The Collision of Quadratic Fields, Binary Quadratic Forms, and Modular Forms

Karen Smith

May 12, 2011

Contents

Chapter 1

Introduction

As indicated by the title *The Collision of Quadratic Fields, Binary Quadratic Forms, and Modular Forms*, this paper leads us to an understanding of the relationship between these three areas of study. In [4], Zagier gives the results of an intriguing example of the relationship between these areas. However there is a large amount of background material that is necessary for an inexperienced reader to fully understand this relationship. Our motivation for writing this paper is thus to fully describe this example including the basic background information.

Our main goal is to understand the specific example, given by Zagier in [4], of the relationship between the quadratic forms of discriminant -23 (see Definitions 2.2 and 2.6), the quadratic field $\mathbb{Q}(\sqrt{-23})$ (see Section 2.2), and the modular form $\eta(z)\eta(23z)$ (see Section 2.3). In fact, we will see that the Fourier coefficients, as defined in Section 2.3, of the modular form $\eta(z)\eta(23z)$ will tell us exactly when the principal ideal (p) splits into principal or nonprincipal prime ideals in the ring of integers of $\mathbb{Q}(\sqrt{-23})$. These concepts are defined in Chapter 2.

To reach our goal, we begin in Chapter 2 by laying out preliminary information about quadratic forms, quadratic fields, modular forms, and a few basic relationships between these areas. In Chapter 3, we explore a relationship between quadratic forms and modular forms involving Hecke's theory of modular forms applied to the theta series of a binary quadratic form. This will leave us fully prepared for our main example, the case $d = -23$, in Chapter 4. In this case, we will consider the three quadratic forms

$$\begin{aligned} Q_0(x,y) &= x^2 + xy + 6y^2, \\ Q_1(x,y) &= 2x^2 + xy + 3y^2, \\ Q_2(x,y) &= 2x^2 - xy + 3y^2. \end{aligned} \tag{1.1}$$

In particular, we will be considering the number of representations $r(Q,n)$ of n by each binary quadratic form Q, (see Section 2.1). We will prove the following theorem of van der Blij (see [18]) that relates the modular form $\eta(z)\eta(23z)$ and the binary quadratic forms of discriminant -23 in (1.1).

Theorem 1.1. *(van der Blij) Let $t(n) \in \mathbb{Z}$ be defined by*

$$\eta(z)\eta(23z) = q\prod_{k=1}^{\infty}(1-q^k)(1-q^{23k}) = \sum_{n=1}^{\infty} t(n)q^n,$$

where $q = e^{2\pi iz}$. Then

$$r(Q_0, n) = \frac{2}{3}\sum_{d|n}\left(\frac{d}{23}\right) + \frac{4}{3}t(n), \tag{1.2}$$

and

$$r(Q_1, n) = \frac{2}{3}\sum_{d|n}\left(\frac{d}{23}\right) - \frac{2}{3}t(n). \tag{1.3}$$

Finally, we will conclude with some applications of van der Blij's theorem including the following theorem given by Zagier in [4] that describes the relationship between the Fourier coefficients of $\eta(z)\eta(23z)$ and the ideals of the form (p) in the ring of integers O_{-23} of $Q(\sqrt{-23})$.

Theorem 1.2. *Let p be prime. In O_{-23}, the ideal (p) decomposes in the following way (where P and P' represent distinct prime ideals):*

$$(p) = \begin{cases} P^2 & \text{if } a_p = 1, \text{ where } P \text{ is principal,} \\ P & \text{if } a_p = 0, \text{ where } P \text{ is principal,} \\ PP' & \text{if } a_p = 2, \text{ where } P,\ P' \text{ are principal,} \\ PP' & \text{if } a_p = -1, \text{ where } P,\ P' \text{ are non-principal.} \end{cases}$$

Here a_p is the Fourier coefficient of q^p in the Fourier expansion of the modular form $\eta(z)\eta(23z)$.

Chapter 2

Preliminaries

2.1 Binary Quadratic Forms

In our discussion of binary quadratic forms, we primarily refer to [5] as we provide background information. As we progress, we will mention additional sources as needed. We begin with some definitions.

Definition 2.1. *A quadratic form is a polynomial of degree two in any number of real variables with integer coefficients for which all monomials with nonzero coefficients have the same total degree.*

In this paper, we will only consider binary quadratic forms.

Definition 2.2. *A binary quadratic form Q is a quadratic form in two variables. I.e., is of the form*

$$Q(x, y) = ax^2 + bxy + cy^2, \ a, b, c \in \mathbb{Z}.$$

Additionally, a binary quadratic form is called primitive if the coefficients a, b, and c are relatively prime.

Example 2.3. *One quadratic form that we will find significant is the primitive quadratic form*

$$Q_0(x, y) = x^2 + xy + 6y^2.$$

We say two binary quadratic forms $Q_1(x, y)$ and $Q_2(x, y)$ are *equivalent* if there exist $p, q, r, s \in \mathbb{Z}$ with $ps - qr = \pm 1$ such that $Q_1(x, y) = Q_2(px + qy, rx + sy)$. From this, we see that Q_1 and Q_2 are equivalent if $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. We say that the equivalence is *proper* if $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Proper equivalence of binary quadratic forms is an equivalence relation. To see the equivalence relation holds, we will show that proper equivalence is reflexive, symmetric, and transitive. For ease of notation, if $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, then

$$fA(x, y) := f(px + qy, rx + sy).$$

For any binary quadratic form, Q, $Q(x,y) = QI(x,y)$ where I is the identity matrix in $SL_2(\mathbb{Z})$, so proper equivalence is reflexive. Now let Q_1, Q_2, and Q_3 be any binary quadratic forms. If $Q_1(x,y) = Q_2A(x,y)$ for $A \in SL_2(\mathbb{Z})$, then we can see that $Q_1A^{-1}(x,y) = Q_2(x,y)$, so proper equivalence is symmetric. If $Q_1(x,y) = Q_2A(x,y)$ and $Q_2(x,y) = Q_3B(x,y)$ for $A, B \in SL_2(\mathbb{Z})$, then $Q_1(x,y) = Q_3BA(x,y)$, so proper equivalence is transitive.

We note that a comparable proof works to prove that $GL_2(\mathbb{Z})$-equivalence is also an equivalence relation. However, we will be interested in primarily considering proper equivalence in this paper.

Example 2.4. *If $Q_1(x,y) = 2x^2 + xy + 3y^2$ and $Q_2(x,y) = 2x^2 - xy + 3y^2$, then we see $Q_1(x,y) = Q_2(-x,y)$. Because $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is in $GL_2(\mathbb{Z})$ but not $SL_2(\mathbb{Z})$, Q_1 and Q_2 are equivalent binary quadratic forms, but the equivalence is not proper.*

An integer m is *represented by a form $Q(x,y)$* if the equation $m = Q(x,y)$ has a solution $(x_0, y_0) \in \mathbb{Z}^2$. The *number of representations of n by Q* is defined by

$$r(Q,n) = \left|\left\{(x_0,y_0) \in \mathbb{Z}^2 : Q(x_0,y_0) = n\right\}\right|.$$

The next theorem is a useful observation about representations by binary quadratic forms.

Theorem 2.5. *Equivalent binary quadratic forms represent the same integers.*

Proof. If binary quadratic forms Q_1 and Q_2 are equivalent, then $Q_1(x,y) = Q_2A(x,y)$ for some $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. If Q_1 represents an integer $m \in \mathbb{Z}$, then for some $(a,b) \in \mathbb{Z}^2$, $Q_1(a,b) = m$. Then we also have $Q_2A(a,b) = Q_2(pa + qy, ra + sy) = m$, and we see that Q_2 must also represent m. Likewise, since equivalence is symmetric, if Q_2 represents $m \in \mathbb{Z}$, so does Q_1. □

Definition 2.6. *The discriminant d of a binary quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is defined to be*

$$d = b^2 - 4ac.$$

The discriminant can provide useful information about quadratic forms as will be seen in the following theorem.

Theorem 2.7. *Equivalent forms have the same discriminant.*

Proof. Suppose that Q_1 and Q_2 are equivalent quadratic forms. Then

$$Q_1(x,y) = Q_2A(x,y), \tag{2.1}$$

for $A \in GL_2(\mathbb{Z})$. Suppose that the discriminant of Q_1 is d_1 and the discriminant of Q_2 is d_2. Using (2.1), straightforward computations reveal that $d_1 = (\det(A))^2 d_2$. Since $A \in GL_2(\mathbb{Z})$, we conclude that $d_1 = d_2$. □

Definition 2.8. *The set of equivalence classes of properly equivalent binary quadratic forms of discriminant d is denoted by $C(d)$.*

Example 2.9. *As seen already,* $Q_1(x,y) = 2x^2 + xy + 3y^2$ *and* $Q_2(x,y) = 2x^2 - xy + 3y^2$ *are equivalent forms. The discriminant of* Q_1 *is* $1^2 - 4(2)(3) = -23$*, and the discriminant of* Q_2 *is* $(-1)^2 - 4(2)(3) = -23$*.*

The discriminant of a binary quadratic form can also be used to determine whether the quadratic form is positive or negative definite.

Definition 2.10. *A binary quadratic form* $Q(x,y)$ *is positive definite (resp. negative definite) if* $Q(x,y)$ *represents nonnegative integers (resp. nonpositive integers) and* $Q(x,y) = 0$ *if and only if* $x, y = 0$*.*

Theorem 2.11. *Let* $Q(x,y) = ax^2 + bxy + cy^2$ *be a binary quadratic form with discriminant* $d < 0$*. If* $a > 0$*, then* $Q(x,y)$ *is positive definite. If* $a < 0$*, then* $Q(x,y)$ *is negative definite.*

Proof. Notice that

$$4aQ(x,y) = 4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - dy^2. \tag{2.2}$$

Then if $d < 0$, the right-hand side of (2.2) is nonnegative and is equal to zero if and only if $x, y = 0$. By considering the left-hand side of (2.2), we now see that if $a > 0$, $Q(x,y) \geq 0$, and if $a < 0$, $Q(x,y) \leq 0$. □

To further our understanding of quadratic forms, we now consider quadratic forms with a specific type of discriminant.

Definition 2.12. *A discriminant* d *of a binary quadratic form is called a fundamental discriminant if* d *cannot be represented as* $d'r^2$ *with* $d' \equiv 0, 1 \pmod 4$ *and* $r > 1$*.*

Example 2.13. *For each of the forms* Q_0*,* Q_1*, and* Q_2 *from our prior examples, the discriminant is* -23 *and the coefficient of* x^2 *is greater than zero. Thus each of these forms is positive definite. Also, the discriminant* -23 *can only be factored as* $(-23)(\pm 1)^2$*, so we also have that* $d = -23$ *is a fundamental discriminant.*

We note here that, as seen in the previous example, any discriminant that is square-free will be a fundamental discriminant. We will be primarily concerned with quadratic forms with negative fundamental discriminant, so we also note that the first ten negative fundamental discriminants are -3, -4, -7, -8, -11, -15, -19, -20, -23, -24, and -31.

Next we state a definition that will help us to make some observations about the equivalence of quadratic forms.

Definition 2.14. *A primitive positive definite form* $ax^2 + bxy + cy^2$ *is said to be reduced if* $|b| \leq a \leq c$*, and* $b \geq 0$ *if either* $|b| = a$ *or* $a = c$*.*

Example 2.15. *We see that* $Q_0(x,y) = x^2 + xy + 6y^2$ *satisfies the criteria to be a reduced primitive positive definite form. However, the form* $Q(x,y) = 6x^2 + xy + y^2$ *is not reduced.*

The following theorem can help determine whether or not quadratic forms are properly equivalent.

Theorem 2.16. *Every primitive positive definite form is properly equivalent to a unique reduced form.*

The proof of this theorem is omitted for brevity. (See [5], Theorem 2.8.)

Example 2.17. *We can see that the forms $Q_0(x,y) = x^2 + xy + 6y^2$, $Q_1(x,y) = 2x^2 + xy + 3y^2$, and $Q_2(x,y) = 2x^2 - xy + 3y^2$ are all reduced forms. We already saw that Q_1 and Q_2 are equivalent but not properly equivalent. However, since each form is reduced, by Theorem 2.16, no two of these three forms are properly equivalent.*

We will end this section with the significant observation that the set $C(d)$ of equivalence classes of properly equivalent binary quadratic forms is an abelian group.

For brevity, we omit the proofs of the following lemma and theorem. (See [5], Lemma 3.2 and Theorem 3.9.)

Lemma 2.18. *Assume that $Q(x,y) = ax^2 + bxy + cy^2$ and $Q'(x,y) = a'x^2 + b'xy + c'y^2$ have discriminant d and satisfy*

$$gcd(a, a', (b+b')/2) = 1.$$

Then there is a unique integer B modulo $2aa'$ such that

$$B \equiv b \pmod{2a}$$

$$B \equiv b' \pmod{2a'}$$

$$B^2 \equiv D \pmod{4aa'}.$$

We can now define a group structure on the set $C(d)$.

Theorem 2.19. *Let $Q(x,y) = ax^2 + bxy + cy^2$ and $Q'x,y) = a'x^2 + b'xy + c'y^2$ such that Q_1 and Q_2 are both of discriminant $d < 0$, $d \equiv 0, 1 \pmod 4$. Then*

$$(Q_1 * Q_2)(x,y) = aa'x^2 + Bxy + \frac{B^2 - d}{4aa'}y^2,$$

where B is as described in Lemma 2.18. The set $(C(d), *)$ forms an abelian group. The order of the group $C(d)$ is the number of equivalence classes, denoted $h(d)$.

2.2 Quadratic Fields

There is an interesting connection between quadratic forms and quadratic fields that we will use. To understand this connection, we begin by recalling basic definitions and theorems regarding quadratic fields. Here we will assume a basic familiarity with algebraic number theory. For the reader without a background in algebraic number theory, we recommend [16] for a nice introduction to quadratic fields.

Recall, a field K is a *number field* if it is a finite degree field extension of $\mathbb{Q}$. An element $\alpha \in K$ is called an *algebraic integer* if the minimal polynomial of α is contained in $\mathbb{Z}[x]$. The set of algebraic integers O_K forms a ring called the *ring of integers of* K.

A *quadratic field* is a degree two extension of $\mathbb{Q}$. A quadratic field has the form $\mathbb{Q}(\sqrt{d})$ for square-free d. Fix such a square-free d, and let $K = \mathbb{Q}(\sqrt{d})$. Then the ring of integers of K is ([16], Theorem 3.2),

$$O_d = \begin{cases} [1, \sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ [1, \frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4, \end{cases} \tag{2.3}$$

where

$$[a, b] := \{ma + nb : m, n \in \mathbb{Z}\}.$$

Example 2.20. *In this paper, we will be primarily concerned with the quadratic field* $\mathbb{Q}(\sqrt{-23})$. *The corresponding ring of algebraic integers is*

$$O_{-23} = \left[1, \frac{1+\sqrt{-23}}{2}\right].$$

For future use, we recall the definitions of two norms. If $\alpha \in \mathbb{Q}(\sqrt{d})$, with $\alpha = a + b\sqrt{d}$, then the *norm of* α is defined to be

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

Recall, if $\alpha \in O_d$, $N(\alpha) \in \mathbb{Z}$ (see [16], p. 49). We also note that if A is an ideal of O_K, then the *norm of* A is defined to be

$$N(A) = |O_K/A|.$$

Additionally, we see that if (α) is a principal ideal where $\alpha = a + b\sqrt{d}$, then $N((\alpha)) = |a^2 - b^2 d|$ (see [16], Corollary 5.10).

Remark 2.21. *In order to reach our goals, we note that we spend most of this section simply collecting the definitions and theorems from algebraic number theory that we will need in later sections. We will omit many proofs of theorems; however, sources will be provided for each theorem stated. To conclude the section, we prove Theorem 2.33.*

Now we provide the definitions of the Legendre and Kronecker symbols along with propositions about the ideals of O_d.

Definition 2.22. *Let $a \in \mathbb{Z}$ and p be an odd prime. The Legendre symbol is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a^{(p-1)/2} \equiv 1 \pmod{p}, \\ -1 & \text{if } a^{(p-1)/2} \equiv -1 \pmod{p}, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Equivalently, in terms of quadratic residues,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Definition 2.23. *Let n be an integer with prime factorization $n = up_1^{e_1}...p_k^{e_k}$ where $u = \pm 1$ and each p_i is prime. The Kronecker symbol is a function of integers a and n and is defined by*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

where for odd prime p_i, $\left(\frac{a}{p_i}\right)$ is the Legendre symbol, for $p_i = 2$, we define

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \text{ is even}, \\ 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } a \equiv \pm 3 \pmod{8}, \end{cases}$$

and we also define

$$\left(\frac{a}{1}\right) = 1,$$

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0, \\ -1 & \text{if } a < 0, \end{cases}$$

and

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = \pm 1, \\ 0 & \text{otherwise.} \end{cases}$$

As we will be considering the factorization of ideals, we state the following important theorem. (See [16], Theorem 5.6.)

Theorem 2.24. *Every non-zero ideal of O_d can be written as a product of prime ideals uniquely up to the order of the factors.*

The following proposition is a useful fact about factors of principal ideals. (See [19], Chapter 2 Section 4.)

Proposition 2.25. *Every ideal A of O_d divides the principal ideal (α), where $\alpha = N(A)$.*

In a general number field, there is a method to compute the *discriminant of the number field.* For $\mathbb{Q}(\sqrt{d})$, the discriminant D_d is given by ([16], Section 3.1)

$$D_d = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Next we will consider the factorization of (p) in O_d. (See [13], Section 6.2 and [8] Proposition 13.1.4.)

Proposition 2.26. *Let p be any prime. Then in O_d we have*

$$(p) = \begin{cases} PP' & \text{where } P \neq P' \text{ if } \left(\frac{D_d}{p}\right) = 1, \\ P & \text{if } \left(\frac{D_d}{p}\right) = -1, \\ P^2 & \text{if } \left(\frac{D_d}{p}\right) = 0, \end{cases}$$

where P, P' are prime ideals of O_d.

Example 2.27. *Consider the quadratic field $Q(\sqrt{-23})$. In this case, $-23^{\frac{5-1}{2}} = -529 \equiv 1 \pmod 5$ and thus $\left(\frac{-23}{5}\right) = 1$, so we see that (5) is a prime ideal in O_{-23}. Similarly, we also know that $(23) = P^2$ for a prime ideal P because $\left(\frac{-23}{23}\right) = 0$.*

Next we introduce the idea of fractional ideals of a quadratic field.

Definition 2.28. *A subset $F \subset \mathbb{Q}(\sqrt{d})$ is called a fractional ideal of $\mathbb{Q}(\sqrt{d})$ if there exists $\beta \in O_d$, $\beta \neq 0$, such that βF is an ideal of O_d. The set of fractional ideals of $\mathbb{Q}(\sqrt{d})$ is denoted F_d.*

Notice that if F is a fractional ideal, then

$$F = \left\{ \frac{\alpha}{\beta} : \alpha \in A \right\}$$

for some ideal A of O_d and element $\beta \in O_d$. Then $\beta F = A$. We define the multiplication of two fractional ideals F_1 and F_2 by

$$F_1 F_2 = (\beta_1 \beta_2)^{-1} A_1 A_2,$$

where A_1 and A_2 are the ideals of O_d such that $F_1 = \beta_1^{-1} A_1$ and $F_2 = \beta_2^{-1} A_2$.

Next we consider the group structure of the set F_d, (see [16], Theorem 5.5.)

Theorem 2.29. *The set F_d of nonzero fractional ideals of $\mathbb{Q}(\sqrt{d})$ forms an abelian group under multiplication. The identity of the group is O_d. The inverse of the fractional ideal F is*

$$F^{-1} = \left\{ \alpha \in \mathbb{Q}(\sqrt{d}) : \alpha F \subseteq O_d \right\}.$$

We also note that the set of principal ideals $B_d \subset F_d$, is a subgroup of F_d.

Definition 2.30. *The quotient group $H_d = F_d/B_d$ is called the ideal class group of $\mathbb{Q}(\sqrt{d})$. The order of H_d is h_d, the class number of $\mathbb{Q}(\sqrt{d})$.*

Example 2.31. *If $h_d = 1$, then all fractional ideals are in the same equivalence class in H_d, so each fractional ideal is equivalent to the principal ideal $(1) = O_d$ modulo multiplication by principal ideals. That is, for each fractional ideal A there exists $\alpha \in O_d$ such that $(\alpha)A = (1) = O_d$. Then $A = \left(\frac{1}{\alpha}\right)$, and we can see that every fractional ideal, and thus every ideal, is principal.*

It is important to note that regardless of the class number, the principal ideals form one equivalence class within the class group H_d. Additionally, it is worth noting that each ideal class contains an actual ideal that is not fractional. To see this, notice that if $F = \beta^{-1}A$ for some ideal A and $\beta \in O_d$, then $F(\beta) = A$ will be an integral ideal in the ideal class FB_d. Such an ideal of O_d that is not fractional is called an *integral ideal.*

We are now ready to see the connection between binary quadratic forms and quadratic fields as found in [5], (see Theorem 7.7).

Theorem 2.32. *Let $d < 0$ be a fundamental discriminant. Then the map $\phi : C(d) \to H_d$ defined by*

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

is a group isomorphism between the class group of binary quadratic forms of discriminant d and the ideal class group of $\mathbb{Q}(\sqrt{d})$. In particular, $h(d) = h_d$.

We next see that there is an even deeper connection between binary quadratic forms and ideal classes.

Theorem 2.33. *For a positive-definite binary quadratic form Q with fundamental discriminant $d < 0$,*

$$r(Q, n) = w_d \cdot r(\mathcal{A}, n),$$

where w_d is the number of units in O_d, and $r(\mathcal{A}, n)$ is the number of integral ideals with norm n in the corresponding ideal class $\mathcal{A}$.

The rest of this section we build toward proving Theorem 2.33. First we compute the number of units in the ring of integers O_d.

Theorem 2.34. *The number of units in O_d is*

$$w_d = \begin{cases} 4 & \text{for } d = -1, \\ 6 & \text{for } d = -3, \\ 2 & \text{for } d = -2 \text{ or } d < -4. \end{cases} \tag{2.4}$$

Proof. Let $d < 0$, and let $\alpha = a + b\sqrt{d} \in O_d$ be a unit. Then there exists $\beta \in O_d$ such that $\alpha\beta = 1$. In this case, $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $\alpha, \beta \in O_d$, $N(\alpha), N(\beta) \in \mathbb{Z}$. Thus, we must have $N(\alpha) = \pm 1$. This happens exactly when

$$N(\alpha) = a^2 - db^2 = 1 \tag{2.5}$$

since $a^2 - db^2 > 0$ when $d < 0$.

By (2.3), if $d \equiv 2, 3 \pmod 4$, then $a, b \in \mathbb{Z}$. Then by (2.5), $a = \pm 1$ and $b = 0$, or, if $d = -1$, also $a = 0$ and $b = \pm 1$.

By (2.3), if $d \equiv 1 \pmod 4$, then $(2a)^2 - d(2b)^2 = 4$ where $2a, 2b \in \mathbb{Z}$. Then by (2.5), either $a = 1$ and $b = 0$, or, if $d = -3$, also $a = \pm 1/2$ and $b = \pm 1/2$.

Counting the number of units for each case, we see that the claim of the theorem holds. □

Recall that two forms $Q_0(x, y)$ and $Q_1(x, y)$ are properly equivalent when

$$Q_0(x, y) = Q_1A(x, y) = Q_1(px + qy, rx + sy),$$

where $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. If for $A \in SL_2(\mathbb{Z})$ we have that $Q(x, y) = QA(x, y)$, we call A an *automorph of the quadratic form* Q. It will be useful to know the number of automorphs for a quadratic form. (For the following theorem, see [20], Section 8.)

Theorem 2.35. *If $Q(x, y) = ax^2 + bxy + cy^2$ is a primitive quadratic form with discriminant d, then the number of automorphs for Q is*

$$a_Q = \begin{cases} 6 & \text{for } d = -3, \\ 4 & \text{for } d = -4, \\ 2 & \text{for } d < -4. \end{cases} \tag{2.6}$$

Moreover, the set of automorphs for Q can be described as

$$\left\{ \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix} : (t, u) = \begin{cases} (\pm 2, 0) \text{ or } (\pm 1, \pm 1) \text{ if } d = -3, \\ (\pm 2, 0) \text{ or } (0, \pm 1) \text{ if } d = -4, \\ (\pm 2, 0) \text{ if } d < -4. \end{cases} \right\}$$

We note that by comparing (2.4) and (2.6) for each primitive quadratic form Q with fundamental discriminant $d < 0$ and by observing that $\mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(\sqrt{-1})$, it can be seen that $a_Q = w_d$.

We are nearly able to prove Theorem 2.33, but first we state the following lemmas, (see [5], Section 7B).

Lemma 2.36. *If $Q(x, y) = ax^2 + bxy + cy^2$ is a positive-definite quadratic form with fundamental discriminant d, then $a[1, \tau]$ is an integral ideal of $[1, a\tau]$, where $\tau = \frac{-b+\sqrt{d}}{2a}$. Additionally,*

$$O_d = [1, a\tau].$$

Lemma 2.37. *Let $\mathcal{A}$ be the ideal class in H_d corresponding to the positive definite quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ with fundamental discriminant $d < 0$ via the isomorphism defined in Theorem 2.32. Then every integral ideal in $\mathcal{A}$ can be expressed as $\alpha[1,\tau]$ for some $\alpha \in O_d$. Additionally, if $A = \alpha[1,\tau]$ is an integral ideal of O_d, then $N(A) = N(\alpha)/a$.*

We are now ready to prove Theorem 2.33.

Proof. Let $Q(x,y) = ax^2+bxy+cy^2$ be a positive definite binary quadratic form with fundamental discriminant $d = b^2 - 4ac < 0$. As in Theorem 2.32, the quadratic form $Q(x,y)$ corresponds to the ideal class $\mathcal{A}$, containing the fractional ideal $A = a[1,\tau]$, where $\tau = \frac{-b+\sqrt{d}}{2a}$. By Lemma 2.36, we know that A is an integral ideal of O_d. Let B be an integral ideal of O_d of norm n in $\mathcal{A}$. By Lemma 2.37, we know that $B = \alpha[1,\tau]$ for some $\alpha \in O_d$ and that $N(\alpha)/a = n$. Since $\alpha, \alpha\tau \in O_d = [1, a\tau]$, we know $\alpha = p + qa\tau$ and $\alpha\tau = r + sa\tau$ for some $p,q,r,s \in \mathbb{Z}$. Then using the fact that $(p+qa\tau)\tau = r + sa\tau$ and the fact that, by the definition of τ, $a\tau^2 = -b\tau - c$, we see that $p = as + bq$.

Now we can see that

$$\begin{aligned} n = \frac{N(\alpha)}{a} &= \frac{1}{a} N\left(p - \frac{qb}{2} + \frac{q\sqrt{d}}{2}\right) \\ &= \frac{1}{a}\left(p - \frac{qb}{2} + \frac{q\sqrt{d}}{2}\right)\left(p - \frac{qb}{2} - \frac{q\sqrt{d}}{2}\right) \\ &= \frac{1}{a}(p^2 - bpq + acq^2) \\ &= \frac{1}{a}((as+bq)^2 + absq + acq^2) \\ &= as^2 + bsq + cq^2 \\ &= Q(s,q) \end{aligned}$$

Then we see that Q represents n. Next notice that if $B \neq B' \in \mathcal{A}$ with $N(B) = n = N(B')$, then $B = \alpha[1,\tau]$ and $B' = \alpha'[1,\tau]$ with $\alpha \neq \alpha'$. Using B' in the process above, we find numbers $s', q' \in \mathbb{Z}$ such that $Q(s',q') = n$. Also, we must have that $(s',q') \neq (s,q)$ or else we would have $\alpha = \alpha'$. Then we have that each integral ideal of norm n corresponds to a solution of $Q(x,y) = n$, and the solutions are different if the ideals are not equal.

Next we consider any $(s,q) \in \mathbb{Z}^2$ with $Q(s,q) = n$. By verifying closure under multiplication by elements in O_d using straightforward calculations, it can be shown that if $p = as + bq$ and $\alpha = p + qa\tau$, then $B = \alpha[1,\tau]$ is an integral ideal in $\mathcal{A}$. Then every solution of $Q(x,y) = n$ corresponds to an integral ideal in $\mathcal{A}$.

So far we have seen that each integral ideal of norm n in $\mathcal{A}$ corresponds to a different solution of $Q(x,y) = n$, and every solution of $Q(x,y) = n$ corresponds to at least one ideal of norm n

in $\mathcal{A}$. In terms of $r(Q,n)$ and $r(\mathcal{A},n)$, we now have that $r(Q,n) \geq r(\mathcal{A},n)$. What remains to be seen is that, in fact, each integral ideal in $\mathcal{A}$ leads to exactly w_d solutions of $Q(x,y) = n$, where w_d is the number of units in the ring of integers O_d. To see this, using basic calculations along with the explicit statement of the automorphs of Q in Theorem 2.35, it can be shown that if $Q(x,y) = Q(tx+uy, vx+wy)$ (that is, if $\left(\begin{smallmatrix} t & u \\ v & w \end{smallmatrix}\right)$ is an automorph for Q), then the solution (s,q) with $Q(s,q) = n$ and the solution $(tx+uy, vx+wy)$ correspond to the same ideal in $\mathcal{C}$. For example, if (s,q) is a solution that corresponds to $B = \alpha[1,\tau]$, it is relatively easy to see the the solution $(-s,-q)$ corresponds to $-\alpha[1,\tau] = B$ as well.

□

2.3 Modular Forms

We now brush the surface of the basics of modular forms. We primarily rely on [6] and [14] as references as we provide definitions and theorems.

Definition 2.38. *The upper-half plane $\mathbb{H}$ is the set of complex numbers*

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im(z)} > 0\}.$$

Definition 2.39. *Let f be a function, $f : \mathbb{H} \to \mathbb{C}$, and let k be an integer. The function f is called a modular form of weight k on $SL_2(\mathbb{Z})$ if*

1. *for all $z \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$,*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z). \tag{2.7}$$

2. *f is holomorphic on $\mathbb{H}$.*

3. *f is holomorphic at $i\infty$.*

Example 2.40. *We will show that if f is a modular form of weight k and g is a modular form of weight l, then fg is a modular form of weight $k+l$. First note that the product fg will still be holomorphic on $\mathbb{H}$ and at $i\infty$. Additionally we see*

$$\begin{aligned} (fg)\left(\frac{az+b}{cz+d}\right) &= f\left(\frac{az+b}{cz+d}\right) g\left(\frac{az+b}{cz+d}\right) \\ &= (cz+d)^k f(z)(cz+d)^l g(z) \\ &= (cz+d)^{k+l}(fg)(z). \end{aligned}$$

Modular forms can also be considered as functions on lattices of $\mathbb{C}$, so we will take some time to develop an understanding of lattices.

Definition 2.41. *If $\omega_1, \omega_2 \in \mathbb{Z}$ with $\omega_1/\omega_2 \notin \mathbb{R}$, then the lattice of $\mathbb{C}$ generated by ω_1 and ω_2 is defined to be*

$$\Lambda =< \omega_1, \omega_2 >= \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}.$$

We call $\{\omega_1, \omega_2\}$ a basis of Λ.

We note that each lattice is an additive subgroup of $\mathbb{C}$. If $\Lambda' =< \alpha_1, \alpha_2 >$ is a subgroup of $\Lambda =< \omega_1, \omega_2 >$, then we know that each α_i is an integral combination of ω_1 and ω_2. Then we have

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \tag{2.8}$$

for some 2×2 integral matrix A. We call Λ' a *sublattice of* Λ if $\alpha_1/\alpha_2 \notin \mathbb{R}$. In fact, letting A be as in (2.8), $\Lambda' := \Lambda(A)$ is a sublattice exactly when $\det(A) \neq 0$. We note that every 2×2 integral matrix A with nonzero determinant corresponds to exactly one sublattice $\Lambda(A)$ of Λ. Additionally, if $\Lambda(A) = \Lambda(B)$, then $A = UB$ for a matrix U with determinant ± 1. We say the *index of the sublattice Λ' of Λ* is $|\det(A)|$ where $\Lambda' = \Lambda(A)$. For a more detailed discussion of sublattices, we refer the reader to [17].

An additional proposition about sublattices will be useful in a later section.

Proposition 2.42. *The sublattices of Λ of index m are in bijective correspondence with the 2×2 integral matrices*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

such that $0 < b < d$ and $ad = m$.

We omit the proof of this proposition for brevity, (see [17]).

Now we are prepared to continue our discussion of modular forms. A function F mapping from the set of lattices of $\mathbb{C}$ to $\mathbb{C}$ is a *modular form of degree $-k$* if $F(\lambda\Lambda) = \lambda^{-k}F(\Lambda)$ for all lattices Λ of $\mathbb{C}$ and all $\lambda \in \mathbb{C}$ with $\lambda \neq 0$. We can see the connection between a modular form F on lattices and and a modular form f on $\mathbb{H}$ by letting $f(z) = F(< z, 1 >)$. Then as a result,

$$F(\Lambda) = \omega_2^{-k} f(\omega_1/\omega_2),$$

where $\{\omega_1, \omega_2\}$ is any oriented basis of Λ. Note that we can choose an ordering ω_1, ω_2 such that $\omega_1/\omega_2 \in \mathbb{H}$.

Example 2.43. *If f is a modular form of weight k,*

$$f\left(\frac{-1}{z}\right) = F\left(\left\langle 1, \frac{-1}{z}\right\rangle\right) = z^k F(< z, -1 >) = z^k F(< z, 1 >) = z^k f(z).$$

We note that this corresponds to (2.7) *for the matrix* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

It is sometimes convenient to view a modular form in terms of its Fourier expansion at $i\infty$. For more details about Fourier expansions, see [6], Section 1.1. A modular form f has the Fourier expansion at $i\infty$

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

where the a_n are called the *Fourier coefficients of* f, and $q = e^{2\pi iz}$. If $a_0 = 0$, then f is a called a *cusp form.* Note that this means that f vanishes at $i\infty$.

Example 2.44. *We define the* Δ*-function by*

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

where $q = e^{2\pi iz}$*. The* Δ*-function is a cusp form of weight 12 on* $SL_2(\mathbb{Z})$*. (See [4], p. 20.)*

Our next topic will be modular forms on congruence subgroups.

Definition 2.45. *If* N *is a positive integer, then define the level* N *congruence subgroups* $\Gamma_0(N)$ *and* $\Gamma_1(N)$ *by*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \text{ and } c \equiv 0 \pmod{N} \right\}.$$

Definition 2.46. *Let* f *be a function,* $f : \mathbb{H} \to \mathbb{C}$*, and let* k *be an integer. The function* f *is said to be a modular form of weight* k *on the congruence subgroup* Γ *of level* N *if*

1. *for all* $z \in \mathbb{H}$ *and* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$*,*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

2. f *is holomorphic on* $\mathbb{H}$*.*

3. *if* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$*, then*

$$g(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

has a Fourier expansion of the form

$$g(z) = \sum_{n \geq n_A \geq 0} a_A(n) q_N^n,$$

where $q_N = e^{2\pi iz/N}$ *and* $a_A(n_A) \neq 0$*.*

If $n_A > 0$ for each $A \in SL_2(\mathbb{Z})$, then f is called a cusp form on Γ.

A modular form f on congruence subgroup Γ has the Fourier expansion at $i\infty$

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = e^{2\pi i z}$. (See [14], Chapter 1.)

We denote the set of modular forms of weight k by $\mathcal{M}_k$ and the set of modular forms of weight k on a congruence subgroup Γ by $\mathcal{M}_k(\Gamma)$. Note that $\mathcal{M}_k = \mathcal{M}_k(\Gamma_0(1))$. Similarly, we denote the set of cusp forms of weight k by $\mathcal{S}_k$ and the set of cusp forms of weight k on a congruence subgroup Γ by $\mathcal{S}_k(\Gamma)$. Each of the sets $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ are complex vector spaces. We will briefly examine the structure of $\mathcal{M}_k$ and $\mathcal{S}_k$ as a vector space over $\mathbb{C}$ with the operations of function addition and scalar multiplication of functions by elements of $\mathbb{C}$. It is fairly straightforward to verify that the properties of a vector space are satisfied by each of these sets. As an example of the necessary calculations, we will show that $\mathcal{M}_k$ and $\mathcal{S}_k$ are closed under addition. For $f, g \in \mathcal{M}_k$, we have that for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$,

$$\begin{aligned} (f+g)\left(\frac{az+b}{cz+d}\right) &= f\left(\frac{az+b}{cz+d}\right) + g\left(\frac{az+b}{cz+d}\right) \\ &= (cz+d)^k f(z) + (cz+d)^k g(z) \\ &= (cz+d)^k (f+g)(z). \end{aligned}$$

When examining the cusp forms, if $f, g \in \mathcal{S}_k \subset \mathcal{M}_k$, we already know that $f+g \in \mathcal{M}_k$. Then it remains to show that the constant term of Fourier expansion of $f+g$ is zero. However, since both of the Fourier expansions for f and g have constant term zero, it is seen by adding these two expansions together that the Fourier expansion for $f+g$ will also have constant term zero. The rest of the verification of vector space structure will be left to the reader.

We now turn our focus to Dirichlet characters modulo n.

Definition 2.47. *A character on a finite abelian group G is a group homomorphism from G to $\mathbb{C}^*$. A Dirichlet character modulo n, $\chi : \mathbb{Z} \to \mathbb{C}^*$, is a character on the group $(\mathbb{Z}/n\mathbb{Z})^*$ that additionally satisfies*

$$\chi(m) = 0 \text{ if } \gcd(m,n) \neq 1$$

and

$$\chi(m) = \chi(m+n) \text{ for all } m \in \mathbb{Z}.$$

Example 2.48. *There are two Dirichlet characters modulo 3. We can see that*

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \equiv 1, 2 \pmod 3 \\ 0 & \text{if } n \equiv 0 \pmod 3. \end{cases}$$

and

$$\chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 3 \\ -1 & \text{if } n \equiv 2 \pmod 3 \\ 0 & \text{if } n \equiv 0 \pmod 3. \end{cases}$$

are the Dirichlet characters modulo 3.

If χ is a Dirichlet character modulo N, then we say that *a modular form* $f \in \mathcal{M}_k(\Gamma_1(N))$ *(resp.* $\mathcal{S}_k(\Gamma_1(N))$*) has Nebentypus character* χ if for all $z \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z).$$

The space of modular forms (resp. cusp forms) of weight k on $\Gamma_0(N)$ with Nebentypus character χ is denoted by $\mathcal{M}_k(\Gamma_0(N), \chi)$ (resp. $\mathcal{S}_k(\Gamma_0(N), \chi)$).

Modular forms can also be defined to have half-integral weight. (See [14], p. 10.) An important example is Dedekind's eta-function which is denoted by $\eta(z)$. Dedekind's eta-function is defined by

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1-q^n) \tag{2.9}$$

where $q = e^{2\pi i z}$. Notice that $\Delta(z) = \eta(z)^{24}$. More about Dedekind's eta-function can be found in [14].

We will not venture into the theory of half-integral weight modular forms because the theory will not be necessary for our purposes. However, we will see the η-function play an important role in the rest of our discussion.

While we have seen the basic definitions needed for our purposes, the reader can find these definitions and a more detailed discussion of modular forms in [6] or [14].

Chapter 3

Relating Quadratic Forms and Modular Forms

3.1 Theta Series

In this section, we focus on the subject of theta series for quadratic forms. Since we are only interested in binary quadratic forms, we will consider only this case. This theory, along with the generalization to all quadratic forms, is described by Zagier in [4].

Let $Q(x, y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form.

Definition 3.1. *The theta series of Q is defined to be*

$$\theta_Q(z) = \sum_{n=0}^{\infty} r(Q, n)q^n,$$

where $q = e^{2\pi iz}$, and $r(Q, n)$ denotes the number of representations of n by Q.

We will soon see that $\theta_Q(z)$ is a modular form, but first we must gather more information. The quadratic form $Q(x, y)$ can be written in the form

$$Q(x, y) = \frac{1}{2}(x, y)A(x, y)^t, \tag{3.1}$$

where $A = \left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$. Note that A is symmetric. The symmetric matrix A is called *positive definite* if $(x, y)A(x, y)^t > 0$ for all nonzero $(x, y) \in \mathbb{R}^2$. Then we can see that since Q is positive definite, we must have that A is positive definite.

Proposition 3.2. *Every positive definite matrix A is invertible.*

We omit the proof of this proposition for brevity. (See [11], Chapter 6 Section 7.)

By Proposition 3.2, we may now assume that A from (3.1) has an inverse, and we will use this fact in the next definition.

Definition 3.3. *If $Q(x,y) = \frac{1}{2}(x,y)A(x,y)^t$, then the level of Q is the smallest positive integer, $N = N_Q$, such that NA^{-1} is again a matrix with integral elements and the a_{ii} are even for each i.*

Example 3.4. *If $Q_0(x,y) = x^2 + xy + 6y^2$, then $Q_0(x,y) = (x,y)A(x,y)^t$ where $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 12 \end{smallmatrix}\right)$. Then we have that $A^{-1} = \left(\begin{smallmatrix} 12/23 & -1/23 \\ -1/23 & 2/23 \end{smallmatrix}\right)$. From this, we can see that the level of Q_0 is 23.*

Definition 3.5. *If $Q(\mathbf{x}) = \frac{1}{2}(x,y)A(x,y)^t$, then the* discriminant $\Delta = \Delta_Q$ of A *is defined to be $det(A)$.*

Example 3.6. *Let $Q(x,y) = a^2 + bxy + cy^2$. Then $A = \left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$, and the discriminant of A is $det(A) = b^2 - 4ac$. Then we see that the discriminant of A is the discriminant of Q.*

There is an associated character to our quadratic form $Q(x,y) = (x,y)A(x,y)^t$ with level N and discriminant Δ of A. The associated character, χ_Δ (Kronecker symbol), is the unique Dirichlet character modulo N satisfying

$$\chi_\Delta(p) = \left(\frac{\Delta}{p}\right) \text{ (Legendre symbol)}$$

for any odd prime p that does not divide N. (See [15], p. 303.)

These ideas lead us to an important theorem.

Theorem 3.7. *Let Q be a positive definite binary quadratic form of level N and discriminant Δ. Then θ_Q is a modular form on $\Gamma_0(N)$ of weight 1 and character χ_Δ. In particular,*

$$\theta_Q\left(\frac{az+b}{cz+d}\right) = \chi_\Delta(a)(cz+d)^k\theta_Q(z)$$

for all $z \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

We omit the proof of this theorem for brevity. (See [1], Theorem 2.2.)

3.1.1 Hecke Theory

Let Λ be a lattice on $\mathbb{C}$ with basis $\{\omega_1, \omega_2\}$. For each integer $m \geq 1$, for any given k there exists a linear operator $T_m : \mathcal{M}_k \to \mathcal{M}_k$, called the m^{th} *Hecke operator*. For a modular form F of degree $-k$ on lattices $\Lambda \subset \mathbb{C}$, we have (up to a suitable normalizing constant ensuring that the image of a form with integral Fourier coefficients has integral Fourier coefficients) $T_m F(\Lambda) = \sum F(\Lambda')$ where the

sum is over sublattices $\Lambda' \subset \Lambda$ of index m. Translating this using the fact that $F(<1,z>) = f(z)$ for a modular form f of weight k, the operation is

$$T_m f(z) = m^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})\backslash M_m} (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \tag{3.2}$$

for $z \in \mathbb{H}$, where M_m denotes the set of 2×2 integral matrices of determinant m, and $SL_2(\mathbb{Z})\backslash M_m$ is a set of representatives from M_m such that each sublattice $\Lambda' = \Lambda(A)$ for exactly one element $A \in SL_2(\mathbb{Z})\backslash M_m$. (Note that the constant m^{k-1} has been introduced for later convenience.)

Our current goal is to use our theory to express $T_m f(z)$ in a more useful form. By Proposition 2.42, we may choose our set $SL_2(\mathbb{Z})\backslash M_m$ to be the set of matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ such that $0 < b < d$ and $ad = m$. Combining this fact with (3.2), we have

$$T_m f(z) = m^{k-1} \sum_{\substack{ad=m \\ a,d>0 \\ 0<b<d}} d^{-k} f\left(\frac{az+b}{d}\right),$$

or, in a another form,

$$T_m f(z) = m^{k-1} \sum_{\substack{ad=m \\ a,d>0}} d^{-k} \sum_{b \bmod d} f\left(\frac{az+b}{d}\right).$$

Using the Fourier expansion of f, we can now carry this equation a few steps forward:

$$\begin{aligned}
T_m f(z) &= m^{k-1} \sum_{\substack{ad=m \\ a,d>0}} d^{-k} \sum_{b \bmod d} \sum_{n \geq 0} a_n e^{2\pi i n(az+b)/d} \\
&= m^{k-1} \sum_{\substack{ad=m \\ a,d>0}} d^{-k} \sum_{n \geq 0} a_n e^{2\pi i n a z/d} \sum_{b \bmod d} e^{2\pi i b n/d} \\
&= m^{k-1} \sum_{\substack{ad=m \\ a,d>0}} d^{-k} d \sum_{\substack{n \geq 0 \\ d|n}} a_n e^{2\pi i n a z/d} \\
&= \sum_{\substack{d|m \\ d>0}} \left(\frac{m}{d}\right)^{k-1} \sum_{\substack{n \geq 0 \\ d|n}} a_n q^{mn/d^2}.
\end{aligned}$$

We can conclude that

$$T_m f(z) = \sum_{n \geq 0} \left(\sum_{\substack{r|(m,n) \\ r>0}} r^{k-1} a_{mn/r^2} \right) q^n. \tag{3.3}$$

Since T_m is a linear operator on functions, it is natural to consider the eigenfunctions of T_m. We call $f \in M_k$ a *simultaneous eigenform* if it is an eigenfunction of the T_m for all m with corresponding eigenvalues λ_m. If f is a simultaneous eigenform, then

$$T_m f(z) = \lambda_m f(z) = \lambda_m \sum_{n=0}^{\infty} a_n q^n. \tag{3.4}$$

We have the the coefficient of q in the expansion of $T_m f(z)$ is a_m when using (3.3) and $\lambda_m a_1$ when using (3.4). Thus, $\lambda_m a_1 = a_m$. We can now conclude that if f is not identically zero, then $a_1 \neq 0$. If we normalize f by dividing all coefficients by a_1, then f is called a *normalized Hecke eigenform*. In this case we have that

$$T_m f = a_m f \tag{3.5}$$

and

$$a_m a_n = \sum_{r|(m,n)} r^{k-1} a_{mn/r^2} \quad \text{if } m, n \geq 1. \tag{3.6}$$

The following is a theorem of Hecke.

Theorem 3.8. *$\mathcal{M}_k$ has a basis of normalized simultaneous eigenforms for all k, and that basis is unique.*

We omit the proof of this theorem for brevity. (See [9], Section 7.3.)

We conclude this section by noting that Hecke's theory generalizes to congruence subgroups of $SL_2(\mathbb{Z})$. (See [4], p. 39).

3.1.2 L-series of Eigenforms

We begin by defining the L-series of a modular form.

Definition 3.9. *If $f(z) = \sum_{n=0}^{\infty} a_n q^n$ is a modular form (resp. a normalized simultaneous eigenform) in any space of modular forms, then we define the L-series (resp. Hecke L-series) of f to be*

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

The goal of this section is to develop a different and useful representation for $L(f, s)$ where f is a normalized simultaneous eigenform in $\mathcal{M}_k$. In particular, we will show that

$$L(f, s) = \prod_{p \in P} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}$$

where P is the set of prime numbers. First, using (3.6) when $(m,n)=1$, we obtain that

$$a_m a_n = a_{mn}. \tag{3.7}$$

Using (3.6) when $m = p^v$ and $n = p$ for p prime, we obtain that

$$a_{p^{v+1}} = a_p a_{p^v} - p^{k-1} a_{p^{v-1}}. \tag{3.8}$$

By (3.7), the Fourier coefficients of f are multiplicative. Thus, (see [4], Page 39), the Hecke L-series of f has the Euler product,

$$L(f,s) = \prod_{p \in P} \left(1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + ...\right), \tag{3.9}$$

where P is the set of prime numbers.

Next we will use a proposition to rewrite the Euler product in an improved form.

Proposition 3.10. *Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ be a normalized simultaneous eigenform in $\mathcal{M}_k$. Then for each prime p,*

$$\sum_{v=0}^{\infty} a_{p^v} p^{-vs} = \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$

Proof. First, define a new series

$$\left(\sum_{v=0}^{\infty} a_{p^v} p^{-vs}\right)(1 - a_p p^{-s} + p^{k-1-2s}).$$

The coefficient of p^{-s} in this series is $a_p - a_1 a_p = a_p - a_p 0$ since $a_1 = 1$ for a normalized eigenform. For $n \geq 1$, the coefficient of $p^{-(n+1)s}$ in this series is $a_{p^{n+1}} - a_{p^n} a_p + a_{p^{n-1}} p^{k-1} = 0$ by (3.8). Then we find that the sum of the series is $a_1 = 1$. □

Applying Proposition 3.10 to (3.9), we can see that

$$L(f,s) = \prod_{p \in P} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}},$$

which is Hecke's fundamental Euler product for the L-series of a normalized Hecke eigenform $f \in \mathcal{M}_k$.

3.2 Modular Forms and Algebraic Number Theory

We can learn more about the number of representations $r(Q,n)$ of n by the binary quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ by considering the weight one theta series $\theta_Q(z) = \sum_{n=0}^{\infty} r(Q,n)q^n$ from Definition 3.1. In this section, consider the case where Q is a binary quadratic form with fundamental discriminant $d < 0$.

Recall that by Theorem 2.33, we know $r(Q,n) = w_d \cdot r(\mathcal{A},n)$. Then we can express the L-series

$$L(\theta_Q, s) = \sum_{n=1}^{\infty} \frac{r(Q,n)}{n^s}$$

as

$$L(\theta_Q, s) = w_d \sum_{A \in \mathcal{A}} N(A)^{-s},$$

where the sum is over the integral ideals of $\mathcal{A}$. We will define the "partial zeta-function" $\zeta_{K,\mathcal{A}}(s)$ by the following:

$$\zeta_{K,\mathcal{A}}(s) = \sum_{A \in \mathcal{A}} N(A)^{-s}.$$

Let χ be a character on H_d, and let $K = \mathbb{Q}(\sqrt{d})$. Then we can define a new L-series

$$L_K(s,\chi) = \sum_{A} \frac{\chi(A)}{N(A)^s},$$

where the sum is over the integral ideals of O_d. This can be rewritten as

$$L_K(s,\chi) = \sum_{\mathcal{A} \in H_d} \chi(\mathcal{A}) \sum_{A \in \mathcal{A}} N(A)^{-s} = \sum_{\mathcal{A} \in H_d} \chi(\mathcal{A}) \zeta_{K,\mathcal{A}}(s).$$

Next we will see a connection between modular forms and $L_K(s,\chi)$ thus justifying our L-series notation. We know $\theta_Q(z) = \sum_{n=1}^{\infty} r(Q,n)q^n$. Then if we define

$$\theta_{\mathcal{A}}(z) = w_d \sum_{n=1}^{\infty} r(\mathcal{A},n)q^n,$$

we have that $\theta_Q(z) = \theta_{\mathcal{A}}(z)$ where $\mathcal{A}$ is the ideal class corresponding to Q. Next we introduce the function

$$f_\chi(z) = w_d^{-1} \sum_{\mathcal{A} \in H_d} \chi(\mathcal{A}) \theta_{\mathcal{A}}(z). \tag{3.10}$$

Since $\theta_{\mathcal{A}}(z) = \theta_Q(z)$, using Theorem 3.7 along with the fact that adding weight one modular forms results in a weight one modular form, we can conclude that $f_\chi(z)$ is a weight one modular form.

Also, using Definition 3.9, it can be seen that the L-series of $f_\chi(z)$ is $L_K(s,\chi)$. Indeed, we have

$$\begin{aligned} L(f_\chi, s) &= \sum_{n=1}^{\infty} \frac{\sum_{\mathcal{A}\in H_d} \chi(\mathcal{A}) r(\mathcal{A}, n)}{n^s} \\ &= \sum_{\mathcal{A}\in H_d} \chi(\mathcal{A}) \sum_{n=1}^{\infty} \frac{r(\mathcal{A}, n)}{n^s} \\ &= \sum_{\mathcal{A}\in H_d} \chi(\mathcal{A}) \sum_{A\in\mathcal{A}} N(A)^{-s} \\ &= \sum_{\mathcal{A}\in H_d} \chi(\mathcal{A}) \zeta_{K,\mathcal{A}}(s) \\ &= L_K(s,\chi) \end{aligned}$$

By the unique prime decomposition of ideals in K, we can use a process to sieve the prime ideals out of the sum and see that $L_K(s,\chi)$ has a resulting Euler product. (See [10], Section 1.5.) The condition of f being a Hecke eigenform is equivalent to its L-function series having an Euler product, (see [6]). Then we can conclude that f_χ is a Hecke eigenform. The following theorem shows us what form the the Euler product will have.

Theorem 3.11. *Let $f \in \mathcal{M}_k(\Gamma_0(N), \chi)$, $f(z) = \sum_{n=0}^{\infty} a_n q^n$. The following are equivalent:*

1. *f is a normalized eigenform*
2. *$L(s, f)$ has an Euler product expansion*

$$L(s,f) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1},$$

where the product is taken over all primes.

We omit the proof of this theorem for brevity. (See [6], Theorem 5.9.2.)

Next we will consider the specific character $\chi = \chi_0$ where χ_0 is the trivial character.

Definition 3.12. *Let $K = \mathbb{Q}(\sqrt{d})$. Then the Dedekind zeta function of K is*

$$\zeta_K(s) = \sum_A N(A)^{-s},$$

where the sum is over the integral ideals of O_d.

If $\chi = \chi_0$, then we can see that

$$L_K(s,\chi) = \sum_A N(A)^{-s} = \zeta_K(s).$$

As we progress, we will rely heavily on the character

$$\epsilon_{D_d}(n) = \left(\frac{D_d}{n}\right) \quad \text{(Kronecker symbol)}.$$

Our goal now is to prove the following theorem.

Theorem 3.13. *Let K be a quadratic field. Then for $Re(s) > 1$,*

$$\zeta_K(s) = \zeta(s)L(s, \epsilon_{D_d}),$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function and $L(s, \epsilon_{D_d}) = \sum_{n=1}^{\infty} \epsilon_{D_d}(n)n^{-s}$ is the Dirichlet L-series of the character $\epsilon_{D_d}(n)$.

We will use this theorem to gain more information about the number $r(Q, n)$. In particular, we will prove the following proposition.

Proposition 3.14. *Let Q be a positive definite binary quadratic form with fundamental discriminant $d < 0$. Then*

$$\sum_{[Q]\in C(d)} r(Q, n) = w_d \sum_{b|n} \epsilon_{D_d}(b).$$

Remark 3.15. *In order to reach our goals, we will omit the proofs for the lemmas leading to the proof of Theorem 3.13. For more details regarding the following lemmas, we refer the reader to [19] where the following lemmas are given with more detail. We will also provide additional sources for lemmas as we proceed.*

Lemma 3.16. *Let (a_n) be a sequence of complex numbers. Suppose there exist $c, r > 0$ such that $\left|\sum_{n=1}^{M} a_n\right| \leq cM^r$ for all $M \geq 1$. Then the Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges for all s with $Re(s) > r$.*

(For proof, see [12], Chapter 7 Lemma 1.)

Lemma 3.17. *Let (a_n) be a multiplicative sequence of complex numbers. Suppose there exists $c > 0$ such that $\sum_{n=1}^{M} |a_n| \leq cM$ for all $M \geq 1$. Then $\sum_{n=1}^{\infty} a_n n^{-s} = \prod_p \left(\sum_{j=0}^{\infty} a_{p^j} p^{-js}\right)$ for all s with $Re(s) > 0$.*

(For proof, see [2], Theorem 11.7.)

Let υ_m be the number of ideals of O_d with norm m.

Lemma 3.18. *The sequence (υ_n) is multiplicative. Additionally, for prime p and $Re(s) > 1$,*

$$\sum_{n=0}^{\infty} \frac{\upsilon_{p^n}}{p^{ns}} = \begin{cases} (1-p^{-s})^{-2} \text{ if } \left(\frac{D_d}{p}\right) = 1, \\ (1-p^{-s})^{-1} \text{ if } \left(\frac{D_d}{p}\right) = 0, \\ (1-p^{-2s})^{-1} \text{ if } \left(\frac{D_d}{p}\right) = -1. \end{cases}$$

(For proof, see [19], Lemma 5.1.)

Now we are ready to consider specifically $\zeta_K(s)$. First we note that since $\zeta_K(s) = \sum_A N(A)^{-s}$ and υ_n is the number of ideals of O_d with norm n, then we have that $\zeta_K(s) = \sum_{n=1}^{\infty} \upsilon_n n^{-s}$.

Lemma 3.19. *Let*

$$A_d = \begin{cases} \sqrt{-d} & -d \equiv 1, 2 \pmod 4, \\ \frac{\sqrt{-d}}{2} & -d \equiv 3 \pmod 4. \end{cases}$$

There exists a constant c such that

$$\left| \sum_{n=1}^{M} \upsilon_n - \frac{h_d \pi}{A_d w_d} M \right| \leq c\sqrt{M},$$

for all $M \geq 1$.

(For proof, see [19], Proposition 5.2.)

This brings us to a point where we can prove Theorem 3.13.

Proof. To show that $\zeta_K(s)$ converges, first we will show that there exists a constant c such that

$$\left| \sum_{n=1}^{M} \upsilon_n \right| \leq \left(\left| \frac{h_d \pi}{Aw} \right| + c \right) M \tag{3.11}$$

for all $M \geq 1$. By Lemma 3.19, we know there exists a constant c such that

$$\left| \sum_{n=1}^{M} \upsilon_n - \frac{h_d \pi}{A_d w_d} M \right| \leq c\sqrt{M}$$

for all $M \geq 1$. Using the reverse triangle inequality, we see

$$\left| \left| \sum_{n=1}^{M} \upsilon_n \right| - \left| \frac{h_d \pi}{A_d w_d} M \right| \right| \leq \left| \sum_{n=1}^{M} \upsilon_n - \frac{h_d \pi}{A_d w_d} M \right| \leq c\sqrt{M}.$$

Then

$$\left| \sum_{n=1}^{M} \upsilon_n \right| - \left| \frac{h_d \pi}{A_d w_d} M \right| \leq c\sqrt{M},$$

and we can conclude that

$$\left| \sum_{n=1}^{M} \upsilon_n \right| \leq \left(\left| \frac{h_d \pi}{Aw} \right| + c \right) M$$

for all $M \geq 1$. Notice that by Lemma 3.16, using (3.11), we know that $\zeta_K(s)$ converges for $Re(s) > 1$.

Next we will show that $\zeta_K(s)$ has the Euler product

$$\zeta_K(s) = \prod_{p,\left(\frac{D_d}{p}\right)=1} (1-p^{-s})^{-2} \prod_{p,\left(\frac{D_d}{p}\right)=0} (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=-1} (1-p^{-2s})^{-1}.$$

Since (υ_n) is multiplicative and $\upsilon_n > 0$ for each n, by Lemma 3.17,

$$\sum_{n=1}^{\infty} \upsilon_n n^{-s} = \prod_p \left(\sum_{j=0}^{\infty} \upsilon_{p^j} p^{-js} \right).$$

Then by Lemma 3.18,

$$\prod_p \left(\sum_{j=0}^{\infty} \upsilon_{p^j} p^{-js} \right) = \prod_{p,\left(\frac{D_d}{p}\right)=1} (1-p^{-s})^{-2} \prod_{p,\left(\frac{D_d}{p}\right)=0} (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=-1} (1-p^{-2s})^{-1}.$$

Thus, we have

$$\zeta_K(s) = \prod_{p,\left(\frac{D_d}{p}\right)=1} (1-p^{-s})^{-2} \prod_{p,\left(\frac{D_d}{p}\right)=0} (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=-1} (1-p^{-2s})^{-1}, \tag{3.12}$$

where the first product is over the set of primes, p, such that $\left(\frac{D_d}{p}\right) = 1$ and similarly for the other two products. Continuing to simplify (3.12), we see

$$\begin{aligned}
\zeta_K(s) &= \prod_{p,\left(\frac{D_d}{p}\right)=1} (1-p^{-s})^{-2} \prod_{p,\left(\frac{D_d}{p}\right)=0} (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=-1} (1-p^{-s})^{-1}(1+p^{-s})^{-1} \\
&= \prod_p (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=1} (1-p^{-s})^{-1} \prod_{p,\left(\frac{D_d}{p}\right)=-1} (1+p^{-s})^{-1} \\
&= \prod_p (1-p^{-s})^{-1} \prod_p \left(1 - \left(\frac{D_d}{p}\right) p^{-s}\right)^{-1} \\
&= \zeta(s) L(s, \epsilon_K).
\end{aligned}$$

□

Using Theorem 3.13, we will now prove Proposition 3.14.

Proof. Recall that $L(\theta_Q, s) = \sum_{n=1}^{\infty} \frac{r(Q,n)}{n^s} = w_d \zeta_{K,\mathcal{A}}(s)$. Then we have that for $Re(s) > 1$,

$$\begin{aligned}
\zeta_K(s) &= \sum_{\mathcal{A} \in H_d} \zeta_{K,\mathcal{A}}(s) \\
&= \frac{1}{w_d} \sum_{[Q] \in C(d)} \sum_{n=1}^{\infty} \frac{r(Q,n)}{n^s} \\
&= \frac{1}{w_d} \sum_{n=1}^{\infty} \frac{\sum_{[Q]} r(Q,n)}{n^s}.
\end{aligned} \tag{3.13}$$

Note that we are able to interchange sums since $\zeta_K(s)$ converges absolutely on some half-plane. By Theorem 3.13,

$$\sum_{\mathcal{A}\in H_d} \zeta_{K,\mathcal{A}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \left(\frac{D_d}{n}\right) \frac{1}{n^s}. \tag{3.14}$$

By comparing coefficients of n^{-s}, we will see that for each n,

$$\sum_{[Q]} r(Q,n) = w_d \sum_{b|n} \epsilon_{D_d}(b).$$

The coefficient of n^{-s} in (3.13) is $\frac{1}{w_d}\sum_{[Q]} r(Q,n)$. In (3.14), n^{-s} appears exactly when the product of the indices of the two sums is n. In such a case, when $jk = n$, we see that we collect the term

$$j^{-s}\left(\frac{D_d}{k}\right)k^{-s} = \left(\frac{D_d}{k}\right)n^{-s}.$$

From this we can see that the coefficient of n^{-s} in (3.14) is $\sum_{b|n}\epsilon_{D_d}(b)$. □

With the theory we have developed, we wish to return to our consideration of the weight one modular form $f_\chi(z)$ from (3.10). We will continue to let $\chi = \chi_0$. Using our theory, we now see

$$\begin{aligned}
f_{\chi_0}(z) &= \frac{1}{w_d}\sum_{\mathcal{A}} \theta_{\mathcal{A}}(z) \\
&= \frac{1}{w_d}\sum_{[Q]} \theta_Q(z) && (3.15)\\
&= \frac{1}{w_d}\sum_{n=0}^{\infty}\left(\sum_{[Q]} r(Q,n)\right)q^n && (3.16)\\
&= \frac{1}{w_d}\sum_{[Q]} r(Q,0) + \frac{1}{w_d}\sum_{n=1}^{\infty}\left(w_d\sum_{b|n}\left(\frac{D_d}{b}\right)\right)q^n \\
&= \frac{h(d)}{w_d} + \sum_{n=1}^{\infty}\left(\sum_{b|n}\left(\frac{D_d}{b}\right)\right)q^n. && (3.17)
\end{aligned}$$

Using the fact the $\theta_Q(z) = \theta_{\mathcal{A}}(z)$ when $[Q]$ and $\mathcal{A}$ are corresponding classes, it can be seen that for any character χ,

$$f_\chi(z) = w_d^{-1}\sum_{\mathcal{A}} \chi(\mathcal{A})\theta_{Q_{\mathcal{A}}}(z),$$

where $Q_{\mathcal{A}}$ is a quadratic form from the class $[Q]$ corresponding to $\mathcal{A}$. Additionally, if the order of χ is greater than two, then f_χ is a cusp form (see [4], p.42).

Chapter 4

The Case $d = -23$

We now can consider the case $d = -23$ as given by Zagier in [4]. In the case of $d = -23$, it turns out that $h_d = 3$. (See [3], p. 42.) Then we know by Theorem 2.32 that there exist three equivalence classes of binary quadratic forms in $C(d)$. These three classes can be represented by the three forms

$$\begin{aligned} Q_0(x,y) &= x^2 + xy + 6y^2, \\ Q_1(x,y) &= 2x^2 + xy + 3y^2, \\ Q_2(x,y) &= 2x^2 - xy + 3y^2. \end{aligned} \tag{4.1}$$

As shown in Example 2.17, none of these forms are property equivalent. Thus, we can tell that these three forms are representatives of the three different classes in $C(-23)$. However, we saw in Example 2.4 that Q_1 is equivalent to Q_2, so Q_1 and Q_2 represent the same integers. Thus, the theta series of Q_1 and Q_2 are equal, so we find that our three representative forms have only two distinct theta series, θ_{Q_0} and θ_{Q_1}. Using the fact that $w_{-23} = 2$ and $D_{-23} = -23$, by (3.15) and (3.17), we have

$$f_{\chi_0}(z) = \frac{1}{2}(\theta_{Q_0}(z) + 2\theta_{Q_1}(z)) = \frac{3}{2} + \sum_{n=1}^{\infty} \left(\sum_{b|n} \left(\frac{-23}{b} \right) \right) q^n.$$

Suppose χ is one of the two non-trivial characters on H_d. Since $h_d = 3$, χ must take on values z that satisfy $z^3 = 1$. First notice that using the isomorphism from Theorem 2.32, we know that the quadratic form $Q_0(x,y) = x^2 + xy + 6y^2$ gets mapped to the ideal class containing the ideal

$$[1, \frac{-1 + \sqrt{-23}}{2}] = O_{-23} = (1).$$

Thus, Q_0 gets mapped to the identity of the ideal class group, so $\chi(Q_0) = 1$. Also, χ will take values $e^{\pm 2\pi i/3}$ on Q_1 and Q_2. Using these results along with (3.10), we see that in this case we have that $f_\chi = \frac{1}{2}(\theta_{Q_0} - \theta_{Q_1})$ which is a Hecke eigenform in the space of cusp forms over the group $\Gamma_0(23)$

with character $\epsilon_{-23}(n) = \left(\frac{-23}{n}\right)$ (Kronecker symbol). By Theorem 3.11, if the Fourier expansion of f_χ is $f_\chi(z) = \sum_{n=0}^{\infty} a_n q^n$, then its L-series has the form

$$L(f_\chi, s) = \prod_p \frac{1}{1 - a_p p^{-s} + \epsilon_{-23}(p) p^{-2s}}.$$

We also note that for any prime p, $\epsilon_{-23}(p)$ equals the Legendre symbol $\left(\frac{p}{23}\right)$ because if p is an odd prime,

$$\begin{aligned} \left(\frac{-23}{p}\right) &= (-1)^{\frac{p-1}{2}} \left(\frac{23}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{23-1}{2}} \left(\frac{p}{23}\right) \\ &= \left(\frac{p}{23}\right), \end{aligned}$$

and by quadratic reciprocity, we additionally have that

$$\left(\frac{-23}{2}\right) = 1 = \left(\frac{2}{23}\right).$$

Now we can determine a_p for each prime p.

Theorem 4.1. *Let a_p be the Fourier coefficient of q^p for the modular form f_χ where χ is one of the nontrivial characters on H_{-23}. Then*

$$a_p = \begin{cases} 1 & \text{if } p = 23, \\ 0 & \text{if } \left(\frac{p}{23}\right) = -1, \\ 2 & \text{if } \left(\frac{p}{23}\right) = 1 \text{ and } p \text{ is represented by } Q_0, \\ -1 & \text{if } \left(\frac{p}{23}\right) = 1 \text{ and } p \text{ is represented by } Q_1. \end{cases} \tag{4.2}$$

Proof. Since $f_\chi(z) = \frac{1}{2}(\theta_{Q_0} - \theta_{Q_1})$, we have

$$a_p = \frac{1}{2}(r(Q_0, p) - r(Q_1, p)). \tag{4.3}$$

However, we also know

$$\sum_{[Q]} r(Q, n) = w \sum_{b|n} \epsilon_{D_d}(b),$$

so

$$r(Q_0, p) + 2r(Q_1, p) = 2\left(1 + \left(\frac{p}{23}\right)\right).$$

These equations, along with the fact that $r(Q_0, p)$ and $r(Q_1, p)$ must be even (because if (x, y) is a solution then $(-x, -y)$ is a solution) logically lead us to the conclusion of our theorem. □

We will next find a connection between the a_p from (4.2) and the eta product $\eta(z)\eta(23z)$, where $\eta(z)$ is as defined in (2.9). We will first prove that the space $\mathcal{S}_1(\Gamma_0(23), \epsilon_{-23})$ is one-dimensional and spanned by $\eta(z)\eta(23z)$. We will need a few lemmas to reach this conclusion. For brevity, we will omit the proofs of some lemmas, but we will refer the reader to the source of the lemma.

Lemma 4.2. *If $f(z) = \prod_{\delta|N} \eta(\delta z)^{r_\delta}$ with $k = \frac{1}{2}\sum_{\delta|N} r_\delta \in \mathbb{Z}$ and with the additional properties that*

$$\sum_{\delta|N} \delta r_\delta \equiv 0 \pmod{24}$$

and

$$\sum_{\delta|N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24},$$

then $f(z) \in S_k(\Gamma_0(N), \chi)$ where χ is defined by $\chi(d) := \left(\frac{(-1)^k s}{d}\right)$, where $s := \prod_{\delta|N} \delta^{r_\delta}$.

(See [14], Theorem 1.64.)

Lemma 4.3. *Let $f(z) = \eta(z)\eta(23z)$ where*

$$\eta(z)\eta(23z) = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}). \tag{4.4}$$

Then $f(z) \in \mathcal{S}_1(\Gamma_0(23), \epsilon_{-23})$.

Proof. We apply Lemma 4.2 with $N = 23$, and $f(z) = \eta(z)\eta(23z)$. In this case, $k = 1$. We see that

$$23(1) + 1(1) = 24 \equiv 0 \pmod{24}$$

and

$$\frac{23}{1}(1) + \frac{23}{23}(1) = 24 \equiv 0 \pmod{24}.$$

Then we conclude that $f(z) \in \mathcal{S}_1(\Gamma_0(23), \chi)$ where χ is defined by $\chi(n) = \left(\frac{-23}{n}\right) = \epsilon_{-23}(n)$. □

Lemma 4.4. *Let k and N be positive integers such that $k(N+1)=24$. If $\mathcal{S}_k(\Gamma_1(N))$ is nonzero, then it is one-dimensional space spanned by $\eta(z)\eta(23z)$.*

(See [6], Proposition 3.2.2.)

Lemma 4.5. *The space $\mathcal{S}_k(\Gamma_1(N))$ has the following decomposition (where the direct sum is over all Dirichlet characters modulo N):*

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{S}_k(\Gamma_0(N), \chi).$$

(See [14], p.5.)

Theorem 4.6. *The space $S_1(\Gamma_0(23), \epsilon_{-23})$ is one-dimensional and is spanned by $\eta(z)\eta(23z)$.*

Proof. By Lemma 4.3, we know that $\mathcal{S}_1(\Gamma_0(23), \epsilon_{-23})$ is nonzero. Then since ϵ_{-23} is a Dirichlet character modulo 23, we know by Lemma 4.5 that $\mathcal{S}_1(\Gamma_1(23))$ is nonzero. Thus, by Lemma 4.4, $\mathcal{S}_1(\Gamma_1(23))$ is one-dimensional and is spanned by $\eta(z)\eta(23z)$. Since

$$\mathcal{S}_1(\Gamma_1(23)) = \bigoplus_{\chi} \mathcal{S}_1(\Gamma_0(23), \chi),$$

and $\eta(z)\eta(23z) \in \mathcal{S}_1(\Gamma_0(23), \epsilon_{-23})$, we must also have that $\mathcal{S}_1(\Gamma_0(23), \epsilon_{-23})$ is one-dimensional and spanned by $\eta(z)\eta(23z)$. □

In the next section, it will be proved that the a_p from (4.2) are equal to the Fourier coefficients of q^p in the product (4.4).

4.1 A Theorem of van der Blij

Let Q_0, Q_1 and Q_2 be as defined in (4.1). From (3.16) and (3.17), we have the relation

$$r(Q_0, n) + 2r(Q_1, n) = 2\sum_{d|n} \left(\frac{-23}{d}\right),$$

noting that $2r(Q_1, n) = r(Q_1, n) + r(Q_2, n)$ since Q_1 and Q_2 are equivalent. However, we already saw that for any prime p,

$$\left(\frac{-23}{p}\right) = \left(\frac{p}{23}\right).$$

Additionally,

$$\left(\frac{-23}{1}\right) = 1 = \left(\frac{1}{23}\right).$$

Then for each positive integer n, we have that

$$\left(\frac{-23}{n}\right) = \left(\frac{n}{23}\right).$$

Thus,

$$r(Q_0, n) + 2r(Q_1, n) = 2\sum_{d|n} \left(\frac{d}{23}\right). \tag{4.5}$$

Along with this observation, we will also need the following lemma to prove the theorem of van der Blij.

Lemma 4.7. *(The Pentagonal Number Theorem)*

For any number x,

$$\prod_{k=1}^{\infty}(1-x^k)=\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{1}{2}m(3m+1)}.$$

We omit the proof of this lemma for brevity. (See [7], p. 225.)

Now we are prepared to prove one of our main theorems, Theorem 1.1. The proof we provide is as given by van der Blij in [18].

Proof. We will use the identity from Lemma 4.7

$$\prod_{k=1}^{\infty}(1-x^k)=\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{1}{2}m(3m+1)}.$$

With some manipulation, we can see that

$$\prod_{k=1}^{\infty}(1-x^k)=x^{-\frac{1}{24}}\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{1}{24}(6m+1)^2}.$$

Then using $x=q^{23}$, we have

$$\prod_{k=1}^{\infty}(1-q^{23k})=q^{-\frac{23}{24}}\sum_{m=-\infty}^{\infty}(-1)^m q^{\frac{23}{24}(6m+1)^2}.$$

Now we have that

$$\begin{aligned}\sum_{n=1}^{\infty}t(n)q^n &= q(q^{\frac{-1}{24}})(q^{\frac{-23}{24}})\sum_{m=-\infty}^{\infty}(-1)^m q^{\frac{1}{24}(6m+1)^2}\sum_{p=-\infty}^{\infty}(-1)^p q^{\frac{23}{24}(6p+1)^2}\\ &= \sum_{m,p=-\infty}^{\infty}(-1)^{m+p}q^{\frac{1}{24}(6m+1)^2+\frac{23}{24}(6p+1)^2}. \qquad (4.6)\end{aligned}$$

Let $u=6m+1$ and $v=6p+1$. Using (4.6), we can see that the term q^n appears whenever $u^2+23v^2=24n$ and $m+p$ is even which occurs when $u\equiv v\equiv 1 \pmod{12}$ or $u\equiv v\equiv 7 \pmod{12}$. We can also see that the term $-q^n$ appears whenever $u^2+23v^2=24n$ and $m+p$ is odd which occurs when $u\equiv 1$, $v\equiv 7$ or $u\equiv 7$, $v\equiv 1 \pmod{12}$. We will count the number of times q^n and $-q^n$ occur, and then we will be able to deduce the number $t(n)$.

First we claim that $r(Q_0,n)$ is the number of solutions (u,v) of $u^2+23v^2=24n$ when $u\equiv v \pmod{12}$. We can see this by noting

$$\begin{aligned}24Q_0(x,y) &= 24(x^2+xy+6y^2)\\ &= (x+12y)^2+23x^2.\end{aligned}$$

Second we claim that $r(Q_1, n)$ is the number of solutions (u, v) of $u^2 + 23v^2 = 24n$ with $u \equiv 5v \pmod{12}$. To prove this, we compare $r(Q_1, n) = 2x^2+xy+3y^2 = n$ and $(5x+7y)^2+23(x-y)^2 = 24n$. When the latter equation is expanded and simplified, it directly implies the former equation. Also, we see from the latter equation that $u = 5x + 7y$ and $v = x - y$. Combining these, we have $u = 5v + 12y$ which implies that $u \equiv 5v \pmod{12}$.

Now, along with the above two claims, we will use the fact that the number of solutions (u, v) congruent (a, b) and the number of those congruent $(-a, b)$, $(a, -b)$, and $(-a, -b)$ must all be equal. For example, if $u \equiv v \equiv 2 \pmod{12}$, then $r(Q_1, n) = r(Q_0, n)$ since in the second claim we will have $u \equiv 10$, $v \equiv 2 \pmod{12}$, and $(10, 2) \equiv (-2, 2) \pmod{12}$. After all possible combinations are considered, we can see that

$$r(Q_0, n) - r(Q_1, n) = 2t(n). \tag{4.7}$$

Now combining (4.5) and (4.7), we obtain (1.2) and (1.3). □

We are now prepared to prove that the a_p from (4.2) are equal to the Fourier coefficients of q^p in the product (4.4).

Corollary 4.8. *Let*

$$a_p = \begin{cases} 1 & \text{if } p = 23, \\ 0 & \text{if } \left(\frac{p}{23}\right) = -1, \\ 2 & \text{if } \left(\frac{p}{23}\right) = 1 \text{ and } p \text{ is represented by } Q_0, \\ -1 & \text{if } \left(\frac{p}{23}\right) = 1 \text{ and } p \text{ is represented by } Q_1. \end{cases} \tag{4.8}$$

Then a_p is equal to the Fourier coefficient of q^p for the modular form $\eta(z)\eta(23z)$.

Proof. Let $\eta(z)\eta(23z) = \sum_{n=1}^{\infty} t(n)q^n$. Then $t(p)$ is the Fourier coefficient of q^p in the Fourier expansion of $\eta(z)\eta(23z)$. By Theorem 1.1, we have that

$$\begin{aligned} r(Q_0, p) &= \frac{2}{3}\sum_{d|p}\left(\frac{d}{23}\right) + \frac{4}{3}t(p) \\ &= \frac{2}{3} + \frac{4}{3}t(p), \end{aligned} \tag{4.9}$$

and

$$\begin{aligned} r(Q_1, p) &= \frac{2}{3}\sum_{d|p}\left(\frac{d}{23}\right) - \frac{2}{3}t(p) \\ &= \frac{2}{3} - \frac{2}{3}t(p). \end{aligned} \tag{4.10}$$

Subtracting (4.9) and (4.10), we have that $r(Q_0, p) - r(Q_1, p) = 2t(p)$. As seen in (4.3), $a_p = \frac{1}{2}(r(Q_0, p) - r(Q_1, p))$. Thus, we can see that $t(p) = a_p$. □

Chapter 5

Applications and Conclusion

5.1 Ramanujan's Tau Function

Ramanujan's Tau Function appears in the Fourier expansion of the cusp form $\Delta(z)$ seen in Example 2.44.

Recall that for all $z \in \mathbb{H}$, $\Delta(z) = q\prod_{n=1}^{\infty}(1-q)^{24}$, and $\Delta(z)$ is a cusp form of weight 12 on $SL_2(\mathbb{Z})$. Ramanujan's tau function $\tau(n)$ is defined by

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n,$$

where $q = e^{2\pi i z}$.

It is easy to see given the definition of $\Delta(z)$ that $\tau(n)$ is integral for all n. There are also congruences known about $\tau(n)$. For example, it is known that

$$\tau(n) \equiv \begin{cases} 1 \pmod 2 & \text{if } n \text{ is an odd square,} \\ 0 \pmod 2 & \text{otherwise,} \end{cases}$$

and interestingly,

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \text{ for all } n \geq 1$$

where $\sigma_{11}(n) = \sum_{d|n} d^{11}$ (see [4], p. 24).

Next we will see that there is a relationship between the a_p from (4.2) and $\tau(p)$. To see this, note that for each n,

$$(1-q^n)^{24} = 1 - \binom{n}{1} q^n + \binom{n}{2} q^{2n} - \cdots - 24q^{23n} + q^{24n}.$$

Then, $(1-q^n)^{24} \equiv 1 - q^n - q^{23n} + q^{24n} \pmod{23}$. Then we have

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) \equiv q\prod_{n=1}^{\infty}(1-q^n)^{24} \pmod{23}.$$

Since a_p is the coefficient of q^p in $q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})$, we have that

$$\tau(p) \equiv a_p \pmod{23}.$$

Thus, the modular form $\eta(z)\eta(23z)$ reveals something about Ramanujan's tau function.

5.2 Modular forms and questions of number theory

We have already seen a connection between the modular form $\eta(z)\eta(23z)$ and the quadratic field $\mathbb{Q}(\sqrt{-23})$. However, we can learn even more about the prime ideals of $\mathbb{Q}(\sqrt{-23})$ by considering the the coefficients a_p of q^p in $\eta(z)\eta(23z) = \sum_{n=1}^{\infty} a_n q^n$. In particular, we will see that the number a_p will indicate whether or not the ideal (p) splits into principal or nonprincipal prime ideals.

We are now prepared to prove our second main theorem, Theorem 1.2.

Proof. Recall that using the isomorphism from Theorem 2.32, Q_0 gets mapped to the ideal class that consists of the principal ideals of O_{-23}. Let $\mathcal{A}_i$ be the ideal class that corresponds to the quadratic form Q_i for each i.

Recall from Section 2.2 that if the norm of an ideal, A, is a prime number, p, then $A|(p)$ as ideals. Recall also from Section 2.2 that for prime p,

$$(p) = \begin{cases} P & \text{if } \left(\frac{-23}{p}\right) = -1, \\ PP' & \text{if } \left(\frac{-23}{p}\right) = 1, \text{ where } P \neq P', \\ P^2 & \text{if } \left(\frac{-23}{p}\right) = 0, \end{cases}$$

where each ideal on the right-hand side is prime, and

$$a_p = r(\mathcal{A}_0, p) - r(\mathcal{A}_1, p).$$

Then if $a_p = 1$, then $p = 23$ and $r(\mathcal{A}_0, p) = 1$, so we know that (23) splits into the square of a principal prime ideal. If $a_p = 0$, then $\left(\frac{p}{23}\right) = -1$ and we know that (p) does not split. If $a_p = 2$, then $\left(\frac{p}{23}\right) = 1$ and $r(\mathcal{A}_0, p) = 2$, so (p) splits into the product of two distinct principal prime ideals. Finally, if $a_p = -1$, then $\left(\frac{p}{23}\right) = 1$ and $r(\mathcal{A}_0, p) = 0$, so (p) splits into the product of two distinct nonprincipal prime ideals. □

5.3 Conclusion

Now we have experienced the full collision of binary quadratic forms, quadratic fields, and modular forms. In Chapter 2, we saw the basics of these three areas and the isomorphism from $C(d)$ to H_d that connected binary quadratic forms and quadratic fields. Theta series were introduced in Chapter 3 which provided a connection between binary quadratic forms and modular forms. In Chapters 4 and 5, we saw these connections all unfold through the specific case $d = -23$. In particular, we saw how the representatives of $C(-23)$ as given in (4.1) gave us enough information to determine the Fourier coefficients of q^p, for odd prime p, of the modular form $\eta(z)\eta(23z)$. We then concluded by using these Fourier coefficients to determine information about the ideals of the ring of integers O_{-23}.

Bibliography

[1] A.N. Andrianov and V.G. Zhuravlev. *Modular forms and Hecke operators*. Amer Mathematical Society, 1995.

[2] T.M. Apostol. *Introduction to analytic number theory*. Springer, 1986.

[3] S. Arno, M.L. Robinson, and F. Wheeler. Imaginary quadratic fields with small odd class number. *Acta Arithmetica*, 83:295–330, 1998.

[4] J.H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of modular forms*. Springer, 2008.

[5] D.A. Cox. *Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication*. Wiley, 1989.

[6] F. Diamond and J.M. Shurman. *A first course in modular forms*. Springer Verlag, 2005.

[7] W. Dunham. *The genius of Euler: reflections on his life and work*. The Mathematical Association of America, 2007.

[8] K.F. Ireland and M.I. Rosen. *A classical introduction to modern number theory*. Springer, 1990.

[9] Matthew Johnson. Hecke Eigenforms as Products of Eigenforms, 2008. http://math.arizona.edu/∼johnsoma/Master's%20Thesis.pdf.

[10] Franz Lemmermeyer. Class Field Theory, 2007. http://www.fen.bilkent.edu.tr/∼franz/cft/cfb.pdf.

[11] S.J. Leon. *Linear algebra with applications*. Prentice Hall Upper Saddle River, NJ, 2006.

[12] D.A. Marcus. *Number fields*. Springer, 1977.

[13] H.P. McKean and V. Moll. *Elliptic curves: function theory, geometry, arithmetic*. Cambridge Univ Pr, 1999.

[14] K. Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*. National Science Foundation, 2004.

[15] A.A. Panchishkin. *Introduction to modern number theory: fundamental problems, ideas and theories*. Springer Verlag, 2005.

[16] I. Stewart and D.O. Tall. *Algebraic number theory and Fermat's last theorem.* AK Peters Ltd, 2002.

[17] A. Straub. Hermite Normal Form Introduction and Basic Application, 2007. http://arminstraub.com/files/hermitenormalform.pdf.

[18] F. van der Blij. Binary quadratic forms of discriminant -23. *Indagationes Mathematicae*, 1952.

[19] T. Weston. Lectures on the Dirichlet Class Number Formula for Imaginary Quadratic Fields. http://www.math.umass.edu/∼weston/oldpapers/cnf.pdf.

[20] D.B. Zagier. *Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie.* Springer, 1981.