On congruences for the coefficients of modular forms and some applications

by

Kevin Lee James

B.S. The University of Georgia, 1991

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

ATHENS, GEORGIA
1997

Kevin Lee James On con gruences for the coefficients of modular forms and some applications

(Under the direction of Andrew Granville)

In this dissertation, we will study two different conjectures about elliptic curves and modular forms. First, we will exploit the theory developed by Shimura and Waldspurger to address Goldfeld's conjecture which states that the density of rank zero curves in a family of quadratic twists of an elliptic curve should be 1/2. In particular, we will find lower bounds for the density of rank zero curves in several families of quadratic twists. Next, we will use a beautiful theorem of Frey to verify that the 3-part of the Birch and Swinnerton-Dyer conjecture holds for four different families of elliptic curves. More precisely, we will verify for four different elliptic curves E and for all D in some subset S_E of the square-free natural numbers having positive lower density that

$$\operatorname{ord}_3\left(\frac{L(E_D,1)}{\Omega_{E_D}}\right)=0 \quad \text{if and only if} \quad \operatorname{ord}_3\left(\frac{\#Ш\prod_p c_p(E_D)}{\#E(\mathbb{Q})^2_{\text{tor}}}\right)=0.$$

INDEX WORDS: Elliptic Curves, L-series, Modular Forms, Shimura Lift, Ternary Quadratic Forms, Waldspurger.

Table of Contents

Chapter

1. Introduction 1

2. Elliptic Curves 11

2.1 Elliptic Curves 11

2.2 The Group Law 11

2.3 Complex Multiplication of Elliptic Curves 12

2.4 Weierstrass Equations 12

2.5 Reduction of Elliptic Curves 13

2.6 L-series 14

2.7 Twisting 16

3. Modular Forms 17

3.1 Modular Forms of Integral Weight 17

3.2 Hecke Operators and the Petersson Inner Product 18

3.3 Oldforms and Newforms 19

3.4 L-series for Modular Forms 19

3.5 Modular Elliptic Curves 21

3.6 Modular Froms of Half-Integral Weight 21

3.7 The Theory of Shimura and Waldspurger 22

3.8 Computation 26

4. Ternary Quadratic Forms 31
4.1 Constructing Cusp Forms from Ternary Quadratic Forms 31
4.2 Representations by a Genus of Ternary Quadratic Forms 34
5. Prime Twists 39
5.1 Statement of Results 39
5.2 Proof of Results 39
6. Positive Density Nonvanishing Results 43
6.1 A Positive Density Nonvanishing Result 43
6.2 More Positive Density Nonvanishing Results 51
7. Birch and Swinnerton-Dyer Type Results 58
7.1 A Theorem of Frey 60
7.2 Results 61
References 69

Chapter 1

Introduction

We start with a brief overview of the necessary theory: Given any cusp form $f = \sum_{n\geq 1} a_n(f)q^n$ of weight k, we denote by $L(f,s)$ the L-function of f. For $\mathrm{Re}(s) > k/2+1$, the value of $L(f,s)$ is given by $L(f,s) = \sum_{n\geq 1} \frac{a_n(f)}{n^s}$ and, one can show that $L(f,s)$ has analytic continuation to the entire complex plane. The value of $L(f,s)$ at $s = k/2$ will be of particular interest to us, and we will refer to this value as the *central critical value* of $L(f,s)$.

Let χ_D denote the Dirichlet character associated to the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, that is $\chi_D(n) = \left(\frac{\Delta_D}{n}\right)$, where Δ_D denotes the discriminant of $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, and $\left(\frac{\Delta_D}{n}\right)$ is the Kronecker-Legendre symbol. Define the D^{th} *quadratic twist of* f to be $f_{\chi_D} = \sum_{n\geq 1} a_n(f)\chi_D(n)q^n$. For any integer D, the L-function of f_{χ_D} is the *twist* of $L(f,s)$ by χ_D, that is $L(f_{\chi_D},s)$ is the analytic continuation of $\sum_{n\geq 1} \frac{a_n(f)\chi_D(n)}{n^s}$ to the whole complex plane. We will be interested in determining how often $L(f_{\chi_D},s)$ has nonzero central critical value as D varies. Since $\chi_{Dm^2} = \chi_D$, we will restrict our attention to the square-free integers D. We expect that as we let D vary over all of the square-free integers, a positive proportion of the L-functions $L(f_{\chi_D},s)$ will have nonzero central critical value. In fact it has been conjectured by Goldfeld in [19] that for eigenforms f of weight 2, $L(f_{\chi_D},1) \neq 0$ for $\frac{1}{2}$ of the square-free integers.

Given an elliptic curve $E : y^2 = x^3 + Ax^2 + Bx + C$ with $A,B,C \in \mathbb{Z}$ of conductor N_E and an integer D, we define the D^{th} *quadratic twist of* E to be the curve $E_D : y^2 = x^3 + ADx^2 + BD^2x + CD^3$. Let $L(E_D,s)$ denote the L-function associated to E_D (see section 2). For square-free D coprime to $2N$, $L(E_D,s)$ is simply the D^{th} quadratic twist of $L(E_1,s)$.

Given a weight 2 newform f with integer coefficients, we can use the theory of Eichler and Shimura to find an elliptic curve E over $\mathbb{Q}$ so that $L(E,s) = L(f,s)$. Thus if D is coprime to $6N_E$, then $L(E_D,s) = L(f_{\chi_D},s)$. Also, one has the following theorem which was developed from deep ideas of Kolyvagin [28], by Murty, Murty [34] and by Bump, Friedberg and Hoffstein [7] (see also [22] for a shorter proof).

THEOREM 1.1. *Let E be a modular elliptic curve. If $L(E,1) \neq 0$, then the rank of E is 0.*

So, if f is a weight 2 newform having the property that a positive proportion of the twists of $L(f,s)$ have nonzero central critical value and if E is the elliptic curve associated to f through the theory of Eichler and Shimura, then this implies that a positive density of the quadratic twists E_D of E have rank 0.

There have been many papers which have proved results in this direction. For example, in [5, 7, 17, 22, 32, 34, 39, 53, 54] one can find general theorems on the vanishing and nonvanishing of the quadratic twists of a given L-function. These theorems ensure that an infinite number of the quadratic twists of an L-function associated to a cusp form will have nonzero central critical value. In [40], Ono has shown several examples of cusp forms f associated to elliptic curves such that for a positive density of the primes p, the p^{th} quadratic twist of $L(f,s)$ will have nonzero central critical value. Ono also proves a Theorem which gives sufficient conditions under which a cusp form associated to an elliptic curve will have this property.

Using methods similar to those of Ono, we prove the following theorem (see Chapter 5).

THEOREM 1.2. *The elliptic curve $E_p : y^2 = x^3 - 32p^3$ has rank 0 for at least $1/3$ of the primes p.*

An outline of the proof is as follows. Let $E : y^2 = x^3 + 4$. Since E has complex multiplication by $\sqrt{-3}$ it follows that it is modular. Let F denote the weight 2 newform with $L(F,s) = L(E,s)$. We are able to exhibit a weight $3/2$ eigenform

$f = \sum_{n\geq 1} a_n(f)q^n$ which lifts through the Shimura correspondence to F. Then using Waldspurger's theorem we see that $L(E_{-2D}, 1) = 0$ if and only if $a_D(f) = 0$, for any square-free D coprime to 6. Thus it follows from Theorem 1.1 that if $a_D \neq 0$ then E_D has rank 0. Next, using a theorem of Sturm we prove that $a_n(F) \equiv a_n(f)$ modulo 2. Thus, we have that if $a_D(F)$ is odd then $a_D(f) \neq 0$ and therefore E_{-2D} has rank 0. Now, we recall that for odd primes p, $a_p(F) \equiv \#E(\mathbb{F}_p)$ modulo 2. So for any odd prime p such that $E(\mathbb{F}_p)$ contains no points of order 2, we will have that E_{-2p} has rank 0. Note that $E(\mathbb{F}_p)$ contains order 2 points precisely when $x^3 + 4$ has a root modulo 2. Now, we can use the Chebotarev density theorem to see that $x^3 + 4$ has no root modulo 2 for $1/3$ of the primes p, and the theorem follows.

Subsequently, Ono and Skinner [43] used the theory of Galois representations to extend Ono's theorem to all even weight eigenforms. Using the theorems of Waldspurger, they argue that if F is a weight $2k$ newform then there exists an integer N and an eigenform $g(z) = \sum_{n\geq 1} a_n(g)q^n \in S_{k+\frac{1}{2}}(N)$ such that for each square-free natural number D,

$$a_D(g)^2 = \begin{cases} \pm L(F_{\chi_{(-1)^k D}}, k)D^{k-\frac{1}{2}}, & \text{if } D \text{ is relatively prime to } 4N \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Then using the theory of Galois representations and the Chebotarev density theorem, they prove the following theorem.

THEOREM 1.4. *Suppose $E/\mathbb{Q}$ is a modular elliptic curve, and F is the weight 2 newform for which $L(E, s) = L(F, s)$. Let $g \in S_{3/2}(N)$ be an eigenform with integer coefficients satisfying (1). Define s_0 by*

$$s_0 = min\{s : a_D(g) \not\equiv 0 \pmod{2^{s+1}} \text{ for any square-free } D > 1 \text{ coprime to } 4N\}.$$

If there exists a single prime p_1 not dividing $4N$ for which $a_{p_1}(g) \not\equiv 0$ modulo 2^{s_0+1}, then the rank of E_{-p} is 0 for a positive proportion of the primes p.

Ono and Skinner verify the hypotheses of this theorem for all modular elliptic curves of conductor ≤ 100.

In a series of two papers [20, 21], Heath-Brown has done an extensive investigation of the behavior of the 2-Selmer groups associated to the quadratic twists of the congruent number curve: $y^2 = x^3 - x$. He states as a corollary to one of his theorems that at least 5/16 of these quadratic twists have rank 0. This implies via the Birch and Swinnerton-Dyer conjecture that at least 5/16 of the quadratic twists of the L-function $L(E, s)$ associated to the congruent number curve should have nonzero central critical value. It is well known that the congruent number curve is modular, thus there is a weight 2 modular form f such that $L(f, s) = L(E, s)$.

In [54], Gang Yu has used similar techniques to those developed in [20, 21] to study the twists of all elliptic curves whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Assuming the parity conjecture for elliptic curves, he shows that any elliptic curve with torsion subgroup as above has the property that a positive density of its quadratic twists have rank zero.

Using some ideas developed by Frey in [16] and a theorem of Davenport and Heilbronn [12] as improved by Nakagawa and Horie [35], Wong [53] was able to show the existence of an infinite family of non-isomorphic elliptic curves such that a positive proportion of the quadratic twists of each curve has rank 0. Thus, the Birch and Swinnerton-Dyer and Shimura-Taniyama conjectures plus the result of Wong imply the existence of an infinite family of weight 2 cusp forms $\{f_i\}$ such that a positive proportion of the twists of each $L(f_i, s)$ have nonzero central critical value.

In Chapter 6, we exhibit weight 2 newforms F such that $L(F_{\chi_D}, 1) \neq 0$ for a positive density of the square-free natural numbers D. We will now describe the first of those results.

Let E denote the elliptic curve with equation $y^2 = x^3 - x^2 + 72x + 368$. Then E is a modular curve (it is the -1 twist of $X_0(14)$). We let F denote the weight 2 cusp form whose Mellin transform is $L(E, s)$. We then prove unconditionally:

THEOREM 1.5. *For F as above we have that for at least 7/64 of the square-free*

natural numbers D,

$$L(F_{\chi_D}, 1) \neq 0.$$

In light of Theorem 1.1, we have as a corollary to Theorem 1.5

COROLLARY 1.6. *For at least* $7/64$ *of the square-free natural numbers* D, E_D : $y^2 = x^3 - Dx^2 + 72D^2x - 368D^3$ *has rank 0.*

Our proof differs from those of Heath-Brown and Wong in that while they work directly with the Selmer groups of elliptic curves, our proof uses the theory of modular forms developed by Waldspurger and Shimura to gain information about the central critical values of the L-functions associated to elliptic curves. An outline of the proof of Theorem 1.5 is as follows. Using ideas of Schoeneberg [44] and Siegel [46], we construct a weight $3/2$ cusp form f as the difference of the theta functions associated to two inequivalent ternary quadratic forms Q_1 and Q_2 which together make up a genus of ternary forms. This f will be an eigenform for all of the Hecke operators and will lift through the Shimura correspondence to $F_{\chi_{-1}}$. By a theorem of Waldspurger [51] we will be able to equate the vanishing of the central critical values of the quadratic twists of $L(F, s)$ to the vanishing of certain Fourier coefficients of f. Since our ternary forms Q_1 and Q_2 are the only forms in a certain genus of ternary forms, we are able to study the automorph structure of these forms to show that the Fourier coefficients of f are related modulo 3 to certain class numbers of imaginary quadratic number fields. We will then use the Davenport-Heilbronn Theorem (see [35]) to show that at least $7/64$ of these class numbers are not divisible by 3, and hence, the associated Fourier coefficients of f are nonzero. It will then follow that at least $7/64$ of the quadratic twists of $L(F, s)$ have nonzero central critical value.

We will also show in Chapter 6:

THEOREM 1.7. *Suppose that k is a positive integer. Then there exists a cusp form $\Phi \in S_{2k}(126 \cdot C)$ with the property that $L(\Phi_{\chi_n}, k) \neq 0$ for at least $7/64$ of the square-free natural numbers n where C is 1 (resp. 9) when k is even (resp. odd).*

An outline of the proof is as follows. Let S denote the set of square-free natural numbers n so that $3 \nmid a_n(f)$. Then it follows from the outline of the proof of Theorem 1.5 given above that the lower density of S is at least $7/64$. Given any positive integer k, we multiply our weight $3/2$ cusp form f by a weight k modular form with integer coefficients which is congruent to 1 modulo 3, thus obtaining a weight $(2k+3)/2$ cusp form ϕ_k, whose Fourier coefficients, having indices in S, are not divisible by 3 and hence are nonzero. We then write this form as a finite linear combination of forms f_i which are eigenforms for all but finitely many of the Hecke operators. Next, we lift each of the forms f_i through the Shimura correspondence [45] to a weight $2k+2$ form F_i. It is not hard to see from the definition of the Shimura Lift and from the definitions of the Hecke operators that each F_i is also eigenform for all but finitely many of the Hecke operators having the same eigenvalues as f_i. Thus by the theory of newforms developed in [1, 31] we know that there exist newforms G_i of weight $2k+2$ such that for each i, G_i and f_i are eigenforms having the same eigenvalues for all but finitely many of the Hecke operators. Next, we are able to use Waldspurger's theorem to see that since for all $n \in S$, $a_n(\phi_k) \neq 0$, it follows that for such n, $L((G_i)_{\chi_n}, 1) \neq 0$ for at least one of the G_i's. Thus there is some linear combination Φ of the G_i's having the property that $L(\Phi_{\chi_n}, 1) \neq 0$ for all $n \in S$.

Next we summarize the techniques used to prove Theorem 1.5 into the following proposition.

PROPOSITION 1.8. *Suppose that Q_1 and Q_2 are even integral primitive positive definite ternary quadratic forms and that Q_1 and Q_2 are the only forms in a genus*

of forms. Let A_i denote the number of automorphs of Q_i $(i = 1, 2)$. Assume that $3 \nmid A_1A_2$ but $3 \mid A_1 + A_2$. Suppose also that $f = (\theta_{Q_1} - \theta_{Q_2}) \in S_{3/2}(N, \chi_q)$ is a Hecke-eigenform which lifts through the Shimura correspondence to a cusp form $F \in S_2(N/2)$. Then F is also a Hecke-eigenform, and hence there is a unique weight 2 newform G of trivial character having $\lambda_p(F) = \lambda_p(G)$ for all but finitely many of the primes p. Letting N_G denote the level of G, we put

$$W = \text{lcm}[\prod_{\substack{p,\ \text{odd} \\ p|N_G}} p, \prod_{\substack{p,\ \text{odd} \\ p|d_{Q_1}}} p],$$

$$R = \left\{ a \in (\mathbb{Z}/8W\mathbb{Z})^* : \exists \quad \begin{array}{c} \text{a square-free } n \equiv a \\ (\text{mod } 8W) \text{ with } 3 \nmid a_n(f) \end{array} \right\} \qquad \text{and,} \tag{6.19}$$

$$\delta = \frac{\#R}{12W \prod_{p|W}(1 - \frac{1}{p^2})}.$$

Then, the set of square-free natural numbers n such that $L(G \cdot \chi_{-qn}, 1) \neq 0$ has lower density at least δ in the square-free natural numbers.

Using Proposition 1.8, we prove results similar to Theorem 1.5 for nine other families of curves. We summarize these results in the table below. For each curve E, we list a Weierstrass equation for E, the conductor N_E of E, and the lower bound δ_E on the lower density of square-free natural numbers d such that $L(E_{-d}, 1) \neq 0$.

E	N_E	δ_E
$y^2 = x^3 + 8$	576	1/4
$y^2 = x^3 + 1$	36	5/24
$y^2 = x^3 + 4x^2 - 144x - 944$	19	19/240
$y^2 = x^3 + x^2 + 4x + 4$	20	5/72
$y^2 = x^3 + x^2 - 72x - 496$	26	13/112
$y^2 = x^3 + x^2 + 24x + 144$	30	5/128
$y^2 = x^3 + x^2 - 48x + 64$	34	17/144
$y^2 = x^3 + x^2 + 3x - 1$	44	11/144
$y^2 = x^3 + 5x^2 - 200x - 14000$	50	5/24

In chapter 7, we turn our attention to the Birch and Swinnerton-Dyer conjecture. As a special case of the Birch and Swinnerton-Dyer conjecture, we have the following:

CONJECTURE 1.9. *If E is an elliptic curve of rank 0 then*

$$\frac{L(E,1)}{\Omega_E} = \frac{\#Ш(E/\mathbb{Q}) \prod_p c_p(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\text{tor}}}. \tag{2}$$

In [36], Nekovář studies the 3-part of the Birch and Swinnerton-Dyer conjecture for the curves $E_D : y^2 = 4x^3 - 27D^3$ for all square-free D with $|D| \equiv 1$ modulo 3 excluding $0 > D \equiv 5$ modulo 8 and $1 < D \equiv 1$ modulo 8. In particular, he proved that for E and D as above:

$$\frac{L(E_D,1)}{\Omega_{E_D} \prod_{p,\text{ prime}} c_p(E_D/\mathbb{Q})} \not\equiv 0 \pmod 3 \quad \text{if and only if} \quad S(E_D/\mathbb{Q})_3 = 0, \tag{3}$$

where $S(E_D/\mathbb{Q})_3$ denotes the subgroup of points of order 3 of the Selmer group of E_D. We note that in the case that E_D has rank 0 and no 3-torsion, one has $S(E_D/\mathbb{Q})_3 = Ш(E_D/\mathbb{Q})_3$.

Nekovář explicitly calculated the Selmer ranks of these curves in terms of the 3-rank of certain class groups of imaginary quadratic fields. He then used Waldspurger's Theorem to calculate the central critical values of the L-functions of these curves in terms of the Fourier coefficients of certain weight 3/2 forms. Next, he obtained congruences modulo 3 between these Fourier coefficients and class numbers of the imaginary quadratic fields mentioned above. These congruences unfortunately fail to hold for $0 > D \equiv 5$ modulo 8 and $1 < D \equiv 1$ modulo 8. In [41], Ono is able to prove the correct congruences for these missing D's using a theorem of Sturm. Ono thus removes the condition that $D \not\equiv 1$ modulo 8 when $D > 1$ and the condition that $D \not\equiv 5$ modulo 8 when D is negative.

In chapter 7, we partially verify the 3-part of the Birch and Swinnerton-Dyer conjecture for four different families of curves. We use a general theorem of Frey which relates the 3-part of Selmer groups of elliptic curves to the 3-part of certain class groups of imaginary quadratic fields. Using Frey's Theorem along with our work in chapter 6, we are able to prove:

PROPOSITION 1.10. *Suppose that $f \in S_{3/2}(N)$ and $G \in S_2(M)$ are as in Proposition 1.8. Let $E/\mathbb{Q}$ be the elliptic curve with $L(E,s) = L(G,s)$. Suppose that E has a rational point P of order 3. Assume that either E is given by $y^2 = x^3 + 1$ or that P is not in the kernel of the reduction modulo 3 map. Further, suppose that for all odd primes $q \mid N_E$ with $q \equiv 2$ modulo 3, we have that $3 \mid \mathrm{ord}_3(\Delta_E)$. Define*

$$W = \mathrm{lcm}\left[\prod_{\substack{p\mid M\\ p\neq 2,3}} p, \prod_{\substack{p\mid N\\ p\neq 2,3}} p\right]. \tag{1.11}$$

Let R be the set of all $a \in (\mathbb{Z}/24W\mathbb{Z})^*$ satisfying the following conditions:

1. *There exists a square-free natural number $n \equiv a$ modulo $24W$ such that $3 \nmid a_n(f)$ and such that $\mathrm{ord}_3\left(\frac{L(E_{-n})}{\Omega_{E_{-n}}}\right) = 0$.*
2. *For all square-free natural numbers $d \equiv a$ modulo $24W$, $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$*
3. *There exists an integer m depending only on a such that for all square-free natural numbers $d \equiv a$ modulo $24W$, $\Omega_{E_{-d}}\sqrt{d}/\Omega_{E_{-1}} = m$.*
4. *If $2 \mid N_E$ then $a \equiv 1$ modulo 4.*
5. *If $\ell \neq 2,3$ is prime and $\ell \mid N_E$, then*

$$\left(\frac{-a}{\ell}\right) = \begin{cases} -1, & \text{if } \mathrm{ord}_\ell(j_E) \geq 0 \\ -1, & \text{if } \mathrm{ord}_\ell(j_E) < 0 \text{ and } \gamma_\ell(E) = 1 \\ 1, & \text{otherwise.} \end{cases} \tag{1.12}$$

6. *If $\mathrm{ord}_3(j_E) < 0$ then $a \equiv 1$ modulo 3.*

Put

$$\delta = \frac{\#R}{32W\prod_{p\mid W}(1-\frac{1}{p^2})} \tag{1.13}$$

Then there exists a subset S of the square-free natural numbers having lower density at least δ such that for all $d \in S$ we have

$$\mathrm{ord}_3\left(\frac{L(E_d,1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q})\prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \tag{1.14}$$

We then use Proposition 1.10 to prove for the four elliptic curves E in the table below of conductor N_E that there exists a subset S_E of the square-free natural numbers having lower density at least δ_E such that for all $d \in S$ (1.14) holds.

E	N_E	δ_E
$y^2 = x^3 + 1$	36	1/8
$y^2 = x^3 + x^2 + 72x - 368$	14	7/128
$y^2 = x^3 + 4x^2 - 144x - 944$	19	19/640
$y^2 = x^3 + x^2 - 72x - 496$	26	13/224

The remainder of the dissertation is organized as follows. Chapters 2,3 and 4 give a brief explanation of the background material that we will need: In chapter 2, we will review the basic theory of elliptic curves. In chapter 3, we will review the basic theory of modular forms and explain the theory of Shimura and Waldspurger. In chapter 4, we will explain our construction of modular forms of weight 3/2 from ternary quadratic forms. In chapter 5, we will obtain nonvanishing results for the L-functions of the prime quadratic twists of a particular elliptic curve. In particular we will prove Theorem 1.2. In chapter 6, we will obtain nonvanishing results for the L-functions of a positive density of the quadratic twists of ten different curves. In chapter 7, we will partially verify the 3-part of the Birch and Swinnerton-Dyer conjecture for four different families of elliptic curves.

Chapter 2

Elliptic Curves

In this chapter, we will review the basic terminology and facts about elliptic curves which we will need in the remainder of this thesis. However, we will not attempt to give a complete treatment of the theory of elliptic curves. For a more detailed account of this theory, the reader is referred to [27, 47].

2.1 Elliptic Curves.

An *elliptic curve* over a number field k is the set of all solutions in $\mathbb{C}^2$ of a non-singular cubic polynomial in $k[x, y]$ (ie. a cubic polynomial $f(x, y)$ in two variables with coefficients in k such that for every pair $(a, b) \in \mathbb{C}^2$ satisfying $f(a, b) = 0$, we have either $\frac{\partial f}{\partial x}|_{(a,b)} \neq 0$ or $\frac{\partial f}{\partial y}|_{(a,b)} \neq 0$) plus one point at infinity. We denote the set of points on E with coordinates in k^2 by $E(k)$. Two elliptic curves E and E' over k are said to be biratinally equivalent over k if we can obtain the equation of E' from the equation of E via a k-linear change of variables. Thus we may think of an elliptic curve as being expressed by many different equations.

2.2 The Group Law.

Given an elliptic curve E defined over k, we can define a group law on $E(k)$ as follows. We take the point at infinity to be the identity element denoted O. For points P and Q of $E(k)$, let L denote the line passing through P and Q and denote by $P * Q$ the third point of intersection of L with E. Then define $P + Q$ to be the reflection of $P * Q$ through the x-axis. One can prove that the operation $+$ makes $E(k)$ into an abelian group. Also, it can be shown that the $x-$ and $y-$coordinates

of $(P+Q)$ can be expressed as rational functions defined over k in the $x-$ and $y-$ coordinates of P and Q. Thus, if two elliptic curves are birationally equivalent, then it follows that their group structures are isomorphic.

By the Mordell-Weil theorem we know that $E(k)$ is finitely generated. Thus, $E(k) \cong E(k)_{\text{tor}} \oplus \mathbb{Z}^r$, where $E(k)_{\text{tor}}$ denotes the subgroup of $E(k)$ consisting of all elements in $E(k)$ which have finite order. The number r is referred to as the *rank* of E. In what follows we will be interested in elliptic curves defined over $\mathbb{Q}$. The torsion subgroups of these curves are very well understood. Therefore, we will restrict our attention to the ranks of these curves.

2.3 Complex Multiplication of Elliptic Curves.

Given an elliptic curve E defined over $\mathbb{Q}$, an endomorphism of E is a birational map $\phi : E \to E$ which is a group homomorphism on $E(\mathbb{Q})$. We will denote the ring of endomorphisms of a curve E by $End(E)$. For any curve the *multiplication by n* maps $[n] : E \to E$ given by

$$[n](P) = \underbrace{P + P + \cdots + P}_{n \text{ times}} \tag{2.1}$$

are endomorphisms. In fact, for almost all elliptic curves over $\mathbb{Q}$ the multiplication by n maps are the only endomorphisms. If $End(E)$ contains any nontrivial maps which are not given by multiplication by n for some n, then we say that E has *complex multiplication*.

For example if $E : y^2 = x^3 - x$, then the map $\phi : E \to E$ given by $\phi((x,y)) = (-x, iy)$ is an endomorphism of E and it is not the same as multiplication by n for any integer n. In this case, E is said to have complex multiplication by $\mathbb{Z}[i]$.

2.4 Weierstrass Equations.

One can show that any elliptic curve over $\mathbb{Q}$ is birationally equivalent to one given by an equation in so called *Weierstrauss* form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.2}$$

where the a_i's are in $\mathbb{Z}$.

Given a Weierstrass equation as in (2.2), we define the following quantities:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{and} \\
j_E &= \frac{c_4^3}{\Delta}.
\end{aligned} \tag{2.3}$$

If E is an elliptic curve given by a Weierstrass equation as above and p is a prime, then we say that this equation for E is *minimal at* p if $\mathrm{ord}_p(\Delta)$ is minimal over all possible Weierstrass equations for E. It is a theorem of Tate [49] that for any elliptic curve E defined over $\mathbb{Q}$ there exists a *minimal Weierstrass equation* for E which is simultaneously minimal at all primes. We define the *minimal discriminant* Δ_E of E to be the discriminant of the minimal Weierstrass equation for E.

2.5 Reduction of Elliptic Curves.

Given an elliptic curve E over $\mathbb{Q}$ with minimal Weierstrass equation as in (2.2), we can consider the reduction $\tilde{E}$ of E modulo a prime p. That is we can consider the the set of all solutions in $\bar{\mathbb{F}}_p^2$ to the equation

$$y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6, \tag{2.4}$$

where $\tilde{a}_i$ denotes the reduction of a_i modulo p. We denote this set of solutions along with the point at infinity by $\tilde{E}$, and we denote the set of all solutions to (2.4) with coordinates in $\mathbb{F}_p^2$ as $E(\mathbb{F}_p)$.

Note that equation (2.4) gives a nonsingular curve if and only if $p \nmid \Delta_E$ and, in this case, we say that E has *good reduction* at p. If $p \mid \Delta_E$, then we say that E has *bad reduction* at p. There are two types of bad reduction. If $\tilde{E}$ has only double point, then we say that E has *multiplicative reduction*, but if $\tilde{E}$ has a cusp then we say that E has *additive reduction*.

In any case, the set of nonsingular points $\tilde{E}_{\text{ns}}$ of $\tilde{E}$ can be made into a group with an addition law analogous to the one discussed in section 2.2. In the case of bad reduction, one can prove that

$$E_{\text{ns}}(\mathbb{F}_p) \cong \begin{cases} \mathbb{F}_p^* & \text{if } E \text{ has multiplicative reduction} \\ \mathbb{F}_p^+ & \text{if } E \text{ has additive reduction.} \end{cases} \tag{2.5}$$

We define the *conductor* N_E of an elliptic curve E to be the integer,

$$N_E = \prod_{p|\Delta_E} p^{f_p}, \tag{2.6}$$

where if $p \geq 5$, f_p is given by,

$$f_p = \begin{cases} 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p. \end{cases} \tag{2.7}$$

In any case (including $p = 2$ and 3), f_p can be calculated using the following formula due to Ogg:

$$f_p = ord_p(\Delta_E) + 1 - \mathcal{M}_p, \tag{2.8}$$

where $\mathcal{M}_p$ denotes the number of irreducible components on the special fiber of the Néron minimal model of E at p. The quantity $\mathcal{M}_p$ can be easily computed using Tate's Algorithm [49]

2.6 *L*-series.

If we are given an elliptic curve E defined over $\mathbb{Q}$ with minimal discriminant Δ_E, then putting $a_p = p + 1 - \#E(\mathbb{F}_p)$, we can define the *L-series of* E by

$$L(E, s) = \prod_{p|\Delta_E} \frac{1}{1 - a_p p^{-s}} \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \quad (s \in \mathbb{C}) \tag{2.9}$$

Using Hasse's theorem which says that $|a_p| < 2\sqrt{p}$, one can show that the product in (2.9) converges and is holomorphic for $Re(s) > 3/2$. Also, we have the following conjecture:

CONJECTURE 2.6.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $L(E,s)$ be its associated L-series. Then*

1. *$L(E,s)$ has analytic continuation to the entire complex plane.*
2. *$L(E,s)$ satisfies a functional equation relating the functions $L(E,s)$ and $L(E,2-s)$.*

This conjecture is easily shown to be true for all *modular* elliptic curves (see chapter 3 for the definition of *modular*) and, we will always assume that we are working with *modular* curves. In fact, by the recent work of Wiles and Taylor [50, 52] we now know that large families of elliptic curves are indeed modular.

Our motivation for studying the L-series $L(E,s)$ of the curve E is the following conjecture of Birch and Swinnerton-Dyer [2, 3]:

CONJECTURE 2.6.2. *Suppose that E is an elliptic curve defined over $\mathbb{Q}$ with associated L-series $L(E,s)$. Then*

1. *The order of vanishing of $L(E,S)$ at $s=1$ is equal to the rank of E.*
2. *Let r denote the rank of E. Then*

$$\frac{\lim_{s\to 1}\left[\frac{L(E,s)}{(s-1)^r}\right]}{\Omega_E} = \frac{\#Ш(E/\mathbb{Q})2^r R(E/\mathbb{Q})\prod_p c_p}{\#E(\mathbb{Q})^2_{\text{tor}}}, \tag{2.10}$$

where Ω_E denotes the real period of E, $Ш(E/\mathbb{Q})$ denotes the Tate-Shafarevic group of E, $R(E/\mathbb{Q})$ denotes the elliptic regulator of E and the c_p's are the local Tamagawa factors for E (see [47] *for the definitions of these).*

In fact, Coates and Wiles [8] proved that if E is an elliptic curve having complex multiplication and if $L(E,1)\neq 0$ then E has rank 0. Later Kolyvagin [28] showed that if E is a modular curve and if $L(E,1)\neq 0$ then E can be proved to have rank 0 provided that E satisfies one additional somewhat technical condition. (The condition is that there must exist a suitable imaginary quadratic extension $K/\mathbb{Q}$ with a Heegner point y_K of $E(K)$ having infinite order.) This condition can be simplified to the following hypothesis (see for instance [6]).

HYPOTHESIS 2.6.3. *For any modular elliptic curve E, there exists a square-free integer D such that $L(E_D, s)$ has a first order zero at $s = 1$ and such that $\chi_D(p) = 1$ for all primes $p \mid N_E$, where N_E denotes the conductor of E.*

Two completely different proofs that Hypothesis 2.6.3 holds for all modular elliptic curves were independently found by Bump, Friedberg and Hoffstein [5, 7] and by Murty and Murty [34] (see also [22] for a shorter proof). Thus we have the following extension of Coates and Wiles' theorem.

THEOREM 2.6.4. *If E is a modular elliptic curve over $\mathbb{Q}$ such that $L(E, 1) \neq 0$ then the E has rank zero and $Ш(E/\mathbb{Q})$ is finite.*

2.7 Twisting.

For any elliptic curve $E : y^2 = x^3 + Ax + B$ defined over $\mathbb{Q}$ and any integer D, we define the D^{th} *quadratic twist* E_D of E to be the curve given by

$$E_D : Dy^2 = x^3 + Ax + B$$

which can be rewritten $E_D : y^2 = x^3 + AD^2x + BD^3$. We note that E_{Dm^2} is birationally equivalent to E_D over $\mathbb{Q}$ for all $m \in \mathbb{Z}$, so we may restrict our attention to quadratic twists by a square-free integer. As D varies over the square-free integers, we get an infinite family of quadratic twists of E. It was conjectured by Goldfeld [19] that the rank of E_D should be 0 for density one half of the square-free integers D and 1 for density one half of the square-free integers with curves of higher rank occurring too sparsely to account for a positive density of the square-free integers. In [29], there is substantial computational evidence supporting this conjecture.

Constructing the L-series associated to E_D as above, we see that for D coprime to $6N_E$ it is just the D^{th} *quadratic twist* of the L-series of E, that is

$$L(E_D, s) = \prod_{p \mid \Delta_E} \frac{1}{1 - a_p \chi_D(p) p^{-s}} \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p \chi_D(p) p^{-s} + p^{1-2s}}, \tag{2.11}$$

where $\chi_D(t)$ is the quadratic character associated to the quadratic extension $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, that is $\chi_D(t) = \left(\frac{\Delta}{t}\right)$, where Δ denotes the discriminant of $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Chapter 3

Modular Forms

In this section, we recall some basic definitions and theorems for modular forms of integral and half integral weight that we will need. For a more detailed account of the theory of modular forms, see [27] or [45].

3.1 Modular Forms of Integral Weight.

Let $\Gamma_0(N)$ denote the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $c \equiv 0 \pmod{N}$.

Definition 3.1.1. *Let k be an integer, N a natural number and let χ be a Dirichlet character modulo N. Denote by $\mathbb{H}$ the upper half complex plane $\{\tau \in \mathbb{C} : Re(\tau) > 0\}$. We define a modular form of weight k, level N and character χ to be a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following conditions:*

1. *$f(\frac{a\tau+b}{c\tau+d}) = \chi(d)(c\tau+d)^k f(\tau)$ for all $\tau \in \mathbb{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$*
2. *f is holomorphic at all of the cusps of $\mathbb{H}/\Gamma_0(N)$.*

The space of such functions is denoted $M_k(N, \chi)$ If, in addition, f vanishes at all of the cusps of $\mathbb{H}/\Gamma_0(N)$ then f is called a cusp form. The subspace of cusp forms is denoted $S_k(N, \chi)$.

Note that if the character χ in the above definition is the trivial character modulo N, then we will denote the space of modular forms and the subspace of cusp forms of level N, weight k and character χ simply by $M_k(N)$ and $S_k(N)$ respectively. If f is a modular form, then by condition 1 above, $f(\tau + 1) = f(\tau)$. So, f has a Fourier expansion of the form: $f(\tau) = \sum_{n \geq 0} a_n(f) q^n$, where $q = e^{2\pi i \tau}$. If f is a cusp form then $a_0(f) = 0$.

3.2 Hecke Operators and the Petersson Inner Product

Next, we define the *Hecke operators* T_p on a space of modular forms as follows.

DEFINITION 3.2.1. *Let $f \in M_k(N, \chi)$ be a modular form with Fourier expansion $f(\tau) = \sum_{n \geq 0} a_n(f) q^n$. Then for each prime p we put $(T_p f)(\tau) = \sum_{n \geq 0} b_n q^n$, where*

$$b_n = a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f) \tag{3.1}$$

with $a_{n/p}(f) = 0$ if $p \nmid n$.

It can be proven that, if $f \in M_k(N, \chi)$, then $T_p f \in M_k(N, \chi)$, and if f is a cusp form then so is $T_p f$.

If $f \in S_k(N, \chi)$, and if there is a complex number $\lambda_p(f)$ such that $T_p f = \lambda_p(f) f$, then we say that *f is an eigenform for T_p with eigenvalue $\lambda_p(f)$*. In fact, one can show that there exists a basis for $S_k(N, \chi)$ of forms which are eigenforms for all of the T_p with $p \nmid N$. The proof follows from the fact that the Hecke operators are self-adjoint with respect to the *Petersson inner product* which we define below. We will refer to any modular form which is an eigenform for all but finitely many of the Hecke operators as a *Hecke-eigenform*.

There is a hermitian inner product, the Petersson inner product, defined on the spaces of cusp forms as follows.

DEFINITION 3.2.2. *Let $f, g \in S_k(N, \chi)$ be two cusp forms and let R denote a fundamental domain for the action of $\Gamma_0(N)$ on $\mathbb{H}$. Then, we define the Petersson inner product of f and g by*

$$< f, g >= \int_R f(\tau) \bar{g(\tau)} \sigma^k \frac{d\rho d\sigma}{\sigma^2},$$

where $\tau = \rho + i\sigma$.

One can prove that this definition is independent of the choice of fundamental domain R.

3.3 Oldforms and Newforms

Given a particular cusp form, it is straight forward to construct other cusp forms of higher levels: Indeed, if $N = AB$ and if $f(\tau) \in S_k(A, \chi)$, then we also have $f(\tau) \in S_k(N, \chi)$ and $f(B\tau) \in S_k(N, \chi)$. Cusp forms in $S_k(N, \chi)$ formed in this way are called *old forms*, and the space spanned by these old forms is denoted $S_k^{\text{old}}(N, \chi)$. The orthogonal complement with respect to the Petersson inner product of $S_k^{\text{old}}(N, \chi)$ is denoted $S_k^{\text{new}}(N, \chi)$. It is important to note that the forms in $S_k^{\text{new}}(N, \chi)$ are referred as new forms (two words), while the term *newform* (one word) is reserved for more special members of this space (see the next paragraph).

If we restrict our attention to $S_k^{\text{new}}(N, \chi)$, then there is a basis of forms which are eigenforms for all of the Hecke operators and whose first nonzero coefficient is 1. We will refer to members of such a basis for $S_k^{\text{new}}(N, \chi)$ as the *newforms* of $S_k(N, \chi)$. By the work of Atkin and Lehner [1] and Li [31], we know that no two newforms have the same set of eigenvalues, and that if $f \in S_k(N, \chi)$ is a Hecke-eigenform then there is a unique newform $g \in S_k^{\text{new}}(M, \chi)$ for some $M \mid N$ such that for all primes $p \nmid N$, $\lambda_p(f) = \lambda_p(g)$, and f can be written

$$f(\tau) = \sum_{d \mid \frac{N}{M}} c_d g(d\tau) \tag{3.2}$$

where the $c_d \in \mathbb{C}$. This property of integral weight cusp forms is referred to as "Multiplicity One". (See [1],[26], [27], and [31] for a more detailed discussion of old and newforms.)

3.4 L-series for Modular Forms.

For any cusp form $f(\tau) = \sum_{n \geq 1} a_n(f) q^n \in S_k(N, \chi)$, we have an L-series given by the Mellin transform of f:

$$L(f, s) = \sum_{n \geq 1} \frac{a_n(f)}{n^s.} \tag{3.3}$$

One can prove that this sum converges for $Re(s) > k$ and that $L(f, s)$ has analytic continuation to the whole complex plane. Also, if χ is a real character, then one

can prove that any cusp form $f \in S_k(N,\chi)$ can be written as a sum of two forms $f_1, f_2 \in S_k(N,\chi)$ such that each $L(f_i,s)$ $(i=1,2)$ satisfies the following functional equation:

$$\left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(f_i,s) = (-1)^i \left(\frac{\sqrt{N}}{2\pi}\right)^{k-s} \Gamma(k-s)L(f_i,k-s). \tag{3.4}$$

It is of interest to determine the behavior of these L-functions in the *critical strip*, $0 \leq Re(s) \leq k$. In particular, we will be interested in determining the so called *central critical value* $L(f,k/2)$. It is this value which is conjectured to contain certain arithmetic information. For example, if we are given any weight 2 newform of trivial character, then by the theory of Eichler and Shimura, we can find an elliptic curve E such that $L(E,s) = L(f,s)$, and then the Birch and Swinnerton-Dyer conjecture implies that $L(f,1)$ determines the rank of E.

As for elliptic curves, there is a notion of twisting of modular forms defined as follows. If $f(\tau) = \sum a_n(f)q^n \in S_k(N,\chi)$ and ψ is a Dirichlet character modulo M, then $f_\psi(\tau) = \sum a_n(f)\psi(n)q^n \in S_k(NM^2,\chi\psi^2)$. This new cusp form f_ψ is called the *twist of* f *by* ψ.

The Mellin transform of f_ψ is the twist of $L(f,s)$ by ψ:

$$L(f_\psi,s) = L(f\otimes\psi,s) = \sum_{n\geq 1} \frac{a_n(f)\psi(n)}{n^s}. \tag{3.5}$$

We note that if $f(\tau) = \sum_{n\geq 1} a_n(f)q^n \in S_k(N,\chi)$ is an eigenform for all of the Hecke operators T_p with corresponding eigenvalue $\lambda_p(f)$, then its L-series has an Euler product expansion:

$$L(f,s) = a_1(f) \prod_{p \text{ prime}} \frac{1}{1-\lambda_p(f)p^{-s}+\chi(p)p^{k-1-2s}}. \tag{3.6}$$

Also, if f is as above, and if ψ is a Dirichlet character modulo M, then it follows from the definition of the Hecke operators that $f_\psi \in S_k(NM^2,\chi\psi^2)$ is also an eigenform for all of the Hecke operators T_p acting on $S_k(NM^2,\chi\psi^2)$ with corresponding

eigenvalues $\lambda_p(f_\psi) = \psi(p)\lambda_p(f)$. Thus,

$$L(f_\psi, s) = a_1(f) \prod_{p \text{ prime}} \frac{1}{1 - \lambda_p(f)\psi(p)p^{-s} + \chi(p)\psi^2(p)p^{k-1-2s}}. \tag{3.7}$$

As for elliptic curves, we will be interested in quadratic twists of cusp forms and their L-series, that is twists by quadratic characters. So, as in chapter 2 we will denote by χ_n the character associated to the quadratic extension $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

3.5 Modular Elliptic Curves.

As mentioned in the previous section, if we are given $f \in S_2^{\text{new}}(N, \chi)$, then we can find an elliptic curve E defined over $\mathbb{Q}$ of conductor N such that $L(E, s) = L(f, s)$. Any such elliptic curve coming from modular forms is called a *modular elliptic curve*. In fact it is conjectured that all elliptic curves over $\mathbb{Q}$ are modular, and the recent papers of Wiles [52], Taylor and Wiles [50] and Diamond [13] show that large families of elliptic curves are indeed modular.

3.6 Modular Forms of Half-Integral Weight.

We will also need to discuss modular forms of half-integral weight, which are defined as follows:

Definition 3.6.1. *Let k be an odd integer, N an integer which is divisible by 4 and let χ be a Dirichlet character modulo N. Then a modular form of weight $k/2$, level N, and character χ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following conditions:*

1. $f(\frac{a\tau+b}{c\tau+d}) = \begin{cases} \chi(d)\chi_c(d)\epsilon_d^{-k}(\sqrt{c\tau+d})^k f(\tau), & \text{if } c \neq 0 \\ \chi(d)f(\tau), & \text{otherwise} \end{cases}$

   for all $\tau \in \mathbb{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

   where $\epsilon_d = \begin{cases} 1, & \text{if } d \equiv 1 \pmod 4 \\ i, & \text{if } d \equiv 3 \pmod 4. \end{cases}$

2. *f is holomorphic at all of the cusps of $\mathbb{H}/\Gamma_0(N)$.*

As before, the space of such functions will be denoted $M_{k/2}(N,\chi)$ *and if* f *vanishes at all of the cusps of* $\mathbb{H}/\Gamma_0(N)$ *then* f *will be called a cusp form. The subspace of cusp forms is denoted* $S_{k/2}(N,\chi)$.

As in the case of integral weight forms, there are Hecke operators on the spaces of half-integral weight modular forms:

DEFINITION 3.6.2. *Suppose* $f(\tau)=\sum_{n\geq 1}a_n(f)q^n\in S_{k/2}(N,\chi)$. *Let* $\lambda=\frac{k-1}{2}$. *Then for* p *a prime, we put* $(T_pf)(\tau)=\sum_{n\geq 1}b_nq^n$ *where*

$$b_n=a_{p^2n}(f)+\chi(p)\left(\frac{(-1)^\lambda n}{p}\right)p^{\lambda-1}a_n(f)+\chi(p^2)p^{k-2}a_{n/p^2}(f) \tag{3.8}$$

with $a_{n/p^2}(f)=0$ *if* $p^2\nmid n$.

As before, if $f\in S_{k/2}(N,\chi)$ then so is T_pf, and one can prove that there is a basis for $S_{k/2}(N,\chi)$ of forms which are eigenforms for all of the T_p with $p\nmid N$. However, if we define oldforms and newforms as in the integral weight case, the spaces of half-integral weight cusp forms do not, in general, have the 'Multiplicity One" property. The notion of twisting by a Dirichlet character ψ modulo M is very similar to that of the integral weight case the only difference being that if $f\in S_{k/2}(N,\chi)$ is an eigenform for T_p with eigenvalue $\lambda_p(f)$ then $f_\psi\in S_{k/2}(NM^2,\chi\psi^2)$ is an eigenform for T_p with eigenvalue $\lambda_p(f_\psi)=\psi^2(p)\lambda_p(f)$.

3.7 The Theory of Shimura and Waldspurger.

The main link between modular forms of integral weight and those of half-integral weight is the correspondence given by the following theorem of Shimura [45].

THEOREM 3.7.1. [Shimura] *Let* $k\geq 3$ *be an odd integer,* $N\in 4\mathbb{N}$, χ *a Dirichlet character modulo* N, *and let* $f(\tau)=\sum_{n\geq 1}a_n(f)q^n\in S_{k/2}(N,\chi)$. *Further, let* t *be a square-free positive integer, and* ψ_t *the character modulo* tN *defined by*

$$\psi_t(m)=\chi(m)\left(\frac{-1}{m}\right)^{\frac{k-1}{2}}\left(\frac{t}{m}\right). \tag{3.9}$$

Define a function $g_t(\tau) = \sum_{n\geq 1} a_n(g)q^n$ *by the formal identity:*

$$\sum_{n\geq 1} \frac{a_n(g)}{n^s} = \left(\sum_{m\geq 1} \frac{\psi_t(m)m^{\frac{k-3}{2}}}{m^s}\right)\left(\sum_{m\geq 1} \frac{a_{tm^2}(f)}{m^s}\right). \tag{3.10}$$

Suppose that f *is an eigenform for* T_p *for all prime factors* p *of* N *not dividing the conductor of* ψ_t*. Then* $g_t \in M_{k-1}(M, \chi^2)$ *for some integer* M*. If* $k \geq 5$*, then* g_t *is a cusp form.*

It was later proven by Niwa [37] that M could be taken to be $N/2$. Any of the forms g_t in Theorem 3.7.1 are often referred to as a *Shimura lift* of f, or f is said to *lift through the Shimura correspondence to* g_t. One can show that the Shimura lift commutes with the Hecke operators. So, if the form f in Theorem 3.7.1 is an eigenform for some T_p on $S_{k/2}(N, \chi)$ with eigenvalue $\lambda_p(f)$, then the forms g_t are also eigenforms for the corresponding T_p on $M_{k-1}(M, \chi^2)$ with the same eigenvalue, that is $\lambda_p(g) = \lambda_p(f)$.

Next, we need to understand a little of the theory developed by Waldspurger in [51] which will provide a tool for obtaining information about the central critical values of the L-series $L(f_{\chi_n}, s)$ associated to the quadratic twists of a particular integral weight newform f. Before stating his results, we need to introduce one more bit of notation. If $f \in S_{2k}(N, \chi)$ is a newform, and if ψ is a Dirichlet character modulo M, then $f_\psi \in S_{2k}(NM^2, \chi\psi^2)$ is an eigenform for all of the Hecke operators. Hence, by the theory of newforms developed in [1] and [31], there exists a unique newform of weight $2k$ and character $\chi\psi^2$ which we will denote $f \cdot \psi$ with the same eigenvalues as f_ψ for all but finitely many of the Hecke operators. In fact, it is the central critical values of the $L(f \cdot \psi, s)$ which Waldspurger's theorem allows us to relate to the Fourier coefficients of a half-integral weight form.

Since f_ψ and $f \cdot \psi$ have the same eigenvalues for all but a finite number of the Hecke operators, it follows that $L(f \cdot \psi, s)$ and $L(f_\psi, s)$ differ only by a finite number of Euler factors. In fact, $f \cdot \psi$ and f_ψ can have different eigenvalues only for those

T_p with $p \mid NM^2$. Hence, letting S denote the finite set of primes at which the Euler factors of $L(f \cdot \chi_n, s)$ and $L(f_{\chi_n}, s)$ differ, it follows from (3.6) and (3.7) that for $Re(s) \geq k+1$, $A(s)L(f \cdot \psi, s) = B(s)L(f_\psi, s)$ where

$$\begin{aligned} A(s) &= \prod_{p \in S} \frac{1}{1 - \lambda_p(f)\psi(p)p^{-s}} \\ B(s) &= \prod_{p \in S} \frac{1}{1 - \lambda_p(f \cdot \psi)p^{-s}}. \end{aligned} \tag{3.11}$$

Since f and $f \cdot \psi$ are newforms, it follows from Theorem 2, Corollary 1 and Corollary 2 of [38], that for $p \in S$, $|\lambda_p(f)|$ and $|\lambda_p(f \cdot \psi)|$ are either 0, p^{k-1} or $p^{\frac{2k-1}{2}}$ depending on the conductor of χ. In any of these cases, we can see that $A(s)$ and $B(s)$ are both meromorphic on $\mathbb{C}$ and that neither of them has a pole at $s = k$. Thus, we may pick an open region U in $\mathbb{C}$ such that $U \cap \{s : Re(s) > k+1\}$ is nonempty, $k \in U$ and the function $A(s)L(f \cdot \psi, s) - B(s)L(f_\psi, s)$ is holomorphic on U. Since $A(s)L(f \cdot \psi, s) - B(s)L(f_\psi, s)$ is identically 0 on $U \cap \{s : Re(s) > k+1\}$, it follows that $A(s)L(f \cdot \psi, s) - B(s)L(f_\psi, s) = 0$ for all $s \in U$. In particular, we have $A(k)L(f \cdot \psi, k) = B(k)L(f_\psi, k)$. Since $A(k), B(k) \neq 0$, we have that $L(f_\psi, k) = 0$ if and only if $L(f \cdot \psi, k) = 0$. We note also that if E is a modular elliptic curve and if f is the weight 2 newform associated to E, then $f \cdot \chi_n$ is the newform associated to the n^{th} quadratic twist E_n of E.

Now, we are ready to state a special case of the main theorem in [51]:

THEOREM 3.7.2. *Let $k \geq 3$ be an odd integer, N an integer divisible by 4, χ a Dirichlet character modulo N, and M some divisor of N so that χ^2 is a Dirichlet character modulo M. Suppose $F \in S_{k-1}^{\text{new}}(M, \chi^2)$ is a newform with Hecke eigenvalues $\lambda_p(F)$. Suppose also that there exists a cusp form $f \in S_{k/2}(N, \chi)$ having the property that for all but finitely many primes p, $T_p f = \lambda_p(F)f$. Finally suppose that the Dirichlet character ν defined by $\nu(n) = \chi(n)(\frac{-1}{n})^{\frac{k-1}{2}}$ has conductor divisible by 4. Let $\mathbb{N}^{sf}$ denote the square-free natural numbers. Then there is a function*

$\mathbb{A} : \mathbb{N}^{sf} \to \mathbb{C}$, *depending only on* F *and satisfying the following condition:*

$$(\mathbb{A}(t))^2 = L(F \cdot \nu^{-1}\chi_t, \frac{k-1}{2}) \cdot \epsilon(\nu^{-1}\chi_t, 1/2), \tag{3.12}$$

where $\epsilon(\psi, s)$ *is chosen so that if* $L(\psi, s)$ *is the Dirichlet L-function for the Dirichlet character* ψ *and if*

$$\Lambda(\psi, s) = \begin{cases} \pi^{-s/2}\Gamma(\frac{s}{2})L(\psi, s) & \text{if } \psi(-1) = 1 \\ \pi^{-(s+1)/2}\Gamma(\frac{s+1}{2})L(\psi, s) & \text{if } \psi(-1) = -1 \end{cases}$$

then

$$\Lambda(\psi^{-1}, 1-s) = \epsilon(\psi, s)\Lambda(\psi, s).$$

Moreover f *can be written as a finite* $\mathbb{C}$*-linear combination of Hecke eigenforms* f_i *such that* $a_t(f_i) = c(t^{sf}, F)\mathbb{A}(t)$*, where* t^{sf} *denotes the square-free part of* t *and* $c(t^{sf}, F) \in \mathbb{C}$*.*

In particular, we can deduce from Theorem 3.7.2 that if $a_t(f) \neq 0$ then $L(F \cdot \nu^{-1}\chi_t, \frac{k-1}{2}) \neq 0$. Also, we will find it convenient to use the following theorem which is stated as Corollary 2 to the main theorem in [51]:

THEOREM 3.7.3. *Let* k*,* N*,* χ*,* M*,* F *and* f *be as in Theorem 3.7.2. If* n_1 *and* n_2 *are positive square-free integers such that* $\frac{n_1}{n_2} \in (\mathbb{Q}_p^\times)^2$ *for all* $p \mid N$*, then letting* $\ell = \frac{k-1}{2}$ *we have:*

$$a_{n_1}(f)^2 L(F \cdot \chi_{-1}^\ell \chi^{-1}\chi_{n_2}, \ell)\chi(n_2/n_1)n_2^{\ell-\frac{1}{2}} = a_{n_2}(f)^2 L(F \cdot \chi_{-1}^\ell \chi^{-1}\chi_{n_1}, \ell)n_1^{\ell-\frac{1}{2}}.$$

So, letting

$$W = \begin{cases} \prod\limits_{p|N} p & \text{if } 2 \nmid N \\ 8 \prod\limits_{\substack{p|N \\ p>2}} p & \text{if } 2 \mid N, \end{cases} \tag{3.13}$$

if we can find a set of representatives $m_i \in \mathbb{N}$ for $(\mathbb{Z}/W\mathbb{Z})^\times/(\mathbb{Z}/W\mathbb{Z})^{\times 2}$ such that $a_{m_i}(f) \neq 0$, then from Theorem 3.7.3 we have for any positive square-free integer n coprime to W:

$$L(F \cdot \chi_{-1}^\ell \chi^{-1}\chi_n, \ell) = \chi^{-1}(n)\frac{a_n(f)^2}{n^{\ell-\frac{1}{2}}}\beta_{m_i} \tag{3.14}$$

where

$$\beta_{m_i} = \chi^{-1}(m_i^{-1}) \frac{L(F \cdot \chi_{-1}^{\ell} \chi^{-1} \chi_{m_i}, \ell) m_i^{\ell - \frac{1}{2}}}{a_{m_i}(f)^2}, \tag{3.15}$$

and $m_i \equiv n$ in $(\mathbb{Z}/W\mathbb{Z})^\times/(\mathbb{Z}/W\mathbb{Z})^{\times 2}$. So, if $\beta_{m_i} \neq 0$, then in order to determine how often the twists of $L(F, s)$ have non-zero central critical value, it is enough to understand how often the Fourier coefficients of f are non-zero.

3.8 Computation.

Finally, we note that since the spaces $S_k(N, \chi)$ and $S_{k/2}(N, \chi)$ are finite dimensional, we can use computers to work with the forms in them. For instance to check that two forms in the same space are equal it suffices to check that their first few Fourier coefficients agree. In particular we have the following theorem (see [15] for a proof).

THEOREM 3.8.1. *Suppose that $f, g \in M_k(N, \chi)$ and suppose that $a_n(f) = a_n(g)$ for $0 \leq n \leq \frac{kN}{12} \prod_{p|N} \left(1 + \frac{1}{p}\right)$. Then $f = g$.*

COROLLARY 3.8.2. *Suppose that $f, g \in M_{k/2}(N, \chi)$ where k is odd and $4 \mid N$. Suppose also that $a_n(f) = a_n(g)$ for $0 \leq n \leq \frac{(k+1)N}{24} \prod_{p|N} \left(1 + \frac{1}{p}\right)$. Then $f = g$.*

PROOF. Let $\theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2}$ denote the classical theta-function. Then we know that $\theta \in M_{1/2}(4, \chi_2)$. Thus $f\theta, g\theta \in M_{\frac{k+1}{2}}(N, \chi\chi_2)$. Now the result follows from Theorem 3.8.1.

Also, checking that a given modular form is an eigenform with respect to a given T_p only requires a finite computation. In particular, we have the following corollary of Theorem 3.8.1.

COROLLARY 3.8.3. *Suppose $h \in M_k(N, \chi)$ (resp. $M_{k/2}(N, \chi)$) is a nonzero cusp form and let t denote the smallest natural number such that $a_t(h) \neq 0$. Then h is an eigenform for T_p if and only if $a_i(T_p h) = \frac{a_t(T_p h)}{a_t(h)} a_i(h)$ for all $0 \leq i \leq \frac{kN}{12} \prod_{p|N} \left(1 + \frac{1}{p}\right)$ (resp. $0 \leq i \leq \frac{(k+1)N}{24} \prod_{p|N} \left(1 + \frac{1}{p}\right)$.*

PROOF. By definition h is an eigenform for T_p if and only if there is a $\lambda \in \mathbb{C}$ such that $T_p h = \lambda h$. Since, $a_t(h) \neq 0$, the only possibility for λ is $\frac{a_t(T_p h)}{a_t(h)}$. Now the desired result follows by taking $f = T_p h$ and $g = \frac{a_t(T_p(h)}{a_t(h)} h$ in Theorem 3.8.1 (resp. Corollary 3.8.2).

We also have the following analog of Theorem 3.8.1, due to Sturm [48], which enables us to check when the Fourier coefficients of two integral weight modular forms having integer coefficients are congruent modulo a prime.

THEOREM 3.8.4. *Let f and $g \in M_k(N, \chi)$ be modular forms with integer coefficients and let p be any prime. Suppose that $a_n(f) \equiv a_n(g)$ modulo p for $0 \leq n \leq \frac{k}{12} N \prod_{p|N}(1 + \frac{1}{p})$. Then $a_n(f) \equiv a_n(g)$ modulo p for all nonnegative integers n.*

Similarly, to check that $f \in S_k(N, \chi)$ is an eigenform for all of the Hecke operators T_p with $p \nmid N$, it suffices to check that f is an eigenform for the first few primes not dividing N. More precisely, from the theory of newforms developed in [1] and [31] we have the following theorem.

THEOREM 3.8.5. *Let $\mathcal{N}$ denote the set of all newforms of weight k, character χ and level any divisor of N. Pick a set of primes $P = \{p_1, p_2, \ldots, p_j\}$ not dividing N such that for any form $g \in \mathcal{N}$ the sequence of eigenvalues, $\lambda_{p_1}(g), \ldots, \lambda_{p_j}(g)$, distinguish g among all the forms in $\mathcal{N}$. Then $f \in S_k(N, \chi)$ is an eigenform for all of the Hecke operators T_p with $p \nmid N$ if and only if f is an eigenform for all T_p with $p \in P$.*

PROOF. By the main results in [1] and [31], we know that any $f \in S_k(N, \chi)$ can be uniquely written as

$$f(\tau) = \sum_{g \in \mathcal{N}} \sum_{d | \frac{N}{N_g}} c_{g,d} g_d(\tau), \tag{3.16}$$

where N_g denotes the level of the newform $g \in \mathcal{N}$, and $g_d(\tau) = g(d\tau)$. By the definition of the Hecke operators (Definition 3.2.1), it follows that for all primes

$p \nmid N$, $\lambda_p(g_d) = \lambda_p(g)$ and that the Hecke operators are linear. Hence, we have for any prime $p \nmid N$,

$$\begin{aligned}(T_p f)(\tau) &= \sum_{g \in \mathcal{N}} \sum_{d \mid \frac{N}{N_g}} c_{g,d} (T_p g_d)(\tau) \\ &= \sum_{g \in \mathcal{N}} \sum_{d \mid \frac{N}{N_g}} c_{g,d} \lambda_p(g) g_d(\tau).\end{aligned} \tag{3.17}$$

Thus, from our assumption that $T_p f = \lambda_p(f) f$ for all $p \in P$, it follows that for all $p \in P$ and for all g_d in (3.17) with $c_{g,d} \neq 0$ that $\lambda_p(g_d) = \lambda_p(f)$. By our choice of P, it follows that there is at most one $g \in \mathcal{N}$ such that $\lambda_p(g) = \lambda_p(f)$ for all $p \in P$. Thus,

$$f(\tau) = \sum_{d \mid \frac{N}{N_g}} c_d g_d(\tau). \tag{3.18}$$

It follows form (3.18) that for all primes $p \nmid N$, f is an eigenform for T_p with eigenvalue $\lambda_p(f) = \lambda_p(g)$.

The number j of primes needed in P depends on N, k and χ and can be determined by looking at tables of newforms. For instance, if we examine the tables of Cremona [11], we find that there are three newforms of weight 2, trivial character and level dividing 38. Each of these newforms has a distinct eigenvalue for T_3. So, in this case, we can take $P = \{3\}$. Further examining the tables of [11], we see that there are twelve newforms of weight 2, trivial character and level dividing 978. Letting $f_1, \ldots, f_{12}$ denote these newforms, we list their eigenvalues for T_5, T_7 and T_{11} in the following table:

i	$\lambda_5(f_i)$	$\lambda_7(f_i)$	$\lambda_{11}(f_i)$
1	-4	2	-6
2	-1	-1	0
3	-1	-3	-4
4	-3	-1	0
5	0	3	-3
6	2	2	4
7	-3	-3	-6
8	-4	5	1
9	-3	1	2
10	-1	-1	-2
11	-3	-3	-4
12	0	-1	3

We can see that in this case we can take $P = \{5, 7, 11\}$. For cusp forms of low weight, we note that in practice the size of P is usually quite small.

As a corollary to Theorem 3.8.5, we can prove a similar statement for cusp forms of half-integral weight. Before stating the corollary, however, we need to discuss a few more details. Let ψ denote a Dirichlet character of conductor r with $\psi(-1) = -1$. Then $\theta_{\psi,t}(\tau) = \sum_{n=1}^{\infty} \psi(n) n q^{tn^2}$ is a weight $3/2$ cusp form (see [45]). In fact, $\theta_{\psi,t}(\tau) \in S_{3/2}(4tr^2, \left(\frac{-1}{\cdot}\right)\psi)$. Let $U_{3/2}(N, \chi)$ denote the orthogonal complement of $< \theta_{\psi,t} >$ in $S_{3/2}(N, \chi)$. It can be shown [18] that any $f \in U_{3/2}(N, \chi)$ lifts through the Shimura lift to a cusp form. Also, $U_{3/2}(N, \chi)$ is fixed by the Hecke operators. Now we are ready to state the corollary.

COROLLARY 3.8.6. *Suppose that k is odd, $N \in 4\mathbb{N}$, and that χ is a Dirichlet character modulo N. Suppose that $f \in S_{k/2}(N, \chi)$ ($U_{3/2}(N, \chi)$ if $k = 3$). Let $\mathcal{N}$ denote the set of all newforms of weight $k-1$, character χ^2 and level any divisor of $N/2$. Pick a set of primes P as in Theorem 3.8.5. Then f is an eigenform for all of the Hecke operators T_p with $p \nmid N$ if and only if for all $p \in P$, f is an eigenform for T_p.*

PROOF. Choose a basis $\{f_i\}_{i=1}^{M}$ for $S_{k/2}(N, \chi)$ (or $U_{3/2}(N, \chi)$ if $k = 3$) such that each f_i is an eigenform for all of the Hecke operators T_p with $p \nmid N$. For each f_i

we choose a square-free natural number t_i such that $a_{t_i m^2}(f_i) \neq 0$ for some natural number m. Then we apply Theorem 3.7.1 with $t = t_i$ to each of the f_i to get a nontrivial Hecke-eigenform $F_i \in S_{k-1}(N/2, \chi^2)$. Now for each $1 \leq i \leq M$ let G_i denote the unique newform of weight $k-1$ and character χ with $\lambda_p(G_i) = \lambda_p(F_i)$ for all primes $p \nmid N$. Then, we define a map $\mathcal{S} : S_{k/2}(N, \chi) \to S_{k-1}(N/2, \chi^2)$ in the following way. If $f \in S_{k/2}(N, \chi)$, then for $1 \leq i \leq M$, we choose $c_i \in \mathbb{C}$ so that $f = \sum_{i=1}^{M} c_i f_i$ and, we define $\mathcal{S}(f) = \sum_{i=1}^{M} c_i G_i$. Since the Shimura map commutes with the Hecke operators, it follows that our map $\mathcal{S}$ also commutes with the Hecke operators. Thus, f is a Hecke-eigenform if and only if $\mathcal{S}(f)$ is a Hecke-eigenform and they have the same eigenvalues. Now the desired result follows from Theorem 3.8.5.

Chapter 4

Ternary Quadratic Forms

In this chapter we recall some basic definitions and facts from the theory of ternary quadratic forms. We will be particularly interested in building weight 3/2 cusp forms from ternary quadratic forms.

4.1 Constructing Cusp Forms from Ternary Quadratic Forms.

Let Q be the ternary quadratic form given by

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy \tag{4.1}$$

with $a, b, c, r, s, t \in \mathbb{Z}$. Then, define Θ_Q formally as

$$\Theta_Q(\tau) = \sum_{x,y,z \in \mathbb{Z}} q^{Q(x,y,z)}. \tag{4.2}$$

It turns out for certain types of ternary forms Q, that Θ_Q is a modular form of weight 3/2. We will be able to say more about this theta function (eg. what its level and character are) a bit later, but first we need to review some facts about ternary forms.

Henceforth, we will be concerned only with positive definite ternary quadratic forms with integer coefficients, that is forms $Q(x, y, z)$ as above satisfying:

1. $Q(x, y, z) \geq 0$ for all $x, y, z \in \mathbb{R}$, and
2. $Q(x, y, z) = 0$ if and only if $x = y = z = 0$.

Also, we will restrict our attention to the forms $Q(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$ which are primitive, that is forms with $\gcd(a, b, c, r, s, t) = 1$.

Given a ternary quadratic form $Q(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$, we associate to it the matrix

$$A_Q = \begin{pmatrix} 2a & t & s \\ t & 2b & r \\ s & r & 2c \end{pmatrix}. \tag{4.3}$$

We define the discriminant d_Q and divisor m_Q of Q as

$$d_Q = \frac{det(A_Q)}{2} = 4abc + rst - ar^2 - bs^2 - ct^2, \tag{4.4}$$

$$m_Q = \gcd(A_{1,1}, A_{2,2}, A_{3,3}, 2A_{2,3}, 2A_{1,3}, 2A_{1,2}), \tag{4.5}$$

where $A_{i,j}$ denotes the (i,j)-cofactor of A_Q. Finally, we define the *level* of Q to be

$$N_Q = \frac{4d_q}{m_Q}. \tag{4.6}$$

We note that we could also define N_Q to be the smallest positive integer N such that NA_Q^{-1} is an integral matrix having even diagonal entries. Then we have the following special case of a theorem in [45] which is a generalization of an earlier idea of Schoenberg [44]:

THEOREM 4.1.1. *Suppose that Q is a primitive positive definite ternary quadratic form. Letting the notation be as above we have: $\Theta_Q \in M_{3/2}(N_Q, \chi_{d_Q})$.*

Two ternary forms Q_1 and Q_2 with coefficients in a ring R are said to be *equivalent over R* if there is a 3×3 matrix U with entries in R and determinant a unit in R such that $A_{Q_2} = UA_{Q_1}U^T$, where U^T denotes the transpose of U. If Q_1 and Q_2 are equivalent over $\mathbb{Z}$ then we simply say that they are *equivalent*. Since the only units in $\mathbb{Z}$ are ± 1, we see that if Q_1 and Q_2 are equivalent, then they have the same discriminants. The forms of a certain discriminant can then be grouped into equivalence classes. In fact, if we are given a particular discriminant d then there are only a finite number of equivalence classes of forms having that discriminant. This fact comes from our next theorem which is due to Eisenstein and is Proposition 3 in [30] (see also [14] and [24]).

DEFINITION 4.1.2. *Given a ternary quadratic form $Q(x,y,z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$, we say that Q is reduced if all of the following conditions hold:*

1. $a \leq b \leq c$,

2. *r, s and t are either all positive or all non-positive,*
3. *$a \geq |t|$; $a \geq |s|$; $b \geq |r|$,*
4. *$a + b + r + s + t \geq 0$,*
5. *if $a = t$ then $s \leq 2r$; if $a = s$ then $t \leq 2r$; if $b = r$ then $t \leq 2s$,*
6. *if $a = -t$ then $s = 0$; if $a = -s$ then $t = 0$; if $b = -r$ then $t = 0$,*
7. *if $a + b + r + s + t = 0$ then $2a + 2s + t \leq 0$,*
8. *if $a = b$ then $|r| \leq |s|$; if $b = c$ then $|s| \leq |t|$.*

THEOREM 4.1.3. *Every primitive positive definite ternary quadratic form is equivalent to a unique reduced form. Also, if $Q(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$ is a reduced form of discriminant d then $d/4 \leq abc \leq d$.*

If Q_1 and Q_2 are ternary forms with coefficients in $\mathbb{Z}$ which are equivalent over the p-adic integers $\mathbb{Z}_p$ for all primes p and are equivalent over the reals, then we say that Q_1 and Q_2 are in the same *genus*. Equivalently, we may think of two ternary quadratic forms Q_1 and Q_2 as being in the same genus if Q_1 and Q_2 represent the same set of values as we let the variables x, y and z vary over all rational numbers. It follows from our definitions that forms which are equivalent are in the same genus. It can be shown that all forms in a given genus have the same discriminant and level (see [30]). Hence we can speak of breaking a genus up into its equivalence classes, and by Theorem 4.1.3 and condition 3 of Definition 4.1.2, there are only finitely many of these equivalence classes in a genus of forms. Also, we have the following theorem due to Siegel [46].

THEOREM 4.1.4. *Let Q_1 and Q_2 be two positive definite quadratic forms which are in the same genus. Then $(\Theta_{Q_1} - \Theta_{Q_2})$ is a cusp form.*

Let $r_i(n) = \#\{x, y, z \in \mathbb{Z} : Q_i(x, y, z) = n\} \quad (i = 1, 2)$. Then,

$$\Theta_{Q_1}(\tau) - \Theta_{Q_2}(\tau) = \sum_{n \geq 1} (r_1(n) - r_2(n)) q^n \in S_{3/2}(N_{Q_1}, \chi_{d_{Q_1}}). \tag{4.7}$$

We note that if Q_1 and Q_2 are equivalent, then $r_1(n) = r_2(n)$ for all positive integers n. We only get a nonzero cusp form if Q_1 and Q_2 are in the same genus but are not equivalent.

We can check if two ternary forms are in the same genus as follows. Given a primitive positive definite ternary quadratic form $Q(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$, we put

$$\begin{aligned} a' &= \frac{A_{1,1}}{m_Q}, \qquad & r' &= \frac{2A_{2,3}}{m_Q}, \\ b' &= \frac{A_{2,2}}{m_Q}, \qquad & s' &= \frac{2A_{1,3}}{m_Q}, \\ c' &= \frac{A_{3,3}}{m_Q}, \qquad & t' &= \frac{2A_{1,2}}{m_Q}. \end{aligned} \tag{4,8}$$

Then we can define the reciprocal of Q to be the ternary form

$$Q'(x, y, z) = a'x^2 + b'y^2 + c'z^2 + r'yz + s'xz + t'xy. \tag{4.9}$$

By replacing Q with an equivalent form if necessary, we can ensure that a and c' are coprime to each other and to $m_Q m_{Q'}$ (see [30, p.410]). For odd primes $p \mid m_Q$ we define $(\frac{Q}{p}) = (\frac{a}{p})$, where $(\frac{a}{p})$ denotes the Legendre symbol. Similarly, for odd primes $p \mid m_{Q'}$, we define $(\frac{Q'}{p}) = (\frac{c'}{p})$. If $16 \mid m_Q$ then we put $(\frac{Q}{4}) = (-1)^{\frac{a-1}{2}}$ and if $32 \mid m_Q$ then we put $(\frac{Q}{8}) = (-1)^{\frac{a^2-1}{8}}$. We define $(\frac{Q'}{4})$ and $(\frac{Q'}{8})$ similarly. We call this collection of symbols the *genus symbols* for Q. The following theorem, which is Proposition 4 in [30], gives a way to tell when two forms are in the same genus:

THEOREM 4.1.5. *Let Q_1 and Q_2 be primitive positive definite ternary quadratic forms with coefficients in $\mathbb{Z}$. Then Q_1 and Q_2 are in the same genus if and only if they have the same discriminant, the same level and the same collection of genus symbols.*

4.2 Representations by a Genus of Ternary Quadratic Forms.

We will also be interested in the number of representations of an integer n by a ternary quadratic form, since differences of these representation numbers will be the

coefficients of our weight 3/2 cusp forms. We will be particularly interested in the case when n is a square-free integer. In general, these representation numbers may be very hard to understand, hence we will content ourselves with understanding the number of representations of an integer n by a genus of forms. First we need some more terminology.

If Q is a ternary form and $X = (x_0, y_0, z_0)^T$ is such that $Q(X) = \frac{1}{2}X^T A_Q X = n$, then we will refer to X as a *representation* of n by Q. If $\gcd(x_0, y_0, z_0) = 1$ then we say that X is a *primitive representation*. We will restrict our attention to only considering primitive representations, and we note that if n is a square-free integer then all representations of n are primitive. We note also that if there is a representation X of n by Q, then there exists a solution X to $Q(X) = n$ in $\mathbb{Z}_p$ for all primes p. However, the converse is not true. What can be said is the following (see [24, pp. 186–187] for a proof).

THEOREM 4.2.1. *If there is a solution to $Q(X) \equiv n \pmod{p^{r+1}}$ for every prime $p \mid 2d_Q$, where p^r is the highest power of p dividing n or $4n$ depending on whether p is odd or even, and if there is a real solution to $Q(X) = n$, then n is represented by some form Q' which is in the same genus as Q.*

We call a 3×3 matrix U with integer coefficients an *automorph* of the ternary form Q if U has determinant 1 and if $U^T A_Q U = A_Q$. If U is an automorph of Q and $X = (x_0, y_0, z_0)^T$ is a representation of n by Q, then putting $Y = UX$, we find that $Q(Y) = \frac{1}{2}Y^T A_Q Y = \frac{1}{2}X^T U^T A U X = \frac{1}{2}X^T A X = Q(X) = n$. We will think of such representations X and Y as being essentially the same. Hence, we say that two representations X_1 and X_2 are *essentially distinct* if there is no automorph U of Q such that $X_1 = UX_2$.

Now, suppose that $\{Q_1, Q_2, \ldots, Q_k\}$ is a complete set of representatives for the equivalence classes of forms belonging to a particular genus of positive definite ternary quadratic forms. We will denote by $r_i(n)$ the number of representations of

n by Q_i, and we will denote by $R_i(n)$ the number of essentially distinct primitive representations of n by Q_i. When n is square-free we have

$$R_i(n) = r_i(n)/A_i, \tag{4.10}$$

where A_i denotes the number of automorphs of Q_i. We will also denote by $R(Q, n)$ the number of essentially distinct primitive representations of n by the genus containing Q. Thus for any $1 \leq i \leq k$ we have

$$R(Q_i, n) = \sum_{j=1}^{k} R_j(n). \tag{4.11}$$

There is a theorem due to Gauss which relates the values of $R(Q, n)$ to the values of class numbers of orders in imaginary quadratic fields. Before stating this theorem, we need to define the Hilbert symbol.

DEFINITION 4.2.2. *For a and b nonzero p-adic integers, we define the Hilbert symbol $(a, b)_p$ as follows*

$$(a, b)_p = \begin{cases} 1, & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } \mathbb{Q}_p \\ -1, & \text{otherwise.} \end{cases} \tag{4.12}$$

The Hilbert symbol is fairly easy to compute using the following Theorem (see [24] for a proof).

THEOREM 4.2.3. *Let a and b be nonzero p-adic integers. Then*

1. $(a, b)_p = (b, a)_p$.
2. $(a\rho^2, b\sigma^2)_p = (a, b)_p$.
3. $(a, -a)_p = 1$.
4. *If $a = p^r a_1$ and $b = p^s b_1$ where a_1 and b_1 are units, then*

$$(a, b)_p = \begin{cases} \left(\frac{-1}{p}\right)^{rs} \left(\frac{a_1}{p}\right)^{s} \left(\frac{b_1}{p}\right)^{r}, & \text{if } p \text{ is odd} \\ \left(\frac{2}{a_1}\right)^{s} \left(\frac{2}{b_1}\right)^{r} (-1)^{(a_1-1)(b_1-1)/4}, & \text{if } p = 2. \end{cases} \tag{4.13}$$

We note that if $p \nmid 2ab$, then it follows immediately from statement 4 of Theorem 4.2.3 that $(a, b)_p = 1$. Now we can state Gauss' Theorem (see [24] Theorem 86).

THEOREM 4.2.4. *Let $Q = ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy$ be a primitive positive definite ternary quadratic form with matrix A and let Ω denote the* gcd *of the 2-rowed minors of A. Put $\Delta_n = \frac{4d_Q n}{\Omega^2}$. Then, for all $n > 1$ and prime to $2d_Q$ we have*

$$R(Q,n) = \begin{cases} 2^{-t(\Delta_1)} h(-4\Delta_n)\rho, & \text{if the genus of } Q \text{ represents } n \\ 0 & \text{otherwise.} \end{cases} \tag{4.14}$$

where $t(n)$ denotes the number of odd prime factors of n, $h(d)$ denotes the class number of the quadratic order with discriminant d and

$$\rho = \begin{cases} \frac{1}{2}, & \text{if } \Delta_n \equiv 1,2 \pmod 4 \text{ or } 4 \pmod 8 \\ 2, & \text{if } \Delta_n \equiv 7 \pmod 8 \text{ and } \Omega \text{ is odd} \\ 1, & \text{if } \Delta_n \equiv 7 \pmod 8 \text{ and } \Omega \text{ is even} \\ 1, & \text{if } \Delta_n = 3 \\ 1, & \text{if } \Delta_n \equiv 3 \pmod 8,\ \Delta_n \neq 3 \text{ and } c_2(Q)(-1)^r = 1 \\ \frac{1}{3}, & \text{if } \Delta_n \equiv 3 \pmod 8,\ \Delta_n \neq 3 \text{ and } c_2(Q)(-1)^r \neq 1 \\ \frac{1}{4}, & \text{if } \Delta_n \equiv 0 \pmod 8. \end{cases} \tag{4.15}$$

where r is the highest power of 2 in Ω and

$$c_2(Q) = (-1, \frac{-\det(A)}{8})_2 (a, t^2 - ab)_2 (ab - t^2, \frac{-\det(A)}{8})_2$$

denotes the Hasse symbol.

Since we will find it more convenient to work with the class number of the ring of integers in a imaginary quadratic field, we state the following theorem which relates the class number of an order in an imaginary quadratic field to the class number of the ring of integers of that field (see [10] for a proof).

THEOREM 4.2.5. *Let $D \equiv 0,1$ modulo 4 be negative and let m be a positive integer. Then,*

$$h(m^2 D) = \frac{h(D)m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right),$$

where $\mathcal{O}^*$ and $\mathcal{O}'^*$ are the unit groups of the orders of discriminant D and $m^2 D$, respectively.

We remark that since we are dealing with orders $\mathcal{O}$ in imaginary quadratic fields, the group of units $\mathcal{O}^*$ of $\mathcal{O}$ is simply $\{\pm 1\}$ except in the following two cases. If $\mathcal{O} = \mathbb{Z}[i]$, then $\mathcal{O}^* = \{\pm 1, \pm i\}$, and if $\mathcal{O} = \mathbb{Z}[\omega]$ where ω denotes a cube root of unity, then $\mathcal{O}^* = \{\pm 1, \pm\omega, \pm\omega^2\}$.

For a more detailed account of quadratic forms, see the books of Jones [24] and Dickson [14], and for more information on how to build cusp forms from ternary quadratic forms, see the paper of Lehman [30], especially the tables in the appendix.

Chapter 5

Prime Twists

As in Chapter 2 we will denote by E_D the D^{th} quadratic twist of an elliptic curve E and by $L(E_D, s)$ the L-function associated to E_D. We will obtain information on how often $L(E_p, 1) \neq 0$ as p varies over all prime numbers.

5.1 Statement of Results

In this chapter,we will prove the following theorem.

Theorem 5.1.1. *Let $E_p : y^2 = x^3 - 32p^3$. Then $L(E_p, 1) \neq 0$ for at least $\frac{1}{3}$ of the primes p.*

Although this theorem follows from a more general theorem of Ono and Skinner mentioned in Chapter 1, it is not included in the specific examples worked out in [40]. We would like to discuss a different and somewhat simpler proof of this result that does not explicitly involve the theory of Galois representations.

Using the Coates-Wiles theorem (see Theorem 2.6.4), we can then deduce the following.

Corollary 5.1.2. *The curve $y^2 = x^3 - 32p^3$ has only the trivial point (at infinity) for at least $\frac{1}{3}$ of the primes p.*

5.2 Proof of Results

Denote by E_D the elliptic curve $E_D : y^2 = x^3 + 4D^3$ where D is any square-free integer, and let $L(E_1, s) = \sum_{n \geq 1} \frac{a_n}{n^s}$.

Now, we note that E_D has complex multiplication by $\mathbb{Z}[\omega]$, where ω is a cube root of unity. Thus, it follows form work of Shimura that E_D is modular. Therefore, for

square-free D coprime to 6 $f_D(z) = \sum_{n=1}^{\infty} a_n \left(\frac{D}{n}\right) q^n \in S_2(N_D) \quad (q = e^{2\pi iz})$ where N_D is the conductor of E_D. Also, f_D is an eigenform for all of the Hecke operators.

Let,

$$g(z) = \frac{1}{2}\left(\sum_{x,y,z\in\mathbb{Z}} q^{x^2+27y^2+6z^2} - \sum_{x,y,z\in\mathbb{Z}} q^{4x^2+2xy+7y^2+6z^2}\right) = \sum_{n=1}^{\infty} b_n q^n. \tag{5.1}$$

Then by Theorems 4.1.1 and 4.1.4, we have that $g(z) \in S_{\frac{3}{2}}(216, \left(\frac{2}{\cdot}\right))$. By Theorem 3.7.1, we see that the Shimura lift G of g is in $S_2(108)$. Using (5.1) and Theorem 3.7.1, We calculated the first 100 Fourier coefficients of G and noticed that $a_n(G) = a_n(f_1)$ for $0 \leq n \leq 100$. Thus it follows from Theorem 3.8.1 that $G = f_1$, that is g lifts through the Shimura correspondence to f_1. Now we can apply Waldspurger's Theorem (Theorem 3.7.3) to gain information about the values $L(E_D, 1)$. In our case Waldspurger's theorem specializes to the following.

THEOREM 5.2.1. *For $D \equiv 1$ modulo 6,*

$$L(E_{-2D}, 1) = \frac{b_D^2}{\sqrt{D}}\beta, \tag{5.2}$$

where $\beta = L(E_{-2}, 1) \approx 1.363$.

Thus, $L(E_{-2D}, 1) = 0$ if and only if $b_D = 0$.

Let $\theta_t(\tau) = \sum_{n\in\mathbb{Z}} q^{tn^2}$. Then $\theta_t \in S_{1/2}(4t, \chi_t)$. Thus, $f_1 \in S_2(108) \subseteq S_2(216)$, and $g\theta_2 \in S_2(216)$. We calculated the first 100 Fourier coefficients of f_1 and $g\theta_2$ and noted that $a_n(f_1) \equiv a_n(g\theta_2)$ modulo 2 for $0 \leq n \leq 100$. Thus by Sturm's theorem (see Theorem 3.8.4), we have that $a_n(f_1) \equiv a_n(g\theta_2)$ modulo 2 for all nonnegative integers n, that is $g\theta_2 \equiv f_1$ modulo 2. Now, we notice that $\theta_2 \equiv 1$ modulo 2. Hence $g \equiv f_1$ modulo 2. So, for all nonnegative integers n we have

$$a_n(f_1) \equiv a_n(g) \pmod 2. \tag{5.3}$$

Recall now that $a_p(f_1) = p + 1 - \#E_1(\mathbb{F}_p)$. Thus, it follows from (5.3) that for any odd prime p, $a_p(g) \equiv \#E_1(\mathbb{F}_p)$ modulo 2. Next we note that $\#E_1(\mathbb{F}_p) \equiv 1$

modulo 2 precisely when $E_1(\mathbb{F}_p)$ has no point of order 2, that is when x^3+4 has no root modulo p. In particular, if x^3+4 has no root modulo p, then $a_p(g) \neq 0$. So, Theorem 5.1.1 follows from Theorem 5.2.1 and the following lemma.

LEMMA 5.4. *The polynomial x^3+4 has no root modulo p for $\frac{1}{3}$ of the primes p.*

PROOF. Note that for $p \equiv 2$ modulo 3, cubing is an automorphism of $\mathbb{F}_p$. So, x^3+4 always has a root modulo p when $p \equiv 2$ modulo 3. Thus we will restrict our attention to $p \equiv 1$ modulo 3 from now on. Hence, we have $\left(\frac{-3}{p}\right) = 1$. Now, we note that $\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right) = 1$, which implies that p splits in $\mathbb{Z}[\omega]$, where ω denotes a cube root of unity.

We have

$$\begin{array}{cc} \mathbb{Q}(\omega) & \mathfrak{p}_1\mathfrak{p}_2 \\ | & | \\ \mathbb{Q} & p \equiv 1 \pmod 3 \end{array}$$

Now, x^3+4 is irreducible over $\mathbb{Z}[\omega]$ and it has a root in $\mathbb{Z}[\omega]/\mathfrak{p}_i$ $(i=1,2)$ if and only if it has a root modulo p. (In fact $\mathbb{Z}[\omega]/\mathfrak{p}_i \cong \mathbb{F}_p$.) Thus the splitting of x^3+4 modulo p determines the splitting of $\mathfrak{p}_i$ in $\mathbb{Z}[\omega, 4^{\frac{1}{3}}]$. In particular, if x^3+4 has no root modulo p, then the $\mathfrak{p}_i$'s remain inert in $\mathcal{O}_{\mathbb{Q}(\omega,4^{\frac{1}{3}})}$, and p splits into exactly two primes in $\mathcal{O}_{\mathbb{Q}(\omega,4^{\frac{1}{3}})}$

$$\begin{array}{cc} \mathbb{Q}(\omega, 4^{\frac{1}{3}}) & \mathfrak{P}_1\mathfrak{P}_2 \\ | & | \\ \mathbb{Q} & p \equiv 1 \pmod 3 \end{array}$$

Now, $\mathbb{Q}(\omega, 4^{\frac{1}{3}})/\mathbb{Q}$ is a Galois extension with Galois group S_3. So, the residual degrees $f(\mathfrak{P}_1)$ and $f(\mathfrak{P}_2)$ are the same, and the ramification indices of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the same namely 1. Thus $f(\mathfrak{P}_1) = f(\mathfrak{P}_2) = 3$. This tells us that the order of the Frobenius $\sigma_{\mathfrak{P}_i}$ is 3. So, the size of the conjugacy class of $\sigma_{\mathfrak{P}_i}$ in S_3 is 2. The Lemma now follows from the Chebetarev Density Theorem.

Since f is an eigenform for all of the Hecke operators, it follows that the a_n's are multiplicative, that is if $\gcd(m,n) = 1$ then $a_{mn} = a_m a_n$. Thus we can deduce the following corollary form Theorem 5.1.1:

COROLLARY 5.2.2. *If D is a square free natural number such that if $p \mid D$ then $x^3 + 4$ has no root modulo p, then $L(E_D, 1) \neq 0$.*

Chapter 6

Positive Density Nonvanishing Results

In this Chapter we will be interested in studying certain cusp forms and the behavior of their Mellin transforms. In particular, we will exhibit examples of weight two newforms f for which we can prove that $L(f_{\chi_D}, 1) \neq 0$ for a positive density of square-free integers D. We will then be able to show the existence of cusp forms of higher weight having this property. In the first section we will discuss our first positive density result in detail. In the second section we will give some other positive density results, but will omit some of the details as the techniques used are the same as those discussed in section one.

6.1 A Positive Density Nonvanishing Result

Let $F \in S_2^{\text{new}}(112)$ be the newform associated to the modular elliptic curve $E : y^2 = x^3 - x^2 + 72x + 368$ of conductor 112, that is $L(F, s) = L(E, s)$. It turns out that $F_{\chi_{-1}} = \eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau)$, where

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n \geq 1} (1 - q^n). \tag{6.1}$$

Now putting

$$\begin{aligned} Q_1(x, y, z) &= x^2 + 7y^2 + 7z^2, \text{ and} \\ Q_2(x, y, z) &= 2x^2 + 4y^2 + 7z^2 - 2xy, \end{aligned} \tag{6.2}$$

we can define $f(\tau)$ formally as

$$\begin{aligned} f(\tau) &= \frac{1}{2}\left(\sum_{x,y,z \in \mathbb{Z}} q^{Q_1(x,y,z)} - \sum_{x,y,z \in \mathbb{Z}} q^{Q_2(x,y,z)} \right) \\ &= \sum_{n \geq 1} a_n(f) q^n. \end{aligned} \tag{6.3}$$

Using Theorem 4.1.5, one can prove the following Lemma.

LEMMA 6.1.1. *If Q_1 and Q_2 are defined as above then Q_1 and Q_2 are in the same genus. Furthermore, up to equivalence of forms, Q_1 and Q_2 are the only forms in the genus containing them.*

PROOF. Using Theorem 4.1.3 we can find all reduced forms of discriminant 196. There are 13 of them in all. Computing the levels of each of these, we see that there are only 3 forms having discriminant 196 and level 28:

$$\begin{aligned} Q_1(x,y,z) &= x^2 + 7y^2 + 7z^2, \\ Q_2(x,y,z) &= 2x^2 + 4y^2 + 7z^2 - 2xy, \text{ and} \\ Q_3(x,y,z) &= 3x^2 + 5y^2 + 5z^2 - 4yz - 2xz - 2xy. \end{aligned} \tag{6.4}$$

Now, we would like to compute the genus symbols of each of these 3 forms. It will be necessary, however, to first replace Q_1, Q_2 and Q_3 by the equivalent forms

$$\begin{aligned} S_1(x,y,z) &= 11x^2 + y^2 + 7z^2 + 4xy, \\ S_2(x,y,z) &= 11x^2 + 2y^2 + 7z^2 + 14xz + 2xy, \text{ and} \\ S_3(x,y,z) &= 5x^2 + 5y^2 + 3z^2 + 2yz - 2xz + 4xy. \end{aligned} \tag{6.5}$$

To see that these forms are equivalent, let

$$U_1 = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 0 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad U_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{6.6}$$

Then we have $U_i A_{Q_i} U_i^T = A_{S_i}$ for $i = 1, 2, 3$. Now, we compute the reciprocals of S_1, S_2, and S_3;

$$\begin{aligned} S_1'(x,y,z) &= x^2 + 11y^2 + z^2 - 4xy, \\ S_2'(x,y,z) &= 2x^2 + 4y^2 + 3z^2 + 2yz - 4xz - 2xy, \text{ and} \\ S_3'(x,y,z) &= 2x^2 + 2y^2 + 3z^2 - 2yz - 2xz - 2xy. \end{aligned} \tag{6.7}$$

Each of these has divisor 4. Thus, the only genus symbols that are defined for Q_1, Q_2, and Q_3 are: $\left(\frac{Q_1}{7}\right) = \left(\frac{S_1}{7}\right) = 1$, $\left(\frac{Q_2}{7}\right) = \left(\frac{S_2}{7}\right) = 1$, and $\left(\frac{Q_3}{7}\right) = \left(\frac{S_3}{7}\right) = -1$. Therefore, it follows from Theorem 4.1.5 that Q_1 and Q_2 are in the same genus.

Since Q_1, Q_2, and Q_3 are the only forms up to equivalence having discriminant 196 and level 28, and since Q_3 has a different genus symbol than Q_1 and Q_2, it also follows from Theorem 4.1.5 that Q_1 and Q_2 are the only forms in the genus containing them.

It now follows from Theorem 4.1.1, Lemma 6.1.1 and Theorem 4.1.4 that $f \in S_{3/2}(28)$. There are no cusp forms of the form $\theta_{\psi,t}$ in $S_{3/2}(28)$ Thus, we can use Theorem 3.8.6 to check by computer that f is a Hecke-eigenform. Also, we can use Theorem 3.7.1 and Theorem 3.8.1 to check that f lifts through the Shimura correspondence to $F_{\chi_{-1}}$.

Now applying (3.14) with $W = 56$ and choosing as representatives for the square classes modulo 56: $m_1 = 1$, $m_2 = 15$, and $m_3 = 85$ (none of the other square classes modulo 56 have any integers m in them with $a_m \neq 0$), we have the following theorem.

THEOREM 6.1.2. *For square-free natural numbers $n \equiv 1$, 9, 15, 23, 25, 29, 37, 39 or 53 modulo 56,*

$$L(F\chi_n, 1) = \frac{a_n(f)^2}{\sqrt{n}}\beta, \tag{6.8}$$

where $\beta \approx 1.325$ (the value of β was approximated by using the Apecs package with MAPLE).

Since Q_1 and Q_2 represent all of the equivalence classes of ternary quadratic forms in the same genus as themselves, we can combine Theorem 4.2.1, Theorem 4.2.4, and Theorem 4.2.5 to get the following theorem.

THEOREM 6.1.3. *For all square-free natural numbers $n \geq 11$ with $n \equiv 1$, 9 or 11 modulo 14,*

$$R(Q_1, n) = \begin{cases} \frac{h(-4n)}{2}, & \text{if } n \equiv 1, 9, 25 \pmod{28} \\ 3H(-n), & \text{if } n \equiv 11, 43, 51 \pmod{56} \\ h(-n), & \text{if } n \equiv 15, 23, 39 \pmod{56}, \end{cases} \tag{6.9}$$

where $h(\Delta)$ denotes the class number of the imaginary quadratic extension of $\mathbb{Q}$ with discriminant Δ.

From (6.3) we have that $2a_n(f) = r_1(n) - r_2(n)$, where $r_i(n)$ denotes the number of representations of n by Q_i. A simple calculation shows that the number of automorphs of Q_1 and Q_2 are 8 and 4, respectively. Thus, we have $R(Q_1, n) = \frac{r_1(n)}{8} + \frac{r_2(n)}{4}$ and, hence $r_1(n) - r_2(n) \equiv 2R(Q_1, n)$ modulo 3. So, by Theorem 6.1.3, we have for square-free $n \geq 9$ and $n \equiv 1, 9$ or 11 modulo 14

$$\begin{aligned} 2a_n(f) = r_1(n) - r_2(n) &\equiv 2R(Q_1, n) \pmod 3 \\ &\equiv \begin{cases} h(-4n) \pmod 3, & \text{if } n \equiv 1, 9, 25 \pmod{28}, \\ 0 \pmod 3, & \text{if } n \equiv 11, 43, 51 \pmod{56}, \\ 2h(-n) \pmod 3, & \text{if } n \equiv 15, 23, 39 \pmod{56}. \end{cases} \end{aligned} \tag{6.10}$$

Thus, we can immediately deduce:

PROPOSITION 6.1.4. *Suppose $n \geq 9$ is square-free. Then,*

1. *If $n \equiv 1$, 9 or 25 modulo 28 then*

$$a_n(f) \equiv 0 \pmod 3 \quad \text{if and only if} \quad h(-4n) \equiv 0 \pmod 3$$

2. *If $n \equiv 15$, 23 or 39 modulo 56 then*

$$a_n(f) \equiv 0 \pmod 3 \quad \text{if and only if} \quad h(-n) \equiv 0 \pmod 3$$

Now, we recall the following theorem of Davenport and Heilbronn [12] as improved by Nakagawa and Horie [35].

THEOREM 6.1.5. *Let $h_3(\Delta)$ denote the number of ideal classes of the quadratic extension of $\mathbb{Q}$ of discriminant Δ having order 1 or 3. Further, suppose that m and N satisfy:*

1. *If p is an odd prime dividing (N, m) then $p^2 \mid N$ and $p^2 \nmid m$, and*
2. *If N is even, then either $4 \mid N$ and $m \equiv 1$ modulo 4 or $16 \mid N$ and $m \equiv 8$ or 12 modulo 16.*

Then

$$\sum_{\substack{0>\Delta>-x \\ \Delta\equiv m \pmod N}}{}' h_3(\Delta) \sim 2\#\{\Delta : 0 > \Delta > -x; \Delta \equiv m \pmod N\} \tag{6.11}$$

as $X \to \infty$*, where* $\sum'$ *denotes the sum over fundamental discriminants* Δ*.*

From Theorem 6.1.5, we can deduce:

COROLLARY 6.1.6. *Suppose that* m *and* N *are as in Theorem 6.1.5. Let* T *denote the set of discriminants* Δ *of imaginary quadratic extensions of* $\mathbb{Q}$ *in the arithmetic progression* $\Delta \equiv m$ *modulo* N*. Then there is a subset* S *of* T *having lower density at least* $\frac{1}{2}$ *in* T *such that if* $\Delta \in S$ *then* $3 \nmid h(\Delta)$*, that is,*

$$\liminf_{x\to\infty}\left(\frac{\#\{\Delta : 0 > \Delta > -x; \Delta \in S\}}{\#\{\Delta : 0 > \Delta > -x; \Delta \in T\}}\right) \geq \frac{1}{2} \tag{6.12}$$

PROOF. Note that Δ always denotes the discriminant of some imaginary quadratic extension of $\mathbb{Q}$. We have

$$\begin{aligned}\sum_{\substack{0>\Delta>-x \\ \Delta\equiv m \pmod N}}{}' h_3(\Delta) &\geq \Bigg(\sum_{\substack{0>\Delta>-x \\ \Delta\equiv m \pmod N \\ 3\mid h(\Delta)}}{}' 3\Bigg) + \Bigg(\sum_{\substack{0>\Delta>-x \\ \Delta\equiv m \pmod N \\ 3\nmid h(\Delta)}}{}' 1\Bigg) \\ &= 3\cdot\#\{\Delta : 0 > \Delta > -x; \Delta \equiv m \pmod N\} - \\ &\quad 2\cdot\#\{\Delta : 0 > \Delta > -x; \Delta \equiv m \pmod N; 3 \nmid h(\Delta)\}.\end{aligned}$$

The result now follows from Theorem 6.1.5.

Combining Corollary 6.1.6 with Proposition 6.1.4, we obtain:

THEOREM 6.1.7. *There is a subset S of the square-free natural numbers $n \equiv 1$, 9, 15, 23, 25, 29, 37, 39 or 53 modulo 56 having lower density at least $\frac{1}{2}$, that is*

$$\liminf_{x\to\infty}\left(\frac{\#\{0<n<x : n\in S\}}{\#\left\{\begin{array}{c} n \text{ is square-free; } n\equiv 1,\ 9,\\ 0<n<x : 15,\ 23,\ 25,\ 29,\ 37,\ 39 \text{ or}\\ 53 \pmod{56}\end{array}\right\}}\right) \geq \frac{1}{2}, \tag{6.13}$$

such that $a_n(f) \neq 0$ for all $n \in S$.

PROOF. For square-free natural numbers $n \equiv 1$, 9 or 25 modulo 28, there is a quadratic extension k of $\mathbb{Q}$ with discriminant $\Delta_k = -4n$, namely, $k = \mathbb{Q}(\sqrt{-n})$. Also, $\Delta_k = -4n \equiv 12, 76$ or 108 modulo 112 and, these arithmetic progressions satisfy the hypotheses of Corollary 6.1.6. So, there is a subset S' of the square-free natural numbers $n \equiv 1$, 9 or 25 modulo 28 having lower density $\frac{1}{2}$ such that for all $n \in S'$, $h(-4n)$ is not divisible by 3.

On the other hand if $n \equiv 15$, 23 or 39 modulo 56, then there is a quadratic extension k of $\mathbb{Q}$ with discriminant $\Delta_k = -n$, namely, $k = \mathbb{Q}(\sqrt{-n})$. As before, we note that we have $\Delta_k = -n \equiv 17$, 33 or 41 modulo 56 and, these arithmetic progressions also satisfy the hypotheses of Corollary 6.1.6. So, there is a subset S'' of the square-free natural numbers $n \equiv 15$, 23 or 39 modulo 56 having lower density 1/2 such that for all $n \in S''$, $h(-n)$ is not divisible by 3.

So taking $S = S' \cup S''$, and combining the statements above with Proposition 6.1.4, gives the desired result.

Now, we note that the lower density of our set S above is 7/64. To see this, note that we are considering 9 arithmetic progressions modulo 56, which gives 63 arithmetic progressions modulo 392. Also, recall that we are only concerned with the square-free numbers, and there are only 288 arithmetic progressions modulo 392 in which square-free numbers appear. This is because the arithmetic progressions $n \equiv m$ modulo 392 do not contain any square-free numbers when m is a multiple of

either 4 or 49. Thus, our 63 arithmetic progressions modulo 392 account for 7/32 (= 62/288) of the square-free numbers and 1/2 of these are in S. Thus, combining Theorem 6.1.7 with (6.8) gives us our first positive density nonvanishing result.

THEOREM 6.1.8. *There is a subset S of the square-free natural numbers having lower density at least 7/64 such that $L(F_{\chi_D}, 1) \neq 0$ for all $D \in S$.*

Now, by Theorem 2.6.4, we know that if the L-series associated to an elliptic curve has nonzero central critical value, then the curve has Mordell-Weil rank 0. Thus, since $L(E_n, 1) = L(F_{\chi_n}, 1)$, we deduce from Theorem 6.1.8:

COROLLARY 6.1.9. *For at least 7/64 of the square-free natural numbers n, the elliptic curve $E_n : y^2 = x^3 - nx^2 + 72n^2x + 368n^3$ has rank 0.*

Now, we would like similar results for forms of higher weight. Let's start by considering the modular form

$$g(\tau) = \frac{\eta^3(\tau)}{\eta(3\tau)} = \prod_{n\geq 1} \frac{(1-q^n)^3}{(1-q^{3n})} \in M_1(9, \chi_{-3}). \tag{6.14}$$

First we note that $\frac{(1-q^n)^3}{1-q^{3n}} \equiv 1 \pmod 3$, so that $g \equiv 1 \pmod 3$. Thus, if we construct a modular form ϕ_k as $\phi_k(\tau) = f(\tau)g^k(\tau)$, then $\phi_k \equiv f \pmod 3$ and, $\phi_k \in S_{\frac{2k+3}{2}}(252, \chi_3^k)$. Thus writing the Fourier expansion of ϕ_k as

$$\phi_k(\tau) = \sum_{n\geq 1} a_n(\phi_k) q^n, \tag{6.15}$$

we have $a_n(\phi_k) \equiv a_n(f)$ modulo 3. Thus, from Theorem 6.1.7, we know that there exists a subset S of the square-free natural numbers having lower density 7/64 such that $a_n(\phi_k) \neq 0$ for all $n \in S$.

Next we write $\phi_k = \sum_{i=1}^{L} \alpha_i f_i$, where each of the f_i's is in $S_{\frac{2k+3}{2}}(252, \chi_3^k)$ and is an eigenform for all of the Hecke operators T_p with $p \neq 2, 3$ or 7. Let $F_i \in S_{2k+2}(126)$ denote a Shimura lift of f_i for $i = 1, \ldots, L$. Then it is not hard to check from the definition of the Hecke operators and the definition of the Shimura lift (see Chapter

3) that each F_i is also an eigenform for all of the Hecke operators T_p with $p \neq 2, 3$ or 7, and for such p, $\lambda_p(F_i) = \lambda_p(f_i)$. From the main theorem in [1], we can then deduce that there are weight $2k+2$ newforms G_i of trivial character and of level some divisor of 126 with $\lambda_p(G_i) = \lambda_p(f_i)$.

Define a primitive Dirichlet character $\mu : (\mathbb{Z}/32\mathbb{Z})^\times \to \mathbb{C}$ of order 8 by setting $\mu(3) = \mu(5) = e^{\frac{\pi i}{4}}$. Note that μ^2 is an order 4 Dirichlet character modulo 16, and that $\mu^4(n) = (\frac{2}{n})$.

We note that $G_i \cdot \mu^2$ is an eigenform for all of the Hecke operators T_p with $p \neq 2, 3$ or 7 having $\lambda_p(G_i \cdot \mu^2) = \mu^2(p)\lambda_p(G_i) = \lambda_p((f_i)_\mu)$. Also, $(f_i)_\mu \in S_{\frac{2k+3}{2}}(252 \cdot 16^2, \chi_3^k \mu^2)$. Hence the character ν from Theorem 3.7.2 is given by

$$\nu = \begin{cases} \chi_3 \mu^2, & \text{if } k \text{ is odd} \\ \chi_{-1} \mu^2, & \text{if } k \text{ is even.} \end{cases} \tag{6.16}$$

In either case, the conductor of ν is divisible by 4. Thus each of the $G_i \cdot \mu^2$ satisfies the hypotheses of Theorem 3.7.2. Thus, by part 1 of Theorem 3.7.2, there exist functions $\mathbb{A}_i : \mathbb{N}^{sf} \to \mathbb{C}$, where $\mathbb{N}^{sf}$ denotes the square-free natural numbers, such that

$$(\mathbb{A}_i(D))^2 = L(G_i \cdot \psi_k \chi_D, k+1) \cdot \epsilon(\psi_k \chi_D, 1/2), \tag{6.17}$$

where

$$\psi_k = \begin{cases} \chi_3, & \text{if } k \text{ is odd} \\ \chi_{-1}, & \text{if } k \text{ is even.} \end{cases} \tag{6.18}$$

By part 2 of Theorem 3.7.2, we can write $(f_i)_\mu = \sum_{j=1}^{M} \beta_j f_{i,j}$, where $a_n(f_{i,j})$ is some multiple of $\mathbb{A}_i(n)$. Thus, for any odd square-free n if $a_n(f_i) \neq 0$, then $\mathbb{A}_i(n) \neq 0$ and therefore $L(G_i \cdot \psi_k \chi_n, k+1) \neq 0$.

We saw above that if $n \in S$, then $a_n(\phi_k) \neq 0$, which implies that for some $1 \leq i \leq L$, we have $a_n(f_i) \neq 0$ and therefore $L(G_i \cdot \psi_k \chi_n, k+1) \neq 0$, which also implies that $L((G_i)_{\psi_k \chi_n}, k+1) \neq 0$. In Lemma 6.1.10 below we show that there exist $\gamma_1, \ldots, \gamma_L \in \mathbb{C}$ such that if we put $\Phi = \sum_{i=1}^{L} \gamma_i G_i$ then we will have $L(\Phi_{\psi_k \chi_n}, k+1) = \sum_{i=1}^{L} \gamma_i L((G_i)_{\psi_k \chi_n}, k+1) \neq 0$ for all $n \in S$. Thus replacing Φ by Φ_{ψ_k}, we will have proved

THEOREM 6.1.11. *Suppose that k is a positive integer. Then there exists a cusp form $\Phi \in S_{2k}(126 \cdot C)$ with the property that $L(\Phi_{\chi_n}, k) \neq 0$ for all $n \in S$, where S is the same set of lower density at least $7/64$ as in Theorem 6.1.8and C is 1 (resp. 9) when k is even (resp. odd).*

Now it remains to prove:

LEMMA 6.1.10. *Suppose that for each $1 \leq i \leq N$ we have a sequence $\{s_i(n)\}_{n \in \mathbb{N}}$ of complex numbers with the property that for each $n \in \mathbb{N}$ at least one of the $s_i(n)$'s is non-zero. Then there exists $\gamma_1, \ldots, \gamma_N \in \mathbb{C}$ such that $\sum_{i=1}^{N} \gamma_i s_i(n) \neq 0$ for all $n \in \mathbb{N}$.*

PROOF. For any $n \in \mathbb{N}$ there is at least one i such that $s_i(n) \neq 0$. Thus, $\sum_{i=1}^{N} s_i(n) x_i = 0$ is the equation of an $(N-1)$-dimensional hyperplane A_n in $\mathbb{C}^N$. Letting A denote the union of all of the A_n's, we have that A is a measure zero subset of $\mathbb{C}^N$. Thus, the complement of A is non-empty. Now, we can choose any $\gamma_1, \ldots, \gamma_N$ where $(\gamma_1, \ldots, \gamma_N) \notin A$.

REMARK. Actually, this proof shows that Theorem 6.1.11holds for "almost all" cusp forms in $S_{2k}(126 \cdot C)$. The techniques used in the proof of Theorem 2 will work for several other curves as well (see section 2 of this chapter). We hope to generalize Theorem 2 to include large families of curves. Then, applying the same techniques as in the proof of Theorem 4, we will be able to show the existence of many cusp spaces of arbitrary even weight in which almost all cusp forms F will have the property that for a positive proportion of the square-free natural numbers n, $L(F_{\chi_n}, 1) \neq 0$.

6.2 More Positive Density Nonvanishing Results

In this section we will first summarize the techniques of section 1 into one proposition (Proposition 6.2.1). Then, we will show nine more examples of weight 2 newforms f for which we can prove, using Proposition 6.2.1, that $L(f_{\chi_D}, 1) \neq 0$ for a positive proportion of the square-free numbers D.

PROPOSITION 6.2.1. *Suppose that Q_1 and Q_2 are the only ternary quadratic forms in a genus of forms. Let A_i denote the number of automorphs of Q_i $(i = 1, 2)$. Assume that $3 \nmid A_1A_2$ but $3 \mid A_1 + A_2$. Suppose also that $f = (\theta_{Q_1} - \theta_{Q_2}) \in S_{3/2}(N_{Q_1}, \chi_{d_{Q_1}})$ is a Hecke-eigenform which lifts through the Shimura correspondence to a cusp form $F \in S_2(N_{Q_1}/2)$. Then F is also a Hecke-eigenform, and hence there is a unique weight 2 newform G of trivial character having $\lambda_p(F) = \lambda_p(G)$ for all but finitely many of the primes p. Letting N_G denote the level of G, we put*

$$\begin{aligned} W &= \operatorname{lcm}[\prod_{\substack{p,\ \text{odd} \\ p \mid N_G}} p, \prod_{\substack{p,\ \text{odd} \\ p \mid d_{Q_1}}} p], \\ R &= \left\{ a \in (\mathbb{Z}/8W\mathbb{Z})^* : \exists \quad \text{a square-free } n \equiv a \pmod{8W} \text{ with } 3 \nmid a_n(f) \right\} \qquad \text{and,} \\ \delta &= \frac{\#R}{12W \prod_{p \mid W}(1 - \frac{1}{p^2})}. \end{aligned} \tag{6.19}$$

Then, the set of square-free natural numbers n such that $L(G \cdot \chi_{-d_{Q_1}n}, 1) \neq 0$ has lower density at least δ in the square-free natural numbers.

We note that the character $\chi_{d_{Q_1}}$ is by definition the same as $\chi_{d_{Q_1}^{sf}}$ where a^{sf} denotes the square-free part of a. We omitted the square-free notation in the statement of Proposition 6.2.1 simply to ease notation. In the examples that follow the proof of Proposition 6.2.1, we will only write the square-free part of d_{Q_1}.

PROOF. Suppose that $a \in R$. Then there exists $n \equiv a$ modulo $8W$ such that $3 \nmid a_n(f)$, and hence $a_n(f) \neq 0$. By Waldspurger's main theorem (Theorem 3.7.2), we know that $L(G \cdot \chi_{-q_{Q_1}n}, 1) \neq 0$. Thus, putting

$$\beta_a = \frac{L(G \cdot \chi_{-d_{Q_1}n}, 1)\sqrt{n}}{a_n(f)^2}, \tag{6.20}$$

Theorem 3.7.3 gives us for all square-free $m \equiv a$ modulo $8W$,

$$L(G \cdot \chi_{-d_{Q_1}m}, 1) = \frac{a_m(f)}{\sqrt{m}}\beta_a. \tag{6.21}$$

Thus, for $m \equiv a$ modulo $8W$, we have that $L(G \cdot \chi_{-d_{Q_1}m}, 1) = 0$ if and only if $a_m(f) = 0$.

Now we note that since $a_n(f) \neq 0$, it follows from our choice of W and Theorem 4.2.1 that for all $m \equiv a$ modulo $8W$, $R(Q_1, m) \neq 0$. Thus, combining Gauss' theorem (Theorem 4.2.4) with Theorem 4.2.5, we have that for all $m \equiv a$ modulo $8W$,

$$R(Q_1, m) = \rho h(\Delta_m), \tag{6.22}$$

where Δ_m denotes the discriminant of $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, and ρ depends only on the congruence class of a modulo $8W$. Since $3 \nmid A_1A_2$ and $3 \mid (A_1 + A_2)$, we have that $A_1A_2R(Q_1, m) = A_2r_1(m) + A_1r_2(m) \equiv A_2(r_1(m) - r_2(m))$ modulo 3. From our construction of f, we have that $a_m(f) = r_1(m) - r_2(m)$. Therefore, $3 \mid a_m(f)$ if and only if $3 \mid \rho h(\Delta_m)$. Recall that $3 \nmid a_n(f)$ and $n \equiv a$ modulo $8W$. Thus, $3 \nmid \rho h(\Delta_n)$. Since $h(\Delta_n) \in \mathbb{N}$, it follows that $\mathrm{ord}_3(\rho) \leq 0$. Also, by the Davenport-Heilbronn theorem (Theorem 6.1.5), we have for at least half of the square-free natural numbers $m \equiv a$ modulo $8W$, that $3 \nmid h(\Delta_m)$. Since $\rho h(\Delta_m) = R(Q_1, m) \in \mathbb{N}$, we have that $\mathrm{ord}_3(\rho) = 0$ and hence $3 \mid a_m(f)$ if and only if $3 \mid h(\Delta_m)$. Now, applying Theorem 6.1.5 again, we see for each $a \in R$, that for at least $1/2$ of the square-free $m \equiv a$ modulo $8W$, $L(G \cdot \chi_{-d_{Q_1}m}, 1) \neq 0$. We note that each $a \in R$ gives rise to W arithmetic progressions modulo $8W^2$, and that the total number of arithmetic progressions modulo $8W^2$ in which square-free numbers reside is $8W^2(1 - \frac{1}{4}) \prod_{p|W}(1 - \frac{1}{p^2})$. Thus the density of square-free natural numbers m which are congruent modulo $8W$ to some $a \in R$ is $\frac{\#R \cdot W}{6W^2 \prod_{p|W}(1 - \frac{1}{p^2})}$. The proposition now follows from Theorem 6.1.5.

We now compute several examples. We begin with forms Q_1 and Q_2 with automorphs A_1 and A_2 respectively, where both have discriminant Δ, level N and character χ_Δ. Let q denote the square-free part of Δ. We use Theorem 4.1.5 to check that Q_1 and Q_2 are the only forms in the genus of ternary forms

containing them. It then follows from Theorem 4.1.1 and Theorem 4.1.4, that $f(\tau) = (\Theta_{Q_1}(\tau) - \Theta_{Q_2}(\tau)) \in S_{3/2}(N, \chi_q)$. In each of the examples which we computed it was the case that there were no modular forms of type $\theta_{\psi,t}$ in $S_{3/2}(N, \chi_q)$. Thus, we could use Theorem 3.8.6 to check computationally that f was a Hecke-eigenform. Also, using Theorem 3.8.1, we checked that f lifted through the Shimura lift to an integer multiple of a normalized weight 2 newform H. In particular, $\lambda_p(f) = \lambda_p(H)$ for all primes $p \nmid N$. Thus in each example, f satisfied the conditions of Proposition 6.2.1 with H taking the role of the newform G. Now let $F = H \cdot \chi_{-q}$. By the theory of Eichler and Shimura, we know that there is an elliptic curve F such that $L(E, s) = L(F, s)$. In our examples the level of F was always less than 1000. So, we were able to determine E simply by consulting the tables of Cremona [11]. It was then a simple matter to calculate W. Also, we were able to determine R by computing the first few hundred Fourier coefficients of f and thus determine δ. So, Proposition 6.2.1, yields the following result.

THEOREM 6.2.2. *There is a subset S of the square-free natural numbers having lower density at least δ such that $L(F_{\chi_D}, 1) \neq 0$ for all $D \in S$.*

Applying Theorem 2.6.4, we have,

COROLLARY 6.2.3. *For at least δ of the square-free natural numbers n, the elliptic curve E_n has rank 0.*

Examples

1.
$$Q_1(x, y, z) = x^2 + y^2 + 18z^2,$$
$$Q_2(x, y, z) = 2x^2 + 2y^2 + 5z^2 - 2xz,$$
$$A_1 = 8, \quad A_2 = 4.$$
$$\Delta = 72, \quad N = 72, \quad q = 2,$$
$$E : y^2 = x^3 - 8 \text{ and}$$
$$\delta = 1/4.$$

2.

$$Q_1(x,y,z) = x^2 + 4y^2 + 10z^2 - 4yz,$$
$$Q_2(x,y,z) = 2x^2 + 2y^2 + 9z^2,$$
$$A_1 = 8, \quad A_2 = 4,$$
$$\Delta = 144, \quad N = 72, \quad q = 1,$$
$$E : y^2 = x^3 - 1 \text{ and}$$
$$\delta = 5/24.$$

3.

$$Q_1(x,y,z) = 4x^2 + 19y^2 + 20z^2 - 4xz,$$
$$Q_2(x,y,z) = 7x^2 + 11y^2 + 23z^2 - 10yz - 6xz - 2xy,$$
$$A_1 = 4, \quad A_2 = 2,$$
$$\Delta = 5776, \quad N = 76, \quad q = 1,$$
$$E : y^2 = x^3 - 4x^2 - 144x + 944 \text{ and}$$
$$\delta = 19/240.$$

4.

$$Q_1(x,y,z) = x^2 + 10y^2 + 10z^2,$$
$$Q_2(x,y,z) = 4x^2 + 5y^2 + 6z^2 - 4xz,$$
$$A_1 = 8, \quad A_2 = 4,$$
$$\Delta = 400, \quad N = 40, \quad q = 1,$$
$$E : y^2 = x^3 - x^2 + 4x - 4 \text{ and}$$
$$\delta = 5/72.$$

5.

$$Q_1(x,y,z) = 2x^2 + 7y^2 + 13z^2 - 2xy,$$

$$Q_2(x,y,z) = 5x^2 + 6y^2 + 8z^2 + 6yz + 2xz + 4xy,$$

$$A_1 = 4, \quad A_2 = 2,$$

$$\Delta = 676, \quad N = 52, \quad q = 1,$$

$E : y^2 = x^3 - x^2 - 72x + 496$ and

$\delta = 13/112.$

6.

$$Q_1(x,y,z) = x^2 + 15y^2 + 15z^2,$$

$$Q_2(x,y,z) = 4x^2 + 4y^2 + 15z^2 - 2xy,$$

$$A_1 = 8, \quad A_2 = 4,$$

$$\Delta = 900, \quad N = 60, \quad q = 1,$$

$E : y^2 = x^3 - x^2 + 24x - 144n^3$ and

$\delta = 5/128.$

7.

$$Q_1(x,y,z) = x^2 + 17y^2 + 17z^2,$$

$$Q_2(x,y,z) = 2x^2 + 9y^2 + 17z^2 - 2xy,$$

$$A_1 = 8, \quad A_2 = 4,$$

$$\Delta = 1156, \quad N = 68, \quad q = 1,$$

$E : y^2 = x^3 - x^2 - 48x - 64$ and

$\delta = 17/144.$

8.
$$Q_1(x,y,z) = 2x^2 + 11y^2 + 22z^2,$$
$$Q_2(x,y,z) = 6x^2 + 8y^2 + 11z^2 - 4xy,$$
$$A_1 = 4, \quad A_2 = 2,$$
$$\Delta = 1936, \quad N = 88, \quad q = 1,$$
$$E : y^2 = x^3 - x^2 + 3x + 1 \text{ and}$$
$$\delta = 11/144.$$

9. In this example we use 4 ternary quadratic forms. We simply apply the process described above twice and combine the results.

$$Q_1(x,y,z) = 2x^2 + 3y^2 + 25z^2 - 2xy,$$
$$Q_2(x,y,z) = 3x^2 + 7y^2 + 7z^2 + 4yz + 2xz + 2xy,$$
$$Q_3(x,y,z) = x^2 + 10y^2 + 15z^2 - 10yz,$$
$$Q_4(x,y,z) = 4x^2 + 4y^2 + 9z^2 - 2yz - 2xz - 2xy,$$
$$A_1 = 4, \quad A_2 = 2, \quad A_3 = 4, \quad A_4 = 2,$$
$$\Delta = 500, \quad N = 100, \quad q = 5,$$
$$E : y^2 = x^3 - 5x^2 - 200x + 14000 \text{ and}$$
$$\delta = 5/24.$$

Chapter 7

Birch and Swinnerton-Dyer Type Results

In this chapter, we consider part 2 of the Birch and Swinnerton-Dyer Conjecture (Conjecture 2.6.2) modulo 3 for certain rank zero elliptic curves. More precisely, we consider the following congruence which is a weak form of the Birch and Swinnerton-Dyer conjecture.

Conjecture 7.1. *Let E be a rank zero elliptic curve. Then*

$$\frac{L(E,1)}{\Omega_E}\#E(\mathbb{Q})^2_{\text{tor}} \equiv \#Ш(E/\mathbb{Q})\prod_p c_p(E/\mathbb{Q}) \pmod 3, \tag{7.1}$$

where $L(E,s)$, Ω_E, $Ш(E/\mathbb{Q})$ and $c_p(E/\mathbb{Q})$ denote the L-series, real period, Tate-Shafarevic group and local Tamagawa factors of E respectively.

We will use a theorem due to Frey [16] along with some of the techniques in Chapter 6 to prove for certain elliptic curves E that for a positive proportion of the square-free integers d,

$$\text{ord}_3\left(\frac{L(E_d,1)}{\Omega_{E_d}}\right)=0 \quad \Longleftrightarrow \quad \text{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q})\prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\text{tor}}}\right)=0. \tag{7.2}$$

We note that we can use Tate's algorithm [49] to calculate the $c_p(E_d/\mathbb{Q})$'s. In the examples we consider here, Tate's algorithm shows that if we let $W=\prod_{\substack{p|N_E\\ p\neq 2,3}} p$, then there exist $a \in (Z/24W\mathbb{Z})^*$ such that $3 \nmid \prod_p c_p(E_d/\mathbb{Q})$ for all $d \equiv a$ modulo $24W$.

We also have the following lemma concerning $\#E_d(\mathbb{Q})_{\text{tor}}$.

LEMMA 7.2. *Let E be an elliptic curve defined over $\mathbb{Q}$. There are at most 2 square-free integers d such that $3 \mid E_d(\mathbb{Q})_{\text{tor}}$. Further, if E_{d_1} and E_{d_2} both have a 3-torsion point, then $d_2 = -3d_1$.*

PROOF. We will let C denote the conductor of $\chi_{[d_1,d_2]}$, where $[m,n]$ denotes the least common multiple of m and n. Suppose that E_{d_1} and E_{d_2} both have a point of order 3, where $d_1 \neq d_2$ and where d_1 and d_2 are both square-free. Then we have that for all primes $p \nmid d_1 d_2 \Delta_E$, $3 \mid \#E_{d_1}(\mathbb{F}_p)$ and $3 \mid \#E_{d_2}(\mathbb{F}_p)$ (see [47], Proposition VII.3.1). Also, we note that

$$\#E_{d_2}(\mathbb{F}_p) = (p+1)(1 - \chi_{[d_1,d_2]}(p)) + \chi_{[d_1,d_2]}(p)\#E_{d_1}(\mathbb{F}_p). \tag{7.3}$$

Thus, by (7.3) we obtain $3 \mid (p+1)(1-\chi_{[d_1,d_2]}(p))$ whenever $p \nmid d_1 d_2 \Delta_E$. If additionally $p \equiv 1$ modulo 3, then we deduce $\chi_{[d_1,d_2]}(p) = 1$. Suppose now that $3 \nmid C$. Since $d_1 \neq d_2$, $\chi_{[d_1,d_2]}$ is not trivial. Thus, there is an a coprime to C such that if $n \equiv a$ modulo C, then $\chi_{[d_1,d_2]}(n) = -1$. Now we can use the Chinese remainder theorem to find an a' such that $a' \equiv a$ modulo C and $a' \equiv 1$ modulo 3. By Dirichlet's theorem on primes in an arithmetic progression, we then see that there are infinitely many primes $p \equiv a'$ modulo $3C$. Now, if $p \equiv a'$ modulo $3C$, then $p \equiv a$ modulo C and hence, $\chi_{[d_1,d_2]}(p) = -1$. On the other hand, for such $p \nmid \Delta_E$, we have that $p \equiv 1$ modulo 3 and we have already seen that this implies that $\chi_{[d_1,d_2]}(p) = 1$ contradicting our last statement. Thus, we deduce that $3 \mid C$ and hence, that $3 \mid [d_1,d_2]$. Now write $[d_1,d_2] = 3b$. Then we have for primes $p \nmid d_1 d_2 \Delta_E$

$$\chi_{[d_1,d_2]}(p) = \chi_3(p)\chi_b(p) = \begin{cases} \chi_b(p), & \text{if } p \equiv 1 \pmod{12} \\ -\chi_b(p), & \text{if } p \equiv 7 \pmod{12}, \end{cases} \tag{7.4}$$

and therefore

$$\chi_b(p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{12} \\ -1, & \text{if } p \equiv 7 \pmod{12}, \end{cases} \tag{7.5}$$

Let C' denote the conductor of χ_b. Since $[d_1,d_2]$ is square-free, it follows that $3 \nmid b$ and therefore, $3 \nmid C'$. Since $\chi_b(n)$ is completely determined by the congruence class

of n modulo C', and since $3 \nmid C'$, it follows from (7.5) that for primes $p \nmid d_1 d_2 \Delta_E$

$$\chi_b(p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{7.6}$$

Thus, we see that C' must be 4 and that $c = -1$. This proves the lemma.

The Theorem of Frey discussed in the next section will allow us to relate the 3-divisibility of $Ш(E_d/\mathbb{Q})$ to the 3 divisibility of $h(\mathbb{Q}(\sqrt{-d}))$. Then using the techniques from Chapter 6 we will be able to establish (7.2) for certain elliptic curves.

7.1 A Theorem of Frey.

In this section, we discuss a theorem of Frey [16] which relates the subgroups of elements of order p in the Selmer groups of twists of an elliptic curve to the subgroups of elements of order p of certain class groups where $p = 3, 5$ or 7. First, we need to introduce some notation.

Let E be an elliptic curve over $\mathbb{Q}$ with minimal Weierstrauss equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. We define the quantities c_4, c_6 and j_E as in (2.3), and make the following definition.

DEFINITION 7.1.1. *Let E be an elliptic curve over $\mathbb{Q}$ with $ord_p(j_E) < 0$ and let q be an odd prime not dividing N_E. Then we define $\gamma_q(E) = \left(\frac{-c_4 c_6^{-1}}{q}\right)$, where c_6^{-1} denotes the inverse of c_6 modulo q.*

Now we are ready to state Frey's Theorem. Actually, we will only state a weak version of the Corollary to the main Theorem in [16].

THEOREM 7.1.2. *Let E be an elliptic curve over $\mathbb{Q}$ with a rational point P of odd prime order p. Assume also that either E is given by $y^2 = x^3 + 1$ or that P is not in the kernel of the reduction modulo p map. Further, suppose that for all odd primes $q \mid N_E$, we have that if $q \equiv -1$ modulo p, then $\mathrm{ord}_q(\Delta_E) \equiv 0$ modulo p. Let d be a square-free natural number prime to pN_E such that*

1. *If $2 \mid N_E$ then $d \equiv 1$ modulo 4.*

2. *If* $q \neq 2$ *or* p *but* $q \mid N_E$*, then*

$$\left(\frac{-d}{q}\right) = \begin{cases} -1, & \text{if } \mathrm{ord}_q(j_E) \geq 0 \\ -1, & \text{if } \mathrm{ord}_q(j_E) < 0 \text{ and } \gamma_q(E) = 1 \\ 1, & \text{otherwise.} \end{cases} \tag{7.7}$$

3. *If* $\mathrm{ord}_p(j_E) < 0$ *then* $\left(\frac{-d}{p}\right) = -1$.

Finally let Δ_d *denote the discriminant of* $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$*. Then,*

$$h(\Delta_d)_p \quad | \quad \#S(E_{-d}/\mathbb{Q})_p \quad | \quad (h(\Delta_d)_p)^2, \tag{7.8}$$

where $h(\Delta)_p$ *denotes the order of the subgroup of elements of order* p *in the ideal class group for the ring of integers of* $\mathbb{Q}(\sqrt{-d})$*, and* $S(E/\mathbb{Q})_p$ *denotes the subgroup of elements of order* p *in the Selmer group of* E*.*

The Selmer and Tate-Shafarevic groups of an elliptic curve are difficult to explicitly define. The reader is referred to [47 pages 296–306] for a discussion of these groups. We simply note that the Selmer group $S(E/\mathbb{Q})$ of E and the Tate-Shafarevic group $Ш(E/\mathbb{Q})$ of E are related by the following short exact sequence which holds for any prime p.

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to S(E/\mathbb{Q})_p \to Ш(E/\mathbb{Q})_p \to 0. \tag{7.9}$$

In particular, we see that if $E_{-d}(\mathbb{Q})$ has rank zero and has no p-torsion then it follows from (7.9) that $S(E_{-d}/\mathbb{Q})_p \cong Ш(E_{-d}/\mathbb{Q})_p$. This last observation will allow us to gain information about $Ш(E_{-d}/\mathbb{Q})$ via Theorem 7.1.2.

7.2 Results.

In this section, we will combine Frey's Theorem (Theorem 7.1.2) with Proposition 6.2.1 to establish (7.2) for certain elliptic curves over $\mathbb{Q}$ (see Proposition 7.2.1). We will also give four examples of such curves.

Before stating the proposition we note that for any square-free natural number d coprime to $6N_E$, $\Omega_{E_{-d}} = \frac{m\Omega_{E_{-1}}}{\sqrt{d}}$, where $m \in \mathbb{N}$. If we have a minimal equation for

E_{-1} and we twist it by a square-free natural number d coprime to $6N_E$, then the new equation may no longer be minimal at 2 and 3. The integer m just accounts for any change of variables which may be necessary in order to make this new equation for E_{-d} minimal. In fact m can be calculated as follows. For $p = 2, 3$, we put $m_p = \mathrm{ord}_p(\Delta_{E_{-1}}) - \mathrm{ord}_p(\Delta_{E_{-d}})$. Then, $m = 2^{m_2/12}3^{m_3/12}$.

PROPOSITION 7.2.1. *Suppose that $f \in S_{3/2}(N)$ and $G \in S_2(M)$ are as in Proposition 6.2.1. Let E be the modular elliptic curve with $L(E, s) = L(G, s)$, and suppose that E satisfies the hypotheses of Theorem 7.1.2 with $p = 3$. Also, define*

$$W = \mathrm{lcm}\left[\prod_{\substack{p|M \\ p\neq 2,3}} p, \prod_{\substack{p|N \\ p\neq 2,3}} p\right]. \tag{7.10}$$

Let R be the set of all $a \in (\mathbb{Z}/24W\mathbb{Z})^*$ satisfying the following conditions:

1. *There exists a square-free natural number $n \equiv a$ modulo $24W$ such that $3 \nmid a_n(f)$ and such that $\mathrm{ord}_3\left(\frac{L(E_{-n},1)}{\Omega_{E_{-n}}}\right) = 0$.*
2. *For all square-free natural numbers $d \equiv a$ modulo $24W$, $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$*
3. *There exists an integer m depending only on a such that for all square-free natural numbers $d \equiv a$ modulo $24W$, $\Omega_{E_{-d}}\sqrt{d}/\Omega_{E_{-1}} = m$.*
4. *If $2 \mid N_E$ then $a \equiv 1$ modulo 4.*
5. *If $\ell \neq 2, 3$ is prime and $\ell \mid N_E$, then*

$$\left(\frac{-a}{\ell}\right) = \begin{cases} -1, & \text{if } \mathrm{ord}_\ell(j_E) \geq 0 \\ -1, & \text{if } \mathrm{ord}_\ell(j_E) < 0 \text{ and } \gamma_\ell(E) = 1 \\ 1, & \text{otherwise.} \end{cases} \tag{7.11}$$

6. *If $\mathrm{ord}_3(j_E) < 0$ then $a \equiv 1$ modulo 3.*

Put

$$\delta = \frac{\#R}{32W\prod_{p|W}(1 - \frac{1}{p^2})} \tag{7.12}$$

Then there exists a subset S of the square-free natural numbers having lower density at least δ such that for all $d \in S$ we have

$$\mathrm{ord}_3\left(\frac{L(E_d, 1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q})\prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \tag{7.13}$$

PROOF. Suppose that $a \in R$. Then there exists $n \equiv a$ modulo $24W$ such that $3 \nmid a_n(f)$, and hence $a_n(f) \neq 0$. By Waldspurger's main theorem (Theorem 3.7.2), we know that $L(G \cdot \chi_{-n}, 1) \neq 0$. Thus, putting

$$\beta_a = \frac{L(G \cdot \chi_{-n}, 1)\sqrt{n}}{a_n(f)^2}, \tag{7.14}$$

Theorem 3.7.3 gives us for all square-free $d \equiv a$ modulo $24W$,

$$L(G \cdot \chi_{-d}, 1) = \frac{a_d(f)^2}{\sqrt{d}}\beta_a. \tag{7.15}$$

Dividing through (7.15) by $\Omega_{E_{-1}}$ and using condition 3 above we have for all square-free natural numbers $d \equiv a$ modulo $24W$:

$$\frac{L(E_{-d}, 1)}{\Omega_{E_{-d}}} = a_d(f)^2\alpha_a, \tag{7.16}$$

where

$$\alpha_a = \frac{L(E_{-n}, 1)}{\Omega_{E_{-n}} a_n(f)^2}. \tag{7.17}$$

From condition 1 we have that $\mathrm{ord}_3(\alpha_a) = 0$. Thus, $\mathrm{ord}_3(L(E_{-d}, 1)/\Omega_{E_{-d}}) = 0$ if and only if $3 \nmid a_d(f)$.

Arguing as in the proof of Proposition 6.2.1, we can show that for all square-free $d \equiv a$ modulo $24W$, $3 \mid a_d(f)$ if and only if $3 \mid h(\Delta_d)$. Thus, we have for all square-free natural numbers $d \equiv a$ modulo $24W$,

$$\mathrm{ord}_3\left(\frac{L(E_{-d}}{\Omega_{E_{-d}}}\right) = 0 \quad \iff \quad 3 \nmid h(\Delta_d). \tag{7.18}$$

Let S be the set of all square-free natural numbers d such that $d \equiv a$ modulo $24W$ for some $a \in R$ and such that $a_d(f) \neq 0$. We note that by the Davenport-Heilbronn theorem (Theorem 6.1.5), we know that for any $a \in R$, at least half of the square free natural numbers $d \equiv a$ modulo $24W$ have the property that $3 \nmid h(\Delta_d)$. For such d it follows that $3 \nmid a_d(f)$. Thus for each $a \in R$ at least half of the square-free natural numbers $d \equiv a$ modulo $24W$ are in S. So, an argument analogous to the

one given in the proof of Proposition 6.2.1 will yield that S has lower density at least δ in the set of all square-free natural numbers. Also, by Lemma 7.2, we can remove from S any d for which $E_{-d}(\mathbb{Q})$ has points or order 3 without affecting the density of S. Hence, we will assume for the remainder of the proof that S contains no such d.

Now, we note that for any $d \in S$, we have that $a_d(f) \neq 0$ and therefore by (7.15) it follows that $L(E_{-d}, 1) \neq 0$. Thus, by Theorem 2.6.4, we know that E_{-d} has rank 0. Therefore, for all $d \in S$ we have that E_{-d} has rank 0 and that $3 \nmid E_{-d}(\mathbb{Q})_{\text{tor}}$. Hence, it follows from (7.9) that $Ш(E_{-d}/\mathbb{Q})_3 \cong S(E_{-d}/\mathbb{Q})$ for all $d \in S$. Since we are assuming that E satisfies the hypotheses of Theorem 7.1.2, and since the conditions 4, 5 and 6 imposed on d are the same as the conditions imposed on d in Theorem 7.1.2, it follows that for all $d \in S$,

$$h(\Delta_d)_3 \quad | \quad \#Ш(E_{-d}/\mathbb{Q})_3 \quad | \quad (h(\Delta_d)_3)^2, \tag{7.19}$$

Thus for all $d \in S$ we have

$$3 \mid Ш(E_{-d}/\mathbb{Q}) \quad \Longleftrightarrow \quad 3 \mid h(\Delta_d). \tag{7.20}$$

Now, the proposition follows from (7.18), (7.20) condition 2 and our assumption that for all $d \in S$, $3 \nmid E_{-d}(\mathbb{Q})_{\text{tor}}$.

Example 7.2.1 Let $E : y^2 = x^3 + 1$ be the modular elliptic curve of conductor 36 and let

$$f = \frac{1}{2} \sum_{x,y,z \in \mathbb{Z}} (q^{x^2+4y^2+10z^2-4yz} - q^{2x^2+2y^2+9z^2}). \tag{7.21}$$

Let $G \in S_2(36)$ denote the newform with $L(G, s) = L(E, s)$. We recall from Example 6.2.2 that f and G satisfy the hypotheses of Proposition 6.2.1. Since $E : y^2 = x^3 + 1$ and since the only odd prime dividing N_E is 3, we see that E satisfies the hypotheses of Theorem 7.1.2. Thus, we can apply Proposition 7.2.1.

In this case, we have $W = 1$. We will let $R_0 \subset (\mathbb{Z}/24\mathbb{Z})^*$ be the set $R_0 = \{1, 5, 13, 17\}$.

We can verify that each $a \in R_0$ satisfies condition 1, by simply calculating the first 20 coefficients of f and using the APECS package with MAPLE to compute the values of $L(E_{-n},1)/\Omega_{E_{-n}}$. Next, we use Tate's Algorithm to check that for each $a \in R_0$ and for all square-free natural numbers $d \equiv a$ modulo 312, we have $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$. Thus, all of the $a \in R_0$ satisfy condition 2. Also, using Tate's Algorithm, we can verify that for all square-free natural numbers d coprime to 12, we have $\Omega E_{-d}\sqrt{d}/\Omega E_{-1} = 1$. Thus, condition 3 is satisfied by each $a \in R_0$. Since for each $a \in R_0$, $a \equiv 1$ modulo 4, condition 4 is also satisfied. In this case, condition 5 is vacuous. Since, $j_E = 0$, condition 6 is vacuous. Thus we can take $R = R_0$ and we calculate $\delta = 1/8$. Thus by Proposition 7.2.1, we have proved:

THEOREM 7.2.2. *Let $E : y^2 = x^3 + 1$. Then there is a set $S \subset \mathbb{N}$ having lower density 1/8 in the square-free natural numbers such that for all $d \in S$*

$$\mathrm{ord}_3\left(\frac{L(E_d,1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q})\prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \quad (7.22)$$

Example 7.2.2 Let, $E : y^2 = x^3 + x^2 + 72x - 368$ be the modular curve of conductor 14. Actually, E is the twist by -1 of the elliptic curve considered in section 6.1. Let

$$f = \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} (q^{x^2+7y^2+7z^2} - q^{2x^2+4y^2+7z^2-2xy}) \in S_{3/2}(28). \quad (7.23)$$

Let $G \in S_2(14)$ denote the newform with $L(G,s) = L(E,s)$. We recall from section 6.1 that f and G satisfy the hypotheses of Proposition 6.2.1. Also, $P = (2,2) \in E(\mathbb{Q})$ has order 3 and is not in the kernel of the reduction modulo 3 map. Further, we note that the only odd prime dividing N_E is 7 which is 1 modulo 3. Thus, E satisfies the hypotheses of Theorem 7.1.2.

In this case, we have $W = 7$ (and therefore 24W=168). We will let $R_0 \subset (\mathbb{Z}/168\mathbb{Z})^*$ be the set $R_0 = \{1, 25, 29, 37, 53, 65, 85, 109, 113, 121, 137, 149\}$

By calculating the first 500 coefficients of f and using the APECS package with MAPLE to calculate $L(E_{-n},1)/\Omega_{E_{-n}}$, we were able to verify condition 1 for each

$a \in R_0$. We can use Tate's Algorithm to calculate that for $d \equiv 1$ modulo 4, $c_2(E_{-d}/\mathbb{Q})$ is either 2 or 4. Similarly, we can check that for $d \equiv 1$, 2, or 4 modulo 7, $c_7(E_{-d}/\mathbb{Q}) = 1$. For any other prime p not dividing d, we have $c_p = 1$. For primes $p \mid d$ ($p \neq 2, 7$), Tate's Algorithm yields that $c_p(E_{-d}/\mathbb{Q})$ is 1, 2 or 4. Thus, all of the $a \in R_0$ satisfy condition 2 of Proposition 7.2.1. Also, using Tate's Algorithm, we can verify that for all square-free natural numbers $d \equiv 1$ modulo 4 with $(d, 42) = 1$, we have $\Omega E_{-d}\sqrt{d}/\Omega E_{-1} = 1$. Thus, condition 3 is satisfied by each $a \in R_0$. Since for all $a \in R_0$, we have $a \equiv 1$ modulo 4, condition 4 is satisfied. Now, we note that $\mathrm{ord}_7(j_E) = -3$ and that $\gamma_7(E) = 1$. Since for all $a \in R_0$, $a \equiv 1$, 2 or 4 modulo 7 we have that $\left(\frac{-a}{7}\right) = -1$, and therefore condition 5 is also satisfied. Since, $ord_3(j_E) = 0$, condition 6 is vacuous. Thus we can take $R = R_0$ and we calculate $\delta = 7/128$. Thus by Proposition 7.2.1, we have proved:

THEOREM 7.2.3. *Let $E : y^2 = x^3 + x^2 + 72x - 368$. Then there is a set $S \subset \mathbb{N}$ having lower density at least 7/128 in the square-free natural numbers such that for all $d \in S$*

$$\mathrm{ord}_3\left(\frac{L(E_d, 1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q}) \prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \quad (7.24)$$

Example 7.2.3 Let $E : y^2 = x^3 + 4x^2 - 144x - 944$ be the modular elliptic curve of conductor 19 from Example 6.2.3, and let

$$f = \frac{1}{2} \sum_{x,y,z \in \mathbb{Z}} (q^{4x^2+19y^2+20z^2-4xz} - q^{7x^2+11y^2+23z^2-10yz-6xz-2xy}). \quad (7.25)$$

Let $G \in S_2(19)$ denote the newform with $L(G, s) = L(E, s)$. We recall from Example 6.2.3 that f and G satisfy the hypotheses of Proposition 6.2.1. Also, $P = (5, -10) \in E(\mathbb{Q})$ has order 3 and is not in the kernel of the reduction modulo 3 map. Further, we note that the only odd prime dividing N_E is 19 which is 1 modulo 3. Thus, E satisfies the hypotheses of Theorem 7.1.2.

In this case, we have $W = 19$ (and therefore 24W=456). We will let $R_0 \subset (\mathbb{Z}/456\mathbb{Z})^*$ be the set $R_0 = \{7, 11, 23, 35, 43, 47, 55, 163, 175, 187, 191, 199, 215, 311, 343, 347, 359, 367\}$.

As in the previous example we can verify that each $a \in R_0$ satisfies condition 1, by calculating the first several coefficients of f and using APECS and MAPLE to compute the values of $L(E_{-n},1)/\Omega_{E_{-n}}$. As before, we use Tate's Algorithm to check that for each $a \in R_0$ and for all square-free natural numbers $d \equiv a$ modulo $24W$, we have $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$. Thus, all of the $a \in R_0$ satisfy condition 2 of Proposition 7.2.1. Also, using Tate's Algorithm, we can verify that for all $d \equiv 3$ modulo 4 and coprime to 114, we have $\Omega E_{-d}\sqrt{d}/\Omega E_{-1} = 1$. Thus, condition 3 is satisfied by each $a \in R_0$. Since $2 \nmid N_E$, condition 4 is vacuous. Now, we note that $\mathrm{ord}_{19}(j_E) = -3$ and that $\gamma_{19}(E) = 1$, and it is not hard to check that for all $a \in R_0$ that $\left(\frac{-a}{19}\right) = -1$. Thus, condition 5 is also satisfied. Since, $ord_3(j_E) = 0$, condition 6 is vacuous. Thus we can take $R = R_0$ and we calculate $\delta = 19/640$. Thus by Proposition 7.2.1, we have proved:

THEOREM 7.2.4. *Let $E : y^2 = x^3 + 4x^2 - 144x - 944$. Then there is a set $S \subset \mathbb{N}$ having lower density at least 19/640 in the square-free natural numbers such that for all $d \in S$*

$$\mathrm{ord}_3\left(\frac{L(E_d,1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q})\prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \quad (7.27)$$

Example 7.2.4 Let $E : y^2 = x^3 + x^2 - 72x - 496$ be the modular elliptic curve of conductor 26 from Example 6.2.5, and let

$$f = \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} (q^{2x^2+7y^2+13z^2-2xy} - q^{5x^2+6y^2+8z^2+6yz+2xz+4xy}). \quad (7.28)$$

Let $G \in S_2(26)$ denote the newform with $L(G,s) = L(E,s)$. We recall from Example 6.2.5 that f and G satisfy the hypotheses of Proposition 6.2.1. Also, $P = (4,4) \in E(\mathbb{Q})$ has order 3 and is not in the kernel of the reduction modulo 3 map. Further, we note that the only odd prime dividing N_E is 13 which is 1 modulo 3. Thus, E satisfies the hypotheses of Theorem 7.1.2.

In this case, we have $W = 13$ (and therefore 24W=312). We will let $R_0 \subset (\mathbb{Z}/312\mathbb{Z})^*$ be the set $R_0 = \{5, 37, 41, 73, 85, 89, 97, 109, 125, 137, 145, 149, 161, 193, 197, 229, 241, 245, 253, 265, 281, 293, 301, 305\}$.

As before, we can verify that each $a \in R_0$ satisfies condition 1, by calculating the first several coefficients of f and using APECS and MAPLE to compute the values of $L(E_{-n}, 1)/\Omega_{E_{-n}}$. As before, we use Tate's Algorithm to check that for each $a \in R_0$ and for all square-free natural numbers $d \equiv a$ modulo 312, we have $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$. Thus, all of the $a \in R_0$ satisfy condition 2. Also, using Tate's Algorithm, we can verify that for all square-free natural numbers $d \equiv 1$ modulo 4 and coprime to 78, we have $\Omega E_{-d}\sqrt{d}/\Omega E_{-1} = 1$. Thus, condition 3 is satisfied by each $a \in R_0$. Since for each $a \in R_0$, $a \equiv 1$ modulo 4, condition 4 is also satisfied. Now, we note that $\mathrm{ord}_{13}(j_E) = -3$ and that $\gamma_{13}(E) = 1$, and it is not hard to check that for all $a \in R_0$ that $\left(\frac{-a}{19}\right) = -1$. Thus, condition 5 is also satisfied. Since, $ord_3(j_E) = 0$, condition 6 is vacuous. Thus we can take $R = R_0$ and we calculate $\delta = 13/224$. Thus by Proposition 7.2.1, we have proved:

THEOREM 7.2.5. *Let $E : y^2 = x^3 + x^2 - 72x - 496$. Then there is a set $S \subset \mathbb{N}$ having lower density at least 13/224 in the square-free natural numbers such that for all $d \in S$*

$$\mathrm{ord}_3\left(\frac{L(E_d, 1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q}) \prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \quad (7.29)$$

References

1. A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

2. B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves (I)*, J. Reine Angew. Math. **212** (1963), 7–25.

3. B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves (II)*, J. Reine Angew. Math. **218** (1965), 79–108.

4. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109** (1992), 445–472.

5. D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives*, Ann. of Math. **131** (1990), 53–127.

6. ———, *A nonvanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **21** (1989), no. 1, 89–93.

7. ———, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Inventiones Math. **102** (1990), 543–618.

8. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.

9. J. H. Conway, N. Sloane, *Sphere-packings, lattices, and groups*, Springer-Verlag, 1988.

10. D. A. Cox, *Primes of the form* $x^2 + ny^2$*. Fermat, class field theory and complex multiplication*, John Wiley & Sons, Inc., New York, 1989.

11. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

12. H. Davenport and H. Heilbronn, *On the density of descriminants of cubic fields II*, Proc. Roy. Soc. London ser. A **322** (1971), 405–420.

13. F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), no. 3, 299–304.

14. L. E. Dickson, *Studies in the theory of numbers*, Chelsea Pub. Co., 1957.

15. G. Frey, *Construction and arithmetical applications of modular forms of low weight*, Elliptic curves and related topics, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., 1994, pp. 1–20, Providence, RI.

16. _____, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **40** (1988), 649–665.

17. S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on $GL(2)$*, Ann. of Math. **142** (1995), no. 2, 385–423.

18. S. Gelbart and I. Piatetski-Shapiro, *On Shimura's correspondence for modular forms of half-integral weight*, Proc. International Colloquium on Automorphic Fomrs, Representation Theory and Arithmetic, Bombay, 1979.

19. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math, vol. 751, Springer, 1979, pp. 108–118, Berlin.

20. D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem I*, Invent. Math. **111** (1993), no. 1, 171–195.

21. _____, *The size of Selmer groups for the congruent number problem II*, Invent. Math. **118** (1994), no. 2, 331–370.

22. H. Iwaniec, *On the order of vanishing of modular L-series at the critical point*, Seminaire de Theorie des Nombres, Bordeaux 2 (1990), 365–376.

23. K. James, *An example of an elliptic curve with a positive density of prime quadratic twists which have rank zero*, preprint.

24. B. Jones, *The Arithmetic Theory of Quadratic Forms*, Mathematical Association of America, 1950.

25. B. Jones, *A Table of Eisenstein Reduced Ternary Quadratic Forms of discriminant* ≤ 200.

26. A. Knapp, *Elliptic Curves*, Princeton University Press, 1992.

27. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

28. V.A. Kolyvagin, *The Mordell-Weil and Shafarevich-Tate groups for Weil Elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat **52** (1988), no. 6, 1154–1180, 1327.

29. G. Kramarz and D. Zagier, *Numerical investigations related to the L-series of certain elliptic curves.*, J. Indian Math. Soc.(N.S.) **52** (1987), 51–69.

30. J. L. Lehman, *Levels of positive definite ternary quadratic forms*, Math. Comp. **58** (1992), no. 197, 399–417, S17–S22.

31. W. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

32. D. Lieman, *Nonvanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. (2) **140** (1994), no. 1, 81–108.

33. Kumar Murty, *A nonvanishing theorem for quadratic twists of modular L-functions*, preprint.

34. M.R. Murty and V.K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. **133** (1991), 447–475.

35. J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. A.M.S. **104** (1988), 20–25.

36. J. Nekovář, *Class numbers of quadratic fields and Shimura's correspondence*, Math. Ann. **287** (1990), 577–594.

37. S. Niwa, *Modular forms of half integral wieght and the integral of certain theta-functions*, Nagoya Math J. **56** (1975), 147–161.

38. A. Ogg, *On the eigenvalues of Hecke operators*, Math. Ann. **179** (1969), 101–108.

39. K. Ono, *Rank zero quadratic twists of modular elliptic curves*, Compositio Math. **104** (1996), no. 3, 293–304.

40. _____, *Twists of elliptic curves*, Compositio Math. **106** (1997), no. 3, 349–360.

41. _____, *A note on a question of J. Nekovàř and the Birch and Swinnerton-Dyer conjecture*, Proc. Amer. Math. Soc. (to appear).

42. K. Ono and C. Skinner, *On the Fourier coefficients of half-integral weight modular forms modulo ℓ*, Ann. of Math. (to appear).

43. _____, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. (to appear).

44. B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. **116**, 511–523.

45. G. Shimura, *On modular forms of half integral wieght*, Ann. of Math. (2) **97** (1973), 440–481.

46. C. Siegel, *Gesammelte Abhandlungen Bd. 3*, Springer-Verlag, 1966, pp. 326–405.

47. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

48. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), Springer-Verlag, 275–280.

49. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Lecture Notes in Math., vol. 476, Springer-Verlag, 1975, pp. 33–52.

50. R. Taylor and A. Wiles, *Ring–theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), no. 3, 553–572.

51. J.L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures. et Appl. **60** (1981), 375–484.

52. A. Wiles, *Modular ellliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

53. Siman Wong, *Rank zero twists of elliptic curves*, preprint.

54. G. Yu, *Quadratic twists of a given elliptic curve over* $\mathbb{Q}$, preprint.