Generalization of Rational Circle Group

Arahat D. Chikkatur

Received September 19, 2023
Accepted January 15, 2024
Electronic access January 31, 2024

In number theory and group theory, class numbers are used to quantify the "closeness" of a quadratic ring to being a unique factorization domain, where a class number of 1 implies unique factorization. Gauss conjectured that the only negative and even discriminants that have a class number of 1 are $\Delta = -4, -8, -12, -16, -28$. This is the simplest example of a class number theorem, which attempts to find all discriminants associated with a given class number. In 1934, Gauss' conjecture was generalized, using complex analysis, to the statement that there exist a finite number of discriminants for a given class number. In this paper, we use the theory of binary quadratic forms to present an alternative and more elementary proof of class number theorems. The paper explores group structures on quadratic curves in $\mathbb{Z}[X,Y]$ over $\mathbb{Q}$. In particular, we define a general elliptical rotational group of rational points on a quadratic curve $C : ax^2 + by^2 = c$, denoted Q_C. This is a natural extension of the well-studied circle group, which is a geometric interpretation of $\mathbb{Z}[i]$ through the rational points on a unit circle. The circle group can also be thought of as a group structure on the set of all Pythagorean triples. The general elliptical group is then used to show that the irreducible elements in Q_C relate to irreducible numbers in $\mathbb{Z}[\sqrt{D}]$. Two elementary proofs for the class number theorem for $h = 1, 2$ are presented, which can then be generalized to all discriminants of the form $\Delta = 2^n$. These proofs are used to classify the irreducible elements of Q_C for curves that use quadratic forms with the given discriminant.

Keywords: Rational Points, Quadratic Curves, Group Structures, Class numbers, Quadratic Forms

Introduction

In this paper, we will explore the condition for the existence of rational points curves of the form $ax^2 + bxy + cy^2 = d$, where $a, b, c, d \in \mathbb{Z}$ and the group structures that they create. We will also explore the group structures of quadratic forms $Q \in \mathbb{Z}[x,y]$, namely the class group $CG(\Delta)$, using the principal forms with discriminant Δ. Finally, we use the group structures of the rational points on quadratic curves to solve class number theorems using an elementary approach, which are solutions to the equation $|CG(\Delta)| = k$ for some $k \in \mathbb{N}$.

According to Shanks, Gauss conjectured that the only discriminants of the form $-4k$ such that $|CG(-4k)| = 1$ are $\Delta = -4, -8, -12, -16, -28$ [1,2]. This corresponds to the forms $x^2 + y^2, x^2 + 2y^2, x^2 + 3y^2, x^2 + 4y^2$ and $x^2 + 7y^2$ respectively. A more general conjecture pertaining to all negative discriminants was proven over 170 years later by Kurt Heegner, which was related refined by Harold Stark [3,4].

In 1934, Heilbronn and Linfoot showed that the number of solutions to $|CG(\Delta)| = k$ is always finite for any $k \in \mathbb{N}$ when Δ is negative, although this is still an open problem for positive Δ. However, the machinery used by Heilbronn and Linfoot involves complex analysis and elliptical forms [5].

In this paper, we will use the group structures defined in the below sections to give a more elementary version of the proof for $k = 1, 2$, which also has implications for the group structures on the rational points on ellipses.

A natural generalization of this simpler approach examines the rational points on different forms Q of varying degrees and finds a group structure on a manifold that has a similar connection, similar to the connection seen for Lie Groups [6]. An example of such a proposed connection would be between quadratic forms of three variables and quadric surfaces.

Definitions and Representations

A quadratic form is any polynomial $Q \in \mathbb{R}[X_1, X_2, \ldots, X_n]$, where $\mathbb{R}$ is an arbitrary ring. This can be written as

$$Q = \sum_{i \leq j} a_{ij} X_i X_j$$

where $a_{ij} \in \mathbb{R}$ and $1 \leq i \leq j \leq n$. For example, the polynomial $x^2 + y^2$ is a quadratic form in $\mathbb{Z}[x,y]$. Another representation of quadratic forms is the matrix form, given as

$$Q = \mathbf{x}^T \mathbf{A} \mathbf{x}$$

where $\mathbf{x} = ((X_1 \,|\, X_2) \,|\, (\ldots \,|\, X_n))$ and $\mathbf{A}$ is an $n \times n$ symmetric matrix defined by

$$A_{ij} = A_{ji} = \frac{1}{2} a_{ij} \quad \text{when} \quad j \neq i \quad \text{and} \quad A_{ii} = a_{ii}$$

For the case of $x^2 + y^2$, the matrix form is $\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. This paper will concern itself with quadratic forms in $\mathbb{Z}[X,Y]$, which are all polynomials of the form $ax^2 + bxy + cy^2$, where $a,b,c \in \mathbb{Z}$. The form $ax^2 + bxy + cy^2$ is also denoted by $[a,b,c]$. In this case, the related matrix **A** is simply

$$A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

The discriminant of a quadratic form Δ is $b^2 - 4ac = 4\det(\mathbf{A})$. As the form $Q = ax^2 + bxy = cy^2$ is also a form in $\mathbb{Q}$, embedding the form Q in $\mathbb{Q}[X,Y]$ leads to rational points in $\mathbb{A}^2(\mathbb{Q})$.

$$a(x + \frac{b}{2a}y)^2 + \left(c - \frac{b^2}{4a^2}\right)y^2 = ax^2 + bxy + cy^2 = d$$

By clearing the denominator to ensure all coefficients are integers, the equation becomes $a'x^2 + b'y^2 = c'$. Since this paper studies rational solutions, letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ transforms the equation into $a'X^2 + b'Y^2 - c'Z^2 = 0$, which is the equivalent integer equation to $a'x^2 + b'y^2 = c$.

Some Conditions on a', b', and c'

This section will show a bijection between the rational solutions to any quadratic curve to one with positive, square-free, and pairwise coprime coefficients exist. If for some curve $C_1 : a'x^2 + b'y^2 = c$, there exists another curve C_2 such that C_1 has a rational point if and only if C_2 has one, this bijection will be denoted as $C_1 \to_{eq} C_2$ for two quadratic curves C_1, C_2.

Lemma 1.2.1. For any quadratic curve C, $C \to_{eq} C_1$, where C_1 has square-free coefficients.

Proof. Assume that the coefficients a', b', c' are not square-free, meaning $a' = m_1^2 s_1$, $b' = m_2^2 s_2$, $c' = m_3^2 s_3$ where s_i is square-free for $i = 1,2,3$. Then

$$C_1 : a'X^2 + b'Y^2 - c'Z^2 = 0$$

is equivalent to

$$C_2 : s_1(m_1X)^2 + s_2(m_2Y)^2 - s_3(m_3Z)^2 = 0.$$

These two curves have a bijective map, as any rational point $(x,y) \in C_1$ has the corresponding rational point $\left(\frac{m_1 x}{m_3}, \frac{m_2 y}{m_3}\right) \in C_2$.

Lemma 1.2.2. For any quadratic curve C, $C \to_{eq} C_2$, where C_2 has pairwise coprime coefficients.

Proof. Without loss of generality, we can assume that $\gcd(a',b',c') = 1$ as if $\gcd(a',b',c') > 1$, then dividing each coefficient by $\gcd(a',b',c')$ ensures $\gcd(a',b',c') = 1$ without changing the curve. Now assume that $\gcd(a',b') = d > 1$. Then, using the equivalent integer equation, we have that $d \mid a'X^2 + b'Y^2$, implying $d \mid c'Z^2$. Since $\gcd(a',b',c') = 1$, $\gcd(c',d) = 1$, meaning $d \mid Z^2$. Furthermore, as every divisor of a square-free integer is square-free, $d \mid Z^2$ implies $d \mid Z$. Letting $Z = dZ'$ and dividing by d, $a'X^2 + b'Y^2 - c'Z^2 = 0$ becomes

$$\frac{a'}{d}X^2 + \frac{b'}{d}Y^2 + c'dZ'^2 = 0.$$

Clearly, these two curves are related through the simple bijective map $(X,Y,Z) \to (X,Y,Z')$. Applying this argument for (b',c') and $(a'c')$ proves the lemma.

Lemma 1.2.3. For any quadratic curve C, $C \to_{eq} C_3$, where $C_3 : a'x^2 + b'y^2 = c'$ such that a', b', and c' are positive.

Proof. If only a' and b' are negative or only c' is negative, the only solution to $a'X^2 + b'Y^2 - c'Z^2 = 0$ is $(0,0,0)$, which produces indeterminate results. If c' and either a' or b' is negative, then making the change of variables $(X,Y,Z) \to (Z,X,Y)$ or $(X,Y,Z) \to (X,Z,Y)$ will make all coefficients positive. Finally, if one or three coefficients are negative, multiplying by -1 reduces it to the cases discussed above.

Using these three lemmas, we have a bijection to the set of quadratic curves with all coefficients to be positive, pairwise co-prime, and square-free.

The Class Group

For any given quadratic form, there is a multitude of forms that have similar properties to it. For example, the forms $5X^2 + 2Y^2$ and $5X^2 + 10XY + 7Y^2$ are equivalent under the substitution $(X,Y) \to (X+Y,Y)$. Note that this change of variables can be represented by the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ since $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}$. In general, a change of variables can be expressed as $P \begin{pmatrix} x \\ y \end{pmatrix}$ for some 2×2 matrix P. Therefore, for a quadratic form that has an associated matrix A, the change of variables is equivalent to the matrix transformation $A \to P^T AP$. For defining the class group, we will be interested in transformations that leave the discriminant unchanged, meaning that $\det(A) = \det(P^T AP)$. This implies that $\det(P) = \pm 1$. However, the rest of the paper will only be concerned with the case where $\det(P) = 1$, or $P \in SL_2(\mathbb{Z})$, which will be made clear from lemmas 1.3.4 and 1.3.8. For the rest of the paper, we will also use the following definitions:

Definition 1.3.1. Two forms Q_1 and Q_2 are said to be properly equivalent if and only if there exists some unique $P \in SL_2(\mathbb{Z})$ that transforms Q_1 to Q_2, denoted $Q_1 \cong Q_2$.

Definition 1.3.2. A number $n \in \mathbb{Z}$ is said to represent a form Q if there exists some $(x_0, y_0) \in \mathbb{Z}^2$ such that $Q(x_0, y_0) = n$. n is said to be a principal representative if $\gcd(x_0, y_0) = 1$.

Lemma 1.3.3. Two equivalent forms represent the same set of numbers.

Proof. By definition, for two forms Q_1 and Q_2 to be equivalent, there exists some $P \in SL_2(\mathbb{Z})$ that encodes the transformation from Q_1 to Q_2. Since $SL_2(\mathbb{Z})$ forms a group, there exists an inverse matrix P^{-1} that encodes the transformation from Q_2 to Q_1. Therefore, if n_1 represents Q_1, then $Q_1(x_0,y_0) = n_1$, meaning $(x_2,y_2) = P^{-1}(x_0,y_0)$ describes the point such that $Q_2(x_2,y_2) = n_1$, meaning for any n_1 that represents Q_1, it also represents Q_2. Similarly, for any n_2 that represents Q_2, it also represents Q_1, which proves the lemma.

We will now define the notion of principal forms, using the following lemma:

Lemma 1.3.4. *n is a principal representative of a form Q if and only if $Q \cong nx^2 + b'xy + cy^2$.*

Proof. By definition, there must exist some $(x_0,y_0) \in \mathbb{Z}^2$ such that $Q(x_0,y_0) = n$. Now consider the matrix $P = \begin{pmatrix} x_0 & y_0 \\ x_1 & y_1 \end{pmatrix}$ such that $x_0y_1 - y_0x_1 = 1$. The existence of (x_1,y_1) is guaranteed since $\gcd(x_0,y_0) = 1$. By making the substitution $x \to Px$ and expanding terms, we get

$$Q' = (ax_0^2 + bx_0y_0 + cy_0^2)x^2 + \cdots = nx^2 + \ldots$$

Similarly, if $Q(x,y) \cong nx^2 + b'xy + cy^2$, then letting $(x,y) = (1,0)$ and using Lemma 1.3.3 proves the lemma.

Theorem 1.3.5. Every form with a negative discriminant is properly equivalent to a form $ax^2 + hxy + cy^2$ such that $0 \le h \le a \le c$.

Proof. Let $Q = a'x^2 + b'xy + c'y^2$ be a form with a negative discriminant. It can be assumed that a' is positive since $b'^2 - 4a'c' < 0 \to a' > 0$. Now let H denote the Hessian matrix, defined by

$$H = \begin{pmatrix} \frac{\partial^2 Q}{\partial x^2} & \frac{\partial^2 Q}{\partial x \partial y} \\ \frac{\partial^2 Q}{\partial x \partial y} & \frac{\partial^2 Q}{\partial y^2} \end{pmatrix}$$

For a quadratic form $\det(H) = -\Delta > 0$, meaning Q has a maximum or minimum. Since $a' > 0$, a minimum of Q exists in $\mathbb{R}^2$. Now let a denote the smallest integer value of Q. From Lemma 1.4.3, $Q \cong ax^2 + hxy + cy^2$ denoted Q^*. Since a is the minimum, $a \le c$ by definition. Since $Q^*(1,-1) = a + c - h \ge c$, we have $h \le a$.

By letting $D = -\Delta$, we have $4ac = h^2 + D$, meaning we can test values of h with the same parity as D. Since $0 \le h \le a \le c$, $4h^2 \le 4ah \le 4ac = h^2 + D$, implying $3h^2 \le D$. Therefore, only values of h satisfying this inequality need to be tested. Any form that meets all these properties is called primitive forms.

Corollary 1.3.6. There are a finite number of primitive discriminants for each negative Δ.

This directly follows from $3h^2 \le D$.

Example 1.3.7. To calculate all primitive forms for $\Delta = -120$, we must have $h^2 \le 40 \to -6 \le h \le 6$, and $h \le a \le c$. Since $ac = \frac{h^2 - \Delta}{4}$, h must be even as well. The following table summarizes the results.

h	ac	(a,c)
0	30	$(1,30)$, $(2,15)$, $(3,10)$, $(5,6)$
± 2	31	$(1,31)$
± 4	34	$(1,34)$, $(2,17)$
± 6	39	$(1,39)$, $(3,13)$

Since we only consider solutions where $h \le a$, the only primitive forms with $\Delta = -120$ are $x^2 + 30y^2$, $2x^2 + 15y^2$, $3x^2 + 10y^2$, and $5x^2 + 6y^2$. For example, by letting $(a,c) = (2,17)$, we see that $2x^2 \pm 4xy + 17y^2 = 2(x \pm y)^2 + 15y^2 \cong 2x^2 + 15y^2$.

The class group, denoted $CG(\Delta)$ is the group of principal forms with a fixed discriminant Δ. The group operation is defined by considering the product $F_1(x_1,y_1)F_2(x_2,y_2)$ where (x_1,y_1) and (x_2,y_2) are independent sets of variables and writing the product as $AX^2 + BXY + CY^2$, where X,Y are linear combinations of $x_1x_2, x_1y_2, y_1x_2, y_1y_2$. See section 6.1 of Long's work for more details on this multiplication[7]. To check whether this operation is well-defined, we use the following lemma:

Lemma 1.3.8. If $Q_1 \cong Q_1^*$ and $Q_2 \cong Q_2^*$, then $Q_1Q_2 \cong Q_1^*Q_2^*$.

Proof: Let $n_1 \in \mathbb{Z}$ be a primitive representative of Q_1 and $n_2 \in \mathbb{Z}$ be a primitive representative of Q_2. Then by definition, n_1n_2 represents Q_1Q_2. By choosing n_1 and n_2 such that n_1n_2 is a primitive representative, $Q_1Q_2 \cong n_1n_2x^2 + bxy + y^2$. From Lemma 1.3.3, n_1 represents Q_1^* and n_2 represents Q_2^*, meaning n_1n_2 represents $Q_1^*Q_2^*$, implying $Q_1^*Q_2^* \cong n_1n_2x^2 + bxy + y^2$, proving the lemma.

Due to the "if and only if" nature of Lemma 1.3.4, the above lemma only works for proper equivalence. If the forms Q_1 and Q_2 were related by a change of variables such that $\det(P) = -1$, the multiplication of quadratic forms would not be well-defined.

Example 1.3.9. To demonstrate the above lemma, consider the forms $Q_1 = x^2 + 30y^2$ and $Q_2 = 2x^2 + 15y^2$. By making the change of variables $(x,y) \to (x+2y,y)$ and $(x,y) \to (x+y,x)$, we see that $Q_1 \cong x^2 + 4xy + 34y^2$ and $Q_2 \cong 2x^2 + 4xy + 17y^2$. To compute the product Q_1Q_2, we see that

$$(x_1^2 + 30y_1^2)(2x_2^2 + 15y_2^2) = 2x_1^2x_2^2 + 15x_1^2y_2^2 + 60y_1^2x_2^2 + 450y_1^2y_2^2$$

$$= 2(x_1x_2 + 15y_1y_2)^2 + 15(x_1y_2 - 2y_1x_2)^2$$

Meaning that $Q_1Q_2 \cong Q_2$. However, by letting $Q_1^* = x^2 + 4xy + 34y^2$, $Q_2^* = 2x^2 + 4xy + 17y^2$, and computing their product gives

$$(x_1^2 + 4x_1y_1 + 34y_1^2)(2x_2^2 + 4x_2y_2 + 17y_2^2)$$

$$= 2(x_1x_2 - 17y_1y_2)^2 + 4(x_1x_2 - 17y_1y_2)(x_1y_2 + 2x_2y_1 + 4y_1y_2)$$

$$+17(x_1y_2 + 2x_2y_1 + 4y_1y_2)^2 \cong 2X^2 + 4XY + 17Y^2$$

Which means that $Q_1^*Q_2^* \cong Q_2^* \cong Q_2$, demonstrating the lemma for this specific case.

Example 1.3.10. For CG(-120), for each form $Q_i \in$ CG(-120), $Q_1Q_i = Q_i$, where $Q_1 = x^2 + 30y^2$, meaning Q_1 is the identity. Furthermore, $Q_i^2 = Q_1$. By letting $Q_1 = 2x^2 + 15y^2$, $Q_4 = x^2 + 120y^2$, every $Q_i \in$ CG(-120) can be described using

only Q_2 and Q_4, meaning $CG(-120) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ through the isomorphism $\phi : Q_2^a Q_4^b \to (a,b)$ for $a,b \in \mathbb{Z}/2\mathbb{Z}$.

In general, since the multiplication of forms is a commutative operation, $CG(-\Delta)$ is Abelian, meaning it can be decomposed into the product of cyclic groups.

Prime representatives

This section will look at the prime representatives of the forms in $CG(\Delta)$ for a fixed Δ, as the prime representatives can be used to find every representative of a given form in $CG(\Delta)$ using. To motivate the study of prime representatives, we first start with a few lemmas:

Lemma 1.4.1. If $n \in \mathbb{N}$ is a primitive representative of a form $Q \in CG(\Delta)$, every divisor of n is represented by another form $Q^* \in CG(-\Delta)$

Proof. From Lemma 1.3.4, if n is represented by Q, then

$$Q \cong nx^2 + bxy + cy^2.$$

Therefore, for any d such that $d|n$, d is represented by $Q^* = dx^2 + bxy + \frac{c}{d}y^2$. Note that $\Delta(Q^*) = b^2 - 4d\frac{c}{d} = b^2 - 4nc = \Delta(Q)$, meaning $Q^* \in CG(\Delta)$.

Lemma 1.4.2. For any prime representing a form $Q \in CG(\Delta)$ that doesn't divide Δ, $(\Delta/p) = 1$, where (Δ/p) is the Legendre symbol.

Proof. Using Lemma 1.4.1, $Q \cong px^2 + bxy + cy^2$ where $\Delta = b^2 - 4pc$. Since $p \nmid \Delta$, $b^2 \not\equiv 0 \pmod{p}$. Since, $\Delta \equiv b^2 \pmod{p}$, $(\Delta/p) = 1$.

Lemma 1.4.3. A reduced form $Q = ax^2 + bxy + cy^2$ has order 2 in $CG(\Delta)$ if and only if $a = c$ or $a = b$

Proof. Let $Q = ax^2 + bxy + cy^2$, $Q^* = ax^2 - bxy + cy^2$ with discriminant $\Delta = b^2 - 4ac$. Then $(a - b + c)(a + b + c) = (a+c)^2 + (4ac - b^2)$ represents $Q_1 Q_2$. Note that this is a primitive representative of the identity element, implying $QQ^* = Q_1$. Therefore, Q has order 2 if and only if $Q \cong Q^*$. Since any transformation taking Q to Q^* must fix the x^2 and y^2 coefficients, the transformation must be of the form $(x,y) \to (x \pm ny, y)$ or $(x,y) \to (-y \pm nx, x)$, where $n \in \mathbb{N}$. However, if $b < a$, the coefficient of xy in $Q = a(x+ny) - b(x+ny)y + cy^2$ is $2an - b > b$, meaning no such transformation can exist. Therefore, the only valid transformation is $(x,y) \to (-y \pm nx, x)$, giving $Q = cx^2 + \ldots$, implying that $a = c$ if $b < a$. This proves the lemma.

These lemmas are the beginning of classifying what primes represent different forms in $CG(\Delta)$. For example, when $\Delta = -40$, $x^2 + 10y^2, 2x^2 + 2xy + 11y^2 \in CG(\Delta)$, so any primes representing these two forms must satisfying

$$\left(\frac{-40}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{5}{p}\right)$$

. To analyze these expressions further, we use the following theorems without proof:

Theorem 1.4.4. Law of Quadratic Reciprocity: For odd primes p, q

$$(p/q)(q/p) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Theorem 1.4.5. $-\frac{1}{p} = (-1)^{p-1/2}$, $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}$

$$\left(-\frac{1}{p}\right) = (-1)^{p-1/2},$$
$$\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}.$$

Therefore, we see that if $p \equiv 1 \pmod 4$, then for any odd prime q,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

If $p \equiv 3 \pmod 4$, this can be used to drastically simplify the expression for (Δ/q) in general. For example,

$$\left(\frac{-40}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{5}{p}\right).$$

Using Theorem 1.5.4, the value of Δ remains constant for representatives of the same form, and $\left(\frac{-2}{p}\right)$ can be easily calculated using Theorem 1.4.5. Hence, only using the coefficients of x^2 and y^2, we can derive what primes represent a given form in $CG(\Delta)$. However, this method can fail to distinguish between forms, most notably the forms $Q = ax^2 + bxy + cy^2$ and $Q^* = ax^2 - bxy + cy^2$. If $\text{ord}(Q) > 2$, then $Q \not\equiv Q^*$, meaning this method works best when $\text{ord}(Q) \leq 2$ for all $Q \in CG(\Delta)$. This is equivalent to $CG(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^m$, for some $m \in \mathbb{N}$. In this case, it becomes possible to distinguish the primitive representatives for all $Q \in CG(\Delta)$ using quadratic residues. Gauss conjectured that there existed 65 such Δ for which this holds. We will explore some Δ such that $CG(\Delta) = (\mathbb{Z}/2\mathbb{Z})^m$ in Section 2.5.

The final piece necessary to find prime representatives is the following theorem:

Theorem 1.4.6. If p and q are odd primes, then $\left(\frac{p}{q}\right) = 1 \implies p \equiv \pm(2\beta + 1)^2 \pmod{4q}$, where β is arbitrary.

Example 1.4.7. To find all prime representatives for the form $5x^2 + 6y^2 \in CG(-120)$, we first write

$$\left(\frac{-120}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{5}\right).$$

Using the coefficients of the quadratic form (5 and 6), we see that $\left(\frac{2}{5}\right) = -1$, $\left(\frac{5}{3}\right) = -1$, $\left(\frac{6}{5}\right) = 1$, meaning that for any prime representative of $5x^2 + 6y^2$, $\left(\frac{2}{p}\right) = -1$, $\left(\frac{p}{3}\right) = -1$, $\left(\frac{p}{5}\right) = 1$. This means $p \equiv 3,5 \pmod 8$, $p \equiv 2 \pmod 3$, $p \equiv 1,4 \pmod 5$, implying $p \equiv 11, 29, 59, 101 \pmod{120}$. Hence,

the primes $11, 29, 59, 101, 131, \ldots$ are prime representatives of $5x^2 + 6y^2$.

1.5 Legendre's Theorem on Quadratic Curves

This section examines Legendre's theorem on quadratic curves, giving the exact conditions for the solvability of an equation of the form $ax^2 + by^2 - cz^2 = 0$, which is given below:

Theorem 1.5.1. The Diophantine equation $aX^2 + bY^2 - cZ^2 = 0$ has a solution $(X,Y,Z) \neq (0,0,0)$ if and only if $bc \equiv r_1^2 \pmod{a}$, $ac \equiv r_2^2 \pmod{b}$, and $ac \equiv r_3^2 \pmod{c}$, and all three coefficients have the same sign.

Proving one direction of this theorem becomes trivial with a few simple lemmas presented below when combined with the results of Section 1.4.

Lemma 1.5.2. X, Y, and Z are pairwise coprime.

Proof. It can be assumed without loss of generality that $\gcd(X,Y,Z) = 1$. If $\gcd(X,Y,Z) > 1$, then the triple

$$\left(\frac{X}{\gcd(X,Y,Z)}, \frac{Y}{\gcd(X,Y,Z)}, \frac{Z}{\gcd(X,Y,Z)}\right)$$

satisfies $ax^2 + by^2 - cz^2$. Now assume that $\gcd(X,Y) > 1$, meaning for some prime p, $p \mid \gcd(X,Y)$. This means $p^2 \mid aX^2 + bY^2$, implying $p^2 \mid cZ^2$. Since c is square-free, $p \mid Z^2 \implies p \mid Z$. This violates the fact that $\gcd(X,Y,Z) = 1$, meaning no such p exists. Therefore, $\gcd(X,Y) = 1$. Repeating this argument for (Y,Z) and (X,Z) gives the desired result.

Lemma 1.5.3. $\gcd(b,Z) = 1$.

Proof. Assume that $\gcd(b,Z) > 1$. Then, there would exist some prime p such that $p \mid \gcd(b,Z)$, implying $p \mid b$ and $p \mid Z$. However, since $cZ^2 - bY^2 = aX^2$, either $p \mid a$ or $p \mid X$. However, if $p \mid a$, then $\gcd(a,b) \geq p > 1$, contradicting Lemma 1.2.2, and if $p \mid X$, then $\gcd(X,Z) \geq p > 1$, contradicting Lemma 1.5.2. This proves the lemma.

A very similar argument is used to show $\gcd(c,X) = 1$. The final lemma we need is from Proposition 6.19 of Allen Hatcher's "Topology of Numbers"[8].

Theorem 1.5.4. For any n that represents a form Q, $\left(\frac{n}{p}\right)$ takes the same value for any odd prime dividing $|\Delta|$, given that $\gcd(n,p) = 1$.

If $aX^2 + bY^2 - cZ^2 = 0$ has a non-trivial solution $(X,Y,Z) \neq (0,0,0)$, then by making the substitution $n = ab$, we see that $X^2 + abY^2 - acZ^2 = 0$, implying that acZ^2 is a representative of $Q = x^2 + aby^2$. Hence, from Lemma 1.4.2, for any $p \mid b$, $\left(\frac{acZ^2}{p}\right)$ must take the same value for any representative. Since 1 represents Q, $\left(\frac{acZ^2}{p}\right) = 1$ for all $p \mid b$, meaning $ac \equiv r_1^2 \pmod{b}$. By making the substitution $X \to X/b$ and $X \to X/c$ and repeating the above procedure, we recover the other two conditions from Legendre's theorem.

From Legendre's theorem, we are able to know when a quadratic curve C has a rational point, which is key to studying the group of rational points on a quadratic curve, explored in the next few sections below.

Group of Rational Points

Parameterization of Rational Points

Assuming that the curve $C : ax^2 + by^2 = c$ has a rational point $\left(\frac{p}{r}, \frac{q}{r}\right)$ (See Section 1.5 for more details), using the natural embedding in the plane to generate every rational point along C. First, construct a line through $\left(\frac{p}{r}, \frac{q}{r}\right)$ with slope m, where $m \in \mathbb{Q}$. The equation for this line is $y - \frac{q}{r} = m\left(x - \frac{p}{r}\right)$ or $y = mx + \frac{q-mp}{r}$. The intersection between this line and C can be found through substitution, as

$$ax^2 + b\left(mx + \frac{q-mp}{r}\right)^2 = c$$

or

$$ax^2r^2 + b(mrx + q - mp)^2 = cr^2.$$

Expanding this out and simplifying it gives

$$r^2\left(a + bm^2\right)x^2 + 2bmr(q-mp)x + b(q-mp)^2.$$

Since the line will always intersect the curve at $x = \frac{p}{r}$, this quadratic must have a factor of $(rx - p)$. Furthermore, as (p,q,r) satisfies $ax^2 + by^2 - cz^2 = 0$, $bq^2 - cr^2 = -ap^2$. Therefore,

$$r^2\left(a + bm^2\right)x^2 + 2bmr(q-mp)x + b(q-mp)^2$$

$$= (rx - p)\left(r\left(a + bm^2\right)x - \left(bpm^2 - 2bqm - ap\right)\right).$$

Meaning either $x = \frac{p}{r}$ or

$$x(m) = \frac{bpm^2 - 2bqm - ap}{r(a + bm^2)}.$$

Using this, the expression for y becomes

$$y(m) = mx + \frac{q-mp}{r} = \frac{-bqm^2 - 2apm + aq}{r(a + bm^2)}.$$

Clearly, if $m \in \mathbb{Q}$, then $x \in \mathbb{Q}$. However, for any rational point P on C, there exists a unique line connecting P to the point $\left(\frac{p}{r}, \frac{q}{r}\right)$ which must have a rational slope, meaning there exists some $m \in \mathbb{Q}$ that generates P. Therefore, the above parameterization generates every rational point on C, denoted $\mathbb{Q}_C$.

Group Action Motivation: The Circle Group

Before moving on to a general quadratic curve, we will first investigate the rational points on the unit circle. First of all, it is clear that all points on a circle form a group with the operation being rotation. The group structure is made more clear through the isomorphism $\phi : \theta \to (\cos(2\pi\theta), \sin(2\pi\theta))$, where $\theta \in \mathbb{R}^+$ mod 1, denoting the group formed by all real numbers $r \in (0,1]$.

Theorem 2.2.1. The rational points of a circle form a group under rotation.

Proof. Consider the rotation matrix,

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

Using the parameterization $P \in (\cos(\theta), \sin(\theta))$, $\theta \in [0, 2\pi)$ to describe each point on the unit circle, given two rational points (r_1, r_2), (r_3, r_4) where $r_n \in \mathbb{Q}$, the rotation operation is equivalent to the following matrix multiplication

$$\begin{bmatrix} r_3 & -r_4 \\ r_4 & r_3 \end{bmatrix} \begin{bmatrix} r_1 & -r_2 \\ r_2 & r_1 \end{bmatrix} = \begin{bmatrix} r_1 r_3 - r_2 r_4 & -r_2 r_3 - r_1 r_4 \\ r_2 r_3 + r_1 r_4 & r_1 r_2 - r_2 r_4 \end{bmatrix}$$

Which suggests the following operation

$$(r_1, r_2) \circ (r_3, r_4) = (r_1 r_3 - r_2 r_4, r_2 r_3 + r_1 r_4)$$

Since the rational points form a subgroup of the entire circle, we only need to show closure and inverses exist. The point $(1,0)$ is the identity as $(r_1, r_2) \circ (1,0) = (r_1, r_2) = (1,0) \circ (r_1, r_2)$ and the inverse element of (r_1, r_2) is given by $(r_1, -r_2)$, as $(r_1, r_2) \circ (r_1, -r_2) = (r_1^2 + r_2^2, 0) = (1,0)$. The operation is also closed since $\mathbb{Q}$ forms a field.

This group action for the unit circle, defined by $x^2 + y^2 = 1$ is the simplest and a very well-studied group. Each rational point on the unit circle corresponds to an integer solution to $x^2 + y^2 - z^2 = 1$. In the next section, we will generalize this to all curves of the form $ax^2 + by^2 = c$ with a rational point.

General Rotational Group of Rational Points

Consider a curve $C : ax^2 + by^2 = c$ with a given rational point $P = \left(\frac{p}{r}, \frac{q}{r}\right)$. P will be defined as the generator of the group of rational points on C, denoted Q_C. From Section 1.2, it can be assumed that a, b, and c are positive, meaning C describes an ellipse. The counterclockwise parameterization of an ellipse is given by $\left(\sqrt{\frac{c}{a}}\cos(\theta), \sqrt{\frac{c}{b}}\sin(\theta)\right)$, for some $\theta \in [0, 2\pi)$. This means for some $\theta_P \in [0, 2\pi)$, $\cos(\theta_P) = \frac{p\sqrt{a}}{r\sqrt{c}}$, $\sin(\theta_P) = \frac{q\sqrt{b}}{r\sqrt{c}}$. From section 2.1, we can pick two additional rational points $R_1 = (r_1, r_2)$, $R_2 = (r_3, r_4)$ on C, meaning that for some θ_{R_1}, $\theta_{R_2} \in [0, 2\pi)$,

$$\cos(\theta_{R_1}) = \frac{r_1\sqrt{a}}{\sqrt{c}}, \quad \sin(\theta_{R_1}) = \frac{r_2\sqrt{b}}{\sqrt{c}}$$
$$\cos(\theta_{R_2}) = \frac{r_3\sqrt{a}}{\sqrt{c}}, \quad \sin(\theta_{R_2}) = \frac{r_4\sqrt{b}}{\sqrt{c}}$$

We now define the action of "rotationally" adding two points (r_1, r_2) and (r_3, r_4) around the axis created by the origin, defined as rotating (r_3, r_4) around C ellipse by the angle between P and (r_1, r_2). This is a generalization of the rotational action of the circle group. By considering the point at the angle $\theta_{R_1} + \theta_{R_2} - \theta_P$, we see that

$$\begin{aligned} \sin(\theta_{R_1} + \theta_{R_2} - \theta_P) &= \sin(\theta_{R_1} + \theta_{R_2})\cos(\theta_P) - \cos(\theta_{R_1} + \theta_{R_2})\sin(\theta_P) \\ &= \left(\frac{r_2\sqrt{b}}{\sqrt{c}}\frac{r_3\sqrt{a}}{\sqrt{c}} + \frac{r_4\sqrt{b}}{\sqrt{c}}\frac{r_1\sqrt{a}}{\sqrt{c}}\right)\frac{p\sqrt{a}}{r\sqrt{c}} \\ &\quad - \left(\frac{r_1\sqrt{a}}{\sqrt{c}}\frac{r_3\sqrt{a}}{\sqrt{c}} - \frac{r_2\sqrt{b}}{\sqrt{c}}\frac{r_4\sqrt{b}}{\sqrt{c}}\right)\frac{q\sqrt{b}}{r\sqrt{c}} \\ &= \sqrt{\frac{b}{c}}\left(\frac{ap(r_2 r_3 + r_4 r_1)}{cr} - \frac{q(ar_1 r_3 - br_2 r_4)}{cr}\right) \end{aligned}$$

Similarly,

$$\begin{aligned} \cos(\theta_{R_1} + \theta_{R_2} - \theta_P) &= \cos(\theta_{R_1} + \theta_{R_2})\cos(\theta_P) + \sin(\theta_{R_1} + \theta_{R_2})\sin(\theta_P) \\ &= \left(\frac{r_1\sqrt{a}}{\sqrt{c}}\frac{r_3\sqrt{a}}{\sqrt{c}} - \frac{r_2\sqrt{b}}{\sqrt{c}}\frac{r_4\sqrt{b}}{\sqrt{c}}\right)\frac{p\sqrt{a}}{r\sqrt{c}} \\ &\quad + \left(\frac{r_2\sqrt{b}}{\sqrt{c}}\frac{r_3\sqrt{a}}{\sqrt{c}} + \frac{r_4\sqrt{b}}{\sqrt{c}}\frac{r_1\sqrt{a}}{\sqrt{c}}\right)\frac{q\sqrt{b}}{r\sqrt{c}} \\ &= \sqrt{\frac{a}{c}}\left(\frac{p(ar_1 r_3 - br_2 r_4) + bq(r_2 r_3 + r_4 r_1)}{cr}\right) \end{aligned}$$

Therefore, we can define the group action as

$$(r_1, r_2) \circ (r_3, r_4) =$$
$$\left(\frac{p(ar_1 r_3 - br_2 r_4) + bq(r_2 r_3 + r_4 r_1)}{cr}, \frac{ap(r_2 r_3 + r_4 r_1) - q(ar_1 r_3 - br_2 r_4)}{cr}\right)$$

The identity is $P = \left(\frac{p}{r}, \frac{q}{r}\right)$, as the point is along the axis of rotation, meaning it adds an angle of zero, leaving the second point unchanged. This can also be verified algebraically. To find an inverse of a rational point (r_1, r_2), consider $(r_1, r_2) \circ (r_3, r_4) = \left(\frac{p}{r}, \frac{q}{r}\right)$ giving two linear equations of two variables, which can be solved. Furthermore, $(r_1, r_2) \circ (r_3, r_4) \in Q_C$ by definition, meaning the rational points on C form a group under the operation $\circ$.

Example 2.3.1. Consider the curve $C : 2x^2 + 3y^2 = 5$ with rational point $P = (1,1)$. Then $p = q = 1$, meaning that the group operation for rotationally adding two points around P becomes

$$(r_1, r_2) \circ (r_3, r_4) =$$
$$\left(\frac{2r_1 r_3 - 3r_2 r_4 + 3(r_2 r_3 + r_1 r_4)}{5}, \frac{2(r_2 r_3 + r_1 r_4) - (2r_1 r_3 - 3r_2 r_4)}{5}\right)$$

From section 2.1, points on C can be parameterized as follows:

$$x(m) = \frac{3m^2 - 6m - 2}{2 + 3m^2}, \quad y(m) = \frac{-3m^2 - 4m + 2}{2 + 3m^2}$$

By letting $m = -1, 2$ in these parameterizations, we get the points $\left(\frac{7}{5}, \frac{3}{5}\right)$ and $\left(\frac{11}{7}, -\frac{1}{7}\right)$ on C. Hence,

$$\left(\frac{7}{5}, \frac{3}{5}\right) \circ \left(\frac{11}{7}, -\frac{1}{7}\right) = \left(\frac{1}{5}(3 \times \frac{26}{35} + \frac{163}{35}), \frac{1}{5}(2 \times \frac{26}{35} - \frac{163}{35})\right)$$

Which is the point $\left(\frac{241}{175}, -\frac{111}{175}\right)$, and is on C as

$$2 \times (241)^2 + 3 \times (-111)^2 = 5 \times 175^2$$

Theorem 2.3.2. For any $c_1, c_2 \in \mathbb{N}$, such that $C_1 : ax^2 + by^2 = c_1$ and $C_2 : ax^2 + by^2 = c_2$ have rational solutions for some fixed $a, b \in \mathbb{N}$, there exists an isomorphism from $\mathbb{Q}_{C_1}$ to $\mathbb{Q}_{C_2}$ irrespective of the generators of the two groups.

To see why this theorem holds true, let the generator of $\mathbb{Q}_{C_1}$ be $P_1 = \left(\frac{p_1}{r_1}, \frac{q_1}{r_1}\right)$ and the generator of $\mathbb{Q}_{C_2}$ be $P_2 = \left(\frac{p_2}{r_2}, \frac{q_2}{r_2}\right)$. For some rational points $(t_1, t_2), (t_3, t_4) \in C$, from the results of section 2.1, there exist some $m_1, m_2 \in \mathbb{Q}$ such that

$$t_1 = \frac{bp_1m_1^2 - 2bq_1m_1 - ap_1}{r_1(a + bm_1)^2}, \quad t_3 = \frac{bp_1m_2^2 - 2bq_1m_2 - ap_1}{r_1(a + bm_2)^2}$$

$$t_2 = \frac{-bq_1m_1^2 - 2bp_1m_1 + aq_1}{r_1(a + bm_1)^2}, \quad t_4 = \frac{-bq_1m_2^2 - 2bp_1m_2 + aq_1}{r_1(a + bm_2)^2}$$

Plugging these expressions into the group operation gives an extremely cumbersome algebraic expression, though the most important observation is that neither the definition of t_i or group operation depend on c_1, meaning that an isomorphism can be defined by "swapping" p_1 with p_2, q_1 with q_2, and r_1 with r_2 in both the parameterizations of t_i and the group operation. Since the parameterizations of t_i are unique, the resulting mapping from points on C_1 to C_2.

Group Structures of $\mathbb{Q}_C$

For any rational points $(r_1, r_2), (r_3, r_4)$ on a quadratic curve C, there exists some $m_1, m_2 \in \mathbb{Q}$ that parameterize the points $(r_1, r_2), (r_3, r_4)$. Now let $m_1 = \frac{A_1}{B_1}$, $m_2 = \frac{A_2}{B_2}$, with $A_i, B_i \in \mathbb{Z}$ such that $\gcd(A_1, B_1) = \gcd(A_2, B_2) = 1$. Then the triple (x_i, y_i, z_i) defined as

$$\left(bpA_i^2 - 2bqA_iB_i - apB_i^2, -bqA_i^2 - 2apA_iB_i + aqB_i^2, r(bA_i^2 + aB_i^2)\right)$$

which satisfies the equation $ax^2 + by^2 - cz^2 = 0$, where $i = 1, 2$. Using the definition of the group operation from section 2.3, we have that $(r_1, r_2) \circ (r_3, r_4)$ corresponds to

$$(x, y, z) = (P_1(A_i, B_i), P_2(A_i, B_i), cr^3(bA_1^2 + aB_1^2)(bA_2^2 + aB_2^2))$$

where P_1, P_2 are degree 4 polynomials. Since there must exist some $M \in \mathbb{Q}$ that can parameterize this point, letting we see that

$$cr^2(bA_1^2 + aB_1^2)(bA_2^2 + aB_2^2) = aB^2 + bA^2.$$

Therefore, the following claim is made:

Claim 2.4.1. A point P is defined to be reducible if it can be expressed as $P_1 \circ P_2$, for some P_1, P. If $M = \pm\frac{A}{B}$, $A, B \in \mathbb{Z}_{\geq 0}$, parameterize P. Then P is reducible if $bA^2 + aB^2 = cr^2(bA_1^2 + aB_1^2)(bA_2^2 + aB_2^2)$ for some $A_i, B_i \in \mathbb{Z}$.

From the discussion above, it seems that the above claim should hold true, but in order to prove rigorously such a claim, we need to examine the structure of $\mathbb{Q}_C$ further. For that, the following theorem is very useful:

Theorem 2.4.2. Let $f_1 = a_1x_1^2 + a_2cy_1^2$, $f_2 = a_2x_2^2 + a_1cy_2^2$ where a_1, a_2 and c are pairwise coprime non-zero integers. Then the product f_1f_2 can be written as $a_1a_2X^2 + cY^2$ in two distinct ways (up to multiplication by -1), where X and Y are integer polynomials of x_1, y_1, x_2, y_2.

Proof. Expanding the product f_1f_2 gives $a_1a_2x_1^2x_2^2 + a_1^2cx_1^2y_2^2 + a_2^2cy_1y_2^2 + a_1a_2c^2y_1^2y_2^2$. Since a_1a_2 and c are coprime, only terms that contain a_1a_2 can form $a_1a_2X^2$. However, if we only choose the term $a_1a_2(x_1x_2)^2$ for $a_1a_2X^2$ (in effect letting $X = x_1x_2$), the remaining three terms can never be of the form cY^2. This is because Y must be of the form $C_1x_1x_2 + C_2x_2y_2 + C_3y_1x_2$, $C_1, C_2, C_3 \in \mathbb{Z}$ meaning

$$Y^2 = a_1^2x_1^2y_2^2 + a_2^2y_1^2x_2^2 + a_1a_2cy_1^2y_2^2.$$

Comparing terms shows that $C_1 = \pm a_1$, $C_2 = \pm a_2$, and $C_3 = \sqrt{a_1a_2c}$. However, since a_1, a_2 and c are non-zero, there will always be extra non-zero terms such as $C_2C_3x_2^2y_1y_2$ which are not present in the expansion of f_1f_2, leading to a contradiction. Therefore, $a_1a_2X^2$ must contain the terms $a_1a_2x_1^2x_2^2$ and $a_1a_2c^2y_1^2y_2^2$, implying $X = C_1x_1x_2 + C_2y_1y_2$. By comparing terms, $C_1 = \pm 1$ and $C_2 = \pm c$. Since we are interested in uniqueness up to multiplication by -1, we can assume that $C_1 = 1$ and $C_2 = \pm c$, meaning

$$a_1a_2X^2 = a_1a_2x_1^2x_2^2 + a_1a_2c^2y_1^2y_2^2 \pm 2a_1a_2cx_1y_1x_2y_2.$$

This implies that

$$Y^2 = a_1^2x_1^2y_2^2 + a_2^2y_1^2x_2^2 \pm 2a_1a_2x_1y_1x_2y_2,$$

meaning

$$Y = a_1x_1y_2 \mp a_2y_1x_2.$$

Therefore, $(X, Y) = (x_1x_2 - cy_1y_2, a_1x_1y_2 + a_2y_1x_2)$ or $(x_1x_2 + cy_1y_2, a_1x_1y_2 - a_2y_1x_2)$.

Corollary 2.4.3.

$$(ax_1^2 + a_2y_1^2)(a_1x_2^2 + a_2y_2^2)(a_1x_3^2 + a_2y_3^2)$$

This can be shown by applying the theorem twice.

As an example, consider $f_1 = 6x^2 + 21y^2$ and $f_2 = 7x^2 + 18y^2$. Equating coefficients, we see that $a_1 = 6$, $a_2 = 7$, $c = 3$. Theorem 2.4.2 then states that

$$(6x_1^2 + 21y_1^2)(7x_2^2 + 18y_2^2) = 42X^2 + 3Y^2,$$

where $X = x_1x_2 - 3y_1y_2$, $Y = 6x_1y_2 + 7x_2y_1$ or $X = x_1x_2 + 3y_1y_2$, $Y = 6x_1y_2 - 7x_2y_1$.

Theorem 2.4.2 is a special case of a more general form of the statement, which includes a bxy term in both f_1 and f_2, the proof of which is contained in Proposition 7.5 of Allen Hatcher's "Topology of Numbers". This will be referred to as the generalized version of Theorem 2.4.1. The following lemma using generalized Theorem 2.4.1 is constructed:

Lemma 2.4.4. If the discriminant of Q is even for $Q = ax^2 + bxy + cy^2$ where $\gcd(a,c) = 1$, $Q^2 \cong x^2 - \frac{\Delta}{4}y^2$.

Proof. Using the generalized Theorem 2.4.1, $Q^2 \cong X^2 + bXY + acY^2$. Since $\Delta = b^2 - 4ac$ is even, b^2 must be even implying b is even. Next, we use the substitution $X \to X + \frac{b}{2}$, $Y \to Y$, which is equivalent to the matrix $P = \begin{bmatrix} 1 & \frac{b}{2} \\ 0 & 1 \end{bmatrix}$. Note that $\det(P) = 1$, meaning that

$$Q^2 \cong X^2 + \left(-\frac{b^2}{4} + ac\right)y^2 = X^2 - \frac{\Delta}{4}Y^2.$$

To make use of the theory of quadratic forms introduced in section 1.4, we will need the following definition of a reducible representative of a quadratic form Q and a theorem relating Q_C and the quadratic forms.

Definition 2.4.5. A primitive representative of the quadratic form Q_n is said to be reducible if n is the product of two or more primitive representatives of Q.

Theorem 2.4.6. Let C be a curve of the form $C : ax^2 + by^2 = c$, where a,b,c are positive. A point $P \in Q_C$ parameterized by $m = A/B$ where $\gcd(A,B) = 1$ is irreducible if and only if $n = aB^2 + bA^2$ is an irreducible representative of the quadratic form $Q = aX^2 + bY^2$.

Proof. By using the principle of contraposition, the theorem statement is equivalent to proving a point P is reducible if and only if $n = aB^2 + bA^2$ is reducible. By definition, if a point P is reducible, then $aB^2 + bA^2$ is the product of (at least) 3 principle representatives. Now if $aB^2 + bA^2$ is reducible, and Q is not the identity in $CG(-4ab)$, then using Corollary 2.4.3, $aB^2 + bA^2 = (ax_1^2 + by_1^2)(ax_2^2 + by_2^2)(ax_3^2 + by_3^2)$. From Theorem 2.3.2, there is an isomorphism mapping Q_C generated by P to Q_{C_2}, where C_2 is the curve defined by $ax^2 + by^2 = ax_1^2 + by_1^2$ and Q_{C_2} is generated by the point (x_1, y_1). By letting $m_1 = y_2/x_2$, $m_2 = y_3/x_3$, we see that P_1 generated by m_1 and P_2 generated by m_2 have the property that $P_3 = P_1 \circ P_2$ is generated by $m = A/B$ and is reducible by Claim 2.4.1. If Q is the identity and $n = aB^2 + bA^2$ is a reducible representative, then $Q = x^2 + by^2$. Hence, by letting $C_2 : x^2 + by^2 = 1$, using Theorem 2.3.2 shows $Q_C \cong Q_{C_2}$, where Q_{C_2} is generated by the point $(1,0)$. Since Q is reducible $Q(B,A) = Q(x_1,y_1)Q(x_2,y_2)$, where $x_1,x_2,y_1,y_2 \in \mathbb{Z}$. Since $Q(B,A) = Q(1,0)Q(x_1,y_1)Q(x_2,y_2)$, we see that the point generated by $m = \frac{A}{B}$ is reducible by Claim 2.4.1.

Using Theorem 2.4.6, the following claim is constructed:

Claim 2.4.7.

For any $m = \frac{A}{B}$ such that $aB^2 + bA^2$ is prime, the point generated by m is an irreducible element of $\mathbb{Q}_C$. It might seem that these are all the irreducible elements, though by considering the form $x^2 + 5y^2$ when $(x,y) = (1,1)$, we see that despite 6 being composite, it is a primitive representative as $x^2 + 5y^2 = 2$ and $x^2 + 5y^2 = 3$ have no solutions. In fact, these two primes represent the other primitive form in $CG(-20)$, namely $2x^2 + 2xy + 3y^2$. However, Claim 2.4.7 can be made stronger when $|CG(\Delta)| = 1$, using the following theorem:

Theorem 2.4.8. If $|CG(-4ab)| = 1$, the collection of points parameterized by m such that $aB^2 + bA^2$ is prime describes all irreducible elements of $\mathbb{Q}_C$.

Proof. Assume that for some $m \in \mathbb{Q}$, $aB^2 + bA^2$ factors into d_1d_2, where $d_1, d_2 > 1$. From Lemma 2.4.8, both d_1 and d_2 must be represented by a form in $|CG(-4ab)|$, but since there is only one form in $CG(-4ab)$, d_1, d_2 must be represented by $aX^2 + bY^2$. Therefore, $aB^2 + bA^2$ is a reducible representative.

Theorem 2.4.9. Let P_k^* be the set of primes represented by a form $Q_k \in CG(\Delta)$. If $|CG(-4ab)| = 2$ and if $Q_1 = aX^2 + bY^2$ is the identity, the collection of points generated by $m = \frac{A}{B}$ such that $Q_1(B,A) = p_1$ or $Q_1(B,A) = p_2q_2$, where $p_1 \in P_1^*$ and $p_2, q_2 \in P_2^*$, describe all irreducible elements of $\mathbb{Q}_C$. If $Q_2 = aX^2 + bY^2$ is not the identity, then the collection of points generated by $m = \frac{A}{B}$ such that $Q_2(B,A) = n_1p_2$ where

$$n_1 = \prod_{p \in P_1^*} p, \quad p_2 \in P_2^*$$

describes all irreducible points.

Proof. Using Claim 2.4.7, if $aB^2 + bA^2$ is prime, then it is a primitive representative. If $aB^2 + bA^2$ is not prime, then from Lemma 2.4.8, every divisor of $aB^2 + bA^2$ is represented by Q_1 or Q_2. Now, if $aX^2 + bY^2 = Q_1$ is the identity in $CG(-4ab)$ and there exists some $d < Q_1(B,A)$, $d|Q_1(B,A)$ that represents Q_1, then by definition $\frac{Q_1(B,A)}{d}$ is a primitive representative of Q_1, meaning that $Q_1(B,A)$ is reducible. Therefore, either $Q_1(B,A)$ is prime or all divisors of $Q_1(B,A)$ are represented by Q_2 (except 1). However, if $Q_1(B,A)$ has more than three factors d_1, d_2, d_3 that represent Q_2, then by considering the divisor pair d_1d_2, $\frac{Q_1(B,A)}{d_1d_2}$, both numbers are representatives of Q_1, meaning $Q_1(B,A)$ is reducible.

If $aX^2 + bY^2 = Q_2$ is not the identity, using Lemma 2.4.8 again shows that every divisor of $Q_2(B,A)$ is represented by Q_2 or Q_1. By applying Theorem 2.4.1, if $Q_2(B,A)$ contains three prime divisors that all represent Q_2, then $Q_2(B,A)$ is reducible. Furthermore, if $Q_2(B,A)$ contains two prime divisors, p_1, p_2 that represent Q_2, then p_1p_2 represents Q_1. Hence, $\frac{Q_2(B,A)}{p_1p_2}$ represents Q_2, meaning $Q_2(B,A)$ is reducible. Therefore, Q_2 can only contain one prime divisor representing Q_2, which is equivalent to the theorem statement.

Class Number Problem

This section will give an elementary proof for a special case of the class number problem, which looks for the solutions to $|CG(\Delta)| = k$ for a given $k \in \mathbb{N}$ and $\Delta \in \mathbb{Z}^-$, for which Linfoot and Heilbronn showed there existed finitely many of $\frac{1}{2}$. Only $k = 1,2$ and even Δ will be considered in our case, as outlined in the introduction. Before moving on to the proof, the concept of "multiple identities" will be introduced, which is central to defining the class group and hence solving class number problems. This will expand upon Sections 1.3 and 1.4, and give some of the special cases for which $CG(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^m$ for $m = 0$ and 1. As discussed in Section 1.4, forms in these class groups have prime representatives that are rather easy to compute, giving us a way to compute the irreducible elements of Q_C for where C is defined as the curve $Q(x,y) = c, Q \in CG(\Delta)$.

Consider the forms for which $\Delta = -28$. Using the method shown in Example 1.4.6, the possible forms are $Q_1 : x^2 + 7y^2$, $Q_2 : 2x^2 - 2xy + 4y^2$, $Q_3 : 2x^2 + 2xy + 4y^2$. By using the generalized version of Theorem 2.4.2 and Lemma 1.4.8, $Q_1Q_1 = Q_1$, $Q_2Q_2 = Q_2$, $Q_3Q_3 = Q_3$, meaning they act like an identity element. This leads to a problem when defining a class group since groups cannot have multiple identities. Instead, the class group is defined only to contain the principal form with discriminant Δ defined below:

Definition 2.5.1. The principal form for a discriminant Δ is defined as $x^2 + \frac{\Delta}{4}y^2$ if $\Delta \equiv 0 \pmod 4$ or $x^2 + xy + \frac{(1-\Delta)}{4}y^2$ if $\Delta \equiv 1 \pmod 4$

Lemma 2.5.2. A reduced form $Q = ax^2 + bxy + cy^2$ is in the principal class group if and only if $\gcd(a,b,c) = 1$

Proof. If $d = \gcd(a,b,c) > 1$, then $Q = dQ'$ where the coefficients of Q' share no common factors. Therefore, for every n that represents Q, $d \mid n$. Note that if $Q \in CG(\Delta)$, then for some $m \in \mathbb{N}$, $Q^m \cong Q_1$ where Q_1 is the principal form. However, $Q^2 = (dQ')(dQ') = dQ'^2$, meaning that every representative of Q^2 is also divisible by d. In general, every representative of Q^m is divisible by d. From Lemma 1.3.3, every representative of Q^m is a representative of Q_1. However, since 1 represents the principal form, 1 must represent Q^m, leading to a contradiction.

Now we are ready to tackle the class number problem for $k = 1$ and even Δ

Lemma 2.5.3. The Diophantine equation $2^m - p^j = 1$ has no solution for $j \geq 2$ and any odd prime p.

Proof. We know that $m \geq 4$ since $2^m > p^j \geq 3^2 = 9$. Therefore, $p^j = 2^m - 1 \equiv 1 \pmod 4$. This means j must be odd since the only quadratic residues mod 4 are 0 and 1. Letting $j = 2k+1$ gives

$$2^m = p^{2k+1} + 1 = (p+1) + \sum_{i=0}^{2k} (-1)^i p^i$$

Therefore, $p+1 = 2^{m_1}$, $\sum_{i=0}^{2k}(-1)^i p^i = 2^{m_2}$ where $m_1 + m_2 = m$. Note that $m_1 \geq 2$ and $m_2 \geq m_1$. Using the fact that $p^{2k} = p^{2k-1} + 1 = (p^2-1)f(p) + 1 = (p+1)F(p) + 1$ and $p + 1 - p^{2k-1} = 1 + p(p^{2k-1} - 1) = 1 + G(p)(p+1)$, where f, F, G are some polynomials in p, we have the following identity:

$$\sum_{i=0}^{2k} (-1)^i p^i = (p+1)H(p) + (2k+1) = 2^{m_1}H(p) + (2k+1)$$

Where $H(p)$ is a polynomial in p. This leads to a contradiction since 2^{m_2} must be odd and a multiple of 4 simultaneously. Therefore, no solutions to this Diophantine equation can exist.

Theorem 2.5.4 The only negative even discriminants such that $|CG(\Delta)| = 1$ are $\Delta = -4, -8, -12, -16, -28$.

Proof. Since Δ is even, we assume that $\Delta \equiv 0 \pmod 4$ since $b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod 4$. Now let $\Delta = -4m, m > 0$. If m contains two or more distinct prime divisors, then by letting $m = d_1 d_2$ where $\gcd(d_1, d_2) = 1$ and $d_1, d_2 > 1$, the form $Q = d_1 x^2 + d_2 y^2 \in CG(\Delta)$ since $Q^2 \equiv x^2 + d_1 d_2 y^2 \pmod \Delta$ using Theorem 2.4.2, which is the principal form. This leads to a contradiction since $CG(\Delta) > 1$. Now if $m = p^j$ for some odd prime p and $j \geq 2$, by letting $m + 1 = 2k \times d$, then $2kx^2 \pm 2xy + dy^2 \in CG(\Delta)$. From Lemma 2.5.2, $d > 1$, this is a reduced form. This implies $|CG(\Delta)| \geq 2$, which again is a contradiction. Hence, the only possibilities are m being an odd prime or $m = 2^j$. If $m = 2^j$, $j \geq 3$ then consider the same construction with $h = \pm 2$. Then, we must have $ac = 2^j + 1$. This always factors into two distinct odd factors unless j is a power of 2, in which case we consider $h = \pm 4$. This is valid since $3h^2 = 48 < 64 \leq -\Delta$. Then $ac = 2^{2j} + 2 = 2(2^{2j-1} + 1)$ which again factors into relatively prime divisor pairs. Hence, $|CG(\Delta)| \geq 2$ in this case. Finally, if m is an odd prime, then let $h = \pm 2$ again, meaning $ac = m + 1$. If $m+1$ is not a power of 2, then $m+1$ can factor into relatively prime divisor pairs. Hence, m must be of the form $m = 2k - 1$. If $k \geq 5$, then by considering $h = 6$ (which is valid since $3h^2 = 108 < 124 \leq 4m$), we have $ac = 2k - 1 + 9 = 2k + 8 = 8(2k - 3 + 1)$. Letting $Q = 8x^2 + 6xy + (2k - 3 + 1)y^2$ and using Lemma 2.4.4 shows that $|CG(\Delta)| \geq 2$, another contradiction.

Summarizing the above, $|CG(\Delta)| = 1$ if $m = 1, 2, 4$ (powers of 2) or $m = 3, 7$ (Mersenne Primes). Below are the calculations for finding primitive forms for the corresponding Δ.

$\Delta = -4$

h	ac	(a,c)
0	1	$(1,1)$

$\Delta = -8$

h	ac	(a,c)
0	2	$(1,2)$

$\Delta = -12$

h	ac	(a,c)
0	3	$(1,3)$
2	4	$(2,2)$

$\Delta = -16$

h	ac	(a,c)
2	4	$(1,4),(2,2)$
± 2	5	–

$\Delta = -28$

h	ac	(a,c)
0	7	$(1,7)$
± 2	8	$(2,4)$

However, from Lemma 2.5.2, the forms $2x^2+2y^2$, $2x^2 \pm 2xy+2y^2$ and $2x^2 \pm 2xy+4y^2$ are not in the principal class group. Hence $|CG(-\Delta)| = 1$ for even Δ if and only if $\Delta = -4,-8,-12,-16,-28$.

Combining Theorem 2.5.3 with Theorem 2.4.8 can give very powerful results, as it can be used to exactly describe every irreducible element of QC if $C : x^2+by^2 = c$, $b = 1,2,3,4,7$, $c \in \mathbb{N}$.

Lemma 2.5.5 For any $m > 58$, there exists no such m such that $\left(\frac{-m}{p}\right) = -1$ for all odd primes $p < \sqrt{m}$.

Proof. We first use the fact that there is always a prime residue less than $6\ln(m)$ [9]. Furthermore, since $m > 58$, we must consider the primes $p = 3,5,7$, which give the following residues: $m \equiv 37,193,253,277,337,373$. Notice that the smallest $m > 58$ is $m = 193$, which means both the primes $p = 11,13$ need to be considered. The smallest solution that satisfies all these constraints is larger than 4620, and we can check that $4620 > 6\ln(4620)$.

Theorem 2.5.6 The only negative even discriminants such that $|CG(\Delta)| = 2$ are $\Delta = -20,-24,-32,-36,-40,-48,-52,-60,-64,-88,-100,-112,-148,-232$.

Proof. Let $\Delta = -4m$ for some $m \in \mathbb{N}$. If m has three distinct prime divisors p_1,p_2,p_3, then $p_1x^2+\frac{m}{p_1}y^2, p_2x^2+\frac{m}{p_2}y^2, p_3x^2+\frac{m}{p_3}y^2 \in CG(\Delta)$ leading to a contradiction. Therefore, m can have up to two distinct prime divisors.

Case 1: $\mathbf{m = p_1^{j_1}p_2^{j_2}}$ with $\mathbf{p_1,p_2}$ odd

Since $p_1^{j_1}x^2+p_1^{j_2}x^2, x^2+my^2 \in CG(\Delta)$, no additional forms can be in $CG(\Delta)$. Therefore, if $m+1$ has an odd divisor $d \geq 1$, then $dx^2+2xy+\frac{(m+1)}{d}y^2 \in CG(\Delta)$, meaning $|CG(\Delta)| > 2$. Therefore, $m+1 = 2k$, $k \in \mathbb{N}$. If $m > 27$, then the forms $8x^2 \pm 6xy+(2k-3+1) \in CG(\Delta)$. These are reduced forms as $3 \times 6^2 < 4m = -\Delta$. Hence $|CG(\Delta)| > 2$, leading to a contradiction. Therefore, the only possibilities are $m = 15,21$ and since $21+1 \neq 2^k$, the only possibility in this case is $m = 15, \Delta = -60$.

Case2 : $\mathbf{m = 2^{j_1}p_1^{j_2}}$, $\mathbf{j_1}$ or $\mathbf{j_2 \geq 2}$

In this case, $2^{j_1}x^2+p_1^{j_2}x^2, x^2+my^2 \in CG(\Delta)$, meaning no additional forms can be in $CG(\Delta)$. Since $m \geq 2 \times 3^2 = 12$, $|h| \leq 4$. Therefore, if $m+4$ has an odd divisor d, then $dx^2+4xy+\frac{(m+4)}{d}y^2 \in CG(\Delta)$, leading to a contradiction. This means $m+4 = 2k_1$, $k_1 \in \mathbb{N}$, implying $j_1 = 2$. From Lemma 2.5.2, $j_2 = 1$, meaning $m = 4p_1$. For $m+4$ to be a power of 2, $p_1 = 2k_2-1$. However, if $p_1 \geq 127$, then $32x^2+12xy+(2k_2-3+1) \in CG(-\Delta)$ and if $p_1 = 31$, then $7x^2 \pm 6xy+19y^2 \in CG(\Delta)$, where $\Delta = 16p_1$. Hence, the only possibilities are $p_1 = 3,7 \rightarrow \Delta = -48,-112$.

Case 3: $\mathbf{m = p^j, j \geq 2}$

In this case, $x^2+p^jy^2 \in CG(\Delta)$. From Lemma 2.5.2, $m+1 = 2kd$, where $d \geq 1$ and odd. However, if $k \geq 2$, then $dx^2 \pm 2xy+2ky^2 \in CG(\Delta)$, as these are distinct forms from Lemma 1.5.3. Hence, $4 \nmid pj+1$, implying either $p \equiv 1 \mod 4$ or j is even. Now if $pj \geq 12$, then if $d_1 | pj+4$, $5 \leq d_1 < pj+4$, then $d_1x^2 \pm 4xy+\frac{(p^j+4)}{d_1} \in CG(\Delta)$, a clear contradiction. Finally, if $pj \geq 27$ and $d_2 | pj+4$, $d_2 \geq 6$, then $d_2x^2 \pm 6xy+\frac{(p^j+9)}{d_2} \in CG(\Delta)$, meaning $pj+9 = d_3 \times 2^k$, where $d_3 = 1,3,5$. If $d_3 = 5$, then $5 | pj+4$, leading to a contradiction. If $d_3 = 3$, then $p = 3$, but clearly the equation $3^j+9 = 3 \times 2^k$ has no solutions for $j \geq 2$. Finally, if $d_3 = 1$ and k is even, then $p^j = (2^{k/2}-3)(2^{k/2}+3)$ implying for some $j_1, j_2 \geq 1$, $p^{j_2}-p^{j_1} = 6$. This is only possible when $p = 3$, which leads to a contradiction. Finally, if k is odd, then $p^j+4 = 2^k-5 \equiv 0 \mod 3$, which is another contradiction. Hence, the only possible values for m are $m = 9,25 \rightarrow \Delta = -36,-100$.

Case 4: $\mathbf{m = 2^j, j \geq 3}$

Since for $\Delta = -4,-8,-16$, $|CG(\Delta)| = 1$, we only consider $j \geq 3$. If $j \geq 4$, $x^2+2jy^2, 4x^2+4xy+(2j-2+1) \in CG(\Delta)$. However, if $2j+1$ is not prime, for any odd d such that $d \mid 2^j+1$ $dx^2 \pm 2xy+\frac{(2^j+1)}{d} \in CG(\Delta)$, leading to a contradiction. Hence, $j = 2k$ for some $k \geq 2$. If $k \geq 3$, then the reduced forms $16x^2+8xy+(2j-4+1) \in CG(\Delta)$, meaning that $j = 4$ is the only possibility when $j \geq 4$. Hence the only possibilities are $m = 8,16 \rightarrow \Delta = -32,-64$.

Case 5: m is a non-Mersenne prime, $\mathbf{m \leq 48}$

Clearly, the form $x^2+my^2 \in CG(\Delta)$. Since m is not a Mersenne prime, $m+1 = 2^k \times d$ where $d > 1$ and odd. If $k \geq 2$, then by lemma 1.5.3, $dx^2 \pm 2xy+2ky^2$ are distinct forms, meaning $|CG(\Delta)| > 2$. Hence $k = 1$. Furthermore, if $d = d_1d_2$, $d_1,d_2 > 1$, then $2d_1x^2 \pm 2xy+d_2y^2 \in CG(\Delta)$, implying $|CG(\Delta)| > 1$. Therefore, $m+1 = 2p$, where p is prime. The only $m \leq 12$ satisfying this condition is $m = 5$. If $m > 12$ and if $m+4 = d_1d_2$, $d_1,d_2 > 1$, then $d_1 > 3$ as that implies $3 | m+1 \rightarrow m = 5$. However, $d_1x^2 \pm 4xy+d_2y^2 \in CG(\Delta)$, meaning $m+4$ must be prime. The only $m \leq 27$ satisfying both conditions is $m = 13$. If $m > 27$ and $m+9 = d_1d_2$, $d_1,d_2 \geq 6$,then $d_1x^2 \pm 6xy+d_2y^2 \in CG(\Delta)$. Assuming $d_1 < d_2$, then $d_1 = 2, d_1 = 3, d_1 = 5$. If $d_1 = 5$, $5 | m+4$, contradicting the primality of $m+4$. If $d_1 = 3$, $3 | m$, another contradiction. Hence $d_1 = 2$, implying either $m+9 = 2p$ for some prime p or $m+9 = 2r$, $r \in \mathbb{N}$. However, for even r, $m = (2^{r/2}-3)(2^{r/2}+3)$ and if r is odd, $m+4 = 2r-5 \equiv 0 \mod 3$. Hence, $(m+9)/2$

must also be prime. The only $m \leq 48$ that satisfies all three conditions is $m = 37$. Hence $m = 5, 13, 37 \rightarrow \Delta = -20, -52, -148$.

Case 6: m is a non-Mersenne prime, m > 48

For each primality condition discussed in Case 5, there are restrictions on the values for m modulo a given prime q. For example, $m+4$ being prime implies that $m \not\equiv 2 \mod 3, m \not\equiv 1 \mod 3, \ldots$. The general primality condition in Case 5 is that $(m+x^2)/2$ is prime for some odd x and $m+x^2$ is prime for even x. This means for any $p < 2x$, $m \not\equiv x^2 \mod p$, where $m \geq 3x^2$. For example, when $m \geq 48$, the conditions are equivalent to $m \equiv 37, 193, 253, 277, 337, 373 \mod 420$. This statement is equivalent to $((-m)/p) = -1$ for all $p \leq \sqrt{4m/3}$, which contradicts Lemma 2.5.5. Hence there are no solutions in this case.

Case 7: m is a Mersenne prime

If m is a Mersenne prime, then for $m = 3, 7$, $|CG(-4m)| = 1$. For $m \geq 127$, $8x^2 \pm 6xy + (2k-3+1)y^2 \in CG(\Delta)$ and when $m = 31$, $7x^2 \pm 4xy + 5y^2 \in CG(\Delta)$, meaning $CG(\Delta) \neq 2$ when m is a Mersenne prime.

Case 8: m = 2p, p is prime

Since $x^2 + 2py^2$, $2x^2 + py^2 \in \mathrm{CG}(\Delta)$, there cannot be any other forms in $\mathrm{CG}(\Delta)$. Therefore, $2p+1$ must also be prime. If $p > 6$ and $2p+4$ has an odd divisor d_1, then $2d_1x^2 \pm 4xy + \frac{(p+2)}{d_1}y^2 \in \mathrm{CG}(\Delta)$, meaning $p+2$ is also a prime. The only $p \leq 13$ that satisfies these two conditions is $p = 11$. If $p > 13$, and if $2p+9$ has some divisor $d_1 \geq 7$, then we have another contradiction. Furthermore, $5|2p+9$ implies $5|2p+4$, leading to a contradiction, and $3|2p+9$ also leads to a contradiction, meaning $2p+9$ must also be prime. There exists no $p < 24$ satisfying all three conditions. If $p > 24$, then $2p+16$ cannot have any odd divisors. If there was some odd divisor d_1, if $d_1 \geq 5$, then $2d_1x^2 \pm 8xy + \frac{(p+8)}{d_1}y^2 \in \mathrm{CG}(\Delta)$ and if $d_1 = 3$, then $3|2p+4$. Hence, $p+8$ must also be prime. Note that the general primality condition is both $p+2x^2$ being prime or $2p+(2x+1)^2$ being prime, where $x \in \mathbb{N}$. This can be transformed into the more general statement $\left(\frac{-2p}{p_2}\right) = -1$ for all $p_2 < \sqrt{p}$ that is prime. However, from lemma 2.5.4, this has no solutions for $p > 29$. It can be checked that $p = 29$ satisfies all four primality conditions, as $29+2 = 31$, $29+8 = 37$, $2 \times 29 + 1 = 59$, $2 \times 29 + 9 = 67$. Hence, the only possibilities are $p = 3, 5, 11, 29 \rightarrow \Delta = -24, -40, -88, -232$.

By combining the results of the above theorem and theorem 2.4.9 with the calculations shown in example 1.4.7, we can calculate the irreducible elements of Q_C, where $C : Q(x,y) = c$, $Q \in \mathrm{CG}(\Delta)$, $c \in \mathbb{N}$ for any Δ listed in the above theorem, given C contains a rational point.

Example 2.5.7. For the irreducible elements of a curve $C : 3x^2 + 5y^2 = c$ where C has a rational point, we first calculate the prime representatives of both forms in $\mathrm{CG}(-60)$. From the results of section 1.5, any $p_1 = x^2 + 15y^2 \rightarrow p_1 \equiv 1, 19, 49, 91 \pmod{120}$ and any $p_2 = 3x^2 + 5y^2 \rightarrow p_2 \equiv 17, 83, 107, 113 \pmod{120}$ along with $p_2 = 3, 5$. Using theorem 2.4.9, irreducible representatives of $3x^2 + 5y^2$ include $57 = 19 \times 3$, and $2363 = 139 \times 17$. Since $Q(2,3) = 57, Q(19,16) = Q(11,20) = 2363$, the points parameterized by $m = 3/2, 16/19, 20/11$ are all irreducible elements of Q_C irrespective of the generator. Note that the listed values for m are also the irreducible elements of any curve defined by $Q(x,y) = c$, where Q is a binary quadratic form with discriminant -60.

Conclusion

In conclusion, by defining the group of rational points on a given quadratic curve $C : ax^2 + by^2 = c$ as

$$(r_1, r_2) \circ (r_3, r_4) = \left(\frac{p(ar_1r_3 - br_2r_4) + bq(r_2r_3 + r_4r_1)}{cr}, \frac{ap(r_2r_3 + r_4r_1) - q(ar_1r_3 - br_2r_4)}{cr} \right)$$

for $(r_1, r_2), (r_3, r_4) \in C$ and $\left(\frac{p}{r}, \frac{q}{r}\right)$ as a generator, we showed there is an explicit connection between the group structure of Q_C and the irreducible elements of a quadratic form Q. Using this connection, we can describe the irreducible elements for quadratic forms Q, such that $|\mathrm{CG}(\Delta_Q)| = 1, 2$ where Δ_Q is the discriminant of the quadratic form Q. Future work could include generalizing the proofs given in Section 2.5 to class numbers that are not of the form 2^n.

Acknowledgements

I would like to thank Ph.D. student Daniel Epelbaum for his mentorship and feedback during the learning, writing, and editing process for this paper. Without his support and inspiration for this paper, it would not have been possible. I would also like to thank Jose Morin of the Lumiere program for his helpful feedback during the writing process, and the Lumiere program in general for their full support. Finally, I thank an anonymous reviewer from the journal for their guidance and feedback, which has strengthened this paper further.

References

1 D. Shanks, *Mathematics of Computation*, **23**, 151–163,.

2 C. Gauss, D. Arithmeticae, Y. U. Press, N. Haven and Conn.

3 K. Heegner, *Mathematische Zeitschrift*, **56**, 227–253,.

4 H. Stark, *Clay Mathematics Proceeding*, **7**, 247– 256,.

5 H. Heilbronn and E. Linfoot, *The Quarterly Journal of Mathematics*, **5**, 293–301,.

6 V. Gorbatsevich, E. Vinberg, L. Groups and L. A. I, *Foundations of Lie Theory Lie Transformation Groups*, **20**, year.

7 L. Long, *Binary quadratic forms*.

8 A. Hatcher, *Topology of numbers*, American Mathematical Society, vol. 145.

9 L. Fjellstedt, *Arkiv f or Matematik*, **3**, 287–291,.