The Structure of the Class Group of Imaginary Quadratic Fields

Nicole Miller

Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

Mathematics

APPROVED:
Dr. Charles Parry
Dr. Peter Haskell
Dr. Ezra Brown

May 11, 2005
Blacksburg, Virginia

Keywords: Binary Quadratic Fields, Class Group, Genera, Positive Definite Forms, 5-rank, 7-rank

©2005, Nicole Miller
The Structure of the Class Group of Imaginary Quadratic Fields

Nicole Miller

Abstract

Let $\mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with discriminant $\Delta$. We use the isomorphism between the ideal class groups of the field and the equivalence classes of binary quadratic forms to find the structure of the class group. We determine the structure by combining two of Shanks’ algorithms [7, 8]. We utilize this method to find fields with cyclic factors that have order a large power of 2, or fields with class groups of high 5-ranks or high 7-ranks.
To my parents, who never gave up.
Acknowledgements

A massive amount of thanks goes to my advisor, Dr. Charles Parry, for his extensive involvement in generating this work. Without his support, dedication, and limitless supply of patience, this paper would not have been realized. Most of all, I am indebted to him for having confidence in me when I was lacking.

I also want to thank the graduate students in McBryde 465 for their constant encouragement and optimistic visions. In particular, I would like to thank Sharon, Sarah, Elizabeth, and Katarina for reminding me of life’s bigger picture.
# Table of Contents

1  Introduction ........................................ 1

2  Representation and Equivalence ...................... 1

3  Reduction of Forms .................................. 2
   3.1 Reduction Algorithm. ............................... 3

4  Correspondence Between Forms and Ideals .......... 4
   4.1 The Relationship. ................................. 4
   4.2 Example. ........................................ 7

5  Genera ............................................. 7

6  Composition of Forms ................................. 9
   6.1 Relation Between Forms. ......................... 9
   6.2 Composition Algorithm. ......................... 11

7  Obtaining the 2-Class Group ......................... 11
   7.1 Theory Behind the Algorithm. .................... 11
   7.2 Square Root Locating Algorithm. ................. 14
   7.3 Example. ........................................ 16
   7.4 Finding the 2-Class Group of Rank 1 and 2. .... 18

8  Obtaining the Odd Part of the Class Group ........ 22
   8.1 Estimating the Class Number. .................... 22
   8.2 Baby Step Giant Step. ............................. 23
   8.3 Finding Independent Forms ....................... 25

9  Class Groups with 5-Rank ........................... 28

10 Class Groups with 7-Rank ............................ 31
List of Tables

7.1 Fields with cyclic 2-group ........................................... 19
7.2 $\Delta = pq$ where $p \not\equiv q \pmod{4}$. ................................. 19
7.3 Fields with discriminant $\Delta$ of form $2pq$ .......................... 20
7.4 Fields with discriminant $\Delta$ of form $4pq$ .......................... 20
7.5 Fields with discriminant $\Delta$ of form $pqr$ .......................... 21
9.1 Class group having 5-rank equal to 4 ................................. 29
9.2 Class group having cyclic factors of order $5^6 = 15625$. ............. 31
10.1 Class group having cyclic factors of order 7 ............................ 32
1. Introduction

It is well known that the equivalence classes of binary quadratic forms create a group under composition that is isomorphic to the class group of a quadratic field of the same discriminant. From now on these groups will be referred to as a class group. In ([9]), Shanks gave an efficient method for computing the 2-Sylow subgroup of the class group. In another article ([8]), Shanks gave a method that became known as the Baby Step Giant Step Algorithm for computing the odd part of the class group. We combine these two methods to provide an efficient algorithm for computing the class group.

As an application of our method, we compute class groups for certain sets of discriminants described by Mestre ([5]) and Schoof ([7]) that give factors of order 5 or 7 in the class group.

First we present some background on the theory of binary forms and their relation to ideals in an imaginary quadratic number field. ([3])

A binary quadratic form is a quadratic form in two variables and has the form \( f(x, y) = ax^2 + bxy + cy^2 \), which is commonly written as \( f = (a, b, c) \). A form has discriminant, \( \Delta = b^2 - 4ac \), that must be congruent to 1 or 0 (mod 4) since only 0 and 1 are quadratic residues mod 4. Most often we will be dealing with primitive forms that also have the criterion that the gcd \( (a, b, c) = 1 \).

In this paper, we will be working with forms having discriminant \( \Delta < 0 \) and \( a \) and \( c \) both positive, which are called positive definite forms.

2. Representation and Equivalence

We say a form represents an integer \( m \) if there are integers \( x \) and \( y \) such that \( ax^2 + bxy + cy^2 = m \). This representation is primitive if the gcd \( (x, y) = 1 \). Given a form that represents \( m \), we can rewrite the equation such that \( 4am = (2ax + by)^2 - \Delta y^2 \). This allows us to see that when \( \Delta \) is negative, the equation is a sum of squares, and we have only finitely many possible solutions for \( x \) and \( y \).

We can also take a given form to another form through a transformation. Consider the transfor-
mation matrix
\[ A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \]

where \(\alpha, \beta, \gamma, \text{ and } \delta\) are integers with \(\alpha\delta - \beta\gamma \neq 0\). Given the form \(f(x, y)\), \(A\) transforms \(f(x, y)\) to \(f'(x', y') = a'x'^2 + b'x'y' + c'y'^2\) by
\[
\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}
\]

where \(a' = a\alpha^2 + b\alpha\gamma + c\gamma^2\), \(b' = b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta)\), \(c' = a\beta^2 + b\beta\delta + c\delta^2\), and \(\Delta' = b'^2 - 4ac' = (\alpha\delta - \beta\gamma)^2\Delta\). We see that \(\Delta = \Delta'\) if and only if \(\alpha\delta - \beta\gamma = \pm1\). We say that a form \(f'(x', y') = (a', b', c')\) is equivalent to a form \(f(x, y) = (a, b, c)\), and we write \(f \sim f'\), if and only if \(f'\) can be obtained from \(f\) by a transformation for which \(\alpha\delta - \beta\gamma = 1\). This relation between forms is an equivalence relationship for it fulfills reflexivity, symmetry, and transitivity properties.

Since we have defined equivalence of forms, it is only logical to find a class representative. To determine the representative for each equivalence class, we will use the process of reduction of forms, and in doing so, we will see that the number of classes of forms of a given discriminant \(\Delta\), known as the class number \(h = h(\Delta)\), will be finite.

We are following the development given in Buell ([1]). Proofs of the results stated in the next three sections can be found in Chapter 4 of his book.

3. Reduction of Forms

We will assume \(\Delta\) is negative valued from this point forward. We define \(f = (a, b, c)\) to be reduced if \(|b| \leq a \leq c\).

\textbf{Lemma 1} If \(f = (a, b, c)\) is a reduced form of discriminant \(\Delta\), then \(|b| \leq \sqrt{|\Delta|/3}\)

\textbf{Proof:} \(4b^2 \leq 4ac = b^2 + |\Delta|, \text{ so } 3b^2 \leq |\Delta|\)
Theorem 1  The number of reduced forms of a fixed discriminant $\Delta$ is finite.

Proof: By lemma 1, the set of possible $b$ values is finite and each $b$ value determines a finite set of factorizations of $b^2 + |\Delta|$ into $4ac$. Therefore there are only finitely many possibilities for reduced forms.

Theorem 2  Every form $f$ of discriminant $\Delta$ is equivalent to a reduced form of the same discriminant.

3.1 Reduction Algorithm:
Let $(a, b, c)$ be a form of discriminant $\Delta$. If this form is not reduced then

**Step 1:** Choose integer $\delta$ such that $|−b + 2c\delta| \leq |c|$. This gives us an equivalent form $(c, −b + 2c\delta, a − b\delta + c\delta^2) = (a', b', c')$ by the transformation matrix

$$A = \begin{pmatrix}
0 & -1 \\
1 & \delta
\end{pmatrix}$$

This form has the property $|b'| \leq a'$.

**Step 2:** If $a' \leq c'$, then we stop. If not, repeat Step 1.

Since we only continue to do Step 1 if $c' < a' = c$, and our forms are positive definite, then the repetition must end, which will give us a reduced form.

Theorem 3  With the exception of $(a, b, a) \sim (a, −b, a)$ and $(a, a, c) \sim (a, −a, c)$ no distinct reduced forms are equivalent.

Eliminating the exceptional cases in the above statement, we will be choosing our class representative to have a nonnegative center coefficient.

Theorem 4  Every form of discriminant $\Delta$ is equivalent to a unique reduced form.

Theorem 5  The number of equivalence classes for a given discriminant is finite.
Proof: Combine Theorem 1 and 2.

Three important types of forms are the principal form, ambiguous forms, and opposite form. The principal form is reduced and defined as \((1, 1, \frac{|\Delta| - 1}{4})\) or \((1, 0, \frac{|\Delta|}{4})\) depending on the parity of \(\Delta\). The ambiguous forms need not be reduced and are defined as \((k, kn, c)\) or \((a, b, a)\) and belong to the ambiguous class. These ambiguous forms are named appropriately because they will help us determine Sylow-2 groups. The opposite of a form \((a, b, c)\) is \((a, -b, c)\). An ambiguous form is equivalent to its own opposite, for if \(b = ka\), then the choice \(\delta = k\) gives \((a, b, c) \sim (c, -b, a) \sim (a, b - 2a\delta, c - b\delta + a\delta^2) = (a, b, c)\).

4. Correspondence Between Forms and Ideals

4.1 The Relationship

In this section, we describe the correspondence between equivalence classes of quadratic forms with negative discriminant and ideal classes in imaginary quadratic fields. We follow the development given in Cohn ([3, Chapter 12]).

Let the ring of integers of the quadratic field \(\mathbb{Q}(\sqrt{d})\) of discriminant \(\Delta\) be called \(O_d\) where \(\Delta = d\) if \(d \equiv 1 (mod 4)\) and \(\Delta = 4d\), otherwise has basis \([1, \omega]\) where \(\omega = \frac{1 + \sqrt{d}}{2}\) if \(d \equiv 1 (mod 4)\) or else \(\omega = \sqrt{d}\). If \(\alpha, \beta \in O_d\) then \([\alpha, \beta]\) denotes the \(\mathbb{Z}\) span of \(\alpha\) and \(\beta\) in \(O_d\).

**Theorem 6** If \(I = [a, b + c\omega]\), then \(I\) is a non-zero ideal of \(O_d\) if and only if \(c|a, c|b, and ac|N(b + c\omega). ([6])\)

A primitive ideal is an ideal that is not divisible by any rational integer factors except \(\pm 1\). By the above theorem, we can take \(c = \pm 1\), when \(I\) is primitive.

When we consider the ideal \(I = [a, b + c\omega]\), we need to distinguish between \(I\) and \(I' = [a, b - c\omega]\), because when we later describe how to find forms from an ideal, the forms obtained from \(I\) will not always be equivalent to the forms obtained from \(I'\).

Given an ideal \(I = [a, b + c\omega] = [\alpha, \beta]\), we say \([\alpha, \beta]\) is an ordered basis if \(\frac{a\beta' - \beta a'}{\sqrt{d}} > 0\) where \(\alpha'\) and \(\beta'\) are conjugates of \(\alpha\) and \(\beta\) respectively. If \(\frac{a\beta' - \beta a'}{\sqrt{d}} < 0\), then the ordered basis for \(I\) is \([\beta, \alpha]\).
Lemma 2  If \( I = [\alpha, \beta] \) is an ordered basis for the primitive ideal \( I \) in the ring \( O_d \) of discriminant \( \Delta \), then the form \( f(x, y) = N(\alpha x + \beta y) = Ax^2 + Bxy + Cy^2 \) has integral coefficients and is a primitive form of discriminant \( \Delta \). The form is said to belong to the ideal \( I \) with basis \([\alpha, \beta]\).

Conversely, we can go from a form to an ideal. Since we can represent any form primitively, we have the following lemma.

Lemma 3  Suppose we are given the primitive quadratic form \( f(x, y) = ax^2 + bxy + cy^2 \) with discriminant \( \Delta \). If \( \Delta \equiv 1 \pmod{4} \) then let \( d = \Delta \), otherwise, let \( d = \frac{\Delta}{4} \). Then the ideal \( I \) of ring \( O_d \) is \( I = [a, b - \sqrt{d}] \).

Lemma 4  Given the primitive ideal \( I = [a, b \pm \omega] \) where \( a \) is the least positive integer in \( I \), \( |O_d : I| = a \).

Proof: Suppose \( \alpha \in O_d \), then \( \alpha = r + s\omega \) where \( r, s \in Z \). Since \( b \pm \omega \in I \), then \( \omega \equiv \mp b \pmod{I} \), so \( \alpha \equiv r \mp sb \pmod{I} \). This means \( \alpha \equiv t \pmod{I} \) for some \( t \in Z \). Since \( t \in Z \), \( t \equiv k \pmod{a} \) where \( 0 \leq k < a \). Since \( a \in I \) then \( \alpha \equiv k \pmod{I} \). Thus, \( |O_d : I| \leq a \).

Now, suppose that \( t_1 + I = t_2 + I \) where \( 0 < t_1 < t_2 \leq a \). Then \( t_2 - t_1 \in I \) implies that \( t_2 - t_1 = ua + v(b + \omega) \) for \( u, v \in Z \). If \( v \neq 0 \) then \( t_2 - t_1 - ua = b = \omega \) where \( t_2, t_1, ua, v, b \in Z \) hence \( \omega \in Q \) but this is a contradiction since \( \omega \) is irrational. So, \( v = 0 \) which implies that \( t_2 - t_1 \equiv 0 \pmod{a} \) so \( |O_d : I| \geq a \). Therefore \( |O_d : I| = a \).

Lemma 5  Primitive ideals correspond to primitive forms in \( O_d \).

Proof: Let \( I = [a, b \pm \omega] \) be a primitive ideal of \( O_d \) for cases 1 and 2.

Case 1: Assume \( d \not\equiv 1 \pmod{4} \). Then \( \omega = \sqrt{d} \), and by Lemma 2, \( f(x, y) = ax^2 + 2bxy + \frac{(b^2 - d)}{a}y^2 \). Let \( \gcd(a, 2b, \frac{(b^2 - d)}{a}) = g \). Suppose there exists an odd prime \( p \) such that \( p|g \), then \( p|a, p|b \), and \( p|\frac{(b^2 - d)}{a} \). Since \( a|(b^2 - d) \) by Lemma 2, then \( ap|(b^2 - d) \) which implies that \( p^2|(b^2 - d) \). Since \( p|b \)
then $p^2|b^2$ so $p^2|d$, but this is a contradiction that $d$ is square free. Thus, $g = 1$ or $g = 2$. Suppose $g = 2$. If $b$ is even, the previous argument works, so suppose $b$ is odd. Since $4|(b^2 - d)$ then $(b^2 - d)$ must be even. Since $b$ is odd, then $d$ must be odd. Since $d$ is odd and $d \not\equiv 1 \pmod{4}$, then $d \equiv 3 \pmod{4}$. Since $b$ is odd, then $b^2 \equiv 1 \pmod{4}$. Thus, $(b^2 - d) \equiv 2 \pmod{4}$. But, this contradicts the fact that $4|(b^2 - d)$. So $g = 1$.

Case 2: Assume $d \equiv 1 \pmod{4}$, then $\omega = \frac{1+\sqrt{\Delta}}{2}$. Then by Lemma 2, $f(x, y) = ax^2 + (2b + 1)xy + \frac{((2b+1)^2-d)}{4a}y^2$. Let $gcd(a, 2b + 1, \frac{((2b+1)^2-d)}{4a}) = g$. Clearly $2 \nmid g$ since $g|(2b + 1)$. Suppose there exists $p|g$ where $p$ is an odd prime. Then $p|a$, $p|(2b + 1)$, and $p|\frac{((2b+1)^2-d)}{4a}$ which implies that $p^2|((2b + 1)^2 - d)$. Since $p|(2b + 1)$ then $p^2|(2b + 1)^2$ which means that $p^2|d$, but this contradicts that $d$ is square free. So $g = 1$.

So we obtain primitive forms from primitive ideals.

Now let $f(x, y) = (a, b, c)$ be a primitive form.

Suppose $\Delta \equiv 0 \pmod{4}$. By Lemma 3, we obtain the corresponding ideal $[a, \frac{b-\sqrt{\Delta}}{2}]$. Since $b^2 - 4ac = \Delta$ then $4|b^2$ so $b = 2b_1$ which implies that $[a, \frac{b-\sqrt{\Delta}}{2}] = [a, b_1 - \sqrt{d}]$ which is primitive.

Suppose $\Delta \equiv 1 \pmod{4}$. By Lemma 3, we obtain the corresponding ideal $[a, \frac{b-\sqrt{\Delta}}{2}]$. Since $\Delta \equiv 1 \pmod{4}$ then $b^2 \equiv 1 \pmod{4}$, which means $b^2$ is odd, which implies that $b$ is odd. Then $\frac{b-\sqrt{\Delta}}{2} = \frac{b+1-1-\sqrt{\Delta}}{2} = \frac{b+1}{2} - \frac{1-\sqrt{\Delta}}{2} = \frac{b+1}{2} + \omega$ and $\frac{b+1}{2}$ is an integer. So $[a, \frac{b-\sqrt{\Delta}}{2}] = [a, \frac{b+1}{2} + \omega]$, which is primitive.

So we obtain primitive ideals from primitive forms.

Using Lemma 2 and Lemma 3, we can construct the following correspondence between forms and ideals of $O_d$.

**Theorem 7** Two forms with the same discriminant are equivalent if and only if the ideals constructed by Lemma 3 for each form are equivalent.
4.2 Example

Let $\Delta = -56$.

Since $\Delta = -56$, and $\frac{-56}{4} = -14 \equiv 2 \ (mod\ 4)$, then $d = -14$ and we are finding ideals in the ring of $O_{-14}$. Since the class number, $h(\Delta)$ of $O_{-14}$ is 4, we have 4 ideal classes: $[1, \sqrt{-14}], [2, \sqrt{-14}], \ [3, 1 + \sqrt{-14}], \text{and} \ [3, 1 - \sqrt{-14}]$. Then ordered bases for these ideals are $[1, -\sqrt{-14}], [2, -\sqrt{-14}], \ [3, 1 - \sqrt{-14}], \text{and} \ [3, -1 - \sqrt{-14}]$. From these ideals we can use Lemma 2 to get the following forms.

Given the principal ideal class $[1, \sqrt{-14}]$ we have $(x - \sqrt{-14}y)(x + \sqrt{-14}y) = x^2 + 14y^2 = (1, 0, 14)$. Given the ideal $[2, -\sqrt{-14}]$ we get the form $(2x - \sqrt{-14}y)(2x + \sqrt{-14}y) = 2x^2 + 7y^2 = (2, 0, 7)$. Given the ideal $[3, 1 - \sqrt{-14}]$, we get the form $(3x + (1 - \sqrt{-14})y)(3x + (1 + \sqrt{-14})y) = 3x^2 + 2xy + 5y^2 = (3, 2, 5)$. Given the ideal $[3, -1 - \sqrt{-14}]$ we get the form $(3x + (1 + \sqrt{-14})y)(3x + (1 - \sqrt{-14})y) = 3x^2 - 2xy + 5y^2 = (3, -2, 5)$.

Conversely, suppose we are given the primitive reduced forms $(1, 0, 14), (2, 0, 7), (3, 2, 5), \text{and} \ (3, -2, 5)$. We can find an ideal for each form in $O_{-14}$ by using Lemma 3. Given $(1, 0, 14)$ we find $I_1 = [1, 0 - \sqrt{\Delta}] = [1, -\frac{\sqrt{-14}}{2}] = [1, -\sqrt{-14}]$. Similarly, given $(2, 0, 7)$ we find $I_2 = [2, -\sqrt{\Delta}] = [2, -\sqrt{-14}]$. Given $(3, 2, 5)$ we find $I_3 = [3, \frac{\sqrt{-14}}{2}] = [3, 1 - \sqrt{-14}]$. Given $(3, -2, 5)$ we find $I_4 = [3, -\frac{\sqrt{-14}}{2}] = [3, -1 - \sqrt{-14}]$.

5. Genera

The generic characters of a discriminant $\Delta$ are the Legendre symbols $(\frac{r}{p})$, where $p$ is an odd prime divisor of $\Delta$, and $r$ is any number represented by a specific form. There will also be a character $(s)$, $(\frac{-1}{r})$, and/or $(\frac{2}{r})$ when $\Delta$ is even. These characters are multiplicative functions from the integers to $(+1, -1)$. We will refer to the values $+1$ and $-1$ as the assigned values. The set of generic characters for a given discriminant is determined as follows. ([1, § 4.1])

1. $(\frac{1}{p})$ for all odd primes $p$ that divide $\Delta$
2. $(\frac{-1}{p})$ if $\Delta$ is even and $(\frac{2}{p}) \equiv 3, 7 \ (mod\ 8)$
3. $(\frac{2}{p})$ if $\Delta$ is even and $(\frac{4}{p}) \equiv 2 \ (mod\ 8)$
4. $(\frac{-1}{p})(\frac{2}{p})$ if $\Delta$ is even and $(\frac{4}{p}) \equiv 6 \ (mod\ 8)$
5. \( (\frac{-1}{r}) \), and \( (\frac{2}{r}) \) if \( \Delta \) is even and \( (\frac{\Delta}{4}) \equiv 0 \pmod{8} \)

**Lemma 6** All the integers \( r \) relatively prime to \( \Delta \) which are representable by forms in a given equivalence class possess the same assigned values of generic characters.

This equivalence class of forms having the same assigned values of generic characters is called a genus. The genus that has all assigned character values of +1 must contain the principal form and is called the principal genus. We will see later that not all possible combinations of assigned values need to exist.

**Lemma 7** The principal genus consists exactly of the subgroup of squares of classes of forms.

A discriminant \( \Delta \) of quadratic forms is called fundamental if either holds:

1. \( \Delta \) is odd and square free
2. \( \Delta \) is even, \( \frac{\Delta}{4} \) is square free, and \( \frac{\Delta}{4} \equiv 2 \text{ or } 3 \pmod{4} \)

Since we are working in \( \mathbb{Q}(\sqrt{d}) \) where \( d \) is negative and square free, we will be only dealing with fundamental discriminants. Hence we will only encounter the first four descriptions of generic characters.

**Lemma 8** The number of generic characters is the number of primes dividing the discriminant.

**Proof:** We note that for odd primes dividing \( \Delta \), we have \( (\frac{\Delta}{p}) \) for each prime \( p \). If \( 2 | \Delta \), then we will have one more generic character according to \( \frac{\Delta}{4} \pmod{8} \).

**Lemma 9** If \( \Delta \) is a fundamental discriminant, then exactly half of the possible genera exist.

**Lemma 10** Let \( \Delta \) be a fundamental discriminant. Then the product of the assigned values for the characters for any given genus is +1.

**Lemma 11** The number of ambiguous classes (including the principal class) is equal to half the number of possible genera.
By combining the four previous lemmas, we see that the number of ambiguous classes that generate the 2-class group is $t - 1$ where $t$ is the number of primes dividing the discriminant.

6. Composition of Forms

6.1 Relation Between Forms

We are aiming to prove that the classes of forms for a specific discriminant make a finite abelian group with composition of forms acting as the group operation and the principal form acting as the identity.

Before we define composition of forms, we will define united forms, which are useful for proving statements, but not as useful for computation. Two forms $(a_1, b_1, c_1)$ and $(a_2, b_2, c_2)$ of the same discriminant are united if the $gcd(a_1, a_2, \frac{b_1 + b_2}{2}) = 1$. We follow the development given in Buell ([1, Chapter 7]).

**Lemma 12** A primitive form can primitively represent an integer that is relatively prime to any chosen number.

**Proof:** Given the form $f = (a, b, c)$ and any integer $m$. Let $Q$ be the product of primes dividing $a$ and $m$ but not $c$. Let $R$ be the product of primes dividing $c$ and $m$ but not $a$. Let $S$ be the product of the remaining primes dividing $m$ but do not divide $a$ nor $c$. The form $f$ represents $aQ^2 + bQRS + c(RS)^2$, which will be shown to be relatively prime to $m$. Let $A = aQ^2 + bQRS + c(RS)^2$.

Case 1: Suppose $p|A$, $p|m$, $p|a$, and $p \nmid c$. Then $p|Q$ and $p \nmid R$ by definition of $Q$ and $R$. Since $p|A$ this means that $p$ must divide $S$. But this is a contradiction since $p|a$.

Case 2: Suppose $p|A$, $p|m$, $p|c$, $p \nmid a$. By definition, $p \nmid Q$, $p|R$, and $p \nmid S$. Since $p|A$ then $p|a$ but this is a contradiction.

Case 3: Suppose $p|A$, $p|m$, $p|a$, and $p|c$. By definition, $p \nmid Q$, $p \nmid R$, and $p \nmid S$. Since $p|A$ then $p$ must divide $b$, but since the form is primitive, this is a contradiction.

Case 4: Suppose $p|A$, $p|m$, but $p$ divides neither $a$ nor $c$. By definition, $p|S$ and $p \nmid Q$. Since $p|A$ then $p$ must divide $a$, but this is a contradiction.
Theorem 8  Given any two forms $f_1$ and $f_2$ of the same discriminant, then there exists a form $f_3$ such that $f_2 \sim f_3$ and $f_1$ and $f_3$ are united. Hence, any two forms of the same discriminant can be written as united forms.

Proof: Given $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ then we know by the above lemma that $f_2$ primitively represents an integer $a_3$ with $\gcd(a_1, a_3) = 1$. This means that $a_3 = a_2u^2 + b_2uv + c_2v^2$ and $\gcd(u, v) = 1$. Since $\gcd(u, v) = 1$ we can use the Euclidean algorithm to find $r$ and $s$ such that $1 = ur + vs$. Now we can make the tranformation matrix

$$A = \begin{pmatrix} u & -s \\ v & r \end{pmatrix}$$

with determinant 1. Thus, the effect of our transformation gives us that $x = ux' - sy'$ and $y = vx' + ry'$. Since $a' = a_2u^2 + b_2uv + c_2v^2 = a_3$ then $f_2 \sim f_3 = (a_3, b_3, c_3)$. Since $\gcd(a_1, a_3) = 1$, then $\gcd(a_1, a_3, \frac{b_1 + b_2}{2}) = 1$; therefore, $f_1$ and $f_3$ are united.

Lemma 13 If $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ are united forms, then there exist forms $(a_1, B, a_2C)$ and $(a_2, B, a_1C)$ such that $(a_1, b_1, c_1) \sim (a_1, B, a_2C)$ and $(a_2, b_2, c_2) \sim (a_2, B, a_1C)$.

If we have the united forms $f_1$ and $f_2$ as above then the form compounded is $(a_1a_2, B, C)$ which we write $f_1 \circ f_2$.

Theorem 9 Under composition, the classes of forms of a fixed discriminant form a finite abelian group. The identity of the group is the principal form and the inverse of the class of any form is the class of the opposite of the form.

Note that the composition of forms is similar to the composition of ideal classes. Furthermore, the classes which are of order 2 in the class group are precisely those classes which contain ambiguous forms.

Lemma 14 The classes which are of order 1 and 2 in the class group are precisely those classes which contain ambiguous forms. Furthermore, the rank of the 2 class group is $t-1$ where $t$ is the number of primes dividing the discriminant.
6.2 Composition Algorithm

To compound \( f_1 = (a_1, b_1, c_1) \) and \( f_2 = (a_2, b_2, c_2) \)

**Step 1:** Let \( \beta = \frac{b_1 + b_2}{2} \); let \( m = \gcd(a_1, \beta) \); let \( n = \gcd(m, a_2) \).

**Step 2:** Solve \( a_1 x + \beta y = m \) for \( x \) and \( y \) by using Euclidean algorithm.

**Step 3:** Solve \( m z n = b_2 - b_1 - c_1 y (mod \ a_2 n) \) for \( z \) by using the fact that \( n = \gcd(m, a_2) \) so \( \gcd\left(\frac{m}{n}, \frac{a_2}{n}\right) = 1 \) and using the Euclidean algorithm to find the inverse of \( \frac{m}{n} \ (mod \ \frac{a_2}{n}) \).

**Step 4:** The form compounded of \( f_1 \) and \( f_2 \) is then \( (\frac{a_1 a_2}{m^2}, \frac{b_1 + 2 b_1 z}{n}, \ast) \) where * is computed from the discriminant formula.

7. Obtaining the 2- Class Group

7.1 Theory Behind the Algorithm

If an ambiguous class is in the principal genus, then Lemma 3 tells us that it’s a square; hence, it has a square root. Shanks ([9]) states how to compute the square root of a form given a discriminant. Shanks basically follows a method of Gauss that can be found in Disquisitiones Arithmeticae ([5]).

We reiterate the algorithm of finding the square root of a form until we obtain a form that is not in the principal genus. The number of iterations will provide us with the order of that particular form, for when we take the square root \( k \) times then our form will have order \( 2^{k+1} \). Since we know that the rank of the 2-class group is \( t - 1 \) where \( t \) is the number of prime divisors of \( \Delta \), then we need to begin with \( t - 1 \) independent ambiguous forms.

In accordance with Shanks ([9]), we will use his notation in this section. For a quadratic form \( F = A\epsilon^2 + 2B\epsilon y + Cy^2 \), \( F = (A, B, C) \), we see that the middle term is halved. We call \( D = B^2 - AC \) the determinant of \( F \). Using his notation, \( \Delta = 4(B^2 - AC) = 4D \). If \( \Delta \equiv 1 \ (mod \ 4) \), we use the forms of discriminant \( 4\Delta = \delta \), because the primitive binary quadratic forms of discriminant \( 4\Delta \) constitute a group isomorphic to that of \( \mathbb{Q}(\sqrt{\Delta}) \). Hence, we will let \( \delta = 4\Delta \) if \( \Delta \equiv 1 \ (mod \ 4) \), and \( \delta = \Delta \) otherwise.
Assume that $F = (a_1, b_3, a_2) = a_1x^2 + 2b_3xy + a_2y^2$ is in the principal genus. We want to find $f = (a, b, c)$ such that $f^2 \sim F$ under composition. By adding three terms we enlarge $F$ into a ternary form $a_1x^2 + a_2y^2 + a_3z^2 + 2b_1yz + 2b_2xz + 2b_3xy$ which we write as

$$t = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

We define the determinant of $t$ as $D(t) = b_2^2a_1 - b_2^2a_2 + b_3^2a_3 - a_1a_2a_3 - 2b_1b_2b_3 = +1$. The form $t$ has an adjoint which we define as

$$T = \begin{pmatrix} A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \end{pmatrix}$$

where entries are given by the equations:

$$A_1 = b_1^2 - a_2a_3,$$
$$A_2 = b_2^2 - a_1a_3,$$
$$A_3 = b_3^2 - a_1a_2,$$
$$B_1 = a_1b_1 - b_2b_3,$$
$$B_2 = a_2b_2 - b_1b_3,$$
$$B_3 = a_3b_3 - b_1b_2.$$ 

Since the adjoint of $T$ is $t$ because $D(t) = 1$, then we also have the equations:

$$a_1 = B_1^2 - A_2A_3,$$
$$a_2 = B_2^2 - A_1A_3,$$
$$a_3 = B_3^2 - A_1A_2,$$
$$b_1 = A_1B_1 - B_2B_3,$$
$$b_2 = A_2B_2 - B_1B_3,$$
$$b_3 = A_3B_3 - B_1B_2.$$ 

We see that $A_3$ is the determinant of $F$. $F$ represents $a_1$ and $a_2$, and since $F$ is in the principal genus, then $a_1$ and $a_2$ are quadratic residues of all prime divisors of $A_3$. Therefore we can find solutions consistent with the above equations for $B_1^2 = a_1 + A_2A_3$, $B_2^2 = a_2 + A_1A_3$, and $B_1B_2 = -b_3 + B_3A_3$ by solving appropriate congruences. This is done as follows. Since we are given the form, we know $a_1$, $b_3$, and $a_2$. Therefore, we can compute $A_3 = b_3^2 - a_1a_2$, which allows
us to solve the following congruences: \( B_2^2 \equiv a_2 \pmod{A_3} \) and \( B_1^2 \equiv a_1 \pmod{A_3} \). We also know that \( (B_1B_2)^2 \equiv a_1a_2 \equiv b_3^2 \pmod{A_3} \). We need to choose \( B_2 \) such that \( B_1B_2 \equiv -b_3 \pmod{A_3} \). It easy to choose \( B_2 \) that makes \( B_1B_2 \equiv -b_3 \pmod{A_3} \) if \( A_3 \) is prime because taking a square root mod a prime number is ± the same value, so we just have to choose the sign of \( B_2 \). However, if \( A_3 \) is not prime we have more choices. The solving of the congruences as well as the choosing of \( B_2 \) is found in our com function in Mathematica, known by Shanks ([9]) as COMTAT. We choose \( B_2 \) using the following logic.

We factor \( A_3 \) into its prime factors: \( p_1, p_2, ..., p_n \). We then find a square root of \( a_1 \pmod{p_i} \) for each \( p_i \) in the same order as we factored \( A_3 \). Call this ordered list Sqa1. Then we do the same for finding a square root of \( a_2 \pmod{p_i} \) and call this ordered list Sqa2. We make an array with first row Sqa1 and the second row Sqa2. Now we create a \( m \times n \) array, called \( A \), where \( n \) is the number of prime divisors of \( A_3 \) and \( m = 2^n \). Each vector has values of ±1. The array \( A \) is an exhaustive list of all sign combinations. This will allow us to change the values in Sqa2. Each time we change a sign combination in Sqa2, we use the Chinese Remainder Theorem to compute \( B_1 \) and \( B_2 \).

We then check to see if the side condition \( B_1B_2 \equiv -b_3 \pmod{A_3} \) is satisfied; when it is, then we stop.

Once we find \( B_1 \) and \( B_2 \), we can solve \( a_1 = B_1^2 - A_2A_3 \) for \( A_2 \), \( a_2 = B_2^2 - A_1A_3 \) for \( A_1 \), and \( b_3 = A_3B_3 - B_1B_2 \) for \( B_3 \). This will give us \( T \) so we can compute \( a_3, b_1, \) and \( b_2 \) needed to complete \( t \) from above.

After computing the above, we have the matrix \( t \). Then through a series of linear transformations that culminate in

\[
M = \begin{pmatrix} - & - & - \\ - & - & - \\ X & Y & Z \end{pmatrix}
\]

which tranforms \( t \) into

\[
u = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}
\]
If \( \epsilon \) is the sign of \( X \), then \( f = (\epsilon X, -Y, 2\epsilon Z) \) or \( f = (2\epsilon X, -Y, \epsilon Z) \) accordingly as \( X \) is odd or even. We do this through the program called \textit{GATESR}.

In \textit{GATESR}, we start with the form \((a_1, b_3, a_2)\) that is in the principal genus. After following the above algorithm, we find \( t \). In reducing the ternary form \( t \) to \( u \), we must make a series of binary form reductions. We perform these reductions using our reduction algorithm found in Section 3, only we end up with the satisfied inequality \( 2|b| \leq a \leq c \) because of our new notation in this section.

After reduction, we apply two phases: \textit{Phase 0} and \textit{Phase 1}. Phase 0 will be a reduction on the form \((A_3, B_1, A_2)\). This form will have determinant \( a_1 \). Phase 1 will be a reduction on the form \((a_1, b_3, a_2)\). This form will have a determinant \( A_3 \). We will alternate reductions of these forms for which each time we will obtain a new form for both. After a finite number of Phase 0 and Phase 1 transformations, we will obtain \( a_1 + A_3 = 0 \) or \(|a_1| = |A_3| = 1 \). If \( a_1 + A_3 = 0 \) or \(|a_1| = |A_3| = 1 \) is satisfied, there are five cases, and in each one we may transform the current \( t \) into \( u \) by an explicit matrix \( \mu \). Now we find \( f \) using \( f = (\epsilon X, -Y, 2\epsilon Z) \) or \( f = (2\epsilon X, -Y, \epsilon Z) \).

We apply \textit{GATESR} to each form in the list \( L1b \), which is described below, to collect a set of forms and their respective orders that generate the 2-Class Group.

### 7.2 Square Root Locating Algorithm

**Step 1.** Compute a list of ambiguous forms as follows:

For each odd prime divisor \( p \) of \( \Delta \), add the form \((p, 0, \frac{-\delta}{4p})\). If \( \Delta \) is even and for \( \Delta' = \frac{\Delta}{4} \), add one of the following forms: \((2, 2, c)\) where \( c \) is odd if \( \Delta' = 2c - 1 \) is odd, or \((2, 0, \frac{\Delta'}{2})\) if \( \Delta' \equiv 2, 6 \pmod{8} \).

Therefore we will have \( t \) ambiguous forms in our list where \( t \) is the number of prime divisors of \( \Delta \). We prepend a 1 to each form to indicate its order is \( 2^t \) and call the list \( L1b \).

**Step 2.** Calculate the generic character table for the list of forms in \( L1b \).

In order to calculate a generic character, we need to factor \( \Delta \).
Add all odd prime divisors of $\Delta$ to a list called $L_p$. If $\Delta$ is even, then we prepend $-1$ if $\frac{\Delta}{4}$ is odd, we prepend $2$ if $\frac{\Delta}{4} \equiv 2 \pmod{8}$, or we prepend $-2$ if $\frac{\Delta}{4} \equiv 6 \pmod{8}$.

In order to calculate the generic table, we need to find the Jacobi Symbol for each ambiguous form using the above list $L_p$. To compute future forms, we induce an isomorphism $\phi$ that takes the assigned values of $+1$ and $-1$ from the Jacobi Symbol from a multiplicative group to an additive group $\mathbb{Z}_2$ by $\phi(-1) = 1$ and $\phi(1) = 0$. We then have an adjusted valued generic table. In our Mathematica program, it is a set of vectors such that the first vector corresponds to the assigned values under the isomorphism calculated from the first ambiguous form with respect to the list $L_p$.

The number of entries in each vector is $t$ when $\Delta$ is odd and $t + 1$ otherwise, where $t$ is the number of odd prime divisors $\Delta$. In our program, the set of these vectors are referred to CharTab.

**Step 3.** We take the above set of vectors (CharTab) and find the nullspace ($\pmod{2}$) of this set.

After finding the nullspace of the set CharTab, we will receive a list of vectors, call it $V$, with $t$ entries of values 0 or 1, where $t$ is the number of prime divisors of $\Delta$. In fact, each entry of a vector in $V$ corresponds to a product of forms in the list $L_1b$. For each vector in $V$, we locate the 1-valued entries and take the corresponding forms in $L_1b$ and compose them. This will give us a form in the principal genus, because each generic character of this new form will have a value of $+1$. We then compute the square root of each form in the nullspace and call this set of square roots $S$.

**Step 4.** We make a new list of forms. We replace $L_1b$ with this new list.

We make a new list having the same number of forms as we had in $L_1b$. To do this, we add $S$ and take out the forms corresponding to the last 1 value in each vector of $V$. For instance, suppose we have the ambiguous forms $f_1$, $f_2$, $f_3$ and $f_4$. Suppose one of the nullspace vectors looks like $(1, 1, 0, 0)$. This tells us that we compose $f_1$ and $f_2$ to get a new form $f_5$. We then compute the square root $f_6$ of $f_5$, which is in the principal genus. Then we make a new list by including $f_6$ and deleting $f_2$, where $f_6$ has the order of $f_2$ plus one. Hence, we will get a new list with the same number of forms.

**Step 5.** Repeat the process.
After obtaining this new list of forms, we begin the process all over again by generating a new CharTab for the new list of forms and then finding its nullspace. We repeat this process until the nullspace is empty, which will make CharTab independent. Given the final $L_1b$ list, we can easily obtain the 2-class group structure from the exponent entries.

7.3 Example

Let $\Delta = -1560$.

**Step 1:** $\Delta = 2^3 \cdot 3 \cdot 5 \cdot 13$. $\Delta$ is even and $\frac{\Delta}{4} \equiv 2 \pmod{8}$ so $L_1b = \{(1,(2,0, 195)), \{(3,0, 130)), \{(5,0, 78)), \{(13,0, 30))\} = \{\{1,f_1\}, \{1,f_2\}, \{1,f_3\}, \{1,f_4\}\}$.

**Step 2:** The prime list will be $L_p = \{2, 3, 5, 13\}$ because $\frac{\Delta}{4} \equiv 2 \pmod{8}$.

We can quickly see that the first and last coefficients are represented by each form. For instance, the form $f_1$ can represent $2 = 2x^2 + (0)xy + 195y^2$ when $x=1$ and $y=0$ or $195 = 2x^2 + (0)xy + 195y^2$ when $x=0$ and $y=1$. We choose the first number for each form to represent if it is not divisible by the prime associated with the character, otherwise we choose the last number. Therefore the generic table will be:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_1$</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$f_2$</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$f_3$</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$f_4$</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

Now we apply $\phi$ to get CharTab:

$$CharTab = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0
\end{pmatrix}$$
If we compose all the ambiguous forms in the list $L1b$, we will obtain the principal form. Therefore, we can eliminate an ambiguous form of the form $(p, 0, \frac{\delta}{16})$ where $p$ is an odd prime. We chose to eliminate the last form in $L1b$, hence we can eliminate the last row of the above matrix. In future calculations, we will disregard the last form. We can also eliminate the last column of this matrix because the product of all the character values is $+1$, or under $\phi$, the sum of the entries is zero. Therefore, we obtain the new matrix

$$\begin{pmatrix}
1 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 1
\end{pmatrix}$$

**Step 3:** Now we want to find the nullspace of the above matrix so we row reduce the following

$$\begin{pmatrix}
1 & 1 & 1 & a \\
1 & 0 & 1 & b \\
1 & 1 & 1 & c
\end{pmatrix}$$

to receive

$$\begin{pmatrix}
1 & 0 & 1 & b \\
0 & 1 & 0 & a + b \\
0 & 0 & 0 & a + c
\end{pmatrix}$$

This means if we compose $f_1$ with $f_3$ we will obtain a form which has a square root. In this case $f_1 \circ f_3 = (10, 0, 39) = f_5$ which has the square root $(7, -3, 57) = f_6$.

**Step 4:** The next time our $L1b = \{1,f_1\}, \{1,f_2\}, \{2,f_6\}$.

**Step 5:** When we repeat the process we will get the following generic table
\[
\begin{array}{c|c|c|c|c}
 & 2 & 3 & 5 & 13 \\
\hline
f_1 & -1 & -1 & -1 & -1 \\
f_2 & -1 & 1 & -1 & 1 \\
f_6 & 1 & 1 & -1 & -1 \\
\end{array}
\]

and

\[
\text{CharTab} = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 \\
\end{pmatrix}
\]

So we get

\[
\begin{pmatrix}
1 & 1 & 1 & a \\
1 & 0 & 1 & b \\
0 & 0 & 1 & c \\
\end{pmatrix}
\]

When we find the nullspace we obtain

\[
\begin{pmatrix}
1 & 0 & 0 & 2a + b + c \\
0 & 1 & 0 & a + b \\
0 & 0 & 1 & c \\
\end{pmatrix}
\]

Our nullspace is empty, so our \( L1b = \{ \{1, f_1\}, \{1, f_2\}, \{2, f_6\} \} \). We see that the structure of our 2-class group is \( Z_2 \times Z_2 \times Z_4 \), since our exponents are 1, 1, 2.

### 7.4 Finding the 2-Class Group of Rank 1 and 2

After producing our algorithm to find the 2-class group of a field with discriminant \( \Delta \), we generated \( \Delta \) values to obtain particular 2-class groups.
First we generated Δ values so that we would have exactly 2 discriminantal divisors, which would make our 2-class group be cyclic. We took Δ values of the form 2p, or p if \( p \equiv 1 \pmod{4} \). We let p run over the first 2,000,000 primes, and our results follow. In the table, we denote by \( (2^n) \) the class group \( Z_{2^n} \).

<table>
<thead>
<tr>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>1500039</td>
<td>(2)</td>
<td>46686</td>
<td>(2^6)</td>
<td>1528</td>
<td>(2^{11})</td>
</tr>
<tr>
<td>749958</td>
<td>(2^2)</td>
<td>23488</td>
<td>(2^7)</td>
<td>705</td>
<td>(2^{12})</td>
</tr>
<tr>
<td>375163</td>
<td>(2^3)</td>
<td>11721</td>
<td>(2^8)</td>
<td>134</td>
<td>(2^{13})</td>
</tr>
<tr>
<td>187601</td>
<td>(2^4)</td>
<td>5756</td>
<td>(2^9)</td>
<td>1</td>
<td>(2^{14})</td>
</tr>
<tr>
<td>94101</td>
<td>(2^5)</td>
<td>2877</td>
<td>(2^{10})</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7.1: Fields with cyclic 2-group

Then we generated Δ values so the 2-class group would be cyclic and Δ would be comprised of two odd primes \( p \) and \( q \) such that \( p \not\equiv q \pmod{4} \). We let \( p \) and \( q \) run over the first 2000 primes for which we got the following results.

<table>
<thead>
<tr>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>505641</td>
<td>(2)</td>
<td>15644</td>
<td>(2^6)</td>
<td>448</td>
<td>(2^{11})</td>
</tr>
<tr>
<td>248457</td>
<td>(2^2)</td>
<td>7542</td>
<td>(2^7)</td>
<td>153</td>
<td>(2^{12})</td>
</tr>
<tr>
<td>123365</td>
<td>(2^3)</td>
<td>3857</td>
<td>(2^8)</td>
<td>36</td>
<td>(2^{13})</td>
</tr>
<tr>
<td>62130</td>
<td>(2^4)</td>
<td>1847</td>
<td>(2^9)</td>
<td>7</td>
<td>(2^{14})</td>
</tr>
<tr>
<td>30755</td>
<td>(2^5)</td>
<td>935</td>
<td>(2^{10})</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7.2: Δ = \( pq \) where \( p \not\equiv q \pmod{4} \)

Next, we generated Δ values so that we would have exactly 3 discriminantal divisors, which would make our 2-class group have rank 2. These values took the form \( 2pq \) where \( p \) and \( q \) are both odd, and \( p \) and \( q \) run up to the 2000th prime. We tracked the structure of our 2-class groups by using a matrix, whose entry values recorded the number of 2-class groups with the row number representing the lowest factor of the 2-group, and the column number representing the highest factor of
the 2-group. We obtained the following results. In the table, we denote by \((2^n, 2^m)\) the class group \(\mathbb{Z}_{2^n} \times \mathbb{Z}_{2^m}\).

<table>
<thead>
<tr>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>880645</td>
<td>(2,2)</td>
<td>51179</td>
<td>(2^2,2^3)</td>
<td>430</td>
<td>(2^3,2^7)</td>
</tr>
<tr>
<td>469185</td>
<td>(2^2,2)</td>
<td>25178</td>
<td>(2^2,2^4)</td>
<td>204</td>
<td>(2^3,2^8)</td>
</tr>
<tr>
<td>234130</td>
<td>(2^2,3)</td>
<td>12808</td>
<td>(2^2,2^5)</td>
<td>107</td>
<td>(2^3,2^9)</td>
</tr>
<tr>
<td>116554</td>
<td>(2^2,14)</td>
<td>6404</td>
<td>(2^2,2^6)</td>
<td>50</td>
<td>(2^3,2^{10})</td>
</tr>
<tr>
<td>58320</td>
<td>(2^5)</td>
<td>3186</td>
<td>(2^2,2^7)</td>
<td>10</td>
<td>(2^3,2^{11})</td>
</tr>
<tr>
<td>29108</td>
<td>(2^6)</td>
<td>1565</td>
<td>(2^2,2^8)</td>
<td>251</td>
<td>(2^4,2^4)</td>
</tr>
<tr>
<td>14599</td>
<td>(2^7)</td>
<td>731</td>
<td>(2^2,2^9)</td>
<td>198</td>
<td>(2^4,2^5)</td>
</tr>
<tr>
<td>7362</td>
<td>(2^8)</td>
<td>392</td>
<td>(2^2,2^{10})</td>
<td>108</td>
<td>(2^4,2^6)</td>
</tr>
<tr>
<td>3667</td>
<td>(2^{10})</td>
<td>157</td>
<td>(2^2,2^{11})</td>
<td>53</td>
<td>(2^4,2^7)</td>
</tr>
<tr>
<td>1845</td>
<td>(2^{11})</td>
<td>50</td>
<td>(2^2,2^{12})</td>
<td>24</td>
<td>(2^4,2^8)</td>
</tr>
<tr>
<td>856</td>
<td>(2^{12})</td>
<td>1</td>
<td>(2^2,2^{13})</td>
<td>9</td>
<td>(2^4,2^9)</td>
</tr>
<tr>
<td>403</td>
<td>(2^{13})</td>
<td>4250</td>
<td>(2^3,2^3)</td>
<td>1</td>
<td>(2^4,2^{10})</td>
</tr>
<tr>
<td>99</td>
<td>(2^{14})</td>
<td>3261</td>
<td>(2^3,2^4)</td>
<td>1</td>
<td>(2^4,2^{11})</td>
</tr>
<tr>
<td>2</td>
<td>(2^{15})</td>
<td>1631</td>
<td>(2^3,2^5)</td>
<td>15</td>
<td>(2^5,2^5)</td>
</tr>
<tr>
<td>67243</td>
<td>(2^2,2^2)</td>
<td>712</td>
<td>(2^3,2^6)</td>
<td>11</td>
<td>(2^5,2^6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 7.3: Fields with discriminant \(\Delta\) of form \(2pq\)

Next we used \(\Delta\) values of the form \(4pq\) where \(p\) and \(q\) odd primes and \(pq \equiv 1 \pmod{4}\) that run up to the 5000 prime. We tracked the structure of our 2-class groups as above and our results follow.

<table>
<thead>
<tr>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>2359536</td>
<td>(2,2)</td>
<td>26064</td>
<td>(2^2,2^5)</td>
<td>15</td>
<td>(2^3,2^{12})</td>
</tr>
<tr>
<td>1758793</td>
<td>(2^2,2)</td>
<td>13096</td>
<td>(2^2,2^6)</td>
<td>1</td>
<td>(2^3,2^{13})</td>
</tr>
<tr>
<td>877076</td>
<td>(2^4)</td>
<td>6597</td>
<td>(2^2,2^7)</td>
<td>530</td>
<td>(2^4,2^4)</td>
</tr>
<tr>
<td>439093</td>
<td>(2^4)</td>
<td>3260</td>
<td>(2^2,2^8)</td>
<td>420</td>
<td>(2^4,2^5)</td>
</tr>
<tr>
<td>219774</td>
<td>(2^5)</td>
<td>1595</td>
<td>(2^2,2^9)</td>
<td>209</td>
<td>(2^4,2^6)</td>
</tr>
</tbody>
</table>
Table 7.4: Fields with discriminant $\Delta$ of form $4pq$

We can also use $\Delta$ values of the form $pqr$ where $p, q,$ and $r$ are odd primes that run up to the 200th prime, and $pqr \equiv 3 \pmod{4}$ to make our 2-group have rank 2. We tracked the structure of our 2-class groups as above and our results follow.
### Table 7.5: Fields with discriminant Δ of form $pqr$

<table>
<thead>
<tr>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
<th>No. of Fields</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>211</td>
<td>$(2,2^{11})$</td>
<td>3</td>
<td>$(2^2,2^{12})$</td>
<td>16</td>
<td>$(2^4,2^7)$</td>
</tr>
<tr>
<td>84</td>
<td>$(2,2^{12})$</td>
<td>1</td>
<td>$(2^2,2^{13})$</td>
<td>4</td>
<td>$(2^4,2^8)$</td>
</tr>
<tr>
<td>18</td>
<td>$(2,2^{13})$</td>
<td>1197</td>
<td>$(2^3,2^{3})$</td>
<td>5</td>
<td>$(2^4,2^9)$</td>
</tr>
<tr>
<td>3</td>
<td>$(2^5,2^{5})$</td>
<td>895</td>
<td>$(2^3,2^{4})$</td>
<td>3</td>
<td>$(2^5,2^{6})$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

8. Obtaining the Odd Part of the Class Group

8.1 Estimating the Class Number

The first thing we have to do to find the odd part of the class group is to estimate the class number. The class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ is

$$h(\Delta) = \left\lfloor (2\pi)^{-1} \sqrt{|\Delta|} \right\rfloor \frac{P}{\prod_p \frac{1}{1 - \frac{1}{N(p)}}},$$

and $\Delta$ is the discriminant of $\mathbb{Q}(\sqrt{d})$. The first product is over all primes $p$, and the second product runs over all primes $p | \Delta$.

If $p | \Delta$ then $(p) = p^2$ and $N(p) = p$ where $N(p)$ is the norm of $p$, so the term in $P$ is 1 for these primes. Therefore, primes dividing $\Delta$ will contribute nothing to $h(\Delta)$. Suppose $p$ is an odd prime such that $p \nmid \Delta$, then either $(p) = p_1p_2$ if $(\frac{d}{p}) = +1$, or $(p)$ is a prime ideal if $(\frac{d}{p}) = -1$. In the first case, $N(p_1) = N(p_2) = p$, so the term in $P$ is

$$\frac{1}{(1 - \frac{1}{p})^2} = \frac{1}{(1 - \frac{1}{p})^2}. \quad \text{In the second case, } N(p) = p^2, \text{ so}$$

the term in $P$ is

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

In general, for odd prime $p$, we can write

$$\frac{1}{1 - \frac{1}{p}}$$

for the term determined by $p$. If $2 \nmid \Delta$, then $P$ will either have a factor of $\frac{3}{2}$ if $\Delta \equiv 5 \pmod{8}$, or a factor of 2 if $\Delta \equiv 1 \pmod{8}$ corresponding to the prime 2.

To estimate the class number, we compute the above product over a finite number of primes. We usually use between 4096 and 1048576 primes. In our program, we call our class number estimate $Qa$. As we compute the product for $Qa$, we place all primes less than 500 with $(\frac{d}{p}) = +1$ in a list called $Lpa$. We use $Lpa$ to create a form $(p,B,C)$ for which we’ll check its order. Since the Jacobi symbol for each prime in $Lpa$ is $+1$, we can calculate the square root of $\Delta \pmod{p}$, which we call $B$. If $B$ is even and $\Delta$ is odd, then we let $B = B + p$. We then compute $C = \frac{B^2 + \Delta}{4p}$. Now we want
to determine the order of this form \((p, B, C)\) by using our order function.

In our order function, we divide \(Qa\) by the order of the 2-class group and continue to call the resulting number \(Qa\). We create a interval centered around \(Qa\) such that the length of the interval is \(Baa - Caa\) where \(Caa = (1 - \epsilon)Qa\), \(Baa = (1 + \epsilon)Qa\), and \(\epsilon\) will allow for adjustment. We are using Shanks’ Baby Step Giant Step ([8]) quoted by Cohen ([2]). If we can not find the order of the form using Shank’s Baby Step Giant Step Algorithm, we will either adjust \(\epsilon\) to increase our interval, or recompute \(Qa\) by using more primes in the Euler product to get a better estimate. Shank’s Baby Step Giant Step Algorithm checks strips of the interval of length \(qa = \lceil \sqrt{\frac{Baa - Caa}{2}} \rceil\). If \(qa\) is too big, then our program will overload, so we decrease \(\epsilon\) so \(qa\) will be smaller and more manageable.

### 8.2 Baby Step Giant Step Algorithm

Since we know the structure of our 2-class group, let \(y\) be the highest order of the factors in the 2-class group. Therefore, \(y\) is the highest power of 2 that can divide the order of any form. Given the form \((p, B, C)\), chances are that the order of this form is not odd. So, if we let \(x_1 = (p, B, C)^y\) then \(x_1\) will have odd order. We let \(qa\) be the length of the specific strip we’re checking in the interval of length \(Baa - Caa\), and we compute the ordered list \(X\) containing the values \(x^j_1\) where \(0 \leq j \leq qa\) and \(j + 1\) is the position of that value. We check the list \(X\) to see if any values are equal. If two values in \(X\) are equal, say \(x^a_1 = x^b_1\), then the order of \(x_1\) divides \(a - b\). If two values in \(X\) are not equal, then let \(z = x^{Caa+qa}_1\). Now we check to see if \(z\) and \(z^{-1}\) are in \(X\). If \(z\) is in \(X\), then \(x^{Caa+qa}_1 = x^i_1\) where \(0 \leq i \leq qa\) and hence a multiple of the order of \(x_1\) is in the interval from \(Caa\) to \(Caa + qa\). If \(z^{-1}\) is in \(X\), then \(x^{Caa-qa}_1 = x^i_1\) where \(0 \leq i \leq qa\) and hence a multiple of the order of \(x_1\) is in the interval from \(Caa + qa\) to \(Caa + 2qa\). If we do not find the order of \(x_1\), we update \(z\) to \(z = x^{Caa+3qa}_1\). After each iteration, we let \(z = z_1 * x^{2qa}_1\) where \(z_1\) was the \(z\) value during the previous iteration.

If we check through the whole interval of length \(Baa - Caa\) and \(z\) is not in \(X\), then we either expand our interval by increasing the value of \(\epsilon\) and use the Baby Step Giant Step algorithm again until we find a value in \(X\), we use more primes when computing the Euler product, or we can discard the form and use another form obtained by the multitude of primes in \(Lpa\).
Let \( M = p_1^{c_1} p_2^{c_2} \ldots p_t^{c_t} \) be a multiple of the order of \( x_1 \). To find the order of \( x_1 \), we methodically start raising \( x_1 \) to \( M \) divided by a power of a prime factor to see if the value is the identity. For instance, we start off with \( x_1^{\frac{M}{p_1^{c_1}}} \) and check if this is the identity form. If it is the identity, and \( c_1 > 1 \), then we check to see if \( x_1^{\frac{M}{p_2^{c_2}}} \) is the identity. We keep doing this until \( i = c_1 \) and \( x_1^{\frac{M}{p_i^{c_i}}} \) is the identity, or \( x_1^{\frac{M}{p_i^{c_i}}} \) is not the identity. If \( x_1^{\frac{M}{p_i^{c_i}}} \) is not the identity for some \( i \leq c_1 \) then we replace \( M \) with \( M_1 = p_1^{c_1-i+1} p_2^{c_2} \ldots p_t^{c_t} \). Then we start over using \( M_1 \) as our new \( M \) and the next prime factor instead of \( p_1 \). We will eventually get the order of \( x_1 \). Now we have a completed the order function for \( x_1 \), which has order \( n_1 \).

We divide \( Qa \) by \( n_1 \), and continue to call it \( Qa \). We recompute \( qa \), \( Caa \), and \( Baa \) based on this new \( Qa \). We let \( ea \) be the order of the odd part of the group we have already obtained, since we have only computed one form, \( ea = n_1 = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \). We want to find which, if any, \( p_j \)'s are greater than \( Baa \). If all primes are less than or equal to \( Baa \), then \( j = t + 1 \) and \( dl = 1 \). Otherwise, we let \( j \) be the smallest subscript such that \( p_j > Baa \) and \( dl = p_j^{a_j} \ldots p_t^{a_t} \). We do this because assuming \( Baa \) is accurate, there will not exist any more generating forms with orders divisible by primes in \( dl \).

We also use \( n_1 = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \) to obtain the forms \( x_{1j} = x_1^{n_{1j}} \) for each prime \( p_j \) where \( 1 \leq j \leq t \) and \( n_{1j} = \frac{n_1}{p_j} \). Each form will have order \( p_j^{a_j} \). We place each form \( x_{1j} \) with its corresponding order into a list called \( Gen \). \( Gen \) will be our set of forms that will eventually generate our group.

Now we go back to our \( Lpa \) list and take another prime \( q \) to get the form \( (q,b,c) \) and let \( x = (q,b,c)^{dl} \) where \( y \) is the highest cyclic order of our 2-group. We run \( x \) through our order function to find its order \( n \). We also use \( n = q_1^{b_1} q_2^{b_2} \ldots q_s^{b_s} \) to obtain the forms \( x_k = x^{n_k} \) where \( n_k = \frac{n}{q_k} \) and \( 1 \leq k \leq s \). Each form \( x_k \) will have order \( q_k^{b_k} \). Instead of just appending all forms to \( Gen \) like we did in the first time through, we need to make sure that the forms in \( Gen \) are independent. Therefore, we only append the form \( x_k \) and its order to \( Gen \) if there is no form in \( Gen \) with order a power of \( q_k \). Otherwise, we let \( p = q_k \) and create a list \( Genp \) consisting of all the forms currently in \( Gen \) that have order a power of \( p \) together with its order. Then we let \( nfp = x_k \).
8.3 Finding Independent Forms

If Genp is not empty, then we call the function NewGenp which sorts Genp by the orders of the forms in increasing order and creates two new lists Genpa and Genpb. Genpa will contain all the forms in Genp that have order less than the order of nfp, and Genpb will contain all the forms with orders greater than or equal to the order of nfp. These two lists will be sorted by increasing order.

If Genpb is empty, then we append nfp and its order to Genpb, otherwise, we append it with its order to the last position of Genpa. We then reverse the arrangement of Genpa. If there is only one form in Genpb, we call the form g10, and we call the first form in Genpa, f10. We use the function testgp1 on f10 and g10. If f10 has smaller order than g10, then we raise g10 to a power to make its resulting order equal to the order of f10 and continue to call this form g10. Now we send g10, f10, and their equal order ddd to the function binaq, which determines the intersection of the two cyclic groups generated by each form using the Baby Step Giant Step Algorithm.

In the Baby Step Giant Step Algorithm, we let qa = ⌊√ddd⌋ and we compute the set X = {g100, g101, ..., g10qa}. We let z = f10 and and check to see if z or z−1 is in X. If neither are in X, then we update z by multiplying it by g10−qa, so we check if z = g10−qa f10 and z−1 are in X. The next time and subsequent times thereafter, we multiply g10−2qa to z. We multiply g10−2qa to z, ⌊qa/2⌋ times. If f10 is a power of g10, then we return that exponent as well as true to testgp1. If f10 is never a power of g10, then we return false to testgp1. If testgp1 receives a false, then we need to check if a power of f10 is in the subgroup generated by g10. Suppose p|ddd, then let g11 = g10p and f11 = f10p. We send g11 and f11 with order ddd/p to binaq and we go through binaq again. If f11 is a power of g11 then we stop and retain that power. If not we return to testgp1 and update g11 and f11 by another power of p until the common order becomes ddd/ppe = 1.

Suppose no power of f10 is in the subgroup generated by g10. This means the subgroups generated by f10 and g10 are independent, so we append f10 and its order to the list Genpc. However, suppose a power of f10 is in the cyclic subgroup generated by g10, i.e. f10kp g10−kjp = g10jp where k = ±1 which has order ppe. We see that (f10 · g10−i−kj)kp = identity which means we append f10 · g10−i−kj and its order ppe to the list Genpc as long as it is not the identity form. Now
we let $f_{10}$ be the second form in the list $Genpa$. We do the same to it as we did to the first element in $Genpa$. We continue through the list $Genpa$ until we do this to all the forms.

Now, if $Genpc$ has forms in it, we reverse the arrangement of $Genpc$ as to have forms of larger order ahead of forms with smaller order. We take the first form in $Genpc$ and place it in $Genpb$. Now we set $Genpa$ equal to $Genpc$ minus the form we just placed in $Genpb$. Hence $|Genpb| \geq 2$.

We know the forms in $Genpb$ are independent, because of $testgp1$, and we want to find out whether the next form in $Genpa$ is independent with forms in $Genpb$, so we can add the independent forms to the list $Genpa$. To check if the forms are independent we use our $testgp2$ function. We start with the first form in $Genpa$ and call it $for$ with order $pqa$. We let $nft = for^{\frac{pqa}{w}}$ where $jo = 1$. So $nft$ has order $p$ and we check to see if it is in $Genpb$ by using our $testgp2$ function. If it is, then we increase $jo$ by 1, so we have $nft = for^{\frac{pqa}{w}}$ with order $p^2$. We continue to check if $nft$ is in $<Genpb>$ until one of two things happen: either we get $for$ itself in $<Genpb>$, or $nft = for^{\frac{pqa}{w}}$ is not in $<Genpb>$ for some $jo \geq 1$. If $for$ is in $<Genpb>$, then we throw $for$ away and start this process over with the second form in $Genpa$. If $nft$ is not in the group generated by $Genpb$ when $nft = for^{\frac{pqa}{w}}$, i.e. $jo = 1$, then we append $for$ to $Genpb$.

Here is how the $testgp2$ function determines if $nft = for^{\frac{pqa}{w}}$ is in the group generated by $Genpb$. We take each form in $Genpb$ and raise it to the power of its order divided by $p^{w}$ so each resulting form will have order $p^{w}$, and we place these forms into a list called $Gent$. We do a coset decomposition with our forms in $Gent$. So suppose there are $k$ forms in our $Gent$ list. Then we take $\lceil \frac{k}{2} \rceil$ of the forms to generate a subgroup, $G1$, and $\lfloor \frac{k}{2} \rfloor$ of the forms to generate a list of coset representatives, $C1$. To generate $G1$ we call the first form in $Gent$, $g_{10}$. We send $g_{10}$ to the function $cgpa$, which computes the cyclic group generated by it and we call this group $G1$. If $\lceil \frac{k}{2} \rceil = 1$, then we move on to generate the coset representatives. However, if $\lceil \frac{k}{2} \rceil > 1$, then we send the next form in $Gent$ to $cgpa$ to generate its cyclic subgroup and call it $G2$. Then we send $G1$ and $G2$ to the function $gptaba$, which crosses the groups $G1$ and $G2$ and continues to call it $G1$. If $\lceil \frac{k}{2} \rceil = 2$, then we move to finding the cosets. If not, then we take the third element of $Gent$ and take it to $cgpa$ and calls its cyclic subgroup $G2$. Then we cross $G1$ with $G2$ and continue to call it $G1$. We repeat until we use $\lceil \frac{k}{2} \rceil$ forms. Now, we take the form in the position $\lceil \frac{k}{2} \rceil + 1$ in $Gent$ and send it to $cgpa$ which computes its cyclic subgroup, and we call it $C1$. If $\lceil \frac{k}{2} \rceil < 4$ then we stop; otherwise we take the
next form in Gent and send it to $c_{gpa}$ and call its cyclic subgroup $C_2$. We then $C_1 = C_1 \times C_2$. We continue to do this until we have done it to $\lfloor \frac{k}{2} \rfloor$ forms.

Now we test to find exactly what form in the group generated by the forms in Gent that $nft$ is equal to. We send $G_1$, $C_1$, and $nft$ to the function $finG$, which does the testing. This function is the analogue to the $binaq$ function. The idea is that given $nft \in < Genpb >$ that $c_1 \cdot nft \in G_1$ which means that $c_1^{-1} \cdot G_1 = nft \cdot G_1$ where $c_1$ is some coset representative in $C_1$. So $finG$ runs through each $c \in C_1$ and checks if $c \cdot nft \in G_1$. If $c \cdot nft \notin G_1$ for all $c \in C_1$ and $jo = 1$, then we append for to $Genpb$ because it’s independent to all forms in $Genpb$. Since $nft$ depends on $jo$, let us rename it $nft[jo]$. Assume $jo \geq 2$ and $c \cdot nft \notin G_1$ for all $c \in C_1$ for some minimum value of $jo > 1$ and $p^{jo} \leq pqa$, then there exists $c_1 \in C_1$ such that $c_1 \cdot nft[jo - 1] \in G_1$. We identify the form in the subgroup $G_1$ by obtaining its position in $G_1$ as well as the identity $c_1$ by obtaining its position in $C_1$. By using the position of the form in $G_1$, we can get the product of the generators with their exponents that compose to this element in $G_1$. Likewise, we get the generators with their exponents that compose to give us $c_1$.

If $\lfloor \frac{k}{2} \rfloor = 1$, then we have one form generating our subgroup $G_1$, call it $f_1$, and we let $exk$ be the exponent such that $c_1 \cdot nft[jo - 1] = f_1^{exk}$. Also, $C_1$ is generated by one form, call it $f_2$ and we let $nno$ be the exponent such that $f_2^{nno} = c_1$. So we have $f_2^{nno} \cdot nft[jo - 1] = f_1^{exk}$. Now let $Genpb = \{g_1, g_2\}$ with respective orders $p^s$ and $p^t$. Let $pqa = p^m$. Then $Gent = \{f_1, f_2\}$ where $f_1 = g_1^{p^s \cdot jo - 1}$ and $f_2 = g_2^{p^t \cdot jo + 1}$, and $nft[jo - 1] = for^{p^m \cdot jo + 1}$. Since $f_2^{nno} \cdot nft[jo - 1] = f_1^{exk}$ then $g_2^{nno(p^t \cdot jo - 1)} \cdot for^{p^m \cdot jo - 1} = g_1^{nno(p^t \cdot jo + 1)}$. Hence we have $g_2^{nno(p^t \cdot jo - 1)} \cdot for^{p^m \cdot jo - 1} g_1^{-exk(p^t \cdot jo + 1)} = identity$ and this means $(g_2^{nno(p^t \cdot m)} \cdot for \cdot g_1^{-exk(p^t \cdot m)})^{p^m \cdot jo - 1} = identity$. Thus, we add the form $g_2^{nno(p^t \cdot m)} \cdot for \cdot g_1^{-exk(p^t \cdot m)}$ to $Genpb$ with its order $p^m \cdot jo + 1$.

Assume $\lfloor \frac{k}{2} \rfloor > 1$, and we have two generators for $G_1$ and one generator for $C_1$. Assume $f_1$ and $f_2$ generate $G_1$ and $f_3$ generates $C_1$. Then this time $exk$ will be a pair or exponents $\{a_1, a_2\}$ such that $c_1 \cdot nft[jo - 1] = f_1^{a_1} f_2^{a_2}$. Here $nno$ will be such that $f_3^{nno} = c_1$. So we have $f_3^{nno} \cdot nft[jo - 1] = f_1^{a_1} f_2^{a_2}$. Now if $Genpb = \{g_1, g_2, g_3\}$ with respective orders $p^s$, $p^t$, and $p^r$, then we have $(g_3^{nno(p^r \cdot m)} \cdot for \cdot g_1^{-a_1(p^s \cdot m)} \cdot g_2^{-a_2(p^t \cdot m)})^{p^m \cdot jo - 1} = identity$. Then we take the form $g_3^{nno(p^r \cdot m)} \cdot for \cdot g_1^{-a_1(p^s \cdot m)} \cdot g_2^{-a_2(p^t \cdot m)}$ and append it with its order to $Genpb$. 27
Now assume $\lceil \frac{k}{2} \rceil > 1$ and we have $f_1$ and $f_2$ generate $G1$ and $f_3$ and $f_4$ generate $C1$. We have never encountered a prime with more than rank 4, so this is our last case to discuss. Then not only will $exk$ be a pair of exponents for $f_1$ and $f_2$, but $nno$ will be a pair of exponents for $f_3$ and $f_4$ where $nno = \{a_3, a_4\}$. So we have $f_3^{a_3}f_4^{a_4}nfj = f_1^{a_1}f_2^{a_2}$. Now suppose $Genpb = \{g_1, g_2, g_3, g_4\}$ with respective orders $p^s, p^l, p^l$, and $p^v$, then we have $(g_3^{a_3(p^r-m)}g_4^{a_4(p^v-m)} for g_1^{-a_1(p^r-m)}g_2^{-a_2(p^v-m)})^{p^m-j_{o}+1} = identity$. Thus we will append the form $g_3^{a_3(p^r-m)}g_4^{a_4(p^v-m)} for g_1^{-a_1(p^r-m)}g_2^{-a_2(p^v-m)}$ to $Genpb$ along with its order.

We take out all the elements that were in the intersection of the $Gen$ set and $Genp$ before we entered the $NewGenp$ function and continue to call this set $Gen$. We then take the union $Gen$ and our new list of generators in $Genpb$, and continue to call it $Gen$. $Gen$ will be an independent set of generating forms for a subgroup of the class group. Now we update $ea$ such that $ea$ is the product of the orders in $Gen$, and we update $dl$ appropriately. We repeat this process until $Qa < 3$, then we should have our set $Gen$ be generators for the class group.

9. Class Groups with 5-rank

Since we can find the generators of our class group, we want to use this knowledge to find imaginary quadratic fields with a large number of generators of the 5-primary part of the class group, the 5-rank of the class group. We computed imaginary quadratic fields with 5-rank of their class groups equal to 4 and lower. We were able to compute these imaginary quadratic fields by using a polynomial, $M(t) \in Z(t)$, which parameterizes a series of complex quadratic fields with class groups having 5-rank $\geq 2$. The polynomial we used, $M(t) = -(t^2 + t + 1)(47t^6 + 21t^5 + 598t^4 + 1561t^3 + 1198t^2 + 261t + 47)$, was constructed by Schoof ([7]) using ideas of finding points on an elliptic curve from Mestre ([5]). The domain of this polynomial is the rational numbers and the range is the absolute discriminant of the field.

Using this polynomial, Schoof computed class groups of 356 complex quadratic fields of which 74 had 5-rank of their class groups equal to 3 and one had 5-rank of their class group equal to 4. We used this polynomial and our programs to compute class groups of 23695 complex quadratic fields of which 4176 had 5-rank of their class groups equal to 3 and 46 had their class groups equal to 4.
In addition to using the polynomial, Schoof also made congruence conditions on his domain that we did not. We took \( t = \frac{p}{q} \in \mathbb{Q} \) where \( \gcd(p, q) = 1 \), and \( 1 \leq p, q \leq 200 \). He included the restriction that \( p \not\equiv 2q, -4q, 4q \pmod{11} \). We found that these conditions were sufficient but not necessary to obtain class groups having 5-rank \( \geq 2 \). Comparing our data against his leads us to believe that the rate of increase in the fields with 5-rank equal to 1 becomes stable for the higher the value of \( M(t) \).

The following table shows the 46 complex quadratic fields with discriminant \( \Delta \) with class group having 5-rank equal to 4. In the table, we denote by \((n_1, n_2, ..., n_t)\) the class group \( \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_t} \).

<table>
<thead>
<tr>
<th>(-\Delta)</th>
<th>( h(\Delta) )</th>
<th>5-part</th>
<th>odd part</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>34754645786142204847</td>
<td>(5,5,125)</td>
<td>(3,49,121)</td>
<td>(2,2,16)</td>
</tr>
<tr>
<td>2</td>
<td>855964398235866239</td>
<td>(5,5,25)</td>
<td>(46867)</td>
<td>(2,2)</td>
</tr>
<tr>
<td>3</td>
<td>13266306529809894687</td>
<td>(5,5,25)</td>
<td>(163627)</td>
<td>(2,2,2)</td>
</tr>
<tr>
<td>4</td>
<td>19766003964268239447</td>
<td>(5,5,25)</td>
<td>(29,1321)</td>
<td>(2,2,2,2,4)</td>
</tr>
<tr>
<td>5</td>
<td>5886868250058139599</td>
<td>(5,5,25)</td>
<td>(19,55697)</td>
<td>(2,4)</td>
</tr>
<tr>
<td>6</td>
<td>63091281862850532919</td>
<td>(5,5,25)</td>
<td>(3,41,49,157)</td>
<td>(2,2)</td>
</tr>
<tr>
<td>7</td>
<td>258559351511807</td>
<td>(5,5,5)</td>
<td>(2957)</td>
<td>(2,4)</td>
</tr>
<tr>
<td>8</td>
<td>482352676182047</td>
<td>(5,5,5)</td>
<td>(2029)</td>
<td>(2,2,2)</td>
</tr>
<tr>
<td>9</td>
<td>9488653101577151</td>
<td>(5,5,5)</td>
<td>(31531)</td>
<td>(2,4)</td>
</tr>
<tr>
<td>10</td>
<td>1161276472794747</td>
<td>(5,5,5)</td>
<td>(27,29)</td>
<td>(2,2,8)</td>
</tr>
<tr>
<td>11</td>
<td>1529308397903039</td>
<td>(5,5,5)</td>
<td>(27,97)</td>
<td>(2,2,8)</td>
</tr>
<tr>
<td>12</td>
<td>32085344603169297</td>
<td>(5,5,5)</td>
<td>(3,11,17,53)</td>
<td>(8)</td>
</tr>
<tr>
<td>13</td>
<td>2998026935972976719</td>
<td>(5,5,5)</td>
<td>(47,4973)</td>
<td>(2,2,4)</td>
</tr>
<tr>
<td>14</td>
<td>64278220486249012799</td>
<td>(5,5,5)</td>
<td>(31,3221)</td>
<td>(2,2,4)</td>
</tr>
<tr>
<td>15</td>
<td>2467715454394303679</td>
<td>(5,5,5)</td>
<td>(7,89,991)</td>
<td>(2,2)</td>
</tr>
<tr>
<td>16</td>
<td>12074074625094255599</td>
<td>(5,5,5)</td>
<td>(47381)</td>
<td>(2,2,32)</td>
</tr>
<tr>
<td>17</td>
<td>335366474574263003679</td>
<td>(5,5,5)</td>
<td>(8089)</td>
<td>(2,4,4,16)</td>
</tr>
<tr>
<td>18</td>
<td>40619701855263629423</td>
<td>(5,5,5)</td>
<td>(23,4327)</td>
<td>(2,2,2,2,8)</td>
</tr>
<tr>
<td>19</td>
<td>75286345336097243327</td>
<td>(5,5,5)</td>
<td>(1581193)</td>
<td>(2,2)</td>
</tr>
<tr>
<td>20</td>
<td>78921242954430809567</td>
<td>(5,5,5)</td>
<td>(3,239,1201)</td>
<td>(2,2,4)</td>
</tr>
<tr>
<td>21</td>
<td>93920213643973848047</td>
<td>(5,5,5)</td>
<td>(3,11,1061)</td>
<td>(2,2,2,2,8)</td>
</tr>
<tr>
<td>(-\Delta)</td>
<td>(h(\Delta))</td>
<td>5-part</td>
<td>odd part</td>
<td>2-part</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>22</td>
<td>106994885997905465007</td>
<td>((5,5,5,5))</td>
<td>((3,11,4913))</td>
<td>((2,2,2,2,2))</td>
</tr>
<tr>
<td>23</td>
<td>125092604835421460447</td>
<td>((5,5,5,5))</td>
<td>((477857))</td>
<td>((2,2,8))</td>
</tr>
<tr>
<td>24</td>
<td>13727242936184920207</td>
<td>((5,5,5,5))</td>
<td>((3,3,98737))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>25</td>
<td>177218331077887002399</td>
<td>((5,5,5,5))</td>
<td>((3,149,2341))</td>
<td>((2,2,2,2))</td>
</tr>
<tr>
<td>26</td>
<td>189377090240627802719</td>
<td>((5,5,5,5))</td>
<td>((4030963))</td>
<td>((2,4))</td>
</tr>
<tr>
<td>27</td>
<td>21262874245802875119</td>
<td>((5,5,5,5))</td>
<td>((179,4547))</td>
<td>((2,2,2,4))</td>
</tr>
<tr>
<td>28</td>
<td>307979756794598661359</td>
<td>((5,5,5,5))</td>
<td>((587,7507))</td>
<td>((2,2))</td>
</tr>
<tr>
<td>29</td>
<td>32586009174984426047</td>
<td>((5,5,5,5))</td>
<td>((121,127))</td>
<td>((2,2,2,4,16))</td>
</tr>
<tr>
<td>30</td>
<td>40756426646922264287</td>
<td>((5,5,5,5))</td>
<td>((3,1013,1361))</td>
<td>((2,2,2))</td>
</tr>
<tr>
<td>31</td>
<td>46572734412535720287</td>
<td>((5,5,5,5))</td>
<td>((3,19,47,677))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>32</td>
<td>683932715949009682127</td>
<td>((5,5,5,5))</td>
<td>((3,7,83,547))</td>
<td>((2,2,2,2,2))</td>
</tr>
<tr>
<td>33</td>
<td>793785073509324696527</td>
<td>((5,5,5,5))</td>
<td>((1044653))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>34</td>
<td>87866505163724699519</td>
<td>((5,5,5,5))</td>
<td>((3,61,649))</td>
<td>((2,2))</td>
</tr>
<tr>
<td>35</td>
<td>112582974933629655167</td>
<td>((5,5,5,5))</td>
<td>((3,3,98737))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>36</td>
<td>13754913943503077039</td>
<td>((5,5,5,5))</td>
<td>((19,77719))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>37</td>
<td>191934558570486405999</td>
<td>((5,5,5,5))</td>
<td>((3,13,4863))</td>
<td>((2,2,2,4))</td>
</tr>
<tr>
<td>38</td>
<td>1932638884475660162319</td>
<td>((5,5,5,5))</td>
<td>((3,53,219))</td>
<td>((2,2,16))</td>
</tr>
<tr>
<td>39</td>
<td>2046235407290223911039</td>
<td>((5,5,5,5))</td>
<td>((7,9,18637))</td>
<td>((2,2,4))</td>
</tr>
<tr>
<td>40</td>
<td>3275800695511409263439</td>
<td>((5,5,5,5))</td>
<td>((67,373,2221))</td>
<td>((2))</td>
</tr>
<tr>
<td>41</td>
<td>4102239650237010450719</td>
<td>((5,5,5,5))</td>
<td>((7,293431))</td>
<td>((2,2,8))</td>
</tr>
<tr>
<td>42</td>
<td>4799151247307129560127</td>
<td>((5,5,5,5))</td>
<td>((113,5483))</td>
<td>((2,2,2,16))</td>
</tr>
<tr>
<td>43</td>
<td>5286012244646379116687</td>
<td>((5,5,5,5))</td>
<td>((283,49871))</td>
<td>((2,4))</td>
</tr>
<tr>
<td>44</td>
<td>788253319254419423887</td>
<td>((5,5,5,5))</td>
<td>((27,61,4013))</td>
<td>((2,2,2))</td>
</tr>
<tr>
<td>45</td>
<td>87273708405297636313887</td>
<td>((5,5,5,5))</td>
<td>((1176191))</td>
<td>((2,2,2,4))</td>
</tr>
<tr>
<td>46</td>
<td>1326112931797995101599</td>
<td>((5,5,5,5))</td>
<td>((2133539))</td>
<td>((2,64))</td>
</tr>
</tbody>
</table>

**Table 9.1:** Summary of results of 46 complex quadratic fields with discriminant \(\Delta\) with class group having 5-rank equal to 4.

The following table shows the 4 complex quadratic fields with discriminant \(\Delta\) with class group having cyclic factors of order \(5^6 = 15625\). In the table, we denote by \((n_1, n_2, ..., n_t)\) the class group.
We also found 41 complex quadratic fields with a cyclic factor equal to $5^5$.

\[
\begin{array}{cccccc}
-\Delta & h(\Delta) & \text{5-part} & \text{odd part} & \text{2-part} \\
1 & 2937871683555287 & 49687500 & (15625) & (3,5,53) & (2,64) \\
2 & 8041127635782567 & 252437500 & (15625) & (7,577) & (2,64) \\
3 & 718828743574221287 & 644625000 & (15625) & (27,191) & (2,64) \\
4 & 13691907671030701367 & 4138468750 & (15625) & (13,61,167) & (2,64) \\
\end{array}
\]

Table 9.2: Summary of results of 4 complex quadratic fields with discriminant $\Delta$ with class group having cyclic factors of order $5^6 = 15625$.

10. Class Groups with 7-Rank

As with the previous section, we wanted to find the structure of imaginary quadratic fields with class groups having 7-rank. Since Schoof ([7]) did not generate a polynomial for 7-rank, we used Mestre’s ideas of finding rational points on elliptic curves to generate a polynomial that would give us discriminants of quadratic fields that would produce class groups having positive 7-rank. ([5])

Lemma 15 Let $D(x, u, v) = 4x^3 + B_2(u, v)x + 2B_4(u, v) + B_6(u, v)$, let $u \equiv 2 \pmod{3}$, and $v \equiv 1 \pmod{3}$. Let a rational number $x$ satisfy the following conditions:

i) For every prime divisor $l$ of $u^3 - 8u^2v + 5uv^2 + v^3$, $x \not\equiv -28u^2 + 20uv + 3v^2 \pmod{l}$

ii) $x$ is an integer modulo 3

Then the field $\mathbb{Q}(\sqrt{D(x, u, v)})$ has a class number divisible by 7. ([5])

In the above Lemma, $B_2(u, v) = u^4 - 6u^3v + 3u^2v^2 + 2uv^3 + v^4$, $B_4(u, v) = uv(u-v)(-10u^5 - 10u^4v + 61u^3v^2 - 81u^2v^3 + 59uv^4 - 10v^5)$, and $B_6(u, v) = uv(u-v)(-4u^9 - 36u^8v + 148u^7v^2 - 280u^6v^3 + 528u^5v^4 - 843u^4v^5 + 727u^3v^6 - 304u^2v^7 + 72uv^8 - 4v^9)$.

We used $u = 5$ and $v = 1$ to generate our elliptic curve $D(x, 5, 1) = 4x^3 - 39x^2 - 1264600x - 269614880$. We find rational values for $x$ and $y$ such that $x \neq y$ but $D(x, 5, 1) = D(y, 5, 1)$ by using the equation $f(x, y) = \frac{D(x, 5, 1) - D(y, 5, 1)}{x-y} = 0$, which is a conic that has a parameterization for $x$ and $y$. We find that $f(-546, -22) = 0$. Now, since we know the point $(-546, -22)$ is on this conic, then we can find the equation of the line connecting $(-546, -22)$ to $(t, 0)$. The slope of this line is $\frac{22}{t+546}$, and hence the equation of the line is $y = -22 + \frac{22(x+546)}{t+546}$. Thus we have parameterized $y$ in terms of $x$ and $t$. Now we substitute this parameterized value of $y$
into \( f(x, y) \). Since \((-546, -22)\) is on this conic, then \((-546, -22)\) is a root of \( f(x, y) \), so we let
\[
g(x, y) = \frac{f(x, y + 546)}{x + 546} = \frac{t^2 (4x - 2311) + ((4456x - 2528342) + 16(77653x - 43154475))}{(t + 546)^2},
\]
which is a polynomial in \( x \) with coefficients in terms of \( t \). To get the parameterization of \( x \), we solve \( g(x, y) = 0 \) for \( x \). This gives us 
\[
x = \frac{-2311t^2 + 2528342t + 690471600}{4t^2 + 4456t + 1242448}.
\]
We take this parameterized \( x \) and plug it into \( D(x, 5, 1) \), which will give us a rational function in terms of \( t \). According to Mestre, we can multiply this rational function by squares without affecting the outcome of our polynomial values.

Hence, to remove the denominator, we multiply our rational function by \((4t^2 + 4456t + 1242448)^4\) to obtain 
\[
M(t) = -(t^2 + 1114t + 310612)(967420592t^6 + 3357431864104t^5 + 4850215147029559t^4 + 3733303907396739212t^3 + 161486079883872478748t^2 + 372194367477864525882560t + 35710426345286513538594560).
\]
We then used this polynomial for 7-ranks just as we did for finding quadratic fields with class group of 5-ranks. We took \( t = \frac{p}{q} \in \mathbb{Q} \) where \( \gcd(p, q) = 1 \), and \(-20 \leq p \leq 20 \) and \( 1 \leq q \leq 10 \).

The following table shows the 9 complex quadratic fields with discriminant \( \Delta \). Two of these fields have class group with 7-rank equal to 3, five of these fields have class group with cyclic factors of order 7 and 49, and two of them have class group with cyclic factors of order 343. In the table, we denote by \((n_1, n_2, ..., n_t)\) the class group \( \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_t} \).

<table>
<thead>
<tr>
<th>(-\Delta)</th>
<th>(h(\Delta))</th>
<th>7-part</th>
<th>odd part</th>
<th>2-part</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>821749413733200545517948803</td>
<td>(7,7,7)</td>
<td>(848373473)</td>
<td>(2,2,2,2)</td>
</tr>
<tr>
<td>2</td>
<td>3026821677925604704792156595</td>
<td>(7,7,7)</td>
<td>(29,257,361,421)</td>
<td>(2,2,2,2)</td>
</tr>
<tr>
<td>3</td>
<td>7058964606286806888680</td>
<td>(7,49)</td>
<td>(25,797,1511)</td>
<td>(2,2,2,4)</td>
</tr>
<tr>
<td>4</td>
<td>775221245437068878781455</td>
<td>(7,49)</td>
<td>(41,47,6583)</td>
<td>(2,2,2)</td>
</tr>
<tr>
<td>5</td>
<td>57459366474487256582887595</td>
<td>(7,49)</td>
<td>(18617,32579)</td>
<td>(2,2,4,4)</td>
</tr>
<tr>
<td>6</td>
<td>35496409204186102856275028</td>
<td>(7,49)</td>
<td>(584562347)</td>
<td>(2,2,2,4)</td>
</tr>
<tr>
<td>7</td>
<td>9404420385523076822860197155</td>
<td>(7,49)</td>
<td>(71,1869567)</td>
<td>(2,2,2,2,2)</td>
</tr>
<tr>
<td>8</td>
<td>4688226294892938551047036068</td>
<td>(7,49)</td>
<td>(37,457,977,1429)</td>
<td>(2,2,2,2,2)</td>
</tr>
<tr>
<td>9</td>
<td>868114009805226589243791913892</td>
<td>(7,49)</td>
<td>(1938761873)</td>
<td>(2,2,4,32)</td>
</tr>
<tr>
<td>10</td>
<td>18614199409085188463889092198120</td>
<td>(7,49)</td>
<td>(5,157,19412893)</td>
<td>(2,2,2,2)</td>
</tr>
<tr>
<td>11</td>
<td>71942195</td>
<td>(243)</td>
<td>(2,2)</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>80430655777257141928205795</td>
<td>(343)</td>
<td>(6011,23087)</td>
<td>(2,2,2,2)</td>
</tr>
</tbody>
</table>

**Table 10.1:** Summary of results of 9 complex quadratic fields with discriminant \( \Delta \) with class group with cyclic factors of order 7.
References


Nicole Renée Miller

Born: February 22, 1979 in Harrisburg, PA

Education:

Virginia Polytechnic Institute and State University  Master of Science in Mathematics  2005

Salisbury University  Bachelor of Science in Mathematics, Minor in French  2001

Professional Development:

Teaching Assistant  Virginia Polytechnic Institute and State University  2003-2005
Elementary Calculus with Trigonometry
Differential Calculus
Integral Calculus

Student Researcher  Salisbury University/National Science Foundation  Summer 2001
Analyzed lab exercises for Abstract Algebra I and II
Designed a computer program to compute the evolution of 2-D Cellular Automata
Examined similarities in the evolution of different initial conditions
Investigated and applied previously completed research

Presenter

NCUR (National Conference of Undergraduate Research)  March 2001
Also published ”Periodicity and Long Term Evolution of 2-D Cellular Automata” in the Proceedings

CUR (Council of Undergraduate Research)  March 2001

SSURC (Salisbury State Undergraduate Research Conference)  April 2001
Also presented ”Evacuation Routes of South Carolina” from the Mathematical Contest in Modeling

MathFest 2001  August 2001

Awards:

Cunningham Fellowship  Virginia Polytechnic Institute and State University  2002-2005

Most Promising Mathematician  Salisbury University  2001