University of Hawai‘i at Mānoa

Submitted in Partial Fulfillment of the Plan B Requirements for the Degree of Master of Arts in Mathematics

Reduction Theory of Binary Quadratic Forms

M.A. Candidate:
Krystin Manguba-Glover

Committee:
Robert Harron, Advisor

July 27, 2018

Contents

Chapter 1

Introduction and Motivation

In this paper we will discuss several properties of binary quadratic forms along with several ways of transforming these forms using both matrix multiplication and a geometric interpretation. Before we define these terms formally, let's first describe some applications.

Binary quadratic forms were largely used in the development of algebraic and elementary number theory. The most famous application of them can be found in Fermat's Two-Squares Theorem which states that every positive prime $p \equiv 1 \pmod 4$ can be written as $p = x^2 + y^2$. They have also been applied to studying and solving Pell's equation, $x^2 - my^2 = 1$, and can be found in Gauss' proof of the quadratic reciprocity law. Now lets formally define some of the basic terminology needed to study these forms.

A *form* of degree n over the ring of integers $\mathbb{Z}$ in k variables is a linear combination of terms $x_1^{e_1} \cdots x_k^{e_k}$ such that $e_1 + \cdots + e_k = n$. A *binary quadratic form (over* $\mathbb{Z}$*)* is a quadratic form in two variables, usually denoted

$$Q(x, y) = Ax^2 + Bxy + Cy^2 \text{ or } Q = (A, B, C)$$

where the coefficients A, B, and C are integers. The *discriminant* of Q is the integer $\Delta(Q) = B^2 - 4AC$. From this definition it is clear that $\Delta \equiv 0, 1 \pmod 4$ and as such can be written as $\Delta = -4k$ or $\Delta = 1 - 4k$ for $k \in \mathbb{Z}$.

We say that an integer n is *represented* by Q if there exists two integers x and y such that $Q(x, y) = n$. If x and y are coprime, we say that n is *represented primitively.* Similarly, we say that a form (A, B, C) is *primitive* if $\gcd(A, B, C) = 1$. To study integers represented by (dA, dB, dC) we can multiply those represented by the form (A, B, C) by the common divisor d. As such, we will only consider primitive forms. A discriminant Δ is called *fundamental* if every form of discriminant Δ is primitive.

Proposition 1 (Lemma 1.8 of Lemmermeyer)**.** *A discriminant Δ is fundamental if and only if*

$$\Delta = \begin{cases} 4k, & k \equiv 2, 3 \pmod 4 \\ k, & k \equiv 1 \pmod 4 \end{cases}$$

for some squarefree integer k.

Proof. We break the proof into two cases: $\Delta \equiv 0 \pmod 4$ and $\Delta \equiv 1 \pmod 4$.

Consider $\Delta \equiv 1 \pmod 4$. Assume Δ is not fundamental, then there exists a binary form (A, B, C) such that $p \mid A, B, C$ for some prime p. This implies $p^2 \mid \Delta$ and hence Δ is not squarefree.

Now assume $\Delta \equiv 1 \pmod 4$ is not squarefree. Then $\Delta = dp^2$ for some prime p. Since $\Delta \equiv 1 \pmod 4$, p must be odd with $p^2 \equiv 1 \pmod 4$ and hence $d \equiv 1 \pmod 4$. We now have that $Q = (p, p, p(\frac{1-d}{4}))$ is a non-primitive quadratic form of discriminant Δ and conclude that Δ is not fundamental. This proves the theorem for $\Delta \equiv 1 \pmod 4$.

If $\Delta \equiv 0 \pmod 4$, let $\Delta = 4k$ and assume k is not squarefree. By assumption we have that there is a prime p such that $p^2 \mid k$. If p is odd with $\Delta = dp^2$ then $d \equiv 0 \pmod 4$ and $Q = (p, 0, -\frac{d}{4}p)$ has discriminant Δ, so Δ is not fundamental. If $p = 2$ then $k \equiv 0 \pmod 4$. Writing $k = 4k'$, we have that $Q = (2, 0, -2k')$ is a quadratic form of discriminant Δ and hence Δ is not fundamental. This shows that if Δ is fundamental then k is squarefree.

Since k is squarefree we know that $k \not\equiv 0 \pmod 4$. If $k \equiv 1 \pmod 4$ then $Q = (2, 2, \frac{1-k}{2})$ has discriminant Δ so Δ is not fundamental which is a contradiction.

For the reverse direction, assume $\Delta \equiv 0 \pmod 4$ is not fundamental. Then there exists a quadratic form $Q = (A, B, C)$ of discriminant Δ with $p \mid A, B, C$ for some prime p. If p is odd then $p^2 | 4k$ implies $p^2 \mid k$ so k is not squarefree. If $p = 2$, writing $(A, B, C) = (2a, 2b, 2c)$ gives $k = b^2 - 4ac$ and hence $k \equiv 0, 1 \pmod 4$. If $k \equiv 0 \pmod 4$ then k is not squarefree and if $k \equiv 1 \pmod 4$ then $k \not\equiv 2, 3 \pmod 4$. This completes the proof. □

To each form (A, B, C) we associate two matrices

$$M(Q) = \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \text{ and } m(Q) = \frac{1}{2}M(Q) = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$$

The following facts are true about $M(Q)$ and $m(Q)$:

(1) $4Q(x, y) = (x, y)M(Q)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$

(2) $Q(x, y) = (x, y)m(Q)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$

(3) $\Delta(Q) = -\det M(Q) = -4 \det m(Q)$

In studying quadratic forms we may find that two forms that represent the exact same set of integers and can be transformed into each other through unimodular matrices; these forms are called *equivalent*.

Example 1. Consider $Q(x, y) = 2x^2 + 2xy + y^2$. Since $2x^2 + 2xy + y^2 = (x + y)^2 + x^2$, we can conclude that the forms $Q = (2, 2, 1)$ and $Q' = (1, 0, 1)$ represent the same integers. In fact we have $Q'(x + y, x) = Q(x, y)$ and $Q(x, y - x) = Q'(x, y)$.

Note, however that sometimes forms that represent the same integers are not equivalent. Further, two forms having the same discriminant does not guarantee equivalence.

To define equivalent forms more formally, recall that the *special linear group* or *modular group* is defined by

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \middle| r, s, t, u \in \mathbb{Z}, ru - st = 1 \right\}$$

Given any matrix $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and its transpose N^T, we can act on the quadratic form (A, B, C) by either computing

$$N^T M(Q) N = \begin{pmatrix} 2(Ar^2 + Brt + Ct^2) & 2(Ars + Ctu) + B(ru + st) \\ 2(Ars + Ctu) + B(ru + st) & 2(As^2 + Bsu + Cu^2) \end{pmatrix}$$

or

$$N^T m(Q)N = \begin{pmatrix} Ar^2 + Brt + Ct^2 & \frac{1}{2}[2(Ars + Ctu) + B(ru + st)] \\ \frac{1}{2}[2(Ars + Ctu) + B(ru + st)] & As^2 + Bsu + Cu^2 \end{pmatrix}$$

to produce $M(Q|_N)$ (respectively $m(Q|_N)$) for a new quadratic form

$$Q|_N = (A', B', C') = (Ar^2 + Brt + Ct^2, 2(Ars + Ctu) + B(ru + st), As^2 + Bsu + Cu^2)$$

Given two matrices N_1 and N_2 we have

$$M(Q|_{N_1N_2}) = (N_1N_2)^T M(Q)(N_1N_2) = (N_2)^T (N_1)^T M(Q)N_1N_2$$

Thus $Q|_{N_1N_2} = (Q|_{N_1})|_{N_2}$. In other words, the action of $SL_2(\mathbb{Z})$ on a quadratic form Q is a right action.

Proposition 2. *If* $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ *then* $Q|_N = Q(rx + sy, tx + uy) = Q\left(\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)\right)$

Proof. Assume $Q'(x, y) = Q|_N(x, y)$, then we have

$$\begin{aligned} Q'(x, y) &= \begin{pmatrix} x & y \end{pmatrix} m(Q') \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} N^T m(Q) N \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix} m(Q) \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} rx + sy & tx + uy \end{pmatrix} m(Q) \begin{pmatrix} rx + sy \\ tx + uy \end{pmatrix} \\ &= Q(rx + sy, tx + uy) \end{aligned}$$

□

We say that two binary quadratic forms Q and Q' are *equivalent*, denoted $Q' \sim Q$, if there exists an $N \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q' = Q|_N$. Since $\mathrm{SL}_2(\mathbb{Z})$ is a group, this defines an equivalence relation on binary quadratic forms. We denote the equivalence class containing the form Q by $[Q]$ and define the *class number* (in the strict sense) to be the number of equivalence classes of primitive binary quadratic forms with fixed discriminant Δ, denoted $h^+(\Delta)$ or simply $h(\Delta)$ for $\Delta < 0$.

Proposition 3 (Proposition 1.1 of Lemmermeyer)**.** *If* $Q = (A, B, C)$ *is a binary quadratic form,* $N \in SL_2(\mathbb{Z})$*, and* $Q' = Q|_N = (A', B', C')$*, then the following are true:*

(i) $\Delta(Q) = \Delta(Q')$

(ii) $gcd(A, B, C) = gcd(A', B', C')$

(iii) Q *and* Q' *represent exactly the same integers. Further they represent exactly the same integers primitively.*

Proof.

(i) We know that $N^T M(Q)N = M(Q')$. Taking the determinants of both sides and using the multiplication property of determinants we have

$$\det N^T \cdot \det M(Q) \cdot \det N = \det M(Q')$$

and hence

$$\det M(Q) = \det M(Q')$$

Using fact (1) about $M(Q)$ we have the desired equality.

(ii) Let $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ then we have

$$\begin{aligned} A' &= Ar^2 + Brt + Ct^2 \\ B' &= 2(Ars + Ctu) + B(ru + st) \\ C' &= As^2 + Bsu + Cu^2 \end{aligned}$$

From the above relationships we know that $\gcd(A, B, C) | \gcd(A', B', C')$. Similarly since $\det N = 1$, N is invertible so we have

$$\begin{aligned} M(Q'|_{N^{-1}}) &= (N^{-1})^T M(Q')N^{-1} \\ &= (N^{-1})^T N^T M(Q)NN^{-1} \\ &= M(Q) \end{aligned}$$

Therefore we also have $\gcd(A', B', C') | \gcd(A, B, C)$.

(iii) Assume $Q(x, y) = n$ and recall that $Q'(x, y) = Q(rx + sy, tx + uy)$ where $(x, y)N^T = (rx + sy, tx + uy)$. Using the fact that $Q = Q'|_{N^{-1}}$ and a slight abuse of notation we have $n = Q(x, y) = Q'((x, y)(N^{-1})^T) = Q'(x', y')$. Since $N \in \mathrm{SL}_2(\mathbb{Z})$ we also have $N^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ which gives that $x', y' \in \mathbb{Z}$. The second claim can be proved by combining (ii) with the first claim.

□

Example 2. Acting on $Q = (A, B, C)$ by the *shift operation* $T_n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ gives

$$Q' = Q|_{T_n} = (A, B + 2An, An^2 + Bn + C)$$

(Note that $C' = Q(n, 1)$) Shifting is often used to reduce B modulo $2A$.
The *flip operation* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ transforms Q into

$$Q' = Q|_S = (C, -B, A)$$

A natural question when studying binary quadratic forms is how can we decide if two forms are equivalent, and if they are, how can we find the matrix that relates the two? Answering this question lead mathematicians to develop a theory known as reduction. It was discovered that the method of reducing a quadratic form depended on the type of integers represented by that form. This leads us to the following definitions.

A binary quadratic form Q is:

- *positive definite* if $Q > 0$ for all $x, y \neq 0$

- *negative definite* if $Q < 0$ for all $x, y \neq 0$
- *positive semi-definite* if $Q \geq 0$ for $x, y \neq 0$
- *negative semi-definite* if $Q \leq 0$ for $x, y \neq 0$
- *indefinite* if Q takes on both positive and negative values.

Proposition 4. *Let $Q = (A, B, C)$ be a binary quadratic form. The the following is true:*

(i) If $\Delta > 0$, then Q is indefinite.

(ii) If $\Delta = 0$, then Q is semi-definite but not definite.

(iii) If $\Delta < 0$, then Q is positive definite with $A, C > 0$ or negative definite with $A, C < 0$.

Proof. To prove some cases we will make use of the identity

$$4AQ(x, y) = (2Ax + Ay)^2 - \Delta y^2.$$

(i) Assume $\Delta > 0$. Then $Q(1, 0) = A$ and $Q(B, -2A) = -A\Delta$ have opposite signs unless $A = 0$. Using symmetry we also have $Q(0, 1) = C$ and $Q(-2C, B) = -C\Delta$ with opposite signs unless $C = 0$. Consider, then, the case that both A and C are 0. Then we have $Q(x, y) = Bxy$ with $Q(1, 1) = B$ and $Q(1, -1) = -B$ of opposite sign.

(ii) Assume $\Delta = 0$ and $A \neq 0$, then the identity above becomes

$$4AQ(x, y) = (2Ax + By)^2$$

Since the right hand side is always positive, we have that A and the non-zero values of Q must always have the same sign. Note that $Q(B, -2A) = -AD = 0$ where $A \neq 0$ so the form is not definite. Now assume $A = 0$, that gives that $\Delta = B^2 = 0$ and hence $B = 0$ so the form is $Q = Cy^2$ whose non-zero values always has the same sign as C. Noting that $Q(x, 0) = 0$ for any x shows that the form is not definite.

(iii) Finally, Assume $\Delta < 0$ then we have

$$4AC = B^2 - \Delta \geq -\Delta > 0$$

which gives that A and C must have the same sign. From the identity we also know that $4AQ(x, y) > 0$ for $(x, y) \neq (0, 0)$ giving that Q and A always have the same sign. Hence if $A, C > 0$ then Q is positive definite and if $A, C < 0$ then Q is negative definite.

□

Joseph-Louis Lagrange proved that for every fixed discriminant, $\Delta \neq 0$, there are finitely many classes of binary quadratic forms with discriminant Δ. He then proposed an algorithm to find a canonical representative for each of these equivalence classes by finding the form with the smallest possible coefficients. This reduction method was widely accepted but only for forms of negative discriminant. When it came to the case of positive discriminants, several different methods of reduction arose with no one agreeing on which method was the best.

The goal of this paper is to give a brief introduction to Lagrange reduction, the reduction theory used for binary forms of negative discriminant and to consolidate the applications and results of three different methods of reduction for positive discriminants: Gauss, Zagier, and Siegel. Finally, we will add a bit to the study of Siegel reduction as it is the reduction theory that is least developed and discuss how the different methods are related. Sections on Lagrange, Gauss, and Zagier reduction primarily are taken from Franz Lemmermeyer's Binary Quadratic Forms [Lem10], sections on Siegel-reduction are primarily taken from C.L. Siegel's Lectures on Quadratic Forms [SR55].

Chapter 2

Lagrange Reduction

Lagrange's development of reduction was motivated by trying to find a canonical representative of each equivalence class by calculating the form in the class with the smallest possible coefficients. He began by minimizing the first coefficient and found that given a binary quadratic form $Q = (A, B, C)$, the form with minimal first coefficient A in the equivalence class [Q] is that one such that $A = n$ where n is the smallest integer represented by Q. Continuing this process of minimizing coefficients, we get the following proposition.

Proposition 5 (Proposition 1.4 of Lemmermeyer)**.** *Every equivalence class of binary quadratic forms contains a form* (A, B, C) *with* $|B| \leq |A| \leq |C|$.

Proof. Let $Q = (A, B, C)$ with minimal $|A|$ and apply the shift operation T_n to reduce B modulo $2A$. Continue this process until you find an equivalent form $Q' = (A, B', C')$ such that $|B'| \leq |A|$. Since $A = n$ is the smallest integer represented by $[Q]$ and $|Q'(0,1)| = |C'|$ we also have $|A| \leq |C'|$. □

A form that satisfies the above inequalities is called *Lagrange-Reduced*. Proposition 5 shows that every form is equivalent to a Lagrange-reduced form. To reduce a given quadratic form $Q = (A, B, C)$ to its corresponding Lagrange-Reduced form we can follow the following process:

(1) If $|B| \leq |A|$ then either Q is already reduced or $|A| > |C|$. If Q is reduced then we are done. Otherwise apply $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to produce $Q' = (C, -B, A) = (A', B', C')$. If $|B'| = |B| \leq |A|$ then $|B'| \leq |A'| < |C'|$ and we are done. Otherwise $|B| > |A'|$ and we proceed to the following steps with $Q = Q'$.

(2) If $|B| > |A|$, choose an n such that $|2An - B| \leq |A| < |B|$ (such n is guaranteed to exist by the division algorithm applied to $\frac{B}{2A}$ with remainder in $[-A, A]$).

(3) Apply the matrix $R_n = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -n \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to produce the form

$$Q' = (A', B', C') = Q|_{R_n} = (An^2 - Bn + C, 2An - B, A)$$

By choice of the n above, we have $|B'| \leq |C'|$ and $|B'| < |B|$.

(4) Continue this process of reducing $|B|$ by applying the necessary R_n. Since $|B|$ cannot decrease indefinitely, we must eventually reach a form $Q'' = (A'', B'', C'')$ where $|B''| \leq |C''|$ and $|B''| \leq |A''|$. If $|A''| \leq |C''|$ then Q'' is Lagrange-reduced. Otherwise, applying a flip we get $Q''|_S = (C'', -B'', A'')$ is Lagrange-reduced.

Proposition 6 (Proposition 1.5 of Lemmermeyer)**.** *The coefficients of a Lagrange-Reduced form* (A, B, C) *satisfy the following inequalities:*

$$|B| \le \sqrt{\frac{-\Delta}{3}}, \qquad |A| \le \sqrt{\frac{-\Delta}{3}}, \qquad |C| \le \frac{1-\Delta}{4}, \qquad \text{if } \Delta < 0, \text{ and}$$
$$|B| \le \sqrt{\frac{\Delta}{5}}, \qquad |A| \le \frac{\sqrt{\Delta}}{2}, \qquad |C| \le \frac{\Delta}{4}, \qquad \text{if } \Delta > 0$$

Proof. We will split the proof into two cases. First assume that $Q = (A, B, C)$ is a form with discriminant $\Delta = B^2 - 4AC < 0$. $\Delta < 0$ implies $AC > 0$ and since Q is Lagrange-reduced we have

$$-\Delta = 4AC - B^2 \ge 4A^2 - A^2 = 3A^2$$

which immediately gives

$$|B| \le |A| \le \sqrt{\frac{-\Delta}{3}}$$

To get the last inequality we need to do some algebraic manipulations.

$$|C| = \frac{4|AC|}{4|A|} = \frac{4AC}{4|A|} = \frac{B^2 - (B^2 - 4AC)}{4|A|} = \frac{B^2}{4|A|} - \frac{\Delta}{4|A|}$$

Using the fact that Q is Lagrange-reduced we have

$$|C| \le \frac{A^2}{4|A|} - \frac{\Delta}{4|A|} = \frac{|A|}{4} - \frac{\Delta}{4|A|}.$$

Since $A \ne 0$, there are two cases to consider:

$$1 \le A \le \sqrt{\frac{-\Delta}{3}} \text{ or } \sqrt{\frac{-\Delta}{3}} \le A \le -1$$

If $A \ge 1$ then the inequality becomes

$$|C| \le \frac{A^2 - \Delta}{4A}$$

The right hand side is decreasing as a function of A on the interval $[1, \sqrt{-\Delta}]$ and thus the maximum must be attained at $A = 1$. Similarly, if $|A| \le -1$ we have

$$|C| \le \frac{-A^2 + \Delta}{4A}$$

where the right hand side is an increasing function of A on the interval $[-\sqrt{-\Delta}, -1]$ and hence the maximum must be attained at $A = -1$. Putting these together we have that the maximum occurs at $|A| = 1$ and hence

$$|C| \le \frac{1}{4} - \frac{\Delta}{4} = \frac{1-\Delta}{4}$$

as needed.

Now assume that $Q = (A, B, C)$ has discriminant $\Delta = B^2 - 4AC > 0$. Since Q is Lagrange-reduced we have $B^2 \leq |AC|$ and since $B^2 - 4AC > 0$ we also have $B^2 > 4AC$. This shows that $AC < 0$. Using these facts we have

$$5B^2 = B^2 + 4B^2 \leq B^2 + 4|AC| = \Delta$$

which gives the needed inequality for $|B|$. Now, using the fact that $B^2 \geq 0$ and Q is Lagrange-reduced we have

$$\Delta = B^2 + 4|AC| \geq 4A^2$$

Giving the desired condition for A. Lastly we have

$$4|C| \leq 4|AC| = \Delta - B^2 \leq \Delta$$

isolating C finishes the proof. □

This proposition not only proves that there are only finitely many equivalence classes for fixed discriminant Δ, but it also allows us to compute all Lagrange-reduced forms will small discriminant.

Δ	Lagrange-Reduced Forms
21	$(1, \pm1, -5), (-1, \pm1, 5)$
20	$(1, 0, -5), (-1, 0, 5), (2, \pm2, -2)$
17	$(1, \pm1, -4), (-1, \pm1, 4), (\pm2, 1 \mp 2), (\pm2, -1, \mp2)$
13	$(1, \pm1, -3), (-1, \pm1, 3)$
12	$(1, 0, -3), (-1, 0, 3)$
8	$(1, 0, -2), (-1, 0, 2)$
5	$(1, \pm1, -1), (-1, \pm1, 1)$
−3	$(1, \pm1, 1)$
−4	$(1, 0, 1)$
−7	$(1, \pm1, 2)$
−8	$(1, 0, 2)$
−11	$(1, \pm1, 3)$
−12	$(1, 0, 3), (2, \pm2, 2)$
−15	$(1, \pm1, 4), (2, \pm1, 2)$
−16	$(1, 0, 4), (2, 0, 2)$

Table 2.1: Lagrange-reduced forms with $-16 \leq \Delta \leq 21$, Δ fundamental

1 Reduction of Positive Definite Forms

The reduction theory of primitive forms of negative discriminant is simpler than that of those with positive discriminant. In fact, by using Lagrange-reduction for positive definite forms, we only need a slight adjustment to ensure that there is exactly one reduced form in each equivalence class of quadratic forms. As such, positive definite binary quadratic forms have been much developed, while indefinite forms have not. We will first give a brief summary on the reduction of forms with negative discriminant before we move on to the main part of the paper on the reduction of indefinite forms.

Recall from the introduction that a form (A, B, C) is *positive definite* if $Ax^2 + Bxy + Cy^2 > 0$ for any $(x, y) \neq (0, 0)$. For simplicity, we will only consider positive definite forms that are primitive. We say that a positive definite primitive form $Q = (A, B, C)$ is *reduced* if it is Lagrange-reduced ($|B| \leq A \leq C$) and $B \geq 0$ when one of the inequalities is not strict.

For each discriminant $\Delta \equiv 0, 1 \pmod 4$, we associate a Lagrange-reduced form Q_0 called the *principal form*. The principal form is defined by

$$Q_0 = \begin{cases} (1, 0, k), & \Delta = -4k \\ (1, 1, k), & \Delta = 1 - 4k \end{cases}$$

Lemma 1 (Legendre's Lemma)**.** *If $Q = (A, B, C)$ is reduced, then the smallest integers primitively represented by Q (in ascending order) are:*

$$\begin{aligned} &A,\ C,\ A - B + C && \text{if } B > 0 \\ &A,\ C,\ A + B + C && \text{if } B < 0 \end{aligned}$$

Proof. Assume $B > 0$ and note that $Q(\pm 1, 0) = A$, $Q(0, \pm 1) = C$, and $Q(\pm 1, \mp 1) = A - B + C$. There are three cases for $Q(x, y) \neq A, C, A - B + C$.

If $|x| = |y|$

$$Q(x, y) = Ax^2 + Bx(\pm x) + Cx^2 = x^2(A \pm B + C) \geq x^2(A - B + C) > A - B + C$$

If $|x| > |y|$ then

$$\begin{aligned} Q(x, y) &\geq Ax^2 - B|x||y| + Cy^2 > A|x||y| - |Bxy| + Cy^2 = |xy|(A - B) + Cy^2 \\ &\geq (A - B + C)y^2 > A - B + C \end{aligned}$$

If $|x| < |y|$ then

$$Q(x, y) \geq Ax^2 - |Bxy| + Cy^2 > x^2(A - B + C) > A - B + C$$

Lastly, since Q is Lagrange-reduced, we have $A \leq C$ and $C \leq A - B + C$.

For the corresponding cases of $B < 0$, simply note that the two forms $Q = (A, B, C)$ and $Q' = (A, -B, C)$ represent the same integers primitively as $Q(x, y) = Q'(x, -y)$ □

Corollary 1 (Corollary 1.13 of Lemmermeyer)**.** *If Q is a positive definite quadratic form that represents 1, then $Q \sim Q_0$.*

Proof. Without loss of generality, assume $Q = (A, B, C)$ is reduced (otherwise find its equivalent reduced form). By Legendre's Lemma we have that $A = 1$ and since $|B| \leq |A| = 1$ either $Q = (1, 0, C)$ or $Q = (1, 1, C)$. □

Theorem 1 (Theorem 1.11 of Lemmermeyer)**.** *Every class of primitive positive definite quadratic forms contains a unique reduced form.*

Proof. Assume $Q = (A, B, C)$ and $Q' = (A', B', C')$ are equivalent and reduced. By Legendre's Lemma, since Q and Q' are reduced and represent the same integers, we have that $C, C' \geq A = A'$. This splits the proof into two cases.

Assume $C = A$. Then we have that $Q(\pm 1, 0) = Q(0, \pm 1) = A$ so A is represented at least four times by Q and Q'. This gives that $C' = A = C$. Since $\Delta(Q) = \Delta(Q')$ we have that $|B| = |B'|$ but Q and Q' are both reduced with $A = C$ and $A' = C'$ so $B, B' > 0$ and $Q = Q'$.

Now assume $C > A$. We have that Q and Q' represent A exactly twice with $A = A' = Q(\pm 1, 0) = Q'(\pm 1, 0)$. By Legendre's Lemma, we have that C is the second smallest integer represented by Q and C' the second smallest integer represented by Q' which gives $C = C'$. Now by the same argument as above we have that $B' = \pm B$. If $B' = B$, we are done so assume $B' = -B$. We then have that $(A, B, C) \sim (A, -B, C)$ with $Q' = Q|_N$ for some $N \in \mathrm{SL}_2(\mathbb{Z})$. Let $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$, then we have

$$A = A' = Ar^2 + Brt + Ct^2$$

By assumption $C > A$ which gives $t = 0$ and subsequently $r = \pm 1$ and $u = r$. With these values of t, r, and u we have

$$B' = -B = 2As + B \text{ or equivalently } B' = -B = As$$

Again, Q is reduced so $|B| \leq A$ which gives $s = 0$ or $s = \pm 1$. If $s = 0$ then $B' = B = 0$ and if $s = \pm 1$ then $B = -A$ or $B' = -A'$ which is impossible since Q and Q' are reduced. □

The number of Lagrange-reduced forms of discriminant Δ is called the *Kronecker class number*, denoted $H(\Delta)$. Recall from Chapter 1 that the class number, $h(\Delta)$, is the number of primitive reduced forms of discriminant $\Delta < 0$.

Corollary 2. *$H(\Delta) = h(\Delta)$ when Δ is a fundamental discriminant. Furthermore $h(\Delta) = 1$ if and only if the only primitive reduced form is Q_0*

Proof. The first claim is clear by the definition of a fundamental discriminant and the second follows immediately from Theorem 1 along with the fact that the principal form Q_0 is primitive for every discriminant. □

We can now create a table of reduced forms of small discriminant.

Δ	$H(\Delta)$	Lagrange-Reduced Forms	$h(\Delta)$	Primitive Reduced Forms
-3	1	$(1,1,1)$	1	$(1,1,1)$
-4	1	$(1,0,1)$	1	$(1,0,1)$
-7	1	$(1,1,2)$	1	$(1,1,2)$
-8	1	$(1,0,2)$	1	$(1,0,2)$
-11	1	$(1,1,3)$	1	$(1,1,3)$
-12	2	$(1,0,3), (2,2,2)$	1	$(1,0,3)$,
-15	2	$(1,1,4), (2,1,2)$	2	$(1,1,4), (2,1,2)$
-16	2	$(1,0,4), (2,0,2)$	1	$(1,0,4)$

Table 2.2: Reduced forms with $-16 \leq \Delta \leq -3$

Chapter 3

Zagier Reduction

One desired result for both positive definite and indefinite quadratic forms is to define a reduction method where there is one reduced form per equivalence class. Though the definition of a reduced form using Lagrange reduction produced this result in most cases for positive definite forms, it fails to do so for indefinite forms. The first reduction theory for indefinite quadratic forms that we will introduce was developed by Zagier with motivation similar to Lagrange.

1 Zagier-reduced Forms

Given a quadratic form (A, B, C) of discriminant Δ, we find an equivalent form with minimal $A > 0$ and change B modulo $2|A|$ so that $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2A]$. This gives that $AC > 0$ and $A \leq C$ (as $Q(0,1) = C$). We say that a form (A, B, C) with positive non-square discriminant is *Zagier-reduced* if the coefficients satisfy

$$\sqrt{\Delta} < B < \sqrt{\Delta} + 2A \text{ and } \sqrt{\Delta} < B < \sqrt{\Delta} + 2C.$$

Theorem 2 (Theorem 1.14 of Lemmermeyer)**.** *Let (A, B, C) be a primitive indefinite form with discriminant Δ. The following statements are equivalent:*

(i) (A, B, C) *is Zagier-reduced*

(ii) $0 < \frac{B-\sqrt{\Delta}}{2A} < 1 < \frac{B+\sqrt{\Delta}}{2A}$

(iii) $A > 0,\ C > 0,\ B > A + C$

Proof.
$(i) \Rightarrow (ii)$: Since (A, B, C) is Zagier-reduced,

$$\sqrt{\Delta} < B < \sqrt{\Delta} + 2A \text{ and } \sqrt{\Delta} < B < \sqrt{\Delta} + 2C$$

which gives

$$0 < B - \sqrt{\Delta} < 2A \text{ and } 0 < B - \sqrt{\Delta} < 2C$$

We then have

$$2A = \frac{B^2 - \Delta}{2C} < \frac{B^2 - \Delta}{B - \sqrt{\Delta}} = B + \sqrt{\Delta}$$

Combining these inequalities gives

$$0 < B - \sqrt{\Delta} < 2A < B + \sqrt{\Delta}$$

Dividing by $2A$ gives the desired inequality.
$(ii) \Rightarrow (iii)$: If $A < 0$ then multiplying by $2A$ would yield $B + \sqrt{\Delta} < B - \sqrt{\Delta}$, so we know $A > 0$ and $B - \sqrt{\Delta} > 0$.
Now assume $C < 0$. Then we have $\Delta = B^2 - 4AC > B^2$ and hence $\sqrt{\Delta} > B$ which contradicts $B - \sqrt{\Delta} > 0$.
Lastly,

$$\begin{aligned}
\frac{B - \sqrt{\Delta}}{2A} < 1 < \frac{B + \sqrt{\Delta}}{2A} &\Leftrightarrow B - \sqrt{\Delta} < 2A < B + \sqrt{\Delta} \\
&\Leftrightarrow -\sqrt{\Delta} < 2A - B < \sqrt{\Delta} \\
&\Leftrightarrow |B - 2A| < \sqrt{\Delta} \\
&\Leftrightarrow (B - 2A)^2 < \Delta \\
&\Leftrightarrow \Delta - (B - 2A)^2 = 4A(B - A - C) > 0 \\
&\Leftrightarrow B - A - C > 0 \\
&\Leftrightarrow B > A + C.
\end{aligned}$$

$(iii) \Rightarrow (i)$:

$$\begin{aligned}
B > A + C,\ A > 0 &\Rightarrow \Delta - (B - 2A)^2 = 4A(B - A - C) > 0 \\
&\Rightarrow \Delta > (B - 2A)^2 \\
&\Rightarrow \sqrt{\Delta} > |B - 2A| \\
&\Rightarrow B - 2A < \sqrt{\Delta} \\
&\Rightarrow B < \sqrt{\Delta} + 2A
\end{aligned}$$

By a similar argument, $B < \sqrt{\Delta} + 2C$. Finally, since $A, C > 0$ we have $\Delta < B^2$ and hence $\sqrt{\Delta} < B$. □

Proposition 7 (Proposition 1.15 of Lemmermeyer)**.** *The coefficients of Zagier-reduced forms satisfy*

$$0 < A, C \leq \frac{\Delta}{4} \text{ and } \sqrt{\Delta} < B \leq \frac{\sqrt{\Delta^2 + 4\Delta}}{2}$$

Proof. By Theorem 2 we know $A, C > 0$ and $B > A + C$ which gives

$$0 < A = \frac{\Delta - (B - 2A)^2}{4(B - A - C)} \leq \frac{\Delta}{4}$$

By a similar argument, the inequality also holds for C. Using this result, we now have

$$B^2 = \Delta + 4AC \leq \Delta + \frac{\Delta^2}{4} = \frac{\Delta^2 + 4\Delta}{4}$$

Since (A, B, C) is Zagier-reduced we have the desired inequality. □

Proposition 7 shows that there are only finitely many Zagier-reduced forms of fixed discriminant and allows us to compute the following table:

Δ	κ_Z	Primitive Zagier-reduced Forms
5	1	$(1,3,1)$
8	2	$(1,4,2),(2,4,1)$
12	3	$(1,4,1),(2,6,3),(3,6,2)$
13	3	$(1,5,3),(3,5,1),(3,7,3)$
17	5	$(1,5,2),(2,5,1),(2,7,4),(4,7,2),(4,9,4)$
20	4	$(1,6,4),(4,6,1),(4,10,5),(5,10,4)$

Table 3.1: Primitive Zagier-reduced forms of small fundamental discriminant

Here $\kappa_Z(\Delta)$ denotes the amount of Zagier-reduced forms with discriminant Δ and is called the *caliber* of the discriminant.
By construction, we know that every form is equivalent to at least one Zagier-reduced form. To determine if two forms are equivalent, we can simply reduce both forms and check whether their corresponding Zagier-reduced forms are equivalent. To see which Zagier-reduced forms are equivalent, we will make use of a *reduction operator* which has the useful property that two reduced forms are equivalent if they belong to the same cycle of that operator.

2 Zagier-Reduction Operator

Define $\mathcal{F}_\Delta$ to be the set of primitive forms of discriminant Δ and $\mathcal{R}_\Delta$ to be the subset of reduced forms in $\mathcal{F}_\Delta$. We say that a map $\rho : \mathcal{F}_\Delta \to \mathcal{F}_\Delta$ is a *reduction operator* if it satisfies the following

(i) For any $Q \in \mathcal{F}_\Delta$, there exists a non-negative integer ν such that $\rho^\nu(Q)$ is reduced.

(ii) $\rho(Q)$ is reduced if Q is reduced.

We call $\rho(Q)$ the *right neighbor* of Q and say that a form is *semi-reduced* if it is in the image of ρ. To find the right neighbor of a form $Q = (A,B,C)$, apply the matrix $R_n = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ where n is such that $n-1 < \frac{B+\sqrt{\Delta}}{2A} < n$ to get an equivalent form $Q' = (A',B',C')$. (Note that this is the process of applying a shift followed by a flip.) Alternatively we can compute the right neighbor as follows:

(1) $C' = A$

(2) $B + B' \equiv 0 \pmod{2A}$ and $\begin{cases} \sqrt{\Delta} < B' < \sqrt{\Delta} + 2A & \text{if } A > 0 \\ \sqrt{\Delta} + 2A < B' < \sqrt{\Delta} & \text{if } A < 0 \end{cases}$

(3) $(B')^2 - 4A'C' = \Delta$

The proof that this is in fact a reduction map will need the following lemma.

Lemma 2 (Lemma 1.17 of Lemmermeyer)**.** *Let $Q = (A,B,C)$ be an indefinite form of discriminant Δ and let $Q' = (A',B',C')$ be its right neighbor. The following statements hold:*

(i) If $A < 0$ then $A' > A$

(ii) If $A > 0$ then $A' > 0$

(iii) If $A' \geq A > 0$, then Q' is Zagier-reduced

(iv) If Q is Zagier-reduced then $Q' = Q|_{R_n}$ for $R_n = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $n \geq 2$

Proof. Define $0 < \theta < 1$ to be such that $n = \frac{B+\sqrt{\Delta}}{2A} + \theta$. Then we have

$$A' = An^2 - Bn + C = A\left(\frac{B+\sqrt{\Delta}}{2A} + \theta\right)^2 - B\left(\frac{B+\sqrt{\Delta}}{2A} + \theta\right) + C = \theta\sqrt{\Delta} + A\theta^2$$

This gives for $A < 0$

$$A' - A = \theta\sqrt{\Delta} + A\theta^2 - A = A(\theta^2 - 1) + \theta\sqrt{\Delta} > 0$$

which proves (i). Assume $A > 0$, then (ii) follows from $A' = \theta\sqrt{\Delta} + A\theta^2 > 0$.
Assume $A' \geq A > 0$ then

$$\begin{aligned}
0 &\leq A' - A \\
&= \theta\sqrt{\Delta} - A(1-\theta^2) \\
&< (\theta+1)\sqrt{\Delta} - A(1-\theta^2) \\
&= (\theta+1)(\sqrt{\Delta} - A(1-\theta)) \\
&= \frac{\theta+1}{1-\theta}\left(\sqrt{\Delta}(1-\theta) - A(1-\theta)^2\right) \\
&= \frac{\theta+1}{1-\theta}\left(\sqrt{\Delta}\left(1 - \left(n - \frac{B+\sqrt{\Delta}}{2A}\right)\right) - A\left(1 - \left(n - \frac{B+\sqrt{\Delta}}{2A}\right)\right)^2\right) \\
&= \frac{\theta+1}{1-\theta}\left(B' - A' - C'\right)
\end{aligned}$$

This gives $B' > A' + C'$ and since $C' = A$ we have $A' \geq C' > 0$. By Theorem 2, Q' is reduced. Lastly, assume Q is Zagier-reduced. By Theorem 2, $\frac{B+\sqrt{\Delta}}{2A} = n - \theta > 1$ which implies $n \geq 2$ □

Proposition 8 (Proposition 1.18 of Lemmermeyer)**.** *The map ρ defined above is a reduction operator on indefinite forms.*

Proof. There are two things we need to show for $Q = (A, B, C)$:

(1) There is a nonnegative integer ν such that $\rho^\nu(Q)$ is Zagier-reduced.

(2) If Q Zagier-reduced then $\rho(Q)$ is also Zagier-reduced

If $A < 0$ then by Lemma 2, we can apply ρ until we have a form with $A > 0$. Applying ρ once more will give $C' = A > 0$ and $A' > 0$. Since the first coefficient stays positive and can't decrease indefinitely, there must be a point at which $A' \geq A$ and by Lemma 2, applying ρ produces a Zagier-reduced form. Now assume Q is Zagier-reduced, then by Theorem 2 we have $A > 0$, $C > 0$, and

hence $A', C' = A > 0$. Using Theorem 2 we have that $\rho(Q)$ is Zagier-reduced if $B' > A' + C'$ or equivalently $B' - A' - C' > 0$. Indeed

$$B' - A' - C' = \sqrt{\Delta}(1-\theta) - A(1-\theta)^2 = (1-\theta)(\sqrt{\Delta} - A(1-\theta)).$$

Since $\theta < 1$, $(1-\theta) > 0$ and using the results from Theorem 2 and Lemma 2 we have

$$\begin{aligned}\frac{\sqrt{\Delta}}{A} &= \frac{B+\sqrt{\Delta}}{2A} - \frac{B-\sqrt{\Delta}}{2A} \\ &= n - \theta - \xi_2 \\ &> 1 - \theta.\end{aligned}$$

Thus $\sqrt{\Delta} - A(1-\theta) > 0$ and $B' - A' - C' > 0$ as needed. □

With the above definition, some forms may have the same right neighbor. For this reason we define forms to be *semi-reduced (in the Zagier sense)* if they satisfy the following conditions

$$\begin{cases} \sqrt{\Delta} < B < \sqrt{\Delta} + 2A & \text{if } A > 0 \\ \sqrt{\Delta} + 2A < B < \sqrt{\Delta} & \text{if } A < 0 \end{cases}$$

Proposition 9 (Proposition 1.19 of Lemmermeyer)**.** *The reduction operator ρ is injective on semi-reduced forms.*

Proof. Assume (A_1, B_1, C_1) and (A_2, B_2, C_2) are semi reduced forms that both map to (A', B', C'). Immediately we have $C' = A_1 = A_2$ so define A to be this common value. We now have

$$B_1 + B' \equiv 0 \pmod{2A} \text{ and } B_2 + B' \equiv 0 \pmod{2A}$$

As such, let n_1 and n_2 be integers such that

$$B_1 = 2An_1 - B' \text{ and } B_2 = 2An_2 - B'$$

Using this we have $|B_1 - B_2| = 2A|n_1 - n_2|$ and since B_1 and B_2 both lie in an interval of length $2A$ we know that $|B_1 - B_2| < 2A$. This gives $n_1 = n_2$ and thus $B_1 = B_2$. Since Δ is fixed, we have $(A_1, B_1, C_1) = (A_2, B_2, C_2)$ □

This injection on semi-reduced forms allows us to create an inverse reduction operator λ for semi-reduced Q. In this case, $\lambda(Q)$ is called the *left neighbor* of Q. We can find the left neighbor of Q by reversing the above process:

(1) $A = C'$

(2) $B + B' \equiv 0 \pmod{2C'}$ and $\begin{cases} \sqrt{\Delta} < B < \sqrt{\Delta} + 2C' & \text{if } C' > 0 \\ \sqrt{\Delta} + 2C' < B < \sqrt{\Delta} & \text{if } C' < 0 \end{cases}$

(3) $B^2 - 4AC = \Delta$

For primitive quadratic forms $Q = (A, B, C)$ this is equivalent to defining $\lambda(Q)$ as $Q|_{S_n}$ for $S_n = \left(\begin{smallmatrix} 0 & -1 \\ 1 & n \end{smallmatrix}\right)$ for n such that $n - 1 < \frac{B+\sqrt{\Delta}}{2C} < n$ With this definition, the following lemma is clear:

Lemma 3 (Lemma 1.21 of Lemmermeyer)**.** *If Q is semi-reduced, then $\lambda\circ\rho(Q) = Q$ and $\rho\circ\lambda(Q) = Q$*

Corollary 3 (Corollary 1.22 of Lemmermeyer)**.** *The reduction operator ρ permutes the set of reduced forms*

Proof. From Proposition 9 we have that ρ is injective on semi-reduced forms (and hence reduced forms) and by Proposition 8 we know that if Q is reduced then so is $\rho(Q)$. Since the set of reduced forms of a fixed discriminant Δ is finite, we have the needed bijection. □

Using the reduction operator ρ allows us to create the following table of cycles:

Δ	$h^+(\Delta)$	Cycles
5	1	$(1,3,1)$
8	1	$(1,4,2)(2,4,1)$
12	2	$(1,4,1)$
		$(2,6,3)(3,6,2)$
13	1	$(1,5,3)(3,5,1)(3,7,3)$
17	1	$(1,5,2)(2,5,1)(2,7,4)(4,7,2)(4,9,4)$
20	1	$(1,6,4)(4,6,1)(5,10,4)(4,10,5)$
21	2	$(1,5,1)$
		$(3,9,5)(5,9,3)(5,11,5)$
24	2	$(1,6,3)(3,6,1)$
		$(2,8,5)(5,8,2)(6,12,5)(5,12,6)$

Table 3.2: Cycles of Zagier-reduced forms with small discriminant

We know that if two forms are in the same cycle, they must be equivalent, but the converse is true as well. To prove this result we need the following fundamental lemma.

Lemma 4 (Lemma 1.24 of Lemmermeyer)**.** *Let Q and Q' be Zagier-reduced forms. If $Q \sim Q'$ with $Q' = Q|_N$ then N is the product of reduction matrices R_n.*

Proof. Let $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. Then we have that $Q' = (A', B', C')$ where

$$\begin{aligned} A' &= Ar^2 + Brt + Ct^2 = Q(r,t) > 0 \\ C' &= As^2 + Bsu + Cu^2 = Q(s,u) > 0 \\ A' + C' - B' &= (Ar^2 + Brt + Ct^2) + (As^2 + Bsu + Cu^2) - (2Ars + Bru + Bst + 2Ctu) \\ &= A(r-s)^2 + B(r-s)(t-u) + C(t-u)^2 \\ &= Q(r-s, t-u) < 0 \end{aligned}$$

by Theorem 2. If $t = u$ then $Q(r-s, t-u) = Q(r-s, 0) > 0$ which is a contradiction so we know $t \neq u$ and since $Q|_N = Q|_{-N}$ we can assume without loss of generality that $u > t$. We now split the proof into three cases:

(i) If $t = 0$ then $N \in \mathrm{SL}_2(\mathbb{Z})$ implies $ru = 1$ and $u > t = 0$ implies $r = u = 1$. This gives

$$C' = Q(s,1) > 0 > A' + C' - B' = Q(s-1,1).$$

Since Q is Zagier reduced, we know

$$C = Q(0,1) > 0 > Q(-1,1) = A + C - B$$

Since $Q(s,1)$ is a quadratic polynomial, there is at most one integer such that $Q(s,1) > 0 > Q(s-1,1)$ so s must be zero. This gives $N = I$ and $Q' = Q$.

(ii) If $t < 0$, we will show that $Q' = \rho^{\nu}(Q)$ for some $\nu \geq 1$. Let $Q_1 = \rho(Q)$ with corresponding reduction matrix R_{n_1}. Then we have $Q' = Q_1|_{(R_{n_1})^{-1}N}$ so define N_1 as

$$N_1 = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} = \left(R_{n_1}\right)^{-1} N = \begin{pmatrix} -t & -u \\ r+tn & s+nu \end{pmatrix}$$

We then have $r_1 - s_1 = u - t > 0$ so $Q(r_1 - s_1, t_1 - u_1) = (r_1 - s_1)(t_1 - u_1) < 0$ giving that $u_1 > t_1$. This gives that if needed, we can repeat the process with Q_1 to get $Q_2 = \rho(Q_1) = Q_1|_{R_{n_1}}$ and $Q' = Q_2|_{(R_{n_2})^{-1}(R_{n_1})^{-1}N} = Q_2|_{N_2}$ where $N_2 = \left(\begin{smallmatrix} r_2 & s_2 \\ t_2 & u_2 \end{smallmatrix}\right)$
We now claim that eventually $t_\nu = 0$ for some $\nu \geq 1$. To this end we prove that $t < t_1 \leq 0$ and hence t_k is an increasing sequence of nonpositive integers and must eventually reach 0. This is equivalent to showing that $t < r + nt \leq 0$ or

$$n - 1 \leq -\frac{r}{t} \leq n.$$

Note that for $Q(x,-1) = Ax^2 - Bx + C$ we have

$$Q\left(-\frac{r}{t}, -1\right) = A' > 0 > Q\left(\frac{-r+s}{t-u}\right) = A' + C' - B.$$

Since $ru - st = 1 > 0$ we know $-\frac{r}{t} > \frac{-r+s}{t-u}$ which gives

$$\frac{-r+s}{t-u} < \frac{B+\sqrt{\Delta}}{2A} < -\frac{r}{t}$$

By choice of n we get the left side of the desired inequality $n - 1 < \frac{B+\sqrt{\Delta}}{2A} < -\frac{r}{t}$. For the right side, assume that $-\frac{r}{t} > n$ then we have

$$\begin{aligned} -\frac{r}{t} > n \Rightarrow \frac{-r+s}{t-u} &< n < \frac{-r}{t} \\ \Rightarrow -rt + st &< nt(t-u) < -rt + ru \\ \Rightarrow st &< nt(t-u) + rt < ru \end{aligned}$$

$ru - st = 1$ implies that $nt(t-u) + rt$ is not an integer which is a contradiction.

(iii) The proof for $t > 0$ is analogous to the proof of $t < 0$ by showing $0 \leq t_1 < t$ which is again equivalent to $n - 1 \leq -\frac{r}{t} \leq n$.

□

With the above fundamental lemma, the following main theorem of Zagier Reduction is clear.

Theorem 3 (Theorem 1.23 of Lemmermeyer)**.** *Two primitive Zagier-reduced forms of discriminant Δ are equivalent if and only if they belong to the same cycle.*

We end the chapter with a table of the cycles of Zagier-reduced forms of fundamental discriminant less than 100.

Δ	h^+	#	Cycles
5	1	–	$(1,3,1)$
8	1	–	$(2,4,1)(1,4,2)$
12	2	1	$(1,4,1)$
		2	$(3,6,2)(2,6,3)$
13	1	–	$(3,5,1)(3,7,3)(1,5,3)$
17	1	–	$(2,5,1)(4,7,2)(4,9,4)(2,7,4)(1,5,2)$
21	2	1	$(1,5,1)$
		2	$(5,9,3)(5,11,5)(3,9,5)$
24	2	1	$(3,6,1)(1,6,3)$
		2	$(5,8,2)(6,12,5)(5,12,6)(2,8,5)$
28	2	1	$(2,6,1)(1,6,2)$
		2	$(3,8,3)(6,10,3)(7,14,6)(6,14,7)(3,10,6)$
29	1	–	$(5,7,1)(7,13,5)(7,15,7)(5,13,7)(1,7,5)$
33	2	1	$(4,7,1)(3,9,4)(4,9,3)(1,7,4)$
		2	$(2,7,2)(6,9,2)(8,15,6)(8,17,8)(6,15,8)(2,9,6)$
37	1	–	$(3,7,1)(7,11,3)(9,17,7)(9,19,9)(7,17,9)(3,11,7)(1,7,3)$
40	2	1	$(6,8,1)(9,16,6)(10,20,9)(9,20,10)(6,16,9)(1,8,6)$
		2	$(2,8,3)(3,8,2)(5,10,3)(3,10,5)$
41	2	1	$(2,7,1)(5,9,2)(4,11,5)(8,13,4)(10,19,8)(10,21,10)(8,19,10)(4,13,8)(5,11,4)$ $(2,9,5)(1,7,2)$
		2	$(8,13,4)(10,19,8)(10,21,10)(8,19,10)(4,13,8)(5,11,4)(2,9,5)(1,7,2)(2,7,1)$ $(5,9,2)(4,11,5)$
44	2	1	$(5,8,1)(5,12,5)(1,8,5)$
		2	$(7,10,2)(10,18,7)(11,22,10)(10,22,11)(7,18,10)(2,10,7)$
53	1	–	$(7,9,1)(11,19,7)(13,25,11)(13,27,13)(11,25,13)(7,19,11)(1,9,7)$
56	2	1	$(2,8,1)(1,8,2)$
		2	$(7,14,5)(5,14,7)(10,16,5)(13,24,10)(14,28,13)(13,28,14)(10,24,13)(5,16,10)$
57	2	1	$(6,9,1)(7,15,6)(4,13,7)(4,11,4)(7,13,4)(6,15,7)(1,9,6)$
		2	$(3,9,2)(2,9,3)(8,11,2)(12,21,8)(14,27,12)(14,29,14)(12,27,14)(8,21,12)(2,11,8)$
60	4	1	$(1,8,1)$
		2	$(5,10,2)(2,10,5)$
		3	$(11,18,6)(14,26,11)(15,30,14)(14,30,15)(11,26,14)(6,18,11)$
		4	$(7,12,3)(7,16,7)(3,12,7)$
61	1	–	$(5,9,1)(3,11,5)(9,13,3)(13,23,9)(15,29,13)(15,31,15)(13,29,15)(9,23,13)$ $(3,13,9)(5,11,3)(1,9,5)$

Δ	h^+	#	Cycles
65	2	1	$(4,9,1)(10,15,4)(14,25,10)(16,31,14)(16,33,16)(14,31,16)(10,25,14)(4,15,10)$ $(1,9,4)$
		2	$(7,11,2)(8,17,7)(5,15,8)(8,15,5)(7,17,8)(2,11,7)(2,9,2)$
69	2	1	$(3,9,1)(1,9,3)$
		2	$(5,13,5)(11,17,5)(15,27,11)(17,33,15)(17,35,17)(15,33,17)(11,27,15)(5,17,11)$
73	3	1	$(2,9,1)(6,11,2)(4,13,6)(3,11,4)(8,13,3)(9,19,8)(6,17,9)(12,19,6)(16,29,12)$ $(18,35,16)(18,37,18)(16,35,18)(12,29,16)(6,19,12)(9,17,6)(8,19,9)(3,13,8)$ $(4,11,3)(6,13,4)(2,11,6)(1,9,2)$
		2	$(4,11,3)(6,13,4)(2,11,6)(1,9,2)(2,9,1)(6,11,2)(4,13,6)(3,11,4)(8,13,3)(9,19,8)$ $(6,17,9)(12,19,6)(16,29,12)(18,35,16)(18,37,18)(16,35,18)(12,29,16)(6,19,12)$ $(9,17,6)(8,19,9)(3,13,8)$
		3	$(3,11,4)(8,13,3)(9,19,8)(6,17,9)(12,19,6)(16,29,12)(18,35,16)(18,37,18)$ $(16,35,18)(12,29,16)(6,19,12)(9,17,6)(8,19,9)(3,13,8)(4,11,3)(6,13,4)(2,11,6)$ $(1,9,2)(2,9,1)(6,11,2)(4,13,6)$
76	2	1	$(6,10,1)(5,14,6)(9,16,5)(9,20,9)(5,16,9)(6,14,5)(1,10,6)$
		2	$(2,10,3)(3,10,2)(10,14,3)(15,26,10)(18,34,15)(19,38,18)(18,38,19)(15,34,18)$ $(10,26,15)(3,14,10)$
77	2	1	$(1,9,1)$
		2	$(13,21,7)(17,31,13)(19,37,17)(19,39,19)(17,37,19)(13,31,17)(7,21,13)$
85	2	1	$(9,11,1)(15,25,9)(19,35,15)(21,41,19)(21,43,21)(19,41,21)(15,35,19)(9,25,15)$ $(1,11,9)$
		2	$(3,11,3)(7,13,3)(5,15,7)(7,15,5)(3,13,7)$
88	2	1	$(3,10,1)(9,14,3)(11,22,9)(9,22,11)(3,14,9)(1,10,3)$
		2	$(7,16,6)(2,12,7)(7,12,2)(6,16,7)(13,20,6)(18,32,13)(21,40,18)(22,44,21)$ $(21,44,22)(18,40,21)(13,32,18)(6,20,13)$
89	2	1	$(8,11,1)(11,21,8)(10,23,11)(5,17,10)(4,13,5)(2,11,4)(10,13,2)(16,27,10)$ $(20,37,16)(22,43,20)(22,45,22)(20,43,22)(16,37,20)(10,27,16)(2,13,10)(4,11,2)$ $(5,13,4)(10,17,5)(11,23,10)(8,21,11)(1,11,8)$
		2	$(4,11,2)(5,13,4)(10,17,5)(11,23,10)(8,21,11)(1,11,8)(8,11,1)(11,21,8)$ $(10,23,11)(5,17,10)(4,13,5)(2,11,4)(10,13,2)(16,27,10)(20,37,16)(22,43,20)$ $(22,45,22)(20,43,22)(16,37,20)(10,27,16)(2,13,10)$
92	2	1	$(2,10,1)(1,10,2)$
		2	$(11,20,7)(11,24,11)(7,20,11)(14,22,7)(19,34,14)(22,42,19)(23,46,22)(22,46,23)$ $(19,42,22)(14,34,19)(7,22,14)$
93	2	1	$(7,11,1)(7,17,7)(1,11,7)$
		2	$(11,15,3)(17,29,11)(21,39,17)(23,45,21)(23,47,23)(21,45,23)(17,39,21)$ $(11,29,17)(3,15,11)$

Δ	h^+	#	Cycles
97	3	1	$(6,11,1)(3,13,6)(2,11,3)(9,13,2)(12,23,9)(11,25,12)(6,19,11)(8,17,6)(4,15,8)$ $(12,17,4)(18,31,12)(22,41,18)(24,47,22)(24,49,24)(22,47,24)(18,41,22)$ $(12,31,18)(4,17,12)(8,15,4)(6,17,8)(11,19,6)(12,25,11)(9,23,12)(2,13,9)$ $(3,11,2)(6,13,3)(1,11,6)$
		2	$(11,19,6)(12,25,11)(9,23,12)(2,13,9)(3,11,2)(6,13,3)(1,11,6)(6,11,1)(3,13,6)$ $(2,11,3)(9,13,2)(12,23,9)(11,25,12)(6,19,11)(8,17,6)(4,15,8)(12,17,4)$ $(18,31,12)(22,41,18)(24,47,22)(24,49,24)(22,47,24)(18,41,22)(12,31,18)$ $(4,17,12)(8,15,4)(6,17,8)$
		3	$(9,13,2)(12,23,9)(11,25,12)(6,19,11)(8,17,6)(4,15,8)(12,17,4)$ $(18,31,12)(22,41,18)(24,47,22)(24,49,24)(22,47,24)(18,41,22)(12,31,18)$ $(4,17,12)(8,15,4)(6,17,8)(11,19,6)(12,25,11)(9,23,12)(2,13,9)(3,11,2)(6,13,3)$ $(1,11,6)(6,11,1)(3,13,6)(2,11,3)$

Table 3.3: Cycles of primitive Zagier-reduced forms with fundamental $\Delta < 100$

Chapter 4

Gauss Reduction

We now introduce the concept of Gauss reduction, the reduction theory for indefinite forms on which Zagier's was based. Compared to Zagier-reduced forms, Gauss reduction produces smaller coefficients but lengthier proofs.

1 Gauss-reduced Forms

Let $Q = (A, B, C)$ be an indefinite binary quadratic form of discriminant Δ with the condition that Δ is not a square. Let A be such that $|A|$ is the smallest integer represented by Q. Apply the shift operation to reduced B modulo $2A$ until B lies in the interval $\sqrt{\Delta} - 2|A| < B < \sqrt{\Delta}$ of length $2A$ (this differs from the condition $\sqrt{\Delta} < B < \sqrt{\Delta} + 2A$ for Zagier-reduced forms). By the choice of $|A|$ we also have $|A| \leq |C|$ and thus such forms satisfy the following:

$$\begin{cases} \sqrt{\Delta} - 2|A| < B < \sqrt{\Delta} \\ \sqrt{\Delta} - 2|C| < B < \sqrt{\Delta}. \end{cases}$$

We say that a quadratic form Q is *Gauss-reduced* if it satisfies the above two conditions. Forms that satisfy the first condition are called *semi-reduced*.
As expected, Gauss-reduction produces very similar results to those of Zagier-reduction. The following theorem can be contrasted with Theorem 2 in Section 3.1.

Theorem 4 (Theorem 1.36 of Lemmermeyer)**.** *Let $Q = (A, B, C)$ be a primitive indefinite form. The following are equivalent:*

(i) (A, B, C) *is Gauss-reduced*

(ii) $\left(\frac{-B+\sqrt{\Delta}}{2A}\right)\left(\frac{-B-\sqrt{\Delta}}{2A}\right) < 0, \left|\frac{-B+\sqrt{\Delta}}{2A}\right| < 1 < \left|\frac{-B-\sqrt{\Delta}}{2A}\right|$

(iii) $AC < 0,\ B > |A + C|$

Proof. $(i) \Rightarrow (ii)$: Assume Q is Gauss-reduced with $AC > 0$ then $B^2 - 4AC < B^2$ which implies $\sqrt{\Delta} < B$ which contradicts the fact that Q is reduced so we know $AC < 0$. This gives

$$\left(\frac{-B + \sqrt{\Delta}}{2A}\right)\left(\frac{-B - \sqrt{\Delta}}{2A}\right) = \frac{4AC}{4A^2} < 0$$

The second inequality is equivalent to

$$\left|-B+\sqrt{\Delta}\right| < 2|A| < \left|-B-\sqrt{\Delta}\right|$$

Since (A,B,C) is reduced we have $B<\sqrt{\Delta}$ so $0<-B+\sqrt{\Delta}<2|A|$ which gives the left side of the inequality. For the right side we use the fact that $AC<0$ along with the second condition of being reduced to get

$$2|A| = \frac{\Delta - B^2}{2|C|} < \frac{\Delta - B^2}{\sqrt{\Delta}-B} = \sqrt{\Delta}+B = \left|-B-\sqrt{\Delta}\right|$$

$(ii) \Leftrightarrow (iii)$: $\left(\frac{-B+\sqrt{\Delta}}{2A}\right)\left(\frac{-B-\sqrt{\Delta}}{2A}\right) = \frac{AC}{A^2} < 0$ shows that the first two inequalities of each of (ii) and (iii) are equivalent. For the second ones we have

$$\begin{aligned}
\left|\frac{-B+\sqrt{\Delta}}{2A}\right| < 1 < \left|\frac{-B-\sqrt{\Delta}}{2A}\right| &\Leftrightarrow \frac{\sqrt{\Delta}-B}{2|A|} < 1 < \frac{B+\sqrt{\Delta}}{2|A|} \\
&\Leftrightarrow -B+\sqrt{\Delta} < 2|A| < \sqrt{\Delta}+B \\
&\Leftrightarrow -B < 2|A| - \sqrt{\Delta} < B \\
&\Leftrightarrow \left|2|A| - \sqrt{\Delta}\right| < B \\
&\Leftrightarrow (2|A| - \sqrt{\Delta})^2 < B^2 \\
&\Leftrightarrow B^2 - (2|A| - \sqrt{\Delta})^2 = -4|A|\left(|A| - \sqrt{\Delta} + |C|\right) > 0 \\
&\Leftrightarrow |A| - \sqrt{\Delta} + |C| < 0 \\
&\Leftrightarrow |A| + |C| < \sqrt{\Delta} \\
&\Leftrightarrow A^2 - 2AC + C^2 < B^2 - 4AC \\
&\Leftrightarrow (A+C)^2 < B^2 \\
&\Leftrightarrow B > |A+C|\,.
\end{aligned}$$

(ii) and $(iii) \Rightarrow (i)$: We know from above that $AC<0$ which gives $B^2<\Delta$ and hence $B<\sqrt{\Delta}$. Using this we can rewrite the second inequality of (ii) to get $-B+\sqrt{\Delta}<2|A|$ which is equivalent to $\sqrt{\Delta}-2|A|<B$. For the second condition of being reduced we use the same identity above with the second assumption to get

$$2|A| = \frac{\Delta - B^2}{2|C|} < \frac{\Delta - B^2}{\sqrt{\Delta}-B} = \sqrt{\Delta}+B.$$

This gives $\sqrt{\Delta}-B<2|C|$ which is equivalent to $\sqrt{\Delta}-2|C|<B$ as needed. □

The following lemma is the Gauss-reduction equivalent of Proposition 7 for Zagier-reduced forms.

Lemma 5 (Lemma 1.37 of Lemmermeyer)**.** *A Gauss-reduced form $Q=(A,B,C)$ satisfies the following inequalities*

(i) $B>0$

(ii) $AC<0$

(iii) $0 < |A|, B, |C| < \sqrt{\Delta}$

Proof. Conditions (i) and (ii) are immediate from Theorem 4. Theorem 4 combined with the fact that Q is Gauss-reduced gives the final inequality. □

2 Gauss' Reduction Operator

Like Zagier-reduction, there is a reduction operator ρ that works for Gauss-reduced forms. Given a form $Q = (A, B, C)$ of discriminant Δ, the right neighbor $\rho(Q) = Q' = (A', B', C')$ is constructed as follows

(1) $A' = C$

(2) $B + B' \equiv 0 \pmod{2A'}$ and $\sqrt{\Delta} - \left|2A'\right| < B' < \sqrt{\Delta}$

(3) $(B')^2 - 4A'C' = \Delta$

Alternatively, one can notice that this process is equivalent to applying the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & n \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right)$ (i.e. a flip followed by a shift), where n is such that $B + B' = 2Cn$. As such, the difference between the above operator and that for Zagier-reduction is that B' is chosen to be in a different interval.

The properties of the reduction operator for Gauss-reduced forms can be proven in a similar manner than those of Zagier-reduction. We state the following facts analogous to Proposition 8, Proposition 9, and Theorem 3 without proof.

- If Q is a primitive indefinite form, then $\rho(Q)$ is semi-reduced.
- If Q is reduced then $\rho(Q)$ is also reduced.
- Every reduced form belongs to some cycle.
- Two forms are equivalent if and only if they belong to the same cycle.

Combining these facts together yields Gauss' reduction theory for indefinite forms.

Using the reduction operator we make the following table:

Δ	h^+	#	Cycles
5	1	–	$(1,1,-1)(-1,1,1)$
8	1	–	$(1,2,-1)(-1,2,1)$
12	2	1	$(1,2,-2)(-2,2,1)$
		2	$(-1,2,2)(2,2,-1)$
13	1	–	$(1,3,-1)(-1,3,1)$
17	1	–	$(1,3,-2)(-2,1,2)(2,3,-1)(-1,3,2)(2,1,-2)(2,3,1)$
20	1	–	$(1,4,-1)(-1,4,1)$
21	2	1	$(1,3,-3)(-3,3,1)$
		2	$(-1,3,3)(3,3,-1)$
24	2	1	$(1,4,-2)(-2,4,1)$
		2	$(-1,4,2)(2,4,-1)$
28	2	1	$(1,4,-3)(-3,2,2)(2,2,-3)(-3,4,1)$
		2	$(-1,4,3)(3,2,-2)(-2,2,3)(3,4,-1)$
29	1	–	$(1,5,-1)(-1,5,1)$
32	2	1	$(1,4,-4)(-4,4,1)$
		2	$(-1,4,4)(4,4,-1)$
33	2	1	$(1,5,-2)(-2,3,3)(3,3,-2)(-2,5,1)$
		2	$(-1,5,2)(2,3,-3)(-3,3,-2)(2,5,-1)$
37	1		$(1,5,-3)(-3,1,3)(3,5,-1)(-1,5,3)(3,1,-3)(-3,5,1)$
40	2	1	$(1,6,-1)(-1,6,1)$
		2	$(2,4,-3)(-3,2,3)(3,4,-2)(-2,4,3)(3,2,-3)(-3,4,2)$
41	1	–	$(1,5,-4)(-4,3,2)(2,5,-2)(-2,3,4)(4,5,-1)$
			$(-1,5,4)(4,3,-2)(-2,5,2)(2,3,-4)(-4,5,1)$
44	2	1	$(1,6,-2)(-2,6,1)$
		2	$(-1,6,2)(2,6,-1)$
45	2	1	$(1,5,-5)(-5,5,1)$
		2	$(-1,5,5)(5,5,-1)$
48	2	1	$(1,6,-3)(-3,6,1)$
		2	$(-1,6,3)(3,6,-1)$
52	1	–	$(1,6,-4)(-4,2,3)(3,4,-3)(-3,2,4)(4,6,-1)$
			$(-1,6,4)(4,2,-3)(-3,4,3)(3,2,-4)(-4,6,1)$
53	1	–	$(1,7,-1)(-1,7,1)$
56	2	1	$(1,6,-5)(-5,4,2)(2,4,-5)(-5,6,1)$
		2	$(-1,6,5)(5,4,-2)(-2,4,5)(5,6,-1)$

Δ	h^+	#	Cycles
57	2	1	$(1,7,-2)(-2,5,4)(4,3,-3)(-3,3,4)(4,5,-2)(-2,7,1)$
		2	$(-1,7,2)(2,5,-4)(-4,3,3)(3,3,-4)(-4,5,2)(2,7,-1)$
60	4	1	$(1,6,-6)(-6,6,1)$
		2	$(-3,6,2)(2,6,-3)$
		3	$(-1,6,6)(6,6,-1)$
		4	$(3,6,-2)(-2,6,3)$
61	1	–	$(1,7,-3)(-3,5,3)(3,7,-1)(-1,7,3)(3,5,-3)(-3,7,1)$
65	2	1	$(1,7,-4)(-4,1,4)(4,7,-1)(-1,7,4)(4,1,-4)(-4,7,1)$
		2	$(2,5,-5)(-5,5,2)(2,7,-2)(-2,5,5)(5,5,-2)(-2,7,2)$
69	2	1	$(1,7,-5)(-5,3,3)(3,3,-5)(-5,7,1)$
		2	$(-1,7,5)(5,3,-3)(-3,3,5)(5,7,-1)$
73	1	–	$(1,7,-6)(-6,5,2)(2,7,-3)(-3,5,4)(4,3,-4)(-4,5,3)(3,7,-2)(-2,5,6)(6,7,-1)$
			$(-1,7,6)(6,5,-2)(-2,6,3)(3,5,-4)(-4,3,4)(4,5,-3)(-3,7,2)(2,5,-6)(-6,7,1)$
76	2	1	$(1,8,-3)(-3,4,5)(5,6,-2)(-2,6,5)(5,4,-3)(-3,8,1)$
		2	$(-1,8,3)(3,4,-5)(-5,6,2)(2,6,-5)(-5,4,3)(3,8,-1)$
77	2	1	$(1,7,-7)(-7,7,1)$
		2	$(-1,7,7)(7,7,-1)$
85	2	1	$(1,9,-1)(-1,9,1)$
		2	$(3,7,-3)(-3,5,5)(5,5,-3)(-3,7,3)(3,5,-5)(-5,5,3)$
88	2	1	$(1,8,-6)(-6,4,3)(3,8,-2)(-2,8,3)(3,4,-6)(-6,8,1)$
		2	$(-1,8,6)(6,4,-3)(-3,8,2)(2,8,-3)(-3,4,6)(6,8,-1)$
89	1	–	$(1,9,-2)(-2,7,5)(5,3,-4)(-4,5,4)(4,3,-5)(-5,7,2)(2,9,-1)$
			$(-1,9,2)(2,7,-5)(-5,3,4)(4,5,-4)(-4,3,5)(5,7,-2)(-2,9,1)$
92	2	1	$(1,8,-7)(-7,6,2)(2,6,-7)(-7,8,1)$
		2	$(-1,8,7)(7,6,-2)(-2,6,7)(7,8,-1)$
93	2	1	$(1,9,-3)(-3,9,1)$
		2	$(-1,9,3)(3,9,-1)$
97	1	–	$(1,9,-4)(-4,7,3)(3,5,-6)(-6,7,2)(2,9,-2)(-2,7,6)(6,5,-3)(-3,7,4)(4,9,-1)$
			$(-1,9,4)(4,7,-3)(-3,5,6)(6,7,-2)(-2,9,2)(2,7,-6)(-6,5,3)(3,7,-4)(-4,9,1)$

Table 4.1: Gauss-reduced cycles with fundamental $\Delta < 100$

Chapter 5

Siegel Reduction (and Proposing a Siegel Reduction Operator)

The reduction that is least developed is a method of reduction proposed by Siegel. As opposed to the other methods of reduction that are computed algebraically, Siegel's suggested method associates to a quadratic form a semi-circle determined by its roots. A reduced form then is a form whose circle intersects the fundamental domain, $\mathcal{F}$. We define these criteria more specifically in the following sections. For simplicity, we will only consider forms of fundamental discriminant $\Delta < 100$.

1 The Fundamental Domain of the Modular Group

We define the *modular group*, Γ, to be equal to the projective special linear group $\mathrm{PSL}_2(\mathbb{Z})$ where

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{I, -I\}.$$

Equivalently, we can define the modular group to be the group of fractional linear transformations, from the upper half-plane, $\mathbb{H}$, of complex numbers $\mathbb{H} = \{z = x + yi \mid y > 0;\ x, y \in \mathbb{R}\}$ to itself where

$$\begin{array}{ccc} \mathbb{H} & \to & \mathbb{H} \\ z & \mapsto & \dfrac{az+b}{cz+d} \end{array}$$

where $ad - bc = 1$ and $a, b, c, d \in \mathbb{Z}$.
The *fundamental domain* for the modular group is then given by

$$\mathcal{F} = \left\{ z \in \mathbb{H} \;\middle|\; |z| > 1 \ ; \ \left|\mathrm{Re}(z)\right| < \frac{1}{2} \right\}.$$

Graphically, this represents the following shaded region on the complex plane

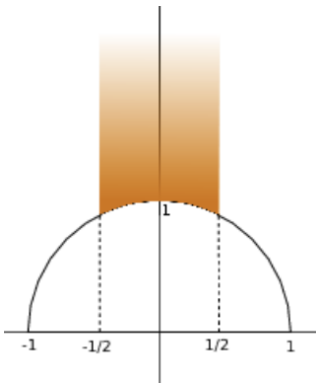

Figure 5.1: The fundamental domain (source: `inspirehep.net/record/1280946/plots`)

2 Siegel-reduced Forms

Let $Q = (A, B, C)$ be a binary quadratic form and define τ_1 and τ_2 in a way such that

$$Ax^2 + Bxy + Cxy^2 = a(x - \tau_1 y)(x - \tau_2 y).$$

Then τ_1 and τ_2 are the roots of the equation

$$A\lambda^2 + B\lambda + C = 0.$$

In other words

$$\tau_{1,2} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

We call an indefinite binary quadratic form *Siegel-reduced* if the semi-circle of diameter τ_1, τ_2 intersects the $\mathcal{F}$ in a non-empty set. Equivalently, if at least one of the"vertices" of $\mathcal{F}$, $(-1/2, \sqrt{3}/2)$ or $(1/2, \sqrt{3}/2)$, lies in (or on) the semi-circle. The center and radius of the semi-circle corresponding to the quadratic form (A, B, C) are given by

$$\text{Center} = \left(-\frac{B}{2A}, 0\right) \text{ and Radius} = \frac{\sqrt{\Delta}}{2|A|}.$$

Proposition 10. *A Siegel-reduced form (A, B, C) of discriminant Δ satisfies the following inequalities:*

$$A^2 \leq \frac{\Delta}{3}, \quad B^2 \leq \frac{4\Delta}{3}, \quad 3AC \leq \frac{\Delta}{4}.$$

This proposition shows that the number of reduced forms of a given discriminant is finite. Unfortunately, a form satisfying the above inequalities need not be Siegel-reduced. This fact is illustrated in the following counter-example.

Example 3. Consider the form $(1, 7, 3)$ with $\Delta = 37$

$$1^2 \leq \frac{37}{3},\ 49 \leq \frac{148}{3},\ 9 \leq \frac{37}{4}$$

$$\text{Center} = \left(-\frac{7}{2}, 0\right), \text{ Radius} = \frac{\sqrt{37}}{2}$$

$$\begin{aligned}\text{Distance from center to} \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) &= \sqrt{16 + \frac{3}{4}} \\ &= \frac{\sqrt{67}}{2} > R\end{aligned}$$

$$\begin{aligned}\text{Distance from center to } \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) &= \sqrt{9 + \frac{3}{4}} \\ &= \frac{\sqrt{39}}{2} > R\end{aligned}$$

Thus the form satisfies the inequalities but is not reduced.

Using this proposition we can create a finite list of possible Siegel-reduced forms and then eliminate those that do not contain a vertex of $\mathcal{F}$. The following is a table of Siegel-reduced forms with fundamental discriminant less than 100.

Δ	h^+	Forms
5	1	$(1,1,-1),(-1,1,1),(1,-1,-1),(-1,-1,1)$
8	1	$(1,0,-2),(-1,0,2),(1,2,-1),(-1,2,1),(1,-2,-1),(-1,-2,1)$
12	2	$(1,0,-3),(-1,0,3),(1,2,-2),(-1,2,2),(1,-2,-2),(-1,-2,2),(2,2,-1),(-2,2,1),$ $(2,-2,-1),(-2,-2,1),(1,4,1),(-1,4,-1),(1,-4,1),(-1,-4,-1)$
13	1	$(1,1,-3),(-1,1,3),(1,-1,-3),(-1,-1,3),(1,3,-1),(-1,3,1),(1,-3,-1),(-1,-3,1)$
17	1	$(1,1,-4),(-1,1,4),(1,-1,-4),(-1,-1,4),(2,1,-2),(-2,1,2),(2,-1,-2),(-2,-1,2),$ $(1,3,-2),(-1,3,2),(1,-3,-2),(-1,-3,2),(2,3,-1),(-2,3,1),(2,-3,-1),(-2,-3,1)$
21	2	$(1,1,-5),(-1,1,5),(1,-1,-5),(-1,-1,5),(1,3,-3),(-1,3,3),(1,-3,-3),(-1,-3,3),$ $(1,5,1),(-1,5,-1),(1,-5,1),(-1,-5,-1)$
24	2	$(1,0,-6),(-1,0,6),(2,0,-3),(-2,0,3),(1,2,-5),(-1,2,5),(1,-2,-5),(-1,-2,5),$ $(1,4,-2),(-1,4,2),(1,-4,-2),(-1,-4,2),(2,4,-1),(-2,4,1),(2,-4,-1),(-2,-4,1)$
28	2	$(1,0,-7),(-1,0,7),(1,2,-6),(-1,2,6),(1,-2,-6),(-1,-2,6),(2,2,-3),(-2,2,3),$ $(2,-2,-3),(-2,-2,3),(3,2,-2),(-3,2,2),(3,-2,-2),(-3,-2,2),(1,4,-3),(-1,4,3),$ $(1,-4,-3),(-1,-4,3),(3,4,-1),(-3,4,1),(3,-4,-1),(-3,-4,1),(1,6,2),(-1,6,-2),$ $(1,-6,2),(-1,-6,-2),(2,6,1),(-2,6,-1),(2,-6,1),(-2,-6,-1)$
29	1	$(1,1,-7),(-1,1,7),(1,-1,-7),(-1,-1,7),(1,3,-5),(-1,3,5),(1,-3,-5),(-1,-3,5),$ $(1,5,-1),(-1,5,1),(1,-5,-1),(-1,-5,1)$
33	2	$(1,1,-8),(-1,1,8),(1,-1,-8),(-1,-1,8),(2,1,-4),(-2,1,4),(2,-1,-4),(-2,-1,4),$ $(1,3,-6),(-1,3,6),(1,-3,-6),(-1,-3,6),(2,3,-3),(-2,3,3),(2,-3,-3),(-2,-3,3),$ $(3,3,-2),(-3,3,2),(3,-3,-2),(-3,-3,2),(1,5,-2),(-1,5,2),(1,-5,-2),(-1,-5,2),$ $(2,5,-1),(-2,5,1),(2,-5,-1),(-2,-5,1)$
37	1	$(1,1,-9),(-1,1,9),(1,-1,-9),(-1,-1,9),(3,1,-3),(-3,1,3),(3,-1,-3),(-3,-1,3),$ $(1,3,-7),(-1,3,7),(1,-3,-7),(-1,-3,7),(1,5,-3),(-1,5,3),(1,-5,-3),(-1,-5,3),$ $(3,5,-1),(-3,5,1),(3,-5,-1),(-3,-5,1)$
40	2	$(1,0,-10),(-1,0,10),(2,0,-5),(-2,0,5),(1,2,-9),(-1,2,9),(1,-2,-9),(-1,-2,9),$ $(3,2,-3),(-3,2,3),(3,-2,-3),(-3,-2,3),(1,4,-6),(-1,4,6),(1,-4,-6),(-1,-4,6),$ $(2,4,-3),(-2,4,3),(2,-4,-3),(-2,-4,3),(3,4,-2),(-3,4,2),(3,-4,-2),(-3,-4,2),$ $(1,6,-1),(-1,6,1),(1,-6,-1),(-1,-6,1)$
41	1	$(1,1,-10),(-1,1,10),(1,-1,-10),(-1,-1,10),(2,1,-5),(-2,1,5),(2,-1,-5),$ $(-2,-1,5),(1,3,-8),(-1,3,8),(1,-3,-8),(-1,-3,8),(2,3,-4),(-2,3,4),(2,-3,-4),$ $(-2,-3,4),(1,5,-4),(-1,5,4),(1,-5,-4),(-1,-5,4),(2,5,-2),(-2,5,2),(2,-5,-2),$ $(-2,-5,2),(1,7,2),(-1,7,-2),(1,-7,2),(-1,-7,-2),(2,7,1),(-2,7,-1),(2,-7,1),$ $(-2,-7,-1)$
44	2	$(1,0,-11),(-1,0,11),(1,2,-10),(-1,2,10),(1,-2,-10),(-1,-2,10),(2,2,-5),$ $(-2,2,5),(2,-2,-5),(-2,-2,5),(1,4,-7),(-1,4,7),(1,-4,-7),(-1,-4,7),(1,6,-2),$ $(-1,6,2),(1,-6,-2),(-1,-6,2),(2,6,-1),(-2,6,1),(2,-6,-1),(-2,-6,1)$
53	1	$(1,1,-13),(-1,1,13),(1,-1,-13),(-1,-1,13),(1,3,-11),(-1,3,11),(1,-3,-11),$ $(-1,-3,11),(1,5,-7),(-1,5,7),(1,-5,-7),(-1,-5,7),(1,7,-1),(-1,7,1),(1,-7,-1),$ $(-1,-7,1)$

Δ	h^+	Forms
56	2	$(1,0,-14),(-1,0,14),(2,0,-7),(-2,0,7),(1,2,-13),(-1,2,13),(1,-2,-13),$ $(-1,-2,13),(1,4,-10),(-1,4,10),(1,-4,-10),(-1,-4,10),(2,4,-5),(-2,4,5),$ $(2,-4,-5),(-2,-4,5),(1,6,-5),(-1,6,5),(1,-6,-5),(-1,-6,5),(1,8,2),(-1,8,-2),$ $(1,-8,2),(-1,-8,-2),(2,8,1),(-2,8,-1),(2,-8,1),(-2,-8,-1)$
57	2	$(1,1,-14),(-1,1,14),(1,-1,-14),(-1,-1,14),(2,1,-7),(-2,1,7),(2,-1,-7),$ $(-2,-1,7),(1,3,-12),(-1,3,12),(1,-3,-12),(-1,-3,12),(2,3,-6),(-2,3,6),$ $(2,-3,-6),(-2,-3,6),(3,3,-4),(-3,3,4),(3,-3,-4),(-3,-3,4),(4,3,-3),(-4,3,3),$ $(4,-3,-3),(-4,-3,3),(1,5,-8),(-1,5,8),(1,-5,-8),(-1,-5,8),(2,5,-4),(-2,5,4),$ $(2,-5,-4),(-2,-5,4),(4,5,-2),(-4,5,2),(4,-5,-2),(-4,-5,2),(1,7,-2),(-1,7,2),$ $(1,-7,-2),(-1,-7,2),(2,7,-1),(-2,7,1),(2,-7,-1),(-2,-7,1)$
60	4	$(1,0,-15),(-1,0,15),(3,0,-5),(-3,0,5),(1,2,-14),(-1,2,14),(1,-2,-14),$ $(-1,-2,14),(2,2,-7),(-2,2,7),(2,-2,-7),(-2,-2,7),(1,4,-11),(-1,4,11),$ $(1,-4,-11),(-1,-4,11),(1,6,-6),(-1,6,6),(1,-6,-6),(-1,-6,6),(2,6,-3),(-2,6,3),$ $(2,-6,-3),(-2,-6,3),(3,6,-2),(-3,6,2),(3,-6,-2),(-3,-6,2),(1,8,1),(-1,8,-1),$ $(1,-8,1),(-1,-8,-1)$
61	1	$(1,1,-15),(-1,1,15),(1,-1,-15),(-1,-1,15),(3,1,-5),(-3,1,5),(3,-1,-5),$ $(-3,-1,5),(1,3,-13),(-1,3,13),(1,-3,-13),(-1,-3,13),(1,5,-9),(-1,5,9),$ $(1,-5,-9),(-1,-5,9),(3,5,-3),(-3,5,3),(3,-5,-3),(-3,-5,3),(1,7,-3),(-1,7,3),$ $(1,-7,-3),(-1,-7,3),(3,7,-1),(-3,7,1),(3,-7,-1),(-3,-7,1)$
65	2	$(1,1,-16),(-1,1,16),(1,-1,-16),(-1,-1,16),(2,1,-8),(-2,1,8),(2,-1,-8),$ $(-2,-1,8),(4,1,-4),(-4,1,4),(4,-1,-4),(-4,-1,4),(1,3,-14),(-1,3,14),$ $(1,-3,-14),(-1,-3,14),(2,3,-7),(-2,3,7),(2,-3,-7),(-2,-3,7),(1,5,-10),$ $(-1,5,10),(1,-5,-10),(-1,-5,10),(2,5,-5),(-2,5,5),(2,-5,-5),(-2,-5,5),$ $(1,7,-4),(-1,7,4),(1,-7,-4),(-1,-7,4),(2,7,-2),(-2,7,2),(2,-7,-2),(-2,-7,2),$ $(4,7,-1),(-4,7,1),(4,-7,-1),(-4,-7,1),(2,9,2),(-2,9,-2),(2,-9,2),(-2,-9,-2)$
69	2	$(1,1,-17),(-1,1,17),(1,-1,-17),(-1,-1,17),(1,3,-15),(-1,3,15),(1,-3,-15),$ $(-1,-3,15),(3,3,-5),(-3,3,5),(3,-3,-5),(-3,-3,5),(1,5,-11),(-1,5,11),$ $(1,-5,-11),(-1,-5,11),(1,7,-5),(-1,7,5),(1,-7,-5),(-1,-7,5),(1,9,3),(-1,9,-3),$ $(1,-9,3),(-1,-9,-3),(3,9,1),(-3,9,-1),(3,-9,1),(-3,-9,-1)$
73	1	$(1,1,-18),(-1,1,18),(1,-1,-18),(-1,-1,18),(2,1,-9),(-2,1,9),(2,-1,-9),$ $(-2,-1,9),(3,1,-6),(-3,1,6),(3,-1,-6),(-3,-1,6),(1,3,-16),(-1,3,16),$ $(1,-3,-16),(-1,-3,16),(2,3,-8),(-2,3,8),(2,-3,-8),(-2,-3,8),(4,3,-4),(-4,3,4),$ $(4,-3,-4),(-4,-3,4),(1,5,-12),(-1,5,12),(1,-5,-12),(-1,-5,12),(2,5,-6),$ $(-2,5,6),(2,-5,-6),(-2,-5,6),(3,5,-4),(-3,5,4),(3,-5,-4),(-3,-5,4),(4,5,-3),$ $(-4,5,3),(4,-5,-3),(-4,-5,3),(1,7,-6),(-1,7,6),(1,-7,-6),(-1,-7,6),(2,7,-3),$ $(-2,7,3),(2,-7,-3),(-2,-7,3),(3,7,-2),(-3,7,2),(3,-7,-2),(-3,-7,2),(1,9,2),$ $(-1,9,-2),(1,-9,2),(-1,-9,-2),(2,9,1),(-2,9,-1),(2,-9,1),(-2,-9,-1)$

Δ	h^+	Forms
76	2	$(1,0,-19),(-1,0,19),(1,2,-18),(-1,2,18),(1,-2,-18),(-1,-2,18),(2,2,-9),$ $(-2,2,9),(2,-2,-9),(-2,-2,9),(3,2,-6),(-3,2,6),(3,-2,-6),(-3,-2,6),(1,4,-15),$ $(-1,4,15),(1,-4,-15),(-1,-4,15),(3,4,-5),(-3,4,5),(3,-4,-5),(-3,-4,5),$ $(5,4,-3),(-5,4,3),(5,-4,-3),(-5,-4,3),(1,6,-10),(-1,6,10),(1,-6,-10),$ $(-1,-6,10),(2,6,-5),(-2,6,5),(2,-6,-5),(-2,-6,5),(5,6,-2),(-5,6,2),(5,-6,-2),$ $(-5,-6,2),(1,8,-3),(-1,8,3),(1,-8,-3),(-1,-8,3),(3,8,-1),(-3,8,1),(3,-8,-1),$ $(-3,-8,1),(2,10,3),(-2,10,-3),(2,-10,3),(-2,-10,-3),(3,10,2),(-3,10,-2),$ $(3,-10,2),(-3,-10,-2)$
77	2	$(1,1,-19),(-1,1,19),(1,-1,-19),(-1,-1,19),(1,3,-17),(-1,3,17),(1,-3,-17),$ $(-1,-3,17),(1,5,-13),(-1,5,13),(1,-5,-13),(-1,-5,13),(1,7,-7),(-1,7,7),$ $(1,-7,-7),(-1,-7,7),(1,9,1),(-1,9,-1),(1,-9,1),(-1,-9,-1)$
85	2	$(1,1,-21),(-1,1,21),(1,-1,-21),(-1,-1,21),(3,1,-7),(-3,1,7),(3,-1,-7),$ $(-3,-1,7),(1,3,-19),(-1,3,19),(1,-3,-19),(-1,-3,19),(1,5,-15),(-1,5,15),$ $(1,-5,-15),(-1,-5,15),(3,5,-5),(-3,5,5),(3,-5,-5),(-3,-5,5),(5,5,-3),$ $(-5,5,3),(5,-5,-3),(-5,-5,3),(1,7,-9),(-1,7,9),(1,-7,-9),(-1,-7,9),(3,7,-3),$ $(-3,7,3),(3,-7,-3),(-3,-7,3),(1,9,-1),(-1,9,1),(1,-9,-1),(-1,-9,1)$
88	2	$(1,0,-22),(-1,0,22),(2,0,-11),(-2,0,11),(1,2,-21),(-1,2,21),(1,-2,-21),$ $(-1,-2,21),(3,2,-7),(-3,2,7),(3,-2,-7),(-3,-2,7),(1,4,-18),(-1,4,18),$ $(1,-4,-18),(-1,-4,18),(2,4,-9),(-2,4,9),(2,-4,-9),(-2,-4,9),(3,4,-6),$ $(-3,4,6),(3,-4,-6),(-3,-4,6),(1,6,-13),(-1,6,13),(1,-6,-13),(-1,-6,13),$ $(1,8,-6),(-1,8,6),(1,-8,-6),(-1,-8,6),(2,8,-3),(-2,8,3),(2,-8,-3),(-2,-8,3),$ $(3,8,-2),(-3,8,2),(3,-8,-2),(-3,-8,2),(1,10,3),(-1,10,-3),(1,-10,3),$ $(-1,-10,-3),(3,10,1),(-3,10,-1),(3,-10,1),(-3,-10,-1)$
89	1	$(1,1,-22),(-1,1,22),(1,-1,-22),(-1,-1,22),(2,1,-11),(-2,1,11),(2,-1,-11),$ $(-2,-1,11),(1,3,-20),(-1,3,20),(1,-3,-20),(-1,-3,20),(2,3,-10),(-2,3,10),$ $(2,-3,-10),(-2,-3,10),(4,3,-5),(-4,3,5),(4,-3,-5),(-4,-3,5),(5,3,-4),$ $(-5,3,4),(5,-3,-4),(-5,-3,4),(1,5,-16),(-1,5,16),(1,-5,-16),(-1,-5,16),$ $(2,5,-8),(-2,5,8),(2,-5,-8),(-2,-5,8),(4,5,-4),(-4,5,4),(4,-5,-4),(-4,-5,4),$ $(1,7,-10),(-1,7,10),(1,-7,-10),(-1,-7,10),(2,7,-5),(-2,7,5),(2,-7,-5),$ $(-2,-7,5),(5,7,-2),(-5,7,2),(5,-7,-2),(-5,-7,2),(1,9,-2),(-1,9,2),(1,-9,-2),$ $(-1,-9,2),(2,9,-1),(-2,9,1),(2,-9,-1),(-2,-9,1)$
92	2	$(1,0,-23),(-1,0,23),(1,2,-22),(-1,2,22),(1,-2,-22),(-1,-2,22),(2,2,-11),$ $(-2,2,11),(2,-2,-11),(-2,-2,11),(1,4,-19),(-1,4,19),(1,-4,-19),(-1,-4,19),$ $(1,6,-14),(-1,6,14),(1,-6,-14),(-1,-6,14),(2,6,-7),(-2,6,7),(2,-6,-7),$ $(-2,-6,7),(1,8,-7),(-1,8,7),(1,-8,-7),(-1,-8,7),(1,10,2),(-1,10,-2),$ $(1,-10,2),(-1,-10,-2),(2,10,1),(-2,10,-1),(2,-10,1),(-2,-10,-1)$
93	2	$(1,1,-23),(-1,1,23),(1,-1,-23),(-1,-1,23),(1,3,-21),(-1,3,21),(1,-3,-21),$ $(-1,-3,21),(3,3,-7),(-3,3,7),(3,-3,-7),(-3,-3,7),(1,5,-17),(-1,5,17),$ $(1,-5,-17),(-1,-5,17),(1,7,-11),(-1,7,11),(1,-7,-11),(-1,-7,11),(1,9,-3),$ $(-1,9,3),(1,-9,-3),(-1,-9,3),(3,9,-1),(-3,9,1),(3,-9,-1),(-3,-9,1)$

Δ	h^+	Forms
97	1	$(1,1,-24),(-1,1,24),(1,-1,-24),(-1,-1,24),(2,1,-12),(-2,1,12),(2,-1,-12),$ $(-2,-1,12),(3,1,-8),(-3,1,8),(3,-1,-8),(-3,-1,8),(4,1,-6),(-4,1,6),$ $(4,-1,-6),(-4,-1,6),(1,3,-22),(-1,3,22),(1,-3,-22),(-1,-3,22),(2,3,-11),$ $(-2,3,11),(2,-3,-11),(-2,-3,11),(1,5,-18),(-1,5,18),(1,-5,-18),(-1,-5,18),$ $(2,5,-9),(-2,5,9),(2,-5,-9),(-2,-5,9),(3,5,-6),(-3,5,6),(3,-5,-6),$ $(-3,-5,6),(1,7,-12),(-1,7,12),(1,-7,-12),(-1,-7,12),(2,7,-6),(-2,7,6),$ $(2,-7,-6),(-2,-7,6),(3,7,-4),(-3,7,4),(3,-7,-4),(-3,-7,4),(4,7,-3),(-4,7,3),$ $(4,-7,-3),(-4,-7,3),(1,9,-4),(-1,9,4),(1,-9,-4),(-1,-9,4),(2,9,-2),(-2,9,2),$ $(2,-9,-2),(-2,-9,2),(4,9,-1),(-4,9,1),(4,-9,-1),(-4,-9,1),(2,11,3),$ $(-2,11,-3),(2,-11,3),(-2,-11,-3),(3,11,2),(-3,11,-2),(3,-11,2),(-3,-11,-2)$

Table 5.1: Siegel-reduced forms with fundamental discriminant $\Delta < 100$

Proposition 11. *If $Q = (A, B, C)$ is a Siegel-reduced binary quadratic form which doesn't intersect a vertex then $Q|_S = (C, -B, A)$ is reduced if and only if the semi-circle corresponding to Q contains only one vertex.*

Proof. ($\Leftarrow$): Without loss of generality, assume that the circle corresponding to Q contains $(1/2, \sqrt{3}/2)$ but not $(-1/2, \sqrt{3}/2)$ (hence $AB > 0$). This gives the following inequalities

$$\sqrt{\left(\frac{1}{2} + \frac{B}{2A}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} \leq \frac{\sqrt{B^2 - 4AC}}{2|A|} \text{ and } \sqrt{\left(-\frac{1}{2} + \frac{B}{2A}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} > \frac{\sqrt{B^2 - 4AC}}{2|A|}.$$

Applying a few algebraic manipulations we have that the two inequalities are equivalent to

$$2A^2 + AB \leq -2AC \text{ and } 2A^2 - AB > -2AC.$$

We now split into two cases.
First assume that $AC > 0$ (so $BC < 0$). Using the same method as above we have that $Q|_S$ contains $(-1/2, \sqrt{3}/2)$ if it satisfies one of the following inequalities:

$$2C^2 + BC < -2AC, \text{ or equivalently } |C| < -|A| + \frac{|B|}{2}.$$

Using the inequality corresponding to Q containing $(1/2, \sqrt{3}/2)$ we have

$$2A^2 + AB < -2AC \Leftrightarrow 2A^2 - |A||B| < -2|A||C|$$

$$\Leftrightarrow |C| < -|A| + \frac{|B|}{2}.$$

Now assume that $AC < 0$ ($BC > 0$). We then have that $Q|_S$ contains $(1/2, \sqrt{3}/2)$ if

$$2C^2 - BC < -2AC, \text{ or equivalently } |C| < |A| + \frac{|B|}{2}.$$

Using the inequality corresponding to Q not containing $(-1/2, \sqrt{3}/2)$ we have

$$2A^2 - AB > -2AC \Leftrightarrow 2A^2 + |A||B| > 2|A||C|$$

$$\Leftrightarrow |C| < |A| + \frac{|B|}{2}$$

as needed. □

3 Permuting Siegel-Reduced Forms

Something that was not explored in Siegel's paper on quadratic forms was the idea of a reduction operator like that of Gauss and Zagier. In order to explore the idea of finding such an operator, the first step is to find a rule that will permute Siegel-reduced forms while preserving equivalence classes. Because the idea of Siegel-reduction is geometric, we will also take a geometric approach for a reduction operator.

Looking at the boundaries of $\mathcal{F}$ we can separate it into three sections: the arc of the unit-circle, the line $x = 1/2$, and the line $x = -1/2$. Taking the circle corresponding to the binary quadratic form (A, B, C), we can look at the "last" place the circle intersects the boundary of $\mathcal{F}$. If it intersects the line $x = 1/2$, we shift the circle left 1 unit, if it intersects the line $x = -1/2$, we shift the circle right 1 unit, and if it intersects the unit circle, we reflect the circle.
Algebraically, shifting a circle by n units corresponds to acting on the binary quadratic form by the shift matrix $T_n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, where $n < 0$ represents a right shift and $n > 0$ represents a left shift. Reflecting a circle corresponds to acting on the form by the flip operation $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
The first question that arrises when applying this strategy is if we start on a circle, which direction do we travel in to determine the last place the circle intersects the fundamental domain? Simply by convention we will say that the direction of the circle corresponding to (A, B, C) is moving

Left,	if $\operatorname{sgn}(A) = \operatorname{sgn}(C) = 1$ or $\operatorname{sgn}(A) \neq \operatorname{sgn}(C) = -1$
Right,	if $\operatorname{sgn}(A) = \operatorname{sgn}(C) = -1$ or $\operatorname{sgn}(A) \neq \operatorname{sgn}(C) = 1$.

We will find later on that direction is preserved by our choice of operator.

Example 4. $\Delta = 37$

Graphing the Siegel-reduced quadratic forms gives the following circles:

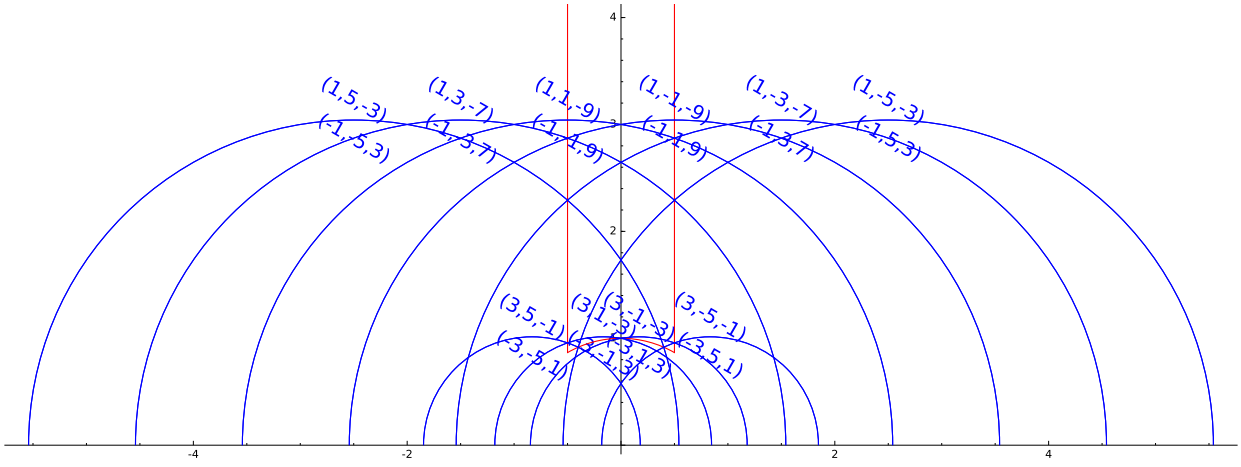

Figure 5.2: Semicircles corresponding to Siegel-reduced forms of discriminant 37

Starting out with the circle corresponding to $(1, -5, -3)$ and applying the rules, we get the following cycle. The direction above each triple indicates the direction in which we are travelling:

$$(1,-5,-3) \overset{\text{left}}{\xrightarrow{S}} (-3,5,1) \overset{\text{right}}{\xrightarrow{T_1}} (-3,-1,3) \overset{\text{right}}{\xrightarrow{S}} (3,1,-3) \overset{\text{left}}{\xrightarrow{T_{-1}}} (3,-5,-1) \overset{\text{right}}{\xrightarrow{S}} (-1,5,3) \overset{\text{right}}{\xrightarrow{T_1}} (-1,3,7) \overset{\text{right}}{\xrightarrow{T_1}}$$

$$(-1,1,9) \overset{\text{right}}{\xrightarrow{T_1}} (-1,-1,9) \overset{\text{right}}{\xrightarrow{T_1}} (-1,-3,7) \overset{\text{right}}{\xrightarrow{T_1}} (-1,-5,3) \overset{\text{right}}{\xrightarrow{S}} (3,5,-1) \overset{\text{left}}{\xrightarrow{T_{-1}}} (3,-1,-3) \overset{\text{left}}{\xrightarrow{S}} (-3,1,3) \overset{\text{right}}{\xrightarrow{T_1}}$$

$$(-3,-5,1) \overset{\text{right}}{\xrightarrow{S}} (1,5,-3) \overset{\text{left}}{\xrightarrow{T_{-1}}} (1,3,-7) \overset{\text{left}}{\xrightarrow{T_{-1}}} (1,1,-9) \overset{\text{left}}{\xrightarrow{T_{-1}}} (1,-1,-9) \overset{\text{left}}{\xrightarrow{T_{-1}}} (1,-3,-7) \overset{\text{left}}{\xrightarrow{T_{-1}}} (1,-5,-3) \overset{\text{left}}{\xrightarrow{T_{-1}}}$$

This idea also preserves equivalence classes since we are always acting by a matrix in $\mathrm{PSL}_2(\mathbb{Z})$. This is displayed in the following example.

Example 5. $\Delta = 24$

The Siegel-reduced forms are the following:

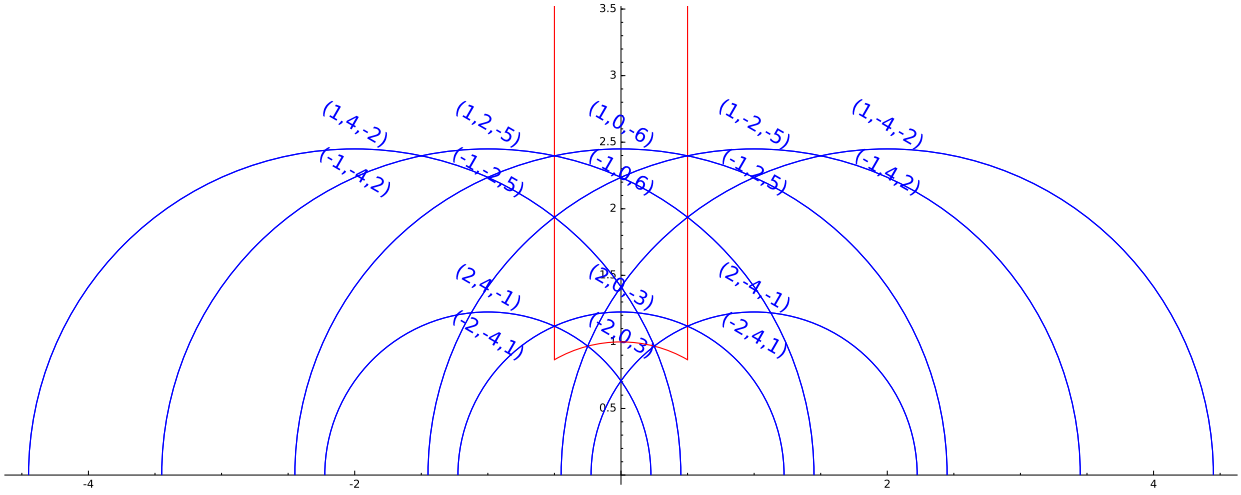

Figure 5.3: Semicircles corresponding to Siegel-reduced forms of discriminant 24

There are two equivalence classes for $\Delta = 24$ and indeed applying the map we get two cycles:

Cycle 1: $(1,-4,-2) \overset{\text{left}}{\underset{S}{\to}} (-2,4,1) \overset{\text{right}}{\underset{T_1}{\to}} (-2,0,3) \overset{\text{right}}{\underset{T_1}{\to}} (-2,-4,1) \overset{\text{right}}{\underset{S}{\to}} (1,4,-2) \overset{\text{left}}{\underset{T_{-1}}{\to}} (1,2,-5) \overset{\text{left}}{\underset{T_{-1}}{\to}} (1,0,-6) \overset{\text{left}}{\underset{T_{-1}}{\to}} (1,-2,-5) \overset{\text{left}}{\underset{T_{-1}}{\to}} (1,-4,-2)$

Cycle 2: $(-1,4,2) \overset{\text{right}}{\underset{T_1}{\to}} (-1,2,5) \overset{\text{right}}{\underset{T_1}{\to}} (-1,0,6) \overset{\text{right}}{\underset{T_1}{\to}} (-1,-2,5) \overset{\text{right}}{\underset{T_1}{\to}} (-1,-4,2) \overset{\text{left}}{\underset{S}{\to}} (2,4,-1) \overset{\text{left}}{\underset{T_{-1}}{\to}} (2,0,-3) \overset{\text{left}}{\underset{T_{-1}}{\to}} (2,-4,-1) \overset{\text{right}}{\underset{T_{-1}}{\to}} (-1,4,2)$

Although this idea seems to work well for most binary forms of $\Delta < 100$, a problem arises when a circle intersects a vertex. The question then becomes, does it count as intersecting the wall, the circle, both, or does it need a different rule completely? Before exploring these problematic forms, we provide a table for those that don't intersect the vertices of $\mathcal{F}$.

Theorem 5. *Let Δ be a discriminant in which none of the reduced forms intersect a vertex of $\mathcal{F}$ and let $S^*(\Delta)$ denote the set of Siegel-reduced forms of discriminant Δ. The reduction operator permutes the forms in $S^*(\Delta)$.*

Proof. We know by definition of our operator that it maps S^* into S^* so all that is left to show is that this mapping is surjective.
Let $Q \in S^*$ and travel along its corresponding circle in the reverse direction. This will give a matrix M that depends on where the circle intersects $\mathcal{F}$ and will send Q to $Q|_M$. Now consider the form $Q|_M \in S^*$. The operation corresponding to traveling along $Q|_M$ in the proper direction will be M^{-1} and as such we have $(Q|_M)|_{M^{-1}} = Q$. □

Δ	No.	Cycle
5	1	$(1,-1,-1)(-1,1,1)(-1,-1,1)(1,1,-1)$
8	1	$(1,-2,-1)(-1,2,1)(-1,0,2)(-1,-2,1)(1,2,-1)(1,0,-2)$
12	2	Not applicable
13	1	$(1,-3,-1)(-1,3,1)(-1,1,3)(-1,-1,3)(-1,-3,1)(1,3,-1)(1,1,-3)(1,-1,-3)$
17	1	$(1,-3,-2)(-2,3,1)(-2,-1,2)(2,1,-2)(2,-3,-1)(-1,3,2)(-1,1,4)(-1,-1,4)(-1,-3,2)$ $(2,3,-1)(2,-1,-2)(-2,1,2)(-2,-3,1)(1,3,-2)(1,1,-4)(1,-1,-4)$
21	1	$(1,-5,1)(1,5,1)(1,3,-3)(1,1,-5)(1,-1,-5)(1,-3,-3)(1,-5,1)$
	2	$(-1,5,-1)(-1,3,3)(-1,1,5)(-1,-3,3)(-1,-5,-1)$
24	1	$(1,-4,-2)(-2,4,1)(-2,0,3)(-2,-4,1)(1,4,-2)(1,2,-5)(1,0,-6)(1,-2,-5)$
	2	$(-1,4,2)(-1,2,5)(-1,0,6)(-1,-2,5)(-1,-4,2)(2,4,-1)(2,0,-3)(2,-4,-1)$
28	2	Not applicable
29	1	$(1,-5,-1)(-1,5,1)(-1,3,5)(-1,1,7)(-1,-1,7)(-1,-3,5)(-1,-5,1)(1,5,-1)(1,3,-5)$ $(1,1,-7)(1,-3,-5)$
33	1	$(1,-5,-2)(-2,5,1)(-2,1,4)(-2,-3,3)(3,3,-2)(3,-3,-2)(-2,3,3)(-2,-2,4)(-2,-5,1)$ $(1,5,-2)(1,3,-6)(1,1,-8)(1,-1,-8)(1,-3,-6)$
	2	$(-1,5,2)(-1,3,6)(-1,1,8)(-1,-1,8)(-1,-3,6)(-1,-5,2)(2,5,-1)(2,2,-4)(2,-3,-3)$ $(-3,3,2)(-3,-3,2)(2,3,-3)(2,-1,-4)(2,-5,-1)$
37	1	$(1,-5,-3)(-3,5,1)(-3,-1,3)(3,1,-3)(3,-5,-1)(-1,5,3)(-1,3,7)(-1,1,9)(-1,-1,9)$ $(-1,-3,7)(-1,-5,3)(3,5,-1)(3,-1,-3)(-3,1,3)(-3,-5,1)(1,5,-3)(1,3,-7)(1,1,-9)$ $(1,-1,-9)(1,-3,-7)$
40	1	$(1,-6,-1)(-1,6,1)(-1,4,6)(-1,2,9)(-1,0,10)(-1,-2,9)(-1,-4,6)(-1,-6,1)(1,6,-1)$ $(1,4,-6)(1,2,-9)(1,0,-10)(1,-2,-9)(1,-4,-6)$
	2	$(2,-4,-3)(-3,4,2)(-3,-2,3)(3,2,-3)(3,-4,-2)(-2,4,3)(-2,0,5)$ $(-2,-4,3)(3,4,-2)(3,-2,-3)(-3,2,3)(-3,-4,2)(2,4,-3)(2,0,-5)$
41	1	$(1,-7,2)(2,7,1)(2,3,-4)(2,-1,-5)(2,-5,-2)(-2,5,2)(-2,1,5)(-2,-3,4)(-2,-7,-1)$ $(-1,7,-2)(-1,5,4)(-1,3,8)(-1,1,10)(-1,-1,10)(-1,-3,8)(-1,-5,4)(-1,-7,-2)$ $(-2,7,-1)(-2,3,4)(-2,-1,5)(-2,-5,2)(2,5,-2)(2,1,-5)(2,-3,-4)(-1,-7,-2)$ $(2,-7,1)(1,7,2)(1,5,-4)(1,3,-8)(1,1,-10)(1,-1,-10)(1,-3,-8)(1,-5,-4)$
44	1	$(1,-6,-2)(-2,6,1)(-2,2,5)(-2,-2,5)(-2,-6,1)(1,6,-2)(1,4,-7)(1,2,-10)(1,0,-11)$ $(1,-2,-10)(1,-4,-7)$
	2	$(-1,6,2)(-1,4,7)(-1,2,10)(-1,0,11)(-1,-2,10)(-1,-4,7)(-1,-6,2)(2,6,-1)$ $(2,2,-5)(2,-2,-5)(2,-6,-1)$
53	1	$(1,-7,-1)(-1,7,1)(-1,5,7)(-1,3,11)(-1,1,13)(-1,-1,13)(-1,-3,11)(-1,-5,7)$ $(-1,-7,1)(1,7,-1)(1,5,-7)(1,3,-11)(1,1,-13)(1,-1,-13)(1,-3,-11)(1,-5,-7)$
56	1	$(1,-8,2)(2,8,1)(2,4,-5)(2,0,-7)(2,-4,-5)(2,-8,1)(1,8,2)(1,6,-5)(1,4,-10)$ $(1,2,-13)(1,0,-14)(1,-2,-13)(1,-4,-10)(1,-6,-5)(1,-8,2)$
	2	$(-1,8,-2)(-1,8,-2)(-1,6,5)(-1,4,10)(-1,2,13)(-1,0,14)(-1,-2,13)(-1,-4,10)$ $(-1,-6,5)(-1,-8,-2)(-2,8,-1)(-2,4,5)(-2,0,7)(-2,-4,5)(-2,-8,-1)$

Δ	No.	Cycle
57	1	$(1,-7,-2)(-2,7,1)(-2,3,6)(-2,-1,7)(-2,-5,4)(4,5,-2)(4,-3,-3)(-3,3,4)$ $(-3,-3,4)(4,3,-3)(4,-5,-2)(-2,5,4)(-2,1,7)(-2,-3,6)(-2,-7,1)(1,7,-2)(1,5,-8)$ $(1,3,-12)(1,1,-14)(1,-1,-14)(1,-3,-12)(1,-5,-8)$
	2	$(-1,7,2)(-1,5,8)(-1,3,12)(-1,1,14)(-1,-1,14)(-1,-3,12)(-1,-5,8)(-1,-7,2)$ $(2,7,-1)(2,3,-6)(2,-1,-7)(2,-5,-4)(-4,5,2)(-4,-3,3)(3,3,-4)(3,-3,-4)(-4,3,3)$ $(-4,-5,2)(2,5,-4)(2,1,-7)(2,-3,-6)(2,-7,-1)$
60	1	$(1,-8,1)(1,8,1)(1,6,-6)(1,4,-11)(1,2,-14)(1,0,-15)(1,-2,-14)(1,-4,-11)$ $(1,-6,-6)$
	2	$(-1,8,-1)(-1,6,6)(-1,4,11)(-1,2,14)(-1,0,15)(-1,-2,14)(-1,-4,11)(-1,-6,6)$ $(-1,-8,-1)$
	3	$(2,-6,-3)(-3,6,2)(-3,0,5)(-3,-6,2)(2,6,-3)(2,2,-7)(2,-2,-7)$
	4	$(-2,6,3)(-2,2,7)(-2,-2,7)(-2,-6,3)(3,6,-2)(3,0,-5)(3,-6,-2)$
61	1	$(1,-7,-3)(-3,7,1)(-3,1,5)(-3,-5,3)(3,5,-3)(3,-1,-5)(3,-7,-1)(-1,7,3)(-1,5,9)$ $(-1,3,13)(-1,1,15)(-1,-1,-15)(-1,-3,13)(-1,-5,9)(-1,-7,3)(3,7,-1)(3,1,-5)$ $(3,-5,-3)(-3,5,3)(-3,-1,5)(-3,-7,1)(1,7,-3)(1,5,-9)(1,3,-13)(1,1,-15)$ $(1,-1,-15)(1,-3,-13)(1,-5,-9)$
65	1	$(1,-7,-4)(-4,7,1)(-4,-1,4)(4,1,-4)(4,-7,-1)(-1,7,4)(-1,5,10)(-1,3,14)$ $(-1,1,16)(-1,-1,16)(-1,-3,14)(-1,-5,10)(-1,-7,4)(4,7,-1)(4,-1,-4)(-4,1,4)$ $(-4,-7,1)(1,7,-4)(1,5,-10)(1,3,-14)(1,1,-16)(1,-1,-16)(1,-3,-14)(1,-5,-10)$
	2	$(2,-9,2)(2,9,2)(2,5,-5)(2,1,-8)(2,-3,-7)(2,-7,-2)(-2,7,2)(-2,3,7)(-2,-1,8)$ $(-2,-5,5)(-2,-9,-2)(-2,9,-2)(-2,5,5)(-2,1,8)(-2,-3,7)(-2,-7,2)(2,7,-2)$ $(2,3,-7)(2,-1,-8)(2,-5,-5)$
69	1	$(1,-9,3)(3,9,1)(3,3,-5)(3,-3,-5)(3,-9,1)(1,9,3)(1,7,-5)(1,5,-11)(1,3,-15)$ $(1,1,-17)(1,-1,-17)(1,-3,-15)(1,-5,-11)(1,-7,-5)$
	2	$(-1,9,-3)(-1,7,7)(-1,5,11)(-1,3,15)(-1,1,17)(-1,-1,17)(-1,-3,15)(-1,-5,11)$ $(-1,-7,5)(-1,-9,-3)(-3,9,-1)(-3,3,5)(-3,-3,5)(-3,-9,-1)$
73	1	$(1,-9,2)(2,9,1)(2,5,-6)(2,1,-9)(2,-3,-8)(2,-7,-3)(-3,7,2)(-3,1,6)(-3,-5,4)$ $(4,5,-3)(4,-3,-4)(-4,3,4)(-4,-5,3)(3,5,-4)(3,-1,-6)(3,-7,-2)(-2,7,3)(-2,3,8)$ $(-2,-1,9)(-2,-5,6)(-2,-9,-1)(-1,9,-2)(-1,7,6)(-1,5,12)(-1,3,16)(-1,1,18)$ $(-1,-1,18)(-1,-3,16)(-1,-5,12)(-1,-7,6)(-1,-9,-2)(-2,9,-1)(-2,5,6)(-2,1,9)$ $(-2,-3,8)(-2,-7,3)(3,7,-2)(3,1,-6)(3,-5,-4)(-4,5,3)(-4,-3,4)(4,3,-4)$ $(4,-5,-3)(-3,5,4)(-3,-1,6)(-3,-7,2)(2,7,-3)(2,3,-8)(2,-1,-9)(2,-5,-6)$ $(2,-9,1)(1,9,2)(1,7,-6)(1,5,-12)(1,3,-16)(1,1,-18)(1,-1,-18)(1,-3,-16)$ $(1,-5,-12)(1,-7,-6)$
76		Not applicable
77	1	$(1,-9,1)(1,9,1)(1,7,-7)(1,5,-13)(1,3,-17)(1,1,-19)(1,-1,-19)(1,-3,-17)$ $(1,-5,-13)(1,-7,-7)$
	2	$(-1,9,-1)(-1,7,7)(-1,5,13)(-1,3,17)(-1,1,19)(-1,-1,19)(-1,-3,17)(-1,-5,13)$ $(-1,-7,7)(-1,-9,-1)$

Δ	No.	Cycle
85	1	$(1,-9,-1)(-1,9,1)(-1,7,9)(-1,5,15)(-1,3,19)(-1,1,21)(-1,-1,21)(-1,-3,19)$ $(-1,-5,15)(-1,-7,9)(-1,-9,1)(1,9,-1)(1,7,-9)(1,5,-15)(1,3,-19)(1,1,-21)$ $(1,-3,-19)(1,-5,-15)(1,-7,-9)(1,-9,-1)$
	2	$(3,-7,-3)(-3,7,3)(-3,1,7)(-3,-5,5)(5,5,-3)(5,-5,-3)(-3,5,5)(-3,-1,7)$ $(-3,-7,3)(3,7,-3)(3,1,-7)(3,-5,-5)(-5,5,3)(-5,-5,3)(3,5,-5)(3,-1,-7)$ $(3,-7,-3)$
88	1	$(1,-10,3)(3,10,1)(3,4,-6)(3,-2,-7)(3,-8,-2)(-2,8,3)(-2,4,9)(-2,0,11)(-2,-4,9)$ $(-2,-8,3)(3,8,-2)(3,2,-7)(2,-4,-6)(3,-10,1)(1,10,3)(1,8,-6)(1,6,-13)(1,4,-18)$ $(1,2,-21)(1,0,-22)(1,-2,-21)(1,-4,-18)(1,-6,-13)(1,-8,-6)$
	2	$(-1,10,-3)(-1,8,6)(-1,6,13)(-1,4,18)(-1,2,21)(-1,0,22)(-1,-2,21)(-1,-4,18)$ $(-1,-6,13)(-1,-8,6)(-1,-10,-3)(-3,10,-1)(-2,4,6)(-3,-2,7)(-3,-8,2)(2,8,-3)$ $(2,4,-9)(2,0,-11)(2,-4,-9)(2,-8,-3)(-3,8,2)(-3,2,7)(-3,-4,6)(-3,-10,-1)$
89	1	$(1,-9,-2)(-2,9,1)(-2,5,8)(-2,1,11)(-2,-3,10)(-2,-7,5)(5,7,-2)(5,-3,-4)$ $(-4,3,5)(-4,-5,4)(4,5,-4)(4,-3,-5)(-5,3,4)(-5,-7,2)(2,7,-5)(2,3,-10)$ $(2,-1,-11)(2,-5,-8)(2,-9,-1)(-1,9,2)(-1,7,10)(-1,5,16)(-1,3,20)(-1,1,22)$ $(-1,-1,22)(-1,-3,20)(-1,-5,16)(-1,-7,10)(-1,-9,2)(2,9,-1)(2,5,-8)(2,1,-11)$ $(2,-3,-10)(2,-7,-5)(-5,7,2)(-5,-3,4)(4,3,-5)(4,-5,-4)(-4,5,4)(-4,-3,5)$ $(5,3,-4)(5,-7,-2)(-2,7,5)(-2,3,10)(-2,-1,11)(-2,-5,8)(-2,-9,1)(1,9,-2)$ $(1,7,-10)(1,5,-16)(1,3,-20)(1,1,-22)(1,-1,-22)(1,-3,-20)(1,-5,-16)(1,-7,-10)$
92	1	$(1,-10,2)(2,10,1)(2,6,-7)(2,2,-11)(2,-2,-11)(2,-6,-7)(2,-10,1)(1,10,2)$ $(1,8,-7)(1,6,-14)(1,4,-19)(1,2,-22)(1,0,-23)(1,-2,-22)(1,-4,-19)(1,-6,-14)$ $(1,-8,-7)$
	2	$(-1,10,-2)(-1,8,7)(-1,6,14)(-1,4,19)(-1,2,22)(-1,0,23)(-1,-2,22)(-1,-4,19)$ $(-1,-6,14)(-1,-8,7)(-1,-10,-2)(-2,10,-1)(-2,6,7)(-2,2,11)(-2,-2,11)$ $(-2,-6,7)(-2,-10,-1)$
93	1	$(1,-9,-3)(-3,9,1)(-3,3,7)(-3,-3,7)(-3,-9,1)(1,9,-3)(1,7,-11)(1,5,-17)$ $(1,3,-21)(1,1,-23)(1,-1,-23)(1,-3,-21)(1,-5,-17)(1,-7,-11)$
	2	$(-1,9,3)(-1,7,11)(-1,5,17)(-1,3,21)(-1,1,23)(-1,-1,23)(-1,-3,21)(-1,-5,17)$ $(-1,-7,11)(-1,-9,3)(3,9,-1)(3,3,-7)(3,-3,-7)(3,-9,-1)$
97	1	$(1,-9,-4)(-4,9,1)(-4,1,6)(-4,-7,3)(3,7,-4)(3,1,-8)(3,-5,-6)(3,-11,2)(2,11,3)$ $(2,7,-6)(2,3,-11)(2,-1,-12)(2,-5,-9)(2,-9,-2)(-2,9,2)(-2,5,9)(-2,1,12)$ $(-2,-3,11)(-2,-7,6)(-2,-11,-3)(-3,11,-2)(-3,5,6)(-3,-1,8)(-3,-7,4)(4,7,-3)$ $(4,-1,-6)(4,-9,-1)(-1,9,4)(-1,7,12)(-1,5,18)(-1,3,22)(-1,1,24)(-1,-1,24)$ $(-1,-3,22)(-1,-5,18)(-1,-7,12)(-1,-9,4)(4,9,-1)(4,1,-6)(4,-7,-3)(-3,7,4)$ $(-3,1,8)(-3,-5,6)(-3,-11,-2)(-2,11,-3)(-2,7,6)(-2,3,11)(-2,-1,12)(-2,-5,9)$ $(-2,-9,2)(2,9,-2)(2,5,-9)(2,1,-12)(2,-3,-11)(2,-7,-6)(2,-11,3)(3,11,2)$ $(3,5,-6)(3,-1,-8)(3,-7,-4)(-4,7,3)(-4,-1,6)(-4,-9,1)(1,9,-4)(1,7,-12)$ $(1,5,-18)(1,3,-22)(1,1,-24)(1,-1,-24)(1,-3,-22)(1,-5,-18)(1,-7,-12)$

Table 5.2: Cycles of Siegel-reduced forms with $\Delta < 100$

4 Partitioning the Axes

Our initial proposed solution to this problem of intersecting the vertex was to find a reduction method that doesn't necessarily look at intersecting the walls or unit circle, but one that will still preserve our idea of what to do in the above cases.
Since our definition of a reduced form deals with intersecting the fundamental domain $\mathcal{F}$, we decided to look at transformations of $\mathcal{F}$ using the matrices T_n and S. Keeping our convention on which direction to move on the circle, we can instead partition the axes into these transformations of $\mathcal{F}$. The picture looks like the following.

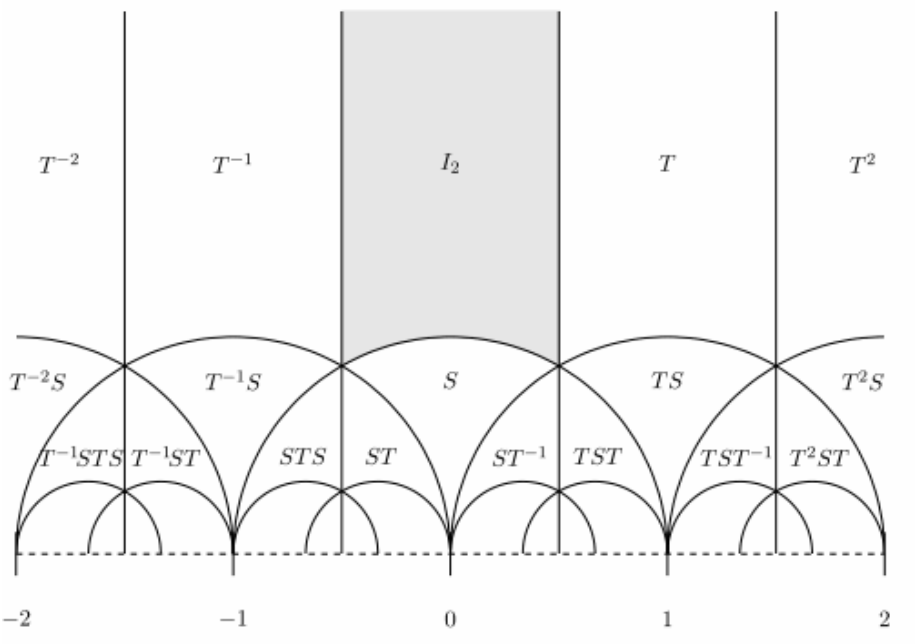

Figure 5.4: Transformations of the fundamental domain where T corresponds to T_1. (source: `www.math.uconn.edu/~kconrad/blurbs/grouptheory/SL(2,Z).pdf`)

When applying the reduction operator to a form we then look at which transformation of $\mathcal{F}$ the circle enters and apply its inverse. This method preserves our first set of rules because if a form intersects the wall (not on the vertex), it passes into a shifted version of the fundamental domain. If the form intersects the unit circle, it will pass into the reflected version of the fundamental domain. While this method seems good in theory, the application of it doesn't exactly work out. In many cases such as the following, the cycle loops back around on itself before hitting all the necessary quadratic forms.

Example 6. $\Delta = 12$

The Siegel-reduced forms are given by:

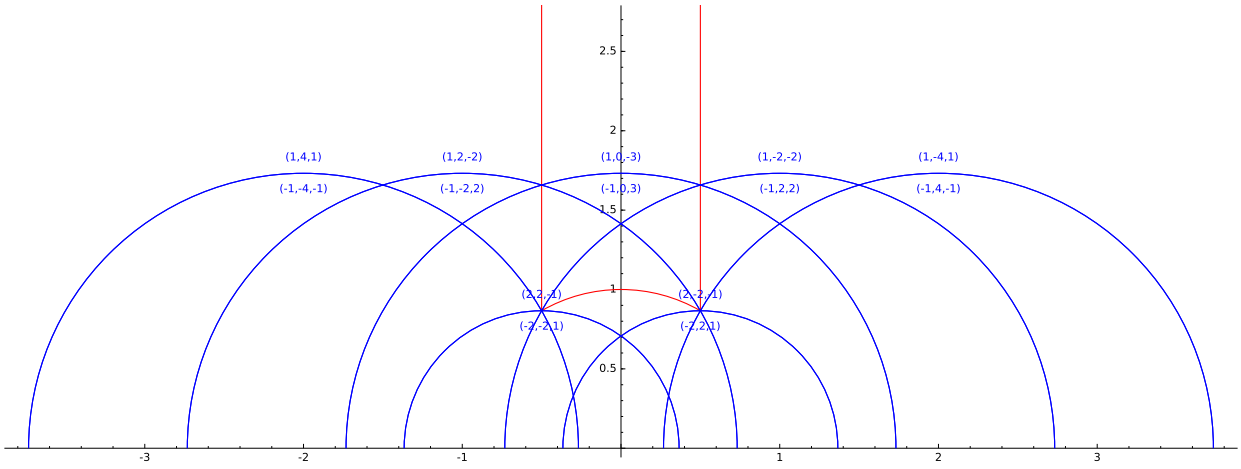

Figure 5.5: Semicircles corresponding to Siegel-reduced forms of discriminant 12

Starting with circle corresponding to the form $(1, -4, 1)$ and applying the above method yields the following cycle:

$$(1,-4,1) \xrightarrow{ST_{-1}} (1,2,-2) \xrightarrow{T_{-1}} (1,0,-3) \xrightarrow{T_{-1}} (1,-2,-2) \xrightarrow{ST_1S} (1,-4,1)$$

Bibliography

[Lem10] Franz Lemmermeyer, *Binary quadratic forms*, `www.rzuser.uni-heidelberg.de/{~}hb3/publ/bf.pdf`, 2010.

[SR55] Carl Ludwig Siegel and KG Ramanathan, *Lectures on quadratic forms*, vol. 7, Tata Institute of Fundamental Research, 1955.