Computationally Feasible Bounds for Representations of Integers by Ternary Quadratic Forms and CM Lifts of Supersingular Elliptic Curves

By

Ben Kane

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2007

Abstract

For $-D$ a fundamental discriminant and p a prime, we investigate the surjectivity of the reduction map from elliptic curves with CM by $\mathcal{O}_{-D}$ to supersingular elliptic curves over $\overline{\mathbb{F}_p}$ whenever p does not split in $\mathcal{O}_{-D}$. Under GRH for Dirichlet L-functions and the L-functions of weight 2 newforms, we are able to show an effectively computable bound D_p such that the reduction map is surjective for every $D > D_p$ with p nonsplit. Our investigation takes a detour through a study of quaternion algebras and quadratic forms. In particular, in showing our result, we obtain as a side effect the following result. For each positive definite quadratic form Q whose associated theta series is in Kohnen's plus space of weight 3/2 and level $4p$, $M_{3/2}^{+}(4p)$, we show an effectively computable bound D_Q, dependent upon GRH) such that Q represents every D for which $D > D_Q$ and p does not split in $\mathcal{O}_{-D}$. Moreover, we give an explicit algorithm to compute D_Q (respectively D_p), and for small p we explicitly compute D_Q (resp. D_p). For a further restricted set of p, we moreover obtain a computationally feasible bound, allowing us to give a full list of fundamental discriminants $-D$ for which the map is not surjective. To determine the full list we develop a specialized algorithm to compute which $D < D_p$ are represented more efficiently whenever all of the elliptic curves are defined over $\mathbb{F}_p$. Additionally, we obtain as an additional side effect a new proof and an explicit algorithm, conditional upon GRH, for the Ramanujan-Petersson conjecture for weight 3/2 cusp forms of level $4N$ in Kohnen's plus space with N odd and squarefree.

Acknowledgements

I would like to thank the many people who helped make this thesis possible.

I would first and foremost like to thank my thesis advisor, Dr. Tonghai Yang, for helping me find an interesting problem, giving me inspiration, and for many hours of useful conversation.

I would also like to thank Professor Ken Ono for advice and guidance. His aid in letting me meet with him during my advisor's illness helped me work through some of the difficult aspects of this thesis.

This thesis would have been entirely impossible if not for many hours of discussion about computational methods with my fellow graduate student, Jeremy Rouse. His suggestions and sharing of knowledge have been invaluable to the success of this thesis.

Thanks to all of the support staff of the mathematics department for making all of the logistical issues involved with research, travel, and university and departmental requirements seem almost non-existent.

I would also like to thank my wife Anne for her motivation and patience while I spent many long nights working on this research.

Finally, I would like to give my appreciation to my extended family and especially my parents, Judith Beck and John Kane, for helping guide my learning and motivating me to work hard towards my goals.

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 CM lifts of Supersingular Elliptic Curves

Let p be a prime, $-D < 0$ be a fundamental discriminant, and $K := \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with ring of integers $\mathcal{O}_{-D}$ such that p does not split in $\mathcal{O}_{-D}$. Furthermore, let E be an elliptic curve defined over $\overline{\mathbb{F}_p}$. It is well known that the ring of endomorphisms $End(E)$ of E are isomorphic either to the ring of integers of an imaginary quadratic field or to a maximal order $\mathcal{O}_E$ of the quaternion algebra ramified precisely at p and ∞. Elliptic curves of the second type are called *supersingular elliptic curves.* For an elliptic curve E' defined over a number field, it is well known that $End(E')$ is isomorphic either to $\mathbb{Z}$ or an order of an imaginary quadratic field. We say that E' has *Complex Multiplication (CM) by* $\mathcal{O}_{-D}$ if the endomorphisms of E' are isomorphic to $\mathcal{O}_{-D}$. It is well known that the reduction map mod $\mathfrak{P}$, the distinct prime above p, from an elliptic curve with CM by $\mathcal{O}_{-D}$ yields a supersingular elliptic curve whenever p does not split in $\mathcal{O}_{-D}$.

For convenience, we will say that D_E (resp. D_p) is a *good bound for E (p)* if E (every supersingular $E/\overline{\mathbb{F}_p}$ is in the image of the reduction map from elliptic curves with CM by $\mathcal{O}_{-D}$ for every $D > D_E$ ($D > D_p$) for which p does not split. The majority of this paper is devoted to proving an effectively computable good bound for E (resp.

p) conditional upon standard conjectures. Moreover, an explicit algorithm is given for computing a good bound for E (resp. p). This algorithm is implemented for small p, and our results are recorded. We will call a good bound D_E a *feasibly good bound* if we have determined, with the help of a computer, the set of $D < D_E$ for which E is in the image of the reduction map. By tweaking certain parameters which arise in our good bounds, we are able to obtain better good bounds for p. Moreover, using a trick to compute the set of $D < D_E$ for which the reduction map is surjective whenever E is defined over $\mathbb{F}_p$, we are able to obtain feasibly good bounds for a larger set of E.

1.2 Reduction to Representations of Integers by Ternary Quadratic Forms

Deuring [8] has shown a one-to-one correspondence between lifts of E to elliptic curves with CM by $\mathcal{O}_{-D}$ and embeddings of $\mathcal{O}_{-D}$ in the maximal order $\mathcal{O}_E$ of the quaternion algebra A ramified precisely at p and ∞. For a maximal order M of the quaternion algebra A, we will say that D_M is a *good bound for M* if $\mathcal{O}_{-D}$ embeds into M whenever $-D < -D_M$ is a fundamental discriminant for which p does not split in $\mathcal{O}_{-D}$. Hence D_M is a good bound for $M = \mathcal{O}_E$ if and only if D_M is a good bound for E. For $-D < 0$ a fundamental discriminant, the ring of integers $\mathcal{O}_{-D}$ is embedded in M if and only if there is an element of M which generates the ring of integers, namely one with minimal polynomial $x^2 - Dx + \frac{D^2+D}{4}$. Let $L_E := \{x \in \mathbb{Z} + 2\mathcal{O}_E | tr(x) = 0\}$ be the so called *Gross lattice* of trace zero elements of the order defined by Gross in [14] with the associated positive definite ternary quadratic form $Q(x) = Nx = -x^2$. It is an easy calculation to see that a generator of $\mathcal{O}_{-D}$ is contained in M if and only if there is an element of L_E with norm D.

We will say that the integer D is *represented (over the ring R) by the quadratic form Q* if there exists $x \in R^3$ such that $Q(x) = D$. For a quadratic form Q, we say that an integer D is an *eligible integer for Q* if it is represented locally ($R = \mathbb{Z}_p$) at every prime, and we will call D_Q a *good bound for Q* if every eligible integer $D > D_Q$ is represented globally ($R = \mathbb{Z}$) by Q. This paper will proceed to find a good bound for M (and hence E or p) by determining a good bound D_Q for Q.

1.3 Representations of Integers by Ternary Quadratic Forms

The question of determining which integers are represented by a given quadratic form is an interesting question in its own right, which has been studied by a variety of authors dating back at least as far as Gauss. One such well known result of Lagrange shows that every positive integer can be represented as the sum of four squares. The amazing “15 theorem”, proven first but unpublished by Conway and Shneeberger and recently shown via a much simpler method by Bhargava, asserts that a positive definite integral quadratic form represents every positive integer if and only if it represents the integers 1,2,3,5,6,7,10,14, and 15 [1]. Such forms are called *universal quadratic forms.* Bhargava and Hanke have since shown that every integer valued quadratic form is universal if and only if it represents every integer less than 290 [2].

Let

$$\theta_Q(\tau) := \sum_{x\in\mathbb{Z}^m} q^{Q(x)}$$

be the theta series associated to a quadratic form Q in m variables, where $q = e(\tau) := e^{2\pi i\tau}$. It is well known that θ is a modular form of weight $\frac{m}{2}$.

Relying on the fact that θ is a modular form, and comparing the growth of the coefficients of the Eisenstein series with the growth of the coefficients of cusp forms, Tartakowsky effectively shows that every sufficiently large eligible integer n is represented by Q when $m \geq 5$ [37]. In the $m = 4$ case the trivial bound for the growth of the coefficients of cusp forms is insufficient, but Kloosterman proved an improved bound (the celebrated result of Deligne proved the optimal bound in the early seventies [7]). The binary case ($m = 2$) was studied extensively by Gauss, and Gauss's well known genus theory was developed during this study. The question of which primes are represented by binary quadratic forms has been studied by a variety of authors (cf. [35]), and there are asymptotics known for the number of integers not represented by a binary quadratic form [13]. In this case comparing the asymptotics for the number of eligible integers with the number of integers represented by the form shows that there is no good bound for binary quadratic forms.

In this paper, we study the trickiest case, namely ternary quadratic forms ($m = 3$). This case is complicated by the fact that the coefficients of the Eisenstein series grows like the Class Number. Therefore, an effective bound requires information about the possible Siegel Zero. Moreover, the convexity bound is insufficient to show that the coefficients of the weight 3/2 cusp forms grow more slowly than the class number. Recently, the amazing subconvexity results of Iwaniec [18] and Duke [9] have removed this complication. There is also a technicality at *anisotropic primes*. The coefficients of the Eisenstein series do not grow with high divisibility by an anisotropic prime l. Duke and Schultze-Pillot combine the above results to show the following ineffective result.

Theorem 1.1 (Duke- Schultze-Pillot [11]). *If Q is a positive definite quadratic form in 3 variables, then every sufficiently large eligible integer with bounded divisibility at the anisotropic primes is represented by Q.*

Assuming GRH for Dirichlet L-functions, the result becomes effective. However, the bound attained is enormous and entirely impractical, as observed by Ono and Soundararajan [29]. By using a deep connection of Waldspurger [38] between half integer weight cusp forms and special values of L-series of weight 2 modular forms, under the additional assumption of GRH for weight 2 modular forms, Ono and Soundararajan obtain a feasible bound of 2×10^{10} for Ramanujan's ternary quadratic form $Q(x, y, z) = x^2 + y^2 + 10z^2$. With the help of a computer, they were able to prove the following.

Theorem (Ono-Soundararajan [29]). *Conditional upon GRH, the eligible integers which are not represented by Q are exactly*

$$3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719.$$

In Chapter 3, we generalize the results of Ono and Soundararajan to ternary quadratic forms Q such that $\theta_Q \in M^+_{3/2}(4p)$, the space of modular forms of weight 3/2 and level $4p$ in Kohnen's plus space (Ramanujan's form does not satisfy this condition). By the theory of modular forms, we know that θ decomposes as follows.

$$\theta = E + \sum_{i=1}^{m} b_i g_i, \tag{1.1}$$

where E is an Eisenstein series, $b_i \in \mathbb{C}$ and g_i are fixed Hecke eigenforms in $S^+_{3/2}(4p)$. Let $G_i \in S_2(p)$ be the Shimura lift of g_i, normalized such that $a_{G_i}(1) = 1$. Throughout the paper we use $a_f(n)$ to denote the n-th coefficient of f. Clearly, Q represents n if and only if $a_\theta(n) \neq 0$. Hence we only need to bound the coefficients of the Eisenstein Series (from below) and the eigenforms (from above). We will denote $-d$ for a discriminant and $-D$ for a fundamental discriminant. Using techniques developed by Duke [10], based upon Siegel's averaging of the quadratic forms, along with a generalized version of the aforementioned method of Ono and Soundararajan [29], we obtain effective bounds for $a_E(D)$ and $a_{g_i}(D)$, where $-D$ is a fundamental discriminant. In [29], Ono and Soundararajan make specific choices to obtain a computable constant for Ramanujan's form. While the bound they obtain is more aesthetically pleasing, allowing these choices to vary yields computationally feasible bounds for a wider range of quadratic forms.

Theorem 1.2. *Fix $1 < \sigma < \frac{3}{2}$ and $\boldsymbol{X} > \boldsymbol{X}_\sigma$, with $\boldsymbol{X}_\sigma$ effectively computable.*

Assume GRH for Dirichlet L-series and weight 2 modular forms. There exists an effectively computable constant $D_{\theta,\boldsymbol{X},\sigma}$ such that for every fundamental discriminant $-D$ with $D > D_{\theta,\boldsymbol{X},\sigma}$ we have $a_\theta(D) \neq 0$.

This result gives us an effectively computable good bound for Q, and hence an effectively good bound for E given the connection. A slight alteration of this method also leads to good bounds for Q which are independent of Q, and only vary with p. Further results of this type may be found in Chapter 3.

1.4 Calculations for Good Bounds

Having established effectively computable good bounds for Q, E, p, and M in Chapter 3, we proceed to give an algorithm for calculating these bounds in Chapter 4. This task is separated into three main parts. In the first part, we calculate the maximal orders of the quaternion algebra ramified exactly at p and ∞ and the associated theta series. Secondly, we decompose the subspace of Kohnen's plus space spanned by these theta series. Having done so, we have decomposed θ as

$$\theta = E + \sum_i g_i',$$

where g_i' are some hecke eigenforms. We then show a method for choosing a certain Shimura lift and hence g_i and b_i. Finally, we calculate other constants involved in the bound $D_{\theta,\boldsymbol{X},\sigma}$ up to a chosen accuracy.

We now have established an algorithm for computing a good bound D_Q, assuming GRH. Given a bound, we would like to determine which good bounds are feasibly good bounds. In order to do so, we must write another algorithm to determine whether a given integer D is represented by the quadratic form Q, and then check all $D < D_Q$. In order to obtain a feasibly good bound for a larger set of Q, we develop a specialized algorithm for checking whether D is represented by Q whenever Q comes from L_E for E defined over $\mathbb{F}_p \subset \overline{\mathbb{F}_p}$ in Section 4.3. For certain p, every supersingular elliptic curve E is defined over $\mathbb{F}_p$, and thus we may obtain a feasibly good bounds for p for a larger set of primes. Finally, in Section 4.4, we implement our algorithm and list good bounds D_Q for each Q with $p \leq 107$. We also give data for the $D < D_Q$ which we have checked with a computer. For $p = 11$, $p = 17$, and $p = 19$ we are able to obtain a feasibly good bound for p, and an explicit list of all D for which the reduction map is not surjective (or the size of the list when it is too large) is given.

Chapter 2

Elliptic Curves and Ternary Quadratic Forms

2.1 CM Liftings of Supersingular Elliptic Curves and Theta Series

We will explain in this chapter the well known connection between determining a good bound D_Q for each theta series θ_Q in Kohnen's plus space of level $4p$ and determining a good bound for p. We will discuss the connection between theta series and CM lifts of supersingular elliptic curves in order to determine how the good bound for these theta series gives us a good bound for p.

A good bound D_p for p is established piecewise by showing a good bound D_E for each supersingular elliptic curve $E/\overline{\mathbb{F}_p}$, and then taking $D_p := \max_E D_E$, relying on the fact that there are only finitely many supersingular elliptic curves over $\overline{\mathbb{F}_p}$ (see [34]) up to isomorphism. This also aids in computing the set of $D < D_p$ for which the map is not surjective, since we only need to check $D < D_E$ for each curve, and not up to the larger bound D_p.

Therefore, we will now fix a supersingular elliptic curve $E/\overline{\mathbb{F}_p}$ and explain how to establish a good bound D_E. To this end, we will now take a detour through quaternion algebras, quadratic forms, theta series, and modular forms. Throughout, when we refer to a θ-series, we will be restricting to a θ-series of the type

$$\theta = \sum_{x,y,z} q^{Q(x,y,z)},$$

where $Q(x, y, z)$ is a positive definite ternary quadratic form and $q = e^{2\pi iz}$.

We will now review the well known connection between CM liftings and θ-series. Deuring [8] showed a one-to-one correspondence between embeddings of $\mathcal{O}_{-D}$ in $\mathcal{O}_E = End(E)$ and lifts of E to elliptic curves with CM by $\mathcal{O}_{-D}$. Therefore, our study of lifts transforms into a study about the number of embeddings of $\mathcal{O}_{-D}$ in $\mathcal{O}_E$. Recall that $End(E)$ is a maximal order of the quaternion algebra ramified exactly at p and ∞. Let A be the quaternion algebra ramified exactly at p and ∞ and let M be a maximal order of A. Then M is a $4-$dimensional $\mathbb{Z}$-module. Let $L_E := \{x \in \mathbb{Z} + 2\mathcal{O}_E | tr(x) = 0\}$ be the so called *Gross lattice* with the associated positive definite ternary quadratic form $Q_E(x) = Nx = -x^2$. Gross proved a bijection between embeddings of $\mathcal{O}_{-D}$ in $\mathcal{O}_E$ and representations of D by Q_E. Moreover, Gross showed that the theta series

$$\theta_E(z) := \sum_{x \in L_E} q^{Q_E(x)} = \sum_{-d \equiv 0,1 \pmod 4} a_E(d) q^d$$

is a weight $3/2$ modular form in Kohnen's plus space of level $4p$. We have seen above that E lifts to an elliptic curve with CM by $\mathcal{O}_{-D}$ if and only if $a_E(D) \neq 0$. Therefore, a good bound for θ_E will give us a good bound for E.

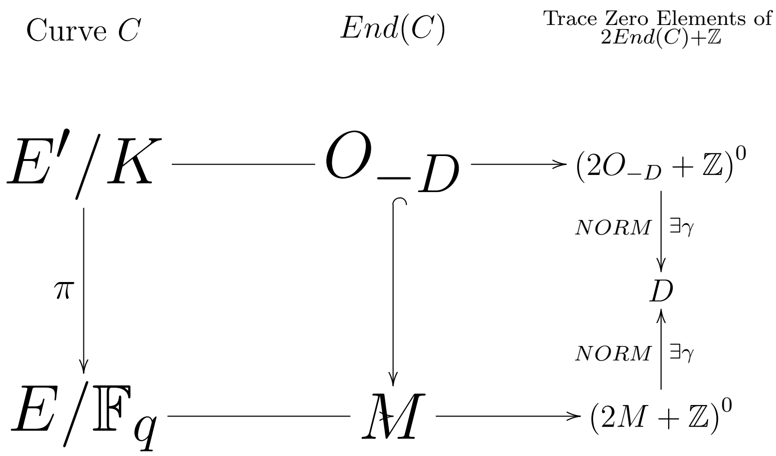

Figure 1: The reduction map from elliptic curves with CM by $\mathcal{O}_{-D}$ to supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

2.2 Details of the Connection between CM lifts and Representations of Integers by Quadratic Forms

The following diagram will help to further explain the connection made by Deuring and Gross. Taking a supersingular elliptic curve E defined over $\overline{\mathbb{F}_p}$, we know that the endomorphisms of E are isomorphic to a maximal order $M = \mathcal{O}_E$ of the quaternion algebra ramified exactly at p and ∞. Taking an elliptic curve E' defined over a number field with CM by $\mathcal{O}_{-D}$, the endomorphisms of E' are isomorphic to $\mathcal{O}_{-D}$. If E is the image of E' under the reduction map, then, since the endomorphisms commute with the reduction map, we know that there is an embedding of endomorphisms $\mathcal{O}_{-D}$ of E' into the endomorphisms M of E. If we take the trace zero elements $(2\mathcal{O}_{-D} + \mathbb{Z})^0$, then the generator of $\mathcal{O}_{-D}$ will correspond to an element with norm D. Thus, the embedding of $\mathcal{O}_{-D}$ under the same operation on M, namely $(2M + \mathbb{Z})^0$, will give an element of norm D. Moreover, if there is an element of M which gives D under this norm map, then it is an easy calculation to see that this element must be a generator for $\mathcal{O}_{-D}$. Thus, there is a one-to-one correspondence between embeddings of $\mathcal{O}_{-D}$ in M and representations of D by the norm form on L_E.

Hence, we have established that if E is in the image of the reduction map, then the norm map represents the integer D. On the other hand, Deuring shows that an embedding of $\mathcal{O}_{-D}$ into $\mathcal{O}_E$ determines an elliptic curve E' with CM by $\mathcal{O}_{-D}$ which gives E under the reduction map. Therefore, there is a one-to-one correspondence between embeddings of $\mathcal{O}_{-D}$ in $\mathcal{O}_E$ and CM lifts of E. Using the one-to-one correspondence between embeddings of $\mathcal{O}_{-D}$ and representations of D by the norm form on L_E, this gives a one-to-one correspondence between CM lifts of E and representations of D by the norm form on L_E.

It is a straightforward calculation to see that the norm form on L_E is a quadratic form in 3 variables, since the elements of L_E are trace zero elements. If L_E is generated over $\mathbb{Z}$ by α', β', and γ', then every element of L_E is of the form

$$x\alpha' + y\beta' + z\gamma'. \tag{2.1}$$

The definition of L_E allows one to see easily that α', β', and γ' are linear combinations of the canonical generators α, β, and $\alpha\beta = \gamma$ with $\alpha\beta = -\beta\alpha$, $\alpha^2 = p$ and $\beta^2 = q$. Thus, we can rewrite (2.1) as

$$a(x,y,z)\alpha + b(x,y,z)\beta + c(x,y,z)\gamma, \tag{2.2}$$

where $a(x,y,z)$, $b(x,y,z)$, and $c(x,y,z)$ are homogeneous and linear in x, y, z. The norm of such an element is

$$(a(x,y,z)\alpha + b(x,y,z)\beta + c(x,y,z)\gamma)^2 = a(x,y,z)^2p + b(x,y,z)^2q + c(x,y,z)^2pq.$$

Since $a(x, y, z)$, $b(x, y, z)$, and $c(x, y, z)$ are homogeneous and linear in x, y, z, the terms of the squares are homogeneous and quadratic in x, y, z. Therefore, this defines a ternary quadratic form in x, y, and z.

The connection to Kohnen's plus space is established by local conditions, since the only integers represented by the norm form are integers d with $-d$ a discriminant. Therefore, $-d \equiv 0$ or $1 \pmod 4$. This is precisely the condition for the theta series to be an element of Kohnen's plus space. Thus, determining a good bound for Q_E, the norm form on L_E, which is a member of Kohnen's plus space of weight 3/2 and level p, will determine a good bound for E. We have now established the desired connection.

It is not a trivial task to write down all supersingular elliptic curves (up to isomorphism), and furthermore, it is an interesting and challenging problem to write down the endomorphisms of a fixed supersingular elliptic curve. This problem is not addressed in this thesis. However, we are rescued by the well known result of Deuring [8], that every maximal order of A is conjugate to $\mathcal{O}_E = End(E)$ for some supersingular elliptic curve E over $\overline{\mathbb{F}_p}$. Moreover, two maximal orders $\mathcal{O}_E$ and $\mathcal{O}_{E'}$ are conjugate if and only only if $E' \cong E$ or $E' \cong E^{(p)}$, the Frobenius of E. Moreover, $E \cong E^{(p)}$ if and only if the Frobenius is an endomorphism on E, which implies that E is defined over $\mathbb{F}_p$. Moreover, the Frobenius gives a trace zero element of $\mathcal{O}_E$ with norm p. Conversely, if there is a trace zero element of norm p, then the curve is defined over $\mathbb{F}_p$. Therefore, we simply need to calculate all maximal orders of A (up to conjugation), which is done in chapter 4. Since the curves over $\mathbb{F}_{p^2}$ occur in pairs $(E, E^{(p)})$, we get exactly the type number t such maximal orders (up to conjugation). In this paper, we will determine good bounds D_M for each maximal order M, and using this connection we have shown good bounds D_E for each supersingular elliptic curve E. However, it is a very interesting question to determine which maximal orders correspond to to which elliptic curves. I hope to investigate the question of efficiently computing $\mathcal{O}_E$ given E and vice versa in the foreseeable future. This question is addressed in David Kohel's Ph.D. Thesis [22], but no sub-exponential algorithm is known.

Chapter 3

Good Bounds for Representations of Integers by Quadratic Forms

3.1 Introduction

Let Q be a positive definite integral quadratic form in m variables and let

$$\theta_Q(\tau) := \sum_{x\in\mathbb{Z}^m} q^{Q(x)}$$

be the associated theta series, where $q = e(\tau) := e^{2\pi i\tau}$. We will omit the subscript Q when it is clear. Throughout this paper, a theta series will always mean θ_Q for some (mostly ternary) positive definite integral quadratic form Q. It is well known that θ is a modular form of weight $\frac{m}{2}$. For general information about quadratic forms, a good source is [25].

The natural question of which positive integers n are *represented by the form* Q, that is whether there exists $x \in \mathbb{Z}^m$ such that $Q(x) = n$, has been studied extensively since Gauss. Recall the following theorem of Ono and Soundararajan [29], previously mentioned in the introduction, for Ramanujan's ternary quadratic form.

Theorem (Ono-Soundararajan [29]). *Conditional upon GRH, the eligible integers which* *are not represented by* $Q(x,y,z) = x^2 + y^2 + 10z^2$ *are exactly*

$$3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719.$$

In this chapter, we generalize the results of Ono and Soundararajan for ternary quadratic forms Q such that $\theta_Q \in M^+_{3/2}(4p)$ in order to prove Theorem 1.2. The proof of Theorem 1.2 leads to an independent proof of the optimal bound, known to the experts, for weight 3/2 cusp forms in Kohnen's Plus Space of level $4N$ with N squarefree and odd, assuming the Riemann Hypothesis for weight 2 cusp forms.

Corollary 3.1. *Let N be squarefree and odd, $\epsilon > 0$, and $g \in S^+_{3/2}(4N)$. Assuming GRH for weight 2 modular forms, there is an effectively computable constant $c_{g,\epsilon}$ such that*

$$|a_g(n)| \leq c_{g,\epsilon} n^{\frac{1}{4}+\epsilon}.$$

Theorem 1.2 is proven by combining explicit bounds from Sections 3.5 and 3.6. These explicit bounds lead to a clear algorithm to calculate the constant $D_{\theta,\boldsymbol{X},\sigma}$. The bounds attained are computationally feasible in some cases. For example, with the help of a computer, Theorem 1.2 implies the following (for details, see [20]).

Theorem 3.2. *Assume GRH for Dirichlet L-functions and weight 2 modular forms. Consider d such that $11^2 \nmid d$ and $\left(\frac{-d}{11}\right) \neq 1$. Then*

(1) $Q(x,y,z) = 4x^2 + 11y^2 + 12z^2 + 4xz$ *represents d if and only if*

$$d \notin \{3, 67, 235, 427\}, \tag{3.1}$$

and Q represents d if and only if Q represents $d(11)^2$.

(2) $Q(x, y, z) = 3x^2 + 15y^2 + 15z^2 - 2xy + 2xz + 14yz$ *represents* d *if and only if*

$$d \notin \{4, 11, 88, 91, 163, 187, 232, 499, 595, 627, 715, 907, 1387, 1411, 3003, 3355, 4411, 5107, 6787, 10483, 11803\}, \quad (3.2)$$

and Q *represents* d *if and only if* Q *represents* $d(11)^2$.

(3) *Moreover, these are a full set of representatives for* Q *such that* $\theta \in M^{+}_{3/2}(44)$.

(4) *If* $-d = -D$ *is a fundamental discriminant other than the* 25 *listed above, then every supersingular elliptic curve over* $\overline{\mathbb{F}_{11}}$ *can be lifted to an elliptic curve over a number field, with CM by* $\mathcal{O}_{-D}$.

Theorem 3.3. *Assume GRH for Dirichlet L-functions and weight 2 modular forms. Consider* d *such that* $19^2 \nmid d$ *and* $\left(\frac{-d}{19}\right) \neq 1$. *Then*

(1) $Q(x, y, z) = 7x^2 + 11y^2 + 23z^2 - 2xy + 6xz + 10yz$ *represents* d *if and only if*

$$d \notin \{4, 19, 163, 760, 1051\}, \quad (3.3)$$

and Q *represents* d *if and only if* Q *represents* $d(19)^2$.

(2) *The form* $Q(x, y, z) = 4x^2 + 19y^2 + 20z^2 + 4xz$ *represents* d *if and only if* d *represents* $d(19)^2$, *the set of* d *as above which* Q *does not represent has size* 40, *and the largest such is* $d = 27955$.

(3) *Moreover, these are a full set of representatives for* Q *such that* $\theta \in M^{+}_{3/2}(76)$.

(4) *If* $-d = -D$ *is a fundamental discrimianant other than the 45 above (in particular if* $D > 27955$*), then every supersingular elliptic curve over* $\overline{\mathbb{F}_{19}}$ *lifts to an elliptic curve over a number field, with CM by* $\mathcal{O}_{-D}$.

In Section 3.3, we deal with $-d$ not fundamental, using the Shimura Lift [32] and the Hecke operators. Fixing a discriminant $-d$ and exploring the representability of $d' = dF^2$, the Hecke operators lead to an equivalence between the following linear system of equations and the representability of d by Q.

Theorem 3.4. *There are recursively defined polynomials $P_{k,m,\pm 1}(x)$ and $Q'(x)$, defined below, such that $a_\theta(dF^2) = 0$ if and only if for every $f = \prod_l l^{r_l}$ dividing F and $s_l \leq \frac{1}{2}v_l(d)$,*

$$\prod_{l \text{ prime}} P_{r_l, s_l, (\frac{-D}{l})}(l) = Q'(f).$$

Remark 3.5. *The power of Theorem 3.4 is that the left side is growing like l, while the right side grows like $2\sqrt{l}$, so that the resulting linear system is seldom consistent.*

Notice that although an effective lower bound for the Class Numbers relies on the Siegel Zeros, the ratio of Class Numbers $H(-dF^2)/H(-d)$ does not. Fix a fundamental discriminant $-D$. We refer to the *spinor square class* of D as all integers DF^2. Due to the explicit ratio, unconditional results may be obtained within the spinor square class of D, since the growth of the ratio is linear in F, while Shimura's lift and Deligne's bound [7] imply that the growth of the coefficients of the cusp forms is like $F^{1/2}$.

Theorem 3.6. *Fix a disciminant $-d$. If $a_\theta(dF^2) = 0$ with $(F, p) = 1$, then*

$$F \ll_\epsilon (p-1)^{2+\epsilon} \left(\sum_{i=1}^{m} |b_i| \right)^{2+\epsilon} d^{\frac{6}{7}+\epsilon}.$$

If we further assume the Riemann Hypothesis for Dirichlet L-functions, then

$$F \ll_\epsilon (p-1)^{2+\epsilon} \left(\sum_{i=1}^{m} |b_i| \right)^{2+\epsilon} d^{-\frac{1}{7}+\epsilon}.$$

Finally, if we additionally assume the Riemann Hypothesis for L-functions of weight 2 modular forms, then

$$F \ll_\epsilon (p-1)^{2+\epsilon}\left(\sum_{i=1}^{m}|b_i|\right)^{2+\epsilon} d^{-\frac{1}{2}+\epsilon}.$$

Here the assumed constants are effectively computable, and moreover $a_\theta(d) = 0$ *if and only if* $a_\theta(dp^2) = 0$.

Combining Corollary 3.1 and Theorem 3.6 along with an argument of Duke [10] to remove the dependence on θ yields the following result.

Theorem 3.7. *Let* p *be a prime,* $\theta \in M_{3/2}^{+}(4p)$*, and* $\epsilon > 0$*. Assuming GRH for Dirichlet L-functions and weight 2 modular forms,* $a_\theta(d) \neq 0$ *for every discriminant* $-d$ *with* $\left(\frac{-d}{p}\right) \neq 1$ *and* $p^2 \nmid d$ *such that*

$$d \gg_\epsilon p^{16+\epsilon}.$$

Here the assumed constant depends only on ϵ *and is effective. Moreover,* $a_\theta(d) = 0$ *if and only if* $a_\theta(dp^2) = 0$.

It is interesting to note that our arguments involving the cusp form part of θ suffice for level $4N$ with N squarefree and odd, so that a generalization can be obtained for any quadratic form with squarefree discriminant, whose theta series is contained in Kohnen's plus space once we know the corresponding Eisenstein series.

Our work has an application to CM liftings of supersingular elliptic curves, and this is the author's original motivation for concentrating on Kohnen's plus space of level $4p$. This connection is explored further, and an explicit algorithm plus a variety of examples are given in a sequel [20]. We will give a brief explanation here of this connection.

The endomorphism ring of a supersingular elliptic curve E is a maximal order $\mathcal{O}_E$

of the quaternion algebra ramified exactly at p and ∞. Deuring [8] has shown a correspondence between maximal embeddings of $\mathcal{O}_{-D}$ and lifts of E to an elliptic curve over a number field which is CM by $\mathcal{O}_{-D}$. Let

$$L_{\mathcal{O}_E} := \{x \in \mathbb{Z} + 2\mathcal{O}_E | \mathrm{Tr}\ x = 0\}$$

be the so called "Gross lattice" with quadratic form $Q(x) = -x^2$ being the reduced norm. Then Gross [14] shows that $\theta_Q \in M^+_{3/2}(4p)$ and $\mathcal{O}_{-D}$ is optimally embedded in $\mathcal{O}_E$ if and only if Q represents D. This explains the fourth part of Theorems 3.2 and 3.3. Interpreting Theorem 3.7 in this manner, we obtain the following.

Theorem 3.8. *Let p be a prime and $\epsilon > 0$. Assume GRH for Dirichlet L-functions and weight 2 modular forms. Let $E/\overline{\mathbb{F}_p}$ be a supersingular elliptic curve. Then E lifts to a elliptic curve over a number field which is CM by $\mathcal{O}_{-D}$ for every*

$$D \gg_\epsilon p^{16+\epsilon}$$

with $\left(\frac{-D}{p}\right) \neq 1$. Here the assumed constant depends only on ϵ and is effective.

Notation and Brief Overview of the Proof of Theorem 1.2

We end the introduction with a brief overview of the proof of Theorem 1.2, and set up useful notation. We will denote half integral weight cusp forms with lower case letters and their Shimura Lift with capital letters.

Let p be an odd prime and $\theta \in M^+_{3/2}(4p)$ be a theta function θ_Q. Assume first that $-D < -4$ is a fundamental discriminant with $a_\theta(D) = 0$. We will denote the Hurwitz class number for a discriminant d by $H(d)$ and the class number by $h(d)$. Equation (1.1) gives

$$-a_E(D) = \sum_{i=1}^{m} b_i a_{g_i}(D). \tag{3.4}$$

Using an explicit formula for the coefficients of the Eisenstein series(cf. [14]) and Dirichlet's Class Number Formula [6],

$$a_E(D) = \frac{12}{(p-1)} \cdot \frac{L(1)\cdot\sqrt{D}}{\pi 2^{v_p(D)}}. \tag{3.5}$$

Here $L(s) := L(\chi, s)$ and $\chi(n) := \chi_{-D}(n) := \left(\frac{-D}{n}\right)$ is a Dirichlet character. Plugging in and using Schwartz's inequality yields

$$\frac{12}{(p-1)\pi 2^{v_p(D)}} \cdot |L(1)| \cdot \sqrt{D} \leq \sqrt{\sum_{i=1}^{m} |b_i|^2} \sqrt{\sum_{i=1}^{m} |a_{g_i}(D)|^2}. \tag{3.6}$$

A variant of the Kohnen-Zagier formula (3.15) gives $|a_{g_i}(D)|^2 = c_i 2^{-v_p(D)} D^{\frac{1}{2}} \cdot L_i(1)$, where

$$c_i := \frac{|a_{g_i}(m_i)|^2}{L(G_i, m_i, 1) m_i^{\frac{1}{2}}}, \tag{3.7}$$

with m_i the first coefficient of g_i such that $a_{g_i}(m_i) \neq 0$ with $(p, m_i) = 1$, and

$$L_i(s) := L(G_i, -D, s) := \sum_{n=1}^{\infty} \frac{\chi(n) a_{G_i}(D)}{n^s}. \tag{3.8}$$

is the L series of G_i twisted by the character χ. Thus, we have obtained

$$\frac{12}{(p-1)\pi 2^{\frac{v_p(D)}{2}}} \cdot D^{\frac{1}{4}} \leq \sqrt{\sum_{i=1}^{m} |b_i|^2} \sqrt{\sum_{i=1}^{m} c_i \frac{L_i(1)}{L(1)^2}}. \tag{3.9}$$

To bound $\frac{L_i(1)}{L(1)^2}$ we define

$$F(s) := F_i(s) := \left(\frac{\sqrt{q}}{2\pi}\right)^{s-1} \frac{L_i(s)\Gamma(s)}{L(s)L(2-s)}, \tag{3.10}$$

where q is the conductor of L_i. Notice that $F(1) = \frac{L_i(1)}{L(1)^2}$.

By the functional equation of $L_i(s)$, we know that $F(s) = F(2-s)$ and GRH for Dirichlet L-functions implies that $F(s)$ is analytic for $\frac{1}{2} < \mathrm{Re}(s) < \frac{3}{2}$. Therefore, for $\frac{1}{2} < \mathrm{Re}(s) = \sigma < \frac{3}{2}$ fixed, we know by the Phragmen-Lindelöf principle that the maximum is attained on the boundary of $\mathrm{Re}(s) = \sigma$ and $\mathrm{Re}(s) = 2-\sigma$. Thus, for $1 < \sigma < \frac{3}{2}$,

$$F(1) \leq \max_t |F(\sigma + it)|.$$

To bound $F(s)$, we bound $L(s)$ from below in Section 3.5 and $L_i(s)$ from above in Section 3.6. Instead of fixing $\sigma = \frac{7}{6}$ as in [29], we allow σ to vary, and get better constants in our bounds for $L(s)$ and $L_i(s)$. Combining these allows us to get the bound obtained in Theorem 1.2.

To deal with discriminants which are not fundamental, we will use the Hecke operators for half integer weight modular forms. For $g \in S_{k+1/2}(4p,\chi)$ and a prime l, we define the Hecke operator T_{l^2} via $g|T_{l^2} = h$ with

$$a_h(d) = a_g(l^2 d) + \chi(l)\left(\frac{(-1)^k}{l}\right) l^{k-1} a_g(d) + \chi(l^2)\left(\frac{(-1)^k}{l^2}\right) l^{2k-1} a_g\left(\frac{d}{l^2}\right). \qquad (3.11)$$

For $d \in \mathbb{N}$, with $d = \prod_l l^{e_l}$, we will denote for notional ease

$$\Omega(d) := \sum_{l\prime} e_l,\ v_l(d) = e_l,\ v(d) = \#\{l : e_l > 0\},\ \textit{and}\ \sigma_k(d) = \sum_{n|d} n^k. \qquad (3.12)$$

We recall the Euler constant

$$\gamma := -\frac{\Gamma'}{\Gamma}(1) \approx .5772 \qquad (3.13)$$

and denote the Riemann Zeta function by $\zeta(s)$. Finally, we denote

$$\psi(x) := \sum_{n \leq x} \Lambda(n). \qquad (3.14)$$

3.2 A Kohnen-Zagier Type Formula

Let N be odd and square-free and let $g \in S^{new}_{k+1/2}(4N)$ be a newform in Kohnen's plus space. Let $G \in S^{new}_{2k}(N)$ be the Shimura lift of g normalized so that $a_G(1) = 1$. Let w_l be the sign of the Atkin-Lehner involution W_l for each prime l dividing N. For a fundamental discriminant D and $\mathrm{Re}(s) > k + 1/2$, let

$$L(G, D, s) := \sum_{n \geq 1} \chi_D(n) a_G(n) n^{-s}$$

be the twisted Hecke L-function of G by χ_D.

Lemma 3.9. *Let $(-1)^k D$ be a fundamental discriminant such that for each prime divisor l of N, either $\left(\frac{D}{l}\right) = w_l$ or $\left(\frac{D}{l}\right) = 0$. Then*

$$\frac{|a_g(D)|^2}{< g, g >} = 2^{v\left(\frac{N}{(N,D)}\right)} \cdot \frac{(k-1)!}{\pi^k} \cdot D^{k-1/2} \cdot \frac{L(G, (-1)^k D, k)}{< G, G >}, \tag{3.15}$$

Remark 3.10. *If the conditions of Lemma 3.15 are not satisfied, then Kohnen proved in [23] that $a_g(D) = 0$.*

Proof. For a binary quadratic form $Q = [a, b, c] = ax^2 + bxy + cy^2$ with discriminant $|Q| = b^2 - 4ac$ and an integer d, we define

$$\omega_d(Q) := \begin{cases} \left(\frac{d}{r}\right) & \text{if } \gcd(a, b, c, d) = 1 \text{ and } r \text{ is represented by } Q \\ 0 & \text{if } \gcd(a, b, c, d) > 1. \end{cases}$$

Next define for n, m with $(-1)^k n$ a discriminant and $(-1)^k m$ a fundamental discriminant, the period integral

$$r_{k,N}(G; (-1)^k n, (-1)^k m) := \sum_{\substack{Q \pmod{\Gamma_0(N)} \\ |Q| = nm,\ Q(1,0) \equiv 0 (\mathrm{mod}\ N)}} \omega_{(-1)^k m}(Q) \cdot \int_{C_Q} f(z) d_{Q,k} z,$$

where C_Q is the image of $\Gamma_0(N)\backslash\mathbb{H}$ of the semicircle $a|z|^2 + b\mathrm{Re}(z) + c = 0$ and $d_{Q,k}z = (az^2 + bz + c)^{k-1}dz$.

In [24], Kohnen proved that for any n, m with $(-1)^k n, (-1)^k m \equiv 0, 1 \pmod 4$ and $(-1)^k m$ a fundamental discriminant

$$\frac{a_g(n) \cdot \overline{a_g(m)}}{< g, g >} = \frac{(-1)^{\lfloor k/2 \rfloor} 2^k}{< G, G >} \cdot r_{k,N}(G; (-1)^k \cdot n, (-1)^k \cdot m). \tag{3.16}$$

Now assume that $n = m = D$ and $\left(\frac{(-1)^k D}{l}\right)$ is as above for each $l \mid N$. A full set of representatives of the quadratic forms $Q \pmod{\Gamma_0(N)}$ with discriminant D^2 and $Q(1, 0) \equiv 0 \pmod N$ are given by

$$\{Q_u \circ W_t : \ u \pmod D, t \mid N, t > 0\},$$

with $Q_u = [0, (-1)^k D, u]$, $W_t = \frac{1}{\sqrt{t}} \begin{pmatrix} t & \alpha \\ N & t\beta \end{pmatrix}$, and $t^2\beta - N\alpha = t$.

Claim 3.11.

$$\omega_{(-1)^k D}(Q_u \circ W_t) = \left(\frac{(-1)^k D}{t}\right) \omega_{(-1)^k D}(Q_u).$$

Proof. An easy calculation shows that $Q_u \circ W_t$ is

$$\left[\frac{N}{t} Nu + ND, uD\alpha\frac{N}{t} + t\beta D + 2uN\beta, uD\alpha\beta + ut\beta^2\right] =: [a, b, c].$$

We first note that $\gcd(t, D, N) \mid \gcd(a, b, c, D)$. Since $t \mid N$ it follows that $\gcd(t, D) \mid \gcd(a, b, c, D)$. Therefore, if $\gcd(t, D) \neq 1$, then $\omega_D(Q_u \circ W_t) = 0$.

Now assume that $\gcd(t, D) = 1$. Since $t\beta + \frac{N}{t}\alpha = 1$, there exist $x, y \in \mathbb{Z}$ such that

$y\beta + x\frac{N}{t} = 1$. Then, since the modulus of the character $\left(\frac{D}{\cdot}\right)$ is $|D|$, we know that

$$\left(\frac{(-1)^k D}{N(\frac{N}{t}u + D)x^2 + (uD\alpha\frac{N}{t} + t\beta D + 2uN\beta)xy + u(D\alpha\beta + t\beta^2)y^2}\right)$$

$$= \left(\frac{(-1)^k D}{(\frac{N}{t}Nu)x^2 + (2uN\beta)xy + (ut\beta^2)y^2}\right) = \left(\frac{(-1)^k D}{ut\left(\left(\frac{N}{t}\right)^2 x^2 + (2\frac{N}{t}\beta)xy + \beta^2 y^2\right)}\right)$$

$$= \left(\frac{(-1)^k D}{ut\left(x\frac{N}{t} + y\beta\right)^2}\right) = \left(\frac{(-1)^k D}{ut}\right) = \left(\frac{(-1)^k D}{u}\right)\left(\frac{(-1)^k D}{t}\right).$$

This is the desired result. □

An easy calculation shows that

$$\omega_{(-1)^k D}(Q_u \circ W_t) = \left(\frac{(-1)^k D}{t}\right)\omega_{(-1)^k D}(Q_u).$$

Given the assumptions above we get:

$$r_{k,N}(G; (-1)^k D, (-1)^k D) = \sum_{t|N}\sum_{u \pmod N} \omega_{(-1)^k D}(Q_u \circ W_t)\int_{C_{Q_u}} (G|W_t)(z) d_{Q_{u,k}}(W_t z)$$

$$= \sum_{t|N}\left(\frac{(-1)^k D}{t}\right)\sum_{u \pmod N} \omega_{(-1)^k D}(Q_u)\int_{C_{Q_u}} (G|W_t)(z) d_{Q_{u,k}}(W_t z)$$

$$= \sum_{t|\frac{N}{(N,D)}}\left(\frac{(-1)^k D}{t}\right)\sum_{u \pmod N} \omega_{(-1)^k D}(Q_u)\int_{C_{Q_u}} (G|W_t)(z) d_{Q_{u,k}}(W_t z)$$

$$= \sum_{t|\frac{N}{(N,D)}}\left(\frac{(-1)^k D}{t}\right)\sum_{u \pmod N} \omega_{(-1)^k D}(Q_u)\int_{C_{Q_u}} \left(\frac{(-1)^k D}{t}\right)\cdot G(z) d_{Q_{u,k}}(W_t z)$$

$$= \left(\sum_{t|\frac{N}{(N,D)}} 1\right)\sum_{u \pmod N}\left(\frac{(-1)^k D}{u}\right)\int_{-u/((-1)^k D)}^{i\infty} G(z)((-1)^k Dz + u)^{k-1} dz$$

$$= 2^{v(\frac{N}{(N,D)})}\sum_{u \pmod N}\left(\frac{(-1)^k D}{u}\right)\int_{-u/(-1)^k D}^{i\infty} G(z)((-1)^k Dz + u)^{k-1} dz$$

$$= 2^{v(\frac{N}{(N,D)})}(Di)^{k-1} i \sum_{u \pmod N} \left(\frac{(-1)^k D}{u}\right) \int_0^\infty G\left(-\frac{u}{(-1)^k D} + it\right) t^{k-1} dt$$

$$= 2^{v(\frac{N}{(N,D)})}(Di)^{k-1} i \int_0^\infty \sum_{u \pmod N} \left(\frac{(-1)^k D}{u}\right) \sum_{n \geq 1} a_G(n) \cdot e^{-2\pi n t} e^{-2\pi i n \frac{u}{(-1)^k D}} t^{k-1} dt$$

$$= 2^{v(\frac{N}{(N,D)})}(Di)^{k-1} i \int_0^\infty \sum_{n \geq 1} a_G(n) e^{-2\pi n t} t^{k-1} \left(\sum_{u (\mathrm{mod}\ N)} \left(\frac{(-1)^k D}{u}\right) e^{-2\pi i n \frac{u}{(-1)^k D}} \right) dt.$$

To continue, we need to use some theory about Gauss sums. For more information about Gauss sums, a common reference is [17].

We will see that if $\chi = \left(\frac{(-1)^k D}{\cdot}\right)$, then

$$\sum_{u \pmod D} \left(\frac{-(-1)^k D}{u}\right) e^{-2\pi i n u/(-1)^k D} = \left(\frac{(-1)^k D}{-1}\right) \sum_{u \pmod D} \left(\frac{(-1)^k D}{u}\right) e^{2\pi i n u/(-1)^k D}$$

$$= \chi(-1)\tau(\chi)\chi(n) = \left(\frac{(-1)^k D}{-1}\right) \tau(\chi) \left(\frac{(-1)^k D}{n}\right),$$

where $\tau(\chi)$ is the associated Gauss sum. One then sees that the above equality is simply a restatement of

$$\sum_{t \pmod D} \chi(t)\zeta^{at} =: \tau_a(\chi) = \overline{\chi}(a)\tau(\chi)$$

with $\zeta = e^{2\pi i/(-1)^k D}$. Using this identity and the fact that χ is a real character, we get the well known identity

$$\tau(\chi) = \sqrt{\chi(-1)} \cdot \sqrt{D}.$$

Plugging this in above gives

$$\sum_{u \pmod D} \left(\frac{(-1)^k D}{u}\right) e^{-2\pi i n u/(-1)^k D} = \chi(-1)\tau(\chi)\chi(n) = \left(\frac{(-1)^k D}{-1}\right)^{\frac{3}{2}} \cdot D^{1/2} \cdot \left(\frac{(-1)^k D}{n}\right).$$

Replacing the inner sum above gives

$$
\begin{aligned}
& 2^{v\left(\frac{N}{(N,D)}\right)}(Di)^{k-1} i \int_0^\infty \sum_{n\geq 1} a_G(n) e^{-2\pi n t} t^{k-1} \left(\sum_{u \pmod N} \left(\frac{(-1)^k D}{u}\right) e^{-2\pi i n \frac{u}{(-1)^k D}} \right) dt \\
= \quad & 2^{v\left(\frac{N}{(N,D)}\right)}(Di)^{k-1} i \left(\frac{(-1)^k D}{-1}\right)^{3/2} D^{1/2} \sum_{n\geq 1} a_G(n) \left(\frac{(-1)^k D}{n}\right) \int_0^\infty e^{-2\pi n t} t^{k-1} dt \\
= \quad & 2^{v\left(\frac{N}{(N,D)}\right)} D^{k-1/2} (-1)^{k/2} \left(\frac{(-1)^k D}{-1}\right)^{k+1/2} \Gamma(k)(2\pi)^{-k} L(G,(-1)^k D, k).
\end{aligned}
$$

Here we use the analytic continuation of the Gamma function in the final equality. Plugging this into Equation 3.16 yields

$$
\frac{|a_g(D)|^2}{< g, g >} = \frac{2^{v\left(\frac{N}{(N,D)}\right)}(k-1)!(-1)^{\lfloor k/2 \rfloor + k/2} \left(\frac{(-1)^k D}{-1}\right)^k \left(\frac{(-1)^k D}{-1}\right)^{1/2}}{\pi^k < G, G >} D^{k-1/2} L(G,(-1)^k D, k).
$$

Notice further that

$$
(-1)^{\lfloor k/2 \rfloor + k/2} \left(\frac{(-1)^k D}{-1}\right)^{k+1/2} = 1.
$$

This yields the desired equality.

□

3.3 Bounding Non-Fundamental Discriminant Coefficients

In this section we employ the power of the Hecke operators and the Shimura lift to obtain information about $-d$ non-fundamental. The argument also repeatedly uses the simple fact that $a_\theta(Dl^2) = 0$ implies $a_\theta(D) = 0$.

Due to the nature of such proofs, many of the results in this section do not require GRH. The results requiring GRH make this assumption to use the bound obtained in Section 3.7 for squarefree coefficients to obtain an overall bound.

Lemma 3.12. *Fix a fundamental discriminant* $-D$ *and* F *with* $(F,p)=1$. *Define* $F' := \prod_{l|F} l$. *Then*

$$|a_{g_i}(DF^2)| \leq \sigma_{-\frac{1}{2}}(F')F^{\frac{1}{2}}\sigma_0(F)|a_{g_i}(D)|, \tag{3.17}$$

where $\sigma_k(n)$ *is defined in equation (3.12).*

Proof. First note that if $a_{g_i}(D)=0$, then $a_{g_i}(DF^2)=0$ by the Hecke operators, so the result follows trivially.

We will use here the D-th Shimura correspondence [32] instead of the Shimura lift, similar to the argument in [11]. Recall that the Shimura correspondence $G_{D,i} \in S_2(2p)$ of g_i satisfies

$$\sum_n \frac{a_{G_{D,i}}(n)}{n^s} := L(s,\chi_{-D})\sum_{n=1}^{\infty}\frac{a_{g_i}(Dn^2)}{n^s}.$$

We will show that if $G=l^m$ such that $m \geq 1$ and $(G,F)=1$, then

$$a_{g_i}(D(FG)^2) = \frac{a_{g_i}(DF^2)}{a_{g_i}(D)}\left[a_{G_{D,i}}(G) - \left(\frac{-D}{l}\right)a_{G_{D,i}}\left(\frac{G}{l}\right)\right]. \tag{3.18}$$

Using equation (3.18), we get the result easily by multiplicativity and Deligne's optimal bound [7] for integer weight eigenforms, which shows that

$$\left|a_{G_{D,i}}(G) - \left(\frac{-D}{l}\right)a_{G_{D,i}}\left(\frac{G}{l}\right)\right| \leq \left(1+\frac{1}{l^{\frac{1}{2}}}\right)\sigma_0(G)G^{\frac{1}{2}}|a_{G_{D,i}}(1)|.$$

We then use the fact that $a_{G_{D,i}}(1) = a_{g_i}(D)$. We now return to showing equation (3.18). Using the multiplicativity of the coefficients of $G_{D,i}$ normalized and the D-th Shimura Correspondence, we obtain

$$\begin{aligned} a_{G_{D,i}}(F)a_{G_{D,i}}(G) = a_{G_{D,i}}(FG)a_{G_{D,i}}(1) &= \sum_{n|FG} a_{g_i}(D)a_{g_i}(Dn^2)\left(\frac{-D}{FG/n}\right) \\ &= \left(\frac{-D}{l}\right)a_{G_{D,i}}(F)a_{G_{D,i}}(G/l) + \sum_{f|F} a_{g_i}(D)a_{g_i}(DG^2f^2)\left(\frac{-D}{F/f}\right). \end{aligned}$$

Rearranging and using the D-th Shimura Correspondence again for $a_{G_{D,i}}(F)$, we obtain

$$0 = \sum_{f|F} \left(a_{g_i}(DG^2 f^2) a_{g_i}(D) - a_{g_i}(Df^2) \left[a_{G_{D,i}}(G) - \left(\frac{-D}{l}\right) a_{G_{D,i}}(G/l) \right] \right) \left(\frac{-D}{F/f}\right).$$

Hence equation (3.18) follows by induction on the number of divisors of F. □

Theorem 3.13. *If $a_\theta(DF^2) = 0$, then*

$$\frac{F^{\frac{1}{2}}}{2^{v(F)}\sigma_{-\frac{1}{2}}(F')\sigma_0(F)} \leq \frac{(p-1)\pi 2^{\frac{v_p(D)}{2}}}{12} D^{-\frac{1}{4}} \cdot \left(\sum_{i=1}^{m} |b_i|^2\right)^{\frac{1}{2}} \cdot \left(\sum_{i=1}^{m} c_i \frac{L_i(1)}{L(1)^2}\right)^{\frac{1}{2}}. \tag{3.19}$$

Here c_i and b_i are given by Equations (3.7) and (1.1), respectively.

Proof. Plugging equation (3.17) into formula (3.9) yields the desired result. □

Proof of Theorem 3.6(Assuming Theorem 1.2). Without loss of generality, let $-d = -D$ be a fundamental discriminant. If $a_\theta(DF^2) = 0$ then using the index formula(see [4]) and Lemma 3.12 yields

$$\frac{F}{2^{v(F)}} \leq \frac{a_E(DF^2)}{a_E(D)} = \frac{\sum_{i=1}^{m} b_i a_{g_i}(DF^2)}{a_E(D)} \leq \frac{\sigma_{-\frac{1}{2}}(F') F^{\frac{1}{2}} \sigma_0(F) \sum_{i=1}^{m} |b_i| \cdot |a_{g_i}(D)|}{a_E(D)}.$$

First we bound $a_E(D)$ trivially from below by $\frac{3}{p-1}$. Now the result follows by using Duke's effective subconvexity bound for Hecke Eigenforms of weight 3/2 [9] to bound $|a_{G_i}(D)| \ll_\epsilon D^{\frac{3}{7}+\epsilon}$.

The remaining assertions follow by improved effective estimates under additional assumptions. Under the Riemann Hypothesis for Dirichlet L-functions, Littlewood bounds $a_E(D)$ from below by $\frac{3}{p-1}\frac{D^{\frac{1}{2}}}{\log(\log(D))}$ [26]. Finally, we will see by Corollary 3.1 that under the assumption of the Riemann Hypothesis for weight 2 modular forms, $|a_{g_i}(D)| \ll_\epsilon D^{\frac{1}{4}+\epsilon}$. □

We next deal with the case $F = p$.

Lemma 3.14. *Fix $\theta \in M^{+}_{3/2}(4p)$. Then $a_\theta(dp^2) = 0$ if and only if $a_\theta(d) = 0$.*

Proof. Note first that $E|U(p^2) = E$. Moreover, $g_i|U(p^2) = \pm g_i$ (cf. [28]). Therefore, we easily see that

$$\theta|U(p^4) = \theta.$$

This shows the desired result, after noting that, since θ is a theta series,

$$a_\theta(d) \leq a_\theta(dp^2) \leq a_\theta(dp^4).$$

□

Theorem 3.4 involves showing a connection between $a_\theta(df^2) = 0$ and the following two recursively defined polynomials.

Definition 3.15. *Set $m, n \in \mathbb{Z}$, and $\epsilon \in \{-1, 0, 1\}$. Define the polynomial $P_{n,m,\epsilon}(x)$ recursively as follows:*

$$P_{n,m,\epsilon}(x) := \begin{cases} 0 & \text{if } n < 0 \text{ or } m < 0, \\ 1 & \text{if } n{=}0, \\ (x-\epsilon)P_{n-1,1,\epsilon}(x) + \epsilon P_{n-1,0,\epsilon} & \text{if } m = 0,\ n > 0, \\ xP_{n-1,2,\epsilon}(x) + \left(\frac{x}{x-\epsilon}\right) P_{n-1,0,\epsilon} & \text{if } m = 1,\ n > 0, \\ xP_{n-1,m+1,\epsilon}(x) + P_{n-1,m-1,\epsilon} & \text{if } m \geq 1,\ n > 0. \end{cases}$$

Definition 3.16. *For $d \in \mathbb{N}$ and l a prime with $l^2 \nmid d$, define*

$$Q_{n,m}(l) := \frac{\sum_i b_i a_{G_i}(l)^n a_{g_i}(dl^{2m})}{-a_E(dl^{2m})}.$$

Theorem 3.17. *Let $-d$ be a discriminant and $l \neq p$ prime. Then $a_\theta(dl^{2m+2n}) = 0$ if and only if*

$$P_{r,s,\left(\frac{-D}{l}\right)}(l) = Q_{r,s}(l),$$

for every $r \leq n$ and $s \leq m$ and $-D$ is the fundamental discriminant associated with d.

Proof. When $n = 0$, the result is obvious, since this equality simply gives

$$1 = \frac{\sum_i b_i a_{g_i}(dl^{2s})}{-a_E(dl^{2s})}.$$

We proceed by induction on n. We note first that $a_\theta(dl^{2m}l^{2n+2}) = 0$ if and only if $a_\theta(dl^{2m+2}l^{2n}) = 0$. Therefore, by inductive hypothesis, $a_\theta(dl^{2m}l^{2n+2}) = 0$ if and only if

$$P_{r,s,\left(\frac{-D}{l}\right)}(l) = Q_{r,s}(l),$$

for every $r \leq n$ and $s \leq m+1$. These conditions match up with the assumptions above other than when $s = m+1$. Thus, it suffices to show assuming $P_{r,s,\left(\frac{-D}{l}\right)}(l) = Q_{r,s}(l)$ for every $r \leq n$ and $s \leq m$ implies that

$$P_{r,m+1,\left(\frac{-D}{l}\right)}(l) = Q_{r,m+1}(l),$$

for every $r \leq n$, is equivalent to

$$P_{n+1,s,\left(\frac{-D}{l}\right)}(l) = Q_{r,s}(l),$$

for every $s \leq m$.

Let $r \leq n$ be given. Using the definition of $Q_{r,m+1}(l)$, we have

$$Q_{r,m+1}(l) = \frac{\sum_i b_i a_{G_i}(l)^r a_{g_i}(Dl^{2m+2})}{-a_E(Dl^{2m+2})}.$$

Since g_i is a hecke Eigenform with G_i the normalized Shimura lift, and $a_{G_i}(1) = 1$, we have

$$\frac{\sum_i b_i a_{G_i}(l)^r a_{g_i}(Dl^{2m+2})}{-a_E(Dl^{2m+2})} = \frac{\sum_i b_i a_{G_i}(l)^{r+1} a_{g_i}(Dl^{2m})}{-a_E(Dl^{2m+2})} - \left(\frac{-Dl^{2m}}{l}\right)\frac{\sum_i b_i a_{G_i}(l)^r a_{g_i}(Dl^{2m})}{-a_E(Dl^{2m+2})} - l\left(\frac{\sum_i b_i a_{G_i}(l)^r a_{g_i}(Dl^{2m-2})}{-a_E(Dl^{2m+2})}\right).$$

Now, we note by the index formula (see [4]) that

$$\frac{-a_E(Dl^{2m+2})}{-a_E(Dl^{2m})} = l - \left(\frac{Dl^{2m}}{l}\right).$$

Therefore, it follows that

$$\begin{aligned}\left(l - \left(\frac{Dl^{2m}}{l}\right)\right) Q_{r,m+1}(l) &= \frac{\sum_i b_i a_{G_i}(l)^{r+1} a_{g_i}(Dl^{2m})}{-a_E(Dl^{2m})} \\ - \left(\frac{-Dl^{2m}}{l}\right) \frac{\sum_i b_i a_{G_i}(l)^{r} a_{g_i}(Dl^{2m})}{-a_E(Dl^{2m})} &- \frac{l}{l - \left(\frac{Dl^{2m-2}}{l}\right)} \cdot \frac{\sum_i b_i a_{G_i}(l)^{r} a_{g_i}(Dl^{2m-2})}{-a_E(Dl^{2m-2})} \\ &= Q_{r+1,m}(l) - \left(\frac{-Dl^{2m}}{l}\right) Q_{r,m}(l) - \frac{l}{l - \left(\frac{Dl^{2m-2}}{l}\right)} \cdot Q_{r,m-1}(l).\end{aligned}$$

Now, assume that $Q_{r,m+1}(l) = P_{r,m+1,\epsilon}$. By assumption, we also have $Q_{r,m} = P_{r,m,\epsilon}$ and $Q_{r,m-1} = P_{r,m-1,\epsilon}$. Therefore, rearranging the above formula gives

$$Q_{r+1,m}(l) = \left(l - \left(\frac{Dl^{2m}}{l}\right)\right) P_{r,m+1,\epsilon}(l) + \left(\frac{-Dl^{2m}}{l}\right) P_{r,m,\epsilon}(l) + \frac{l}{l - \left(\frac{Dl^{2m-2}}{l}\right)} \cdot P_{r,m-1,\epsilon}(l).$$

If $m \geq 2$, then the right hand side is

$$lP_{r,m+1,\epsilon}(l) + P_{r,m-1,\epsilon}(l) = P_{r+1,m,\epsilon}(l),$$

as desired. If $m = 1$, the right hand side is

$$lP_{r,m+1,\epsilon}(l) + \left(\frac{-D}{l}\right) P_{r,m-1,\epsilon}(l) = P_{r+1,m,\epsilon}(l).$$

Notice that we used $l^2 \nmid D$ above so that $\left(\frac{-D}{l}\right) = \left(\frac{-D'}{l}\right)$. Finally, if $m = 0$, we use the same observation above to see that the right hand side is

$$\left(l - \left(\frac{D}{l}\right)\right) P_{r,m+1,\epsilon}(l) + \left(\frac{-D}{l}\right) P_{r,m,\epsilon}(l) = P_{r+1,m,\epsilon}(l).$$

□

Theorem 3.18 (Theorem 3.4)**.** *Let $-d$ be a discriminant and $(F,p)=1$. Then $a_\theta(dF^2)=0$ if and only if for every f dividing F, with $f=\prod_{l\ prime} l^{n_{l,f}}$ and $m_l := \lfloor \frac{v_l(d)}{2} \rfloor$, we have*

$$\prod_{l\ prime} P_{r_l,s_l,\left(\frac{-D}{l}\right)}(l) = \frac{\sum_i b_i \prod_{l\ prime} a_{G_i}(l)^{r_l} a_{g_i}\left(\frac{d}{\prod_{l\ prime} l^{2s_l}}\right)}{-a_E\left(\frac{d}{\prod_{l\ prime} l^{2s_l}}\right)},$$

for every $r_l \le n_{l,f}$ and $s_l \le m_l$, where $-D$ is the fundamental discriminant corresponding to the discriminant $-d$.

Proof. For F a prime power, this is exactly Theorem 3.17. Thus, we will continue by induction on the number of prime divisors of F. Let $F' = Fq^n$ with $(F,q)=1$ and assume the theorem for F. We will continue by induction on n as in the proof of Theorem 3.17. The $n=0$ case is the inductive hypothesis above. Assume the result for n. Then $a_\theta(DF^2q^{2n+2}) = a_\theta((Dq^2)F^2q^{2n})$. Using Dq^2 for D, the inductive hypothesis gives us the result if and only if

$$\prod_{l\neq q \text{ prime}} P_{r_l,s_l,\left(\frac{-D'}{l}\right)}(l) P_{r,s,\left(\frac{-D'}{q}\right)}(q) = \frac{\sum_i b_i \prod_{l\neq q \text{ prime}} a_{G_i}(l)^{r_l} a_{G_i}(q)^r a_{g_i}\left(\frac{D}{\prod_{l\neq q \text{ prime}} l^{2s_l} q^{2s}}\right)}{-a_E\left(\frac{D}{\prod_{l\neq q \text{ prime}} l^{2s_l} q^{2s}}\right)},$$

for every $r_l \le n_{l,f}$, $s_l \le m_l$, $r \le n$, and $s \le m_l + 1$.

We again assume this for every $r_l \le n_{l,f}$, $s_l \le m_l$, $r \le n$, and $s \le m_l$ and show that the equality holds for $r_l \le n_{l,f}$, $s_l \le m_l$, $r \le n$, and $s \le m_l + 1$ if and only if it holds for $r_l \le n_{l,f}$, $s_l \le m_l$, $r \le n+1$, and $s \le m_l$. Defining

$$Q_{r,s} := \frac{\sum_i b_i \prod_{l\neq q \text{ prime}} a_{G_i}(l)^{r_l} a_{G_i}(q)^r a_{g_i}\left(\frac{D}{\prod_{l\neq q \text{ prime}} l^{2s_l} q^{2s}}\right)}{-a_E\left(\frac{D}{\prod_{l\neq q \text{ prime}} l^{2s_l} q^{2s}}\right)},$$

and using the Hecke operators yields the result exactly as in Theorem 3.17. ☐

Remark 3.19. *Notice that for any genus where the Eisenstein series satisfies*

$$\frac{a_E(Dl^2)}{a_E(D)} = l - \chi(D)\left(\frac{-D}{l}\right),$$

where χ is the Nebentypus, the above proof follows mutatis mutandis.

Remark 3.20. *We will in practice use $-D$ a fundamental discriminant, but the induction required us to use a more general D. For $x \geq 1$, the recursive definition of $P_{n,m,\epsilon}(x)$ implies that $P_{n,m\epsilon}(x) \geq x^n$. Therefore, the product above is greater than or equal to f.*

Corollary 3.21. *If $\theta = E + g$ with g an eigenform, and G the Shimura lift of g, then $a_\theta(DF^2) \neq 0$ for every $F \nmid 6$ with $F \neq p^n$.*

Proof. For contradiction, let D, l be such that $a_\theta(Dl^2) = 0$ with $l > 3$, $l \neq p$ prime. Then $a_\theta(D) = 0$, so

$$1 = \frac{a_g(D)}{-\frac{12}{p-1}H_p(D)},$$

and hence

$$l = a_G(l) \cdot \frac{a_g(D)}{-\frac{12}{p-1}H_p(D)} = a_G(l)$$

by Theorem 3.17. But $a_G(l) \leq 2\sqrt{l}$, and $l \leq 2\sqrt{l}$ is impossible.

Now assume that $a_\theta(Dl^4) = 0$, where $l = 2$ or $l = 3$. Then Theorem 3.17 and the fact that $P_{2,0,\epsilon}(l) = l^2 + l - \left(\frac{D}{l}\right)$ imply that

$$l = a_{G_i}(l)$$

and

$$l^2 + l - \left(\frac{D}{l}\right) = a_{G_i}(l)^2.$$

But this would imply $l^2 + l - \left(\frac{D}{l}\right) = l^2$, which is a clear contradiction. ☐

Corollary 3.22. *If $\theta = E + b_1g_1 + b_2g_2$, then for $l \geq 5$ a prime and $-D$ a discriminant,*

$$a_\theta(Dl^4) \neq 0.$$

Moreover, if q is another prime with $(q, 6pl) = 1$, then

$$a_\theta(Dl^2q^2) \neq 0$$

Proof. It suffices to show the result for $-D$ a fundamental discriminant. Let a fundamental discriminant $-D$ be given such that $a_\theta(D) = 0$. Then $a_\theta(Dl^4) = 0$ if and only if

$$Q_{1,0} = P_{1,0,\left(\frac{-D}{l}\right)}(l)$$

and

$$Q_{2,0} = P_{2,0,\left(\frac{-D}{l}\right)}(l).$$

For simplicity, we will denote $P_{k,0,\left(\frac{-D}{l}\right)}(l) = P_k$. Using the recursive definition of P_k, we have $P_1 = l$ and $P_2 = l^2 + l - \left(\frac{-D}{l}\right)$. Therefore, if we denote

$$a_i := \frac{b_i a_{g_i}(D)}{-a_E(D)}$$

and

$$x_i = a_{G_i}(l),$$

then, using $a_1 + a_2 = 1$ from $a_\theta(D) = 0$, the two equalities above become

$$x_1a_1 + x_2a_2 = la_1 + la_2 \tag{3.20}$$

and

$$x_1^2a_1 + x_2^2a_2 = \left(l^2 + l - \left(\frac{-D}{l}\right)\right)a_1 + \left(l^2 + l - \left(\frac{-D}{l}\right)\right)a_2. \tag{3.21}$$

We will show that these equations are inconsistent with $|x_i| \leq 2\sqrt{l}$.

Taking the ratio $\frac{a_1}{a_2}$ in both equations, we have

$$\frac{l-x_2}{x_1-l}=\frac{l^2+l-\left(\frac{-D}{l}\right)-x_2^2}{x_1^2-l^2-l+\left(\frac{-D}{l}\right)},$$

so that

$$(l-x_2)\left(x_1^2-l^2-l+\left(\frac{-D}{l}\right)\right)=(x_1-l)\left(l^2+l-\left(\frac{-D}{l}\right)-x_2^2\right).$$

Rearranging yields

$$-x_1x_2(x_1-x_2)+l(x_1+x_2)(x_1-x_2)-(l^2+l-\left(\frac{-D}{l}\right))(x_1-x_2)=0.$$

Solving this yields the two solutions

$$x_1=x_2$$

or

$$x_1=\frac{l^2+l-\left(\frac{-D}{l}\right)-lx_2}{l-x_2}=l+\frac{l-\left(\frac{-D}{l}\right)}{l-x_2}.$$

In the second equality we have assumed $x_2 \neq l$, but since $|x_2| \leq 2\sqrt{l}$ and $l \geq 5$ this is an empty assumption. Now note that the second equation implies that if $x_2 < l$ then we have $x_1 > l$, which leads to a contradiction since $l > 2\sqrt{l}$.

Thus, only the case $x_1 = x_2$ remains. In this case, our two equations become

$$x_1(a_1+a_2)=l(a_1+a_2)$$

and

$$x_1^2(a_1+a_2)=\left(l^2+l-\left(\frac{-D}{l}\right)\right)(a_1+a_2).$$

But then it follows, by squaring the first equation, that

$$l^2=l^2+l-\left(\frac{-D}{l}\right),$$

which yields another contradiction.

Now assume that $a_\theta(Dl^2q^2) = 0$. Define $x_i := a_{G_i}(l)$, $y_i := a_{G_i}(q)$. Then Theorem 3.4 implies that the following 3 equations hold:

$$x_1a_1 + x_2a_2 = la_1 + la_2$$
$$y_1a_1 + y_2a_2 = qa_1 + qa_2$$
$$x_1y_1a_1 + x_2y_2a_2 = lqa_1 + lqa_2.$$

Taking the third equation minus l times the second yields

$$y_1(x_1 - l)a_1 + y_2(x_2 - l)a_2 = 0.$$

Since the first equation implies that

$$(x_1 - l)a_1 + (x_2 - l)a_2 = 0,$$

and $x_i < l$, it follows that $y_1 = y_2 = q$. But this contradicts the fact that $y_1 \leq 2\sqrt{q}$. $\square$

Example 3.23. *Ono and Soundararajan showed for* $Q_1 = [1, 1, 10, 0, 0, 0]$ *that* $a_\theta(Dl^2) \neq 0$ *for all* l*. However, a simple calculation shows for* $Q_2 = [8, 12, 23, 4, 0, 0]$ *that* $a_\theta(27) = 0$*, so this result cannot hold in general. This form comes from one of the Gross lattices [14]. The dimension of the cuspidal subspace containing the form* Q_2 *in this example is 2, exactly as above.*

3.4 Review of the Work of Ono and Soundararajan

In this section, we review some results of Ono and Soundararajan [29] in preparation for bounding $L(s)$ and $L_i(s)$ in the next two sections. Recall $\chi := \chi_{-D}$, $L(s) := L(\chi, s)$, $L_i(s) := L(G_i, -D, s)$, and $F(s) = F_i(s)$.

3.4.1 Explicit Formulas

We will use the following 2 lemmas from [29] for explicit formulas of $\frac{L'}{L}(s)$ and $\frac{L_i'}{L_i}(s)$. These formulas are derived by studying an integral and shifting the line of integration, giving $\frac{L'}{L}(s)$ or $\frac{L_i'}{L_i}(s)$ as one of the residues.

Lemma 3.24 (Ono-Soundararajan [29])**.**

$$-\frac{L'}{L}(s) = \boldsymbol{G}_1(s, \boldsymbol{X}) + E_{sig}(s) - \frac{L'}{L}(s-1)\boldsymbol{X}^{-1} - R(s),$$

where

$$E_{sig}(s) = \sum_{\rho} \boldsymbol{X}^{p-s}\Gamma(p-s), \text{ and } R(s) = \frac{1}{2\pi i}\int_{-\sigma-1/2-i\infty}^{-\sigma-1/2+i\infty} -\frac{L'}{L}(s+w)\Gamma(w)\boldsymbol{X}^{w}dw$$

and

$$\boldsymbol{G}_1(s, \boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} e^{-n/\boldsymbol{X}}, \tag{3.22}$$

with Λ the Von-Mangoldt function. Here ρ denote the nontrivial zeros of $L(s)$.

Proof. The proof follows by taking for $c > 0$

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s+w)\Gamma(w)\boldsymbol{X}^{w}dw,$$

and moving the line of integration to the far left. This yields

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{L'}{L}(s+w)\Gamma(w)\boldsymbol{X}^{w}dw = G_1(s, \boldsymbol{X}).$$

Moving the line of integration to real part $-\sigma - \frac{1}{2}$ gives a pole at $w = 0$ with residue $-\frac{L'}{L}(s)$. The poles at $w = \rho - s$ contribute $-E_{sig}(s)$, and finally the pole at $w = -1$ contributes $\frac{1}{\boldsymbol{X}} \cdot \frac{L'}{L}(s-1)$. ∎

Lemma 3.25 (Ono-Soundararajan [29])**.** *If $L_i(s) \neq 0$, then*

$$-\frac{L_i'}{L_i}(s) = \boldsymbol{F}_1(s, \boldsymbol{X}) + R_{sig}(s) + R_{tri}(s) + R_{ins}(s),$$

where

$$\boldsymbol{F}_1(s, \boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\lambda_i(n)\chi(n)}{n^s} e^{-n/\boldsymbol{X}} \tag{3.23}$$

with λ_i defined such that for $Re(s) > 3/2$

$$\frac{L_i'}{L_i}(s) = \sum_{n=1}^{\infty} \frac{\lambda_i(n)\chi(n)}{n^s},$$

$$R_{sig}(s) = \sum_{\rho_i} \boldsymbol{X}^{\rho_i - s}\Gamma(\rho_i - s), \quad R_{tri}(s) = \sum_{n=0}^{\infty} \boldsymbol{X}^{-n-s}\Gamma(-n-s),$$

and

$$R_{ins}(s) = \sum_{n=1}^{\infty} \frac{(-\boldsymbol{X})^{-n}}{n!} \cdot \frac{L_i'}{L_i}(s-n).$$

Here ρ_i are the nontrivial zeros of L_i.

Proof. This follows similarly to above, taking the integral

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{L_i'}{L_i}(s+w)\Gamma(w)\boldsymbol{X}^w dw$$

and getting residues at each of the poles.

□

We will fix i and investigate $F(s) := F_i(s)$. Then

$$\frac{F'}{F}(s) = \log\left(\frac{\sqrt{q}}{2\pi}\right) + \frac{L_i'}{L_i}(s) + \frac{\Gamma'}{\Gamma}(s) - \frac{L'}{L}(s) + \frac{L'}{L}(2-s)$$

3.4.2 Bounds for $\frac{\Gamma'}{\Gamma}$

We will need bounds for $\frac{\Gamma'}{\Gamma}$, and will use the bounds obtained in [29].

Lemma 3.26 (Ono-Soundararajan [29]). *Set $s = x + iy$.*

1) If $x \geq 1$, then

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leq \frac{11}{3} + \frac{\log(1+x^2)}{2} + \frac{\log(1+y^2)}{2}. \tag{3.24}$$

2) If $x > 0$, then we have the bound

$$Re\left(\frac{\Gamma'}{\Gamma}(s)\right) \leq \frac{\Gamma'}{\Gamma}(x) + \frac{y^2}{x|s|^2} + \log\left(\frac{|s|}{x}\right). \tag{3.25}$$

3) In general, one has

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leq \frac{9}{2} + \frac{1}{< x > (1- < x >)} + \log(2+|x|) + \frac{\log(1+y^2)}{2}, \tag{3.26}$$

where $< x > := \underset{n\in\mathbb{N}}{min}|x+n|$.

Lemma 3.27. *If $0 < x < 1$, then*

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leq \frac{11}{3} + \frac{\log(2)}{2} + \frac{1}{x} + \frac{\log(1+y^2)}{2}. \tag{3.27}$$

Proof. This follows from

$$\left|\frac{\Gamma'}{\Gamma}(s)\right| \leq \frac{1}{|s|} + \left|\frac{\Gamma'}{\Gamma}(s+1)\right|,$$

and Lemma 3.26, since $\frac{1}{|s|} \leq \frac{1}{x}$ and $\log(1+x^2) \leq \log(2)$. □

Lemma 3.28 (Ono-Soundararajan [29]). *If $L(s) \neq 0$ then*

$$Re\left(\frac{L'}{L}(s)\right) = -\frac{1}{2}\log(m) - \frac{1}{2}Re\left(\frac{\Gamma'}{\Gamma}\left(\frac{s+1}{2}\right)\right) + \sum_{\rho} Re\left(\frac{1}{s-\rho}\right),$$

where the sum is taken over all non-trivial zeros ρ of $L(s)$.

Additionally, if $L_i(s) \neq 0$ *then*

$$Re\left(\frac{L_i'}{L_i}(s)\right) = -\frac{1}{2}\log\left(\frac{q}{4\pi^2}\right) - Re\left(\frac{\Gamma'}{\Gamma}(s)\right) + \sum_{\rho_i} Re\left(\frac{1}{s-\rho_i}\right),$$

where the sum is taken over all non-trivial zeros ρ_i *of* $L_i(s)$*.*

3.5 Bounding L(s) From Below

Fix $1 < \sigma < \frac{3}{2}$. For notational ease, define $s := \sigma + it$, $s_0 := 2 - \sigma + it$, and $\sigma_0 := \mathrm{Re}(s_0)$. Fix $\boldsymbol{X} > e^{\gamma + \frac{1}{\frac{3}{2}-\sigma}}$, recalling the euler constant γ in (3.13). In preparation for bounding $F(s)$, in this section we will find a bound from below for $\log\left(\left|\frac{L(s_0)}{L(s)}\right|\right)$, depending on $\boldsymbol{X}$, t, and σ. The techniques used below were developed by Ono and Soundararajan in [29]. In their application, they set $\sigma = \frac{7}{6}$. In doing so, the bound that they obtain is more astethically pleasing and easier to read, but when dealing with a larger number of forms it is desirable to allow σ to move in order to obtain a better bound for each form.

Set

$$\delta(\boldsymbol{X}) := \max_y \left| \int_{\sigma_0-1/2}^{\sigma-1/2} \boldsymbol{X}^{-u}\Gamma(-u+iy)du \right| \cdot \left(\frac{1}{2}\log\frac{y^2+(\sigma-1/2)^2}{y^2+(\sigma_0-1/2)^2}\right)^{-1}.$$

We note that since Γ decays exponentially in y and the other term only has polynomial growth, $\delta(\boldsymbol{X})$ is well defined. Recall our definition (3.22) of $\boldsymbol{G}_1$ and denote

$$\boldsymbol{G}(s,\boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s \log(n)} e^{-n/\boldsymbol{X}} = \int \boldsymbol{G}_1(w,\boldsymbol{X})dw. \tag{3.28}$$

The goal of this section is to prove the following.

Theorem 3.29. *Assume GRH for Dirichlet L-functions. Let* χ *be a primitive Dirichlet* *character of conductor m and let $L(s) = L(s,\chi)$. For $\boldsymbol{X} > e^{\gamma + \frac{1}{\frac{3}{2}-\sigma}}$ we have*

$$\log\frac{|L(s_0)|}{|L(s)|} \geq \frac{\boldsymbol{X}}{\boldsymbol{X} - 1 - \delta(\boldsymbol{X})\boldsymbol{X}} \Big(\mathit{Re}(\boldsymbol{G}(s_0,\boldsymbol{X})) - \mathit{Re}(\boldsymbol{G}(s,\boldsymbol{X})) + c_{\theta,\sigma,\boldsymbol{X},1} + c_{\theta,\sigma,\boldsymbol{X},t,1} + c_{\theta,\sigma,\boldsymbol{X},m,1}\Big),$$

where the constants are given by

$$\begin{aligned} c_{\theta,\sigma,\boldsymbol{X},1} := (\sigma-\sigma_0)&\frac{|\Gamma(3/2-\sigma_0)|}{2\pi \boldsymbol{X}^{\sigma_0+1/2}}\left(-r\pi\frac{891}{100} + \frac{\pi\log(226)}{2r^2} + \frac{2}{\sqrt{15}r^2}\right) \\ &- \frac{\sigma-\sigma_0}{2\boldsymbol{X}}\left(\frac{22}{3}+\frac{2}{\sigma_0}\right) - \frac{1-\sigma_0}{2\boldsymbol{X}}\left(\frac{\log(1+\left(\frac{3-\sigma_0}{2}\right)^2)}{2} + \frac{\log(2)}{2} + \frac{2}{\sigma_0}\right) \\ &-\left(\frac{\sigma-1}{2\boldsymbol{X}}\right)\left(\log(2)+\frac{2}{3-\sigma_0}\right) - 2\delta(\boldsymbol{X})\log\frac{\Gamma\left(\frac{\sigma+1}{2}\right)}{\Gamma\left(\frac{\sigma_0+1}{2}\right)} - 2\delta(\boldsymbol{X})\log\left(\frac{\sigma+1}{\sigma_0+1}\right), \end{aligned}$$

with $r = \sqrt{(\sigma_0+1/2)(\sigma_0-1/2)}$,

$$c_{\theta,\sigma,\boldsymbol{X},t,1} := (\sigma-\sigma_0)\left(\frac{r|\Gamma(3/2-\sigma_0)|}{4\boldsymbol{X}^{\sigma_0+1/2}} - \frac{1}{2\boldsymbol{X}} - \left(\frac{\delta(\boldsymbol{X})}{2}\right)\right)\log(1+t^2),$$

and finally

$$c_{\theta,\sigma,\boldsymbol{X},m,1} := |\sigma-\sigma_0|\left(\frac{\boldsymbol{X}-1}{\boldsymbol{X}^2} - \frac{\delta(\boldsymbol{X})}{8}\right)\log\left(\frac{m}{\pi}\right).$$

Remark 3.30. *If we knew the position of the Siegel zero, then choosing σ sufficiently close to 1 away from this zero will yield a bound for $\log\left|\frac{L(s_0)}{L(s)}\right|$ and hence, by a slight modification, for the class number. Although asymptotically the same, the constant involved is slightly better than the one obtained by Ono and Soundararajan. We keep the explicit but complicated form for the constants for computational purposes(see [20]). The same is true for the constants in Theorem 3.31.*

Proof. Since

$$\int_{s_0}^{s} G_1(w,\boldsymbol{X})dw = \boldsymbol{G}(s_0,\boldsymbol{X}) - \boldsymbol{G}(s,\boldsymbol{X}),$$

integrating from s_0 to s in Lemma 3.24 yields

$$\log\left(\frac{L(s_0)}{L(s)}\right) = \boldsymbol{G}(s_0,\boldsymbol{X}) - \boldsymbol{G}(s,\boldsymbol{X}) + \int_{s_0}^{s} E_{sig}(w)dw - \int_{s_0}^{s} R(w)dw + \frac{1}{\boldsymbol{X}}\log\left(\frac{L(s_0-1)}{L(s-1)}\right).$$

We will take the real part of both sides, and bound each term, noting that $\mathrm{Re}(\log(x)) = \log(|x|)$.

(i) We will first bound $\int_{s_0}^{s} R(w)dw$. We will show

$$\mathrm{Re}\left(\int_{s_0}^{s} R(w)dw\right) \geq -\left|\int_{s_0}^{s} R(w)dw\right| \geq -|\sigma-\sigma_0|\left[\frac{\log\left(\frac{m}{\pi}\right)}{\boldsymbol{X}^2}\right.$$
$$\left. + \frac{|\Gamma(3/2-\sigma_0)|}{2\pi\boldsymbol{X}^{\sigma_0+1/2}}\left(r\pi\left(\frac{891}{100}+\frac{1}{2}\log(1+t^2)\right) + \frac{\pi\log(226)}{2r^2} + \frac{2}{\sqrt{15}r^2}\right)\right]. \quad (3.29)$$

Using the functional equation of L, we get the equation for the Logarithmic derivative

$$-\frac{L'}{L}(s+w) = \log\left(\frac{m}{\pi}\right) + \frac{1}{2}\cdot\frac{\Gamma'}{\Gamma}\left(\frac{2-s-w}{2}\right) + \frac{1}{2}\cdot\frac{\Gamma'}{\Gamma}\left(\frac{1+s+w}{2}\right) + \frac{L'}{L}(1-s-w).$$

Assume that $w = u+it$, where $\sigma_0 := \mathrm{Re}(s_0) \leq u \leq \mathrm{Re}(s) =: \sigma$. Plugging this in gives

$$R(w) = \frac{1}{2\pi i}\int_{-u-1/2-i\infty}^{-u-1/2+i\infty} \Gamma(z)\boldsymbol{X}^z\left[\log\left(\frac{m}{\pi}\right) + \frac{1}{2}\cdot\frac{\Gamma'}{\Gamma}\left(\frac{2-z-w}{2}\right)\right.$$
$$\left. + \frac{1}{2}\cdot\frac{\Gamma'}{\Gamma}\left(\frac{1+z+w}{2}\right) + \frac{L'}{L}(1-z-w)\right]dz.$$

Consider $z = -u-1/2+iy$. Using Lemma 3.26, with $\mathrm{Re}\left(\frac{1+s+w}{2}\right) = \frac{1+u-u-1/2}{2} = \frac{1}{4}$, $\mathrm{Im}\left(\frac{1+s+w}{2}\right) = \frac{t+y}{2} = -\mathrm{Im}\left(\frac{2-s-w}{2}\right)$, and $\mathrm{Re}\left(\frac{2-s-w}{2}\right) = \frac{2-u+u+1/2}{2} = \frac{5}{4} > 1$, we obtain

$$\frac{\Gamma'}{\Gamma}\left(\frac{1+z+w}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{2-z-w}{2}\right) \leq \frac{74}{5} + \log(1+t^2) + \log(1+y^2)$$

Additionally, since $\mathrm{Re}(1-z-w) = \frac{3}{2}$,

$$\left|\frac{L'}{L}(1-z-w)\right| \leq \sum_{n=1}^{\infty}\frac{|\Lambda(n)\chi(n)|}{n^{\frac{3}{2}}} \leq \frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) \leq \frac{151}{100}.$$

Therefore, we have obtained

$$\left|\frac{L'}{L}(1-z-w)+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1+z+w}{2}\right)+\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{2-z-w}{2}\right)\right| \\ \leq \frac{891}{100}+\frac{1}{2}\log(1+t^2)+\frac{1}{2}\log(1+y^2). \quad (3.30)$$

Since $|\Gamma(x+iy)| \leq |\Gamma(x)|$, the functional equation for Γ yields

$$|\boldsymbol{X}^z\Gamma(z)| = \boldsymbol{X}^{-u-1/2}\cdot\frac{|\Gamma(z+2)|}{|z(z+1)|} \leq \boldsymbol{X}^{-u-1/2}\cdot\frac{|\Gamma(3/2-u)|}{(1/2+u)(u-1/2)+y^2}.$$

It is easy to see that for $\boldsymbol{X} > e^{\gamma+\frac{1}{\frac{3}{2}-\sigma}}$, this function on the right hand side decreases in $[1/2,\sigma]$, so we get that the maximum for $u \in [\sigma_0,\sigma]$ is attained at $u=\sigma_0$.

This gives the bound

$$|\boldsymbol{X}^z\Gamma(z)| \leq \boldsymbol{X}^{-\sigma_0-1/2}\cdot\frac{|\Gamma(3/2-\sigma_0)|}{(1/2+\sigma_0)(\sigma_0-1/2)+y^2}. \quad (3.31)$$

Furthermore, shifting the line of integration in the remaining term to the far left, noting that $-2 < -\sigma-1/2 < -u-1/2 < -\sigma_0-1/2 < -1$, then (for $\boldsymbol{X}$ sufficiently large)

$$\frac{1}{2\pi i}\int_{-u-1/2-i\infty}^{-u-1/2+i\infty}\Gamma(z)\boldsymbol{X}^z\log\left(\frac{m}{\pi}\right) = \log\left(\frac{m}{\pi}\right)\sum_{n=2}^{\infty}\frac{(-\boldsymbol{X})^{-n}}{n!} \leq \frac{\log\left(\frac{m}{\pi}\right)}{\boldsymbol{X}^2}. \quad (3.32)$$

Recall $r=\sqrt{(\sigma_0+1/2)(\sigma_0-1/2)}$. Plugging in the bounds from equations (3.30), (3.31), and (3.32) give

$$\begin{aligned}|R(w)| &\leq \frac{\log\left(\frac{m}{\pi}\right)}{\boldsymbol{X}^2}+\frac{|\Gamma(3/2-\sigma_0)|}{2\pi\boldsymbol{X}^{\sigma_0+1/2}}\int_{-\infty}^{\infty}\frac{1}{y^2+r^2}\left(\frac{891}{100}+\frac{1}{2}\log(1+t^2)+\frac{1}{2}\log(1+y^2)\right)dy \\ &= \frac{\log\left(\frac{m}{\pi}\right)}{\boldsymbol{X}^2}+\frac{|\Gamma(3/2-\sigma_0)|}{2\pi\boldsymbol{X}^{\sigma_0+1/2}}\left(r\pi\left(\frac{891}{100}+\frac{1}{2}\log(1+t^2)\right)+\int_0^{\infty}\frac{\log(1+y^2)}{y^2+r^2}\,dy\right).\end{aligned}$$

Splitting the remaining integral into the range 0 to 15 and 15 to ∞ gives a bound of

$$\begin{aligned}\int_0^{\infty}\frac{\log(1+y^2)}{y^2+r^2}\,dy &= \int_0^{15}\frac{\log(1+y^2)}{y^2+r^2}\,dy+\int_{15}^{\infty}\frac{\log(1+y^2)}{y^2+r^2}\,dy \\ &\leq \frac{\log(1+15^2)}{r^2}\int_0^{\infty}\frac{dy}{1+y^2}+\frac{1}{r^2}\int_{15}^{\infty}\frac{1}{y^{3/2}}dy = \frac{\pi\log(226)}{2r^2}+\frac{2}{\sqrt{15}r^2}.\end{aligned}$$

This gives the overall bound for $|R(w)|$ of

$$|R(w)| \leq \frac{\log\left(\frac{m}{\pi}\right)}{\boldsymbol{X}^2} + \frac{|\Gamma(3/2-\sigma_0)|}{2\pi \boldsymbol{X}^{\sigma_0+1/2}} \left(r\pi \left(\frac{891}{100} + \frac{1}{2}\log(1+t^2) \right) + \frac{\pi \log(226)}{2r^2} + \frac{2}{\sqrt{15}r^2} \right).$$

Since this is independent of w, integrating from $w = s_0$ to $w = s$ gives equation (3.29).

(ii) We will next find a bound for $\frac{1}{\boldsymbol{X}} \log \left|\frac{s_0-1}{s-1}\right|$. We will show

$$\begin{aligned} \frac{1}{\boldsymbol{X}} \log \left| \frac{L(s_0-1)}{L(s-1)} \right| \geq \frac{1}{\boldsymbol{X}} \log \frac{|L(s)|}{|L(s_0)|} + |\sigma - \sigma_0| \log\left(\frac{m}{\pi}\right) \\ - \frac{1-\sigma_0}{2} \left(\frac{22}{3} + \frac{\log(1 + \left(\frac{3-\sigma_0}{2}\right)^2)}{2} + \log(1+t^2) + \frac{\log(2)}{2} + \frac{2}{\sigma_0} \right) \\ - \frac{\sigma-1}{2} \left(\frac{22}{3} + \log(1+t^2) + \log(2) + \frac{2}{3-\sigma_0} + \frac{2}{\sigma_0} \right). \end{aligned} \tag{3.33}$$

Again using the functional equation for $\frac{L'}{L}$, we obtain

$$\log \frac{L(s_0-1)}{L(s-1)} = \log \frac{L(2-s_0)}{L(2-s)} + |\sigma - \sigma_0| \log\left(\frac{m}{\pi}\right) + \frac{1}{2}\int_{s_0}^{s} \left(\frac{\Gamma'}{\Gamma}\left(\frac{3-w}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{w}{2}\right) \right) dw.$$

Since $\sigma_0 = 2-\sigma$, and $\mathrm{Im}(\sigma) = \mathrm{Im}(\sigma_0)$, it follows that $|L(2-s_0)| = |L(s)|$ and $|L(2-s)| = |L(s_0)|$. Therefore

$$\log \frac{|L(s_0-1)|}{|L(s-1)|} \geq \log \frac{|L(s)|}{|L(s_0)|} + |\sigma - \sigma_0| \log\left(\frac{m}{\pi}\right) - \frac{1}{2}\int_{s_0}^{s} \left| \frac{\Gamma'}{\Gamma}\left(\frac{3-w}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{w}{2}\right) \right| |dw|. \tag{3.34}$$

We will again use Lemma 3.26 and also Lemma 3.27. Note that $\mathrm{Re}\left(\frac{3-w}{2}\right) = \frac{3}{2} - \frac{1}{2}\mathrm{Re}(w)$. Therefore, if $\mathrm{Re}(w) \leq 1$, then $\mathrm{Re}\left(\frac{3-w}{2}\right) \geq 1$. In the range $\sigma \geq \mathrm{Re}(w) \geq 1$, we will use equation (3.27).

Thus, for any $w \in [\sigma_0, 1]$, we may bound the term with $\frac{3-w}{2}$ by equation (3.24) and the term with $\frac{w}{2}$ with (3.27) to get

$$\left| \frac{\Gamma'}{\Gamma}\left(\frac{3-w}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{w}{2}\right) \right| \leq \frac{22}{3} + \frac{\log(1 + \left(\frac{3-\sigma_0}{2}\right)^2)}{2} + \log(1+t^2) + \frac{\log(2)}{2} + \frac{2}{\sigma_0}.$$

For $w \in [1, \sigma]$, both will be bounded by equation (3.27), obtaining

$$\left|\frac{\Gamma'}{\Gamma}\left(\frac{3-w}{2}\right)+\frac{\Gamma'}{\Gamma}\left(\frac{w}{2}\right)\right| \leq \frac{22}{3}+\log(1+t^2)+\log(2)+\frac{2}{3-\sigma_0}+\frac{2}{\sigma_0}. \tag{3.35}$$

Combining equations (3.35) and (3.34) yields equation (3.33).

(iii) Finally, we bound $\int_{s_0}^{s} E_{\mathbf{sig}}(w)dw$. We will show here

$$\int_{s_0}^{s} \mathrm{Re}(E_{\mathrm{sig}}(w))dw \geq -\delta(\boldsymbol{X}) \cdot \left[\log\frac{|L(s)|}{|L(s_0)|}+\frac{\sigma-\sigma_0}{8}\log\left(\frac{m}{\pi}\right)+2\log\frac{\Gamma\left(\frac{\sigma+1}{2}\right)}{\Gamma\left(\frac{\sigma_0+1}{2}\right)}\right.$$
$$\left.+\,2\log\left(\frac{\sigma+1}{\sigma_0+1}\right)\cdot\frac{t^2}{t^2+(\sigma_0+1)^2}+\left(\frac{\sigma+1}{2}-\frac{\sigma_0+1}{2}\right)\log\left(1+\frac{t^2}{(\sigma_0+1)^2}\right)\right]. \tag{3.36}$$

An individual zero $\rho := 1/2 + iy$ contributes

$$\int_{s_0}^{s} \mathrm{Re}(\boldsymbol{X}^{\rho-w}\Gamma(\rho-w))dw.$$

The real part of the above integral is greater than or equal to the negative of the absolute value and

$$\mathrm{Re}\left(\int_{s_0}^{s}\frac{dw}{w-\rho}\right)=\mathrm{Re}\left(\log\frac{s-\rho}{s_0-\rho}\right)=\log\frac{|s-\rho|}{|s_0-\rho|},$$

because w has real part larger than $1/2$, and hence $\frac{1}{w-\rho}$ is analytic over this integral. This yields

$$\int_{s_0}^{s} \mathrm{Re}(\boldsymbol{X}^{\rho-w}\Gamma(\rho-w))dw \geq -\left|\int_{\sigma_0}^{\sigma}\boldsymbol{X}^{1/2-u}\Gamma(1/2-u+i(y-t))du\right| \cdot$$
$$\left(\log\frac{|s-\rho|}{|s_0-\rho|}\right)^{-1}\cdot\int_{s_0}^{s}\mathrm{Re}\left(\frac{1}{w-\rho}\right)dw. \tag{3.37}$$

The term (3.37) is 1, so that the right hand side of the inequality is the negative of the absolute value of the integral. We have added the additional term (3.37) so that we may use $\mathrm{Re}\left(\frac{1}{w-\rho}\right)$ later in Hadamard's factorization formula (see [19]).

Since the integral and the log term merely make up one such term for y fixed, we know that they are bounded above by $\delta(\boldsymbol{X})$. Therefore, we have

$$\int_{s_0}^{s} \mathrm{Re}(\boldsymbol{X}^{\rho-w}\Gamma(\rho-w))dw \geq -\delta(\boldsymbol{X})\int_{s_0}^{s} \mathrm{Re}\left(\frac{dw}{w-\rho}\right).$$

Summing the contributions of all zeros gives us

$$\int_{s_0}^{s} \mathrm{Re}(E_{\mathrm{sig}}(w))dw \geq -\delta(\boldsymbol{X})\int_{s_0}^{s}\sum_{\rho}\mathrm{Re}\frac{1}{w-\rho}dw. \tag{3.38}$$

By Hadamard's factorization formula

$$\mathrm{Re}\left(\frac{L'}{L}(w)\right) = -\frac{1}{8}\log\left(\frac{m}{\pi}\right) - \frac{1}{2}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{w+1}{2}\right)\right) + \sum_{\rho}\mathrm{Re}\left(\frac{1}{w-\rho}\right).$$

Integration yields

$$\int_{s_0}^{s}\sum_{\rho}\mathrm{Re}\left(\frac{1}{w-\rho}\right)dw = \log\frac{|L(s)|}{|L(s_0)|} + \frac{\sigma-\sigma_0}{8}\log\left(\frac{m}{\pi}\right) + \int_{s_0}^{s}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{w+1}{2}\right)\right)dw. \tag{3.39}$$

Noting that $\frac{u+1}{2} = \mathrm{Re}\left(\frac{w+1}{2}\right) > \frac{\sigma_0+1}{2} > \frac{3}{4}$, we now use equation (3.25) to obtain

$$\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{w+1}{2}\right)\right) \leq \frac{\Gamma'}{\Gamma}\left(\frac{u+1}{2}\right) + \frac{t^2/4}{\frac{u+1}{2}\left(\left(\frac{u+1}{2}\right)^2 + t^2/4\right)} + \log\left(\sqrt{\frac{t^2}{4\left(\frac{u+1}{2}\right)^2}+1}\right).$$

Integration and $4\left(\frac{u+1}{2}\right)^2 + t^2 \geq t^2 + (\sigma_0+1)^2$ yield

$$\begin{aligned}\int_{s_0}^{s}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{w+1}{2}\right)\right)dw &\leq 2\log\frac{\Gamma\left(\frac{\sigma+1}{2}\right)}{\Gamma\left(\frac{\sigma_0+1}{2}\right)} + 2\log\left(\frac{\sigma+1}{\sigma_0+1}\right)\cdot\frac{t^2}{t^2+(\sigma_0+1)^2} \\ &\quad + \left(\frac{\sigma+1}{2} - \frac{\sigma_0+1}{2}\right)\log\left(1+\frac{t^2}{(\sigma_0+1)^2}\right).\end{aligned} \tag{3.40}$$

Thus, combining equations (3.38), (3.39) and (3.40) yield equation (3.36).

Finally, rearranging equations (3.29), (3.33), and (3.36 and combining the terms involving $\log\frac{L(s_0)}{L(s)}$ yields Theorem 3.29. $\square$

3.6 Bounding $L_i(s)$ from above

We use the same notation as in Section 3.5. We also define $\sigma_1 := 3-\sigma$ and $s_1 := \sigma_1+it$. In addition, we will fix σ_2 and consider $s_2 := \sigma_2 + it$.

We will find a bound from above for $\log(|L_i(s)|)$, depending on $\boldsymbol{X}$, t, and σ. Recall our definition (3.23) of $\boldsymbol{F}_1$ and denote

$$\boldsymbol{F}(w,\boldsymbol{X}) := \sum_{n=1}^{\infty}\frac{\lambda_i(n)\chi(n)}{n^w\log(n)}e^{-n/\boldsymbol{X}} = \int F_1(w,\boldsymbol{X})dw.$$

Theorem 3.31. *Assume GRH for weight 2 modular forms, and $L_i(s) := L(G_i,\chi,s)$ with χ a primitive character such that the modulus of L_i is q. Then, recalling the definition of the euler constant (3.13),*

$$\log|L_i(s)| \le \frac{\boldsymbol{X}}{\boldsymbol{X}+1}\boldsymbol{F}(s,\boldsymbol{X}) - \frac{\boldsymbol{X}((2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X})-\beta(\boldsymbol{X}))}{(\boldsymbol{X}+1)(1+\gamma(\boldsymbol{X}))}\boldsymbol{F}_1(s_2,\boldsymbol{X}) + \frac{\boldsymbol{X}}{\boldsymbol{X}+1}\left(c_{\theta,\sigma,\boldsymbol{X},2}+c_{\theta,\sigma,\boldsymbol{X},t,2}+c_{\theta,\sigma,\boldsymbol{X},q,2}\right),$$

where

$$\begin{aligned}
c_{\theta,\sigma,\boldsymbol{X},2} :=& \left(1-e^{-n/\boldsymbol{X}}\right)\sum_{n=2}^{d}\frac{|\lambda_i(n)|}{n^{\sigma_1}\log(n)} + 2\log(\zeta(\sigma_1-1/2)) - 2\sum_{n=1}^{d}\Lambda(n)n^{\sigma_1-1/2}\log(n)\\
&+\max\{|\Gamma(\sigma)|,|\Gamma(\sigma_1)|\}\cdot\frac{\boldsymbol{X}^{1-\sigma}}{(\boldsymbol{X}-1)\log(x)}\\
&+|\log(\zeta(4-\sigma_1-1/2))-\log(\zeta(4-\sigma-1/2))|\left(\frac{1}{2\boldsymbol{X}^2}+\frac{1}{6(\boldsymbol{X}+1)(\boldsymbol{X}-1)}\right)\\
&+\frac{1}{\boldsymbol{X}}\log(\zeta(3-\sigma-1/2)) + \frac{\sigma_1-\sigma}{2\boldsymbol{X}^2}\left(\frac{49}{6}+\frac{\boldsymbol{X}}{\boldsymbol{X}+1}\log(12)\right)\\
&+\frac{\log\frac{\sigma_1-1}{\sigma-1}-\log\frac{2-\sigma_1}{2-\sigma}}{2\boldsymbol{X}^2}+\frac{2}{\boldsymbol{X}+1}\log\frac{\Gamma(\sigma_1)}{\Gamma(\sigma)}\\
&+\frac{(2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X})-\beta(\boldsymbol{X})}{(1+\gamma(\boldsymbol{X}))}\left(\frac{\Gamma'}{\Gamma}(\sigma_2)+\frac{1}{\sigma_2}\right)\\
&+\frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1}+\frac{1}{\boldsymbol{X}-1}\left(\frac{55}{6}+\frac{1}{(2-\sigma_2)(\sigma_2-1)}+2\left|\frac{\zeta'}{\zeta}(3-1/2-\sigma_2)\right|\right),
\end{aligned}$$

$$c_{\theta,\sigma,\boldsymbol{X},t,2} := \log(1+t^2)\left(\frac{\sigma_1-\sigma}{2\boldsymbol{X}(\boldsymbol{X}+1)} + \frac{2(\sigma_1-\sigma)}{\boldsymbol{X}} + \frac{(2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X})-\beta(\boldsymbol{X})}{2(1+\gamma(\boldsymbol{X}))} + \frac{1}{\boldsymbol{X}-1}\right),$$

$$c_{\theta,\sigma,\boldsymbol{X},q,2} := \log\left(\frac{q}{4\pi^2}\right)\left(\frac{(2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X})-\beta(\boldsymbol{X})}{2(1+\gamma(\boldsymbol{X}))} + \frac{(\alpha(\boldsymbol{X})-\beta(\boldsymbol{X}))}{(1+\gamma(\boldsymbol{X}))}\cdot\frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1} + \frac{1}{\boldsymbol{X}-1} + \frac{\sigma_1-\sigma}{\boldsymbol{X}}\right),$$

$$\gamma(\boldsymbol{X}) := \max_y |\Gamma(1-\sigma_2+iy)|\left((\sigma_2-1)+\frac{y^2}{\sigma_2-1}\right),$$

$$\beta(\boldsymbol{X}) := \begin{cases} \frac{(\sigma_2-1)\boldsymbol{X}^{\sigma_2-1}}{\boldsymbol{X}^{\sigma_2-1}-\Gamma(2-\sigma_2)}\int_\sigma^{\sigma_1} Re\left(\boldsymbol{X}^{1-u}\Gamma(1-u)\right)du & \textit{if } \boldsymbol{X}\le\Gamma(2-\sigma_2) \\ -\frac{(\sigma_2-1)\boldsymbol{X}^{\sigma_2-1}}{\boldsymbol{X}^{\sigma_2-1}+\Gamma(2-\sigma_2)}\int_\sigma^{\sigma_1} Re\left(\boldsymbol{X}^{1-u}\Gamma(1-u)\right)du & \textit{if } \Gamma(2-\sigma_2)<\boldsymbol{X}\le M_{\sigma_2} \\ 0 & \textit{otherwise} \end{cases}, \tag{3.41}$$

and finally

$$\alpha(\boldsymbol{X}) := \max_y \left|\int_\sigma^{\sigma_1}\left(\boldsymbol{X}^{1-u}\Gamma(1-u+iy)\right)du - \left(\beta(\boldsymbol{X})\boldsymbol{X}^{1-\sigma_2}\Gamma(1-\sigma_2+iy)\right)\right| \cdot \left((\sigma_2-1)+\frac{y^2}{\sigma_2-1}\right). \tag{3.42}$$

Remark 3.32. *Choosing σ_2 appropriately, it is suspected that the maximum in (3.42) is attained at $y=0$. In such a case, we would have $\alpha(\boldsymbol{X})=\beta(\boldsymbol{X})$.*

Proof. Integrating both sides of Lemma 3.25 from s to s_1 yields

$$\log L_i(s) = \log L_i(s_1) + \boldsymbol{F}(s,\boldsymbol{X}) - \boldsymbol{F}(s_1,\boldsymbol{X}) + \int_s^{s_1}(R_{\text{sig}}(w)+R_{\text{ins}}(w)+R_{\text{tri}}(w))dw.$$

We take real parts of both sides to bound $\log|L_i(s)|$. Since $|\lambda_i(n)|\le 2\sqrt{n}$, we bound

$$\log|L_i(s_1)| - \text{Re}(\boldsymbol{F}_1(s_1,\boldsymbol{X})) \le \left(1-e^{-n/\boldsymbol{X}}\right)\sum_{n=2}^{d}\frac{|\lambda_i(n)|}{n^{\sigma_1}\log(n)} + \sum_{n=d+1}^{\infty}\frac{2\Lambda(n)}{n^{\sigma_1-1/2}\log(n)}. \tag{3.43}$$

Notic that taking the logarithmic derivative of ζ and integrating yields

$$\sum_{n=d}^{\infty} \frac{2\Lambda(n)}{n^{\sigma_1 - 1/2}\log(n)} = 2\log(\zeta(\sigma_1 - 1/2)) - 2\sum_{n=1}^{d} \Lambda(n) n^{\sigma_1 - 1/2}\log(n),$$

which can easily be computed numerically with a computer.

(i) We first bound the contribution from the trivial zeros:

Since $1 < \sigma < w < \sigma_1 < 2$ and $|\Gamma(-n-w)| < |\Gamma(-w)|$ by the functional equation, we know that the maximum is attained either at s or s_1, so that the maximum is less than or equal to $\max\{|\Gamma(\sigma)|, |\Gamma(\sigma_1)|\}$. Thus

$$\begin{aligned}\int_s^{s_1} R_{\text{tri}}(w)dw &\le \max\{|\Gamma(\sigma)|, |\Gamma(\sigma_1)|\} \sum_{n=0}^{\infty} \int_{\sigma}^{\sigma_1} \boldsymbol{X}^{-n-u} du \\ &\le \max\{|\Gamma(\sigma)|, |\Gamma(\sigma_1)|\} \cdot \frac{\boldsymbol{X}^{1-\sigma}}{(\boldsymbol{X}-1)\log(x)}. \qquad (3.44)\end{aligned}$$

(ii) We now bound the contribution from the poles of Γ: We will show

$$\begin{aligned}\int_s^{s_1} R_{\text{ins}}(w)dw \le{}& |\log(\zeta(4-\sigma_1-1/2)) - \log(\zeta(4-\sigma-1/2))| \left(\frac{1}{2\boldsymbol{X}^2} + \frac{1}{6\boldsymbol{X}^2(\boldsymbol{X}-1)}\right) \\ &- \frac{\log(|L_i(s)|)}{\boldsymbol{X}} + \frac{1}{\boldsymbol{X}}\log(\zeta(3-\sigma-1/2)) + \frac{\sigma_1-\sigma}{2\boldsymbol{X}^2}\left(\frac{49}{6} + \log(1+t^2) + \log(12)\right) \\ &+ \frac{\log\frac{\sigma_1-1}{\sigma-1} - \log\frac{2-\sigma_1}{2-\sigma}}{2\boldsymbol{X}^2} + \frac{2}{\boldsymbol{X}}\log\frac{\Gamma(\sigma_1)}{\Gamma(\sigma)} + \frac{2(\sigma_1-\sigma)}{\boldsymbol{X}}\log(1+t^2) + \frac{(\sigma_1-\sigma)}{\boldsymbol{X}}\log\frac{q}{4\pi^2}.\end{aligned} \qquad (3.45)$$

We use the functional equation to obtain

$$\begin{aligned}\int_s^{s_1} R_{\text{ins}}(w)dw &= \sum_{n=1}^{\infty} \frac{(-\boldsymbol{X})^{-n}}{n!} \int_s^{s_1} \frac{L_i'}{L_i}(w-n)dw \\ &= \sum_{n=1}^{\infty} \frac{(-\boldsymbol{X})^{-n}}{n!} \left(\log\frac{L_i(2+n-s_1)}{L_i(2+n-s)} + (\sigma-\sigma_1)\log\frac{q}{4\pi^2} \right. \\ &\qquad \left. - \int_s^{s_1} \left(\frac{\Gamma'}{\Gamma}(2-w+n) + \frac{\Gamma'}{\Gamma}(w-n)\right) dw\right).\end{aligned}$$

First we note that

$$\sum_{n=1}^{\infty} \frac{(-\boldsymbol{X})^{-n}}{n!}(\sigma-\sigma_1)\log\frac{q}{4\pi^2} \leq \frac{(\sigma_1-\sigma)\log\frac{q}{4\pi^2}}{\boldsymbol{X}}. \tag{3.46}$$

Additionally, we have

$$\log\frac{L_i(2+n-s_1)}{L_i(2+n-s)} \leq \sum_{m=2}^{\infty}\frac{|\lambda_i(m)|}{\log m}\left(\frac{1}{m^{2+n-\sigma_1}}-\frac{1}{m^{2+n-\sigma}}\right).$$

Clearly for $n \geq 2$, $\frac{1}{m^{2+n-\sigma_1}} - \frac{1}{m^{2+n-\sigma}} \leq \frac{1}{m^{4-\sigma_1}} - \frac{1}{m^{4-\sigma}}$, so that we get the bound

$$\left|\log\frac{L_i(2+n-s_1)}{L_i(2+n-s)}\right| \leq \left|\log(\zeta(4-\sigma_1-1/2)) - \log(\zeta(4-\sigma-1/2))\right|.$$

This yields

$$\begin{aligned}\sum_{n=2}^{\infty}&\frac{(-\boldsymbol{X})^{-n}}{n!}\log\frac{L_i(2+n-s_1)}{L_i(2+n-s)}\\ &\leq \left|\log(\zeta(4-\sigma_1-1/2)) - \log(\zeta(4-\sigma-1/2))\right|\left(\frac{1}{2\boldsymbol{X}^2}+\frac{1}{6\boldsymbol{X}^2(\boldsymbol{X}-1)}\right).\end{aligned} \tag{3.47}$$

For $n = 1$, taking the real part and noting that $|L_i(3-s_1)| = |L_i(s)|$, we have

$$\begin{aligned}(-\boldsymbol{X})^{-1}\log\frac{|L_i(3-s_1)|}{|L_i(3-s)|} &= -\frac{\log|L_i(3-s_1)|}{\boldsymbol{X}} + \sum_{m=2}^{\infty}\frac{|\lambda_i(m)|}{m^{3-\sigma}\log m}\\ &\leq -\frac{\log(|L_i(s)|)}{\boldsymbol{X}} + \frac{1}{\boldsymbol{X}}\log(\zeta(3-\sigma-1/2)).\end{aligned} \tag{3.48}$$

It remains to bound

$$\int_s^{s_1}\left(\frac{\Gamma'}{\Gamma}(2-w+n)+\frac{\Gamma'}{\Gamma}(w-n)\right)dw.$$

Since $1 < \sigma \leq w \leq \sigma_1 < 2$, we know that $2-w+n \geq 1$ for all $n \geq 1$, so that we can use equation (3.24) to bound that term. We will use equation (3.26) to bound the term with $w-n$ for $n \geq 2$. For $n = 1$, we have $u - n \in (0,1)$, so that we can use equation

(3.27). We also see, independent of n, $< u-n > (1- < u-n >) = (2-u)(u-1)$, as either $< u-n > \equiv u \pmod 1$ or $< u-n > \equiv -u \pmod 1$, and $< u-n > \in (0,1)$.

This yields, for $n \geq 2$,

$$\begin{aligned}\frac{\Gamma'}{\Gamma}(2-w+n) + \frac{\Gamma'}{\Gamma}(w-n) \\ \leq \frac{49}{6} + \frac{\log\left((3+n-u)(2+n-u)\right)}{2} + \log(1+t^2) + \log(3+n-u).\end{aligned}$$

Now note that for $n \geq 2$, $2+|n-u| = 2+n-u$, and $1+(2+n-u)^2 < (3+n-u)^2$, so that $\frac{\log(1+(2+n-u)^2)}{2} + \log(2+|n-u|) \leq \log\left((3+n-u)(2+n-u)\right)$. For $n=1$, we have $u-1>0$ and $3-u>0$, so that we can use equation (3.25) and the functional equation to obtain

$$\begin{aligned}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(w-1)\right) \leq \mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(w)\right) - \mathrm{Re}\left(\frac{1}{w-1}\right) \leq \mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(w)\right) \\ \leq \frac{\Gamma'}{\Gamma}(u) + \frac{t^2}{u(t^2+u^2)} + \frac{1}{2}\log(1+t^2) \leq \frac{\Gamma'}{\Gamma}(u) + \log(1+t^2)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(3-w)\right) \leq \frac{\Gamma'}{\Gamma}(3-u) + \frac{t^2}{(3-u)(t^2+(3-u)^2)} + \frac{1}{2}\log(1+t^2) \\ \leq \frac{\Gamma'}{\Gamma}(3-u) + \log(1+t^2).\end{aligned}$$

Now we have, since $u>1$ and $\log(n+2)\cdot n < n!$ for $n \geq 3$ and $\boldsymbol{X} > 2$,

$$\begin{aligned}-\sum_{n=1}^{\infty}\frac{(-\boldsymbol{X})^{-n}}{n!}\int_{s}^{s_1}\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(2-w+n) + \frac{\Gamma'}{\Gamma}(w-n)\right) \\ \leq \frac{\sigma_1-\sigma}{2\boldsymbol{X}^2}\left(\frac{49}{6} + \log(1+t^2) + \log(12)\right) + \frac{\log\frac{\sigma_1-1}{\sigma-1} - \log\frac{2-\sigma_1}{2-\sigma}}{2\boldsymbol{X}^2} \\ + \frac{2}{\boldsymbol{X}}\log\frac{\Gamma(\sigma_1)}{\Gamma(\sigma)} + \frac{2(\sigma_1-\sigma)}{\boldsymbol{X}}\log(1+t^2). \quad (3.49)\end{aligned}$$

Rearranging and combining equations (3.46), (3.47), (3.48), and (3.49) yields equation (3.45).

(iii) Finally we bound the contribution from the significant zeros of L_i: We will show

$$\int_s^{s_1} \mathrm{Re}\left(R_{\text{sig}}(w)\right) dw \leq \left(\alpha(\boldsymbol{X}) + \frac{\alpha(\boldsymbol{X}) - \beta(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})}\right)\left(\frac{1}{2}\log\left(\frac{q}{4\pi^2}\right) + \frac{1}{2}\log\left(1+t^2\right)\right.$$
$$\left. + \frac{\Gamma'}{\Gamma}(\sigma_2) + \frac{1}{\sigma_2} - \boldsymbol{F}_1(s_2,\boldsymbol{X})\right) + \frac{\alpha(\boldsymbol{X}) - \beta(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})} \cdot \frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1}\log\left(\frac{q}{4\pi^2}\right)$$
$$+ \frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1} + \frac{1}{\boldsymbol{X}-1}\left(\frac{55}{6} + \frac{1}{(2-\sigma_2)(\sigma_2-1)} + \log(1+t^2)\right.$$
$$\left. + 2\frac{\zeta'}{\zeta}(3-1/2-\sigma_2) + \log\left(\frac{q}{4\pi^2}\right)\right). \quad (3.50)$$

Fix an individiual zero $\rho := 1+iy$.

$$\int_s^{s_1} \mathrm{Re}\left(\boldsymbol{X}^{\rho-w}\Gamma(\rho-w)\right) dw = \mathrm{Re}\left(\beta(\boldsymbol{X})\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right)$$
$$+ \int_s^{s_1} \mathrm{Re}\left(\boldsymbol{X}^{\rho-w}\Gamma(\rho-w)\right) dw - \mathrm{Re}\left(\beta(\boldsymbol{X})\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right)$$
$$\leq \mathrm{Re}\left(\beta(\boldsymbol{X})\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right) + \alpha(\boldsymbol{X})\mathrm{Re}\left(\frac{1}{s_2-\rho}\right).$$

Now, summing over all non-trivial zeros of L_i gives the bound

$$\int_s^{s_1} \mathrm{Re}\left(R_{\text{sig}}(w)\right) dw \leq \beta(\boldsymbol{X})\mathrm{Re}\left(R_{\text{sig}}(s_2)\right) + \alpha(\boldsymbol{X})\sum_\rho \mathrm{Re}\left(\frac{1}{s_2-\rho}\right) \quad (3.51)$$

Now we obtain by lemma 3.28

$$\sum_\rho \mathrm{Re}\left(\frac{1}{s-\rho}\right) = \mathrm{Re}\left(\frac{L_i'}{L_i}(s_2)\right) + \frac{1}{2}\log\left(\frac{q}{4\pi^2}\right) + \mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(s_2)\right) \quad (3.52)$$

We again use the exact formula for $\frac{L_i'}{L_i}$ from Lemma 3.25 to obtain

$$\frac{L_i'}{L_i}(s_2) = -\boldsymbol{F}_1(s_2,\boldsymbol{X}) - R_{\text{sig}}(s_2) - R_{\text{tri}}(s_2) - R_{\text{ins}}(s_2). \quad (3.53)$$

We again need to bound each of these.

Clearly, taking the absolute value and noting that $|\Gamma(-n-s)| \le |\Gamma(-\sigma_2)|$, we have

$$R_{\text{tri}}(s_2) \le |\Gamma(-\sigma_2)| \sum_{n=0}^{\infty} \boldsymbol{X}^{-n-\sigma_2} = \frac{|\Gamma(-\sigma_2)| \boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1}. \tag{3.54}$$

We next bound $R_{\text{ins}}(s_2)$. We use the functional equation of $\frac{L_i'}{L_i}$ to obtain

$$R_{\text{ins}}(s_2) = \sum_{n=1}^{\infty} \frac{n!}{x^{-n}} \left(\frac{L_i'}{L_i}(n+2-s_2) + \frac{\Gamma'}{\Gamma}(s_2-n) + \frac{\Gamma'}{\Gamma}(n+2-s_2) + + \log\left(\frac{q}{4\pi^2}\right)\right). \tag{3.55}$$

Since $\frac{L_i'}{L_i}(w) = \sum_{n=0}^{\infty} \frac{\lambda(m)\chi(m)}{m^w}$ and $\lambda(m) \le 2\sqrt{m}\Lambda(m)$, we know that for $n \ge 1$

$$\left|\frac{L_i'}{L_i}(n+2-s_2)\right| \le \left|\frac{L_i'}{L_i}(3-s_2)\right| \le \sum_{n=0}^{\infty} \frac{2\Lambda(m)}{m^{3-1/2-\sigma_2}} \le 2\left|\frac{\zeta'}{\zeta}(3-1/2-\sigma_2)\right|. \tag{3.56}$$

We again use Equations (3.26) and (3.24) of Lemma 3.26 to obtain

$$\begin{aligned} &\left|\frac{\Gamma'}{\Gamma}(s_2-n) + \frac{\Gamma'}{\Gamma}(n+2-s_2)\right| \\ &\qquad \le \frac{49}{6} + \frac{1}{(2-\sigma_2)(\sigma_2-1)} + \log((n+1)(n+2)) + \log(1+t^2). \end{aligned} \tag{3.57}$$

Therefore, combining equations (3.55), (3.56), and (3.57) yields

$$\begin{aligned} |R_{\text{ins}}(s_2)| \le \frac{1}{\boldsymbol{X}-1} \Bigg(&\frac{55}{6} + \frac{1}{(2-\sigma_2)(\sigma_2-1)} + \log(1+t^2) \\ &+ 2\left|\frac{\zeta'}{\zeta}(3-1/2-\sigma_2)\right| + \log\left(\frac{q}{4\pi^2}\right)\Bigg). \end{aligned} \tag{3.58}$$

We use Equation (3.25) of Lemma 3.26 to obtain

$$\begin{aligned} \operatorname{Re}\left(\frac{\Gamma'}{\Gamma}(s_2)\right) &\le \frac{\Gamma'}{\Gamma}(\sigma_2) + \frac{t^2}{\sigma_2(t^2+\sigma_2^2)} + \frac{1}{2}\log\left(1+\frac{t^2}{\sigma_2^2}\right) \\ &\le \frac{\Gamma'}{\Gamma}(\sigma_2) + \frac{1}{\sigma_2} + \frac{1}{2}\log\left(1+t^2\right). \end{aligned} \tag{3.59}$$

Combining the terms involving $\mathrm{Re}(R_{\mathrm{sig}}(s_2))$, it remains to bound

$$|\beta(\boldsymbol{X}) - \alpha(\boldsymbol{X})|\,\mathrm{Re}(R_{\mathrm{sig}}(s_2)). \tag{3.60}$$

We bound $\mathrm{Re}(R_{\mathrm{sig}}(s_2))$ similarly to the way that we bound R_{sig} bound above. A non-trivial zero ρ of L_i contributes

$$\begin{aligned}\mathrm{Re}\left(\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right) &\le \left|\mathrm{Re}\left(\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right)\right| \\ &= \boldsymbol{X}^{1-\sigma_2}\,|\Gamma(1-\sigma_2+i(y-t))|\left((\sigma_2-1)+\frac{(t-y)^2}{\sigma_2-1}\right)\cdot \mathrm{Re}\left(\frac{1}{s_2-\rho}\right).\end{aligned}$$

We then bound $\gamma(\boldsymbol{X})$ so that we have shown, using the functional equation for $\frac{L_i'}{L_i}$ and the exact formula from Lemma 3.25,

$$\begin{aligned}\mathrm{Re}(R_{\mathrm{sig}}(s_2)) &= \mathrm{Re}\sum_{\rho}\left(\boldsymbol{X}^{\rho-s_2}\Gamma(\rho-s_2)\right) \le \gamma(\boldsymbol{X})\mathrm{Re}\left(\sum_{\rho}\frac{1}{s_2-\rho}\right) \\ &= \gamma(\boldsymbol{X})\left(\frac{1}{2}\log\left(\frac{q}{4\pi^2}\right)+\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(s_2)\right)+\mathrm{Re}\left(\frac{L_i'}{L_i}(s_2)\right)\right) = \gamma(\boldsymbol{X})\cdot \\ &\left(\left(\frac{1}{2}+\frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1}\right)\log\left(\frac{q}{4\pi^2}\right)+\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(s_2)\right)-\boldsymbol{F}_1(s_2,\boldsymbol{X})-\mathrm{Re}(R_{\mathrm{sig}}(s_2))\right).\end{aligned}$$

We have already shown how to bound

$$\mathrm{Re}\left(\frac{\Gamma'}{\Gamma}(s_2)\right) \le \frac{\Gamma'}{\Gamma}(\sigma_2)+\frac{1}{\sigma_2}+\frac{1}{2}\log\left(1+t^2\right),$$

so combining the $\mathrm{Re}(R_{\mathrm{sig}}(s_2))$ terms yields

$$\begin{aligned}|\mathrm{Re}(R_{\mathrm{sig}}(s_2))| \le \frac{1}{1+\gamma(\boldsymbol{X})}&\left(\left(\frac{1}{2}+\frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1}\right)\log\left(\frac{q}{4\pi^2}\right)\right. \\ &\left.+\frac{\Gamma'}{\Gamma}(\sigma_2)+\frac{1}{\sigma_2}+\frac{1}{2}\log\left(1+t^2\right)-\boldsymbol{F}_1(s_2,\boldsymbol{X})\right).\end{aligned} \tag{3.61}$$

The inequalities (3.54), (3.58), and (3.61) bound the terms in equation (3.53). Noting that $\alpha(\boldsymbol{X}) \ge \beta(\boldsymbol{X})$ because plugging $y=0$ into the term we are maximizing in $\alpha(\boldsymbol{X})$ gives exactly $\beta(\boldsymbol{X})$, we get equation (3.50) as a consequence.

Combining equations (3.45), (3.44), and (3.50), and noting that $\alpha(x) + \frac{\alpha(\boldsymbol{X})-\beta(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})} = \frac{\alpha(\boldsymbol{X})(2+\gamma(\boldsymbol{X}))-\beta(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})}$ completes the proof. □

3.7 Fundamental Discriminants and Bounds for Weight 3/2 Cusp Forms

In this section we show how to find a bound $D_{\theta,\sigma,\sigma_2}$ such that for every fundamental discriminant $-D$ with $D > D_{\theta,\sigma,\sigma_2}$ we have $a_\theta(D) > 0$. Thus, combining this result with Section 3.3 gives the result for all discriminants.

3.7.1 Bounds for Fundamental Discriminants and Half Integer Weight Cusp Forms

We now proceed to show how bounds for $\alpha(\boldsymbol{X})$, $\gamma(\boldsymbol{X})$, and $\delta(\boldsymbol{X})$ are obtained.

Lemma 3.33. *Fix a finite number of intervals* $[y_{0,n}, y_{1,n}]$ *with* $0 \leq y_{0,n} < y_{1,n} < \infty$ *such that* $\bigcup_{n=1}^{m}[y_{0,n}, y_{1,n}] \cup [y_{1,m}, \infty) = (0, \infty)$. *Then*

$$\delta(\boldsymbol{X}) \leq max \left\{ max_{n\leq m} \int_{\sigma_0-1/2}^{\sigma-1/2} x^{-u} |\Gamma(-u+iy_{0,n})| du \cdot \left(\frac{1}{2} \log \frac{y_{1,n}^2 + (\sigma-1/2)^2}{y_{1,n}^2 + (\sigma_0-1/2)^2} \right)^{-1}, \right.$$
$$\left. \int_{\sigma_0-1/2}^{\sigma-1/2} x^{-u} |\Gamma(2-u+iy_{1,m})| \frac{2}{\left(\left(\sigma_0 - \frac{1}{2}\right)^2 + y_{1,m}^2 \right) \log \left(\frac{\left(\sigma-\frac{1}{2}\right)^2 + y_{1,m}^2}{\left(\sigma_0-\frac{1}{2}\right)^2 + y_{1,m}^2} \right)} \right\}. \quad (3.62)$$

For $\gamma(\boldsymbol{X})$, we obtain the bound

$$\gamma(\boldsymbol{X}) \leq max\left\{ max_{n\leq m}\left|\Gamma(1-\sigma_2+iy_{0,n})\right| \left((\sigma_2-1)+\frac{y_{1,n}^2}{\sigma_2-1}\right), \right.$$
$$\left. \left|\Gamma(3-\sigma_2+iy_{1,m})\right| \frac{1}{\sigma_2-1}\right\}. \quad (3.63)$$

Finally, for $\alpha(\boldsymbol{X})$ we obtain

$$\alpha(\boldsymbol{X}) \leq max\left\{ max_{n\leq m}\int_{\sigma}^{\sigma_1} \boldsymbol{X}^{1-u}|\Gamma(1-u+iy_{0,n})|\left((\sigma_2-1)+\frac{y_{1,n}^2}{\sigma_2-1}\right)\right.$$
$$-\beta(\boldsymbol{X})x^{1-\sigma_2}\Gamma(1-\sigma_2+iy_{1,n})\left((\sigma_2-1)+\frac{y_{0,n}^2}{\sigma_2-1}\right),$$
$$\left.\int_{\sigma}^{\sigma_1} \boldsymbol{X}^{1-u}|\Gamma(3-u+iy_{1,m})|\left(\frac{(\sigma_2-1)+\frac{y_{1,m}^2}{\sigma_2-1}}{(\sigma-1)^2+y_{1,m}^2}\right)\right\}. \quad (3.64)$$

Proof. We will show the result for $\delta(\boldsymbol{X})$, and the analogous calculation for $\alpha(\boldsymbol{X})$ and $\gamma(\boldsymbol{X})$ is left to the reader.

First define $\delta_{[y_0,y_1]}(\boldsymbol{X})$ to be the max taken in the interval $y_0 \leq y \leq y_1$. Further, define

$$f(y) := \int_{\sigma_0-1/2}^{\sigma-1/2} x^{-u}|\Gamma(-u+iy)|du$$

and

$$g(y) := \left(\frac{1}{2}\log\frac{y^2+(\sigma-1/2)^2}{y^2+(\sigma_0-1/2)^2}\right)^{-1}.$$

Notice first that f is strictly decreasing in $y \geq 0$, while g is strictly increasing. Therefore, noting that both functions are even in y, we fix $0 \leq y_0 < y < y_1 < \infty$, then pull the absolute value inside the integral to give

$$\delta_{[y_0,y_1]}(\boldsymbol{X}) \leq f(y_0)g(y_1).$$

Now we deal with the case where $y_1 = \infty$. The functional equation of $\Gamma(z)$ gives us

$$f(y) = \int_{\sigma_0 - 1/2}^{\sigma - 1/2} x^{-u} \frac{|\Gamma(2-u+iy)|}{(u^2+y^2)^{1/2}((1-u)^2+y^2)^{1/2}} du.$$

Now, noting that $1 - u \geq 1 - \left(\sigma - \frac{1}{2}\right) = \frac{3}{2} - \sigma = \sigma_0 - \frac{1}{2}$ and $u \geq \sigma_0 - \frac{1}{2}$, along with the fact that $|\Gamma(2-u+iy)|$ is decreasing in y, we get

$$f(y) \leq \int_{\sigma_0 - 1/2}^{\sigma - 1/2} x^{-u} |\Gamma(2-u+iy_0)| du \frac{1}{\left(\sigma_0 - \frac{1}{2}\right)^2 + y^2}.$$

Now, defining $z := \left(\sigma_0 - \frac{1}{2}\right)^2 + y^2$ and $a := \left(\sigma - \frac{1}{2}\right)^2 - \left(\sigma_0 - \frac{1}{2}\right)^2$ requires us to bound

$$\frac{2}{z \log\left(1 + \frac{a}{z}\right)}.$$

Since $a > 0$ we easily see that this function is decreasing for $z > 0$. Hence we obtain

$$\delta_{[y_0,\infty)} \leq \int_{\sigma_0 - 1/2}^{\sigma - 1/2} x^{-u} |\Gamma(2-u+iy_0)| \frac{2}{\left(\left(\sigma_0 - \frac{1}{2}\right)^2 + y_0^2\right) \log\left(\frac{\left(\sigma - \frac{1}{2}\right)^2 + y_0^2}{\left(\sigma_0 - \frac{1}{2}\right)^2 + y_0^2}\right)}.$$

□

We have now set up the framework to show our main theorems.

Proof of Corollary 3.1. Let N be squarefree and odd, $g \in S^+_{3/2}(4N)$, and $\epsilon > 0$. Choose $1 < \sigma < 1 + \frac{\epsilon}{2}$.

Observing the bounds for $\alpha(\boldsymbol{X})$, $\beta(\boldsymbol{X})$, and $\gamma(\boldsymbol{X})$ in Lemma 3.33, we see that the coefficient in front of $\log\left(\frac{q}{4\pi^2}\right)$ in Theorem 3.31 goes to zero as $\boldsymbol{X}$ goes to ∞. Using the functional equation for $L(G_i, -D, s)$, we get an additional term $\frac{\sigma-1}{2}\log(q)$. Therefore, taking $\sigma < 1 + \frac{\epsilon}{2}$ and $\boldsymbol{X}$ sufficiently large yields

$$|L_i(1)| \ll_\epsilon D^\epsilon,$$

where the coefficient is explicitly computable from Theorem 3.31.

Now, using Lemma 3.9, if $-D$ is a fundamental discriminant, then we have shown

$$|a_{g_i}(D)| \ll_\epsilon D^{\frac{1}{4}+\epsilon}.$$

Finally, we use Lemma 3.12 to obtain the result for all discriminants. □

Remark 3.34. *This result shows the Ramanujan-Petersson Conjecture for $k = 3/2$ and N squarefree and odd, conditional upon GRH for weight 2 modular forms.*

For weight $2k$ cusp forms we have $L(G, -D, s)$ centered at k with functional equation $s \to 2k - s$ when multiplied by a Γ factor and the appropriate power of q. Therefore, this argument should be easily generalized for all weights $k + \frac{1}{2}$, with $k \geq 1$.

We use the following lemma of Duke [10] to prove Theorem 3.7.

Lemma 3.35 (Duke [10])**.** *Fix $f \in S_{3/2}(\Gamma_0(N), \psi)$. Then*

$$\|f\|^2 \ll \Gamma(\alpha)d(N)N^{2\alpha}\sum_{n=1}^{\infty}|a_n|^2 n^{-\alpha},$$

where $\alpha > \frac{1}{2}$ is any number so that the series exists, $d(\cdot)$ is the divisor function, and the constant is absolute.

Proof of Theorem 3.7. Set $g := \theta - E$. We will bound E and g independent of θ. We will use the bound obtained in Corollary 3.1. However, some of bounds were dependent on θ. We now describe how to bound these terms independent of θ. The terms with $\boldsymbol{F}$ and $\boldsymbol{F}_1$ may be bound independent of L_i by bounding $\lambda_i \leq 2\sqrt{n}\Lambda(n)$ in Theorem 3.31 and taking the absolute value inside the sums $\boldsymbol{F}$ and $\boldsymbol{F}_1$. Thus, Corollary 3.1 yields

$$a_g(d) \ll_\epsilon \|g\| d^{1/4+\epsilon}. \tag{3.65}$$

We know that for a discriminant $-d$ with $\left(\frac{-d}{p}\right) \neq 1$ and $p^2 \nmid d$,

$$a_E(d) = \frac{12}{2^{v_p(d)}(p-1)} \cdot H(-d). \tag{3.66}$$

Assuming the Riemann hypothesis for Dirichlet L-functions, Littlewood has effectively shown that $H(-d) \gg \frac{\sqrt{d}}{\log(\log(d))}$ [26]. Thus

$$a_E(d) \gg_\epsilon \frac{1}{p} d^{1/2-\epsilon}. \tag{3.67}$$

It remains to use Lemma 3.35 to bound $\|g\|$ independent of θ. Define ω_Q to be the number of automorphs of the quadratic form Q. Denote the genus of Q by G. Define further

$$M(G) := \sum_{Q' \in G} \omega_{Q'}^{-1},$$

where the sum is taken over all ternary quadratic forms Q' in the genus.

Siegel proved (cf. [14]) that

$$a_E(d) = \frac{1}{M(G)} \sum_{Q' \in G} \omega_{Q'}^{-1} a_{\theta_{Q'}}(d).$$

Therefore, since $a_{\theta_{Q'}}(d) \geq 0$ for every Q', we have

$$a_g(d) \leq (M(G)\omega_Q + 1) a_E(d).$$

Moreover, it is well known [27] that $\omega_Q \leq 48$, so

$$a_g(d) \ll M(G) a_E(d).$$

Clearly, since $\omega_Q \geq 1$, $M(G) \leq \#G$.

Now notice that for any $Q \neq Q' \in G$, we have $a_{\theta_Q} - a_{\theta_{Q'}} \in S_{3/2}^+(4p)$. Due to the isomorphism between $S_{3/2}^+(4p)$ and $S_2(p)$, we know that

$$\#G \leq \dim_{\mathbb{C}} S_2(p) + 1.$$

It is well known (cf. [28] p. 10) that $\dim_{\mathbb{C}} S_2(p) \leq \lceil \frac{p+1}{12} \rceil + 1$. Thus, $\#G \leq p$. Therefore,

$$a_g(d) \ll p a_E(d).$$

Plugging in equation (3.66), we have

$$a_g(d) \ll p^2 H(-d).$$

Siegel's work [33] shows effectively that $H(-d) \ll_\epsilon d^{1/2+\epsilon}$. Therefore,

$$a_g(d) \ll_\epsilon p^2 d^{\frac{1}{2}+\epsilon}.$$

It is important to note here that our constant does not depend on g.

Therefore, the power of d attained allows us to choose $\alpha = 2 + 2\epsilon$ in Lemma 3.35 for the convergence of the sum. Since we know that $N = p$ is the level, this yields

$$\|g\|^2 \ll p^{4+4\epsilon} p^2.$$

Therefore,

$$a_g(d) \ll_\epsilon \|g\| d^{1/4+\epsilon} \ll_\epsilon p^{3+\epsilon} d^{1/4+\epsilon}. \tag{3.68}$$

Combining equations (3.67) and (3.68), $a_E(d) \gg_\epsilon a_g(d)$ if

$$\frac{1}{p} d^{1/2-\epsilon} \gg_\epsilon p^{3+\epsilon} d^{1/4+\epsilon},$$

i.e.

$$d \gg_\epsilon p^{16+\epsilon}.$$

□

Theorem 3.36 (Theorem 1.2). *Fix $\theta \in M^{+}_{3/2}(4p)$. Assume GRH for Dirichlet L-series and weight 2 modular forms. For every $\boldsymbol{X} > \gamma + \frac{1}{3/2-\sigma}$ such that*

$$\frac{(2+\gamma(\boldsymbol{X}))\gamma(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})} + \frac{2\gamma(\boldsymbol{X})}{1+\gamma(\boldsymbol{X})} \cdot \frac{|\Gamma(-\sigma_2)|\boldsymbol{X}^{1-\sigma_2}}{\boldsymbol{X}-1} + \frac{2(\sigma_1-\sigma)}{\boldsymbol{X}} + \frac{2}{\boldsymbol{X}-1} + \frac{\delta(\boldsymbol{X})}{8} - \frac{\boldsymbol{X}-1}{\boldsymbol{X}^2} + (\sigma-1) < \frac{1}{2}$$

there exists an effectively computable constant $D_{\sigma,\boldsymbol{X}}$ such that for all fundamental discriminants $-D < -D_{\sigma,\boldsymbol{X}}$ with $\left(\frac{-D}{p}\right) \neq 1$, one has $a_\theta(D) \neq 0$.

Moreover, such an $\boldsymbol{X}$ exists, so, assuming GRH for Dirichlet L-functions and weight 2 modular forms, there is an effectively computable constant D_σ such that for all fundamental discriminants $-D < -D_\sigma$ with $\left(\frac{-D}{p}\right) \neq 1$, $a_\theta(D) \neq 0$.

Proof. By equation (3.9), it suffices to bound $F(s)$. By definition,

$$\log|F(s)| = \log(|L_i(s)|) + \log(|\Gamma(s)|) - \log(|L(s_0)|) - \log(|L(s)|) + \frac{\sigma-1}{2}\log\frac{q}{4\pi^2}.$$

Using Theorem 3.31, we obtain constants $c_{\theta,\sigma,\boldsymbol{X},2}$, $c_{\theta,\sigma,\boldsymbol{X},t,2}$, and $c_{\theta,\sigma,\boldsymbol{X},q,2}$ such that

$$\log(|L_i(s)|) \leq \frac{\boldsymbol{X}}{\boldsymbol{X}+1}\boldsymbol{F}(s,\boldsymbol{X}) - \frac{\boldsymbol{X}((2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X}) - \beta(\boldsymbol{X})}{(\boldsymbol{X}+1)(1+\gamma(\boldsymbol{X}))}\boldsymbol{F}_1(s_2,\boldsymbol{X}) + c_{\theta,\sigma,\boldsymbol{X},2} + c_{\theta,\sigma,\boldsymbol{X},t,2} + c_{\theta,\sigma,\boldsymbol{X},q,2}. \quad (3.69)$$

Moreover, Theorem 3.29 gives us constants $c_{\theta,\sigma,\boldsymbol{X},1}$, $c_{\theta,\sigma,\boldsymbol{X},t,1}$, and $c_{\theta,\sigma,\boldsymbol{X},m,1}$ such that

$$\log\frac{|L(s_0)|}{|L(s)|} \geq \frac{\boldsymbol{X}}{\boldsymbol{X}-1-\delta(\boldsymbol{X})\boldsymbol{X}}\left(\mathrm{Re}(\boldsymbol{G}(s_0,\boldsymbol{X})) - \mathrm{Re}(\boldsymbol{G}(s,\boldsymbol{X}))\right) + c_{1,\boldsymbol{X},\sigma,\theta} + c_{\theta,\sigma,\boldsymbol{X},1} + c_{\theta,\sigma,\boldsymbol{X},t,1} + c_{\theta,\sigma,\boldsymbol{X},m,1}. \quad (3.70)$$

Therefore we have obtained

$$\log|F(s)| \leq \frac{\boldsymbol{X}}{\boldsymbol{X}+1}\boldsymbol{F}(s,\boldsymbol{X}) - \frac{\boldsymbol{X}((2+\gamma(\boldsymbol{X}))\alpha(\boldsymbol{X})-\beta(\boldsymbol{X})}{(\boldsymbol{X}+1)(1+\gamma(\boldsymbol{X}))}\boldsymbol{F}_1(s_2,\boldsymbol{X})$$
$$-\frac{\boldsymbol{X}}{\boldsymbol{X}-1-\delta(\boldsymbol{X})\boldsymbol{X}}\left(\operatorname{Re}(\boldsymbol{G}(s_0,\boldsymbol{X}))-\operatorname{Re}(\boldsymbol{G}(s,\boldsymbol{X}))\right)+c_{\theta,\sigma,\boldsymbol{X},2}+c_{\theta,\sigma,\boldsymbol{X},t,2}+c_{\theta,\sigma,\boldsymbol{X},q,2}$$
$$-(c_{\theta,\sigma,\boldsymbol{X},1}+c_{\theta,\sigma,\boldsymbol{X},t,1}+c_{\theta,\sigma,\boldsymbol{X},m,1})+\log|\Gamma(s)|-2\log|L(s)|.$$

Using the fact that $q = pD^2$ and $m = D$, it remains to deal with $\log|\Gamma(s)|$, $2\log|L(s)|$, and the remaining terms involving $\boldsymbol{F}$, $\boldsymbol{F}_1$, and $\boldsymbol{G}$. We will combine the terms $c_{\theta,\sigma,\boldsymbol{X},t,1}$ and $c_{\theta,\sigma,\boldsymbol{X},t,2}$ with $\log|\Gamma(\sigma+it)|$ to remove the dependence on t. The exponential decay of $\Gamma(\sigma+it)$ in the t term will swamp the contribution from the other terms, as a quick calculation indicates these only have polynomial growth. The term dealing with $\log|L(s)|$ may be bound easily by

$$\log|L(s)| \geq -\log|\zeta(\sigma)|. \tag{3.71}$$

If we denote the sum of the terms involving $\boldsymbol{F}$, $\boldsymbol{F}_1$, and $\boldsymbol{G}$, using the notation used in [29], as

$$\sum_{n=2}^{\infty}\operatorname{Re}\frac{\chi(n)}{n^{it}\log(n)}v(n;\boldsymbol{X}), \tag{3.72}$$

then, fixing a constant N_0, we may bound the first N_0 terms by a constant, and the remaining terms we will bound separately. Notice that the dependence on $\boldsymbol{X}$ on the first N_0 terms will be inconsequential for $\boldsymbol{X}$ large, as we can bound $e^{-n/x}$ by 1, whereas for $\boldsymbol{X}$ small we will explicitly use the value of $\boldsymbol{X}$ to obtain a better bound.

Now note that the contribution to $v(n;\boldsymbol{X})$ from the terms involving $\boldsymbol{F}$ and $\boldsymbol{F}_1$ is

$$e^{-n/x}\lambda(n)\chi(n)\cdot\frac{\boldsymbol{X}}{\boldsymbol{X}+1}\cdot\left(\frac{1}{n^{\sigma}}-a_x\frac{\log(n)}{n^{\sigma_2}}\right),$$

where a_x is above. Since $a_x > 0$, we would like $a_x \frac{\log(n)}{n^{\sigma_2}} \leq n^{-\sigma}$ so that we can bound this contribution by

$$\lambda(n)\chi(n) \cdot \frac{\boldsymbol{X}}{\boldsymbol{X}+1} \cdot \left(\frac{1}{n^{\sigma}}\right).$$

Choosing $\sigma_2 > \sigma$, the asymptotic growth shows us that there exists an N_0 such that $n > N_0$ will suffice. Therefore, we will choose N_0 sufficiently large to obtain this result.

Now, using the fact that $|\lambda(n)| \leq 2\Lambda(n)\sqrt(n)$, we have

$$|v(n;\boldsymbol{X})| \leq e^{-n/x}\left(\frac{2\Lambda(n)}{n^{\sigma-1/2}} + b_x\left(\frac{\Lambda(n)}{n^{\sigma_0}} - \frac{\Lambda(n)}{n^{\sigma}}\right)\right) \leq c_x \frac{\Lambda(n)}{n^{\min(\sigma_0,\sigma-1/2)}} e^{-n/x}.$$

Therefore, since c_x is independent of n, it remains to bound sums of the form

$$\boldsymbol{H}(\alpha,\boldsymbol{X}) := \sum_{n=N_0+1}^{\infty} \frac{\Lambda(n)}{n^{\alpha}\log(n)} e^{-n/x}.$$

We will need the following lemma which is a small generalization of a lemma from [29] to proceed with bounding the terms $n \to \infty$. Recall our definition (3.14) of $\psi(x)$.

Lemma 3.37. *Conditional upon the Riemann Hypothesis, one has for* $0 < \alpha < 1$,

$$\boldsymbol{H}(\alpha,\boldsymbol{X}) \leq \frac{e^{-N_0/\boldsymbol{X}}}{N_0^{\alpha}\log(N_0)}(c_{N_0}N_0 - \psi(N_0)) + \frac{c_{N_0}\boldsymbol{X}^{1-\alpha}}{\log(N_0)}\Gamma(1-\alpha, N_0/\boldsymbol{X})$$

where

$$\Gamma(x;y) := \int_y^{\infty} t^{x-1}e^{-t}dt,$$

and $\psi(x) < c_{N_0}x$ *for every* $x \geq N_0$.

Proof. Since $\psi(x)$ jumps only at prime powers, it follows that

$$\boldsymbol{H}(\alpha,\boldsymbol{X}) = \int_{N_0}^{\infty} \frac{e^{-t/\boldsymbol{X}}}{t^{\alpha}\log(t)} d\psi(t)$$

Using the results in Rosser and Schoenfeld [31], we have $\psi(x) < c_{N_0}x$ for $x \geq N_0 - 1/2$, and some $c_{N_0} > 1$. Since Chebyshev showed that $\psi(x) \sim x$ (cf. [15]) this constant goes to 1 as N_0 goes to infinity, but Rosser and Schoenfeld give an explicit constant of

$$1 + \frac{\log(N_0)^2}{8\pi\sqrt{N_0}}$$

assuming the Riemann Hypothesis.

Integration by parts now yields

$$\begin{aligned}
\boldsymbol{H}(\alpha, \boldsymbol{X}) &\leq \frac{e^{-N_0/\boldsymbol{X}}}{N_0^\alpha \log(N_0)}(c_{N_0}N_0 - \psi(N_0) + c_{N_0}\int_{N_0}^{\infty} \frac{e^{-t/\boldsymbol{X}}}{t^\alpha \log(t)}dt \\
&\leq \frac{e^{-N_0/\boldsymbol{X}}}{N_0^\alpha \log(N_0)}(c_{N_0}N_0 - \psi(N_0)) + \frac{c_{N_0}}{\log(N_0)}\int_{N_0}^{\infty} \frac{e^{-t/\boldsymbol{X}}}{t^\alpha}dt \\
&= \frac{e^{-N_0/\boldsymbol{X}}}{N_0^\alpha \log(N_0)}(c_{N_0}N_0 - \psi(N_0)) + \frac{c_{N_0}e^{-N_0/\boldsymbol{X}}\boldsymbol{X}^{1-\alpha}}{\log(N_0)}\Gamma(1-\alpha, N_0/\boldsymbol{X}).
\end{aligned}$$

□

We now return to the proof of Theorem 1.2. Notice that we have now shown that the only terms involving D are the terms $\frac{\sigma-1}{2}\log\left(\frac{q}{4\pi^2}\right)$, $c_{\theta,\sigma,\boldsymbol{X},q,2}$ and $-c_{\theta,\sigma,\boldsymbol{X},m,1}$.

Investigating equation (3.9) shows that if the constant in front of $\log(D)$ is less than $\frac{1}{2}$, then we will have a result of the form $D \leq c$. Therefore, it only remains to show that there is an $\boldsymbol{X}$ such that the coefficient in front of D is less than or equal to $\frac{1}{2}$. Plugging in $m = D$ and $q = pD^2$, and using our bounds for $\alpha(\boldsymbol{X})$, $\gamma(\boldsymbol{X})$ and $\delta(\boldsymbol{X})$ obtained in Lemma 3.33, we see that the limit of the power of D as $\boldsymbol{X} \to \infty$ is $\sigma - 1$. Since $\sigma < \frac{3}{2}$, such an $\boldsymbol{X}$ exists. □

Remark 3.38. *In practice, we will fix a constant N_0 and use cancellation between the first N_0 terms of the sum in equation (3.71) and the first N_0 terms of (3.72) to get a better explicit bound. The details are described further in Section 4.2.3.*

Chapter 4

Explicit Algorithms for Computing Good Bounds for E

4.1 Introduction

In Chapter 3([21]), we have shown an effective bound for certain positive definite ternary quadratic forms representing every integer up to local conditions, conditional upon GRH for Dirichlet L-functions and L-functions of weight 2 newforms. In this chapter, we give an algorithm to compute this bound and use it to obtain a good bound for E. The algorithm is mainly comprised of an efficient decompostion of a certain space of modular forms and the computation of bounds for certain constants defined in Chapter 3 ([21]). Using this algorithm, a good bound for E is calculated for every $E/\overline{\mathbb{F}_p}$ with $p \leq 107$.

The chapter concludes with computational data obtained using the algorithms described herein to obtain good bounds D_p for $p \leq 107$ and computations of the set of fundamental discriminants $-D > -D_p$ for which the map is not surjective. For $p \in \{3, 5, 7, 13\}$, a simple dimension argument about modular forms shows that every D is a good bound for p. Collecting the data for the primes $p \leq 107$, the following theorem is obtained.

Theorem 4.1. *Assume GRH for Dirichlet L-functions and L-functions of weight 2*

p	*Good Bound D_p for p.*	p	*Good Bound D_p for p.*
$3, 5, 7, 13$	1	59	1.166×10^{19}
11	5.359×10^{9}	61	1.413×10^{17}
17	1.221×10^{14}	67	2.323×10^{19}
19	7.544×10^{12}	71	1.793×10^{21}
23	2.418×10^{16}	73	7.035×10^{17}
29	4.305×10^{15}	79	2.370×10^{20}
31	4.866×10^{16}	83	1.033×10^{20}
37	4.552×10^{14}	89	3.257×10^{25}
41	1.786×10^{18}	97	4.750×10^{18}
43	2.069×10^{15}	101	5.296×10^{20}
47	1.804×10^{18}	103	8.748×10^{19}
53	3.817×10^{19}	107	1.761×10^{21}

Table 1: Good bounds D_p for every prime $p \leq 107$.

newforms. Then 3.257×10^{25} *is a good bound for $p \leq 107$. More precisely, we obtain Table 1 of good bounds D_p for each p.*

For a fixed fundamental discriminant $-D$, we also show an algorithm to determine whether the reduction map from elliptic curves with CM by $\mathcal{O}_{-D}$ is surjective. In cases where the good bound obtained is small enough, we furthermore compute whether the map is surjective for each fundamental discriminant $-D > -D_p$, hence giving a full list of D for which the map is surjective, conditional upon GRH. To accomplish this for a wider range of p, a specialized algorithm is given here for computing surjectivity more efficiently for $D < D_p$ when the supersingular elliptic curves are defined over $\mathbb{F}_p$. For those defined over $\mathbb{F}_{p^2}$, to reduce calculations we simply have a loop with variables x, y, and z, and bound x and y by a fixed constant.

The bound D_p is feasible for $p = 11$, $p = 17$, and $p = 19$, using our specialized algorithm and the fact that every supersingular elliptic curve is defined over $\mathbb{F}_p$. This yields the following theorems.

Theorem 4.2. *Assume GRH for Dirichlet L-functions and L-functions of weight 2 newforms. Then the reduction map mod* 11 *from elliptic curves with CM by* $\mathcal{O}_{-D}$ *is surjective for every fundamental discriminant* $-D$ *for which* 11 *does not split if and only if*

$$D \notin \{3, 4, 11, 67, 88, 91, 163, 187, 232, 235, 427499, 595, 627, 715, 907, 1387, \\ 1411, 3003, 3355, 4411, 5107, 6787, 10483, 11803\} \quad (4.1)$$

Theorem 4.3. *Assume GRH for Dirichlet L-functions and L-functions of weight 2 newforms. Then the set of fundamental discriminants* $-D$ *for which* 17 *does not split and the reduction map mod* 17 *from elliptic curves with CM by* $\mathcal{O}_{-D}$ *is not surjective has size* 91*, the largest of which is* $D = 89563$.

Theorem 4.4. *Assume GRH for Dirichlet L-functions and L-functions of weight 2 newforms. Then the set of fundamental discriminants* $-D$ *for which* 19 *does not split and the reduction map mod* 19 *from elliptic curves with CM by* $\mathcal{O}_{-D}$ *is not surjective has size* 45*, the largest of which is* $D = 27955$.

Having established such surjectivity results, it is straightforward to ask whether similar results can be shown about the multiplicity of the reduction map. This question was addressed and an ineffective solution was given by Elkies, Ono, and Yang [12]. We will need to define two functions before giving their result as it is stated in their paper.

For $-D$ a fundamental discriminant, define $\mathbb{H}_D(x) \in \mathbb{Q}[x]$ to be the Hilbert class polynomial, of degree $h(-D)$, whose roots are precisely the j-invariants of the elliptic curves with complex multiplication by $\mathcal{O}_{-D}$. These roots are referred to as *singular moduli of discriminant* $-D$.

Define further $S_p(x) \in \mathbb{F}_p[x]$ to be the polynomial with roots precisely the j-invariants of those elliptic curves defined over $\overline{\mathbb{F}_p}$ which are supersingular. Since the j-invariant is invariant modulo the prime p under the Deuring map, our result may be rewritten as follows.

Theorem 4.5. *Conditional upon GRH for Dirichlet* L*-functions and* L*-functions of weight 2 newforms, there is an effectively computable constant* D_p *such that for all* $D > D_p$ *up to local conditions,*

$$S_p(x) \mid \mathbb{H}_D(x)$$

over $\mathbb{F}_p[x]$.

Elkies, Ono, and Yang have shown unconditionally in [12] the following unconditional but ineffective answer to the question of multiplicity.

Theorem 4.6 (Elkies-Ono-Yang [12])**.** *Fix* $t \geq 1$. *There exists an (ineffective) constant* $D_{p,t}$ *such that, for every fundamental discriminant* $-D < -D_{p,t}$ *for which* p *does not split in* $\mathcal{O}_{-D}$,

$$S_p(x)^t \mid \mathbb{H}_D(x)$$

over $\mathbb{F}_p[x]$.

In terms of our notation, they have shown for every $t \geq 1$, every supersingular elliptic curve over $\overline{\mathbb{F}_p}$ lifts to at least t elliptic curves with CM by $\mathcal{O}_{-D}$ whenever D is sufficiently large. A slight alteration to our proof in [21] would lead to an effectively computable bound of this type, conditional upon GRH for L-functions of weight 2 newforms and Dirichlet L-functions, which should be feasible for small p and small t.

Using the connection between bounds for coefficients of theta series and good bounds for E described in Section 2.1, it will suffice to show a good bound for Q for each Q with associated theta in Kohnen's plus space of level $4p$. In Section 3.7, we obtained a bound for coefficients of these theta series. Given the connection from Section 2.1, this gives a good bound for E, dependent on numerically calculating certain constants, and hence a good bound for p, since there are only finitely many supersingular elliptic curves over $\overline{\mathbb{F}_p}$. In Section 4.2, we fix a basis and decompose a certain space of modular forms in order to calculate some of the constants obtained from Section 3.7. Furthermore, we give explicit algorithms for calculating the remaining constants carefully in order to obtain better good bounds for E. In Section 4.3, we use a trick based on the Ibukiyama's classification [16] of the set of $\mathcal{O}_E$, when E is defined over $\mathbb{F}_p$, in order to calculate the set of $D < D_E$ which are generated by Q_E. Finally, in Section 4.4, we give a summary of the results obtained by explicitly implementing the algorithms from Sections 4.2 and 4.3 for $p \leq 107$.

4.2 Algorithm to compute D_E and D_p

We will first calculate the maximal order, then the corresponding quadratic forms. Once we have obtained the quadratic forms, we decompose the space into the Eisenstein series and a direct sum of Hecke eigenforms. We will also give an algorithm to choose the Hecke eigenforms g_i and a choice of the Shimura lift S. This will allow us to calculate the constants b_i. In order to calculate the constants c_i, we use S in order to obtain the Shimura lifts G_i, and then we may use a result of Cremona [5] in order to calculate the special value of a twist of G_i.

These algorithms are implemented using MAGMA [3] and the C programming language. Many algorithms are made more efficient by built in functionality in MAGMA, and the wonderful implementations made the actual calculations much simpler. I would like to thank anyone who has contributed to this wonderful computer algebra system.

First we need to calculate the maximal orders of the quaternion algebra ramified exactly at p and ∞. We use Pizer's randomized algorithm [30]. This is based on choosing (randomly) an integral element of the algebra, and then finding the corresponding quadratic order. Then membership in the quaternion order is quickly checked, since this simply corresponds to calculating whether adding it to the existing matrix leads to an infinitely generated module over $\mathbb{Z}$ or not.

4.2.1 Calculating Maximal Orders and Theta Series

Using the algorithm of Pizer above, we calculate all of the maximal orders for the quaternion algebra ramified exactly at p and ∞ using a built in function in MAGMA. We next need to calculate the theta series of all of these. Since we have the 4 generators of the maximal order, we will represent any sublattice by a 4×4 matrix. The j-th column will represent the coefficients of the j-th generator in terms of the standard basis of 1, α, β, and $\alpha\beta$ with $\alpha^2 = -p$, $\beta^2 = -q$, and $\beta\alpha = -\alpha\beta$.

We can find another set of generators by applying $SL_4(\mathbb{Z})$ operations. Doing so, we can find a choice of generators so that the corresponding matrix is lower triangular. Since it is lower triangular, finding the trace zero elements is simple, as the only generator which is not trace zero is the element represented by the first column.

Adding an Element to a Lattice

We will describe here the function which takes a $\mathbb{Z}$-module M and an additional element and returns the module generated by the element and M. Using our representation of the lattice as a 4×4 matrix, we generate the new lattice by taking the 4×5 matrix with the first 4 columns identical to the lattice and the 5-th column representing the additional element. We then do column operations until the number of non-zero columns matches the rank of the matrix and the matrix is in lower triangular form.

Getting a Basis for L_E

We take each maximal order, multiply by 2, and add the element $1 = (1, 0, 0, 0)$ using the above function. We have now generated the Gross order. Since our matrix is in lower triangular form, the trace zero elements are simply the elements which are linear combinations of columns 2 through 4. We thus obtain a basis of L_E by taking the generators represented by columns 2 through 4.

Finding the θ-Series

Now that we have computed generators for L_E, we need to calculate the corresponding θ-series up to a fixed chosen C coefficients. To do so, we first need to calculate the quadratic form

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz.$$

This is a simple calculation, since, if the basis of the trace zero elements are $\gamma_2, \gamma_3, \gamma_4$, with $\gamma_i = \sum_{j=2}^{4} L_{j,i}\delta_j$ for $\delta_2 = \alpha$, $\delta_3 = \beta$, $\delta_4 = \alpha\beta$, and $L_{j,i} \in \mathbb{Q}$, then, since the matrix is lower triangular,

$$Q(x,y,z) = N(x\gamma_2+y\gamma_3+z\gamma_4) = (L_{2,2}^2p+L_{3,2}^2q+L_{4,2}^2pq)x^2+(L_{3,3}^2q+L_{4,3}^2pq)y^2+L_{4,4}^2pqz^2$$
$$+ (2(L_{3,3}L_{3,2}q + L_{4,3}L_{4,2}pq))xy + (2L_{4,4}L_{4,2}pq)xz + (2L_{4,4}L_{4,3}pq)yz.$$

We then simply run over all (x, y, z) such that $Q(x, y, z) \leq C$, noting that Q is positive definite. To determine the range of x, y, and z satisfying these conditions, we first assume x and y are fixed and solve the equation $Q(x, y, z) = C$ for z, running our innermost loop between these solutions. Then we find $z_{x,y}$ which minimizes $Q(x, y, z) - C$ with x and y fixed and find the solutions for y to the equation $Q(x, y, z_{x,y}) = C$. Our second most inner loop runs between these solutions. Finally, we solve for y_x which minimizes $Q(x, y, z_{x,y}) - C$ and run our outermost loop between the solutions to $Q(x, y_x, z_{x,y_x}) = C$.

4.2.2 Decomposition and Choice of the Hecke Eigenforms and Shimura Lift

Calculating the Cuspidal Contribution

We subtract the Eisenstein series from each θ-series to get the cuspidal part. This is calculated by using the formula in [14] for the Eisenstein series and the built in functionality of MAGMA to calculate the class numbers. For each θ, we have now calculated the cusp form

$$g := \theta - E \in S_{3/2}^{+}(4p).$$

Finding Significant Coefficients

To distinguish between different cusp forms, we need to find which coefficients of the cusp forms we want to compare, so we must find $t-1$ independent coefficients of the $t-1$ cusp forms, where t is the type number. To do so, we simply add the next coefficient as a new column one at a time to a matrix, and then check the new rank of the matrix. If the rank increases, we keep this coefficient, and otherwise we refill this column with the next possible coefficient. Thus, in the end we return the matrix containing as the i-th row the first $t-1$ independent coefficients of the i-th g, as well as an array listing which coefficients these are. Since Gross [14] showed that the subspace of $S_{3/2}^{+}(4p)$ containing these theta series is spanned by the theta series, these coefficients will suffice to distinguish any cusp forms.

Checking if a form g is in the span of other forms

We will often need to check whether a particular cusp form is in the span of another set of cusp forms, or if it is independent of those forms. To do so, we first calculate as above the significant coefficients.

After we know which coefficients to check, we simply make the matrix as above and then check if adding another row corresponding to the coefficients of our new form is consistent with the matrix. If it is consistent, then this returns a solution so that we can write g in terms of the existing forms. Otherwise, we know that it is not a linear combination of these previous terms.

Calculation of Hecke Eigenforms

We would now like to decompose our cusp form g into a sum of Hecke eigenforms. To do so, we first determine the action of the Hecke algebra on g. First note that $S_2(p) = S_2^{\text{new}}(p)$, so that we have multiplicity one.

Kohnen has shown that there is an isomorphism between $S^+_{3/2}(4p)$ and $S_2^{\text{new}}(p)$ which commutes with the Hecke operators T_n for $(n, p) = 1$ [24]. Therefore, if we fix a newform $g_i \in S^+_{3/2}(4p)$, then we know that the eigenspace of cusp forms which have the same eigenvalues as g_i is dimension one. Furthermore, Sturm has shown that a finite set of Hecke operators generates the Hecke algebra and has given an effectively computable bound N so that $\{T_{n^2}|n \leq N\}$ generates the Hecke algebra [36]. Hence we will only need to diagonalize a finite number of Hecke operators in order to determine the eigenspace.

Calculating the coefficients under the Hecke operators is a simple calculation (cf. [28]). We will diagonalize incrementally each Hecke operator $T = T_{n^2}$. After each diagonalization, we will divide the space into subspaces $V_{1,n}, V_{2,n}, \ldots V_{m,n}$ such that for every $f, g \in V_{i,n}$ the eigenvalues of f equal the eigenvalues of g for every $n' \leq n$. By our discussion above, the dimension of $V_{i,n}$ will be one for every i and some $n \leq N$. For each Hecke operator, we simply iterate the Hecke operator T

$$g, g|T, g|T^2, g|T^3, \ldots,$$

using our function above to check at each stage whether $g|T^n$ is in the span of the set $\{g, g|T, g|T^2, \ldots, g|T^{n-1}\}$. As soon as this occurs, we get an operator matrix with all zeros, except ones directly below the diagonal and the last column is the coefficients of the linear combination of $g|T^i$ that yield $g|T^n$.

The special form of this matrix makes the characteristic polynomial simple to determine and hence it is straightforward to diagonalize.

From computational evidence, the following conjecture seems very likely.

Conjecture 4.7. *There exists a cusp form $g = \theta - E$ such that the closure of g under the Hecke algebra generates the entire subspace of cusp forms spanned by the all of the cusp forms $\theta' - E$.*

Assuming Conjecture 4.7, we can find a particular g such that the closure of g under the Hecke algebra generates the entire space. Take such a g. Note that if this conjecture is not true, we simply need to repeat this process for each subspace, but we have verified the conjecture for all $p < 1000$. We now diagonalize the Hecke operator matrices for this g to determine the eigenvectors. If one of the eigenspaces is dimension greater than one, then we choose another Hecke operator T and diagonalize again, until we have dimension one.

Choosing a Shimura Lift and Choosing g_i

We will now choose an embedding into $S_2(p)$, shown to exist by the Shimura lift between $S^+_{3/2}(4p)$ and $S_2^{\mathrm{new}}(p) = S_2(p)$ [24].

We start by calculating a basis for $S_2(p)$, a built in function in MAGMA. Then we compute enough coefficients of the t-th Shimura correspondence (cf. [28])

$$\sum_{n=1}^{\infty} \frac{a_{g|S_t}(n)}{n^s} := L(\chi_{-t}, s) \sum_{n=1}^{\infty} \frac{a_g(tn^2)}{n^s}$$

for all $t < t_0$ on the form g which generates the subspace. Since g generates the entire subspace, $g|S$ is in $S_2(p)$ if and only if every such $(\theta - E)|S \in S_2(p)$.

We first check that $g|S_t \neq 0$, and iterate this process with t_0 larger until there exist constants c_t such that

$$S := \sum_{t<t_0} c_t S_t$$

satisfies $g|S \in S_2(p)$. Here we again use our function to check whether one form can be written as the sum of other forms to determine whether $g|S$ can be written in terms of the basis for $S_2(p)$, using Sturm's bound to determine which coeffients to compare.

Now that we have the choice S of a Shimura lift, we are ready to choose g_i. We have already decomposed our space above in Section 4.2.2, so we have chosen g_i up to a constant. Under the fixed embedding S, we will normalize g_i so that its Shimura lift G_i has constant coefficient 1.

Calculating b_i

We are now able to calculate b_i. Since we have fixed our choice of g_i in Section 4.2.2, we only need to use our function to determine g as a linear combination of these eigenforms, for each g. The coefficients obtained from this function are b_i, so that $g = \sum_{i=1}^{t} b_i g_i$.

Calculating c_i

Recall first that

$$c_i = \frac{|a_{g_i}(m_i)|^2}{L(G_i, m_i, 1) m_i^{1/2}}$$

for m_i a fixed integer such that $a_{g_i}(m_i) \neq 0$ and $m_i \not\equiv 0 \pmod{p}$. We may simply choose m_i to be the smallest such integer.

Since we have already calculated g_i, we already have $a_{g_i}(m_i)$. It remains to find $L(G_i, m_i, 1)$. After using the Shimura lift to find G_i, we use the following formula of

Cremona [5],

$$L(G_i, m_i, 1) = \sum_{n=1}^{\infty} 2a_L(n)\chi(n)e^{-2\pi i \frac{n}{m_i\sqrt{p}}},$$

which is shown to converge very quickly, so that we may calculate $L(G_i, m_i, 1)$ to a sufficient accuracy by calculating the partial sum

$$\sum_{n=1}^{K} 2a_L(n)\chi(n)e^{-2\pi i \frac{n}{m_i\sqrt{p}}}$$

and choosing K large enough. A very small number of coefficients is actually needed, since the partial sum with $K = 100$ is accurate to beyond 25 decimal places.

4.2.3 Calculating the other constants from Section 3.7

These constants are actually fairly easy to calculate once we show clearly where they come from, given the theoretical results stated in [21]. The methods involved and notation used are similar to those used in [29].

Most of the constants obtained are explicit in terms of Γ and ζ factors along the real line, but we need some work to calculate the terms involving F, F_1, and G. Define $v(n, \boldsymbol{X})$ by

$$v(n, \boldsymbol{X}) := c_{\theta,\boldsymbol{X},1,\boldsymbol{F}} \frac{\lambda_i(n)e^{-n/\boldsymbol{X}}}{n^{\sigma}} + c_{\theta,\boldsymbol{X},1,\boldsymbol{F}_1} \frac{\log(n)\lambda_i(n)e^{-n/\boldsymbol{X}}}{n^{\sigma_2}} - c_{\theta,\boldsymbol{X},2,G} \left(\frac{\Lambda(n)e^{-n/\boldsymbol{X}}}{n^{\sigma_0}} - \frac{\Lambda(n)e^{-n/\boldsymbol{X}}}{n^{\sigma}} \right),$$

where $\sigma = \text{Re}(s)$, $\sigma_0 = \text{Re}(2 - s)$, and $\sigma_2 = \text{Re}(s_2)$, so that

$$\sum_{n=2}^{\infty} \text{Re}\left(\frac{\chi(n)}{n^{it}\log(n)} v(n, \boldsymbol{X}) \right) = c_{\theta,\boldsymbol{X},1,\boldsymbol{F}} \text{Re}(\boldsymbol{F}(s, \boldsymbol{X})) + c_{\theta,\boldsymbol{X},1,\boldsymbol{F}_1} \text{Re}(\boldsymbol{F}_1(s_2, \boldsymbol{X})) - c_{\theta,\boldsymbol{X},2,G} \text{Re}(\boldsymbol{G}(s_0, \boldsymbol{X}) - \boldsymbol{G}(s, \boldsymbol{X})).$$

We will bound the following to get a constant independent of the variables involved. From above, we need to bound

$$-2\log|L(s)| + 2\sum_{n=2}^{N_0}\mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s\log(n)}\right). \tag{4.2}$$

We also need a bound for the constants depending on t, the imaginary part of s. We will use the Γ factor to remove these terms. Thus, we will bound

$$\log|\Gamma(s)| + c_{\theta,\boldsymbol{X},1,t} - c_{\theta,\boldsymbol{X},2,t}. \tag{4.3}$$

A computer is then used to bound

$$\sum_{n=2}^{N_0}\mathrm{Re}\left(\frac{\chi(n)}{n^{it}\log(n)}\left(v(n,\boldsymbol{X}) - \frac{2\Lambda(n)}{n^\sigma}\right)\right). \tag{4.4}$$

Notice that the term we are subtracting is exactly the term being added in Equation (4.2). The only nonzero terms are p powers, so the maximum is taken by calculating $\frac{1}{\log(n)}\left(v(n,\boldsymbol{X}) - \frac{2\Lambda(n)}{n^\sigma}\right)$ for each $n = p^k$ and then noting that either $\chi(p^k) = \chi(p)^k$, which is either one or alternates. Finding the t which maximizes this sum for each p, independent of whether the sum alternates or not, gives the bound, since we then add up the absolute value of each of these terms together.

It remains to bound

$$\sum_{n=N_0+1}^{\infty}\mathrm{Re}\left(\frac{\chi(n)}{n^{it}\log(n)}(v(n,\boldsymbol{X}))\right). \tag{4.5}$$

We first bound the part dependent on t in equation (4.3) by noting that the dependence on t in the logarithm is polynomial in t, while Γ decays exponentially. We will find that in every case that we check for each σ, the decay swamps this growth so that the maximum is attained at $t = 0$. Therefore,

$$\log|\Gamma(s)| + c_{\theta,\boldsymbol{X},1,t} - c_{\theta,\boldsymbol{X},2,t} \le \log|\Gamma(\sigma)|,$$

so this contribution will be added to our constant $c_{\theta,\boldsymbol{X},1}$.

We next show how to bound Equation (4.2), the term involving $\log(L(s))$. Noting that

$$\log(|L(s)|) = \sum_{n=2}^{\infty} \mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s}\log(n)\right),$$

we have

$$-2\log(|L(s)|) + 2\sum_{n=2}^{N_0} \mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s\log(n)}\right) = -2\sum_{n=N_0}^{\infty} \mathrm{Re}\left(\frac{\Lambda(n)}{n^s\log(n)}\right).$$

Therefore, taking the absolute value inside the sum gives

$$-2\sum_{n=N_0}^{\infty} \frac{\Lambda(n)}{n^s\log(n)} \leq 2\sum_{n=N_0+1}^{\infty} \frac{\Lambda(n)}{n^\sigma\log(n)} = 2\log(|\zeta(\sigma)|) - \sum_{n=2}^{N_0} \frac{\Lambda(n)}{n^\sigma\log(n)},$$

and this final finite sum and $\zeta(\sigma)$ are easily computed.

Finally, we need to find a bound for the remaining terms in Equation (4.5). Notice first, since $\sigma_2 > \sigma$, that for n sufficiently (namely we choose N_0 such that this occurs for $n > N_0$) the term from the $\boldsymbol{F}_1$ part of $v(n, \boldsymbol{X})$ satisfies the bound

$$c_{\theta,\boldsymbol{X},1,\boldsymbol{F}_1}\frac{\log(n)}{n^{\sigma_2}} \leq \frac{c_{\theta,\boldsymbol{X},1,\boldsymbol{F}}}{n^\sigma}.$$

Therefore, we see that

$$|v(n,\boldsymbol{X})| \leq e^{-n/\boldsymbol{X}}\left(2c_{\theta,\boldsymbol{X},1,\boldsymbol{F}}\frac{|\lambda_i(n)|}{n^\sigma} + c_{\theta,\boldsymbol{X},2,G}\Lambda(n)\left(\frac{1}{n^{\sigma_0}} - \frac{1}{n^\sigma}\right)\right).$$

Since $\lambda_i(n) \leq 2\sqrt{n}\log(n)$, we can further bound this by

$$c_{\theta,\boldsymbol{X},v}\frac{\Lambda(n)}{n^{min(\sigma-1/2,\sigma_0)}}e^{-n/x}.$$

In [21], we have shown for $\alpha = \min(\sigma - 1/2, \sigma_0)$ an explicit constant c_{N_0} such that

$$\begin{aligned}\boldsymbol{H}(\alpha,\boldsymbol{X}) = &\sum_{n=N_0+1}^{\infty} \frac{\Lambda(n)}{n^\alpha\log(n)}e^{-n/x} \\ &\leq \frac{e^{-N_0/\boldsymbol{X}}}{N_0^\alpha\log(N_0)}(c_{N_0}N_0 - \psi(N_0)) + \frac{c_{N_0}\boldsymbol{X}^{1-\alpha}}{\log(N_0)}\Gamma(1-\alpha, N_0/\boldsymbol{X}). \quad (4.6)\end{aligned}$$

We then calculate the incomplete Gamma factor $\Gamma(1-\alpha, N_0/\boldsymbol{X})$ using another built in function in MAGMA.

4.3 Determining CM Lifts for $D < D_E$ when E is Defined over $\mathbb{F}_p$

In this section, we give an algorithm to determine whether $E/\mathbb{F}_p$ is in the image of the reduction map from elliptic curves with CM by $\mathcal{O}_{-D}$ for a fixed D to deal with $D < D_E$.

4.3.1 Calculating which D are Represented by the Gross Lattice

Lemma 4.8. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ and let L_E be its associated Gross lattice and $\mathcal{O}_E^0$ be the lattice of trace zero coefficients. Then there exists a lattice L satisfying $L_E \subseteq L \subset \mathcal{O}_E^0$ such that L is $\mathbb{Z}$-equivalent to $(\mathbb{Z}, Q)$ of the form*

$$Q(x, y, z) = px^2 + (by^2 + fyz + cz^2).$$

Proof. Ibukiyama [16] shows that all maximal orders of this type are either of the form

$$\mathcal{O}(q, r) := \mathbb{Z} + \mathbb{Z}\frac{1+\beta}{2} + \mathbb{Z}\frac{\alpha(1+\beta)}{2} + \mathbb{Z}\frac{(r+\alpha)\beta}{q} \tag{4.7}$$

or

$$\mathcal{O}'(q, r') := \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(r'+\alpha)\beta}{2q}, \tag{4.8}$$

where q is a prime satisfying $q \equiv 3 \pmod 8$ and $\left(\frac{-q}{p}\right) = -1$, $\alpha^2 = -p$, $\beta^2 = -q$, $\alpha\beta = -\beta\alpha$, $r^2 + p \equiv 0 \pmod q$ and $r'^2 + p \equiv 0 \pmod{4q}$ in the case when $p \equiv 3 \pmod 4$.

The lattice generated by the trace zero coefficients of y even and setting $x' := x - ry$, $y' := z + qy$ and $z' := y$ gives the quadratic form

$$q(x')^2 + \frac{r^2+p}{q}(y')^2 + p(z')^2 + 2rx'y',$$

as desired, since every element of the Gross lattice is an element of this lattice with z even. Changing z to $2z$ above implies that $y' \equiv z' \pmod 2$, while otherwise x', y', and z' can be any arbitrary integer.

For elements of $O'(q, r')$, we have a simpler task. In this case, the corresponding quadratic form for $O'(q, r')$ is simply

$$px^2 + qy^2 + \frac{(r')^2+p}{4q}z^2 + r'yz.$$

To get the elements of the Gross lattice, we simply multiply y and z by 2 to get

$$Q'(x, y, z) := px^2 + (4q)y^2 + \frac{(r')^2+p}{q}z^2 + (4r')yz.$$

□

Given Lemma 4.8, the quadratic forms from L_E are either of the form

$$Q(x', y', z') := q(x')^2 + \frac{r^2+p}{q}(y')^2 + p(z')^2 + 2rx'y',$$

with $y' \equiv z' \pmod 2$, or

$$Q'(x, y, z) := px^2 + (4q)y^2 + \frac{(r')^2+p}{q}z^2 + (4r')yz.$$

To check if an integer n is represented, we first set two integers M and N and do a precomputation for efficiency. For Q, we do a precomputation of the two sets

$$SE_M := \{n \leq M : n = q(x')^2 + \frac{r^2+p}{q}(y')^2 + 2rx'y', y' \text{ even}\},$$

and analogously

$$SO_M := \{n \leq M : n = q(x')^2 + \frac{r^2+p}{q}(y')^2 + 2rx'y', y' \text{ odd}\}.$$

Since we know that, with x' fixed, the minimum value is obtained at $xdiv := (q - \frac{rq}{p+r^2})x'^2$, we run x' from 0 to $\left(\frac{M}{xdiv}\right)^{1/2}$ and then y' from 0 to $\frac{2rx' + \sqrt{4r^2x' - 4\frac{p+r^2}{q}\cdot(q(x')^2 - M)}}{2\frac{p+r^2}{q}}$, and simply calculate $n = Q(x', y', 0)$. If y' is odd, we add n to SO_M, and if y' is even then we add n to SE_M.

Similarly, for Q', we calculate

$$S_M := \{n \leq M : n = Q'(0, y, z)\}.$$

Given SE_M and SO_M, we now calculate

$$T_{N,M} := \{n \leq N : n = m + p(z')^2, m \in SE_M \text{ and } z' \text{ even, or } m \in SO_M \text{ and } z' \text{ odd}\}.$$

Notice that, if we define

$$T_N := \{n \leq N : n = Q(x', y', z'), y' \equiv z' \pmod 2\},$$

then $T_M \subseteq T_{N,M} \subseteq T_N$. Therefore, for every $n \in T_{N,M}$, we know $n \in T_N$, and for every $n \notin T_{N,M}$ with $n \leq M$, we know $n \notin T_N$. Since we expect that after a low bound M we will not have any such eligible elements which are not in T_N, we can set M lower for optimization purposes.

We now describe the algorithm to calculate $T_{N,M}$. For each eligible $D \leq n$, we check from $z' = \left(\frac{D-M}{p}\right)^{1/2}$ to $z' = \left(\frac{D}{p}\right)^{1/2}$. For each z', if z' is even, then we check if $D - p(z')^2 \in SE_M$, and if z' is odd, we check if $D - p(z')^2 \in SO_M$. If so, then we add D to $T_{N,M}$. The algorithm for Q' is entirely analogous, only needing to check membership in S_M instead of breaking it up into the even and odd cases. We know that $np^2 \in T_{N,M}$ if and only if $n \in T_{N,M}$, so we can skip checking these cases.

We shall show that the running time for this function is $O(p+NM^{1/2})$. We need time $O(M)$ to calculate SE_M and SO_M. Calculating the modulus of p which are eligible takes time $O(p)$. For each D, we have to check at most $M^{1/2}$ possible z'. Therefore, since there are $O(N)$ such D, this calculation takes $O(NM^{1/2})$. Thus, the overall running time is $O(M+p+NM^{1/2}) = O(p+NM^{1/2})$ (since we will choose $N > p$, we have $O(NM^{1/2})$).

Notice that for an individual $n \notin T_{N,M}$, we can check membership in T_N in $O(N^{1/2})$ time by calculating checking membership in SE_N and SO_N (or S_N for O'). By doing this as a precomputation again, we get a running time of $O(N + N^{1/2}E)$ where E is the number of exceptional $D \notin T_{N,M}$. Therefore, if we choose M so that $E < (NM)^{1/2}$, then we can calculate T_N in $O(NM^{1/2})$.

4.4 Data

Using the algorithm described in Section 4.2, we will find a good bound for each E with $p \leq 107$. For p fixed, the maximum good bound for E will give a good bound for p.

Example 4.9. *We will now compute good bounds for $p \leq 107$, using $\boldsymbol{X} = 455$, $\sigma = 1.15$, $N_0 = 1000$, and $\sigma_2 = 1.3256$ (These were chosen by a binary search for σ and a heuristically based search for σ_2 given σ.). The table below will give our results in the following manner. For each maximal order M, we will list the prime p, then the size of the field $\mathbb{F}_q$ ($q = p$ or $q = p^2$) which the corresponding elliptic curve is defined over. We will then list the corresponding ternary quadratic form as $[a, b, c, d, e, f] = ax^2 + by^2 + cz^2 + dxy + exz + fyz$. We then list a good bound D_0 for E which suffices* *when $(D,p)=1$, and a good bound D_1 which also suffices when $p \mid D$. We separate these cases since a better bound is obtained for D relatively prime to p and skipping $(D,p)=1$ is a computational gain. We omit here the primes 3, 5, 7, and 13, since we have $D_p = 1$ trivially. Theorem 4.1 follows from the data obtained below in Tables 2, 3, 4, and 5.*

Example 4.10. *Now we use the method of Bhargava [1] described in Section 4.3 to check which discriminants are not represented up to a feasible N. When our feasible bound N is greater than the bounds D_0 and D_1 above, then we have (conditional upon GRH) a full list of all discriminants which are not represented and do not have $p^2 \mid d$ (We know that d is represented if and only if dp^2 is represented [21]). We will list the quadratic form corresponding to our maximal order, along with the bounds N_0/N_1 which we have checked up to, and a full list of all $d < N_0$ and all $d = pd_2 < N_1$ which are not represented by the form. We shall omit dp^2 from our list to save space. This data is presented in Tables 6, 7, and 8 below.*

Looking at Table 6 from Example 4.10 and comparing with the bound from Table 2 in Example 4.9, we see that $N_0 > D_0$ and $N_1 > D_1$ when $p = 11$, $p = 17$ and $p = 19$. This shows Theorems 4.2, 4.3, and 4.4.

p	$\#\mathbb{F}_q$	*Quadratic Form*	D_0	D_1
11	p	$[4, 11, 12, 0, 4, 0]$	1.311×10^7	2.095×10^8
11	p	$[3, 15, 15, -2, 2, 14]$	3.354×10^8	5.359×10^9
17	p	$[7, 11, 20, -6, 4, 8]$	1.850×10^9	1.869×10^{10}
17	p	$[3, 23, 23, -2, 2, 22]$	7.640×10^{12}	1.221×10^{14}
19	p	$[7, 11, 23, -2, 6, 10]$	1.850×10^9	2.956×10^{10}
19	p	$[4, 19, 20, 0, 4, 0]$	4.722×10^{11}	7.544×10^{12}

Table 2: Good bounds D_Q for every $\theta_Q \in M^+_{3/2}(4p)$ with $p \le 19$.

p	$\#\mathbb{F}_q$	*Quadratic Form*	D_0	D_1
23	p	$[8, 12, 23, 4, 0, 0]$	1.143×10^{12}	5.539×10^{12}
23	p	$[4, 23, 24, 0, 4, 0]$	4.638×10^{14}	4.495×10^{15}
23	p	$[3, 31, 31, -2, 2, 30]$	3.870×10^{15}	2.418×10^{16}
29	p	$[11, 12, 32, 8, 4, 12]$	2.741×10^{11}	4.052×10^{11}
29	p	$[8, 15, 31, 4, 8, 2]$	1.377×10^{13}	1.054×10^{14}
29	p	$[3, 39, 39, -2, 2, 38]$	5.628×10^{14}	4.305×10^{15}
31	p	$[8, 16, 31, 4, 0, 0]$	3.730×10^{13}	4.397×10^{14}
31	p	$[7, 19, 36, -6, 4, 16]$	6.606×10^{13}	4.918×10^{14}
31	p	$[4, 31, 32, 0, 4, 0]$	5.219×10^{15}	4.866×10^{16}
37	p^2	$[15, 20, 23, -4, 14, 8]$	1.116×10^{11}	1.783×10^{12}
37	p	$[8, 19, 39, 4, 8, 2]$	2.849×10^{13}	4.552×10^{14}
41	p	$[12, 15, 44, 8, 12, 4]$	9.351×10^{13}	4.228×10^{14}
41	p	$[11, 15, 47, -2, 10, 14]$	4.647×10^{13}	7.424×10^{14}
41	p	$[7, 24, 47, 4, 2, 24]$	2.456×10^{15}	1.757×10^{16}
41	p	$[3, 55, 55, -2, 2, 54]$	2.036×10^{17}	1.786×10^{18}
43	p^2	$[15, 23, 24, 2, 8, 12]$	3.543×10^{10}	5.073×10^{11}
43	p	$[11, 16, 47, 4, 2, 16]$	8.333×10^{12}	1.289×10^{13}
43	p	$[4, 43, 44, 0, 4, 0]$	1.445×10^{14}	2.069×10^{15}
47	p	$[12, 16, 47, 4, 0, 0]$	4.927×10^{13}	6.552×10^{14}
47	p	$[8, 24, 47, 4, 0, 0]$	1.202×10^{15}	1.920×10^{16}
47	p	$[7, 27, 55, -2, 6, 26]$	2.699×10^{15}	2.308×10^{16}
47	p	$[4, 47, 48, 0, 4, 0]$	5.330×10^{16}	6.552×10^{17}
47	p	$[3, 63, 63, -2, 2, 62]$	1.797×10^{17}	1.804×10^{18}
53	p^2	$[20, 23, 32, -12, 4, 20]$	1.257×10^{14}	1.458×10^{15}
53	p	$[12, 19, 56, 8, 12, 4]$	5.001×10^{15}	7.990×10^{16}
53	p	$[8, 27, 55, 4, 8, 2]$	2.238×10^{16}	2.124×10^{17}
53	p	$[3, 71, 71, -2, 2, 70]$	4.046×10^{18}	3.817×10^{19}
59	p	$[15, 16, 63, 4, 2, 16]$	6.695×10^{13}	7.662×10^{14}
59	p	$[15, 19, 64, -14, 8, 12]$	6.695×10^{13}	7.662×10^{14}
59	p	$[7, 35, 68, -6, 4, 32]$	4.612×10^{14}	2.426×10^{15}
59	p	$[12, 20, 59, 4, 0, 0]$	2.811×10^{15}	4.492×10^{16}
59	p	$[4, 59, 60, 0, 4, 0]$	1.106×10^{17}	1.174×10^{18}
59	p	$[3, 79, 79, -2, 2, 78]$	7.295×10^{17}	1.166×10^{19}

Table 3: Good bounds D_Q for every $\theta_Q \in M^+_{3/2}(4p)$ with $23 \leq p \leq 59$.

p	$\#\mathbb{F}_q$	*Quadratic Form*	D_0	D_1
61	p^2	$[23, 24, 32, 16, 4, 12]$	3.596×10^{14}	3.209×10^{15}
61	p	$[7, 35, 71, -2, 6, 34]$	7.292×10^{14}	3.927×10^{15}
61	p	$[8, 31, 63, 4, 8, 2]$	6.102×10^{15}	4.342×10^{16}
61	p	$[11, 23, 68, -6, 8, 20]$	1.696×10^{16}	1.413×10^{17}
67	p^2	$[15, 36, 39, -4, 14, 16]$	1.115×10^{15}	1.781×10^{16}
67	p^2	$[23, 24, 35, 8, 2, 12]$	1.152×10^{15}	1.841×10^{16}
67	p	$[16, 19, 71, 12, 16, 6]$	1.359×10^{16}	2.171×10^{17}
67	p	$[4, 67, 68, 0, 4, 0]$	2.446×10^{17}	2.323×10^{19}
71	p	$[15, 20, 76, 8, 4, 20]$	2.458×10^{16}	1.815×10^{18}
71	p	$[15, 19, 79, -2, 14, 18]$	2.458×10^{16}	1.815×10^{18}
71	p	$[16, 20, 71, 12, 0, 0]$	6.707×10^{16}	9.247×10^{18}
71	p	$[12, 24, 71, 4, 0, 0]$	1.824×10^{17}	1.764×10^{19}
71	p	$[8, 36, 71, 4, 0, 0]$	5.578×10^{17}	7.929×10^{19}
71	p	$[4, 71, 72, 0, 4, 0]$	1.602×10^{19}	9.300×10^{20}
71	p	$[3, 95, 95, -2, 2, 94]$	1.123×10^{19}	1.793×10^{21}
73	p^2	$[15, 39, 40, 2, 8, 20]$	5.001×10^{14}	3.678×10^{15}
73	p^2	$[20, 31, 44, -12, 4, 28]$	2.856×10^{15}	1.710×10^{16}
73	p	$[7, 43, 84, -6, 4, 40]$	7.799×10^{15}	2.953×10^{16}
73	p	$[11, 28, 80, 8, 4, 28]$	8.360×10^{16}	7.035×10^{17}
79	p^2	$[23, 31, 44, 18, 16, 20]$	4.859×10^{15}	3.753×10^{16}
79	p	$[16, 20, 79, 4, 0, 0]$	7.326×10^{16}	8.289×10^{17}
79	p	$[19, 20, 84, 16, 8, 20]$	5.334×10^{17}	8.523×10^{18}
79	p	$[11, 31, 87, -10, 6, 26]$	1.017×10^{18}	1.119×10^{19}
79	p	$[8, 40, 79, 4, 0, 0]$	1.099×10^{18}	1.1402×10^{19}
79	p	$[4, 79, 80, 0, 4, 0]$	1.483×10^{19}	2.370×10^{20}
83	p^2	$[23, 31, 44, -14, 8, 12]$	4.054×10^{15}	6.477×10^{16}
83	p	$[12, 28, 83, 4, 0, 0]$	1.721×10^{16}	2.591×10^{17}
83	p	$[7, 48, 95, 4, 2, 48]$	3.913×10^{16}	6.251×10^{17}
83	p	$[16, 23, 87, 12, 16, 6]$	8.775×10^{16}	1.328×10^{18}
83	p	$[11, 31, 92, -6, 8, 28]$	1.574×10^{16}	2.514×10^{18}
83	p	$[3, 111, 111, -2, 2, 110]$	4.776×10^{18}	7.089×10^{19}
83	p	$[4, 83, 84, 0, 4, 0]$	6.461×10^{18}	1.033×10^{20}

Table 4: Good bounds D_Q for every $\theta_Q \in M^+_{3/2}(4p)$ with $61 \le p \le 83$.

p	$\#\mathbb{F}_q$	*Quadratic Form*	D_0	D_1
89	p^2	$[23, 31, 48, 2, 12, 16]$	1.480×10^{18}	2.869×10^{18}
89	p	$[15, 24, 95, 4, 2, 24]$	3.555×10^{18}	1.012×10^{19}
89	p	$[15, 27, 96, -14, 8, 20]$	3.555×10^{18}	1.012×10^{19}
89	p	$[19, 23, 95, -18, 10, 14]$	4.045×10^{18}	2.048×10^{19}
89	p	$[7, 51, 103, -2, 6, 50]$	1.663×10^{20}	3.582×10^{20}
89	p	$[3, 119, 119, -2, 2, 118]$	5.144×10^{21}	2.900×10^{22}
89	p	$[12, 31, 92, 8, 12, 4]$	5.724×10^{24}	3.257×10^{25}
97	p^2	$[15, 52, 55, -4, 14, 24]$	1.184×10^{16}	4.217×10^{16}
97	p^2	$[20, 39, 59, -4, 8, 38]$	5.265×10^{16}	1.257×10^{17}
97	p^2	$[23, 39, 51, -22, 6, 14]$	2.616×10^{16}	1.599×10^{17}
97	p	$[7, 56, 111, 4, 2, 56]$	1.549×10^{17}	2.616×10^{17}
97	p	$[19, 23, 104, -14, 12, 16]$	9.506×10^{17}	4.750×10^{18}
101	p^2	$[32, 39, 44, -12, 28, 20]$	8.477×10^{15}	3.603×10^{16}
101	p	$[12, 35, 104, 8, 12, 4]$	1.709×10^{17}	1.223×10^{18}
101	p	$[15, 28, 108, 8, 4, 28]$	1.572×10^{18}	3.193×10^{18}
101	p	$[15, 27, 111, -2, 14, 26]$	5.261×10^{17}	3.388×10^{18}
101	p	$[8, 51, 103, 4, 8, 2]$	2.948×10^{18}	7.940×10^{18}
101	p	$[7, 59, 116, -6, 4, 56]$	2.341×10^{18}	1.015×10^{19}
101	p	$[11, 39, 111, -10, 6, 34]$	4.559×10^{18}	2.415×10^{19}
101	p	$[3, 135, 135, -2, 2, 134]$	9.667×10^{19}	5.296×10^{20}
103	p^2	$[23, 36, 59, -4, 22, 16]$	1.076×10^{16}	1.620×10^{16}
103	p	$[16, 28, 103, 12, 0, 0]$	9.459×10^{15}	4.236×10^{16}
103	p^2	$[15, 55, 56, 2, 8, 28]$	4.016×10^{16}	5.313×10^{16}
103	p	$[19, 23, 111, -10, 14, 18]$	1.645×10^{17}	5.558×10^{17}
103	p	$[7, 59, 119, -2, 6, 58]$	1.765×10^{17}	1.861×10^{18}
103	p	$[8, 52, 103, 4, 0, 0]$	1.032×10^{18}	2.160×10^{18}
103	p	$[4, 103, 104, 0, 4, 0]$	2.647×10^{19}	8.748×10^{19}
107	p^2	$[35, 39, 44, -18, 32, 4]$	1.769×10^{16}	9.442×10^{16}
107	p^2	$[23, 40, 56, -16, 40, 20]$	1.352×10^{16}	2.102×10^{17}
107	p	$[16, 27, 111, -4, 16, 2]$	7.861×10^{16}	1.256×10^{18}
107	p	$[12, 36, 107, 4, 0, 0]$	1.061×10^{17}	1.694×10^{18}
107	p	$[19, 23, 116, -6, 16, 20]$	9.625×10^{17}	5.827×10^{18}
107	p	$[11, 39, 119, -2, 10, 38]$	1.105×10^{18}	1.732×10^{19}
107	p	$[4, 107, 108, 0, 4, 0]$	4.853×10^{19}	4.368×10^{20}
107	p	$[3, 143, 143, -2, 2, 142]$	1.102×10^{20}	1.761×10^{21}

Table 5: Good bounds D_Q for every $\theta_Q \in M^+_{3/2}(4p)$ with $89 \leq p \leq 107$.

p	*Quadratic Form*	N_0/N_1	$T = \{d < N$ *not represented.*$\}$ *or* $\#T$ *and largest* $d \in T$
11	$[4, 11, 12, 0, 4, 0]$	3×10^9	$3, 67, 235, 427$
11	$[3, 15, 15, -2, 2, 14]$	10^{10}	$4, 11, 88, 91, 163, 187, 232, 499, 595, 627, 715, 907, 1387, 1411, 3003, 3355, 4411, 5107, 6787, 10483, 11803$
17	$[7, 11, 20, -6, 4, 8]$	2×10^{10}	$3, 187, 643$
17	$[3, 23, 23, -2, 2, 22]$	$8 \times 10^{12}/$ 1.55×10^{14}	$\#T = 88,$ *largest* $= 89563$
19	$[7, 11, 23, -2, 6, 10]$	3×10^{10}	$4, 19, 163, 760, 1051$
19	$[4, 19, 20, 0, 4, 0]$	$5 \times 10^{11}/$ 6×10^{12}	$7, 11, 24, 43, 115, 123, 139, 228, 232, 267, 403, 424, 435, 499, 520, 568, 627, 643, 691, 883, 1099, 1411, 1659, 1672, 1867, 2139, 2251, 2356, 2851, 3427, 4123, 5131, 5419, 5707, 6619, 7723, 8968, 12331, 22843, 27955$
23	$[8, 12, 23, 4, 0, 0]$	3×10^9	$3, 4, 27, 115, 123, 163, 403, 427, 443, 667, 1467, 2787, 3523$
23	$[4, 23, 24, 0, 4, 0]$	3×10^9	$\#T = 78,$ *largest* $= 72427$
23	$[3, 31, 31, -2, 2, 30]$	3×10^9	$\#T = 196,$ *largest* $= 286603$
29	$[11, 12, 32, 8, 4, 12]$	3×10^{11} / 5×10^{11}	$\#T = 24,$ *largest* $= 22243$
29	$[8, 15, 31, 4, 8, 2]$	2×10^9	$\#T = 23,$ *largest* $= 7987$
29	$[3, 39, 39, -2, 2, 38]$	10^9	$\#T = 382,$ *largest* $= 1107307$
31	$[8, 16, 31, 4, 0, 0]$	10^9	$\#T = 36,$ *largest* $= 17515$
31	$[7, 19, 36, -6, 4, 16]$	10^{10}	$\#T = 29,$ *largest* $= 15283$
31	$[4, 31, 32, 0, 4, 0]$	10^{11}	$\#T = 166,$ *largest* $= 174003$
37	$[15, 20, 23, -4, 14, 8]$	10^9	$8, 19, 43, 163, 427, 723, 2923, 3907$
37	$[8, 19, 39, 4, 8, 2]$	2.0×10^{13}	$\#T = 55,$ *largest* $= 24952$
41	$[12, 15, 44, 8, 12, 4]$	10^{10}	$\#T = 60,$ *largest* $= 82123$
41	$[11, 15, 47, -2, 10, 14]$	10^{10}	$\#T = 65,$ *largest* $= 48547$
41	$[7, 24, 47, 4, 2, 24]$	3×10^9	$\#T = 82,$ *largest* $= 83107$
41	$[3, 55, 55, -2, 2, 54]$	10^{10}	$\#T = 896,$ *largest* $= 5017867$

Table 6: The set $d < N_1$ *not represented by* Q *for every* $\theta_Q \in M^+_{3/2}(4p)$ *with* $p \leq 41$*.*

p	*Quadratic Form*	N_0/N_1	$T = \{d < N$ *not represented.*$\}$ *or* $\#T$ *and largest* $d \in T$
43	$[15, 23, 24, 2, 8, 12]$	3.6×10^{10}	$4, 11, 16, 52, 67, 187, 379, 403, 568, 883, 1012, 2347, 2451$
43	$[11, 16, 47, 4, 2, 16]$	1.3×10^{13}	$\#T = 81,$ *largest* $= 73315$
43	$[4, 43, 44, 0, 4, 0]$	10^9	$\#T = 439,$ *largest* $= 1079467$
47	$[12, 16, 47, 4, 0, 0]$	10^9	$\#T = 106,$ *largest* $= 272083$
47	$[8, 24, 47, 4, 0, 0]$	10^9	$\#T = 108,$ *largest* $= 85963$
47	$[7, 27, 55, -2, 6, 26]$	10^9	$\#T = 112,$ *largest* $= 78772$
47	$[4, 47, 48, 0, 4, 0]$	2×10^9	$\#T = 556,$ *largest* $= 5345827$
47	$[3, 63, 63, -2, 2, 62]$	10^9	$\#T = 1165,$ *largest* $= 4812283$
53	$[20, 23, 32, -12, 4, 20]$	10^9	$\#T = 30,$ *largest* $= 33147$
53	$[12, 19, 56, 8, 12, 4]$	10^9	$\#T = 138,$ *largest* $= 178027$
53	$[8, 27, 55, 4, 8, 2]$	10^9	$\#T = 152,$ *largest* $= 137323$
53	$[3, 71, 71, -2, 2, 70]$	10^9	$\#T = 1604,$ *largest* $= 6474427$
59	$[15, 16, 63, 4, 2, 16]$	2×10^9	$\#T = 158,$ *largest* $= 304027$
59	$[15, 19, 64, -14, 8, 12]$	2×10^9	$\#T = 174,$ *largest* $= 318091$
59	$[7, 35, 68, -6, 4, 32]$	2×10^9	$\#T = 228,$ *largest* $= 132883$
59	$[12, 20, 59, 4, 0, 0]$	2×10^9	$\#T = 193,$ *largest* $= 316747$
59	$[4, 59, 60, 0, 4, 0]$	2×10^9	$\#T = 920,$ *largest* $= 3136219$
59	$[3, 79, 79, -2, 2, 78]$	2×10^9	$\#T = 2072,$ *largest* $= 8447443$
61	$[23, 24, 32, 16, 4, 12]$	1.5×10^8	$\#T = 43,$ *largest* $= 11923$
61	$[7, 35, 71, -2, 6, 34]$	2×10^9	$\#T = 271,$ *largest* $= 1096867$
61	$[8, 31, 63, 4, 8, 2]$	2×10^9	$\#T = 233,$ *largest* $= 363987$
61	$[11, 23, 68, -6, 8, 20]$	2×10^9	$\#T = 201,$ *largest* $= 190747$
67	$[15, 36, 39, -4, 14, 16]$	10^9	$\#T = 57,$ *largest* $= 20707$
67	$[23, 24, 35, 8, 2, 12]$	10^9	$\#T = 59,$ *largest* $= 126043$
67	$[16, 19, 71, 12, 16, 6]$	2×10^9	$\#T = 264,$ *largest* $= 421579$
67	$[4, 67, 68, 0, 4, 0]$	10^9	$\#T = 1271,$ *largest* $= 3846403$
71	$[15, 20, 76, 8, 4, 20]$	2×10^9	$\#T = 275,$ *largest* $= 321883$
71	$[15, 19, 79, -2, 14, 18]$	2×10^9	$\#T = 273,$ *largest* $= 267883$
71	$[16, 20, 71, 12, 0, 0]$	2×10^9	$\#T = 310,$ *largest* $= 1540771$
71	$[12, 24, 71, 4, 0, 0]$	2×10^9	$\#T = 307,$ *largest* $= 635947$
71	$[8, 36, 71, 4, 0, 0]$	2×10^9	$\#T = 346,$ *largest* $= 1053427$
71	$[4, 71, 72, 0, 4, 0]$	2×10^9	$\#T = 1450,$ *largest* $= 6463627$
71	$[3, 95, 95, -2, 2, 94]$	2×10^9	$\#T = 3170,$ *largest* $= 15135283$

Table 7: The set $d < N_1$ *not represented by* Q *for every* $\theta_Q \in M^+_{3/2}(4p)$ *with* $43 \leq p \leq 71$.

p	*Quadratic Form*	N_0/N_1	$T = \{d < N$ *not represented.*$\}$ *or* $\#T$ *and largest* $d \in T$
73	$[15, 39, 40, 2, 8, 20]$	10^9	$\#T = 81,$ *largest* $= 53188$
73	$[20, 31, 44, -12, 4, 28]$	10^9	$\#T = 72,$ *largest* $= 111763$
73	$[7, 43, 84, -6, 4, 40]$	2×10^9	$\#T = 420,$ *largest* $= 364708$
73	$[11, 28, 80, 8, 4, 28]$	2×10^9	$\#T = 336,$ *largest* $= 723795$
79	$[23, 31, 44, 18, 16, 20]$	10^9	$\#T = 88,$ *largest* $= 50955$
79	$[16, 20, 79, 4, 0, 0]$	2×10^9	$\#T = 383,$ *largest* $= 1419867$
79	$[19, 20, 84, 16, 8, 20]$	2×10^9	$\#T = 391,$ *largest* $= 1210675$
79	$[11, 31, 87, -10, 6, 26]$	2×10^9	$\#T = 409,$ *largest* $= 12778803$
79	$[8, 40, 79, 4, 0, 0]$	2×10^9	$\#T = 495,$ *largest* $= 1116507$
79	$[4, 79, 80, 0, 4, 0]$	2×10^9	$\#T = 1886,$ *largest* $= 25575460$
83	$[23, 31, 44, -14, 8, 12]$	10^9	$\#T = 97,$ *largest* $= 36763$
83	$[12, 28, 83, 4, 0, 0]$	2×10^9	$\#T = 432,$ *largest* $= 635347$
83	$[7, 48, 95, 4, 2, 48]$	2×10^9	$\#T = 529,$ *largest* $= 1358107$
83	$[16, 23, 87, 12, 16, 6]$	2×10^9	$\#T = 416,$ *largest* $= 1202587$
83	$[11, 31, 92, -6, 8, 28]$	2×10^9	$\#T = 469,$ *largest* $= 1381867$
83	$[3, 111, 111, -2, 2, 110]$	2×10^9	$\#T = 4639,$ *largest* $= 62337067$
83	$[4, 83, 84, 0, 4, 0]$	2×10^9	$\#T = 2134,$ *largest* $= 9405643$
89	$[23, 31, 48, 2, 12, 16]$	10^9	$\#T = 118,$ *largest* $= 137707$
89	$[15, 24, 95, 4, 2, 24]$	5×10^8	$\#T = 502,$ *largest* $= 682147$
89	$[15, 27, 96, -14, 8, 20]$	5×10^8	$\#T = 464,$ *largest* $= 1534723$
89	$[19, 23, 95, -18, 10, 14]$	5×10^8	$\#T = 540,$ *largest* $= 981403$
89	$[7, 51, 103, -2, 6, 50]$	5×10^8	$\#T = 646,$ *largest* $= 1427827$
89	$[3, 119, 119, -2, 2, 118]$	2×10^9	$\#T = 5357,$ *largest* $= 28654707$
89	$[12, 31, 92, 8, 12, 4]$	5×10^8	$\#T = 478,$ *largest* $= 653227$

Table 8: The set $d < N_1$ *not represented by* Q *for every* $\theta_Q \in M^+_{3/2}(4p)$ *with* $73 \leq p \leq 89$.

Appendix A

Notation and Symbols

Bibliography

[1] M. Bhargava, *On the conway-schneeberger fifteen theorem*, in Quadratic Forms and their applications, A. R. E. Bayer-Fluckiger, D. Lewis, ed., Providence, RI, 2000, Amer. Math. Soc., pp. 27–37.

[2] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-theorem.* preprint.

[3] W. Bosma, J. Cannon, and C. Playoust, *The magma algebra system i. the user language.*, J. Symbolic Comput., 24 (1997), pp. 235–265.

[4] D. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.

[5] J. Cremona, *Algorithms for Modular elliptic curves*, Cambridge Univ. Press, Cambridge, UK, 1997.

[6] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 1980.

[7] P. Deligne, *La conecture de weil i*, Inst. Hautes Études Sci. Publ. Math., 43 (1974), pp. 273–307.

[8] M. Deuring, *Die typen der multiplikatoreninge elliptischer funktion korper*, Abh. Math. Sem., 14 (1941), pp. 197–272.

[9] B. Duke, *Hyperbolic distribution problems and half-integral weight maas forms*, Invent. Math., 92 (1988), pp. 73–90.

[10] ——, *On ternary quadratic forms*, J. Num. Theory, 110 (2005), pp. 37–43.

[11] B. Duke and R. Schultz-Pillot, *Representations of integers by postive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math, 99 (1990), pp. 49–57.

[12] N. Elkies, K. Ono, and T. Yang, *Reduction of cm elliptic curves and modular function congruences*, Int. Math. Res. Not., 44 (2005), pp. 2695–2707.

[13] E. Golubeva, *Exceptional integers for binary quadratic forms*, J. Math. Sci., 105 (2001), pp. 2148–2155.

[14] B. Gross, *Heights and special values of l-series*, in Canadian Mathematical Society Conference Proceedings, J. L. H. Kisilevsky, ed., vol. 7, Amer. Math. Soc., 1987, pp. 115–189.

[15] G. Hardy and E. Wright, *Introduction to the Theory of Numbers*, The Clarendon Press, Oxford Univ. Press, Oxford, England, 1979.

[16] T. Ibukiyama, *On maximal order of division quaternion algebras over the rational number field with certain optimal embeddings*, Nagoya Math. J., 88 (1982), pp. 181–195.

[17] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1990.

[18] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math., 87 (1987), pp. 385–401.

[19] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, vol. 53, Amer. Math. Soc., Providence, RI, 2004.

[20] B. Kane, *Cm liftings of supersingular elliptic curves.* preprint.

[21] ——, *Representations of integers by ternary quadratic forms.* preprint.

[22] D. Kohel, *Endomorphism rings of elliptic curves of finite fields.* Ph.D. Thesis.

[23] W. Kohnen, *Newforms of half integral weight*, J. reine agew., 333 (1982), pp. 32–72.

[24] ——, *Fourier coefficients of modular forms of half integer weight*, Math. Ann., 271 (1985), pp. 237–268.

[25] T. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Inc., Reading, MA, 1973.

[26] J. Littlewood, *On the class number of the corpus* $p(\sqrt{-k})$, Proc. London Math. Soc., 27 (1928), pp. 399–417.

[27] M. Newman, *Integral Matrices*, Academic Press, New York, 1970.

[28] K. Ono, *Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, Amer. Math. Soc., Providence, RI, 2003.

[29] K. Ono and K. Soundararajan, *Ramanujan's ternary quadratic form*, Invent. Math, 130 (1997), pp. 415–454.

[30] A. Pizer, *An algorithm for computing modular forms on* $\gamma_0(n)$, J. Algebra, 64 (1980), pp. 340–390.

[31] J. Rosser and L. Schoenfeld, *Sharper bounds for the chebyshev functions* $\theta(x)$ *and* $\psi(x)$, Math. Comp., 29 (1975), pp. 243–269.

[32] G. Shimura, *On modular forms of half integer weight*, Ann. of Math., 97 (1973), pp. 440–481.

[33] C. Siegel, *Uber die klassenzahl quadratischer zahlkorper*, Acta. Arith., 1 (1936), pp. 83–86.

[34] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag, New York, 1986.

[35] B. Spearman and K. Williams, *Representing primes by binary quadratic forms*, Amer. Math. Monthly, 99 (1992), pp. 423–426.

[36] J. Sturm, *On the congruence of modular forms*, in Number Theory, New York, 1987, Springer, pp. 275–280.

[37] W. Tartakowsky, *Die gesamtheit der zahlen, die durch eine quadratische form* $f(x_1, x_2, \dots x_s)$, $(s \geq 4)$ *darstellbar sind.*, Izv. Akad. Nauk SSSR, 7 (1929), pp. 111–122, 165–196.

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