IMRN International Mathematics Research Notices
Volume 2006, Article ID 53864, Pages 1–19

Evil Primes and Superspecial Moduli

Eyal Z. Goren and Kristin E. Lauter

For a quartic non-biquadratic CM field K, we say that a rational prime p is *evil for* K if at least one of the principally polarized abelian varieties with CM by K reduces modulo a prime ideal $\mathfrak{p}|p$ to a product of supersingular elliptic curves with the product polarization. We showed that for fixed K, such primes are bounded by a quantity related to the discriminant of K. We show that evil primes are ubiquitous in the sense that for any rational prime p, there are an infinite number of such CM fields K for which p is evil. (Assuming a standard conjecture, the result holds for a finite set of primes simultaneously.) The proof consists of two parts: (1) showing the surjectivity of the principally polarized abelian varieties with CM by K, for K satisfying some conditions, onto the superspecial points of the reduction modulo p of the Hilbert modular variety associated to the intermediate real quadratic field of K, and (2) showing the surjectivity of the superspecial points of the reduction modulo p of the Hilbert modular variety associated to a real quadratic field with large enough discriminant onto the superspecial points on the reduction modulo p of the Siegel moduli space parameterizing abelian surfaces with principal polarization.

1 Introduction

Given a quartic CM field K, one can study the values at CM points associated to K of Siegel modular functions, specifically of the functions sometimes referred to as the absolute Igusa invariants; see [11] and the references therein. Their values are algebraic numbers

Received 1 March 2006; Revised 31 May 2006; Accepted 29 June 2006
Communicated by James W. Cogdell

which generate unramified abelian extensions of the reflex field of K. Assume that K is a primitive CM field, that is, does not contain a proper subfield which is CM; since K is quartic, this is equivalent to K not being biquadratic. In this case, rational primes appearing in the denominators of the coefficients of the minimal polynomials of such values correspond to primes where at least one of the principally polarized abelian varieties with CM by K reduces to a product of supersingular elliptic curves with the product polarization. We call such primes *evil primes for* K. The occurrence of such primes is an issue in the numerical calculation of the minimal polynomials, a computational problem of interest for generating genus 2 curves for cryptographic applications. The presence of evil primes also appears as an obstruction for the class invariants defined in [4] to be units (see also [11]), and so is connected to problems in algebraic number theory motivated by Stark's conjectures. Evil primes were studied in [11], though without using this terminology, where we showed that for fixed K, such primes are bounded by a quantity related to the discriminant of the field K. In this paper, we prove various results that indicate that evil primes are a very common phenomenon, in particular we prove that every prime is evil for an infinite number of primitive quartic CM fields.

The paper contains two main theorems, Theorems 2.1 and 2.4. Let L be a totally real-number field of strict class number one (we allow arbitrary degree over $\mathbb{Q}$). In Theorem 2.1 we prove that there is a choice of a CM field K such that every principally polarized superspecial abelian variety with real multiplication by L over $\overline{\mathbb{F}}_p$ (corresponding to a superspecial point on the modulo p reduction of the Hilbert modular variety associated to L) arises as the reduction of a principally polarized abelian variety with CM by K. Necessary and sufficient conditions on the field K are $K^+ = L$ (where K^+ denotes the fixed field under complex conjugation), p is unramified in K and satisfies decomposition conditions specified in Theorem 2.1, and the norm of the relative discriminant $\mathrm{Norm}(d_{K/L})$ is large enough. It then follows that there are infinitely many such CM fields K.

Consider now the case where L is a real quadratic field. Since we can easily manufacture a superspecial point on the Hilbert modular variety associated to L corresponding to a product of supersingular elliptic curves with the product polarization, we conclude that for every real quadratic field L in which p is unramified there are infinitely many quartic primitive CM fields K, $K^+ = L$, for which p is an evil prime. Let S be a finite set of rational primes. If one is willing to accept that there is always a real quadratic field L of strict class number one in which every prime of S is unramified (certainly a widely believed conjecture), then Theorem 2.1 has the following conditional corollary: given a finite set of rational primes S, there are infinitely many primitive quartic CM fields for which all primes in S are evil for each field. In this sense evil primes are ubiquitous. Theorem 2.4 will allow us to draw stronger conclusions.

Theorem 2.1 generalizes to arbitrary dimension recent work of Elkies, Ono, and Yang [7], where they study the elliptic curve case corresponding to an imaginary quadratic field K. In [7, Theorem 1.2], they prove that for an odd prime p and an imaginary quadratic field K in which p is inert, (any power of) the supersingular polynomial modulo p divides the Hilbert class polynomial of K modulo p if the discriminant of K is large enough. In other words, every supersingular elliptic curve modulo p is the reduction of an elliptic curve with CM by K for any K satisfying the above conditions. Whereas [7, Theorem 1.2] uses the results of Duke [5], Iwaniec [15], and Siegel to study the asymptotic behavior of a certain theta function, Theorem 2.1 uses the work of Cogdell, Piatetski-Shapiro and Sarnak [3] which generalizes Duke's work to totally real-number fields.

We prove Theorem 2.1 in three steps. Let R be the centralizer of $\mathcal{O}_L$ in the endomorphism ring of A, a principally polarized abelian variety with real multiplication corresponding to a superspecial point on the reduction modulo p of the Hilbert modular variety associated to L. Following [19], we call R a superspecial order; it is an order in the quaternion algebra $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$, where $B_{p,\infty}$ is the rational quaternion algebra ramified at p and ∞ alone. First we establish a one-to-one correspondence between $\mathcal{O}_L$-embeddings of $\mathcal{O}_K$ into the order R up to equivalence and CM lifts of A to principally polarized abelian varieties with CM by K along the lines of what was shown in [11]. Next we show that to give an $\mathcal{O}_L$-embedding of $\mathcal{O}_K$ into the endomorphism ring of A, it is enough that a totally positive generator of the relative discriminant of K/L be represented by the norm form on a certain lattice associated to R. Next we use the theorem on integral representability by positive definite integral ternary quadratic forms over totally real fields [3] to reduce the computation to checking local representability. Checking local representability uses the fact that all superspecial orders in the quaternion algebra $B_{p,L}$ are locally conjugate.

Theorem 2.4 concerns the relationship between the superspecial points on the Hilbert and Siegel moduli spaces. We show that the superspecial points on the modulo p reduction of the Hilbert modular variety associated to a real quadratic field L surject onto the superspecial points on the modulo p reduction of the Siegel moduli variety, if the discriminant of L is large enough. To prove this theorem we need to show how to embed $\mathcal{O}_L$ into the endomorphism ring of A, for A a principally polarized superspecial abelian variety, in a way which is compatible with the polarization. We accomplish this using the description of all possible polarizations given in [14] and the fact that the Tate modules (resp., Dieudonné modules) of any two principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$ of the same dimension are isomorphic.

Combining Theorems 2.4 with 2.1 we get a stronger result on evil primes. Let p be a rational prime unramified in L, a real quadratic field of strict class number one. Then

if the discriminant of L is large enough, any principally polarized superspecial abelian surface, in particular *any* product of supersingular elliptic curves with principal polarization, arises as the reduction of a principally polarized abelian surface with CM by a field K, where K satisfies the conditions of Theorem 2.1 mentioned above. Assuming the same conjecture on real quadratic fields as above, such a conclusion holds also for a finite set S of rational primes simultaneously.

We remark that Theorems 2.1 and 2.4 are also of interest for reasons quite different from those mentioned so far. In [8, 19], one finds an approach to Siegel and Hilbert modular forms through the superspecial locus in the corresponding moduli spaces. For a different motivation see [7]. For yet another motivation see [20], where a result like Theorem 2.1 for the case of quadratic imaginary fields is assumed as part of an algorithm to compute elliptic modular forms. A similar algorithm for Hilbert modular forms would use the results of [19] and make use of Theorem 2.1.

The paper is organized as follows. Section 2 contains precise statements of the results of the paper. Section 3 contains the proof of Theorem 2.1 and Section 4 contains the proof of Theorem 2.4.

2 Statement of results

All number fields are considered as subfields of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Given a CM field K of degree $2g$ over $\mathbb{Q}$, denote by $\mathcal{CM}(K)$ the set of isomorphism classes over $\overline{\mathbb{Q}}$ of abelian varieties (A, λ, ι), where A is an abelian variety of dimension g, $\lambda : A \to A^\vee$ is a principal polarization, $\iota : \mathcal{O}_K \to \mathrm{End}(A)$ is a ring embedding and the Rosati involution $x \mapsto x^\lambda$ induces complex conjugation on $\mathcal{O}_K$. We denote by K^+ the maximal totally real subfield of K. If K^+ has strict class number one then the discriminant ideal $\mathfrak{d}_{K/K^+}$ is generated by a totally negative element of K^+, uniquely determined up to $\mathcal{O}_{K^+}^{\times,2}$ (see Lemma 3.1). We will denote any such generator as $-m$:

$$(m) = \mathfrak{d}_{K/K^+}, \quad m \text{ totally positive.} \tag{2.1}$$

Theorem 2.1. Let L be a totally real field of degree g and strict class number one. Let p be a rational prime, unramified in L, and P a prime of $\overline{\mathbb{Q}}$ above p. Let $\mathcal{SS}(L)$ denote the superspecial points on the reduction modulo P of the Hilbert modular variety $\mathcal{M}_L$ associated to L that parameterizes abelian varieties with real multiplication by $\mathcal{O}_L$ equipped with an $\mathcal{O}_L$-linear principal polarization. There exists a constant $N = N(p, L)$ such that if K is a CM field satisfying

(1) $K^+ = L$;
(2) for every prime $\mathfrak{P}$ of K over p with $\mathfrak{p} = \mathfrak{P} \cap L$,

(a) if $p \neq 2$, then $f(\mathfrak{P}/\mathfrak{p}) + f(\mathfrak{p}/p)$ is odd;
(b) if $p = 2$, then $3m$ is a quadratic residue modulo $\mathfrak{p}^3$ for all $\mathfrak{p} \mid p$;

(3) the norm from L to $\mathbb{Q}$ of the discriminant of K over L is greater than N in absolute value;

then $\mathcal{SS}(L)$ is contained in the image of $\mathcal{CM}(K)$ under the natural reduction map

$$\mathcal{CM}(K) \longrightarrow \mathcal{M}_L \longrightarrow \mathcal{M}_L \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p, \tag{2.2}$$

that is, every superspecial abelian variety with RM by $\mathcal{O}_L$ admits a lift to a characteristic zero abelian variety with CM by $\mathcal{O}_K$. □

Definition 2.2. Let K be a quartic primitive CM field. A rational prime p is *evil* (for K) if for some prime P of $\overline{\mathbb{Q}}$ over p, there is an element of $\mathcal{CM}(K)$ whose reduction modulo P is the product of two supersingular elliptic curves with the product polarization.

Corollary 2.3. Let L be a real quadratic field of strict class number one, and let p be a rational prime unramified in L. Then p is evil for every primitive quartic CM field K satisfying conditions (1)–(3) of Theorem 2.1. □

Theorem 2.4. Let p be a rational prime. Let $\mathcal{A} = \mathcal{A}_{2,1}$ denote the moduli space of principally polarized abelian surfaces, and let $\mathcal{SS}(\mathcal{A})$ denote the superspecial points of $\mathcal{A}$ modulo p. There exists a constant $M = M(p)$ such that if L is a real quadratic field of strict class number one and discriminant greater than M, then the map

$$\mathcal{SS}(L) \longrightarrow \mathcal{SS}(\mathcal{A}) \tag{2.3}$$

is surjective. □

Corollary 2.5. Let L be a real quadratic field of strict class number one, and let p be a rational prime unramified in L, and suppose that L satisfies $d_L > M = M(p)$ from Theorem 2.4. If K is a quartic CM field satisfying conditions (1)–(3) of Theorem 2.1, then every superspecial principally polarized abelian surface in characteristic p has a CM lift to an abelian surface with CM by K, that is, is a reduction of a point in $\mathcal{CM}(K)$. □

Remark 2.6. In Corollaries 2.3 and 2.5, the rational prime p can be replaced by a finite set of rational primes, all unramified in L. The results of the corollaries then hold for fields K satisfying the conditions of Theorem 2.1 for all primes in the set simultaneously. In particular, for any finite set of rational primes S, if there exists a real quadratic field L of strict class number one in which all primes in S are unramified, this gives a field K for which all primes in S are evil for K.

We remark that the existence of a real quadratic field L of strict class number one in which a given finite set of primes is unramified is a slight strengthening of a famous conjecture of Gauss on the existence of infinitely many real quadratic fields of class number one, and is widely believed to be true. More importantly, we expect that our methods can be generalized to remove the condition on strict class number one altogether, and so the results concerning a finite number of primes would then hold unconditionally.

3 Proof of Theorem 2.1

Let L be a totally real-number field of degree g over $\mathbb{Q}$, and let K be a CM field such that $K^+ = L$. We assume that L has strict class number one. We recall that for an abelian variety A/k, k a field, with RM by L, that is, with an action of $\mathcal{O}_L$, one says that the Rapoport condition holds if the tangent space of A at the origin $\mathfrak{T}_{A,0}$ is a free $\mathcal{O}_L \otimes_{\mathbb{Z}} k$-module of rank 1 (cf. [10, Section III.5]). Since we assumed that p is unramified in L, this is equivalent to the Kottwitz condition used in [11] and defined in [16].

Lemma 3.1. (1) One can write $\mathcal{O}_K = \mathcal{O}_L[t]$, where t satisfies the quadratic polynomial $x^2 + bx + c$, with $b, c \in \mathcal{O}_L$. Let $-m = b^2 - 4c$. Then $-m$ is a totally negative generator of $d_{K/L}$ and $\mathcal{D}_{K/L}^{-1} = \mathcal{O}_K[1/\sqrt{-m}]$.

(2) Let A be an abelian variety with real multiplication by $\mathcal{O}_L$ such that the Rapoport condition holds. Then A has an $\mathcal{O}_L$-linear principal polarization which is unique up to automorphism.

(3) Let Φ be a CM type of K and let $\mathfrak{a}$ be a fractional ideal in K. The abelian variety $\mathbb{C}^g/\Phi(\mathfrak{a})$ carries a principal polarization λ such that the Rosati involution associated to it induces complex conjugation on K. Moreover, λ is unique up to automorphism. □

Proof. Since $\mathcal{O}_L$ has strict class number one, and $\mathcal{O}_K$ is a torsion-free $\mathcal{O}_L$-module, we may write $\mathcal{O}_K = \mathcal{O}_L \oplus \mathcal{O}_L \cdot t$. Then $t^2 = -c - bt$ for some $b, c \in \mathcal{O}_L$. It follows that the discriminant ideal $d_{K/L}$ is generated by $\mathrm{Norm}_{K/L}(2t + b) = \mathrm{Norm}_{K/L}(\sqrt{-m}) = m$ (see [22, Chapter 3, Section 6, Corollary 2]) and that $\mathcal{D}_{K/L}^{-1} \supseteq \mathcal{O}_K[1/\sqrt{-m}]$. We deduce equality by comparing the norm to L of these ideals. We conclude part (1).

It is proven in [21] that A has an $\mathcal{O}_L$-linear polarization. Since the polarization module of A is a projective $\mathcal{O}_L$-module with a notion of positivity, it follows that there is an isomorphism of $\mathcal{O}_L$-modules $\mathrm{Hom}_{\mathcal{O}_L}(A, A^\vee)^{\mathrm{sym}} \cong \mathcal{O}_L$, taking the polarizations to the totally positive elements. Since A satisfies the Rapoport condition, it can be lifted as a polarized abelian variety with RM to characteristic zero (see [11], or [23, Chapter X, Corollary 1.8]). The characteristic zero uniformization allows us to deduce that the

degree of a symmetric homomorphism, viewed as an element $\lambda \in \mathcal{O}_L$, is $\mathrm{Norm}(\lambda)^2$. In particular, principal polarizations exist and are in bijection with $\mathcal{O}_L^{\times,+}$.

Now, for any totally real-number field L of degree g we have an exact sequence

$$1 \longrightarrow L^\times / \left(L^{\times,+} \cdot \mathcal{O}_L^\times\right) \longrightarrow \mathrm{Cl}^+(L) \longrightarrow \mathrm{Cl}(L) \longrightarrow 1. \tag{3.1}$$

There is a sign map, $\mathrm{sgn} : L^\times \to \{\pm 1\}^g$, which is a surjective homomorphism with kernel $L^{\times,+}$. Thus, the cardinality of $L^\times/(L^{\times,+} \cdot \mathcal{O}_L^\times)$ is $2^g/|\mathrm{sgn}(\mathcal{O}_L^\times)|$. If we interpret 2^g as the cardinality of $\mathcal{O}_L^\times/\mathcal{O}_L^{\times,2}$ and $|\mathrm{sgn}(\mathcal{O}_L^\times)|$ as the cardinality of $\mathcal{O}_L^\times/\mathcal{O}_L^{\times,+}$ we conclude that $|\mathcal{O}_L^{\times,+}/\mathcal{O}_L^{\times,2}| = h_L^+/h_L$. In particular, the statement $h_L^+ = 1$ is equivalent to the statement that $h_L = 1$ and $\mathcal{O}_L^{\times,+} = \mathcal{O}_L^{\times,2}$.

Now let λ_1, λ_2 be two principal $\mathcal{O}_L$-linear polarizations on the abelian variety with real multiplication (A, ι). We may identify λ_i with totally positive units in $\mathcal{O}_L$ and so there is a unit $\epsilon \in \mathcal{O}_L$ such that $\lambda_2 = \epsilon^2\lambda_1$. That implies that the polarized abelian varieties (A, ι, λ_1) and (A, ι, λ_2) are isomorphic via the multiplication by ϵ map.

Next we address part (3). It is well known that the polarizations on $\mathbb{C}^g/\Phi(\mathfrak{a})$ that induce complex conjugation on K arise from bilinear pairings

$$E_\rho : \mathfrak{a} \times \mathfrak{a} \longrightarrow \mathbb{Z}, \qquad E_\rho(u, v) = \mathrm{Tr}_{K/\mathbb{Q}}(\rho u \bar{v}), \tag{3.2}$$

where $\rho \in (\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$, $\bar{\rho} = -\rho$, and $\mathrm{Im}(\phi(\rho)) > 0$ for all $\phi \in \Phi$. The polarization is principal if and only if $(\rho) = (\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$.

It follows from part (1) that $\mathcal{D}_{K/L} = (\sqrt{-m})$ and since L has strict class number, one we also have $\mathcal{D}_{L/\mathbb{Q}} = (\eta)$ for some totally positive η. Since $\mathcal{D}_{K/\mathbb{Q}} = \mathcal{D}_{K/L}\mathcal{D}_{L/\mathbb{Q}}$, we conclude that $\mathcal{D}_{K/\mathbb{Q}} = (\delta)$, where $\bar{\delta} = -\delta$. Again, the strict class number one condition gives that $\mathrm{sgn}(\mathcal{O}_L^\times) = \{\pm 1\}^g$ and so modifying δ by a unit $\epsilon \in \mathcal{O}_L^\times$ we can achieve also $\mathrm{Im}(\phi(\delta)) > 0$ for all $\phi \in \Phi$. Given a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ there is an $\alpha \in L^+$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$. Letting $\rho = 1/(\delta\alpha)$, we see that $\mathbb{C}^g/\Phi(\mathfrak{a})$ carries a principal polarization. Moreover, the element ρ is unique up to multiplication by elements of $\mathcal{O}_L^{\times,+} = \mathcal{O}_L^{\times,2}$ and the same argument as in part (2) shows that different choices of ρ lead to isomorphic polarized abelian varieties with CM. ∎

Let $A \in \mathcal{SS}(L)$. There is a given embedding $\iota : \mathcal{O}_L \to \mathrm{End}(A)$ and a unique up-to-isomorphism $\mathcal{O}_L$-linear principal polarization for this embedding. The centralizer R of $\mathcal{O}_L$ in $\mathrm{End}(A)$ is an order of the quaternion algebra $B_{p,L} = B_{p,\infty} \otimes L$, where $B_{p,\infty}$ is the quaternion algebra over $\mathbb{Q}$ ramified at p and infinity (cf. [2, Lemma 6]). In particular $B_{p,L}$ is ramified at any infinite place of L. It follows that the Rosati involution coming from an $\mathcal{O}_L$-polarization fixes R and induces on it the canonical involution $x \mapsto \bar{x} := \mathrm{Tr}(x) - x$.

The orders R that arise in this way are called superspecial in [19]. In that thesis, Nicole develops a theory analogous to Deuring's theory for supersingular elliptic curves and we refer the reader to that reference for a comprehensive picture. The only fact that we need here is that if (A_i, ι_i), $i = 1, 2$, are two superspecial abelian varieties with real multiplication by $\mathcal{O}_L$ and $R_i = \mathrm{Cent}_{\mathrm{End}(A_i)}(\mathcal{O}_L)$, then R_1 and R_2 are everywhere locally conjugate. For completeness we sketch the argument.

As is well-known, Tate's theorem for abelian varieties (see, e.g., [25]) can be simplified for supersingular abelian varieties over a finite field of characteristic p and written as

$$\begin{aligned} &\mathrm{Hom}\left(A_1, A_2\right) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}\left(T_\ell(A_1), T_\ell(A_2)\right), \\ &\mathrm{Hom}\left(A_1, A_2\right) \otimes \mathbb{Z}_p \cong \mathrm{Hom}\left(\mathbb{D}(A_1), \mathbb{D}(A_2)\right), \end{aligned} \tag{3.3}$$

where T_ℓ denotes the Tate module at ℓ and $\mathbb{D}(A_i)$ is the covariant Dieudonné module of A_i (the Hom's ones are over $\overline{\mathbb{F}}_p$). It is not hard to see that if A_i have RM by $\mathcal{O}_L$, then we get

$$\begin{aligned} &\mathrm{Hom}_{\mathcal{O}_L}\left(A_1, A_2\right) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}_{\mathcal{O}_L}\left(T_\ell(A_1), T_\ell(A_2)\right), \\ &\mathrm{Hom}_{\mathcal{O}_L}\left(A_1, A_2\right) \otimes \mathbb{Z}_p \cong \mathrm{Hom}_{\mathcal{O}_L}\left(\mathbb{D}(A_1), \mathbb{D}(A_2)\right). \end{aligned} \tag{3.4}$$

Since $T_\ell(A) \cong (\mathcal{O}_L \otimes \mathbb{Z}_\ell)^2$ and the isomorphism type of the Dieudonné module $\mathbb{D}(A)$ does not depend on A if p is unramified (see [12, Theorem 5.4.4]), we conclude that the orders $\mathrm{End}_{\mathcal{O}_L}(A_i)$ are locally isomorphic at every prime.

Given an $\mathcal{O}_L$-embedding of $\mathcal{O}_K$ into R, the action of $\mathcal{O}_K$ will satisfy the Kottwitz condition automatically, because $\mathcal{O}_L$ does by assumption. The Rosati involution defined by any principal $\mathcal{O}_L$-polarization will induce complex conjugation on K. By [11, Lemma 4.4.1] this gives an element of $\mathcal{CM}(K)$ reducing to A.

The problem is thus translated to showing the existence of an embedding of $\mathcal{O}_K$ into such an order R if K satisfies certain conditions. Let R^0 denote the elements of reduced trace 0 in R and let $\Lambda_R = R^0 \cap (\mathcal{O}_L + 2R)$. This is an $\mathcal{O}_L$-lattice of rank 3 equipped with a positive definite $\mathcal{O}_L$-valued quadratic form N (which is just the restriction of the reduced norm on the quaternion algebra $R \otimes_{\mathcal{O}_L} L$ to Λ_R):

$$N : \Lambda_R \longrightarrow \mathcal{O}_L, \qquad x \longmapsto N(x) = x\bar{x} = -x^2. \tag{3.5}$$

Lemma 3.2. Let $-m$ be a totally negative generator of $d_{K/L}$. Then $\mathcal{O}_K \hookrightarrow R$ if and only if m is represented by the ternary quadratic form N on Λ_R. □

Proof. We write $\mathcal{O}_K = \mathcal{O}_L[t]$, where $t^2 + bt + c = 0$ as in Lemma 3.1. If $t = (-b + \sqrt{-m})/2$ is in R, then $\sqrt{-m} = b + 2t \in \Lambda_R$ and its norm is m. Conversely, suppose that there is an element $x \in \Lambda_R$ such that $N(x) = m$. This gives a map $K \to B_{p,L}$ taking $\sqrt{-m}$ to x. We may write $x = x_1 + 2x_2$, where $x_i \in \mathcal{O}_L$, $x_2 \in R$, and so the image of the element $\alpha = (-x_1 + \sqrt{-m})/2$ is in R, hence it is an integral element. That is, $\alpha \in \mathcal{O}_K$. We conclude that $\mathcal{O}_L[\alpha] \subseteq \mathcal{O}_K$. In fact, $\mathcal{O}_L[\alpha] = \mathcal{O}_K$ because $t - \alpha \in L \cap \mathcal{O}_K = \mathcal{O}_L$. Since $\mathcal{O}_L[\alpha] \subset R$, our claim follows. ■

We will use the following theorem of Cogdell [3] in the case of strict class number one.

Theorem 3.3. Let $q(x_1, x_2, x_3)$ be a positive definite integral ternary quadratic form over L. Then there is a constant C_q such that if α is a totally positive square-free integer of $\mathcal{O}_L$ with $\mathrm{Norm}_{L/\mathbb{Q}}(\alpha) > C_q$, then α is represented integrally by q if and only if it is represented integrally locally over every completion of L; that is, when $\mathrm{Norm}_{L/\mathbb{Q}}(\alpha) > C_q$, $\alpha = q(x_1, x_2, x_3)$ for some $x_i \in \mathcal{O}_L$ if and only if for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$, $\alpha = q(x_{1,\mathfrak{p}}, x_{2,\mathfrak{p}}, x_{3,\mathfrak{p}})$ for some $x_{i,\mathfrak{p}} \in \mathcal{O}_{L_\mathfrak{p}}$. □

Using this theorem, one reduces the assertion that $\mathcal{O}_K$ embeds into R if the absolute value of the norm of $d_{K/L}$ is large enough to verify that the norm N on Λ_R represents m locally at every prime $\mathfrak{p}$ of $\mathcal{O}_L$. We note that $\Lambda_R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{p}} = \Lambda_{R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{p}}} := (R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{p}})^0 \cap (\mathcal{O}_{L_\mathfrak{p}} + 2R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{p}})$ (cf. Proposition 3.4). Since all the orders R that arise are locally isomorphic, the isomorphism leaves the trace and norm unchanged, and the formation of the lattices commutes with completions, it suffices to deal with a single-order R, which we now proceed to do.

Let E/k be a supersingular elliptic curve and let $A = E \otimes_{\mathbb{Z}} \mathcal{O}_L$. As an abelian variety A is isomorphic to E^g and its functor of points is canonically given by $A(R) = E(R) \otimes_{\mathbb{Z}} \mathcal{O}_L$. It is thus a superspecial abelian variety with $\mathcal{O}_L$-action. Because the tangent space of A at zero is clearly a locally free $\mathcal{O}_L \otimes k$-module, as $\mathfrak{T}_{E \otimes_{\mathbb{Z}} \mathcal{O}_L, 0} = \mathfrak{T}_{E,0} \otimes_{\mathbb{Z}} \mathcal{O}_L$, A satisfies the Rapoport condition. Lemma 3.1 gives that A carries a unique principal $\mathcal{O}_L$-linear polarization up to isomorphism, thus giving a point of $\mathcal{SS}(L)$. In this case $R = \mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$, where $\mathcal{O} \subset B_{p,\infty}$ is a maximal order identified once and for all with $\mathrm{End}(E)$ (see [19, Proposition 2.5.26.]). Set $\Lambda_\mathcal{O} = \mathcal{O}^0 \cap (\mathbb{Z} + 2\mathcal{O})$, where $\mathcal{O}^0$ are the trace zero elements of $\mathcal{O}$. In this case one can prove the following.

Proposition 3.4. (i) $\Lambda_R = \Lambda_\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$ and the norm form on Λ_R is the extension of scalars of the norm form on $\Lambda_\mathcal{O}$.

(ii) Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ and $\mathcal{O}_{L_\mathfrak{q}}$ the ring of integers of the completion $L_\mathfrak{q}$ of L at $\mathfrak{q}$. Let $q = \mathfrak{q} \cap \mathbb{Z}$. Then $\Lambda_R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_\mathfrak{q}} = (\Lambda_\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathcal{O}_{L_\mathfrak{q}}$.

(iii) $\Lambda_{\mathcal{O}} \otimes_{\mathbb{Z}} \mathbb{Z}_q = (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q)^0 \cap (\mathbb{Z}_q + 2\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q)$ (namely, the construction of the lattice $\Lambda_{\mathcal{O}}$ commutes with localization). Moreover the norm form induced on $\Lambda_{\mathcal{O}} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ is none other than the norm form induced from $B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_q$. □

Proof. Consider the following diagram of $\mathbb{Z}$-modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}^0 \cap (\mathbb{Z}+2\mathcal{O}) & \longrightarrow & \mathbb{Z}+2\mathcal{O} & \xrightarrow{\mathrm{Tr}} & 2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}^0 & \longrightarrow & \mathcal{O} & \xrightarrow{\mathrm{Tr}} & \mathbb{Z} & \longrightarrow & 0 \end{array} \tag{3.6}$$

The rows are exact and the vertical arrows are injections. The only nontrivial claim here is that the trace map $\mathcal{O} \to \mathbb{Z}$ is surjective. This can be checked by a local calculation, which is trivial at odd primes because $\mathbb{Z} \subset \mathcal{O}$, and is easily carried out at the prime 2 using a model for quaternion algebras over $\mathbb{Q}_2$ as appearing below.

Since $\mathcal{O}_L$ is a flat $\mathbb{Z}$-module, the diagram stays exact after tensoring with $\mathcal{O}_L$, and the vertical arrows are still injections. From that one concludes that (a) $\mathcal{O}^0 \otimes_{\mathbb{Z}} \mathcal{O}_L = \mathrm{Ker}[\mathrm{Tr} \otimes 1 : \mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L \to \mathcal{O}_L] = \mathrm{Ker}[\mathrm{Tr} : R \to \mathcal{O}_L] = R^0$, and (b) $(\mathcal{O}^0 \cap (\mathbb{Z} + 2\mathcal{O})) \otimes_{\mathbb{Z}} \mathcal{O}_L$ is $\mathrm{Ker}[\mathrm{Tr} \otimes 1 : (\mathbb{Z} + 2\mathcal{O}) \otimes_{\mathbb{Z}} \mathcal{O}_L \to 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathcal{O}_L] = \mathrm{Ker}[\mathrm{Tr} : \mathcal{O}_L + 2R \to 2\mathcal{O}_L]$ (where the identifications are made using the vertical injective arrows of the diagram tensored with $\mathcal{O}_L$). That is, $\Lambda_{\mathcal{O}} \otimes_{\mathbb{Z}} \mathcal{O}_L = \Lambda_R$, which is the first assertion of the proposition. Of course, (ii) is an immediate consequence of (i). Part (iii) follows from the same reasoning, this time using the flat $\mathbb{Z}$-module $\mathbb{Z}_q$. ■

Picking a convenient model for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q$, we can now calculate $\Lambda_{\mathcal{O}} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ and its norm form explicitly, extend scalars to $\mathcal{O}_{L_q}$, and check that there are no local obstructions to representing m. We consider two cases.

Case 1 ($q \mid q$, $q \neq p$). Outside of p and ∞, $B_{p,\infty}$ is unramified, so

$$\mathcal{O} \otimes \mathbb{Z}_q \cong M_2(\mathbb{Z}_q), \tag{3.7}$$

where the reduced trace is the trace of a matrix and the reduced norm is the determinant of a matrix. So

$$\begin{aligned} (\mathcal{O} \otimes \mathbb{Z}_q)^0 &\cong \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a, b, c \in \mathbb{Z}_q \right\}, \\ \mathbb{Z}_q &\cong \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_q \right\}. \end{aligned} \tag{3.8}$$

So

$$\begin{aligned}\Lambda_{\mathcal{O}} \otimes_{\mathbb{Z}} \mathbb{Z}_q &= \left(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q\right)^0 \cap \left(\mathbb{Z}_q + 2\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q\right) \cong \left\{ \begin{pmatrix} a & 2b \\ 2c & -a \end{pmatrix} : a, b, c \in \mathbb{Z}_q \right\}, \\ \Lambda_R \otimes_{\mathcal{O}_L} \mathcal{O}_{L_q} &\cong \left\{ \begin{pmatrix} a & 2b \\ 2c & -a \end{pmatrix} : a, b, c \in \mathcal{O}_{L_q} \right\}.\end{aligned} \tag{3.9}$$

The question of whether m is represented locally at q is now a question of whether $m = -a^2 - 4bc$, which is obviously the case.

Case 2 ($q \mid p$). Let $\mathbb{Q}_{p^2}$ be the unramified extension of degree two of $\mathbb{Q}_p$ and $\mathbb{Z}_{p^2}$ its maximal order. In this case, we can verify using [24, Chapter II, Théorème 1.1] that

$$B_{p,\infty} \otimes \mathbb{Q}_p = \left\{ \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix} : a, b \in \mathbb{Q}_{p^2},\ \sigma = \text{Frobenius} \right\}. \tag{3.10}$$

This is a division algebra over $\mathbb{Q}_p$, whose trace and norm are in this model the trace and determinant of matrices. The algebra $B_{p,\infty} \otimes \mathbb{Q}_p$ has a unique maximal order consisting of all the elements with integral norm [24, Chapter II, Lemme 1.5]. Therefore, the maximal order is

$$\begin{aligned}\mathcal{O} \otimes \mathbb{Z}_p &= \left\{ \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\}, \\ \left(\mathcal{O} \otimes \mathbb{Z}_p\right)^0 &= \left\{ \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix} : a + a^\sigma = 0,\ a, b \in \mathbb{Z}_{p^2} \right\}.\end{aligned} \tag{3.11}$$

So

$$\begin{aligned}\Lambda_{\mathcal{O}} \otimes \mathbb{Z}_p &= \left(\mathcal{O} \otimes \mathbb{Z}_p\right)^0 \cap \left(\mathbb{Z}_p + 2\mathcal{O} \otimes \mathbb{Z}_p\right) \\ &= \left\{ \begin{pmatrix} a + 2\alpha & 2\beta \\ -2p\beta^\sigma & a + 2\alpha^\sigma \end{pmatrix} : a + \alpha + \alpha^\sigma = 0,\ a \in \mathbb{Z}_p,\ \alpha, \beta \in \mathbb{Z}_{p^2} \right\} \\ &= \left\{ \begin{pmatrix} \alpha - \alpha^\sigma & 2\beta \\ -2p\beta^\sigma & \alpha^\sigma - \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{Z}_{p^2} \right\}.\end{aligned} \tag{3.12}$$

From this point we proceed by considering two possibilities.

Subcase 2.1 ($p \neq 2$). Write $\mathbb{Z}_{p^2} = \mathbb{Z}_p + \sqrt{r}\mathbb{Z}_p$, where r is not a square modulo p. Then we can write down the following $\mathbb{Z}_p$-basis for the above collection of matrices:

$$e_1 = \begin{pmatrix} \sqrt{r} & 0 \\ 0 & -\sqrt{r} \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}, \qquad e_3 = \begin{pmatrix} 0 & \sqrt{r} \\ p\sqrt{r} & 0 \end{pmatrix}. \tag{3.13}$$

Let $\mathfrak{p} \mid p$ be a prime of $\mathcal{O}_L$ dividing p. Via the identifications in Proposition 3.4, this is also a basis for Λ_R over $\mathcal{O}_{L_\mathfrak{p}}$ and we have

$$N(xe_1 + ye_2 + ze_3) = -rx^2 + py^2 - prz^2, \quad x, y, z \in \mathcal{O}_{L_\mathfrak{p}}. \tag{3.14}$$

An application of Hensel's lemma shows that since $p \neq 2$ and is unramified in L, m is represented by $-rx^2 + py^2 - prz^2$ over $\mathcal{O}_{L_\mathfrak{p}}$ if and only if m is represented by $-rx^2$ over $\mathcal{O}_{L_\mathfrak{p}}$. This, in turn, is equivalent to $-m/r$ being a square modulo $\mathfrak{p}$. Now, $(r/\mathfrak{p}) = (-1)^{f(\mathfrak{p}/p)}$ so m is representable if and only if $(-m/\mathfrak{p}) = (-1)^{f(\mathfrak{p}/p)}$. On the other hand, for $p \neq 2$ and unramified in K, we have $(-m/\mathfrak{p}) = (-1)^{f(\mathfrak{P}/\mathfrak{p})+1}$ for one (or any) prime $\mathfrak{P} \mid \mathfrak{p}$. We conclude that m is representable locally at a place $\mathfrak{p} \mid p$ if and only if $f(\mathfrak{P}/\mathfrak{p}) + f(\mathfrak{p}/p)$ is odd for all $\mathfrak{P} \mid \mathfrak{p}$.

Subcase 2.2 ($p = 2$). In this case we write $\mathbb{Z}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$. The form N is now given by

$$\begin{aligned} &N\left(\begin{pmatrix} \alpha - \alpha^\sigma & 2\beta \\ -2p\beta^\sigma & \alpha^\sigma - \alpha \end{pmatrix}\right) = -(\alpha - \alpha^\sigma)^2 + 8\beta\beta^\sigma = 3b^2 + 8\beta\beta^\sigma, \\ &\alpha = a + bx, \quad a, b \in \mathbb{Z}_2, \quad \beta \in \mathbb{Z}_4. \end{aligned} \tag{3.15}$$

This is a ternary quadratic form over $\mathbb{Z}_2$ and we want to find the conditions under which

$$m = 3b^2 + 8\beta\beta^\sigma, \quad b \in \mathcal{O}_{L_\mathfrak{p}},\ \beta \in \mathbb{Z}_4 \otimes_{\mathbb{Z}_2} \mathcal{O}_{L_\mathfrak{p}}. \tag{3.16}$$

We first use Hensel's lemma mod $\mathfrak{p}^3$ (see, e.g., [17, Chapter II, Section 2]). Since $\mathfrak{p}$ is unramified, $m \not\equiv 0 (\mathrm{mod}\, \mathfrak{p})$ and one concludes that m is represented by N if and only if $m = 3b^2$, $b \in \mathcal{O}_{L_\mathfrak{p}}$, and that holds if and only if $m = 3b^2 (\mathrm{mod}\, \mathfrak{p}^3)$. Equivalently, $3m$ is a quadratic residue modulo $\mathfrak{p}^3$. This concludes the proof of Theorem 2.1.

3.1 Scholium

One may ask whether the conditions appearing in Theorem 2.1 imply, in turn, superspecial reduction. This is not the case, as can be learned by comparing our results with [9, Theorem 2, cases (3) and (5)]. That theorem deals with the reduction of abelian surfaces with CM by a quartic non-Galois CM field K. In both cases (3) and (5), the prime p stays

inert in K^+ and splits from K^+ to K and so the conditions of Theorem 2.1 hold. The reduction in case (3) is superspecial, while in case (5) it is ordinary! Nonetheless, there is a sense in which Theorem 2.1 can be strengthened, as we now explain. We remark that [9] deals only with quartic CM fields, while Theorem 2.1 deals with any CM field whose maximal totally real subfield has strict class number 1.

We have shown above that, under the conditions of Theorem 2.1, the natural map $\mathcal{CM}(K) \to \mathcal{M}_L$ has an image that contains the superspecial locus $\mathcal{SS}(L)$. Let Φ be a CM type of K and let $\mathcal{CM}(K)^\Phi$ denote the elements of $\mathcal{CM}(K)$ having CM type Φ. We now explain why there is a CM type Φ such that the image of $\mathcal{CM}(K)^\Phi \to \mathcal{M}_L$ is contained $\mathcal{SS}(L)$. We have seen that the conditions appearing in the theorem guarantee that m is locally represented everywhere by the norm form on Λ_R, where R is the centralizer of $\mathcal{O}_L$ in the endomorphism ring of a superspecial principally polarized abelian variety with RM by $\mathcal{O}_L$. The order R is a superspecial order; those are characterized for p unramified in L as the orders of discriminant p in $B_{p,L}$. At every prime which does not split $B_{p,L}$ such an order is maximal, and at every prime $\mathfrak{p} \mid p$ that splits $B_{p,L}$, it is an Eichler order of conductor $\mathfrak{p}$. It is known [19] that every superspecial order, that is, an order of $B_{p,L}$ of discriminant p, arises this way from a superspecial abelian variety with RM by L. We use now that when a genus of $\mathcal{O}_L$-integral positive definite quadratic forms represents an element $m \in \mathcal{O}_L$ everywhere locally, then *some* form in the genus will represent m globally. See [13, Section 2] and the references therein. There is thus a ternary form (Λ, q) in the genus of $(\Lambda_R, N_{B_{p,L}/L}|_{\Lambda_R})$ that represents m. We claim that such a ternary form q arises again in the same way from an order in a quaternion algebra, which is again superspecial. First, the local data that we have allow us to conclude that there is a lattice $\Lambda^+ \supset \Lambda$ on which q has discriminant p^2 and is still integral; in fact, we choose Λ^+ so that under each local isomorphism of Λ with Λ_R we have Λ^+ corresponding to R^0. Then the method of Clifford algebras allows us to associate a quaternion algebra B over L to (Λ^+, q) such that for some order R' of B we have $(R'^0, N_{B/L}) \cong (\Lambda^+, q)$ as quadratic modules (see [1] and the references therein). It follows then that $B \cong B_{p,L}$ and R' is a superspecial order since its discriminant is p. Identifying B with $B_{p,L}$ we find that $\Lambda_{R'}$ is everywhere locally isomorphic to (Λ, q).

As said, the superspecial order R' is associated to a point in $\mathcal{SS}(L)$, that is, $R' \cong \mathrm{End}_{\mathcal{O}_L}(A)$ for some superspecial abelian variety A with RM over $\overline{\mathbb{F}}_p$; once we make this identification we have a CM type Φ associated to the embedding of $\mathcal{O}_K$ in R' coming from the action of $\mathcal{O}_K$ on $\mathfrak{T}_{A,0}$. We conclude that *some* point of $\mathcal{SS}(L)$ lifts to $\mathcal{CM}(K)$. Since $\mathrm{Hom}(A, B)$ for two characteristic zero abelian varieties with CM by $\mathcal{O}_K$ and of the same CM type Φ always contains an element of degree prime to p, it now follows that *any* abelian variety with CM by $\mathcal{O}_K$ and CM type Φ will have superspecial reduction.

3.2 Proof of Corollary 2.3

Let $L = \mathbb{Q}(\sqrt{d})$, with d a square free positive integer. We need to show that there exist two supersingular elliptic curves E_1, E_2 in characteristic p such that $\mathcal{O}_L$ embeds into $\mathrm{End}(E_1 \times E_2)$ and its image is contained in the elements of $\mathrm{End}(E_1 \times E_2)$ fixed by the Rosati involution coming from the product polarization on $E_1 \times E_2$. Clearly, for any supersingular elliptic curve E_1, we can find a supersingular elliptic curve E_2 and an isogeny $\beta : E_1 \to E_2$ such that the following holds: (a) if $d \equiv 2, 3 (\mathrm{mod}\, 4)$, then $\deg(\beta) = d$; (b) if $d \equiv 1 (\mathrm{mod}\, 4)$, then $\deg(\beta) = (d-1)/4$. Then, in the first case sending $\sqrt{d}$ to $\left(\begin{smallmatrix} 0 & \beta^\vee \\ \beta & 0 \end{smallmatrix}\right) \in \mathrm{End}(E_1 \times E_2)$ provides the required embedding, and in the second case, sending $(1+\sqrt{d})/2$ to $\left(\begin{smallmatrix} 1 & \beta^\vee \\ \beta & 0 \end{smallmatrix}\right) \in \mathrm{End}(E_1 \times E_2)$ provides the required embedding.

4 Proof of Theorem 2.4

There is a unique superspecial surface over $\overline{\mathbb{F}}_p$, which can be taken to be $E_1 \times E_2$ for any choice of supersingular elliptic curves E_i. Elements of $\mathcal{SS}(A)$ are distinguished by their principal polarization (up to isomorphism). Those, by a result going back to Weil, are given by the algebraic equivalence classes of divisors that are either two elliptic curves crossing transversely at their origin, or a nonsingular curve of genus two (all up to automorphisms of the abelian variety). There is another description.

Let $A = E \times E$, where E is supersingular elliptic curve. Let $\lambda : A \to A^\vee$ be any principal polarization. Recall that the Rosati involution on $\mathrm{End}(A)$, $f \mapsto f^\lambda$, is defined as

$$f^\lambda = \lambda^{-1} f^\vee \lambda, \tag{4.1}$$

where $f^\vee : A^\vee \to A^\vee$ is the dual homomorphism. The map from the Neron-Severi group, $\mathrm{NS}(A)$:

$$\mathrm{NS}(A) \longrightarrow \mathrm{End}(A), \qquad \mu \longmapsto \lambda^{-1}\mu, \tag{4.2}$$

identifies $\mathrm{NS}(A)$ with the λ-symmetric elements of $\mathrm{End}(A)$; the polarizations correspond to the λ-totally positive elements under this identification (cf. [18, pages 189-190, 208–210], [14, Section 2.2]). If we choose the product polarization λ_0, coming from the canonical identification of E with $E^\vee$, and $\mathcal{O} = \mathrm{End}(E)$, then the principal polarizations of A are the elements

$$\left\{ \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix} : s, t \in \mathbb{Z},\ s, t > 0,\ r \in \mathcal{O},\ st - rr^\vee = 1 \right\}. \tag{4.3}$$

We first consider a particular case. We take $A = E^2$ with the canonical polarization λ_0. We then want to show that there is an embedding of $\mathcal{O}_L$ into the matrices

$$\Pi(\lambda_0) := \left\{ \begin{pmatrix} s & r \\ r^\vee & t \end{pmatrix} : s, t \in \mathbb{Z},\ r \in \mathcal{O} \right\} \tag{4.4}$$

if the discriminant d_L of L is large enough (these are the symmetric matrices with respect to the polarization we picked). Let $\Pi^0(\lambda_0) = \{M \in \Pi(\lambda_0) : \mathrm{Tr}(M) = 0\}$ and let $\Lambda(\lambda_0) = \Pi^0(\lambda_0) \cap (\mathbb{Z} + 2\Pi(\lambda_0))$. This is a rank 5 lattice that can be described explicitly:

$$\Lambda(\lambda_0) = \left\{ \begin{pmatrix} a & 2r \\ 2r^\vee & -a \end{pmatrix} : a \in \mathbb{Z},\ r \in \mathcal{O} \right\}. \tag{4.5}$$

As in Section 3, one checks that to give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda_0)$ is equivalent to the quintic quadratic form q_{λ_0} given by $a^2 + 4rr^\vee$ representing d_L on $\Lambda(\lambda_0)$. Provided $d_L \gg 0$, this follows from the fact that the quaternary quadratic form $rr^\vee$ on $\mathcal{O}$, a maximal order in $B_{p,\infty}$, represents any large enough integer.

The general case. For every other polarization λ we associate a rank 5 lattice $\Lambda(\lambda)$ with a quadratic form q_λ that will represent d_L if and only if $\mathcal{O}_L$ embeds in the lattice $\Pi(\lambda)$ of λ-symmetric elements of $\mathrm{End}(E^2)$. To show that q_λ represents sufficiently large primitive discriminants, we need to show that there are no local obstructions, for which we will argue that locally the quintic quadratic modules $(\Lambda(\lambda), q_\lambda)$ and $(\Lambda(\lambda_0), q_{\lambda_0})$ are isomorphic.

Take a matrix $M = \left(\begin{smallmatrix} s & r \\ r^\vee & t \end{smallmatrix}\right)$ defining a principal polarization λ. For any matrix $C = \left(\begin{smallmatrix} x & y \\ w & z \end{smallmatrix}\right) \in M_2(B_{p,\infty})$ we let $C^\vee = \left(\begin{smallmatrix} x^\vee & w^\vee \\ y^\vee & z^\vee \end{smallmatrix}\right)$. Denote the Rosati involution defined by λ as $N \mapsto N^\lambda$. Then $N^\lambda = M^{-1}N^\vee M$. Let

$$\Pi(\lambda) = \left\{ N \in M_2(\mathcal{O}) : N^\lambda = N \right\}. \tag{4.6}$$

By what we said above, the lattice $\Pi(\lambda)$ is isomorphic to $\mathrm{NS}(A)$ and so is a rank 6 lattice. We can view $\Pi(\lambda)$ as $\Pi(\lambda) \otimes \mathbb{Q} \cap M_2(\mathcal{O})$. We provide another description of $\Pi(\lambda)$. One may write $M = H^\vee H$ for a suitable $H \in M_2(B_{p,\infty})$ (see [6, Proposition 4.2]). Consider the automorphism of the algebra $M_2(B_{p,\infty})$ given by $N \mapsto H^{-1}NH$. We also denote this by

$$N \longmapsto \phi_H(N) = H^{-1}NH. \tag{4.7}$$

If $N^\vee = N$, that is, $N \in \Pi(\lambda_0)$, then using the formula $(C_1C_2)^\vee = C_2^\vee C_1^\vee$, one finds that

$$M^{-1}\left(H^{-1}NH\right)^\vee M = H^{-1}\left(H^\vee\right)^{-1}H^\vee N^\vee \left(H^{-1}\right)^\vee H^\vee H = H^{-1}NH. \tag{4.8}$$

That is, $\phi_H(N) = H^{-1}NH$ is an element of $\Pi(\lambda) \otimes \mathbb{Q}$. We find that the rank 6 lattice $\Pi(\lambda)$ is given by

$$\Pi(\lambda) = \phi_H\big(\Pi(\lambda_0) \otimes \mathbb{Q}\big) \cap M_2(\mathcal{O}), \tag{4.9}$$

and so we define a rank 5 lattice

$$\Pi^0(\lambda) = \phi_H\big(\Pi^0(\lambda_0) \otimes \mathbb{Q}\big) \cap M_2(\mathcal{O}) \tag{4.10}$$

and a slightly smaller rank 5 lattice

$$\Lambda(\lambda) = \Pi^0(\lambda) \cap \big(\mathbb{Z} + 2\Pi(\lambda)\big). \tag{4.11}$$

The definition of these lattices is independent of the choice of H such that $M = H^\vee H$. To see that, one first reduces to the case of $M = I$, the identity matrix, so that H satisfies $I = H^\vee H$, that is, is a rational automorphism of the polarization λ_0. We remark, though this is not needed for our argument, that for any H one has $H^{-1} = (H^\vee H)^{-1} H^\vee$, and for $\vee$-symmetric matrices $\left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right)$ the inverse *is* given by $1/(x_{11}x_{22} - x_{12}x_{21})\left(\begin{smallmatrix} x_{22} & -x_{12} \\ -x_{21} & x_{11} \end{smallmatrix}\right)$, as usual. The lattice $\Pi(\lambda_0) \otimes \mathbb{Q}$, according to the definition, now consists of matrices $H^{-1}NH = H^\vee NH$ for which $N^\vee = N$, but it is easy to see that these are again just the $\vee$-symmetric matrices. That is, $\Pi(\lambda)$ is well defined under our procedure. Next we consider $\Pi^0(\lambda_0)$. Remark that under the ℓ-adic representation on $T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, $j : B_{p,\infty} \hookrightarrow M_2(\mathbb{Q}_\ell)$, we have $\mathrm{Tr}(x) = \mathrm{Tr}(j(x))$. On the other hand, $B_{p,\infty}$, being a finite dimensional $\mathbb{Q}$-algebra, has an intrinsic trace Tr' coming from the left regular representation on itself, and one has $\mathrm{Tr}' = 2\,\mathrm{Tr}$. Using this it is not hard to see, making use of the ℓ-adic representation, that the intrinsic trace Tr' of an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(B_{p,\infty})$ is just $4\,\mathrm{Tr}(a) + 4\,\mathrm{Tr}(d)$. We conclude that the function $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \mathrm{Tr}(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) := \mathrm{Tr}(a) + \mathrm{Tr}(d)$ is invariant under conjugation because Tr' obviously is. Since $\Pi^0(\lambda_0)$ can be described as the $\vee$-symmetric matrices N with $\mathrm{Tr}(N) = 0$, we conclude that its definition is indeed independent of the choice of H, that is, $\phi_H(\Pi^0(\lambda_0)) = \Pi^0(\lambda_0)$ if $H^\vee H = I$. Note that this argument also gives a more natural definition of the lattice $\Pi^0(\lambda)$ as the integral λ-symmetric matrices of Tr equal to zero and our ad hoc definition is just more convenient for the purpose of our proof.

Lemma 4.1. Let $L = \mathbb{Q}(\sqrt{D})$, $D > 0$ square-free, be a real quadratic field with discriminant d_L.

(1) To give an embedding of L into $\Pi(\lambda) \otimes \mathbb{Q}$ is equivalent to giving an element C of $\Pi^0(\lambda) \otimes \mathbb{Q}$ whose degree as a rational endomorphism is $\deg C = D^2$.

(2) To give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda)$ is equivalent to giving an element of $\Lambda(\lambda)$ whose degree as an endomorphism is d_L^2.

(3) Define

$$q_\lambda : \Lambda(\lambda) \longrightarrow \mathbb{Z}, \qquad q_\lambda(C) = \sqrt{\deg(C)}. \tag{4.12}$$

The function q_λ is a quintic integral positive definite quadratic form and to give an embedding of $\mathcal{O}_L$ into $\Pi(\lambda)$ is equivalent to representing $-d_L$ by q_λ. □

Proof. The whole issue is to map $\sqrt{D}$ to an element $C \in \Pi(\lambda) \otimes \mathbb{Q}$ that will satisfy $C^2 = DI_2$. Composing with ϕ_H^{-1}, one verifies that the condition is that $\mathrm{Tr}(C_1) = 0$ and $\det(C_1) = -D$, where $C_1 = \phi_H^{-1}(C)$ (writing the condition in $\Pi(\lambda)\otimes\mathbb{Q}$ is more complicated; see Section 4.1). However, for the matrices $C_1 = \left(\begin{smallmatrix} s & r \\ r^\vee & -s \end{smallmatrix}\right)$, we have $\deg(C_1)^2 = \deg(C_1^2) = \deg\left(\begin{smallmatrix} s^2+rr^\vee & 0 \\ 0 & s^2+rr^\vee \end{smallmatrix}\right) = (s^2 + rr^\vee)^4 = \det(C_1)^4$ and so $\deg(C_1) = D^2$. However, we have $\deg(C_1) = \deg(C)$ (for the natural extension of the degree map to rational isogenies). Note that this implies that the map $L \to \Pi(\lambda) \otimes \mathbb{Q}$ gives a map $\mathbb{Z}[\sqrt{D}] \to \Pi(\lambda)$ if and only if $C \in \Pi^0(\lambda)$ and $\deg(C) = D^2$.

One now considers the conditions that actually guarantee that $\sqrt{D}$, or $(1+\sqrt{D})/2$ (as the case may be), are in $M_2(\mathcal{O})$. The second part follows.

On $\Pi^0(\lambda_0)$ we have $q_{\lambda_0}\left(\begin{smallmatrix} s & r \\ r^\vee & -s \end{smallmatrix}\right) = s^2 + rr^\vee$, which is visibly a quintic positive definite quadratic form. Since $q_\lambda(C) = q_{\lambda_0}(\phi_H^{-1}(C))$ on $\Phi_H(\Pi^0(\lambda))$ it follows that it too is a quintic positive definite rational quadratic form. The identity $q_\lambda(C) = \sqrt{\deg(C)}$ implies that q_λ is in fact integral. ■

According to [14, Lemma 2.4], given a matrix $M \in \mathrm{GL}_2(\mathcal{O})$ and a prime q we can find a matrix $H = H(q) \in \mathrm{GL}_2(\mathcal{O}_q)$ such that $M = H^\vee H$. This means that locally the lattices $\Lambda(\lambda)$ and $\Lambda(\lambda_0)$ are conjugate by the map ϕ_H. It follows from our definitions that the quadratic modules $(\Lambda(\lambda), q_\lambda)$ and $(\Lambda(\lambda_0), q_{\lambda_0})$ are in the same genus. Therefore, verifying the local representability conditions for q_λ reduces to the case of q_{λ_0} which was already considered.

4.1 Scholium

One can give another explicit description of the lattices $\Lambda(\lambda)$ and the conditions for embedding $\mathcal{O}_L$ in them. For simplicity we only describe $\Pi(\lambda)$ and the conditions for embedding $\mathbb{Z}[\sqrt{D}]$ in it. Let $M = \left(\begin{smallmatrix} s & r \\ r^\vee & t \end{smallmatrix}\right)$ define the principal polarization λ. The elements of $\Pi(\lambda)$ are the matrices $N = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, $\alpha, \beta, \gamma, \delta \in \mathcal{O}$ such that

$$s\alpha + r\gamma \in \mathbb{Z}, \qquad r^\vee\beta + t\delta \in \mathbb{Z}, \qquad \alpha^\vee r + \gamma^\vee t = s\beta + r\delta. \tag{4.13}$$

The conditions for $N^2 = D \cdot I_2$ are

$$\alpha\beta = -\beta\delta, \qquad \gamma\alpha = -\delta\gamma, \tag{4.14}$$

and $\alpha^2 + \beta\gamma = \delta^2 + \gamma\beta = D$, which reduce given (4.14) to one condition:

$$\alpha^2 + \beta\gamma = D. \tag{4.15}$$

As noted, the matrices satisfying (4.13) are a rank 6 lattice over $\mathbb{Z}$. In fact the last equation can be written in the form

$$\alpha^2 + \beta\gamma = \frac{\beta\beta^\vee + (m')^2}{t^2}, \tag{4.16}$$

where $m' = r^\vee\beta + t\delta \in \mathbb{Z}$.

Acknowledgment

We thank the anonymous referee for many helpful suggestions to improve the paper.

References

[1] J. Brzeziński, *Arithmetical quadratic surfaces of genus 0. I*, Mathematica Scandinavica **46** (1980), no. 2, 183–208.

[2] C.-L. Chai, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Inventiones Mathematicae **121** (1995), no. 3, 439–479.

[3] J. W. Cogdell, *On sums of three squares*, Journal de Théorie des Nombres de Bordeaux **15** (2003), no. 1, 33–44, Les XXIIémes Journées Arithmétiques (Lille, 2001).

[4] E. de Shalit and E. Z. Goren, *On special values of theta functions of genus two*, Annales de l'Institut Fourier (Grenoble) **47** (1997), no. 3, 775–799.

[5] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Inventiones Mathematicae **92** (1988), no. 1, 73–90.

[6] T. Ekedahl, *On supersingular curves and abelian varieties*, Mathematica Scandinavica **60** (1987), no. 2, 151–178.

[7] N. Elkies, K. Ono, and T. Yang, *Reduction of CM elliptic curves and modular function congruences*, International Mathematics Research Notices **2005** (2005), no. 44, 2695–2707.

[8] A. Ghitza, *Hecke eigenvalues of Siegel modular forms* ($\mod p$) *and of algebraic modular forms*, Journal of Number Theory **106** (2004), no. 2, 345–384.

[9] E. Z. Goren, *On certain reduction problems concerning abelian surfaces*, Manuscripta Mathematica **94** (1997), no. 1, 33–43.

[10] ———, *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monograph Series, vol. 14, American Mathematical Society, Rhode Island, 2002, with the assistance of M.-H. Nicole.

[11] E. Z. Goren and K. E. Lauter, *Class invariants of quartic CM fields*, to appear in the Annales of the Fourier Institute, http://arxiv.org/abs/math.NT/0404378.

[12] E. Z. Goren and F. Oort, *Stratifications of Hilbert modular varieties*, Journal of Algebraic Geometry **9** (2000), no. 1, 111–154.

[13] J. Hanke, *Some recent results about (ternary) quadratic forms*, Number Theory, CRM Proc. Lecture Notes, vol. 36, American Mathematical Society, Rhode Island, 2004, pp. 147–164.

[14] T. Ibukiyama, T. Katsura, and F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Mathematica **57** (1986), no. 2, 127–152.

[15] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Inventiones Mathematicae **87** (1987), no. 2, 385–401.

[16] R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, Journal of the American Mathematical Society **5** (1992), no. 2, 373–444.

[17] S. Lang, *Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer, New York, 1994.

[18] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, no. 5, Oxford University Press, London, 1970.

[19] M.-H. Nicole, *Superspecial abelian varieties, theta series and the Jacquet-Langlands correspondence*, Doctoral thesis, McGill University, Quebec, June 2005.

[20] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, Journal of Algebra **64** (1980), no. 2, 340–390.

[21] M. Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumenthal*, Compositio Mathematica **36** (1978), no. 3, 255–335.

[22] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer, New York, 1979.

[23] G. van der Geer, *Hilbert Modular Surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 16, Springer, Berlin, 1988.

[24] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.

[25] W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), American Mathematical Society, Rhode Island, 1971, pp. 53–64.

Eyal Z. Goren: Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West, Montreal, QC, Canada H3A 2K6
E-mail address: goren@math.mcgill.ca

Kristin E. Lauter: Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
E-mail address: klauter@microsoft.com