JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Ben KANE

CM liftings of supersingular elliptic curves

Tome 21, n° 3 (2009), p. 635-663.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_635_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 635-663

CM liftings of supersingular elliptic curves

par Ben KANE

Résumé. Sous GRH, nous présentons un algorithme qui, étant donné un nombre premier p, calcule l'ensemble des discriminants fondamentaux $D < 0$, tels que l'application de réduction, modulo un premier aux dessus de p, des courbes elliptiques avec multiplication complexe par $\mathcal{O}_D$ vers les courbes elliptiques supersingulières en caractéristique p est surjective. Dans l'algorithme, nous déterminons d'abord une borne D_p explicite telle que $|D| > D_p$ implique que l'application est nécessairement surjective et nous calculons ensuite explicitement les cas $|D| < D_p$.

Abstract. Assuming GRH, we present an algorithm which inputs a prime p and outputs the set of fundamental discriminants $D < 0$ such that the reduction map modulo a prime above p from elliptic curves with CM by $\mathcal{O}_D$ to supersingular elliptic curves in characteristic p is surjective. In the algorithm we first determine an explicit constant D_p so that $|D| > D_p$ implies that the map is necessarily surjective and then we compute explicitly the cases $|D| < D_p$.

1. Introduction

For $D < 0$ a fundamental discriminant, consider the imaginary quadratic field $K := \mathbb{Q}(\sqrt{D})$ with ring of integers $\mathcal{O}_D$ and Hilbert class field H_K. From the work of Deuring [3], given a prime p which does not split in $\mathcal{O}_D$ and an elliptic curve E/H_K with CM by $\mathcal{O}_D$ the reduction to characteristic p gives a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Elkies, Ono and Yang [8] have deduced that the reduction map is surjective for $|D|$ sufficiently large by using an equidistribution result of Duke and Schulze-Pillot [5], based upon bounds for coefficients of half-integral weight cusp forms by Iwaniec [14] and Duke [4], combined with an (ineffective) lower bound for the class number $h(D)$ of $\mathcal{O}_D$ due to Siegel [27]. Denote the (finite) set of such D for which the reduction map is not surjective by $\mathcal{E}_p$ and define

Manuscrit reçu le 17 septembre 2007.
This research was conducted while the author was a student at the University of Wisconsin-Madison.
Mots clefs. Quaternion Algebra, Elliptic Curves, Maximal Orders, Half Integer Weight Modular Forms, Kohnen's Plus Space, Shimura Lifts.
Classification math.. 11G05, 11E20, 11E45, 11Y35, 11Y70.

$\mathcal{E}'_p := \{|D| : D \in \mathcal{E}_p\}$. We say that $D_p \in \mathbb{N}$ is a *good bound for* p if $\max \mathcal{E}'_p < D_p$ (suppressing p when the context is clear).

Although $\mathcal{E}_p$ is finite, no explicit good bound is given above due to the ineffective nature of Siegel's lower bound. In this paper we present an algorithm which takes as an input a prime p and return the set $\mathcal{E}_p$. The algorithm terminates unconditionally, but the correctness is conditional upon the Generalized Riemann Hypothesis for Dirichlet L-functions and also the Generalized Riemann Hypothesis for the L-series of weight 2 primitive newforms (henceforth simply denoted GRH). The assumption of GRH allows us to use techniques developed by Ono and Soundarajan [23] to explicitly compute a good bound for p.

Theorem 1.1. *Let a prime p be given. Conditional upon GRH, there is an effectively computable good bound for p.*

Explicitly computing the bound given by Theorem 1.1 for $p \leq 113$ we obtain the following.

Theorem 1.2. *Conditional upon GRH, 1.041×10^{23} is a good bound for $p \leq 113$.*

Good bounds are obtained individually for each prime $p \leq 113$ but we simply take the maximum value in the above theorem for brevity. For better bounds for each specific $p \leq 113$, the reader is referred to Table 11 in Appendix A.

After obtaining the good bound D_p from Theorem 1.1, it only remains to explicitly compute the set of $|D| \leq D_p$ for which the mapping is not surjective. For each supersingular elliptic curve $E/\mathbb{F}_{p^2}$ we construct a positive definite (ternary) quadratic form Q_E such that Q_E represents $|D|$ if and only if there exists E' with CM by $\mathcal{O}_D$ which reduces to E. Since there are only finitely many supersingular elliptic curves we then merely need to check which $|D| \leq D_p$ are represented by each Q_E.

One may then use the algorithm by Fincke and Pohst [9] to determine a vector of length $|D|$. The implementations which the author is aware of return all vectors of length $|D|$, of which there are asymptotically $\Omega_p(h(D)) \gg D^{\frac{1}{2}-\epsilon}$ elements. Hence running this algorithm for each $|D| \leq D_p$ to determine $\mathcal{E}_p$ is $\Omega_p\left(D_p^{3/2-\epsilon}\right)$ and the calculation quickly becomes infeasible for moderately large D_p. We hence want to take advantage of the fact that we do not need all representations of $|D|$ but rather only one. In the case where E is defined over $\mathbb{F}_p$ we are able to use a classification result of Ibukiyama [13] to develop a specialized algorithm which determines more efficiently the set of $|D| < D_p$ which are represented (see Section 5). This algorithm has allowed us to compute the full set $\mathcal{E}_p$ for $p = 11, 17$, and 19.

Theorem 1.3. *Assuming GRH, the following hold.*

(1) *The set* $\mathcal{E}_{11}$ *is given by*

$$\mathcal{E}'_{11} = \{3, 4, 11, 67, 88, 91, 163, 187, 232, 235, 427499, 595, 627, 715, 907, 1387, 1411, 3003, 3355, 4411, 5107, 6787, 10483, 11803\}.$$

(2) *The set* $\mathcal{E}_{17}$ *satisfies* $\#\mathcal{E}_{17} = 91$ *and* $\max\ \mathcal{E}'_{17} = 89563$.

(3) *The set* $\mathcal{E}_{19}$ *satisfies* $\#\mathcal{E}_{19} = 45$ *and* $\max\ \mathcal{E}'_{19} = 27955$.

Having established such surjectivity results, one may ask whether similar results can be shown about the multiplicity of the reduction map. This question was addressed and an unconditional but ineffective solution was given by Elkies, Ono, and Yang [8].

Define the Hilbert class polynomial $\mathcal{H}_D(x) \in \mathbb{Z}[x]$ as the unique monic polynomial 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. The degree of the Hilbert class polynomial is $h(D)$. Define further $S_p(x) \in \mathbb{F}_p[x]$ to be the polynomial with roots precisely the j-invariants of the supersingular elliptic curves of characteristic p.

Theorem (Elkies-Ono-Yang [8])**.** For a prime p and $t \in \mathbb{N}$, every sufficiently large fundamental discriminant $D < 0$ for which p does not split in $\mathcal{O}_D$ satisfies

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

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

Here the implied constant depends on p and t. Their result states that for sufficiently large D there are at least t nonisomorphic elliptic curves with CM by $\mathcal{O}_D$ which reduce to each supersingular elliptic curve of characteristic p. We are again able to obtain an effective but conditional result of this nature. For a supersingular elliptic curve E, define w_E to be the number of automorphisms of E and take the canonical measure

$$\mu(E) := \frac{1/w_E}{\sum_{E'} 1/w_{E'}},$$

where the sum is taken over all supersingular elliptic curves of characteristic p. We denote the minimal value of this measure by μ_p.

Theorem 1.4. *Assume GRH. For a prime* p *and* $0 < c < 1$ *there is a effectively computable constant* $D_{p,c} \in \mathbb{N}$ *such that every fundamental discriminant* $D < 0$ *with* $|D| \geq D_{p,c}$ *for which* p *is not split satisfies*

$$S_p(x)^{c\mu_p h(D)} \mid \mathcal{H}_D(x)$$

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

In Section 3 we see that Theorem 1.4 reduces to the same argument given to show Theorem 1.1. Since $h(D) \to \infty$ effectively as $D \to -\infty$ (Oesterlé [20] unconditionally showed the growth is $\Omega(\log(|D|)^{1-\epsilon})$, but Siegel [27] obtained $\Omega(|D|^{1/2-\epsilon})$ conditional on GRH), we also get an effective but conditional version of Elkies, Ono, and Yang's result by choosing for each $t \in \mathbb{N}$ an integer $D_{p,t} \geq D_{p,c}$ large enough so that $c\mu_p h(D) > t$ for every $|D| \geq D_{p,t}$.

Elkies, Ono and Yang are particularly interested in the case $t = 2$ because they obtain a congruence for the Hilbert class polynomial whenever $S_p(x)^2 \mid \mathcal{H}_D(x)$. We briefly expound upon this connection. For a function f with Fourier expansion $f(z) = \sum_{n\in\mathbb{Z}} a(n)q^n$, the action of the operator $U(p)$ is given by $f|U(p)(z) = \sum_{n\in\mathbb{Z}} a(pn)q^n$. Elkies, Ono and Yang [8, Theorem 2.3 (1)] showed that if $S_p(x)^2 \mid f$ then there exist a polynomial $P_{f,p}(x) \in \mathbb{Z}[x]$ such that

$$f(j(z))|U(p) \equiv P_{f,p}(j(z)) \mod p.$$

They hence ineffectively show that such a congruence always exists for $f = \mathcal{H}_D$ whenever D is sufficiently large.

Our results will hence give as an immediate corollary an effective but conditional bound beyond which this existence must occur. Effectively computing the bound for $t = 2$ and noting that Watkins [33] has shown explicitly that $h(D) > 100$ for every $|D| > 2383747$, we can choose $c = 1/20$ for $p = 11$ and $c = 3/50$ for $p = 19$ to effectively show that $S_p(x)^2 \mid \mathcal{H}_D(x)$ for $|D| > 1.370 \times 10^{10}$ and $|D| > 2.675 \times 10^{13}$, respectively. Combining the explicit bound given above with Theorem 2.3 (1) of Elkies, Ono, and Yang [8] we obtain the following corollary after a calculation to determine the explicit exceptions for $p = 19$.

Corollary 1.5. *Assume GRH. If $D < 0$ is a fundamental discriminant satisfying $\left(\frac{D}{19}\right) \neq 1$ and $|D| > 184699$ then there exists a polynomial $P_{D,p}(x) \in \mathbb{Z}[x]$ such that*

$$\mathcal{H}_D(j(z))|U(19) \equiv P_{D,p}(j(z)) \mod 19.$$

The paper begins by reviewing the connection between theta series and $\mathcal{E}_p$ in Section 2. In Section 3, we review how the bound for coefficients of theta series is obtained. Given the connection from Section 2, this gives a good bound for p, dependent on numerically calculating certain constants. In Section 4, we fix a basis and decompose a certain space of modular forms in order to calculate some of the constants obtained from Section 3. Furthermore, we give explicit algorithms for calculating the remaining constants. In Section 5, we use a trick based on the Ibukiyama's classification [13] of the set of supersingular elliptic curves defined over $\mathbb{F}_p$, in order to calculate the set of $|D| < D_p$ which are generated by Q_E. Finally,

in Appendix A we give the data obtained by explicitly implementing the algorithms from Sections 4 and 5 for $p \leq 113$.

Acknowledgements. The author would like to thank T.H. Yang for his help and guidance and would also like to thank K. Bringmann, K. Ono, J. Rouse, and M. Müger for useful comments. Finally, the author would like to thank the anonymous referee for an extremely detailed report which aided the exposition greatly.

2. CM liftings of supersingular elliptic curves and theta series

For a supersingular elliptic curve E we say that D_E is a *good bound* for E if E is in the image of the reduction map for every $|D| > D_E$. Hence we determine a good bound D_p for p piecewise by determining a good bound D_E for each supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and then taking $D_p := \max_E D_E$, relying on the fact that there are only finitely many supersingular elliptic curves (up to isomorphism). This also aids in computing the elements $D \in \mathcal{E}_p$ with $|D| < D_p$, since we only need to check all $|D| < D_E$ for each curve, and not up to the larger bound D_p. The theory involved in determining D_E goes through quaternion algebras, quadratic forms, theta series, and modular forms. For background information on elliptic curves a good reference is Silverman's book [28]. A good reference for quaternion algebras is Vigernas's book [32], while Ono's book [22] contains a good introduction to modular forms. Good sources of information about quadratic forms can be found in Jones' book [15] and O'Meara's book [21].

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. An elliptic curve $\widetilde{E}/H_K$ with CM by $\mathcal{O}_D$ is a *CM (by $\mathcal{O}_D$) lift* of E if the reduction of $\widetilde{E}$ modulo the unique prime above p is isomorphic to E. We now review the connection between CM liftings and theta series. Let $R_E := \mathrm{End}(E)$ be a maximal order of the quaternion algebra $B_p/\mathbb{Q}$ ramified precisely at p and infinity. For p inert in $\mathcal{O}_D$ (resp. p ramified in $\mathcal{O}_D$) there is a one-to-one (resp. two-to-one) correspondence between (non-isomorphic) lifts of E and embeddings of $\mathcal{O}_D$ in R_E. Gross and Zagier [12, Prop. 2.7] cover the case of p inert and Elkies [7, p. 168] extends this to the case where p is ramified. Let $L_E := \{x \in \mathbb{Z} + 2R_E | tr(x) = 0\}$ be the *Gross lattice* with the associated positive definite ternary quadratic form Q_E given by the reduced norm on L_E.

Define the *theta series* for Q_E by

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

where z is in the upper half plane and $q := e^{2\pi i z}$. Noting that $w_E = \#R_E^*$, Gross [11, Prop. 12.9, p. 172] has shown that $a_E(D)$ equals $\frac{w_E}{\#\mathcal{O}_D^*}$ times the number of embeddings of $\mathcal{O}_D$ into R_E. It is hence sufficient to proceed

by bounding the coefficients of the theta series from below, and showing that they must be positive whenever $|D| > D_E$. However, Gross showed that θ_E is a weight $3/2$ modular form in Kohnen's plus space (see the work of Kohnen [18] or Ono's book [22, p. 54] for a definition) of level $4p$ and explicit bounds (conditional on GRH) for coefficients of theta series in this space were established by the author [16]. The methods used to obtain these bounds are reviewed in Section 3.

3. Background

This section is a brief summary of the theory used to bound the coefficients of θ_E. The theta series is first decomposed into a linear combination of an Eisenstein series and a basis of weight $3/2$ Hecke eigenforms. Using an isomorphism to weight 2 cusp forms, the coefficients of the Hecke eigenforms are then compared with the central values of quadratic twists of L-series of weight 2 newforms. The central value of these L-series are bounded in the authors's generalization [16] of Ono and Soundararajan's paper [23] in terms of constants which we introduce here. Section 4 is devoted to explicitly determining the basis of weight $3/2$ Hecke eigenforms, the isomorphism to weight 2 newforms, and explicitly bounding these constants.

For $k \in \mathbb{Z}$ and $N \in \mathbb{N}$ we denote the space of (holomorphic) modular forms of weight k and level N by $M_k(N)$, the cuspidal subspace by $S_k(N)$, and the space of newforms by $S_k^{\text{new}}(N)$. Moreover, for $k \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ we denote Kohnen's plus space of level $4N$ by $M_k^+(4N)$ and the cuspidal subspace by $S_k^+(4N)$. For a modular form g, we denote the n-th Fourier coefficient by $a_g(n)$.

For p^e the highest power of p dividing the square part of $|d|$, we denote $d_p := \frac{d}{p^{2e}}$. Define the Eisenstein series

$$H_\theta(z) := \frac{12}{p-1} + \sum_{d<0,\ d\equiv 0,1 \pmod 4} \frac{12}{p-1} \cdot \frac{1 - \left(\frac{|d_p|}{p}\right)}{2} H(d_p) q^{|d|},$$

where $H(d)$ is the Hurwitz class number. In particular, for $D < 0$ a fundamental discriminant, $H(D)$ equals the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ divided by the number of units modulo ± 1. Gross [11] has shown that $\theta_E - H_\theta \in S_{3/2}^+(4p)$.

Let $g_1, \dots, g_r$ be a basis of Hecke eigenforms (a choice is explicitly made in Section 4) for $S_{3/2}^+(4p)$. We then decompose our theta series as

$$\theta = H_\theta + \sum_{i=1}^{t_p - 1} b_i g_i,$$

for some $b_i \in \mathbb{C}$. Here t_p is the number of distinct conjugacy classes of maximal orders of B_p, called the *type number*.

For a fundamental discriminant $D < 0$ with corresponding Kronecker character χ_D, define the $|D|$-th Shimura correspondence $S_{|D|}$ by

$$\sum_{n=1}^{\infty} \frac{a_{g|S_{|D|}}(n)}{n^s} := L(\chi_D, s) \sum_{n=1}^{\infty} \frac{a_g(|D|n^2)}{n^s}$$

for every $g \in S_{3/2}^+(4p)$. Here and throughout we denote the image of g under an operator T by $g|T$. Shimura [26] showed that $g|S_{|D|} \in S_2(4p)$ and that $S_{|D|}$ commutes with every Hecke operator, namely

$$f|_{3/2}T_{\ell^2}|S_{|D|} = (f|S_t)|_2 T_\ell$$

for every $f \in S_{3/2}^+(4p)$ and every prime $\ell \neq p$. Let $t_i \in \mathbb{Z}_{>0}$ be minimal with $4 \mid t_i$ and $-t_i$ a fundamental discriminant satisfying $a_{g_i}(t_i) \neq 0$. If r_j are chosen so that $\sum_{j=1}^{t_p-1} r_j a_{g_i}(t_j) \neq 0$ for every $1 \leq i \leq t_p - 1$, then Kohnen [18] has shown that the linear combination of Shimura correspondences

$$S := \sum_{i=1}^{t_p-1} r_i S_{t_i}, \tag{3.1}$$

called a *Shimura lift*, forms an isomorphism from $S_{3/2}^+(4p)$ to $S_2^{\text{new}}(p) = S_2(p)$ which sends Hecke eigenforms to Hecke eigenforms.

Denote the Shimura lift of g_i by $G_i := g_i|S$. For a fundamental discriminant $D < 0$ and $\text{Re}(s) > 1$, we denote the L-series of $\chi := \chi_D$ by

$$L(s) := L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

and for $\text{Re}(s) > \frac{3}{2}$ we denote the L-series of G_i twisted by χ as

$$L_i(s) := L(G_i, D, s) := \sum_{n=1}^{\infty} \frac{\chi(n) a_{G_i}(n)}{n^s}. \tag{3.2}$$

The conductor of $L_i(s)$ is $q := p|D|^2$. Denote by m_i the smallest integer such that $a_{g_i}(m_i) \neq 0$ with $(p, m_i) = 1$.

Using the fact that G_i is a Hecke eigenform, the author [16] showed that any fundamental discriminant $D < 0$ satisfying $a_\theta(|D|) = 0$ must also satisfy

$$\frac{12}{(p-1)\pi 2^{\frac{v_p(|D|)}{2}}} \cdot |D|^{\frac{1}{4}} \leq \sqrt{\sum_{i=1}^{t_p-1} |b_i|^2} \sqrt{\sum_{i=1}^{t_p-1} c_i \frac{L_i(1)}{L(1)^2}}, \tag{3.3}$$

where

$$c_i := \frac{|a_{g_i}(m_i)|^2}{L(G_i, m_i, 1) m_i^{\frac{1}{2}}} \tag{3.4}$$

is a constant which comes from taking the ratio of the $|D|$-th coefficient and the m_i-th coefficient in the Kohnen-Zagier formula [19]. Define

$$F(s) := F_i(s) := \left(\frac{\sqrt{q}}{2\pi}\right)^{s-1} \frac{L_i(s)\Gamma(s)}{L(s)L(2-s)} \tag{3.5}$$

and choose $1 < \sigma < \frac{3}{2}$. To obtain a contradiction from equation (3.3) for $|D|$ sufficiently large, it remains to bound $F(1) = \frac{L_i(1)}{L(1)^2}$ from above.

Since equation (3.3) is obtained by assuming $a_\theta(|D|) \leq 0$ and rearranging, we can similarly assume $a_\theta(|D|) \leq c a_{H_\theta}(|D|)$ for a constant $0 < c < 1$ and obtain equation (3.3) with the left hand side multiplied by $1-c$. Hence Theorem 1.4 is also reduced to bounding $F(1)$ and the details are left to the reader.

We describe briefly how Ono and Soundararajan [23] bounded $F(1)$. By the functional equation of $F(s)$ and the Phragmén-Lindelöf principle we have

$$F(1) \leq \max_{t\in\mathbb{R}} F(\sigma + it),$$

so it suffices to bound $F(\sigma + it)$ from above for every $t \in \mathbb{R}$.

For a real number $\boldsymbol{X} > 0$ and an L-series $\widetilde{L}(s)$ with $c > 0$ real chosen such that $s+c$ is in the region of absolute convergence, consider the integral

$$\int_{c-i\infty}^{c+i\infty} \frac{\widetilde{L}'}{\widetilde{L}}(s+w)\Gamma(w)\boldsymbol{X}^w dw. \tag{3.6}$$

On the one hand, if $\widetilde{L}(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ in the region of convergence, then (3.6) can be computed as the sum

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)a(n)}{n^s} e^{-n/\boldsymbol{X}} \tag{3.7}$$

using the fact that

$$\int_{c-i\infty}^{c+i\infty} \Gamma(w)\left(\frac{\boldsymbol{X}}{n}\right)^w dw = \sum_{m=0}^{\infty} \frac{(-1)^m}{m!}\left(\frac{n}{\boldsymbol{X}}\right)^m = e^{-n/\boldsymbol{X}},$$

which follows by shifting the integral $\mathrm{Re}(w) \to -\infty$ and counting the residues at negative integers. On the other hand, we can shift the original integral to the left and count the contribution from residues at each of the poles. The contribution from $w = 0$ gives $\frac{\widetilde{L}'}{\widetilde{L}}(s)$. The assumption of GRH allows us to determine the real part of all of the poles coming from $\frac{\widetilde{L}'}{\widetilde{L}}$, since these correspond to zeros of $\widetilde{L}(s)$. Rearranging the resulting equation gives a formula for $\frac{\widetilde{L}'}{\widetilde{L}}(s)$ which we integrate to get a formula for $\log|\widetilde{L}(s)|$, as shown by Ono and Soundararajan [23, Lemmas 1-2].

Using the above argument with $\widetilde{L}(s) = L(s)$, we define for $\mathrm{Re}(s) > 1$ the integral of equation (3.7) by

$$\boldsymbol{G}(s, \boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s \log(n)} e^{-n/\boldsymbol{X}}. \tag{3.8}$$

Similarly, with λ_i defined so that $\frac{L_i'}{L_i}(s) = \sum\limits_{n=1}^{\infty} \frac{\lambda_i(n)\chi(n)}{n^s}$ when $\mathrm{Re}(s) > 3/2$, define

$$\boldsymbol{F}_1(s, \boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\lambda_i(n)\chi(n)}{n^s} e^{-n/\boldsymbol{X}} \tag{3.9}$$

and

$$\boldsymbol{F}(w, \boldsymbol{X}) := \sum_{n=1}^{\infty} \frac{\lambda_i(n)\chi(n)}{n^w \log(n)} e^{-n/\boldsymbol{X}} = \int \boldsymbol{F}_1(w, \boldsymbol{X}) dw.$$

For $s = \sigma + it$, $s_0 = 2 - \sigma + it$ and $s_2 = \sigma_2 + it$ for any choice $\sigma < \sigma_2 < 2$, the following bound [16] was obtained for $F(s)$. For certain explicit constants $c_{\theta,\sigma,\boldsymbol{X},1}$, $c_{\theta,\sigma,\boldsymbol{X},t,1}$, $c_{\theta,\sigma,\boldsymbol{X},m,1}$, $c_{\theta,\sigma,\boldsymbol{X},2}$, $c_{\theta,\sigma,\boldsymbol{X},t,2}$, and $c_{\theta,\sigma,\boldsymbol{X},q,2}$

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

where $\alpha(\boldsymbol{X})$, $\beta(\boldsymbol{X})$, $\gamma(\boldsymbol{X})$ and $\delta(\boldsymbol{X})$ are defined in the author's previous paper [16] in equations (7.2), (7.1), the line directly proceeding (7.1), and the first equation in Section 6, respectively. Moreover, in Section 8 of that paper, explicit bounds in terms of Γ-factors are given for $\alpha(\boldsymbol{X})$, $\beta(\boldsymbol{X})$, $\gamma(\boldsymbol{X})$, and $\delta(\boldsymbol{X})$.

The decay in $\Gamma(s)$ cancels polynomial growth in t from $c_{\theta,\sigma,\boldsymbol{X},t,i}$. Since $\sigma > 1$, $L(s)$ converges absolutely, so we can explicitly calculate a bound for $2\log|L(s)|$ as well. The other terms involving $\boldsymbol{F}$, $\boldsymbol{G}$, and $\boldsymbol{F}_1$ are also dealt with [16] (Here, we use cancellation in the sums for small n between terms from $2\log|L(s)|$, and then bound the remaining terms separately). We give further details in Section 4 of how to compute better bounds for these constants.

Therefore, the main goal of this paper is to decompose Kohnen's plus space, make a choice of g_i, determine a Shimura lift, and then calculate b_i and c_i. This is described in Section 4. Moreover, in feasible cases we must determine an algorithm to determine whether $|D|$ is represented by a fixed form Q. A specialized algorithm is given in Section 5 to determine this whenever the corresponding elliptic curve is defined over $\mathbb{F}_p$.

4. Algorithm to compute D_E and D_p

This section is broken into four main subsections. We first determine the set of theta series θ_E for every supersingular elliptic curve $E/\mathbb{F}_{p^2}$. We then determine a basis of Hecke eigenforms $\{g_i : i \in \{1, \dots, t_p - 1\}\}$ for the subspace of $S_{3/2}^+(4p)$ generated by these theta series and express the cuspidal part of the theta series as a linear combination of these eigenforms. The third step is to compute an explicit Shimura lift S from $S_{3/2}^+(4p)$ to $S_2(p)$ and finally we compute the constants corresponding to $G_i = g_i|S$.

4.1. Calculating the theta series. Let p be a prime and $C > 0$ be an integer. We describe here how to obtain the quadratic forms Q_E and the first C coefficients of θ_E for every supersingular elliptic curve $E/\mathbb{F}_{p^2}$. If C is chosen too small for the remaining calculations, then we simply double C and rerun the calculations.

We begin by calculating the maximal orders R_E using Kohel's implementation [17], based on an algorithm of Pizer [24], which is built into MAGMA. These are obtained by first using a function to calculate a single maximal order R, then calculating all left ideal classes I_i of R, and finally calculating the right order R_i of I_i, which gives a full set of maximal orders. It is then straightforward to compute L_E and the method of Fincke and Pohst [9] may be used to compute the coefficients $a_E(d)$ for every $d < C$.

4.2. Decomposition of θ_E. We now compute a basis of (cuspidal) Hecke eigenforms $g_1, \dots g_{t_p-1}$ of the space spanned by all of our theta series and then decompose the cuspidal part $g_E := \theta_E - H_\theta$ in terms of these Hecke eigenforms. This gives us the coefficients b_i from section 3.

A computational solution to the decomposition problem for integral weight forms follows from the work of Stein [29] on modular symbols. We recall that Kohnen [18] has shown that the Hecke algebra on $S_{3/2}^+(4p)$ is isomorphic to the Hecke algebra on $S_2^{\text{new}}(p) = S_2(p)$. Furthermore, Sturm has shown for $S_2(p)$ that a finite set of Hecke operators generates the Hecke algebra and has given an effectively computable bound N so that $\{T_n | n \leq N\}$ generates the Hecke algebra [31]. The Hecke eigenspaces of distinct normalized Hecke eigenforms on $S_2(p)$ are at most one dimensional (that is, $S_2(p)$ satisfies *(strong) multiplicity one*, cf. Ono's book [22, p. 29]). Therefore $S_{3/2}^+(4p)$ also satisfies multiplicity one.

We first note that the space generated by our theta series is invariant under the action of the Hecke algebra, so that the space is generated by the set of g_E (which have coefficients in $\mathbb{Q}$). Since $S_{3/2}^+(4p)$ has multiplicity one, we can diagonalize the Hecke operators $T := T_{n^2}$ simultaneously. We only need to diagonalize the operators for $n \leq N$, where N is the Sturm bound on $S_2(p)$ as above. Checking computationally, it appears as though

a single $g_E =: g$ always generates the entire space under the action of the Hecke algebra (we have checked for all $p < 1000$) and we demonstrate how to obtain a basis of Hecke Eigenforms in this case. This assumption is not really restrictive because one merely needs to follow the same argument for the forms $g_{E_1}, g_{E_2}, \ldots$ until the dimension equals $t_p - 1$. We may also choose a particular T such that $g|T^m$ generates the entire subspace (see Stein's book [30, p. 167]).

Given g and T as above we calculate $g|T^m$ for every $0 \le m < t_p$. Then using linear algebra over $\mathbb{Q}$ we obtain $g|T^{t_p-1}$ as a linear combination of $g|T^m$ with $0 \le m < t_p - 1$, giving a matrix M_T, with rational coefficients, which determines the action of T. Let F be the Galois splitting field over $\mathbb{Q}$ of the characteristic polynomial of M_T with absolute polynomial $P(x)$. We note that all elements of F may be represented as vectors over $\mathbb{Q}$ in terms of a generator of F, or, equivalently, as elements of $\mathbb{Q}[x]/(P)$, allowing for linear algebra over F. Since $g|T^m$ has coefficients in $\mathbb{Q}$ we can diagonalize M_T to obtain Hecke eigenforms with coefficients in F. Because $S^+_{3/2}(4p)$ has multiplicity one and T generates the Hecke algebra, the eigenspace of a given eigenvalue has dimension one. Hence we may calculate with linear algebra over F the unique eigenform g_i with eigenvalue λ_i.

We can now decompose each g_E as a linear combination of the g_i by linear algebra over F. This gives the desired coefficients $b_i \in F$ in the decomposition

$$g_E = \sum_{i=1}^{t_p-1} b_i g_i.$$

4.3. Finding a Shimura lift. Having established the Hecke eigenforms g_i, we now choose t_i and r_i as in equation (3.1) to establish a Shimura lift. We recursively choose t_ℓ and r_ℓ such that

$$S(\ell) := \sum_{j=1}^{\ell} r_j S_{t_j}$$

satisfies $g_i|S(\ell) = 0$ if and only if $a_{g_i}(t_j) = 0$ for every $1 \le j \le \ell$.

At each step we choose i smallest such that $g_i|S(\ell - 1) = 0$. We then choose t_ℓ to be the smallest positive integer with $4 \mid t_\ell$, $-t_\ell$ a fundamental discriminant, and $a_{g_i}(t_\ell) \neq 0$, noting existence has been shown by Kohnen [18]. It remains to choose r_ℓ such that for every k we have $\sum_{j=1}^{\ell} r_j a_{g_k}(t_j) = 0$ if and only if $a_{g_k}(t_j) = 0$ for $1 \le j \le \ell$. Since $F = \mathbb{Q}(\alpha)$ is a number field we may consider F as a vector space over $\mathbb{Q}$ with basis α^i.

Let k be given such that $a_{g_k}(t_j) \neq 0$ for some j. If $a_{g_k}(t_\ell) = 0$, then we know by inductive hypothesis that $g_k|S(\ell - 1) + r_\ell S_{t_\ell} \neq 0$ for any r_ℓ. If $a_{g_k}(t_\ell) \neq 0$, then writing it in terms of the basis, we have $a_{g_k}(t_\ell) =$

$\sum_m d_m \alpha^m$ with some $d_{m,k} \neq 0$. Computing

$$\sum_{j=1}^{\ell-1} r_j a_{g_k}(t_j)$$

and rewriting in terms of the basis, we write the coefficient $e_{m,k} \in \mathbb{Q}$ of α^m. We then take

$$r_{\ell,k} := \left| \frac{e_{m,k}}{d_{m,k}} \right| + \frac{1}{2}.$$

Taking $r_\ell := \max_k r_{\ell,k}$, we have

$$|r_\ell d_{m,k}| > |e_{m,k}|$$

and hence $r_\ell d_{m,k} + e_{m,k} \neq 0$. It follows that $g_k|S(\ell) \neq 0$ because the coefficient of α^m in the first Fourier coefficient is nonzero. Since k was arbitrary, we have $g_i|S(\ell) = 0$ if and only $a_{g_i}(t_j) = 0$ for every $1 \leq j \leq \ell$, as desired. We then terminate if $g_i|S(\ell) \neq 0$ for every i, terminating after at most $t_p - 1$ recursions, and otherwise continue the recursion.

4.3.1. ***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 $m_i \neq 0 \pmod p$ and $G_i = g_i|S$. We may simply choose m_i to be the smallest such integer. In the bounds that we obtain it suffices to bound $|c_i|$ from above.

We have already shown how to calculate $a_{g_i}(m_i)$, so it remains to calculate $L(G_i, m_i, 1)$. We use the following formula of Cremona [1],

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

Calculating the partial sum up to a fixed bound N and noting by Deligne's optimal bound [2] that $|a_L(n)| \leq \sigma_0(n) n^{\frac{1}{2}}$, we may bound the error easily by pulling the absolute value inside the sum for $n > N$.

4.4. Calculating the other constants. These constants are actually fairly easy to calculate once we show clearly where they come from, given the theoretical results stated in the author's previous paper [16]. The methods involved and notation used are similar to those used by Ono and Soundararajan [23].

Most of the constants obtained are explicit in terms of Γ and ζ factors along the real line, but we need to do some work to calculate the terms

involving $\boldsymbol{F}$, $\boldsymbol{F}_1$, and $\boldsymbol{G}$ (coming from equation (3.7)). 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 $\sigma = \mathrm{Re}(s)$, $\sigma_0 = \mathrm{Re}(2-s)$, and $\sigma_2 = \mathrm{Re}(s_2)$, so that

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

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

$$-2\log|L(s)| + 2\sum_{n=2}^{N_0}\mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s\log(n)}\right). \tag{4.1}$$

Noting that s is in the region of absolute convergence,

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

Then equation (4.1) becomes

$$-2\log(|L(s)|) + 2\sum_{n=2}^{N_0}\mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s\log(n)}\right) = -2\sum_{n=N_0+1}^{\infty}\mathrm{Re}\left(\frac{\chi(n)\Lambda(n)}{n^s\log(n)}\right).$$

Therefore, taking the absolute value inside the sum gives

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

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

We also need a bound for the constants depending on t, the imaginary part of s. We use the functional equation of the Γ factor to remove the growth from these terms. Since the growth is logarithmic in t we easily obtain

$$\log|\Gamma(s)| + c_{\theta,\boldsymbol{X},1,t} - c_{\theta,\boldsymbol{X},2,t} \le \log|\Gamma(\sigma+r)| \tag{4.2}$$

for some $r \in \mathbb{N}$.

A computer is then used to bound

$$\sum_{n=2}^{N_0}\mathrm{Re}\left(\frac{\chi(n)}{n^{it}\log(n)}\left(v(n,\boldsymbol{X}) - \frac{2\Lambda(n)}{n^{\sigma}}\right)\right). \tag{4.3}$$

Notice that the term we are subtracting is exactly the term being added in equation (4.1). 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 the terms coming from equation (3.7) with n large. We hence look at

$$\sum_{n=N_0+1}^{\infty}\operatorname{Re}\left(\frac{\chi(n)}{n^{it}\log(n)}(v(n,\boldsymbol{X}))\right). \tag{4.4}$$

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

$$\begin{aligned}\boldsymbol{H}(\alpha,\boldsymbol{X}) &:= \sum_{n=N_0+1}^{\infty}\frac{\Lambda(n)}{n^{\alpha}\log(n)}e^{-n/x} \\ &\leq \frac{e^{-N_0/\boldsymbol{X}}}{N_0^{\alpha}\log(N_0)}(c_{N_0}N_0-\psi(N_0))+\frac{c_{N_0}\boldsymbol{X}^{1-\alpha}}{\log(N_0)}\Gamma(1-\alpha,N_0/\boldsymbol{X}).\end{aligned} \tag{4.5}$$

We then calculate the incomplete Gamma factor $\Gamma(1-\alpha,N_0/\boldsymbol{X})$ (cf. the paper of Gautschi [10]), giving the desired bound.

5. 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 $|D|<D_E$. It is based on a classification of R_E given by Ibukiyama [13] when E is defined over $\mathbb{F}_p$. We will first show how to compute the integers represented by a lattice satisfying certain conditions and then we will show that L_E is one such lattice.

5.1. Efficient computation for certain lattices. Let L_1 be a ternary lattice with associated quadratic form Q and L be the lattice $< a > \oplus L_2$, where L_2 is a 2-dimensional lattice and a is some constant. Assume that L_1 satisfies $L_1 \subseteq L \subseteq \mathbb{Z}^3$ and the restriction $x_1 \equiv x_2 \pmod R$ on the lattice L gives the lattice L_1. We would like to compute the integers $n \leq N$ for which there is a vector in L_1 of length n, namely our goal is to compute

$$\begin{aligned} T_N &:= \{n \leq N : \exists x \in L_1,\ n = Q(x)\} \\ &= \{n \leq N : \exists x \in L,\ x_1 \equiv x_2 \pmod R,\ n = Q(x)\}. \end{aligned}$$

Denote the elements (y_1, y_2) of L_2 satisfying $y_1 \equiv i \pmod R$ by $L_{2,i}$. Define the integers $n \leq M$ for which there is a vector of length n in $L_{2,i}$ by

$$S_{M,i} := \{n \leq M : \exists y \in L_{2,i},\ n = Q(0, y)\}.$$

In order to compute T_N, we address first the simpler problem of computing

$$T_{N,M} := \{n \leq N : \exists m \in S_{M,i} \text{ and } x \equiv i \pmod R,\ ax^2 + m = n\}.$$

Clearly we have $T_M \subseteq T_{M,N} \subseteq T_N$ and $T_{N,N} = T_N$. If the set of possible exceptions

$$X_{N,M} := \{M < n \leq N : n \notin T_{M,N},\ n \text{ is locally represented}\}$$

is small, then we can compute $T_N \setminus T_{M,N}$ rather quickly. Notice in particular that if $X_{N,M} = \emptyset$, then $T_N = T_{M,N}$. Since all sufficiently large eligible integers with bounded divisibility at the anisotropic primes are represented by Q (if they are primitively represented by the spinor genus), this implies that we will be able on average to compute T_N by choosing M much smaller. The computational gain in doing so is evidenced in the following proposition.

Proposition 5.1. *Denote the discriminant of L by D_L. The set $T_{N,M}$ can be computed in running time $O(RM + N + D_L^3 + N^{\frac{1}{2}}M)$ and memory $O(RM + D_L^2)$. Moreover, if we denote $X := \#X_{N,M}$, then T_N can be computed in $O(D_L^3 + RN + N^{\frac{1}{2}}(M + X))$ with storage $O(RN + X + D_L^2)$.*

Proof. We first trivially compute the integers locally represented by Q, taking running time $O(D_L^3)$ and we need to store the answer for the resulting $4D_L^2$ integers. We next use the algorithm of Fincke and Pohst [9] to precompute $S_{M,i}$, with a running time of $O(M)$. Repeating this for each $0 \leq i < R$ gives an overall precomputation time of $O(RM + D_L^3)$ and storage is $O(RM + D_L^2)$ bits. If we represent these sets as a bit array, then checking for membership is clearly $O(1)$.

Now let $n \leq N$ be given such that n is locally represented (checked in $O(1)$). If $n \in T_{N,M}$ then there exists an $x \equiv i \pmod R$ such that $n - ax^2 \in S_{M,i}$, and hence $0 \leq n - ax^2 \leq M$ or $\sqrt{\max\left(\frac{n-M}{a}, 0\right)} \leq x \leq \sqrt{\frac{n}{a}}$.

We thus simply check membership of $n - ax^2 \in S_{M,x \pmod R}$ for each such choice of x. For $n \leq M$ there are $\sqrt{\frac{n}{a}}$ choices and checking these takes $O(M^{\frac{3}{2}}) = O(MN^{\frac{1}{2}})$. For $n \geq M$ there are $\left\lfloor \frac{M}{\sqrt{an}+\sqrt{a(n-M)}} \right\rfloor$ such choices. We then bound against the integral $\int_{x=M}^{N} \frac{M}{x^{\frac{1}{2}}}$ to obtain $O(MN^{\frac{1}{2}})$.

Thus, we can compute $T_{N,M}$ (and simultaneously the complementary set $X_{N,M}$) in $O(RM + N + D_L^3 + MN^{\frac{1}{2}})$. To compute T_N it only remains to compute $T_N \setminus T_{M,N}$ or in other words we must determine for each $n \in X_{N,M}$ whether $n \in T_N$ or $n \notin T_N$. To do so we compute $S_{N,i}$, using the algorithm of Fincke and Pohst again, taking $O(RN)$. Then for each $n \in X_{N,M}$ we check membership for $n - ax^2 \in S_{N,i}$ for $O(N^{\frac{1}{2}})$ choices of x. This is precisely the computation to determine membership of n in $T_{N,N} = T_N$, so we can conclude decisively whether $n \in T_N$ or not.

□

In practice we will then start with $M = N^{\frac{1}{2}}$ and dyadically increase M until $X \leq M$. Moreover, the above algorithm will compute T_N quickly on average.

Theorem 5.2. *The set T_N may be computed on average in $O(N^{1+\epsilon})$, where the implied constant depends on the lattice L_1.*

Proof. Let n be an integer which is locally represented by Q on L_1. Moreover, assume that n is not a primitive spinor exception. This condition may be checked in constant time, using the classification given by Schulze-Pillot [25] or an explicit generalization given by Earnest, Hsia, and Hung [6], and furthermore there are only finitely many square classes tn^2 for which this condition may not be satisfied, so we could nonetheless check these in $O(N)$ again using the algorithm above after adding $N^{\frac{1}{2}}$ exceptions to $X_{N,M}$.

Under these conditions, there are $\Omega(n^{\frac{1}{2}-\epsilon})$ vectors of length n in the lattice L_1. This follows by decomposing the theta series for L_1 into an Eisenstein series and a cuspidal contribution. Since n is locally represented, the n-th Fourier coefficient of the Eisenstein series is a class number by the work of Jones [15, Theorem 86], which Siegel [27] has (ineffectively) shown is $\Omega(n^{\frac{1}{2}-\epsilon})$. The fact that n is primitively represented by the spinor genus implies that the n-th Fourier coefficient of the cusp form is the n-th Fourier coefficient of a cusp form in the orthogonal complement of one dimensional theta series. Duke [4] has shown that these coefficients are bounded by $O(n^{\frac{13}{28}+\epsilon})$. Moreover, since the Fourier coefficients of the theta series of a binary quadratic form are $O(1)$ and L_2 is orthogonal to $< a >$, there are $\Omega(n^{\frac{1}{2}-\epsilon})$ choices of x for which there exists a vector $(x, y_1, y_2) \in L_1$ of length n.

There are $O(n^{\frac{1}{2}})$ choices of x for which the vector $(x, y_1, y_2) \in L_1$ may have length n and $\Omega(n^{\frac{1}{2}-\epsilon})$ actually have length n. Hence if we choose one x there is a probability of $\Omega(n^{-\epsilon})$ that there is some $(y_1, y_2) \in L_2$ for which the vector has length n, and we may treat this as a binomial distribution with $p = n^{-\epsilon}$. We now take $M := N^{\frac{1}{2}+2\epsilon}$. Running the algorithm, the expected number of choices of x for which we will find a vector of length n is

$$\Omega\left(\frac{M}{\sqrt{n}} \cdot n^{-\epsilon}\right) = \Omega(N^{\epsilon}).$$

We then note that $n \in X_{N,M}$ if and only if there is no such x chosen. Chernoff's approximation of the cumulative distribution function implies that

$$Pr(n \in X_{N,M}) \ll e^{-\frac{1}{2}N^{\epsilon}}.$$

Hence the expected value for X is $E(X) \ll Ne^{-\frac{1}{2}N^{\epsilon}} \ll M$, and it follows that the running time of the above algorithm is $O(N^{1+\epsilon})$ on average. □

5.2. Calculating which $|D|$ are represented by the Gross lattice. Assume that E is defined over $\mathbb{F}_p$. We next show that L_E satisfies the conditions of Proposition 5.1 with either $R = 1$ or $R = 2$.

Lemma 5.3. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$, L_E be its associated Gross lattice, and R_E^0 be the lattice of trace zero coefficients. Then there exists a lattice L satisfying $L_E \subseteq L \subset R_E^0$ such that the reduced norm on L is*

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

Proof. Since E is defined over $\mathbb{F}_p$, Ibukiyama [13] has shown that R_E is of one of the following two types,

$$R(q, r) := \mathbb{Z} + \mathbb{Z}\frac{1+\beta}{2} + \mathbb{Z}\frac{\alpha(1+\beta)}{2} + \mathbb{Z}\frac{(r+\alpha)\beta}{q} \tag{5.1}$$

or

$$R'(q, r') := \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(r'+\alpha)\beta}{2q}, \tag{5.2}$$

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 $p \equiv 3 \pmod 4$.

For $R_E = R(q, r)$ with basis $\frac{1+\beta}{2}$, $\gamma_1 := \beta$, $\gamma_2 := \frac{\alpha(1+\beta)}{2}$, and $\gamma_3 := \frac{(r+\alpha)\beta}{q}$, R_E^0 is generated by $\gamma_1, \gamma_2, \gamma_3$ while L_E is generated by $\gamma_1, 2\gamma_2, 2\gamma_3$. We take L to be the lattice generated by $\gamma_1, 2\gamma_2, \gamma_3$. If an arbitrary element of L

is written $x\gamma_1 + 2y\gamma_2 + z\gamma_3$, then the change of variables $x' := x - ry$, $y' := z + qy$ and $z' := y$ gives the reduced norm

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

as desired. Changing z to $2z$ above implies that $z' \equiv y' \pmod 2$, so that the reduced norm on L_E is precisely the quadratic form given above with $z' \equiv y' \pmod 2$.

If $R_E = R'(q, r')$, we have a simpler task. In this case, the reduced norm on R_E^0 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 5.3, the reduced norm on L_E is either of the form

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

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

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

We then compute the integers represented by the reduced norm on L_E by using the algorithm given in Proposition 5.1 with $R = 2$ or $R = 1$, respectively.

Appendix A. Data

We now use the algorithm from Section 4 to compute good bounds for $p \leq 113$, 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.). Tables 1, 2, 3, and 4 give the good bounds for E. Combining the good bounds for every $E/\mathbb{F}_{p^2}$ we obtain good bounds for p in Table 11. For each maximal order R_E, we 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 then list the corresponding ternary quadratic form as $[a, b, c, d, e, f] = ax^2 + by^2 + cz^2 + dxy + exz + fyz$. We next 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.

For $N \in \mathbb{N} \cup \{\infty\}$, let $\mathcal{E}_E^N$ be the set of positive integers $n \leq N$ with $p^2 \nmid n$ not represented by Q_E. We omit those n with $p^2 \mid n$ since p is an anisotropic prime and hence n is represented if and only if $\frac{n}{p^2}$ is represented. In Tables 5, 6, 7, 8, 9, and 10 we list $\mathcal{E}_E^N$ computed using the method described in section 5 when E is defined over $\mathbb{F}_p$ and otherwise using the standard method [9]. For each elliptic curve we have chosen N_0 and N_1 and compute $\mathcal{E}_E^{N_0}$ and $\{n \in \mathcal{E}_E^{N_1} | n \equiv 0 \pmod{p}\}$. When $\#\mathcal{E}_E^N$ is small we list the full set $\mathcal{E}_E^N$, while we otherwise simply list $\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$. Although we are only able to determine $\mathcal{E}_p$ for $p = 11, 17, 19$ under GRH, we are able to determine $\mathcal{E}_E := \mathcal{E}_E^\infty$ for a number of forms, which we denote by an asterisk next to the form.

TABLE 1. Good Bounds D_E for $E/\mathbb{F}_{p^2}$.

p	$\#\mathbb{F}_q$	Quadratic Form	D_0	D_1
11	p	[4,11,12,0,4,0]	1.813×10^8	3.163×10^8
11	p	[3,15,15,-2,2,14]	5.142×10^8	8.973×10^9
17	p	[7,11,20,-6,4,8]	1.002×10^{10}	1.748×10^{11}
17	p	[3,23,23,-2,2,22]	8.652×10^{13}	1.510×10^{15}
19	p	[7,11,23,-2,6,10]	3.020×10^9	5.270×10^{10}
19	p	[4,19,20,0,4,0]	9.198×10^{11}	1.606×10^{13}
23	p	[8,12,23,4,0,0]	7.459×10^{10}	3.700×10^{11}
23	p	[4,23,24,0,4,0]	2.050×10^{14}	2.522×10^{15}
23	p	[3,31,31,-2,2,30]	8.297×10^{14}	6.955×10^{15}
29	p	[11,12,32,8,4,12]	6.739×10^{11}	1.008×10^{12}
29	p	[8,15,31,4,8,2]	3.836×10^{13}	3.130×10^{14}
29	p	[3,39,39,-2,2,38]	1.900×10^{16}	1.550×10^{17}
31	p	[7,19,36,-6,4,16]	3.836×10^{12}	4.359×10^{13}
31	p	[8,16,31,4,0,0]	1.245×10^{13}	2.069×10^{14}
31	p	[4,31,32,0,4,0]	8.558×10^{14}	1.008×10^{16}
37	p^2	[15,20,23,-4,14,8]	2.101×10^{11}	3.667×10^{12}

Table 2. Good Bounds D_E for $E/\mathbb{F}_{p^2}$.

p	$\#\mathbb{F}_q$	Quadratic Form	D_0	D_1
37	p	[8,19,39,4,8,2]	6.399×10^{13}	1.117×10^{15}
41	p	[11,15,47,-2,10,14]	1.834×10^{14}	3.201×10^{15}
41	p	[12,15,44,8,12,4]	2.520×10^{14}	7.830×10^{15}
41	p	[7,24,47,4,2,24]	1.967×10^{15}	1.447×10^{16}
41	p	[3,55,55,-2,2,54]	4.375×10^{17}	3.579×10^{18}
43	p^2	[15,23,24,2,8,12]	2.565×10^{12}	4.476×10^{13}
43	p	[11,16,47,4,2,16]	4.056×10^{13}	7.079×10^{14}
43	p	[4,43,44,0,4,0]	1.364×10^{16}	2.379×10^{17}
47	p	[12,16,47,4,0,0]	1.492×10^{14}	2.604×10^{15}
47	p	[7,27,55,-2,6,26]	1.080×10^{15}	1.527×10^{16}
47	p	[8,24,47,4,0,0]	1.056×10^{15}	1.842×10^{16}
47	p	[4,47,48,0,4,0]	2.339×10^{17}	4.082×10^{18}
47	p	[3,63,63,-2,2,62]	3.702×10^{17}	6.461×10^{18}
53	p^2	[20,23,32,-12,4,20]	1.174×10^{14}	1.428×10^{15}
53	p	[12,19,56,8,12,4]	4.015×10^{15}	6.101×10^{16}
53	p	[8,27,55,4,8,2]	5.825×10^{16}	4.883×10^{17}
53	p	[3,71,71,-2,2,70]	6.918×10^{18}	5.467×10^{19}
59	p	[15,16,63,4,2,16]	5.715×10^{15}	4.395×10^{16}
59	p	[12,20,59,4,0,0]	6.442×10^{15}	3.794×10^{16}
59	p	[15,19,64,-14,8,12]	3.103×10^{16}	3.982×10^{17}
59	p	[7,35,68,-6,4,32]	1.330×10^{16}	1.739×10^{17}
59	p	[4,59,60,0,4,0]	4.413×10^{18}	4.573×10^{19}
59	p	[3,79,79,-2,2,78]	6.579×10^{18}	8.386×10^{19}
61	p^2	[23,24,32,16,4,12]	8.254×10^{14}	6.927×10^{15}
61	p	[7,35,71,-2,6,34]	5.007×10^{15}	2.545×10^{16}
61	p	[8,31,63,4,8,2]	5.892×10^{16}	2.803×10^{17}
61	p	[11,23,68,-6,8,20]	5.240×10^{16}	3.797×10^{17}
67	p^2	[23,24,35,8,2,12]	5.517×10^{14}	9.628×10^{15}
67	p^2	[15,36,39,-4,14,16]	1.105×10^{15}	1.928×10^{16}
67	p	[16,19,71,12,16,6]	1.207×10^{16}	1.987×10^{17}
67	p	[4,67,68,0,4,0]	2.623×10^{18}	2.642×10^{19}
71	p	[15,20,76,8,4,20]	7.313×10^{16}	5.485×10^{17}
71	p	[12,24,71,4,0,0]	3.235×10^{16}	2.936×10^{17}
71	p	[15,19,79,-2,14,18]	1.343×10^{17}	5.962×10^{17}

TABLE 3. Good Bounds D_E for $E/\mathbb{F}_{p^2}$.

p	$\#\mathbb{F}_q$	Quadratic Form	D_0	D_1
71	p	[16,20,71,12,0,0]	1.693×10^{17}	1.667×10^{18}
71	p	[8,36,71,4,0,0]	1.450×10^{17}	2.531×10^{18}
71	p	[4,71,72,0,4,0]	2.876×10^{19}	1.379×10^{20}
71	p	[3,95,95,-2,2,94]	2.725×10^{19}	2.191×10^{20}
73	p^2	[15,39,40,2,8,20]	8.979×10^{15}	1.147×10^{17}
73	p^2	[20,31,44,-12,4,28]	6.740×10^{16}	4.422×10^{17}
73	p	[7,43,84,-6,4,40]	1.025×10^{17}	5.334×10^{17}
73	p	[11,28,80,8,4,28]	1.767×10^{18}	1.452×10^{19}
79	p^2	[23,31,44,18,16,20]	2.150×10^{15}	2.481×10^{16}
79	p	[16,20,79,4,0,0]	2.923×10^{16}	3.458×10^{17}
79	p	[19,20,84,16,8,20]	5.009×10^{16}	8.741×10^{17}
79	p	[11,31,87,-10,6,26]	1.112×10^{17}	1.305×10^{18}
79	p	[8,40,79,4,0,0]	1.169×10^{17}	1.503×10^{18}
79	p	[4,79,80,0,4,0]	6.499×10^{18}	1.121×10^{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}
89	p^2	[23,31,48,2,12,16]	3.896×10^{17}	4.145×10^{18}
89	p	[19,23,95,-18,10,14]	1.236×10^{19}	2.906×10^{19}
89	p	[15,27,96,-14,8,20]	2.636×10^{19}	5.543×10^{19}
89	p	[12,31,92,8,12,4]	4.535×10^{19}	1.108×10^{20}
89	p	[15,24,95,4,2,24]	1.052×10^{20}	1.811×10^{20}
89	p	[7,51,103,-2,6,50]	2.994×10^{20}	3.541×10^{20}
89	p	[3,119,119,-2,2,118]	1.017×10^{22}	6.887×10^{22}
97	p^2	[23,39,51,-22,6,14]	1.241×10^{17}	6.289×10^{17}
97	p^2	[15,52,55,-4,14,24]	4.517×10^{17}	2.630×10^{18}
97	p	[7,56,111,4,2,56]	2.204×10^{18}	4.357×10^{18}
97	p^2	[20,39,59,-4,8,38]	5.923×10^{18}	1.541×10^{19}
97	p	[19,23,104,-14,12,16]	2.188×10^{19}	7.815×10^{19}

Table 4. Good Bounds D_E for $E/\mathbb{F}_{p^2}$.

p	$\#\mathbb{F}_q$	Quadratic Form	D_0	D_1
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	[23,40,56,16,4,20]	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}
109	p^2	[32,44,47,20,28,36]	4.420×10^{16}	7.714×10^{17}
109	p^2	[23,39,59,10,14,22]	5.539×10^{16}	9.666×10^{17}
109	p	[8,55,111,4,8,2]	3.843×10^{17}	5.604×10^{18}
109	p^2	[24,39,56,16,12,4]	8.005×10^{18}	1.397×10^{20}
109	p	[11,40,119,4,2,40]	4.199×10^{19}	7.329×10^{20}
109	p	[19,23,119,-2,18,22]	1.341×10^{20}	1.841×10^{21}
113	p^2	[35,39,47,-6,34,10]	1.141×10^{18}	1.133×10^{19}
113	p^2	[23,40,59,8,2,20]	2.158×10^{18}	2.062×10^{19}
113	p^2	[20,47,68,-12,4,44]	4.539×10^{18}	3.297×10^{19}
113	p	[23,24,119,20,10,24]	3.219×10^{19}	1.853×10^{20}
113	p	[19,24,119,4,2,24]	1.649×10^{19}	2.877×10^{20}
113	p	[12,39,116,8,12,4]	1.610×10^{19}	1.029×10^{20}
113	p	[3,151,151,-2,2,150]	1.105×10^{22}	1.041×10^{23}

TABLE 5. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E$ or ($\#\mathcal{E}_E$ and $\max(\mathcal{E}_E)$)
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^{11}	3, 187, 643
17	[3,23,23,-2,2,22]*	9×10^{13} / 2×10^{15}	$\#\mathcal{E}_E^N = 88$ $\max(\mathcal{E}_E^N) = 89563$
19	[7,11,23,-2,6,10]*	10^{11}	4, 19, 163, 760, 1051
19	[4,19,20,0,4,0]*	10^{12}/ 2×10^{13}	7, 11, 24, 43, 115, 123, 139, 228, 232, 267, 403, 424, 435, 499, 520, 568, 627, 643, 691, 883, 1099, 1411, 1659, 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]*	4×10^{11}	3,4,27, 115, 123,163,403,427, 443, 667,1467, 2787, 3523
23	[4,23,24,0,4,0]	3×10^9	$\#\mathcal{E}_E^N = 78$, $\max(\mathcal{E}_E^N) = 72427$
23	[3,31,31,-2,2,30]	3×10^9	$\#\mathcal{E}_E^N = 196$, $\max(\mathcal{E}_E^N) = 286603$
29	[11,12,32,8,4,12]*	7×10^{11} / 2×10^{12}	$\#\mathcal{E}_E^N = 24$, $\max(\mathcal{E}_E^N) = 22243$
29	[8,15,31,4,8,2]*	4×10^{13}/ 4×10^{14}	$\#\mathcal{E}_E^N = 23$, $\max(\mathcal{E}_E^N) = 7987$
29	[3,39,39,-2,2,38]	10^9	$\#\mathcal{E}_E^N = 382$, $\max(\mathcal{E}_E^N) = 1107307$
31	[7,19,36,-6,4,16]*	2×10^{13}/ 3×10^{14}	$\#\mathcal{E}_E^N = 29$, $\max(\mathcal{E}_E^N) = 15283$
31	[8,16,31,4,0,0]*	4×10^{12}/ 5×10^{13}	$\#\mathcal{E}_E^N = 36$, $\max(\mathcal{E}_E^N) = 17515$
31	[4,31,32,0,4,0]	10^{11}	$\#\mathcal{E}_E^N = 166$, $\max(\mathcal{E}_E^N) = 174003$

Table 6. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E^N$ or ($\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$)
37	[15,20,23,-4,14,8]	10^9	8,19,43,163,427,723,2923,3907
37	[8,19,39,4,8,2]*	6.5×10^{13}/ 2×10^{15}	$\#\mathcal{E}_E^N = 55$, $\max(\mathcal{E}_E^N) = 24952$
41	[11,15,47,-2,10,14]	10^{10}	$\#\mathcal{E}_E^N = 65$, $\max(\mathcal{E}_E^N) = 48547$
41	[12,15,44,8,12,4]	10^{10}	$\#\mathcal{E}_E^N = 60$, $\max(\mathcal{E}_E^N) = 82123$
41	[7,24,47,4,2,24]	3×10^9	$\#\mathcal{E}_E^N = 82$, $\max(\mathcal{E}_E^N) = 83107$
41	[3,55,55,-2,2,54]	10^{10}	$\#\mathcal{E}_E^N = 896$, $\max(\mathcal{E}_E^N) = 5017867$
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]*	4.5×10^{13}/ 8×10^{14}	$\#\mathcal{E}_E^N = 81$, $\max(\mathcal{E}_E^N) = 73315$
43	[4,43,44,0,4,0]	10^9	$\#\mathcal{E}_E^N = 439$, $\max(\mathcal{E}_E^N) = 1079467$
47	[12,16,47,4,0,0]	10^9	$\#\mathcal{E}_E^N = 106$, $\max(\mathcal{E}_E^N) = 272083$
47	[7,27,55,-2,6,26]	10^9	$\#\mathcal{E}_E^N = 112$, $\max(\mathcal{E}_E^N) = 78772$
47	[8,24,47,4,0,0]	10^9	$\#\mathcal{E}_E^N = 108$, $\max(\mathcal{E}_E^N) = 85963$
47	[4,47,48,0,4,0]	2×10^9	$\#\mathcal{E}_E^N = 556$, $\max(\mathcal{E}_E^N) = 5345827$
47	[3,63,63,-2,2,62]	10^9	$\#\mathcal{E}_E^N = 1165$, $\max(\mathcal{E}_E^N) = 4812283$
53	[20,23,32,-12,4,20]	10^9	$\#\mathcal{E}_E^N = 30$, $\max(\mathcal{E}_E^N) = 33147$
53	[12,19,56,8,12,4]	10^9	$\#\mathcal{E}_E^N = 138$, $\max(\mathcal{E}_E^N) = 178027$
53	[8,27,55,4,8,2]	10^9	$\#\mathcal{E}_E^N = 152$, $\max(\mathcal{E}_E^N) = 137323$
53	[3,71,71,-2,2,70]	10^9	$\#\mathcal{E}_E^N = 1604$, $\max(\mathcal{E}_E^N) = 6474427$
59	[15,16,63,4,2,16]	2×10^9	$\#\mathcal{E}_E^N = 158$, $\max(\mathcal{E}_E^N) = 304027$
59	[12,20,59,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 193$, $\max(\mathcal{E}_E^N) = 316747$
59	[15,19,64,-14,8,12]	2×10^9	$\#\mathcal{E}_E^N = 174$, $\max(\mathcal{E}_E^N) = 318091$
59	[7,35,68,-6,4,32]	2×10^9	$\#\mathcal{E}_E^N = 228$, $\max(\mathcal{E}_E^N) = 132883$
59	[4,59,60,0,4,0]	2×10^9	$\#\mathcal{E}_E^N = 920$, $\max(\mathcal{E}_E^N) = 3136219$
59	[3,79,79,-2,2,78]	2×10^9	$\#\mathcal{E}_E^N = 2072$, $\max(\mathcal{E}_E^N) = 8447443$

TABLE 7. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E^N$ or ($\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$)
61	[23,24,32,16,4,12]	2×10^9	$\#\mathcal{E}_E^N = 43$, $\max(\mathcal{E}_E^N) = 11923$
61	[7,35,71,-2,6,34]	2×10^9	$\#\mathcal{E}_E^N = 271$, $\max(\mathcal{E}_E^N) = 1096867$
61	[8,31,63,4,8,2]	2×10^9	$\#\mathcal{E}_E^N = 233$, $\max(\mathcal{E}_E^N) = 363987$
61	[11,23,68,-6,8,20]	2×10^9	$\#\mathcal{E}_E^N = 201$, $\max(\mathcal{E}_E^N) = 190747$
67	[23,24,35,8,2,12]	10^9	$\#\mathcal{E}_E^N = 59$, $\max(\mathcal{E}_E^N) = 126043$
67	[15,36,39,-4,14,16]	10^9	$\#\mathcal{E}_E^N = 57$, $\max(\mathcal{E}_E^N) = 20707$
67	[16,19,71,12,16,6]	2×10^9	$\#\mathcal{E}_E^N = 264$, $\max(\mathcal{E}_E^N) = 421579$
67	[4,67,68,0,4,0]	10^9	$\#\mathcal{E}_E^N = 1271$, $\max(\mathcal{E}_E^N) = 3846403$
71	[15,20,76,8,4,20]	2×10^9	$\#\mathcal{E}_E^N = 275$, $\max(\mathcal{E}_E^N) = 321883$
71	[12,24,71,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 307$, $\max(\mathcal{E}_E^N) = 635947$
71	[15,19,79,-2,14,18]	2×10^9	$\#\mathcal{E}_E^N = 273$, $\max(\mathcal{E}_E^N) = 267883$
71	[16,20,71,12,0,0]	2×10^9	$\#\mathcal{E}_E^N = 310$, $\max(\mathcal{E}_E^N) = 1540771$
71	[8,36,71,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 346$, $\max(\mathcal{E}_E^N) = 1053427$
71	[4,71,72,0,4,0]	2×10^9	$\#\mathcal{E}_E^N = 1450$, $\max(\mathcal{E}_E^N) = 6463627$
71	[3,95,95,-2,2,94]	2×10^9	$\#\mathcal{E}_E^N = 3170$, $\max(\mathcal{E}_E^N) = 15135283$
73	[15,39,40,2,8,20]	10^9	$\#\mathcal{E}_E^N = 81$, $\max(\mathcal{E}_E^N) = 53188$
73	[20,31,44,-12,4,28]	10^9	$\#\mathcal{E}_E^N = 72$, $\max(\mathcal{E}_E^N) = 111763$
73	[7,43,84,-6,4,40]	2×10^9	$\#\mathcal{E}_E^N = 420$, $\max(\mathcal{E}_E^N) = 364708$
73	[11,28,80,8,4,28]	2×10^9	$\#\mathcal{E}_E^N = 336$, $\max(\mathcal{E}_E^N) = 723795$
79	[23,31,44,18,16,20]	10^9	$\#\mathcal{E}_E^N = 88$, $\max(\mathcal{E}_E^N) = 50955$
79	[16,20,79,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 383$, $\max(\mathcal{E}_E^N) = 1419867$
79	[19,20,84,16,8,20]	2×10^9	$\#\mathcal{E}_E^N = 391$, $\max(\mathcal{E}_E^N) = 1210675$
79	[11,31,87,-10,6,26]	2×10^9	$\#\mathcal{E}_E^N = 409$, $\max(\mathcal{E}_E^N) = 12778803$
79	[8,40,79,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 495$, $\max(\mathcal{E}_E^N) = 1116507$
79	[4,79,80,0,4,0]	2×10^9	$\#\mathcal{E}_E^N = 1886$, $\max(\mathcal{E}_E^N) = 25575460$

Table 8. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E^N$ or ($\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$)
83	[23,31,44,-14,8,12]	10^9	$\#\mathcal{E}_E^N = 97$, $\max(\mathcal{E}_E^N) = 36763$
83	[12,28,83,4,0,0]	2×10^9	$\#\mathcal{E}_E^N = 432$, $\max(\mathcal{E}_E^N) = 635347$
83	[7,48,95,4,2,48]	2×10^9	$\#\mathcal{E}_E^N = 529$, $\max(\mathcal{E}_E^N) = 1358107$
83	[16,23,87,12,16,6]	2×10^9	$\#\mathcal{E}_E^N = 416$, $\max(\mathcal{E}_E^N) = 1202587$
83	[11,31,92,-6,8,28]	2×10^9	$\#\mathcal{E}_E^N = 469$, $\max(\mathcal{E}_E^N) = 1381867$
83	[3,111,111,-2,2,110]	2×10^9	$\#\mathcal{E}_E^N = 4639$, $\max(\mathcal{E}_E^N) = 62337067$
83	[4,83,84,0,4,0]	2×10^9	$\#\mathcal{E}_E^N = 2134$, $\max(\mathcal{E}_E^N) = 9405643$
89	[23,31,48,2,12,16]	10^9	$\#\mathcal{E}_E^N = 118$, $\max(\mathcal{E}_E^N) = 137707$
89	[19,23,95,-18,10,14]	5×10^8	$\#\mathcal{E}_E^N = 540$, $\max(\mathcal{E}_E^N) = 981403$
89	[15,27,96,-14,8,20]	5×10^8	$\#\mathcal{E}_E^N = 464$, $\max(\mathcal{E}_E^N) = 1534723$
89	[12,31,92,8,12,4]	5×10^8	$\#\mathcal{E}_E^N = 478$, $\max(\mathcal{E}_E^N) = 653227$
89	[15,24,95,4,2,24]	5×10^8	$\#\mathcal{E}_E^N = 502$, $\max(\mathcal{E}_E^N) = 682147$
89	[7,51,103,-2,6,50]	5×10^8	$\#\mathcal{E}_E^N = 646$, $\max(\mathcal{E}_E^N) = 1427827$
89	[3,119,119,-2,2,118]	2×10^9	$\#\mathcal{E}_E^N = 5357$, $\max(\mathcal{E}_E^N) = 28654707$
97	[23,39,51,-22,6,14]	10^9	$\#\mathcal{E}_E^N = 283$, $\max(\mathcal{E}_E^N) = 74011$
97	[15,52,55,-4,14,24]	10^9	$\#\mathcal{E}_E^N = 295$, $\max(\mathcal{E}_E^N) = 94963$
97	[7,56,111,4,2,56]	10^9	$\#\mathcal{E}_E^N = 814$, $\max(\mathcal{E}_E^N) = 851272$
97	[20,39,59,-4,8,38]	10^9	$\#\mathcal{E}_E^N = 277$, $\max(\mathcal{E}_E^N) = 118243$
97	[19,23,104,-14,12,16]	10^9	$\#\mathcal{E}_E^N = 636$, $\max(\mathcal{E}_E^N) = 1336483$
101	[32,39,44,-12,28,20]	10^9	$\#\mathcal{E}_E^N = 158$, $\max(\mathcal{E}_E^N) = 123523$
101	[12,35,104,8,12,4]	10^9	$\#\mathcal{E}_E^N = 652$, $\max(\mathcal{E}_E^N) = 1157083$
101	[15,28,108,8,4,28]	10^9	$\#\mathcal{E}_E^N = 625$, $\max(\mathcal{E}_E^N) = 1299163$
101	[15,27,111,-2,14,26]	10^9	$\#\mathcal{E}_E^N = 652$, $\max(\mathcal{E}_E^N) = 901363$
101	[8,51,103,4,8,2]	10^9	$\#\mathcal{E}_E^N = 803$, $\max(\mathcal{E}_E^N) = 1996467$
101	[7,59,116,-6,4,56]	10^9	$\#\mathcal{E}_E^N = 881$, $\max(\mathcal{E}_E^N) = 1720048$
101	[11,39,111,-10,6,34]	10^9	$\#\mathcal{E}_E^N = 723$, $\max(\mathcal{E}_E^N) = 1305627$
101	[3,135,135,-2,2,134]	10^9	$\#\mathcal{E}_E^N = 7304$, $\max(\mathcal{E}_E^N) = 24487147$

TABLE 9. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E^N$ or ($\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$)
103	[23,36,59,-4,22,16]	10^9	$\#\mathcal{E}_E^N = 174$, $\max(\mathcal{E}_E^N) = 121027$
103	[16,28,103,-12,0,0]	10^9	$\#\mathcal{E}_E^N = 696$, $\max(\mathcal{E}_E^N) = 1004347$
103	[15,55,56,2,8,28]	10^9	$\#\mathcal{E}_E^N = 200$, $\max(\mathcal{E}_E^N) = 353728$
103	[19,23,111,-10,14,18]	10^9	$\#\mathcal{E}_E^N = 709$, $\max(\mathcal{E}_E^N) = 1086547$
103	[7,59,119,-2,6,58]	10^9	$\#\mathcal{E}_E^N = 903$, $\max(\mathcal{E}_E^N) = 1959163$
103	[8,52,103,4,0,0]	10^9	$\#\mathcal{E}_E^N = 896$, $\max(\mathcal{E}_E^N) = 1019467$
103	[4,103,104,0,4,0]	10^9	$\#\mathcal{E}_E^N = 2358$, $\max(\mathcal{E}_E^N) = 6390532$
107	[35,39,44,-18,32,4]	10^9	$\#\mathcal{E}_E^N = 186$, $\max(\mathcal{E}_E^N) = 169467$
107	[23,40,56,16,4,20]	10^9	$\#\mathcal{E}_E^N = 209$, $\max(\mathcal{E}_E^N) = 274387$
107	[16,27,111,-4,16,2]	10^9	$\#\mathcal{E}_E^N = 769$, $\max(\mathcal{E}_E^N) = 2998675$
107	[12,36,107,4,0,0]	10^9	$\#\mathcal{E}_E^N = 817$, $\max(\mathcal{E}_E^N) = 695179$
107	[19,23,116,-6,16,20]	10^9	$\#\mathcal{E}_E^N = 813$, $\max(\mathcal{E}_E^N) = 3142483$
107	[11,39,119,-2,10,38]	10^9	$\#\mathcal{E}_E^N = 856$, $\max(\mathcal{E}_E^N) = 838987$
107	[4,107,108,0,4,0]	10^9	$\#\mathcal{E}_E^N = 3873$, $\max(\mathcal{E}_E^N) = 13204228$
107	[3,143,143,-2,2,142]	10^9	$\#\mathcal{E}_E^N = 8410$, $\max(\mathcal{E}_E^N) = 44363163$
109	[32,44,47,20,28,36]	10^8	$\#\mathcal{E}_E^N = 205$, $\max(\mathcal{E}_E^N) = 193747$
109	[23,39,59,10,14,22]	10^8	$\#\mathcal{E}_E^N = 215$, $\max(\mathcal{E}_E^N) = 1034083$
109	[8,55,111,4,8,2]	10^9	$\#\mathcal{E}_E^N = 1039$, $\max(\mathcal{E}_E^N) = 2522587$
109	[24,39,56,16,12,4]	10^8	$\#\mathcal{E}_E^N = 225$, $\max(\mathcal{E}_E^N) = 215659$
109	[11,40,119,4,2,40]	10^9	$\#\mathcal{E}_E^N = 891$, $\max(\mathcal{E}_E^N) = 947755$
109	[19,23,119,-2,18,22]	10^9	$\#\mathcal{E}_E^N = 857$, $\max(\mathcal{E}_E^N) = 1300915$
113	[35,39,47,-6,34,10]	10^8	$\#\mathcal{E}_E^N = 213$, $\max(\mathcal{E}_E^N) = 142267$
113	[23,40,59,8,2,20]	10^8	$\#\mathcal{E}_E^N = 220$, $\max(\mathcal{E}_E^N) = 146787$
113	[20,47,68,-12,4,44]	10^8	$\#\mathcal{E}_E^N = 247$, $\max(\mathcal{E}_E^N) = 253363$
113	[23,24,119,20,10,24]	5×10^9	$\#\mathcal{E}_E^N = 904$, $\max(\mathcal{E}_E^N) = 1800643$

TABLE 10. The set of exceptions $\mathcal{E}_E^N$.

p	Quadratic Form	N_0/N_1	$\mathcal{E}_E^N$ or ($\#\mathcal{E}_E^N$ and $\max(\mathcal{E}_E^N)$)
113	[19,24,119,4,2,24]	5×10^9	$\#\mathcal{E}_E^N = 1005$, $\max(\mathcal{E}_E^N) = 1997835$
113	[12,39,116,8,12,4]	5×10^9	$\#\mathcal{E}_E^N = 907$, $\max(\mathcal{E}_E^N) = 1130803$
113	[3,151,151,-2,2,150]	5×10^9	$\#\mathcal{E}_E^N = 9302$, $\max(\mathcal{E}_E^N) = 30158683$

TABLE 11. Good Bounds D_p from Theorem 1.1 for $p \leq 113$.

p	D_p	p	D_p
$3, 5, 7, 13$	1	61	3.797×10^{17}
11	8.973×10^9	67	2.642×10^{19}
17	1.510×10^{15}	71	2.191×10^{20}
19	1.606×10^{13}	73	1.452×10^{19}
23	6.955×10^{15}	79	1.121×10^{20}
29	1.550×10^{17}	83	1.033×10^{20}
31	1.008×10^{16}	89	6.887×10^{22}
37	1.117×10^{15}	97	7.815×10^{19}
41	3.579×10^{18}	101	5.296×10^{20}
43	1.364×10^{17}	103	8.748×10^{19}
47	6.461×10^{18}	107	1.761×10^{21}
53	5.467×10^{19}	109	1.841×10^{21}
61	8.396×10^{19}	113	1.041×10^{23}

References

[1] J. CREMONA, *Algorithms for elliptic curves*. Cambridge Univ. Press, 1992.

[2] P. DELIGNE, *La conjecture de weil i*. Inst. Hautes Études Sci. Publ. Math **43** (1974), 273–307.

[3] M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörpen*. Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[4] W. DUKE, *Hyperbolic distribution problems and half-integral weight maass forms*. Invent. Math. **92** (1998), 73–90.

[5] W. DUKE AND R. SCHULZE-PILLOT, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*. Invent. Math. **99** (1990), no. 1, 49–57.

[6] A. EARNEST, J. HSIA, AND D. HUNG, *Primitive representations by spinor genera of ternary quadratic forms*. J. London Math. Soc. (2) **50** (1994), no. 2, 222–230.

[7] N. ELKIES, *Supersingular primes for elliptic curves over real number fields*. Compositio Mathematica **72** (1989), 165–172.

[8] N. ELKIES, K. ONO, AND T. YANG, *Reduction of CM elliptic curves and modular function congruences*. Int. Math. Res. Not. **44** (2005), 2695–2707.

[9] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*. Math. Comp. (1985), 463–471.
[10] W. Gautschi, *A computational procedure for incomplete Gamma functions*. ACM Transactions on Mathematical Software **5** (1979), 466–481.
[11] B. Gross, *Heights and the special values of L-series*. Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.
[12] B. Gross and D. Zagier, *On singular moduli*. J. Reine Angew. Math. **335** (1985), 191–220.
[13] T. Ibukiyama, *On maximal order of division quaternion algebras over the rational number field with certain optimal embeddings*. Nagoya Math J. **88** (1982), 181–195.
[14] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*. Invent. Math. **87** (1987), 385–401.
[15] B. Jones, *The arithmetic theory of quadratic forms*. Carcus Monograph Series, no. 10, The Mathematical Association of America, Buffalo, Buffalo, NY, 1950.
[16] B. Kane, *Representations of integers by ternary quadratic forms*. preprint (2007).
[17] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, Ph.D. Thesis (1996), pp. 1–96.
[18] W. Kohnen, *Newforms of half integral weight*. J. reine angew. Math. **333** (1982), 32–72.
[19] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*. Invent. Math. **64** (1981), 175–198.
[20] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*. Astérique **121-122** (1985), 309–323.
[21] O. T. O'Meara, *Introduction to quadratic forms*. Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition.
[22] K. Ono, *Web of modularity: Arithmetic of the coefficients of modular forms and q-series*. CBMS Regional Conference Series in Mathematics, no. 102, Amer. Math. Soc., Providence, RI, 2003.
[23] K. Ono and K. Soundarajan, *Ramanujan's ternary quadratic form*. Invent. Math. **130** (1997), 415–454.
[24] A. Pizer, *An algorithm for compute modular forms on* $\Gamma_0(N)$. J. Algebra **64** (1980), no. 2, 340–390.
[25] R. Schulze-Pillot, *Darstellungsmaße von Spinorgeschlechtern ternärer quadratischer Formen*. J. Reine Angew. Math., **352** (1984), 114–132.
[26] G. Shimura, *On modular forms of half integer weight*. Ann. of Math. **97** (1973), 440–481.
[27] C. Siegel, *Über die klassenzahl quadratischer zahlkorper*. Acta Arith. **1** (1935), 83–86.
[28] J. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.
[29] W. Stein, *Explicit approaches to modular abelian varieties*. Ph.D. thesis, University of California, Berkeley (2000), pp. 1–96.
[30] ———, *Modular forms, a computational approach*. Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, Appendix by P. Gunnells.
[31] J. Sturm, *On the congruence of modular forms*. Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280.
[32] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*. Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
[33] M. Watkins, *Class numbers of imaginary quadratic fields*. Math. Comp. **73** (2004), 907–938.

Ben Kane
Department of Mathematics
Radboud Universiteit Nijmegen
Heijendaalseweg 135, 6525 AJ Nijmegen, Netherlands
E-mail: bkane@science.ru.nl