Title	On sign changes of cusp forms and the halting of an algorithm to construct a supersingular elliptic curve with a given endomorphism ring
Author(s)	FUNG, KC; Kane, BR
Citation	Mathematics of Computation, 2016
Issued Date	2016
URL	http://hdl.handle.net/10722/231990
Rights	First published in [Publication] in [volume and number, or year], published by the American Mathematical Society; This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

ON SIGN CHANGES OF CUSP FORMS AND THE HALTING OF AN ALGORITHM TO CONSTRUCT A SUPERSINGULAR ELLIPTIC CURVE WITH A GIVEN ENDOMORPHISM RING

KING CHEONG FUNG AND BEN KANE

ABSTRACT. Chevyrev and Galbraith recently devised an algorithm which inputs a maximal order of the quaternion algebra ramified at one prime and infinity and constructs a supersingular elliptic curve whose endomorphism ring is precisely this maximal order. They proved that their algorithm is correct whenever it halts, but did not show that it always terminates. They did however prove that the algorithm halts under a reasonable assumption which they conjectured to be true. It is the purpose of this paper to verify their conjecture and in turn prove that their algorithm always halts.

More precisely, Chevyrev and Galbraith investigated the theta series associated with the norm maps from primitive elements of two maximal orders. They conjectured that if one of these theta series "dominated" the other in the sense that the nth (Fourier) coefficient of one was always larger than or equal to the nth coefficient of the other, then the maximal orders are actually isomorphic. We prove that this is the case.

1. INTRODUCTION

In this paper, we investigate the construction of certain elliptic curves defined over finite fields. For a prime p, let E be an elliptic curve over $\mathbb{F}_{p^2}$. Deuring [4] showed that the endomorphism ring of E is either an order in an imaginary quadratic field (the *ordinary* case) or an order in the quaternion algebra B_p (see Section 2.1) which is ramified at p and infinity (the *supersingular* case). The supersingular case is the primary interest of this paper. To motivate one area of study related to such curves, we momentarily consider elliptic curves over a number field, in which case the endomorphism ring is either isomorphic to $\mathbb{Z}$ or it is isomorphic to an order in an imaginary quadratic field (the *Complex Multiplication* or *CM* case). In the second case, we say that the elliptic curve has (exact) CM by this order. Next recall that the orders of an imaginary quadratic field are entirely determined by their discriminants; that is to say, for each discriminant $d < 0$, there is a unique order $\mathcal{O}_d$ of discriminant d in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ of $\mathbb{Q}(\sqrt{d})$. When p is a prime of good reduction, there is a natural reduction map from elliptic curves over the Hilbert class field of $\mathbb{Q}(\sqrt{d})$ (a certain number field) to elliptic curves over $\mathbb{F}_{p^2}$. Moreover, when p is inert or ramified in $\mathbb{Q}(\sqrt{d})$, this map sends CM elliptic curves to supersingular elliptic curves. An interesting question arises from this connection. Namely, for which d is the reduction map from the set of elliptic curves with CM by $\mathcal{O}_d$ to supersingular elliptic curves surjective? This question was studied by a number of authors (cf. [6] and [13]). It turns out that the reduction map is not always surjective and is not in general one-to-one. Different authors have also approached the question in different directions and from slightly different perspectives. Elkies, Ono and Yang [6] worked on the question when the discriminant d was

restricted to be fundamental. In other words, they considered those elliptic curves with exact CM by the ring of integers $\mathscr{O}_{\mathbb{Q}(\sqrt{d})}$ of an imaginary quadratic field and varied the field. They proved that for d sufficiently large, the image of the reduction map is surjective and furthermore that it is equidistributed across all supersingular elliptic curves. A slight modification of this was investigated by Jetchev and the second author [13], where it was shown that the reduction from curves with exact CM by $\mathscr{O}_d$ is surjective for d sufficiently large but not necessarily fundamental (albeit with some minor restriction on the choice of d). The approach taken in [6] and [13] was to use a correspondence between elliptic curves with CM by $\mathscr{O}_d$ which reduce to a supersingular elliptic curve and *optimal embeddings* of $\mathscr{O}_d$ in its endomorphism ring; roughly speaking, if $\mathscr{O}_d$ embeds into the quaternionic order, then $\mathscr{O}_{dr^2}$ also embeds by multiplying by r, and optimal embeddings are those which do not come from smaller discriminants. These optimal embeddings, in turn, correspond to primitive representations of d by the norm map on trace zero elements in the quaternionic order.

Having given one area of study centered around supersingular elliptic curves, we return to the study of supersingular elliptic curves themselves. Chevyrev and Galbraith [3] constructed an algorithm to compute a supersingular elliptic curve with a given endomorphism ring (a maximal order in the quaternion algebra). Their construction involved *successive minima* (the smallest, second smallest, etc. positive integers that are *primitively* represented) of the quadratic form corresponding to the reduced norm map on the maximal order. They showed that their algorithm gives the correct answer whenever it terminates, but they did not show that the algorithm indeed halts. Although they did not show that it halts, they were able to prove that the algorithm would halt unless there exist a pair of maximal orders satisfying a peculiar relation between their norm maps. Roughly speaking, their algorithm halts unless there are two different maximal orders for which the first one contains more optimal embeddings of $\mathscr{O}_d$ than the second one for all d. For such a pair of maximal orders, Chevyrev and Galbraith said that the first order "dominates" the second order. They then conjectured that no such pair exists (see Conjecture 3.1 for a precise statement and (2.1) for the definition of the relevant quantities).

Conjecture 1.1 (Chevyrev–Galbraith). *Suppose that $\mathscr{O}$ and $\mathscr{O}'$ are maximal orders in the quaternion algebra B_p ramified precisely at p and ∞. If $\mathscr{O}'$ "dominates" $\mathscr{O}$ in the sense that (3.1) holds for all $n \in \mathbb{N} := \{n \in \mathbb{Z} : n \geq 1\}$, then $\mathscr{O}$ and $\mathscr{O}'$ are isomorphic.*

The goal of this paper is to prove Conjecture 1.1, and in turn prove the halting of the algorithm of Chevyrev and Galbraith.

Theorem 1.2. *Conjecture 1.1 is true. Furthermore, the algorithm of Chevyrev and Galbraith halts.*

The peculiar relation mentioned above involves the theta series of maximal orders generated by their norm maps on their trace zero elements, which are in fact ternary quadratic forms. Therefore, in order to solve our problem, some properties and facts about ternary quadratic forms and their theta series are required. As reviewed in Section 2, by the general theory of modular forms we know that the theta series are modular forms of weight $3/2$. Conjecture 1.1 essentially states that if the nth (Fourier) coefficient of the theta series associated with one maximal order is always greater than the nth coefficient of the theta function associated to another maximal order, then the theta functions are the same. Our strategy to attack the problem is to take the difference of the corresponding theta series. Using the *mass formula*, which was introduced by Siegel [24] and later was extended by Schulze-Pillot [22], one can show that the difference of these theta series is a cusp form and that this cusp form is orthogonal to certain functions known as unary theta functions (see Lemma 4.1). The central idea is to use the fact that coefficients of such forms must either vanish identically or change sign

infinitely often. Sign changes of cusp forms have a long history going back to Siegel [25]. The existence of sign changes and bounds for the occurrence of the first sign change were more recently revisited and extended by a number of authors (cf. [1, 2, 10, 11, 14, 16, 17]). We are specifically interested in sign changes of half-integral weight cusp forms (since the theta series are weight $3/2$ modular forms as noted above). The investigation of sign changes of such forms appears to have been instigated by Bruinier and Kohnen [2], who showed the existence of sign changes and conjectured a distribution of the sign changes. This conjecture was later shown in a number of cases by collaboration of Arias-de-Reyna, Inam, and Wiese (see [1, 10, 11]). Bruinier and Kohnen (as well as Arias-de-Reyna, Inam, and Wiese) considered sign changes of special cusp forms known as Hecke eigenforms. For our application we do not always have Hecke eigenforms, so we rely on results about sign changes of more general half-integral weight cusp forms proven by Kohnen, Lau and Wu [16].

The paper is organized as follows. In Section 2 we introduce some of the necessary background and notation for quaternion algebras and modular forms, in Section 3 we give a precise statement of Chevyrev and Galbraith's conjecture, and in Section 4 we prove the their conjecture.

2. PRELIMINARIES

In this section, we introduce some notation and give the main necessary definitions.

2.1. Quaternion algebras.

A *quaternion algebra B* over $\mathbb{Q}$ is a non-commutative rank 4 algebra with the following properties (see [26, Chapter 1] for further information).

(1) As a vector space over $\mathbb{Q}$, there are four generators, 1, α, β, and $\alpha\beta$.
(2) There exist $r, s \in \mathbb{Q}^\times$ such that $\alpha^2 = r$ and $\beta^2 = s$.
(3) We have $\alpha\beta = -\beta\alpha$.
(4) There is an involution, known as the *standard involution* defined for $a, b, c, d \in \mathbb{Q}$ by

$$\overline{a + b\alpha + c\beta + d\alpha\beta} = a - b\alpha - c\beta - d\alpha\beta.$$

The *reduced trace* of an element $h := a + b\alpha + c\beta + d\alpha\beta \in B$ is

$$\mathrm{Tr}(h) := h + \overline{h} = 2a.$$

The trace zero elements we denote by

$$B^0 := \{h \in B : \mathrm{Tr}(h) = 0\}.$$

The *reduced norm* of h is

$$\mathrm{Nr}(h) := h\overline{h} = a^2 - rb^2 - sc^2 + rsd^2.$$

The norm Nr is a quadratic form (i.e., a homogeneous degree 2 polynomial) in 4 variables over $\mathbb{Q}$. We call the quaternion algebra *definite* if the norm map is positive-definite. If B is definite, then it is also a division algebra. For $h \in B$, the *reduced characteristic polynomial* for h is

$$x^2 - \mathrm{Tr}(h)x + \mathrm{Nr}(h).$$

For $h \notin \mathbb{Q}$, this is the minimal polynomial of h over $\mathbb{Q}$. If the coefficients are furthermore in $\mathbb{Z}$, then we call h an *integral* element.

An *order* of B is a rank 4 lattice (over $\mathbb{Z}$) of B which is also a subring of B. An order is called *maximal* if it is not a proper suborder of another order of B. Unlike orders in the ring

of integers of a quadratic field, there may be more than one maximal order; for example, given a maximal order $\mathscr{O}$ and $h \in B$, since B is non-commutative one may obtain a distinct order by conjugation. If two maximal orders $\mathscr{O}$ and $\mathscr{O}'$ are conjugate (i.e., there exists $c \in B_p$ for which $\mathscr{O}' = c^{-1}\mathscr{O}c$ or equivalently the orders are isomorphic), then one says that they have the same *type* and write $\mathscr{O} \sim \mathscr{O}'$. Note further that the elements h of an order $\mathscr{O}$ are necessarily integral because for $h \in \mathscr{O}$, the $\mathbb{Z}$-module $\mathbb{Z}[h]$ is a sublattice of $\mathscr{O}$ and is therefore finitely generated.

Taking the tensor product $B \otimes_{\mathbb{Q}} K$ with a local field $K = \mathbb{R}$ or $K = \mathbb{Q}_p$, one obtains either the ring of 2×2 matrices $M(2,K)$ or a quaternion division algebra. The quaternion division algebra over K is unique up to isomorphism (cf. [26, p. 31]). We say that B is *ramified* at a prime p (resp. ramified at ∞) if $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ (resp. $B \otimes_{\mathbb{Q}} \mathbb{R}$) is the divison algebra and we say that B is *split* (or unramified) at p (resp. ∞) otherwise. In this paper, we are particularly interested in the quaternion algeba B_p ramified precisely at p and ∞. As noted above, the reduced norm on B_p is a *quaternary* (4-variable) quadratic form. For a maximal order $\mathscr{O}$, the reduced norm restricted to the set of trace-zero elements $\mathscr{O} \cap B_p^0$ is an integral *ternary* (3-variable) quadratic form. Slightly modifying this, we define the so-called "Gross lattice" [7, (12.8)] to be

$$\mathscr{O}^T := (2\mathscr{O} + \mathbb{Z}) \bigcap B_p^0 = \{2x - \mathrm{Tr}(x) : x \in \mathscr{O}\}.$$

By [7, Proposition 12.9], elements of $\mathscr{O}^T$ with norm d are essentially in one-to-one correspondence with embeddings of the quadratic order $\mathscr{O}_d$ into $\mathscr{O}$. More precisely, denote the generators of $\mathscr{O}^T$ over $\mathbb{Z}$ by u_1, u_2, u_3 and let

$$a_{\mathscr{O}^T}(d) := \#\left\{ h = h_1 u_1 + h_2 u_2 + h_3 u_3 \in \mathscr{O}^T : \mathrm{Nr}(x) = d, \ \mathfrak{g}(h) = 1 \right\}, \quad \text{with} \qquad (2.1)$$

$$\mathfrak{g}(h) := \gcd(h_1, h_2, h_3), \qquad (2.2)$$

be the number of primitive representations of d for the reduced norm Nr on $\mathscr{O}^T$. Then

$$a_{\mathscr{O}^T}(d) = \frac{h_{\mathscr{O}}(d)}{u(d)}, \qquad (2.3)$$

where $h_{\mathscr{O}}(d)$ denotes the number of optimal embeddings of $\mathscr{O}_d$ into $\mathscr{O}$ and $u(d)$ denotes the number of units in $\mathscr{O}_d$.

2.2. Quadratic forms and theta functions.
As noted above, a quadratic form Q is a homogeneous polynomial in n variables of degree 2. We may associate Q with its (symmetric) Gram matrix A, in which case the quadratic form for $X \in Q^n$ may be written

$$Q(X) = \frac{1}{2}X^T A X.$$

We say that Q is *integral* if all of the entries of A are in $\mathbb{Z}$ and we call Q *integer-valued* if $Q(X) \in \mathbb{Z}$ for all $X \in \mathbb{Z}^n$; to see the difference, consider $Q(X,Y) = X^2 + XY + Y^2$. We call Q *positive-definite* (resp. *negative-definite*) if $Q(X) \geq 0$ (resp. $Q(X) \leq 0$) for all $X \in \mathbb{Q}^n$ and $Q(X) = 0$ if and only if $X = 0$. In this paper, we are mostly interested in positive-definite integral ternary quadratic forms. For further information about ternary quadratic forms, a good survey may be found in [9].

We split the quadratic forms into *classes*, sets of quadratic forms which are equivalent under the action of $\mathrm{GL}_3(\mathbb{Z})$. Two forms Q and $\mathscr{Q}$ in the same class are referred to as *globally-equivalent* and we simply write $Q \sim_{\mathbb{Z}} \mathscr{Q}$ for this relation. Classes are then grouped together based on their local conditions. For a positive-definite integral quadratic form ($a_{ij} \in \mathbb{Z}$)

$$Q(X) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,$$

4

since $\mathbb{Z}$ embeds into the ℓ-adic integers $\mathbb{Z}_\ell$, it is natural to allow $X \in \mathbb{Z}_\ell$ and consider Q as a quadratic form over $\mathbb{Z}_\ell$ (equivalently, we may tensor the Gram matrix with $\mathbb{Z}_\ell$ over $\mathbb{Z}$). Considering Q over all $\mathbb{Z}_\ell$ simultaneously leads to an adelic interpretation; we do not investigate this further here, but simply note that we obtain a quadratic form Q_ℓ for each prime ℓ. Two quadratic forms Q and $\mathcal{Q}$ are *locally-equivalent* at the prime ℓ if they are equal under the action of an element of $\mathrm{GL}_3(\mathbb{Z}_\ell)$, and we denote this equivalence by $Q \sim_{\mathbb{Z}_\ell} \mathcal{Q}$. The set of equivalence classes which are locally-equivalent at all primes we call the *genus* of Q, and (a set of representatives for) the classes in the genus we denote by $\mathrm{gen}(Q)$. For the ternary case, the genus is then further subdivided into sub-genera called *spinor genera* formed by equivalence under the spin group; see [18, Section 102, pp. 297–305] for a description of this equivalence. We use $\mathrm{spn}(Q)$ to denote (a set of representatives for) the classes of the spinor genus of Q.

For a positive-definite integral n-ary quadratic form Q and $m \in \mathbb{N}_0 := \{n \in \mathbb{Z} : n \geq 0\}$, let $r_Q(m)$ denote the number of representations of m by Q. Denoting $q := e^{2\pi i z}$, the *theta series* associated with Q is

$$\Theta_Q(z) := \sum_{m \in \mathbb{N}_0} r_Q(m) q^m = \sum_{X \in \mathbb{Z}^n} q^{Q(X)}. \tag{2.4}$$

Denoting the number of *automorphs* of Q (i.e., the size of the stabilizer of Q in $\mathrm{GL}_3(\mathbb{Z})$) by ω_Q, we can also define theta series

$$\Theta_{\mathrm{gen}(Q)}(z) := \frac{1}{\sum_{\mathcal{Q} \in \mathrm{gen}(Q)} \omega_{\mathcal{Q}}^{-1}} \sum_{\mathcal{Q} \in \mathrm{gen}(Q)} \frac{\Theta_{\mathcal{Q}}}{\omega_{\mathcal{Q}}}$$

for the genus of Q and

$$\Theta_{\mathrm{spn}(Q)}(z) := \frac{1}{\sum_{\mathcal{Q} \in \mathrm{spn}(Q)} \omega_{\mathcal{Q}}^{-1}} \sum_{\mathcal{Q} \in \mathrm{spn}(Q)} \frac{\Theta_{\mathcal{Q}}}{\omega_{\mathcal{Q}}}$$

for the spinor genus of Q.

The theta series Θ_Q are part of a more general family of theta series, where we may insert a polynomial $P(X)$ in front of $q^{Q(X)}$. We only need these more general theta series in the case that $n = 1$, in which case for an odd (Dirichlet) character $\psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and $t \in \mathbb{N}$ we define the *unary theta function*

$$h_{\psi,t}(z) := \sum_{m \geq 1} \psi(m) m q^{tm^2}. \tag{2.5}$$

2.3. Modular forms.
In this paper, we view the theta series associated with quadratic forms from the perspective of (classical holomorphic) modular forms, which we require a few preliminaries to define.

2.3.1. *Basic definitions.*
Let $\mathbb{H}$ denote the *upper half-plane*, i.e., those $z = x + iy \in \mathbb{C}$ with $x \in \mathbb{R}$ and $y > 0$. The matrices $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (the group of two-by-two integral matrices with determinant 1) act on $\mathbb{H}$ via *fractional linear transformations* $\gamma z := \frac{az+b}{cz+d}$. For

$$j(\gamma, z) := cz + d,$$

a *multiplier system* for a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and *weight* $r \in \mathbb{R}$ is a function $\nu : \Gamma \mapsto \mathbb{C}$ such that for all $\gamma, M \in \Gamma$ (cf. [20, (2a.4)])

$$\nu(M\gamma) j(M\gamma, z)^r = \nu(M) j(M, \gamma z)^r \nu(\gamma) j(\gamma, z)^r.$$

The *slash operator* $|_{r,\nu}$ of weight r and multiplier system ν is then

$$f|_{r,\nu}\gamma(z) := \nu(\gamma)^{-1} j(\gamma, z)^{-r} f(\gamma z).$$

A *(holomorphic) modular form* of weight $r \in \mathbb{R}$ and multiplier system ν for Γ is a function $f : \mathbb{H} \to \mathbb{C}$ satisfying the following criteria:

(1) The function f is holomorphic on $\mathbb{H}$.

(2) For every $\gamma \in \Gamma$, we have

$$f|_{r,\nu}\gamma = f. \tag{2.6}$$

(3) The function f is bounded towards every *cusp* (i.e., those elements of $\Gamma\backslash(\mathbb{Q}\cup\{i\infty\})$). This means that at each cusp ρ of $\Gamma\backslash\mathbb{H}$, the function $f_\rho(z) := f|_{r,\nu}\gamma_\rho(z)$ is bounded as $y \to \infty$, where $\gamma_\rho \in \mathrm{SL}_2(\mathbb{Z})$ sends $i\infty$ to ρ.

Furthermore, if f vanishes at every cusp (i.e., the limit $\lim_{z\to i\infty} f_\rho(z) = 0$ for all cusps ρ), then we call f a *cusp form*.

2.3.2. *Half-integral weight forms.*

We are particularly interested in the case where $r = k+1/2$ with $k \in \mathbb{N}_0$ and

$$\Gamma = \Gamma_0(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : M \mid c \right\}$$

for some $M \in \mathbb{N}$ divisible by 4. The multiplier system is given such that there exists a character (also commonly called *Nebentypus*) $\chi : \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$ for which

$$\frac{f(\gamma z)}{f(z)} = \chi(d) \frac{\Theta^{2k+1}(\gamma z)}{\Theta^{2k+1}(z)},$$

where $\Theta(z) := \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 z}$ is the classical Jacobi theta function. The space of such modular forms we call the space of weight $k+1/2$ modular forms of level $4N$ and character χ and denote the space by $M_{k+1/2}(4N,\chi)$. The subspace of cusp forms we denote by $S_{k+1/2}(4N,\chi)$. Whenever the character is trivial, we omit it from the notation. By (2.6) with $\gamma = T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we see that for $f \in M_{k+1/2}(4N,\chi)$, we have $f(z+1) = f(z)$, and hence f has a Fourier expansion $(c_f(n) \in \mathbb{C})$

$$f(z) = \sum_{n\geq 0} c_f(n) e^{2\pi i n z}. \tag{2.7}$$

The restriction $n \geq 0$ follows from the fact that f is bounded as $z \to i\infty$. One commonly sets $q := e^{2\pi i z}$ and associates the above expansion with the corresponding formal power series, using them interchangeably unless explicit analytic properties of the function f are required.

2.3.3. *Kohnen's plus space and natural operators.*

We say that a form $f \in M_{k+1/2}(4N,\chi)$ is in *Kohnen's plus space* [15] if $c_f(n) = 0$ for all $n \in \mathbb{N}_0$ with $(-1)^k n \equiv 2, 3 \pmod 4$. The subspace of forms in Kohnen's plus space is written $M^+_{k+1/2}(N,\chi)$ and the subspace of cusp forms is denoted by $S^+_{k+1/2}(N,\chi)$. For every $\ell \nmid N$, there is a natural family of Hecke operators T_{ℓ^2}, whose action on the Fourier expansion (2.7) of $f \in M^+_{k+1/2}(N,\chi)$ is given by

$$f|T_{\ell^2}(z) := \sum_{n\geq 1} \left(c_f(\ell^2 n) + \chi(\ell) \left(\frac{(-1)^k n}{\ell} \right) \ell^{k-1} c_f(n) + \ell^{2k-1} c_f\left(\frac{n}{\ell^2}\right) \right) q^n.$$

The operators T_{ℓ^2} preserve the space $S^+_{k+1/2}(N,\chi)$. We also make use of the operator U_{ℓ^2} given by

$$f\big|U_{\ell^2}(z) := \sum_{n=1}^{\infty} c_f\left(n\ell^2\right) q^n.$$

It is well-known (cf. Section 3.2 in [19]) that if $f \in S_{k+1/2}(4N,\chi)$, then

$$f\big|U_{\ell^2} \in S_{k+\frac{1}{2}}\left(4N\ell^2, \left(\frac{4\ell^2}{\cdot}\right)\chi\right). \tag{2.8}$$

Moreover, for ℓ_1, ℓ_2 relatively prime with $(\ell_1, N) = 1$, the operators $T_{\ell_1^2}$ and $U_{\ell_2^2}$ commute. Thus if f is a Hecke eigenform, then $f|U_{\ell^2}$ is also a Hecke eigenform with the same eigenvalues.

2.3.4. *Theta series and modular forms.*

Siegel [24] (see also [23, Proposition 2.1]) proved that if Q is an $(2k+1)$-ary quadratic form with Gram matrix A, then $\Theta_Q \in M_{k+1/2}(N, \chi)$ for $N \in \mathbb{N}$ such that NA^{-1} has integral coefficients and moreover

$$\Theta_Q - \Theta_{\text{gen}(Q)} \in S_{k+1/2}(N, \chi). \tag{2.9}$$

Moreover, by [19, Theorem 1.44 and Proposition 3.7 (1)] or [23, Proposition 2.1], the unary theta functions $h_{t,\psi}$ defined in (2.5) are elements of $S_{3/2}(4tN_\psi^2, \chi)$ for $\chi = \psi\chi_{-4}\left(\frac{4t}{\cdot}\right)$ and where N_ψ denotes the conductor of ψ. The subspace of $S_{3/2}(N, \chi)$ spanned by unary theta functions we denote by $U_{3/2}(N, \chi)$ and its orthogonal complement in $S_{3/2}(N, \chi)$ we denote by $U_{3/2}^\perp(N, \chi)$, where orthogonality is taken with respect to the Petersson inner product

$$\langle f, g \rangle := \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4N)]} \int_{\Gamma_0(4N)\backslash\mathbb{H}} f(z)\overline{g(z)} y^{3/2} \frac{dxdy}{y^2}.$$

Here $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4N)]$ is the index of $\Gamma_0(4N)$ in $\mathrm{SL}_2(\mathbb{Z})$. We use the fact that orthogonality from unary theta functions is preserved by U_{ℓ^2}; this is well-known to the experts but we provide a proof for the convenience of the reader.

Lemma 2.1. *If $f \in U_{3/2}^\perp(N, \chi)$ for some $N \in \mathbb{N}$ and character χ, then*

$$f|U_{\ell^2} \in U_{\frac{3}{2}}^\perp\left(4N\ell^2, \left(\frac{4\ell^2}{\cdot}\right)\chi\right).$$

Proof. By (2.8), $f|U_{\ell^2}$ is a cusp form of weight $3/2$, level $4N\ell^2$, and character $\chi' := \left(\frac{4\ell^2}{\cdot}\right)\chi$. It remains to show that the projection of $f|U_{\ell^2}$ to the subspace of unary theta functions is trivial. The basic argument is to show that if this projection is non-zero, then the coefficients of $f|U_{\ell^2}$ grow too fast.

We first decompose

$$f|U_{\ell^2} = f_0 + f_1 \tag{2.10}$$

with $f_0 \in U_{3/2}(4N\ell^2, \chi')$ and $f_1 \in U_{3/2}^\perp(4N\ell^2, \chi')$. However, for $f_1 \in U_{3/2}^\perp(4N\ell^2, \chi')$, Duke [5] has shown that for every $\varepsilon > 0$, we have

$$\left|c_{f_1}(n)\right| \ll_{f_1,\varepsilon} n^{\frac{13}{28}+\varepsilon}. \tag{2.11}$$

Suppose for contradiction that $c_{f_0}(n_0) \neq 0$ for some $n_0 \in \mathbb{N}$. Since

$$f_0 = \sum_{\psi, t} \alpha_{\psi,t} h_{\psi,t},$$

where the sum runs over ψ and t for which $h_{\psi,t}$ belongs to $S_{3/2}(4N\ell^2, \chi')$ (in particular, the conductor of ψ is a divisor of $4N\ell^2$ and $t \mid 4N\ell^2$). By (2.5), we conclude that $n_0 = t_0 m_0^2$ for some $t_0, m_0 \in \mathbb{N}$ with t_0 squarefree and

$$c_{f_0}(n_0) = \sum_{\psi} \sum_{\substack{\frac{t}{t_0} \in \mathbb{Z}^2 \\ \frac{t}{t_0} \mid m_0^2}} \alpha_{\psi,t} c_{h_{\psi,t}}(t_0 m_0^2) = \sum_{\psi} \sum_{\substack{\frac{t}{t_0} \in \mathbb{Z}^2 \\ \frac{t}{t_0} \mid m_0^2}} \alpha_{\psi,t} \psi\left(m_0\sqrt{\frac{t_0}{t}}\right) m_0\sqrt{\frac{t_0}{t}}. \tag{2.12}$$

Note that for every $m \equiv 1 \pmod{4N\ell^2}$, we have $t/t_0 \mid m_0^2 m^2$ if and only if $t/t_0 \mid m_0^2$ (because $t \mid 4N\ell^2$) and

$$\psi\left(m_0 m \sqrt{\frac{t_0}{t}}\right) = \psi\left(m_0\sqrt{\frac{t_0}{t}}\right).$$

Hence (2.5) and (2.12) imply that for every $m \equiv 1 \pmod{4N\ell^2}$, we have

$$c_{f_0}(n_0 m^2) = \sum_\psi \sum_{\substack{\frac{t}{t_0} \in \mathbb{Z}^2 \\ \frac{t}{t_0} \mid m_0^2 m^2}} \alpha_{\psi,t} \psi\left(m_0 m \sqrt{\frac{t_0}{t}}\right) m_0 m \sqrt{\frac{t_0}{t}}$$

$$= m \sum_\psi \sum_{\substack{\frac{t}{t_0} \in \mathbb{Z}^2 \\ \frac{t}{t_0} \mid m_0^2}} \alpha_{\psi,t} \psi\left(m_0 \sqrt{\frac{t_0}{t}}\right) m_0 \sqrt{\frac{t_0}{t}} = m c_{f_0}(n_0).$$

Combining this with (2.10) and (2.11), for $m \equiv 1 \pmod{4N\ell^2}$, we obtain

$$c_f\left(n_0 m^2 \ell^2\right) = c_{f|U_{\ell^2}}\left(n_0 m^2\right) = m c_{f_0}(n_0) + O\left(m^{\frac{13}{14}+\varepsilon}\right).$$

Since $f \in U_{3/2}^\perp(4N, \chi)$, for m sufficiently large this contradicts Duke's bound (2.11). This contradiction implies that $c_{f_0}(n_0) = 0$ for all n_0, so that $f_0 = 0$, yielding the claim. $\square$

3. PRECISE STATEMENT OF CONJECTURE 1.1

Let B_p over $\mathbb{Q}$ be the unique quaternion algebra which ramifies at exactly the primes p and ∞ and let $\mathscr{O}$ be one of its maximal orders. The algorithm by Chevyrev and Galbraith [3] constructs an elliptic curve E over $\mathbb{F}_{p^2}$, such that the endomorphism ring is isomorphic to the maximal order, i.e. $\text{End}(E) \cong \mathscr{O}$. They proved that their algorithm halts unless there exists another non-conjugate maximal order $\mathscr{O}'$ for which

$$a_{\mathscr{O}'^T}(n) \geq a_{\mathscr{O}^T}(n) \tag{3.1}$$

for every $n \in \mathbb{N}_0$, where $a_{\mathscr{O}^T}(n)$ is defined in (2.1). Following [3], we thus say that $\mathscr{O}'^T$ *optimally dominates* $\mathscr{O}^T$ if (3.1) holds for all $n \in \mathbb{N}_0$. Chevyrev and Galbraith then conjectured in [3, Conjecture 1] that no maximal order may optimally dominate another.

Conjecture 3.1 (Chevyrev–Galbraith [3]). *Let $\mathscr{O}$ and $\mathscr{O}'$ be maximal orders of B_p. If $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$, then $\mathscr{O}$ and $\mathscr{O}'$ are of the same type.*

Remarks 3.2.
(1) Conjecture 3.1 is equivalent to Conjecture 1.1 because all isomorphisms of orders come from conjugation.
(2) Paralleling the definition of type for maximal orders, we say that $\mathscr{O}'^T$ and $\mathscr{O}^T$ have the same type if there is a non-zero element $c \in B_p$ such that $c\mathscr{O}^T c^{-1} = \mathscr{O}'^T$, and we write $\mathscr{O}^T \sim \mathscr{O}'^T$. By Lemma 4 in [3], we know that $\mathscr{O}^T \sim \mathscr{O}'^T$ if and only if $\mathscr{O} \sim \mathscr{O}'$.
(3) There is a second conjecture of Chevyrev and Galbraith about the occurrence of the smallest n_0 for which both $a_{\mathscr{O}'^T}(n_1) \geq a_{\mathscr{O}^T}(n_1)$ and $a_{\mathscr{O}'^T}(n_2) < a_{\mathscr{O}^T}(n_2)$ occur for some $n_1, n_2 < n_0$. They conjecture in particular that $n_0 = O(p)$ and determine the running time of their algorithm under this assumption. In our context, this n_0 corresponds to the first sign change. Although there is some discussion in [16] about the size of n_0, there are a number of inexplicit constants which would need to be worked out to determine the size of n_0 implied by

their theorem, and it is not expected that their proof would yield a bound anywhere close to the conjectured $O(p)$. The first author is trying to determine (and improve upon) an explicit bound for n_0 in his Masters thesis.

(4) By Lemma 11 in [3], we have $a_{\mathscr{O}'^T}(n) \geq a_{\mathscr{O}^T}(n)$ for all n if and only if $r_{\mathscr{O}'^T}(n) \geq r_{\mathscr{O}^T}(n)$ for all n.

4. PROOF OF THEOREM 1.2

Recall that for a maximal order $\mathscr{O}$ of B_p, the associated reduced norm Nr on $\mathscr{O}^T$ is a positive-definite integral ternary quadratic form $Q_{\mathscr{O}^T}$. Gross [7, (12.8)] constructed the associated theta series

$$\vartheta_{\mathscr{O}^T} := \Theta_{Q_{\mathscr{O}^T}}, \tag{4.1}$$

which is an element of Kohnen's plus space $M_{3/2}^+(p)$. The following lemma plays a key role in the proof of Conjecture 3.1.

Lemma 4.1. *If $\mathscr{O}$ and $\mathscr{O}'$ are two maximal orders in the quaternion algebra B_p, then*

$$\vartheta_{\mathscr{O}^T} - \vartheta_{\mathscr{O}'^T} \in S_{\frac{3}{2}}^+(p).$$

Furthermore, $\vartheta_{\mathscr{O}^T} - \vartheta_{\mathscr{O}'^T} \in U_{3/2}^\perp(4p)$.

Proof. As noted by Gross (see [7, p. 130]), for all primes ℓ the maximal orders of B_p are all locally conjugate over $\mathbb{Z}_\ell$, from which we conclude that for all primes ℓ

$$Q_{\mathscr{O}^T} \sim_{\mathbb{Z}_\ell} Q_{\mathscr{O}'^T}.$$

Thus $Q_{\mathscr{O}^T}$ and $Q_{\mathscr{O}'^T}$ are in the same genus by definition. Hence, by (2.9),

$$\vartheta_{\mathscr{O}^T} - \vartheta_{\mathscr{O}'^T} = \Theta_{Q_{\mathscr{O}^T}} - \Theta_{\text{gen}(Q_{\mathscr{O}^T})} + \Theta_{\text{gen}(Q_{\mathscr{O}^T})} - \Theta_{Q_{\mathscr{O}'^T}}$$

$$= \Theta_{Q_{\mathscr{O}^T}} - \Theta_{\text{gen}(Q_{\mathscr{O}^T})} + \Theta_{\text{gen}(Q_{\mathscr{O}'^T})} - \Theta_{Q_{\mathscr{O}'^T}} = \left(\Theta_{Q_{\mathscr{O}^T}} - \Theta_{\text{gen}(Q_{\mathscr{O}^T})} \right) + \left(\Theta_{\text{gen}(Q_{\mathscr{O}'^T})} - \Theta_{Q_{\mathscr{O}'^T}} \right)$$

is a cusp form. Moreover, it is contained in Kohnen's plus space of level p by construction.

It remains to show that $\vartheta_{\mathscr{O}^T} - \vartheta_{\mathscr{O}'^T}$ is orthogonal to unary theta functions. However, since p is squarefree and odd, Kohnen has proven in [15, Theorem 2] that $S_{3/2}^+(p)$ is Hecke-isomorphic to $S_2(p)$ under a linear combination of the Shimura lifts defined in [23] (and hence has a basis of simultaneous Hecke eigenforms). Since every element of $S_{3/2}^+(p)$ may be written as a linear combination of Hecke eigenforms, it suffices to show that all of the Hecke eigenforms are orthogonal to unary theta functions.

Next recall that the Hecke operators are Hermitian with respect to the Petersson inner product (see [15, Section 3]). Denoting the eigenvalue of $h_{t,\psi}$ under the Hecke operator T_{ℓ^2} by λ_ℓ and the eigenvalue of an eigenform f in $S_{3/2}^+(p)$ by $\lambda_{f,\ell}$, we see that

$$\lambda_\ell \langle h_{t,\psi}, f \rangle = \langle h_{t,\psi} | T_{\ell^2}, f \rangle = \langle h_{t,\psi}, f | T_{\ell^2} \rangle = \overline{\lambda_{f,\ell}} \langle h_{t,\psi}, f \rangle. \tag{4.2}$$

We conclude that if $h_{t,\psi}$ and f are not orthogonal, then $\lambda_\ell = \lambda_{f,\ell}$ for all ℓ, where we use the fact that the eigenvalues must be real because the Hecke operator is Hermitian. However, the elements of $U_{3/2}(4p) \subset S_{3/2}(4p)$ have the same eigenvalues as weight 2 Eisenstein series and $\lambda_{f,\ell}$ is the eigenvalue for a weight 2 cusp form by Kohnen's Hecke-isomorphism. The eigenvalues cannot always coincide and therefore $h_{t,\psi}$ and f are orthogonal. $\qquad \square$

The strategy of our proof is to study the sign changes of the Fourier coefficients of the differences $\vartheta_{\mathscr{O}'^T} - \vartheta_{\mathscr{O}^T}$. For this, we require [16, Theorem 1] of Kohnen, Lau, and Wu.

Theorem 4.2 (Kohnen, Lau, and Wu). *Let $N \geq 4$ an integer divisible by 4 and χ be a Dirichlet character modulo N. If $g \in U_{3/2}^{\perp}(N, \chi)$, then for each positive squarefree integer t for which $c_g(t) \neq 0$ and the sequence $\{c_g(tn^2)\}_{n \in \mathbb{N}}$ is real, the sequence $\{c_g(tn^2)\}_{n \in \mathbb{N}}$ contains infinitely many sign changes.*

Remarks 4.3.

(1) Kohnen, Lau and Wu actually gave much stronger results in their paper [16] but this sim-plified version is strong enough for our use.

(2) One can use an argument involving the sign changes to directly show that $\vartheta_{\mathscr{O}'^T} - \vartheta_{\mathscr{O}^T} \in U_{3/2}^{\perp}(4p)$ if $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$. To illustrate the usage of Theorem 4.2, we briefly sketch the proof; further details may be found in the first author's upcoming Masters thesis. One sees directly from (2.5) that the coefficients of unary theta functions alternate in sign. Using a bound of Duke [5] for the coefficients of elements of $U_{3/2}^{\perp}(4p)$, the coefficients of the difference $\vartheta_{\mathscr{O}^T} - \vartheta_{\mathscr{O}'^T}$ are dominated by the coefficients of the contribution from unary theta functions and hence alternate unless the contribution from $U_{3/2}^{\perp}(4p)$ is trivial. However, slightly abusing notation by abbreviating

$$r_{\mathscr{O}^T}(n) := r_{Q_{\mathscr{O}^T}}(n),$$

we may split the elements of $h \in \mathscr{O}^T$ by $\mathfrak{g}(h) = f$ (see (2.2)) to obtain

$$r_{\mathscr{O}^T}(n) = \sum_{\substack{f \in \mathbb{Z} \\ f^2 \mid n}} a_{\mathscr{O}^T}\left(\frac{n}{f^2}\right). \tag{4.3}$$

Hence if $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$, then $r_{\mathscr{O}'^T}(n) \geq r_{\mathscr{O}^T}(n)$, and we conclude that the contribution from unary theta functions is trivial.

The next proposition is a key step in the proof of Theorem 1.2.

Proposition 4.4. *Let $\mathscr{O}$ and $\mathscr{O}'$ be maximal orders of B_p. If $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$, then $\vartheta_{\mathscr{O}'^T}(z) = \vartheta_{\mathscr{O}^T}(z)$.*

Write

$$g(z) := \vartheta_{\mathscr{O}'^T}(z) - \vartheta_{\mathscr{O}^T}(z).$$

By Lemma 4.1, $g \in U_{3/2}^{\perp}(4p)$, and we have $c_g(n) \geq 0$ for all $n \in \mathbb{N}$ by assumption. Hence to conclude Proposition 4.4, it suffices to prove the following slightly stronger proposition.

Proposition 4.5. *If $g \in U_{3/2}^{\perp}(4N, \chi)$ for some $N \in \mathbb{N}$ and character χ and $c_g(n) \geq 0$ for all n, then $g = 0$.*

Proof. We show the claim by proving that $c_g(n) = 0$ for all $n \in \mathbb{N}$. To give the idea of the argument suppose that there exists a squarefree $t \in \mathbb{N}$ such that $c_g(t) \neq 0$, then by Theorem 4.2, the sequence $\{c_g(tm^2)\}_{m \in \mathbb{N}}$ has sign changes. But then this contradicts the fact that $c_g(n) \geq 0$ for all positive n. Hence we have $c_g(n) = 0$ for all squarefree $n \in \mathbb{N}$.

We proceed similarly to show that $c_g(n) = 0$ for $n = tm_0^2$ with t squarefree and

$$m_0 = \prod_{j=1}^{J} \ell_j \in \mathbb{N},$$

where ℓ_j are (not necessarily distinct) primes. Suppose for contradiction that $c_g(tm_0^2) \neq 0$. Denoting

$$U_{m_0^2} := \prod_{j=1}^{J} U_{\ell_j^2}$$

and repeatedly using Lemma 2.1, there exists a character χ' for which

$$g|U_{m_0^2} \in U_{\frac{3}{2}}^\perp \left(4pm_0^2, \chi'\right).$$

Thus we may apply Theorem 4.2 to $g|U_{m_0^2}$ to conclude that $\{c_{g|U_{m_0^2}}(tm^2) : m \in \mathbb{Z}\}$ has infinitely many sign changes. However, since

$$c_{g|U_{m_0^2}}\left(tm^2\right) = c_g\left(tm_0^2m^2\right) \geq 0,$$

we obtain a contradiction. Thus $c_g(tm_0^2) = 0$, as desired. $\qquad\square$

We have now established most of the ingredients necessary to prove Theorem 1.2. The main remaining piece is an equivalence between theta series $\vartheta_{\mathscr{O}^T}$ and $\vartheta_{\mathscr{O}'^T}$ agreeing and $\mathscr{O}^T$ and $\mathscr{O}'^T$ having the same type.

Lemma 4.6. *Let $\mathscr{O}$ and $\mathscr{O}'$ be maximal orders of B_p. Then the following statements are equivalent:*

(a) $\mathscr{O}^T \sim \mathscr{O}'^T$;
(b) $\vartheta_{\mathscr{O}^T} = \vartheta_{\mathscr{O}'^T}$;
(c) $Q_{\mathscr{O}^T} \sim_\mathbb{Z} Q_{\mathscr{O}'^T}$.

Proof. (a)⇒(b): Suppose that there is a non-zero element $c \in B_p$ such that $c\mathscr{O}^Tc^{-1} = \mathscr{O}'^T$. Since

$$\mathrm{Nr}\left(cXc^{-1}\right) = \mathrm{Nr}(X)$$

for all $X \in B_p$ and non-zero $c \in B_p$, we conclude (b) by the definition (4.1) of the theta series.

(b)⇒(c): If $\vartheta_{\mathscr{O}^T}(z) = \vartheta_{\mathscr{O}'^T}(z)$, then all the coefficients of their Fourier expansions are the same. By Schiemann [21], we have $Q_1 \sim_\mathbb{Z} Q_2$ (actually, Schiemann gave a much stronger result; roughly speaking, it only requires the first few coefficients of the Fourier expansions to be the same).

(c)⇒(a): This is shown in [8, Section 4] by defining the associated ternary quadratic form on [8, p. 1473] and then showing that the map forms a bijection between orbits under $\mathrm{GL}_3(\mathbb{Z})$ and isomorphism classes of quaternion rings over $\mathbb{Z}$ in [8, Proposition 4.1].

$\qquad\square$

We are finally ready to prove our main theorem, Theorem 1.2, which we state again for the convenience of the reader.

Theorem 4.7. *Let $\mathscr{O}$ and $\mathscr{O}'$ be maximal orders of B_p. If $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$, then $\mathscr{O}$ and $\mathscr{O}'$ are of the same type. Furthermore, the algorithm of Chevyrev and Galbraith halts.*

Proof of Theorem 1.2. By Proposition 4.4, if $\mathscr{O}'^T$ optimally dominates $\mathscr{O}^T$, then $\vartheta_{\mathscr{O}^T} = \vartheta_{\mathscr{O}'^T}$. Hence by the equivalence of (b) and (a) in Lemma 4.6, we obtain that $\mathscr{O}^T \sim \mathscr{O}'^T$. Finally, by Lemma 4 of [3], we conclude that $\mathscr{O}$ and $\mathscr{O}'$ have the same type. $\qquad\square$

REFERENCES

[1] S. Arias-de-Reyna, I. Inam, and G. Wiese, *On conjectures of Sato–Tate and Bruinier–Kohnen*, Ramanujan J. **36** (2015), 455–481.

[2] J. H. Bruinier and W. Kohnen, *Sign changes of coefficients of half integral weight modular forms*, In: Modular forms on Schiermonnikoong (eds. B. Edixhoven et. al.), 57–66, Cambridge Univ. Press, 2008.

[3] I. Chevyrev and S. D. Galbraith, *Constructing supersingular elliptic curves with a given endomorphism ring*, LMS J. Comput. Math. **17** (2014), 71–91.

[4] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörpen*, Abh. Math. Sem. Hambg. **14** (1941), 197–272.

[5] W. Duke, *Hyperbolic distribution problems and half integral weight Maass forms*, Invent. Math. **92** (1988), 73–90.

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

[7] B. H. 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.

[8] B. H. Gross and Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2009), 1468–1478.

[9] J. Hanke, *Some recent results about (ternary) quadratic forms*, CRM Proc. Lect. Notes **36** (2004), 147–164.

[10] I. Inam and G. Wiese, *Equidistribution of signs for modular eigenforms of half integral weight*, Archiv der Math. **101** (2013), 331–339.

[11] I. Inam and G. Wiese, *A short note on the Bruinier–Kohnen sign equidistribution conjecture and Halász' theorem*, Int. J. Number Theory **12** (2016), 357–360.

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

[13] D. Jetchev and B. Kane, *Equidistribution of Heegner points and ternary quadratic forms*, Math. Ann. **350** (2011), 501–532.

[14] M. Knopp, W. Kohnen, and W. Pribitkin, *On the signs of Fourier coefficients of cusp forms*, Ramanujan J. **7** (2003), 269–277.

[15] W. Kohnen, *Newforms of half-integral weight*, J. reine angew. Math. **333** (1982), 32–72.

[16] W. Kohnen, Y.-K. Lau, and J. Wu, *Fourier coefficients of cusp forms of half-integral weight*, Math. Z. **273** (2013), 29–41.

[17] W. Kohnen and J. Sengupta, *On the first sign change of Hecke eigenvalues of newforms*, Math. Z. **254** (2006), 173–184.

[18] O. T. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, 2000, reprint of 1973 edition.

[19] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, Conference Board of the Mathematical Sciences **102**, Amer. Math. Soc., Providence, RI (2004).

[20] H. Petersson, *Konstruktion der Modulformen und der zu gewissen Grenzkreisgruppen gehörigen automorphen Formen von positiver reeller Dimension und die vollständige Bestimmung ihrer Fourierkoeffzienten*, S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl. (1950), 415–474.

[21] A. Schiemann, *Ternary positive definite quadratic forms are determined by their theta series*, Math. Ann. **308** (1997), 507–517.

[22] R. Schulze-Pillot, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. **75** (1984), no. 2, 283–299.

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

[24] C. L. Siegel, *Uber die analytische theorie der quadratisches Formen*, Ann. of Math. **36** (1935), 527–609.

[25] C. L. Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. K., II (1969), 87–102.

[26] M.-F. Vigneras, *Arithmetique des algebres de quaternions*, Lect. Notes in Math. **800** (1980).

MATHEMATICS DEPARTMENT, UNIVERSITY OF HONG KONG, POKFULAM, HONG KONG
E-mail address: mrkcfung@hku.hk

MATHEMATICS DEPARTMENT, UNIVERSITY OF HONG KONG, POKFULAM, HONG KONG
E-mail address: bkane@maths.hku.hk