothesis. The questions of Gauss seem to demand the use of nearly every tool available to number theorists, and have inspire the discovery of new tools. It is also fascinating that the complete classification of class number 1 complex fields was arrived at by two independent mathematicians using completely different techniques. Not to mention that these ideas were completed and submitted only a month apart. It is also unfortunate that Heegner was so close to a solution, but was not recognized for his contributions until shortly after his death.

Bibliography

[Bak68] A. Baker. Linear forms in the logarithms of algebraic numbers. IV. *Mathematika*, 15:204–216, 1968.

[Cho34] S. Chowla. Heilbronn's class-number theorem (ii). *?*, ?:145–146, 1934.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[Gau66] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn., 1966.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *?*, ?:150–160, 1934.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Mor34] L. J. Mordell. On the riemann hypothesis and imaginary quadratic fields with a given class number. *London Math. Soc.*, 9:289–299, 1934.

[Sta67] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[Sta69] H. M. Stark. On the "gap" in a theorem of Heegner. *J. Number Theory*, 1:16–27, 1969.

[Sta07] H. M. Stark. The Gauss class-number problems. In *Analytic number theory*, volume 7 of *Clay Math. Proc.*, pages 247–256. Amer. Math. Soc., Providence, RI, 2007.

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

[Wes04] Tom Weston. Lectures on the dirichlet class number formula for imaginary quadratic fields. *?*, http://www.math.umass.edu/ weston/oldpapers/cnf.pdf:1–63, 2004.