A PROJECT REPORT
ON

"On binary quadratic forms- It's reduction and questions concerning it"'

BY
IRISH DEBBARMA

UNDER THE GUIDANCE OF
Prof. B. Sury

Department of Mathematics
Indian Statistical Institute, Bangalore

ACKNOWLEDGEMENT

I would like to thank **Professor B. Sury** for his expert guidance and continous engagement and encouragement throughout the length of this project; for making sure that I could reach the goal of the project in a structured and fruitful manner.

Irish Debbarma

CERTIFICATE

This is to certify that the project titled

"On binary quadratic forms- It's reduction and questions concerning it"

submitted by

Irish Debbarma

is a record of bonafide work carried out by him. This work is done during year 2020, under my guidance.

Date: / /

(**Professor B.Sury**)

Contents

Chapter 1

Introduction

1.1 Aim

The project is focused on understanding binary quadratic forms and the various questions that naturally get asked regarding them.

1.2 Motivation

As a first year undergraduate with an interest in number theory, I went ahead to explore quadratic reciprocity and binary quadratic forms. Prof. Sury suggested that I should try to understand Zagier's proof as it is a very beautiful proof and can be understood with my knowledge of binary quadratic forms.

1.3 Overview

I learnt and present the following:

1. **Quadratic forms and Linear algebra in reduction theory:** Definition of a binary quadratic form, discriminant, representation by a form which also includes different types of representation. Next we focus on the different types of forms based on what numbers (positive or negative) they can represent and put on some conditions on the discriminant to decide when it represents which kind of numbers. We then introduce the very essential modular group and how its actions affect the coefficients. We also provide a matrix representation of a form and definition of a class number.

2. **Langrange reduction:** Reduced in the sense of Langrange, bounds on the coefficients, reduction of positive definite forms and Legendre's Lemma.

3. **Representations by quadratic forms:** What is a principal form, what is and when is a discriminant fundamental. Link between representation of a prime by a form and "quadratic residue-ness" of the discriminant with respect to the prime.

4. **Zagier's reduction:** Reduced in the sense of Zagier, followed by bounds on the coefficients. And search for a structure to define equivalence among forms, which leads to the reduction operator and the cycle generated by it. Definition of a semi-reduced form and the ultimate fundamental lemma that establishes what it means for two forms to be equivalent.

5. **Gauss reduction:** Very similar to Zagier's reduction. Both deal with reduction of indefinite forms. First as usual we define what it means to be reduced in terms of Gauss and then try to find some analogue to Zagier's theory.

6. **Interpreting Zagier's proof of two squares theorem using binary quadratic form:** First we focus on the proof given by Zagier, that is what the involution is, whether it works as it should and lay out the details which he chose to omit in the proof. A similar analysis of Heath-Brown's proof is also provided. Further, we interpret it using quadratic forms. First we redefine the involution in terms of coefficients of the forms and then introduce a function that does the required mapping as in the case of Zagier's proof.

7. **Gauss's class number problem:** We prove a few simple results and build up a few theorems on that. In the process we come across Euler's prime generating polynomial which has some interesting links to the initial results that we prove.

Chapter 2

Detailed Topics

2.1 Quadratic forms and linear algebra in reduction theory

2.1.1 Quadratic forms

Here, we will discuss what a binary quadratic form is and what representation of a number by binary quadratic form means.
Forms are polynomials $Q(x_1, x_2, \ldots x_s)$ with degree n. It is a sum of monomials $x_1^{r_1} x_2^{r_2} x_3^{r_3} \ldots x_s^{r_s}$ with $r_1 + r_2 + r_3 \ldots r_s = n$. And a **quadratic form** is an expression of the form $\sum_{i,j} c_{ij} x_i x_j$ where $0 \leq i, j \leq s$ and c_{ij} is from some domain.
Hence, **binary quadratic forms** are *quadratic forms* in two variables x, y. It can be expressed as

$$F(x, y) = Ax^2 + Bxy + Cy^2$$

$F(x, y)$ is also written as (A, B, C). We focus our study to very specific binary quadratic forms, the ones with $A, B, C \in \mathbb{Z}$.
We define $\Delta = B^2 - 4AC$ as the *discriminant* of the form (A, B, C). A number n is said to be **represented** by the form F if and only if $F(x, y) = n$ for some integers x, y, and n is said to be *represented primitively* by F if there exists coprime integers r, s such that $F(r, s) = n$.
A form $F(x, y) = (A, B, C)$ is said to be *primitive* if $\gcd(A, B, C) = 1$. In the course of my report we will primarily focus on primitive binary quadratic forms and primitive representation of integers by such forms.

Given a form F we have certain teminologies:

- A form is said to be *indefinite* if it takes both positive and negative values
- A form is said to be *positive semidefinite* (*negative semidefinite*) if the form $F(x, y) \geq 0 (F(x, y) \leq 0)$ for all integers x, y
- A *semidefinite* form is said to be definite if in addition the only integers x, y for which $F(x, y) = 0$ are $x = 0, y = 0$

This leads us to the

Theorem 1. *Let $F(x, y) = Ax^2 + Bxy + Cy^2$ then*

- *If the discriminant Δ is greater than 0, then F is indefinite*
- *If the discriminant Δ is equal to 0, then F is semidefinite*
- *If the discriminant $\Delta < 0$ and $A < 0$ then F is negative definite and if $\Delta < 0$ and $A > 0$ then F is positive definite*

2.1.2 Linear algebra in reduction theory

Modular group action. There is a special linear group also known as *modular group*, a matrix group which has determinant 1 and whose elements are all integers.

$$SL_2\mathbb{Z} = \{\begin{pmatrix} r & s \\ t & u \end{pmatrix} \mid r, s, t, u \in \mathbb{Z} \text{ and } ru - ts = 1\}$$

Forms F and G are said to be equivalent to one another if $F(x, y) = G((x, y)T^T) = G(rx + sy, tx + uy)$ where $T \in SL_2\mathbb{Z}$ and T^T is transpose of T. If $F(x, y) = (A, B, C)$ and $G(x, y) = (A', B', C')$ then from calculations we can see that

$$\begin{aligned} A' &= Ar^2 + Brt + Ct^2 && (2.1) \\ B' &= A(2rs) + B(ru + st) + C(2tu) && (2.2) \\ C' &= As^2 + Bsu + Cu^2 && (2.3) \end{aligned}$$

Coefficient matrix. Every form $F(x, y) = (A, B, C)$ can be assigned matrices

$$m(F) = \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \text{ and } M(F) = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$$
$$4F = (x\ y)m(F)\begin{pmatrix} x \\ y \end{pmatrix} \text{ and } F = (x\ y)M(F)\begin{pmatrix} x \\ y \end{pmatrix}$$

Now, we observe the action of *modular group* on the coefficient matrix. If F and G are equivalent matrices then

$$G = T^T M(F) T$$

where $T \in SL_2\mathbb{Z}$ and T^T is transpose of T.
It can be shown that *equivalent* forms represent exactly the same numbers primitively. *Equivalent* forms have the same discriminant, if a primitive form F is equivalent to G then G is also primitive. This leads us to the classification of forms into *equivalence classes*. Building up on this we define **class number** as the number of equivalence classes of primitive forms with discriminant Δ and we use $h(\Delta)$ to denote it.

Next, we will focus on reducing forms from one to another. Our target is to transform forms with large coefficients into forms with smaller coefficients which is the objective of **Langrange reduction**, or try to find a structure to somehow classify the forms into categories as in **Zagier's reduction**.

2.2 Langrange reduction

We want to know if the class number for a given determinant is finite or not also if a particular equivalence class has a "simplest" form. As we proceed further we will see that this is indeed the case for negative determinants. It is seen that the minimal possible number represented by the forms in a class is related to the minimal possible value of A for all forms (A, B, C) in that class.

Bounds on coefficients. The paper is able to find some bounds on the coefficients of the binary quadratic forms as stated below.

- There is a form (A, B, C) in each equivalence class with $|B| \leq |A| \leq |C|$, and such a form is known as *Langrange-reduced* form. So, we are able to say that every form can be reduced to a *Langrange-reduced* form.

- A *Langrange-reduced* form with $\Delta > 0$ has $|A| \leq \frac{\sqrt{\Delta}}{2}$, $|B| \leq \sqrt{\frac{\Delta}{5}}$ and $|C| \leq \frac{\Delta}{4}$
- A *Langrange-reduced* form with $\Delta < 0$ has $|A| \leq \sqrt{\frac{-\Delta}{3}}$, $|B| \leq \sqrt{\frac{-\Delta}{3}}$ and $|C| \leq \frac{1-\Delta}{4}$

These bounds suggest that there are only finitely many *Langrange-reduced* forms which in turn means finite number of equivalence classes.
The bound is improved in case of indefinite primitive forms (A, B, C) with $AC < 0$ and $0 \leq B \leq |A| \leq |C|$. In such cases $(A, B, C) \sim (1, 1, -1)$ or $|A| \leq \sqrt{\frac{\Delta}{8}}$.

Reduction of positive definite forms. The reduction of positive definite forms is simpler as compared to others and hence we will try to understand it first. So, we are dealing with forms $F = (A, B, C)$ with $A > 0$ and $\Delta = B^2 - 4AC < 0$, additionally we wil only focus on forms with $\gcd(A, B, C) = 1$ or primitive forms.
We know that there are finite number of equivalence classes and now we ask the question whether there exists unique reduced form for each equivalence class. The answer turns out to be 'yes'. The existence proof of this uses our previously proven fact that each equivalence class contains a *Langrange-reduced* form, and the uniqueness theorem is proven using **Legendre's Lemma**.

Lemma 1. (*Legendre's Lemma*): *If a form $F = (A, B, C)$ is reduced then the three smallest integers primitively represented by F are $A, C, A - |B| + C$. More precisely, $A = F(\pm 1, 0)$, $C = F(0, \pm 1)$ and $A - |B| + C = F(\pm 1, \mp 1)$, also*

$$
\begin{aligned}
&F(x, y) \geq A && \text{for } (x, y) \neq (0, 0), (\pm 1, 0) \\
&F(x, y) \geq C && \text{for } (x, y) \neq (0, 0), (0, \pm 1), (\pm 1, 0) \\
&F(x, y) \geq A - |B| + C && \text{for } (x, y) \neq (0, 0), (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)
\end{aligned}
$$

2.3 Representations by Quadratic forms

. We know from section 2.1.1 what it means for a number to be represented by a form. Here, we focus on certain classical results regarding representation of primes by certain binary quadratic forms. First we define what a **principal form** is.

$\Delta = B^2 - 4AC \equiv 0, 1 \pmod 4$ hence $\Delta = -4m$ or $\Delta = 1 - 4m$ for some $m \in \mathbb{Z}$. Therefore, a *principal form* F_0 is defined as

$$F_0 = \begin{cases} (1, 0, m) & \text{for } \Delta = -4m \\ (1, 1, m) & \text{for } \Delta = 1 - 4m \end{cases}$$

We have the following lemma:

Lemma 2. *For a discriminant Δ, the following statements are equivalent:*

1. *$p | F_0(a, b)$ for a pair of coprime integers a, b*
2. *$\left(\frac{\Delta}{p}\right) \neq -1$*
3. *There is a quadratic form $F = (p, B, C)$ with discriminant Δ*
4. *There is a quadratic form F with discriminant Δ that primitively represents p*

Definition: A discriminant Δ is said to be *fundamental* if every form with discriminant Δ is primitive.
It can be proven that a discriminant Δ is *fundamental* if and only if Δ is square-free.

Lemma 3. *A discriminant Δ is fundamental if and only if*

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

with m squarefree.

Following up we have the powerful proposition.

Proposition 1. *If $\left(\frac{\Delta}{p}\right) \neq -1$ for some prime p, then p is represented by a Langrange-reduced form with discriminant Δ.*

As a direct consequence to this proposition we have the following: If m divides a sum of two coprime squares, then m itself can be written as a sum of two squares.

2.4 Zagier's reduction

We now focus our concern to the reduction of indefinite binary quadratic forms. In case of definite forms we have we had Langrange's theory that allowed us to have a unique reduced form for each equivalence class. The objective here is also the same, to define what *reduced* means in case of indefinite forms so that we can obtain in the best case one unique reduced form per equivalence class or atleast small number of reduced forms per equivalence class. To this effect there have been many attempts and it has been seen that it serves us better to have *more* reduced forms as it provides us with a *better* mathematical *structure* which is more valued than cardinality.
We have **Gauss's theory**, **Langrange's theory** and **Zagier's theory**. Gauss's classical theory is the more suitable one for calculation as it's coefficients are smaller but Zagier's thoery has proven more elegant and in this part we are going to discuss that, the following section will take us to the classical theory of Gauss.
Consider the form $F = (A, B, C)$, now if it were to be reduced according to **Langrange's theory** then in a particular equivalence class we would pick the minimal $|A|$ and reduce B modulo $2A$ to find a minimal B. We do something very similar here. We choose the minimal $A > 0$ and B is reduced modulo $2A$ which means $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2A]$, if this is so then $4AC = B^2 - \Delta > 0 \Rightarrow AC > 0 \Rightarrow C > 0$. By the minimality of A we have that $C \leq A$ and since the dlip operation can be performed on the coefficients therefore $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2C]$.
Summing all this up we can say that a form $F = (A, B, C)$ with positive nonsquare discriminant can be called *Zagier reduced*(*Z-reduced*) if the following conditions are met.

- $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2A]$
- $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2C]$

Bounds on coefficients. The number of *Z-reduced* forms with discriminant Δ is called the *calibre* of the discriminant and is denoted by κ_Z. From calculations we find that κ_Z increases at a very rapid rate, almost $\dfrac{\Delta}{4}$ or even more.
The author presents further conditions on the coefficients of the *Z-reduced* forms which is captured in the below theorem

Theorem 2. *Let $F = (A, B, C)$ be a primitive indefinite binary quadratic form with discriminant $\Delta = B^2 - 4AC$ and let $\epsilon_1 = \frac{B-\sqrt{\Delta}}{2A}$ and $\epsilon_2 = \frac{B+\sqrt{\Delta}}{2A}$ be the*

roots of the equation $F(x,-1) = Ax^2 - Bx + C = 0$. *Then the following statements are equivalent*

$$(A,B,C) \text{ is Z-reduced}$$
$$(C,B,A) \text{ is Z-reduced}$$
$$0 < B - \sqrt{\Delta} < 2A < B + \sqrt{\Delta}$$
$$0 < B - \sqrt{\Delta} < 2C < B + \sqrt{\Delta}$$
$$0 < \epsilon_1 < 1 < \epsilon_2$$
$$A > 0, C > 0, B > A + C$$

These results help us to put bounds on the coefficients of the *Z-reduced* forms in the form of the following proposition.

Proposition 2. *There are only finitely many Z-reduced forms with a discriminant* Δ. *The coefficients of the Z-reduced forms have the following conditions:* $0 < A < C \leq \frac{\Delta}{4}$ *and* $\sqrt{\Delta} < B \leq \frac{\Delta+1}{2}$

Proof. Since it is a *Z-reduced* form, from the previous theorem we have $A > 0, C > 0$ and $B > A + C \Rightarrow B - A - C \geq 1$

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

Similarly

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

Now, $B^2 = 4AC + \Delta$ and $AC > 0 \Rightarrow B^2 > \Delta \Rightarrow B > \sqrt{\Delta}$

$B^2 = 4AC + \Delta \leq \frac{\Delta^2}{4} + \Delta < \frac{\Delta^2}{4} + \Delta + 1 = \left(\frac{\Delta+2}{2}\right)^2$

$B < \frac{\Delta+2}{2}$ since B is an integer $B \leq \frac{\Delta+1}{2}$ and the proof is complete. □

Now that we have established the finiteness of the *calibre* of the determinant, we go to the question of equivalence in case of indefinite forms. In the case of definite forms (particularly positive definite forms) each equivalence class had a unique reduced form which is not the case here. So, given a form we apply the reduction operator on it repeatedly

and in the process we obtain cycles. We will prove that two forms are equivalent if they belong to the same cycle.

Reduction map. Let us call $\mathcal{F}_\Delta$ the set of all primitive forms with discriminant Δ and a subset $\mathcal{R}_\Delta$ the set of reduced primitive forms with discriminant Δ then a map $\rho : \mathcal{F}_\Delta \to \mathcal{F}_\Delta$ is called a reduction map if it has the following properties:

- For a form $F \in \mathcal{F}_\Delta$ there exists an integer $\mu > 0$ such that

  $$\rho^\mu(F) = \rho \circ \rho \circ \rho \circ \ldots \rho(F)$$

  is reduced or equivalently for any $\mu > 0$ $\rho^\mu(F) \in \mathcal{R}_\Delta$
- If $F \in \mathcal{R}_\Delta$ then $\rho(F) \in \mathcal{R}_\Delta$ that is ρ maps reduced forms to reduced forms

In such a case, the form $\rho(F)$ is called the **right neighbour** of F and the forms in the image of F are called semi-reduced.

Given a form $F = (A, B, C)$, we can define the right neighbour $\rho(F) = F' = (A', B', C')$ with F' as the product of action of a *modular group* S on F. Here, $S = S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. So, $S \in SL_2\mathbb{Z}$ represents a shift followed by a flip. It is also to be noted that $n - 1 < \frac{B+\sqrt{\Delta}}{2A} < n$.

There is another way of defining a *right-neighbour* without explicitly stating $'n'$. It is as follows

Lemma 4. *The right neighbour of the form $F = (A, B, C)$ can be calculated as follows:*

1. $C' = A$
2. $B + B' \equiv 0 \pmod{2A}$ *and* $\begin{cases} \sqrt{\Delta} < B' < \sqrt{\Delta} + 2A & , A > 0 \\ \sqrt{\Delta} + 2A < B' < \sqrt{\Delta} & , A < 0 \end{cases}$
3. $B'^2 - 4A'C' = \Delta$

Now, we introduce a lemma to prove that ρ is a reduction map

Lemma 5. *Let $F = (A, B, C)$ be a form with positive discriminant Δ and $\rho(F) = F' = (A', B', C')$ be its right neighbour. Then the following are true:*

1. *If* $A < 0$ *then* $A' > A$
2. *If* $A > 0$ *then* $A' > 0$
3. *If* $A' \geq A > 0$*, then* F' *is Z-reduced*
4. *If* F *is Z-reduced then* $\rho(F) = S^T F S$ *for some* $S = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} \in SL_2\mathbb{Z}$ *with* $n \geq 2$

Using this lemma we can prove that ρ is a reduction map. Currently, the map ρ is not injective so we define a new set of forms

Definition 1. A form is said to be **semi-reduced** if
$\begin{cases} \sqrt{\Delta} < B' < \sqrt{\Delta} + 2A & , A > 0 \\ \sqrt{\Delta} + 2A < B' < \sqrt{\Delta} & , A < 0 \end{cases}$

But from lemma 2 we know that applying Zagier reduction on an indefinite form makes it semi-reduced.

Proposition 3. *The map* ρ *is injective is injective on semi-reduced forms*

Proof. Suppose $F_1 = (A_1, B_1, C_1)$ and $F_2 = (A_2, B_2, C_2)$ map to the same form $G = (A, B, C)$. Determinant is invariant under reduction hence F_1, F_2, G have the same discriminant say Δ
First, $C = A_1 = A_2$. And $B_1 + B = 2A_1 n_1$, $B_2 + B = 2A_2 n_2$, which means that $B_2 - B_1 = 2C(n_2 - n_1)$. Also, $|B_1 - \sqrt{\Delta}| < 2C$ and similarly $|B_2 - \sqrt{\Delta}| < 2C$. This implies that $|B_2 - B_1| < 2C$ which means that $n_1 = n_2 \Rightarrow B_1 = B_2$. Since, discriminant is same for both of them therefore we can conclude that $C_1 = C_2$. We can finally conclude that $F_1 = F_2$ or ρ is injective on semi-reduced forms. □

Now, that we have proved that ρ is injective we can define a **left neighbour** $\lambda(F)$ by inverting the reduction map. Suppose $\rho(F) = F'$ then $\lambda(F')$ can be defined in the following
manner$(F = (A, B, C), F' = (A', B', C'))$

1. $A = C'$
2. $B + B' \equiv 0 \pmod{2C'}$ and $\begin{cases} \sqrt{\Delta} < B < \sqrt{\Delta} + 2C' & , C' > 0 \\ \sqrt{\Delta} + 2C' < B < \sqrt{\Delta} & , C' < 0 \end{cases}$
3. $B^2 - 4AC = \Delta$

An alternate formulation of λ can also be defined in terms of matrices. ρ was obtained by applying $S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix}$ on F. λ can be obtained by applying $S_n^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix}$ on $\rho(F)$.
Clearly, ρ and λ are inverse operations of each other on the set of reduced forms. Hence, we have the following lemma.

Lemma 6. *If F is semi-reduced then $\lambda \circ \rho(F) = F$, and $\rho \circ \lambda(F) = F$*

Reduced forms are also semi-reduced hence ρ is injective on semi-reduced forms. Also, if F is semi-reduced then so is $\rho(F)$, this means that ρ is surjective. Hence, we have shown that ρ is a bijection the set of reduced forms, and bijections implies permutation hence we can safely conclude that ρ induces a permutation on the set of reduced forms. λ is just the inverse of ρ, the same results apply to it as well. We know that permutations are basically a union of disjoint cycles, hence we can say that the reduced forms are clubbed into different cycles.
Now, that we have shown that if a form lies in a cycle it is equivalent to forms in that cycle, we ask whether the inverse is true, i.e., if two forms are equivalent then they belong to the same cycle.

Main theorem of Zagier reduction. The main theorem of Zagier's reduction is this: " Two forms F and F' with discriminant Δ are said to be equivalent if and only if they belong to the same cycle."
To prove this we first state the **fundamental lemma**:

Lemma 7. *Assume that there are Z-reduced forms F and F' such that $F' = F|_S$* [1] *where $S \in SL_2\mathbb{Z}$. Then $S = S_1S_2 \dots S_n$ is a product of reduction matrices and the forms $F_1 = F|S_1$,$F_2 = F_1|S_2$,$F_3 = F_2|S_3 \dots F_n = F_{n-1}|S_n$ are all Z-reduced.*

Now, we are equipped to prove the 'main theorem'. Suppose that there are two equivalent forms F and F'. It means that $F' = F|_S$ for some $S \in SL_2\mathbb{Z}$. By the fundamental lemma we know that $S = S_1S_2 \dots S_n$ is a product of reduction matrices and hence F' is in the same cycle as F since F transforms into F' through a series of reduced forms.
Hence, to compute the class number of the determinant, we simply find all the *Z-reduced* forms and determine which cycle they belong to.

[1] $F' = F|_S$ means that F' is obtained by the action of $S \in SL_2\mathbb{Z}$ on F

2.5 Gauss reduction

Many reduction theories have been introduced and one among those is the classical one given by **Gauss**. It is primarily used to do computations as the coefficients obtained by this theory are small and easy to handle. We will see what it means to be reduced in the sense of **Gauss** and also try to introduce a reduction operator similar to the one introduced by Zagier. There will be analogous theorems and formulations in this section.

So, we begin by what it means to be *reduced* according to **Gauss**
Consider the form $F = (A, B, C)$ with a positive non-square determinant Δ. Such a form is said to be *Gauss-reduced* or 'reduced' in this case if

- $\sqrt{\Delta} - 2|A| < B < \sqrt{\Delta}$
- $\sqrt{\Delta} - 2|C| < B < \sqrt{\Delta}$

An analogue to Theorem 2 is the following theorem

Theorem 3. *Let $F = (A, B, C)$ be a primitive indefinite form with discriminant $\Delta = B^2 - 4AC$ and let $\epsilon_1 = \frac{-B+\sqrt{\Delta}}{2A}$, $\epsilon_2 = \frac{-B-\sqrt{\Delta}}{2A}$ denote the two roots of the quadratic equation $F(x, 1) = Ax^2 + Bx + C = 0$. Then the following statements are equivalent:*

1. *(A, B, C) is reduced*
2. *(C, B, A) is reduced*
3. *$0 < \sqrt{\Delta} - B < 2|A| < \sqrt{\Delta} + B$*
4. *$0 < \sqrt{\Delta} - B < 2|C| < \sqrt{\Delta} + B$*
5. *$\epsilon_1\epsilon_2 < 0$ and $|\epsilon_1| < 1 < |\epsilon_2|$*
6. *$AC < 0$, $B > |A + C|$*

Proof. $(1) \Leftrightarrow (2)$ It is trivial to see this due to the underlying symmetry in the definition of reduced form.
$(1) \Rightarrow (3)$ From the definition $0 < \sqrt{\Delta} - 2|A| < B$ and $0 < \sqrt{\Delta} - 2|C| < B$
Consider $2|A| = \dfrac{|B^2 - \sqrt{\Delta}|}{2|C|} < \dfrac{|(\sqrt{\Delta} - B)(\sqrt{\Delta} + B)|}{\sqrt{\Delta} - B} = \sqrt{\Delta} + B$
$(3) \Rightarrow (1)$

$0 < \sqrt{\Delta} - B \Rightarrow B < \sqrt{\Delta}$ and
$2|C| = \dfrac{|B^2 - \sqrt{\Delta}|}{2|A|} > \dfrac{|(\sqrt{\Delta} - B)(\sqrt{\Delta} + B)|}{\sqrt{\Delta} + B} = \sqrt{\Delta} - B$ or $2|C| > \sqrt{\Delta} - B$.
So, we conclude that $(1) \Leftrightarrow (3)$
Similarly, we can say that $(2) \Leftrightarrow (4)$ which means that statements from 1 to 4 are equivalent.
$(3) \Rightarrow (5)$ Take statement 3 and divide by $2|A|$ and follow this up by taking modulus. You shall get $|\epsilon_1| < 1 < |\epsilon_2|$. Now,
$0 < \Delta - B^2 = -4A^2\epsilon_1\epsilon_2$ which implies that $\epsilon_1\epsilon_2 < 0$.
$(5) \Rightarrow (3)$ Multiply the inequality by $2|A|$ to get
$|\sqrt{\Delta} - B| < 2|A| < |\sqrt{\Delta} + B|$. From $\epsilon_1\epsilon_2 < 0$ we get
$(\sqrt{\Delta} - B)(\sqrt{\Delta} + B) > 0$. If both the terms are positive then we get our required inequality of 3 and if both are negative then also the inequality of 3 is obtained. This means that all statements from 1 to 5 are equivalent.
$(5) \Rightarrow (6)$ $4AC = B^2 - \Delta$ and from statement 3 we know that $B^2 - \Delta < 0$ therefore $AC < 0$.
$|\epsilon_1| < 1 < |\epsilon_2|$ means that $\epsilon_1 = \frac{|-B+\sqrt{\Delta}|}{2|A|} < 1 < \frac{|-B-\sqrt{\Delta}|}{2|A|} = \epsilon_2$

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

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

So,

$$\begin{aligned} (2|A| - \sqrt{\Delta}|)^2 &< B^2 \\ 4A^2 + B^2 - 4AC - 4|A|\sqrt{\Delta} &< B^2 \\ |A| + |C| &< \sqrt{\Delta} < B \end{aligned}$$

Important to note is that all these steps can be traced back, they are all equivalent and hence we have that $(6) \Rightarrow (3)$. Hence, our claim is proven. □

Now, we attempt to put a bound on the coefficients of *Gauss-reduced* form.

Lemma 8. *If the form $F = (A, B, C)$ is reduced, then $B > 0$, $AC < 0$ and $0 < |A|, B, |C| < \sqrt{\Delta}$.*

Proof. The first two inequalities are immediate from Theorem 3. Also, $B < \sqrt{\Delta}$ since F is *reduced*.
From Theorem 3 we have $2|A| < \sqrt{\Delta} + B < 2\sqrt{\Delta} \Rightarrow |A < \sqrt{\Delta}|$. Similarly $2|C| < \sqrt{\Delta} + \sqrt{\Delta}$. Hence, claim is proven. □

From this lemma we see that there are finitely many *Gauss-reduced* forms with a positive nonsquare determinant Δ.
Now, we define a reduction operator like the one defined by Zagier.
A form $F = (A, B, C)$ with discriminant Δ we define the *right neighbour* $(\rho(F))$ of F in the following manner:

1. $C' = A$
2. $B + B' \equiv 0 \pmod{2A'}$ and $\sqrt{\Delta} - |2A'| < B' < \sqrt{\Delta}$
3. $B'^2 - 4A'C' = \Delta$

This formulation can also be presented in the form of matrices $(\rho(F) = F|_S)$ by the action of $S = \begin{pmatrix} 0 & 1 \\ -1 & t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}$ which is basically a shift followed by a flip. Here, $t = \frac{B+B'}{2A'}$

Lemma 9. *1. If F is a primitive indefinite form, then $\rho(F)$ is semi-reduced.*

2. If F is reduced then so is $\rho(F)$.

Proof. 1. Let $\rho(F) = (A', B', C')$ then $\sqrt{\Delta} - |2A'| < B' < \sqrt{\Delta}$. If $A' < 0$ then $|2A'| = -2A'$ so $\sqrt{\Delta} + 2A' < B' < \sqrt{\Delta}$. If $A' > 0$ then $|2A'| = 2A'$ so $\sqrt{\Delta} - 2A' < B' < \sqrt{\Delta}$. This clearly proves that $\rho(F)$ is semi-reduced.

2. Let $\rho(F) = (A', B', C')$
   $\sqrt{\Delta} - |2A'| < B' < \sqrt{\Delta}$ by the very way of constructing $\rho(F)$
   $\sqrt{\Delta} - |2C'| < B' < \sqrt{\Delta}$ is true because F is reduced.

□

There are many more properties that are similar to the one obtained by Zagier's reduction operator. We are stating a few properties regarding the cycles generated by ρ:

1. ρ is injective on the set of semi-reduced forms and hence permutes the reduced forms.
2. Two forms are equivalent if and only if they belong to the same cycle as obtained by the permutation of reduced forms by ρ.

2.6 Interpreting Zagier's proof of two squares theorem

Zagier's Proof. Consider the set

$$S = \{(x, y, z) \in \mathbb{N}^3 \ : \ x^2 + 4yz = p\}$$

where $p \equiv 1 \pmod 4$. Now, the map

$$g = \begin{cases} (x + 2z, z, y - x - z) & if x < y - z \\ (2y - x, y, x - y + z) & if y - z < x < 2y \\ (x - 2y, x - y + z, y) & if x > 2y \end{cases}$$

is claimed to be an involution on S with a single fixed point namely $(1, 1, \frac{p-1}{4})$. We are now going to verify all the claims and proceed further with the proof.
Note that $x \neq y - z$ for if it were true then $x^2 + 4yz = (y + z)^2$ which is not a prime, similarly if $x = 2y$ then $x^2 + 4yz = 4(y^2 + yz)$ which is also not a prime therefore the cases below exhaust all posibilities. First, we claim that g maps from S to S and that g indeed is an involution.
Suppose $x < y - z$ then the first case of the mapping is used and we get $g(x, y, z) = (x + 2z, z, y - x - z)$ but $x + 2z > 2z$ therefore $g(g(x, y, z)) = (x, y, z)$
If $x > 2y$ then from the third case of mapping gives us $g(x, y, z) = (x - 2y, x - y + z, y)$ but $x - 2y < x - y + z - y$ therefore $g(g(x, y, z)) = (x, y, z)$
If $y - z < x < 2y$ then the second case of mapping gives us $g(x, y, z) = (2y - x, y, x - y + z)$ but $y - x + y - z < 2y - x < 2y$ therefore $g(g(x, y, z)) = (x, y, z)$
This proves that if there is a fixed point in this involution then it must belong to the second case. So, $2y - x = x$, $y = y$ and $z = x - y + z$ implies that $x = y$.

$$x^2 + 4xz = x(x + 4z) = p$$

but p is a prime therefore only possibility is $x = 1 = y$ and $z = \frac{p-1}{4}$. Hence, the only fixed point of the above involution is $(1, 1, \frac{p-1}{4})$. Thus, S has an odd cardinality.
Now, consider the simpler involution

$$(x, y, z) \mapsto (x, z, y)$$

on the set with odd cardinality then it will have exactly a single fixed point, $y = z$ or $x^2 + 4y^2 = p$ as desired.

The insights to the above involution can be found in [3]

Heath-Brown's version. This version deals with three involutions. First consider the set

$$S = \{(x, y, z) \in \mathbb{Z}^3 \ : \ 4xy + z^2 = p, x > 0, y > 0\}$$

where $p \equiv 1 \pmod 4$
Also, consider the sets

$$T = \{(x, y, z) \in S \ : \ z > 0\}$$

and

$$U = \{(x, y, z) \in S \ : \ x - y + z > 0\}$$

Now, let's define the involution

$$f : (x, y, z) \mapsto (y, x, -z)$$

f maps S to S.
f maps points in T to points in $S\backslash T$ [2].
Similarly, f maps points in U to points in $S\backslash U$.
Thus, a bijection is established between T and $S\backslash T$ as well as between U and $S\backslash U$. This implies that all of them have the same cardinality, i.e., $|T| = |U| = |S\backslash T| = |S\backslash U|$.
A second involution is defined on U by

$$g : (x, y, z) \mapsto (x - y + z, y, 2y - z)$$

it is easy to verify that it is an involution, simply calculate

$$g(g(x, y, z)) = g(x-y+z, y, 2y-z) = (x-y+z-y+2y-z, y, 2y-2y+z) = (x, y, z)$$

Now, if it were to have a fixed point then $x = x - y + z$, $y = y$ and $z = 2y - z$ or $y = z$. Therefore, by similar calculations as in Zagier's proof we obtain the fixed point to be $(\frac{p-1}{4}, 1, 1)$. Since, there is only 1 fixed point therefore the cardinality of U is odd.
Finally consider this involution on T defined by

$$h : (x, y, z) \mapsto (y, x, z)$$

[2] $S\backslash T$ means points in S but not in T

must also have a fixed point since T also has an odd cardinality. Hence, there exists $(x, y, z) \in S$ such that $x = y$ and this implies that $4y^2 + z^2 = p$ as desired.

Interpretation using Quadratic forms. Our first job is to link the set S [3] to the coefficients of a form, to this we say that the points $(x, y, z) \in S$ corresponds to binary quadratic forms $(A, B, C) = (-y, x, z)$ with *discriminant* $\Delta = B^2 - 4AC = x^2 + 4yz = p$.
$A < 0, B > 0$ and $C > 0$ and the fixed point of the second involution is when $y = z$ which corresponds to the form $(-y, x, y)$. So, we can define the same involutions as used by Zagier and apply it to the quadratic form (A, B, C) as follows:

$$g(A,B,C) \mapsto \begin{cases} (C, B+2C, -A-B-C) & if A+B+C<0 \\ (A, -2A-B, A+B+C) & if A+B+C>0, B+2A<0 \\ (-A-B-C, B+2A, -A) & if B+2A>0 \end{cases}$$

$$h : (A,B,C) \mapsto (-C,B,-A)$$

Consider binary quadratic forms (A, B, C) with a prime *discriminant* $\Delta = B^2 - 4AC = p$ where $p \equiv 1 \pmod 4$. Such a form is called **pre-reduced** if $A < 0$, $B > 0$ and $C > 0$. There are only finitely many *pre-reduced* forms and they satisfy $0 < B < \sqrt{\Delta} = \sqrt{p}$,
$0 > A \geq -\frac{\Delta-1}{4} = -\frac{p-1}{4}$ and $0 < C \leq \frac{p-1}{4}$.

Lemma 10. *If (A, B, C) is pre-reduced then so is $(-C, B, -A)$*

This is true from the very definition.
Building up on this we can define a function $\zeta = h \circ g$ that sends a pre-reduced form (A, B, C) to

$$\zeta(A,B,C) \mapsto \begin{cases} (A+B+C, B+2C, C) & if A+B+C<0 \\ (-A-B-C, -2A-B, -A) & if A+B+C>0, B+2A<0 \\ (A, B+2A, A+B+C) & if B+2A>0 \end{cases}$$

If $A + B + C = 0$ then $\Delta = B^2 - 4AC = (A - C)^2$ is a square which is obviously not a prime. Similarly, if $B + 2A = 0$ then $\Delta = 4(A^2 - AC)$ which is even and hence not a prime. Hence, the conditions exhaust all possiblities and are disjoint.

[3] S is the same as described by Zagier in his proof

Proposition 4. *If F is pre-reduced, then so is $\zeta(F)$*

Proof. Set $\zeta(A, B, C) = (A', B', C')$

1. $A + B + C < 0$. Here, $A' = A + B + C < 0$, $B' = B + 2C > 0$ since $B, C > 0$ this also means that $C' = C > 0$
2. $A + B + C > 0$, $B + 2A < 0$. Here, $A' = -(A + B + C) < 0$, $C' = -A > 0$ and $B' = -(2A + B) > 0$
3. $A + B + C > 0$, $B + 2A > 0$. Here, $A' = A < 0$, $B' = B + 2A > 0$ and $C' = A + B + C > 0$

□

Lemma 11. *We have $F \sim \zeta(F)$ where $\sim$ denotes equivalence with respect to the action of $GL_2\mathbb{Z}$* [4]

Proof. We distinguish the three cases

1. $A + B + C < 0$. Here, $\zeta(F) = F|_S$ where $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2\mathbb{Z}$
2. $A + B + C > 0$, $B + 2A < 0$.Here, $\zeta(F) = F|_S$ where $S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2\mathbb{Z}$
3. $A + B + C > 0$, $B + 2A > 0$.Here, $\zeta(F) = F|_S$ where $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2\mathbb{Z}$

□

Now, we are ready to prove the following proposition

Proposition 5. *Every primitive form with discriminant $\Delta \equiv 1 \pmod 4$ is $GL_2\mathbb{Z}$ equivalent to a pre-reduced form.*

Proof. Every primitive form is $SL_2\mathbb{Z}$ equivalent to a *Gauss-reduced* form (A, B, C) which satisfies $B > 0$ and $AC < 0$. If (A, B, C) is not *pre-reduced* then $A > 0$ and $C < 0$ so we can apply $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2\mathbb{Z}$ to obtain $(A', B', C') = (C, B, A)$ which is *pre-reduced* since $A' = C < 0$, $B' = B > 0$ and $C' = A > 0$. □

[4] $GL_2\mathbb{Z}$ is the group of matrices with integer elements and discriminant equal to either $+1$ or -1

Lemma 12. *The map ζ is injective on the set of pre-reduced forms.*

Proof. Let there be two forms F_1 and F_2 such that $\zeta(F_1) = \zeta(F_2)$. But we know that ζ is a composition of two functions. Hence, we analyse in the following manner:

$$h(g(F_1)) = h(g(F_2))$$

Since, both h and g are both involutions therefore we proceed further in following way:

$$\begin{aligned} h(h(g(F_1))) &= h(h(g(F_2))) \\ g(F_1) &= g(F_2) \\ g(g(F_1)) &= g(g(F_2)) \\ F_1 &= F_2 \end{aligned}$$

Hence, our claim is proven. □

Lemma 13. *If $\zeta(A, B, C) = (A', B', C')$ then $\zeta(-C', B', -A') = (-C, B, -A)$.*

Proof. We handle this in a case wise manner:

1. $A + B + C < 0$. Here $(A', B', C') = (A + B + C, B + 2C, C)$. Hence, $\zeta(-C', B', -A') = (-C, B + 2C, -A - B - C)$. Since, $B' - C' - A' = -A > 0$ and $B' - 2C' = B + 4C > 0$ therefore $\zeta(-C', B', -A') = (-C, B, -A)$. (condition 3)

2. $A + B + C > 0$, $B + 2A < 0$. Here $(A', B', C') = (-A - B - C, -2A - B, -A)$. Hence, $\zeta(-C', B', -A') = (A, -2A - B, A + B + C)$. Since, $B' - C' - A' = C > 0$ and $B' - 2C' = -B < 0$ therefore $\zeta(-C', B', -A') = (-C, B, -A)$. (condition 2)

3. $A + B + C > 0$, $B + 2A > 0$. Here $(A', B', C') = (A, B + 2A, A + B + C)$. Hence, $\zeta(-C', B', -A') = (-A - B - C, B + 2A, -A)$. Since, $B' - C' - A' = -C < 0$ therefore $\zeta(-C', B', -A') = (-C, B, -A)$. (condition 1)

□

From all of these we can conclude that the fixed points of ζ are quadratic forms of the like $(A, B, -A)$. And, now we come to prove the main theorem.

Let us first observe an example: the reduction cycle of $\Delta = 41$ produced by ζ

$$(-10,1,1) \to (-8,3,1) \to (-4,5,1) \to (-2,3,4) \to (-5,1,2) \to (-2,5,2) \to$$

$$(-2,1,5) \to (-4,3,2) \to (-1,5,4) \to (-1,3,8) \to (-1,1,10) \to (-10,1,1)$$

Theorem 4. *The principal (anti-symmetric) cycle of ζ containing the form $F = (-\frac{p-1}{4}, 1, 1)$ has an odd length and a single fixed point of the form as mentioned above. Hence, p can be written as the sum of two squares.*

Proof. From Lemma 13 it is clear that if $\zeta(A,B,C) = (A',B',C')$ then $\zeta(-C',B',-A') = (-C,B,-A)$. What this means is that we can extend this cycle by "coupling" a form (A,B,C) with its anti-symmetric partner $(-C,B,-A)$.
Now, if we try to figure if $\zeta(A,B,C) = (-C,B,-A)$ where (A,B,C) is primitive we find that the solution exists only in the case of second condition in map of ζ. Hence, we can say that $-C = -A - B - C$ and $-B - 2A = B$, both of this implies that $A = -B$.
Now, if we consider the form $(A,-A,C)$ then *discriminant* $\Delta = A^2 - 4AC = A(A-4C) = p$. Since p is a prime and $A < 0$ therefore the solution to this is $A = -1$, $A - 4C = -p$ which corresponds to the form $(-1,1,\frac{p-1}{4})$ (anti-symmetric to F). But this means that the cycle cannot have an even length for if there were we would have two solutions to $\zeta(A,B,C) = (-C,B,-A)$. But then this means there is a fixed point in the cycle that gives a form $(A,B,-A)$, and this means $p = B^2 + 4A^2$ as claimed. □

2.7 Gauss's class number problem

Gauss's Conjecture: There are no discriminants less than 163 with class number 1.
We now state and prove a few results.

1. Assume that $m \equiv 2,3 \pmod 4$ is squarefree and $m < -2$ and let $\Delta = 4m$. Then $h(\Delta) > 1$.
   If $m \equiv 3 \pmod 4$ then $(1,0,-m)$ and $(2,2,\frac{1-m}{2})$ are distinct reduced forms with discriminant $4m$. If $m \equiv 2 \pmod 4$, consider $(1,0,-m)$ and $(2,0,-m/2)$.

2. If $\Delta = 1 - 4m$ and $h(\Delta) = 1$, then Δ is a prime.
   Suppose $p|\Delta$, p is represented by some form with discriminant Δ. But $h(\Delta) = 1$ so the only possible form is the principal form $(1, 1, m)$. Thus we have $4F_0(x, y) = 4p = (2x + 1)^2 - \Delta y^2$. The representation is proper and hence $(x, y) = 1$ and $p|(2x + 1) \Rightarrow pk = 2x + 1$.

   $$4p = k^2p^2 - \Delta y^2$$

   Since, $(x, y) = 1$ therefore $y^2 \geq 1$. Now, consider

   $$4 = k^2p - \frac{\Delta}{p}y^2 \geq k^2p - \frac{\Delta}{p} > 3 + 1 = 4$$

   a contradiction. Hence, $k = 0$ which means that $2x + 1 = 0$. So, $4p = -\Delta y^2$. Since $\gcd(\Delta, 4) = 1$ therefore y is even so $p = -\Delta(y')^2$. Thus we can conclude that $y' = 1$ or $y = \pm 2$ which would mean that $\Delta = \pm p$ and our claim is proven.

3. If $\Delta = 1 - 4m < -3$ and $h(\Delta) = 1$, then m is prime.
   Consider the principal form $(1, 1, m)$. It is clearly Langrange-reduced since $|1| \leq 1 \leq m$. Suppose m were not prime then $m = ab$ for some integers a, b. But this means that there is another Langrange-reduced form $(a, 1, \frac{m}{a})$ with discriminant Δ which is a contradiction to $h(\Delta) = 1$ and hence not possible. m is a prime.

4. If $\Delta = 1 - 8m < -7$, then $h(\Delta) > 1$.
   Consider the form $(2, 1, m)$ with $m \geq 2$. It is not equivalent to the principal form hence job is complete.

5. If $\Delta = 1 - 4m$ and $h(\Delta) = 1$, then $\left(\frac{\Delta}{p}\right) = -1$ for all $p < m$.
   From Lemma 2 we know that if $\left(\frac{\Delta}{p}\right) \neq -1$ for all $p < m$ then there is a Langrange-reduced form with discriminant Δ that primitively represents p. If such a case were true then we can say that the principal form $(1, 1, m)$ represents p. The principal form is *Langranged-reduced* and hence by Legendre's Lemma we know that the smallest integers primitively represented by the form are $1, m$ hence, $p \geq m$ which is a contradiction to our assumption. Hence, $\left(\frac{\Delta}{p}\right) = -1$ for all $p < m$.

6. If $\Delta = 1 - 4m$ and $\left(\frac{\Delta}{p}\right) = -1$ for all $p < \sqrt{-\Delta/3}$, then $h(\Delta) = 1$.
   Let $F = (A, B, C)$ be a reduced form with discriminant Δ. If $A > 1$ then there is a prime $p|A$ and this gives us $\left(\frac{\Delta}{p}\right) = 0$. Since, the form F is *Langrange-reduced* therefore $1 \leq p \leq A \leq \sqrt{\frac{-\Delta}{3}}$
   $A = \sqrt{-\Delta/3}$ is possible when $A = B = C = \sqrt{-\Delta/3}$ which is a contradiction as (A, B, C) is primitive.
   Hence, $A = 1$. This gives us $B = -1, 0, 1$. But B and Δ have same parity therefore $B = \pm 1$. Also, $B > 0$ hence $B = 1$. This gives $C = m$. So, we have one unique form $(1, 1, m)$ or equivalently $h(\Delta) = 1$.

Theorem 5. *Let $\Delta = 1 - 4m$ be squarefree and negative. Then the following statements are equivalent:*

1. $h(\Delta) = 1$
2. $\left(\frac{\Delta}{p}\right) = -1$ *for all* $p < \sqrt{-\Delta/3}$
3. $\left(\frac{\Delta}{p}\right) = -1$ *for all* $p < m$

Proof. We know that $(1) \Rightarrow (3)$, $(2) \Rightarrow (1)$. Also, $(3) \Rightarrow (2)$ since $\frac{4m-1}{3} < m$. Thus we conclude that all three statements are equivalent. □

Theorem 6. *For fundamental discriminants $\Delta = 1 - 4m \leq -7$, the following statements are equivalent:*

1. $h(\Delta) = 1$
2. $f(x) = x^2 + x + m$ *attains only prime values for* $x = 0, 1, 2, \ldots m - 2$

Proof. The polynomial f is known as the *Euler polynomial* and the stated theorem is a special case of the *Rabinowitz criterion*. □

Proposition 6. *If $\Delta = 1 - 4m$ and $h(\Delta) = 1$ then every integer $< m^2$ represented by the principal form F_0 with discriminant Δ is prime.*

Proof. Suppose not, then there is an integer $n < m^2$ represented by the principal form with discriminant Δ. Let p be a divisor of n then $p < \sqrt{m^2} = m$ which must also be represented by F_0 but by Legendre's lemma the the smallest integers represented by F_0 are $1, m$ hence $p \geq m$ is a must. A contradiction. Hence, our assumption is wrong. □

Proposition 7. *If $\Delta = -8m$ and $h(\Delta) = 2$, then every integer $< (m+2)^2$ represented by some form with discriminant Δ is prime.*

Proof. Since the class number is 2 the only reduced forms with discriminant $-8m$ are $(1, 0, 2m)$ and $(2, 0, m)$. Both are *Langrange-reduced* and hence Legendre's lemma can be used in similar manner as above to obtain a contradiction. □

Chapter 3

Conclusions

3.1 Conclusion

The most important lesson that I have learnt while doing this project is the importance of a mathematical *structure*. How important it is to first define a *foundation* for the structure and slowly build up on that to give us another platform to investigate. The main objective has always been to build something else on the already established foundation. This was the basis for the reduction theories where we first define what it means to be 'reduced' and then try to find more properties regarding them, then we proceed to classify them and study each group separately and the process continues.
Zagier's proof is a very special proof for it is very short but has a very deep and beatiful structure supporting it. Also, later we can see the link of quadratic forms with different other branches like continued fractions, a geometric view on the complex plane. Gauss's class number problem is another infamous problem that has been tackled by so many people and it is amazing how the proof involves intricate and advanced topics like elliptic curves, class field theory, and others.

3.2 Future Prospects

The study of binary quadratic forms is very important, especially in the study of solutions to the **Pell's equation**. The solution to *Pell's conics* have been of deep interest, as seen in [2] it has been linked to the automorphs in $SL_2\mathbb{Z}$ that are instrumental in reduction of binary quadratic forms. The solutions are also obtained using continued fractions which is also seen in later chapters of [1], [2]. Further study can be done in elliptic curves and

diophantine approximations as well.

Chapter 4

References

Bibliography

[1] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to The Theory of Numbers*, WILEY Fifth edition, preprint 2017. ISBN: 978-81-265-1811-1

[2] Franz Lemmermeyer, *Binary Quadratic forms-An Elementary Approach to the Arithmetic of Elliptic and Hyperelliptic Curves* (2010), http://www.rzuser.uni-heidelberg.de

[3] Christian Elsholtz, *A combinatorial approach to sums of two squares and related problems*, https://www.math.tugraz.at/~elsholtz/WWW/papers/papers30nathanson-new-address3.pdf

[4] R. A. Mollin, *Prime-Producing Quadratics*, *The American Mathematical Monthly , Jun. - Jul., 1997, Vol. 104, No. 6 (Jun. - Jul., 1997), pp. 529-544*, https://www.jstor.org/stable/2975080

[5] George Szekeres, *On the number of divisors of* $x^2 + x + A$

[6] G. Rabinowitsch, *"Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen Zahlkörpern," Journal für die Reine und Angewandte Mathematik*, vol. 142, pp. 153–164, 1913.

[7] D.M. Burton, *Elementary Number Theory*.