Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The distance between superspecial abelian varieties with real multiplication

Eyal Z. Goren *, Kristin E. Lauter

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W., Montreal H3A 2K6, QC, Canada
Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA

ARTICLE INFO

Article history:
Received 17 June 2008

Communicated by B. Conrad

MSC:
primary 14K02
secondary 11E10

Keywords:
Superspecial abelian variety
Real multiplication
Isogeny
CM lift
Theta series
Quaternion algebra

ABSTRACT

Let L be a totally real field of strict class number one and let $\mathcal{O}_L$ be its ring of integers. Let p be a rational prime which is unramified in L. We consider the distance between two superspecial abelian varieties with real multiplication in characteristic p, where by "distance" we mean the minimal degree of an $\mathcal{O}_L$-isogeny. We give upper and lower bounds on the distance between superspecial abelian varieties with real multiplication by L in characteristic p in terms of p and the degree and discriminant of L.

1. Introduction

For distinct primes p and ℓ, Pizer [Piz] considered the regular graph of supersingular elliptic curves over a finite field of p^2 elements, with edges corresponding to isogenies of degree ℓ. These graphs have good expansion properties and in fact are known to be Ramanujan. The diameter of these graphs was considered by Mestre [Mes], and was shown to be bounded by $c \log p$, where c is a constant independent of ℓ. Thus for example taking $\ell = 2$, it follows that there exists an isogeny between any two supersingular elliptic curves in characteristic p of degree at most $2^{c \log p}$. For a given prime p, but independent of ℓ, one can ask for a bound, $N(p)$, such that there exists an isogeny between any

* Corresponding author at: Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W., Montreal H3A 2K6, QC, Canada.
E-mail addresses: goren@math.mcgill.ca (E.Z. Goren), klauter@microsoft.com (K.E. Lauter).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.07.005

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

two supersingular elliptic curves in characteristic p of degree at most $N(p)$. We refer to the minimal degree of an isogeny between two elliptic curves as the *distance* between them, in analogy with the terminology for graphs associated to the choice of a specific prime ℓ. In Section 5.4.1 below, we give fairly sharp upper and lower bounds on $N(p)$, both roughly of the form "a constant times $\sqrt{p}$." These bounds have applications to questions ranging from bounds on the index of a non-zero coefficient of associated theta series, to bounds on the denominators required to express a basis for a maximal order in $B_{p,\infty}$, the quaternion algebra ramified only at p and infinity.

More generally, one can consider the same question for products of supersingular elliptic curves with extra structure (superspecial abelian varieties with real multiplication). Graphs associated to superspecial abelian varieties with real multiplication were studied in [CGL]. In this paper, we give fairly sharp upper and lower bounds on the distance between superspecial abelian varieties with real multiplication. Specifically, for a given prime p and a totally real field L of strict class number one in which p is unramified, the degree, $\deg_L$, of an isogeny between two superspecial abelian varieties with real multiplication by L is a totally positive element of $\mathcal{O}_L$. We define a "norm" which is twice the trace of $\deg_L$, and let $N(p)$ be the minimal integer such that there exists an $\mathcal{O}_L$-isogeny of norm less than $N(p)$ between any two superspecial abelian varieties with real multiplication by L. Theorem 3.3 gives upper and lower bounds on $N(p)$ in terms of p and the discriminant and degree of L. The proof of the upper bound uses an extension of Minkowski's bounds to totally real fields due to Chalk [Cha], but Chalk's variant is only essential in the applications. The lower bound is asymptotic and holds for p large enough with respect to the discriminant and degree of L. The proof of the lower bound uses estimates on the number of isogenies of a given norm coming from estimates of coefficients of modular forms and class numbers. Applications of Theorem 3.3 are given in Section 4.

2. Background material and notation

2.1. Real multiplication

Let L be a totally real field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_L$, whose totally positive elements are denoted $\mathcal{O}_L^+$, and discriminant d_L. Assume that L has strict (or narrow) class number one. This is equivalent to L having class number one and every totally positive unit of $\mathcal{O}_L$ being a square. Let $\sigma_1, \ldots, \sigma_g$ denote the real embeddings of L. Let p be a rational prime which is unramified in L, $p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_a$ its factorization into prime ideals $\mathfrak{p}_i$ of $\mathcal{O}_L$.

Let $B_{p,\infty}$ be the quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞. Let $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$. The algebra $B_{p,L}$ is a quaternion algebra over L ramified at all infinite places of L and at all primes $\mathfrak{p}_i | p$ such that $f(\mathfrak{p}_i/p)$ is odd.

By a principally polarized abelian variety (ppav) with real multiplication (RM) over a base scheme S we mean a triple $\underline{A} = (A, \iota_A, \lambda_A)$, where:

- (A, λ_A) is a principally polarized abelian scheme over S of relative dimension g;
- $\iota : \mathcal{O}_L \hookrightarrow \mathrm{End}_S(A)$ is a ring embedding (it induces a ring embedding on the dual abelian variety $\iota^t : \mathcal{O}_L \hookrightarrow \mathrm{End}_S(A^t)$, $\iota^t(a) := \iota(a)^t$);
- the polarization λ_A is $\mathcal{O}_L$-equivariant;
- the relative tangent space $\mathfrak{T}_{A/S,0}$ of A along its zero section 0, is a locally free $\mathcal{O}_S \otimes_{\mathbb{Z}} \mathcal{O}_L$-module of rank 1. This is often called *the Rapoport condition*.

2.2. Superspecial varieties and the degree of isogenies

Let $k = \overline{\mathbb{F}}_p$. Our interest will be in superspecial ppav over k with RM.

Definition 2.1. $\underline{A}$ is a superspecial ppav with RM if $\underline{A}$ is a ppav with RM and A is isomorphic to a product of supersingular elliptic curves as an abelian variety (though not necessarily as a polarized abelian variety). To simplify terminology we shall say $\underline{A}$ is an *L-superspecial variety*, meaning $\underline{A}$ is a principally polarized superspecial abelian variety with real multiplication by $\mathcal{O}_L$.

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Let $\underline{A}, \underline{B}$ be two L-superspecial varieties. We consider

$$\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B}),$$

the $\mathcal{O}_L$-module of $\mathcal{O}_L$-equivariant homomorphisms $f : A \to B$. We put no condition on $f^*\lambda_B$, but it follows from our assumptions that $f^*\lambda_B = c \cdot \lambda_A$, for some $c \in \mathcal{O}_L^+$. We define, following Nicole [Nic],

$$\deg_L(f) = \deg_{L,\underline{A},\underline{B}}(f) = \lambda_A^{-1} f^t \lambda_B f,$$

so that,

$$f^*\lambda_B = \deg_L(f) \cdot \lambda_A,$$

and we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\deg_L(f)\lambda_A} & A^t \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle f^t} \\ B & \xrightarrow{\lambda_B} & B^t \end{array}$$

Nicole proves [Nic] that

$$\deg_L(\cdot) : \mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B}) \to \mathcal{O}_L$$

is a quadratic form in four variables taking values in $\mathcal{O}_L^+$. The associated bilinear form $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{\lambda_A, \lambda_B}$ is

$$\langle f, g \rangle = \lambda_A^{-1} f^t \lambda_B g + \lambda_A^{-1} g^t \lambda_B f,$$

and has discriminant $p^2\mathcal{O}_L$; that is, choosing an $\mathcal{O}_L$-basis $e_1, \ldots, e_4$ to $\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ as an $\mathcal{O}_L$-module, we get a matrix $M(\underline{A}, \underline{B}) \in M_2(\mathcal{O}_L)$ representing $\langle \cdot, \cdot \rangle$ and the determinant of M generates the ideal $p^2\mathcal{O}_L$.

Lemma 2.2. *Let* $[\cdot, \cdot] = [\cdot, \cdot]_{\underline{A},\underline{B}}$ *be defined by*

$$[f, g] = \mathrm{Tr}_{L/\mathbb{Q}} \langle f, g \rangle, \quad f, g \in \mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B}).$$

This is a positive definite $\mathbb{Z}$*-valued bilinear form on* $\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ *in* $4g$ *variables. Its discriminant is equal to* $p^{2g} d_L^4$.

Proof. Nicole proved that all the $\mathcal{O}_L$-valued quadratic forms $\langle \cdot, \cdot \rangle_{\lambda_A, \lambda_B}$ belong to the same genus. It is therefore enough to prove the statement for one particular quadratic form. Let E be a supersingular elliptic curve over k and let $A = E \otimes_{\mathbb{Z}} \mathcal{O}_L$. The abelian variety A is of dimension g and is endowed with canonical RM; it has an $\mathcal{O}_L$-equivariant principal polarization λ_A and $\mathrm{End}_k(\underline{A}) = \mathrm{End}_k(E) \otimes_{\mathbb{Z}} \mathcal{O}_L$, with the quadratic form $\deg_L$ being the $\mathcal{O}_L$-linear extension of the usual degree form $\deg : \mathrm{End}_k(E) \to \mathbb{Z}$.

Let $e_1, \ldots, e_4$ be a basis over $\mathbb{Z}$ for $\mathrm{End}_k(E)$. Let M_1 be the matrix representing the quadratic form associated to deg, i.e. $\langle f, g \rangle = f^t g + g^t f$, with respect to the basis $\{e_i\}$. Then $\det(M_1) = p^2$.

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Let $h_1, \ldots, h_g$ be a $\mathbb{Z}$-basis for $\mathcal{O}_L$ and M_2 the matrix representing the bilinear form on $\mathcal{O}_L$ given by $\mathrm{Tr}_{L/\mathbb{Q}}(r \cdot s)$, $r, s \in \mathcal{O}_L$, with respect to this basis. Then $\det(M_2) = d_L$.

By definition,

$$[e_a \otimes h_c, e_b \otimes h_d] = \mathrm{Tr}_{L/\mathbb{Q}}\big(\langle e_a, e_b\rangle \cdot h_c h_d\big) = \langle e_a, e_b\rangle \cdot \mathrm{Tr}_{L/\mathbb{Q}}(h_c h_d)$$
$$= (M_1)_{a,b}(M_2)_{c,d}.$$

We conclude that the matrix representing the quadratic form $[\cdot,\cdot]$ is the Kronecker product of the matrices M_1 and M_2. Thus, its determinant is $\det(M_1)^g \det(M_2)^4 = p^{2g} d_L^4$. □

2.3. Traces and norms

Let N be a positive real number. Let

$$U(N) := \left\{ x \in \mathcal{O}_L^+ \colon\ \frac{1}{g}\,\mathrm{Tr}_{L/\mathbb{Q}}(x) < N \right\},$$

and

$$W(N) := \left\{ x \in \mathcal{O}_L^+ \colon\ \mathrm{Norm}_{L/\mathbb{Q}}(x)^{1/g} < N \right\}.$$

As we shall presently see, the sets $U(N)$ are finite. Various finiteness results obtained below are phrased in terms of the sets $U(N)$ and so it is of interest to compare them to the sets $W(N)$. In what follows, $f(N) \sim g(N)$ means $f(N)/g(N)$ tends to 1 as N tends to infinity.

Lemma 2.3. *The sets $U(N)$ and $W(N)$ have the following properties*:

(1) *Each set $U(N)$ is finite and*

$$\big|U(N)\big| \sim \frac{e^g}{\sqrt{2\pi\, g d_L}} \cdot N^g.$$

Moreover, $\mathcal{O}_L^+$ is the increasing union $\bigcup_{N \geqslant 1} U(N)$.

(2) *The positive units $\mathcal{O}_L^{\times +}$ act on $W(N)$ by multiplication. The set $W(N)/\mathcal{O}_L^{\times +}$ is finite and*

$$\big|W(N)/\mathcal{O}_L^{\times +}\big| \leqslant \frac{N^{g \log_2(2g)}}{\log_2(2g)}.$$

Moreover, $\mathcal{O}_L^+$ is the increasing union $\bigcup_{N \geqslant 1} W(N)$.

(3) *Let $\epsilon_1, \ldots, \epsilon_{g-1}$ be a basis for $\mathcal{O}_L^{\times +}$. Let $C = \max\{|\sigma_i(\epsilon_j)^r| \colon\ 1 \leqslant i \leqslant g,\ 1 \leqslant j \leqslant g-1,\ r \in \{\pm 1\}\}$. Then,*

$$W(N) \supseteq U(N) \cdot \mathcal{O}_L^{\times +} \supseteq W\big(C^{-(g-1)^2/2} N\big).$$

Proof. We consider the map $L \to \mathbb{R}^g$, $x \mapsto (\sigma_1(x), \ldots, \sigma_g(x))$, where $\{\sigma_1, \ldots, \sigma_g\} = \mathrm{Hom}(L, \mathbb{R})$. The set $U(N)$ is the intersection of the image of $\mathcal{O}_L$ with the convex body

$$\Delta(gN) := \left\{ (x_1, \ldots, x_g) \colon\ x_i > 0,\ \sum_{i=1}^{g} x_i < gN \right\}.$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

The volume of $\Delta(1)$ is $1/g!$ and so the volume of $\Delta(gN)$ is $(gN)^g/g! \sim (eN)^g/\sqrt{2\pi g}$, by Stirling's formula. On the other hand, $\mathcal{O}_L$ is now a lattice in $\mathbb{R}^g$ whose fundamental parallelotope has volume $d_L^{1/2}$. Since the number of lattice points is approximated by the volume of the convex body divided by the volume of the fundamental parallelotope, (1) follows.

Consider now claim (2). We note that because the narrow class number is 1, $W(N)/\mathcal{O}_L^{\times +}$ is in bijection with integral ideals of norm less than N^g. Consider first the case of ideals of norm p^A for some rational prime p and positive integer A. If $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_a^{e_a}$ in $\mathcal{O}_L$, with residue degrees $f_1, \ldots, f_a$, then an ideal of norm p^A has the form $\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_a^{d_a}$ with $\sum_{i=1}^{a} d_i f_i = A$. It is clear that the number of such ideals, which is equal to the cardinality of the set $\{(d_1, \ldots, d_a) : \sum d_i f_i = A, d_i \in \mathbb{Z}_{\geqslant 0}\}$, is maximized when all $f_i = 1$ and $a = g$. Furthermore, in that case the cardinality is equal to the number of monomials of degree A in the variables $x_1, x_2, \ldots, x_g$, which is $\binom{A+g-1}{g-1}$.

Now, we will use this estimate for $A = 1$, since it is clear that to estimate from above the number of ideals of norm M, we may assume M is square free (roughly speaking, if p^2 is the same size as $q_1 q_2$ then, by the discussion above, p^2 gives us at most $g(g+1)/2$ ideals, while $q_1 q_2$ may contribute g^2 ideals). The number of prime factors of M is at most $\log_2(M)$ and so, all together, the number of ideals of norm M is surely bounded from above by $g^{\log_2(M)} = M^{\log_2(g)}$, and the number of ideals of norm less than N^g is bounded by $\sum_{M=1}^{N^g-1} M^{\log_2(g)} \leqslant \int_{x=1}^{N^g} x^{\log_2(g)} \leqslant N^{g\log_2(2g)}/\log_2(2g)$.

Alternatively, note that since the Dedekind zeta function, $\zeta_L(s) = \sum_{\mathfrak{a} \lhd \mathcal{O}_L} \mathrm{Norm}(\mathfrak{a})^{-s} = \sum a_n n^{-s}$, has, in our case, a simple pole at $s = 1$ with residue $\rho = 2^{g-1} R_L d_L^{-1/2}$, we have $|W(N)/\mathcal{O}_L^{\times +}| = \sum_{n<N^g} a_n \sim 2^{g-1} R_L d_L^{-1/2} N^g$. This asymptotic estimate follows from Tauberian theorems, cf. [dSG, Theorem 4.20], and gives a better estimate (asymptotically only) than the estimate $|W(N)/\mathcal{O}_L^{\times +}| \leqslant \frac{N^{g\log_2(2g)}}{\log_2(2g)}$.

We now prove the third part of the lemma. The inclusion $W(N) \supseteq U(N) \cdot \mathcal{O}_L^{\times +}$ is just the inequality for arithmetic and geometric means. We show the other inclusion. For $x \in L^{\times +}$, let

$$\underline{\sigma}(x) = \big(\log \sigma_1(x), \ldots, \log \sigma_{g-1}(x)\big).$$

Let $\epsilon_1, \ldots, \epsilon_{g-1}$ be a basis for the free abelian group $\mathcal{O}_L^{\times +}$. The vectors $\underline{\sigma}(\epsilon_1), \ldots, \underline{\sigma}(\epsilon_{g-1})$, generate a (full) lattice in $\mathbb{R}^{g-1}$. Suppose that $x \in \mathcal{O}_L^+$, $\mathrm{Norm}(x) = K^g$. Choose $\alpha_i \in \mathbb{R}$ such that

$$\underline{\sigma}(x) + \sum_{i=1}^{g-1} \alpha_i \underline{\sigma}(\epsilon_i) = (\log K, \ldots, \log K).$$

Choose $a_i \in \mathbb{Z}$ such that $|a_i - \alpha_i| \leqslant 1/2$. Let

$$y = x \prod_{i=1}^{g-1} \epsilon_i^{a_i}.$$

We note that $\mathrm{Norm}(y) = \mathrm{Norm}(x)$ and $y \in \mathcal{O}_L^+$. We have

$$\underline{\sigma}(y) = \underline{\sigma}(x) + \sum_{j=1}^{g-1} a_j \underline{\sigma}(\epsilon_j) = (\log K, \ldots, \log K) + \sum_{j=1}^{g-1} (a_j - \alpha_j) \underline{\sigma}(\epsilon_j),$$

whence,

$$\big|\log \sigma_i(y) - \log K\big| \leqslant \frac{1}{2} \sum_{j=1}^{g-1} \big|\log \sigma_i(\epsilon_j)\big|, \quad i = 1, \ldots, g-1.$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Because $\mathrm{Norm}(y) = K^g$, we have $\sigma_g(y) = K^g / \prod_{i=1}^{g-1} \sigma_i(y)$ and so $\log \sigma_g(y) = \log K + \sum_{i=1}^{g-1} (\log K - \log \sigma_i(y))$. This gives the estimate

$$\log \sigma_g(y) \leqslant \log K + \frac{1}{2} \sum_{i,j=1}^{g-1} \left| \log \sigma_i(\epsilon_j) \right|.$$

Let $C = \max\{|\sigma_i(\epsilon_j)^r| :\ 1 \leqslant i \leqslant g,\ 1 \leqslant j \leqslant g-1,\ r \in \{\pm 1\}\}$. We find that $\sigma_i(y) \leqslant K \cdot C^{(g-1)/2}$ for $i = 1, \ldots, g-1$ and $\sigma_g(y) \leqslant K \cdot C^{(g-1)^2/2}$. Therefore, $\frac{1}{g} \mathrm{Tr}(y) \leqslant K \cdot C^{(g-1)^2/2}$. It thus follows that

$$W(K) \subseteq U\left(C^{(g-1)^2/2} K\right) \cdot \mathcal{O}_L^{\times +}. \qquad \square$$

3. Statement of the theorem

Let L be a totally real field of degree g over $\mathbb{Q}$ and of strict class number one. Let p be a rational prime which is unramified in L.

Definition 3.1. Let $N(p)$ be the minimal integer such that for any two L-superspecial abelian varieties $\underline{A}$, $\underline{B}$ in characteristic p there is an $\mathcal{O}_L$-isogeny $f : \underline{A} \to \underline{B}$ with $\|f\|_{\underline{A},\underline{B}} \leqslant N(p)$, where

$$\|f\|_{\underline{A},\underline{B}} = [f, f]_{\underline{A},\underline{B}} = 2\,\mathrm{Tr}_{L/\mathbb{Q}} \deg_{L,\underline{A},\underline{B}}(f),$$

in the notation of Lemma 2.2.

Remark 3.2. Note that if $\underline{A}$, $\underline{B}$ are supersingular elliptic curves, $L = \mathbb{Q}$ and $\|f\|_{\underline{A},\underline{B}}$ is twice the usual degree of the isogeny f.

Let f, g be two real valued functions defined on an unbounded subset of $\mathbb{R}^+$ (such as the prime numbers). We use the notation

$$f(x) \lesssim g(x),$$

if $\limsup_{x \to \infty} f(x)/g(x) \leqslant 1$.

Theorem 3.3. *The following hold*:

(1) *One has*

$$\left((2g)!\right)^{1/(2g)} \pi^{-1} \cdot \sqrt{p} \lesssim N(p) \leqslant 2^2 d_L^{2/g} \cdot \left((2g)!\right)^{1/(2g)} \pi^{-1} \cdot \sqrt{p},$$

where for the lower bound on $N(p)$ we assume p is large enough; for example, that $p > 2^2 d_L^{2/g} ((2g)!)^{1/(2g)} \pi^{-1} p^{1/2}$. In particular, any two L-superspecial abelian varieties $\underline{A}$, $\underline{B}$, in characteristic p are isogenous by an isogeny f of degree less or equal to $d_L^2 p^{g/2}$, where by the degree of f we mean the rank of the finite group scheme $\mathrm{Ker}(f)$ *(it is equal to* $\mathrm{Norm}_{L/\mathbb{Q}} \deg_L(f)$*).*

(2) *Let $\underline{A}$ be an L-superspecial abelian variety in characteristic p. Let μ_2 be the second successive minima (in the sense defined below) of the gauge function* $\mathrm{End}_{\mathcal{O}_L}(\underline{A}) \to \mathbb{R}$ *given by $f \mapsto \|f\|_{\underline{A}}^{1/2}$. Then $\mu_2^2 \leqslant 2^{8/3} d_L^{8/3g} ((2g)!)^{2/3g} \pi^{-4/3} p^{2/3}$. In fact, there exists an element f of* $\mathrm{End}_{\mathcal{O}_L}(A)$*, which is not in $\mathcal{O}_L$, such that*

$$\|f\|_{\underline{A}} \leqslant 2^{8/3} d_L^{8/3g} \left((2g)!\right)^{2/3g} \pi^{-4/3} p^{2/3}.$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Remark 3.4. Stirling's formula says that there is a continuous function $\eta : (0, \infty) \to \mathbb{R}$ such that $0 < \eta(x) < \frac{1}{12x}$ and

$$\Gamma(x) = \sqrt{2\pi} \cdot x^{x-1/2} e^{-x} e^{\eta(x)}.$$

Using the formula for $x = n$ and that $n! = n \cdot \Gamma(n)$, we find that $n! \leqslant \sqrt{2\pi} \cdot n^{n+1/2} e^{-n} e^{1/(12n)}$ and so that

$$(2g)! \leqslant 2^{2g+1} \pi^{1/2} g^{2g+1/2} e^{-2g} e^{1/24}. \tag{3.1}$$

Therefore, $2^2 d_L^{2/g} ((2g)!)^{1/(2g)} \pi^{-1} \leqslant 2^{7/2} \pi^{-3/4} e^{-47/48} d_L^{2/g} g^{1+1/(4g)} \leqslant 2^{7/2} \pi^{-3/4} e^{1/(4e)-47/48} d_L^{2/g} g$. One then concludes that

$$2^2 d_L^{2/g} \big((2g)!\big)^{1/(2g)} \pi^{-1} < 2 d_L^{2/g} g.$$

Thus, the assumption $p > 2^2 d_L^{2/g} ((2g)!)^{1/(2g)} \pi^{-1} p^{1/2}$, appearing in part (1) of the theorem, follows from the simpler inequality

$$p \geqslant 4 \cdot d_L^{4/g} g^2.$$

Similar arguments allow one to get in part (1) that

$$N(p) \leqslant 2 d_L^{2/g} g \sqrt{p},$$

and in part (2) that $\mu_2^2 \leqslant (2 d_L^2 g \sqrt{p})^{4/3}$ and so the existence of an isogeny f with

$$\|f\|_{\underline{A}} \leqslant \big(2 d_L^2 g \sqrt{p}\big)^{4/3}.$$

4. Applications

Before proving the theorem we provide some applications.

4.1. CM lifting

Let $\underline{A}$ be an L-superspecial abelian variety. For example, when $L = \mathbb{Q}$, this means that A is a supersingular elliptic curve. It is a question of some interest to examine the CM lifts of $\underline{A}$.

Nicole proved that for p unramified in L, $\mathrm{End}_{\mathcal{O}_L}(\underline{A})$ is an Eichler order of discriminant p in the quaternion algebra $\mathrm{End}_{\mathcal{O}_L}(\underline{A}) \otimes_{\mathcal{O}_L} L \cong B_{p,L}$ and, conversely, any such order arises this way. He called such orders "superspecial."

Let $\alpha \in \mathrm{End}_{\mathcal{O}_L}(A)$ be an endomorphism not in $\mathcal{O}_L$. Then the order $\mathcal{O}_L[\alpha]$ is a relatively quadratic imaginary order, i.e., $\mathcal{O}_L[\alpha] \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM field whose totally real maximal subfield is L. The discriminant of this order relative to $\mathcal{O}_L$ is the $\mathcal{O}_L$-ideal generated by $\mathrm{Tr}(\alpha)^2 - 4\,\mathrm{Norm}(\alpha)$, a totally negative element of $\mathcal{O}_L$. We therefore begin by examining orders in quadratic extensions of L.

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

4.1.1. Relative quadratic orders

We consider orders $\mathcal{O}$ in quadratic extensions K/L that contain $\mathcal{O}_L$; those shall be called $\mathcal{O}_L$-*orders*. As before, $\mathcal{O}_L$ is assumed to have strict class number one.

Lemma 4.1. *Quadratic orders enjoy the following properties*:

(1) *Let K/L be a quadratic field extension; $\mathcal{O}_K = \mathcal{O}_L[\alpha] = \mathcal{O}_L \oplus \mathcal{O}_L\alpha$ for some $\alpha \in K$. Any $\mathcal{O}_L$-order of K is of the form $\mathcal{O}_L[m\alpha]$ for some $m \in \mathcal{O}_L, m \neq 0$. This element m is unique up to units of $\mathcal{O}_L$. The conductor of the order $\mathcal{O}_L[m\alpha]$ is the principal $\mathcal{O}_K$-ideal $m\mathcal{O}_K$.*
(2) *The map associating to a quadratic $\mathcal{O}_L$-order (in some quadratic extension K/L) its discriminant, an element of $\mathcal{O}_L/\mathcal{O}_L^{\times,2}$, is a well defined injection from the set of quadratic $\mathcal{O}_L$-orders into $\mathcal{O}_L/\mathcal{O}_L^{\times,2}$.*
(3) *Let $\beta \in \mathcal{O}_K, \beta \notin L$. Then $\mathcal{O}_L[\beta]$ is an order of discriminant $-\operatorname{Norm} f'_\beta(\beta)$ and conductor m, where f_β is the minimal polynomial of β over L and where $m^2 = \operatorname{Norm} f'_\beta(\beta)/\operatorname{Norm} f'_\alpha(\alpha)$.*

Proof. One can prove that the conductor of a quadratic order is always an ideal of $\mathcal{O}_L$, augmented to $\mathcal{O}_K$. That is, an ideal of the form $m\mathcal{O}_K$ for some $m \in \mathcal{O}_L$. Clearly, $\mathcal{O}_L[m\alpha] = \mathcal{O}_L + m\mathcal{O}_K$ is the minimal $\mathcal{O}_L$-order of conductor $m\mathcal{O}_K$. It is also the unique $\mathcal{O}_L$-order of that conductor because if R is an $\mathcal{O}_L$-order of conductor $m\mathcal{O}_K$ then $R/m\mathcal{O}_K \subset \mathcal{O}_K/m\mathcal{O}_K = \mathcal{O}_L/m\mathcal{O}_L + \mathcal{O}_L/m\mathcal{O}_L\alpha$. It is not hard to see that $R/m\mathcal{O}_K$ must have the form $\mathcal{O}_L/m\mathcal{O}_L + n\mathcal{O}_L/m\mathcal{O}_L\alpha$, where $n|m$ is an element of $\mathcal{O}_L$. Thus, R is of the form $\mathcal{O}_L + n\mathcal{O}_L\alpha = \mathcal{O}_L[n\alpha]$. Since the conductor of R is $m\mathcal{O}_K$ we must have $n \sim m$. Clearly m is unique up to units.

To prove the second part, we note that the discriminant of the order $\mathcal{O}_L[m\alpha]$ is $D = -m^2 \operatorname{Norm} f'(\alpha)$ where f is the minimal polynomial of α; it is well defined up to $\mathcal{O}_L^{\times,2}$. In particular, $K = L(\sqrt{D})$. This shows that the discriminant determines the order: it is the order of conductor equal to a square root of $D/\operatorname{Norm} f'(\alpha)$ where α is chosen so that $\mathcal{O}_K = \mathcal{O}_L[\alpha]$ and f is the minimal polynomial of α over L.

The third part is clear. □

Corollary 4.2. *The quadratic $\mathcal{O}_L$-orders in CM fields are classified by their discriminants that are totally negative elements of $\mathcal{O}_L/\mathcal{O}_L^{\times,2} = \mathcal{O}_L/\mathcal{O}_L^{\times+}$.*

The next proposition deals with CM lifts of L-superspecial varieties, the key being the existence of lifts with bounded discriminant.

Proposition 4.3. *Let $\underline{A}$ be an L-superspecial abelian variety over $\overline{\mathbb{F}}_p$, p unramified in L. Then $\underline{A}$ can be CM lifted, namely there exists an $\mathcal{O}_L$-principally polarized abelian variety $\underline{\mathscr{A}}$ over a dvr $(R, \mathfrak{m}_R)$, R a finite extension of $W(\overline{\mathbb{F}}_p)$, reducing to $\underline{A}$ and having CM. Moreover,* $\operatorname{End}(\underline{\mathscr{A}})$ *contains a quadratic CM order with discriminant $-m$, where m lies in $U(2^{11/3} d_L^{8/3g}((2g)!)^{2/3g}\pi^{-4/3}g^{-1}p^{2/3}) \subseteq U((2^7 g d_L^8 p^2)^{\frac{1}{3}})$.*

Proof. Results about CM lifting proven in [GL,Yu] allow us to reduce the considerations to finding such an order in $\operatorname{End}_{\mathcal{O}_L}(\underline{A})$. We appeal therefore to the second part of our theorem that says that there exists an element β of $\operatorname{End}_{\mathcal{O}_L}(A)$, which is not in $\mathcal{O}_L$, such that $\operatorname{Tr}_{L/\mathbb{Q}} \deg_L(\beta) \leqslant 2^{5/3} d_L^{8/3g}((2g)!)^{2/3g}\pi^{-4/3}p^{2/3}$. Since $B_{p,L}$ is ramified at all infinite places, the order $\mathcal{O}_L[\beta]$ is an order of a CM field; its discriminant is $-m$, where $m = \operatorname{Norm} f'_\beta(\beta)$, in the notation of Lemma 4.1. The element m is totally positive and, writing $f(x) = x^2 - (\beta + \bar{\beta})x + \deg_L(\beta)$, we have $m = 4\deg_L(\beta) - (\beta + \bar{\beta})^2$. Thus, $m \leqslant 4\deg_L(\beta)$ in any real embedding. It follows that $\frac{1}{g}\operatorname{Tr}_{L/\mathbb{Q}}(m) \leqslant \frac{4}{g}\operatorname{Tr}_{L/\mathbb{Q}} \deg_L(\beta) \leqslant 2^{11/3} d_L^{8/3g}((2g)!)^{2/3g}\pi^{-4/3}g^{-1}p^{2/3}$. For the inclusion $U(2^{11/3} d_L^{8/3g}((2g)!)^{2/3g}\pi^{-4/3}g^{-1}p^{2/3}) \subseteq U((2^7 g d_L^8 p^2)^{\frac{1}{3}})$, cf. Remark 3.4. □

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

4.2. Coefficients of certain theta series

Let $\underline{A}$, $\underline{B}$, be two L-superspecial abelian varieties. To the quadratic $\mathcal{O}_L$-module $(\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B}), \deg_{L,\underline{A},\underline{B}}(\cdot))$ one can associate a theta series:

$$\Theta_{\underline{A},\underline{B}}(q) = \sum_{\nu \in \mathcal{O}_L^+ \cup \{0\}} a(\nu) \cdot q^{\nu},$$

which is a Hilbert modular form of weight 2 for the group

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(L) \colon\ a, d \in \mathcal{O}_L,\ b \in D_L^{-1},\ c \in pD_L \right\}.$$

Here $a(\nu) = a_{\underline{A},\underline{B}}(\nu)$ are the representation numbers of $\deg_{L,\underline{A},\underline{B}}(\cdot))$ (see [Eic, Theorem 1], cf. [Nic, §2.6]). It is easy to see that $a(\nu) = a(\epsilon\nu)$ for any $\epsilon \in \mathcal{O}_L^{\times +} = \mathcal{O}_L^{\times,2}$ and so that $\Theta_{\underline{A},\underline{B}}$ is independent of the choice of $\mathcal{O}_L$-polarizations on $\underline{A}$, $\underline{B}$. We remark that the group $\Gamma_0(p)$ as defined here is the one appearing naturally in the theory and corresponds to classifying principally polarized abelian varieties with RM (see, e.g., [Gor, Corollary 2.19]). It is conjugate to that subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_L)$ such that $c \in p\mathcal{O}_L$.

One would like to know when we first get a nonzero coefficient in $\Theta_{\underline{A},\underline{B}}(q)$. The use of the sets $U(N)$ makes that precise and we deduce the following:

Corollary 4.4. *For any $\underline{A}$, $\underline{B}$ the following holds: For some $\nu \in U(d_L^{2/g}\sqrt{p})$ we have $a_{\underline{A},\underline{B}}(\nu) \neq 0$.*

Proof. By the first part of the theorem, we have a non-zero element $f \in \mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ such that $2\,\mathrm{Tr}_{L/\mathbb{Q}} \deg_{L,\underline{A},\underline{B}}(f) \leqslant 2^2 d_L^{2/g} (2g!)^{1/2g} \pi^{-1} \sqrt{p}$. Let $\nu = \deg_{L,\underline{A},\underline{B}}(f)$. Then, making use of Eq. (3.1) and simple estimates such as $g^{1/4g} \leqslant e^{(1/4e)}$ etc., one finds that $\frac{1}{g}\,\mathrm{Tr}_{L/\mathbb{Q}}(\nu) \leqslant d_L^{2/g}\sqrt{p}$. □

4.3. Denominators required for writing superspecial orders

One knows that $B_{p,L}$ has only finitely many conjugacy classes of orders of bounded discriminant. In particular, finitely many conjugacy classes of maximal orders and finitely many conjugacy classes of superspecial orders. For certain applications one wishes to write a representative for each conjugacy class explicitly (and, more generally, for the ideal classes of each order). For example, this is useful for generating modular forms by theta series and constructing certain Ramanujan graphs whose vertex set is the set of L-superspecial points (cf. [CGL]).

There are well-known examples of maximal orders in $B_{p,\infty}$ specified by a $\mathbb{Z}$-basis. For instance, let $p \equiv 3 \pmod 4$ then $B = (\frac{-1,-p}{\mathbb{Q}})$ is the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified only at p and ∞. It has a basis $\{1, i, j, k\}$ with relations $i^2 = -1$, $j^2 = -p$, $ij = k = -ji$. Let $\mathcal{O} \subset B$ be the $\mathbb{Z}$-span of $\{1, i, \frac{i+j}{2}, \frac{1+k}{2}\}$; it is a maximal order (cf. [Vig, p. 98] for this and other cases).

When we have a $\mathbb{Z}$-basis for a maximal order R of $B_{p,\infty}$ we also get an $\mathcal{O}_L$-basis for the superspecial order $R \otimes_{\mathbb{Z}} \mathcal{O}_L$ in $B_{p,L}$. It is natural then to write other maximal (or superspecial) orders of $B_{p,L}$ relative to this basis. One wants to know how big the denominators might get.

Corollary 4.5. *Let R be a superspecial order with an $\mathcal{O}_L$-basis $e_1, \ldots, e_4$. Let R'' be any other superspecial order. There is superspecial order R' conjugate to R'' and an $\mathcal{O}_L$-basis $e'_1, \ldots, e'_4$ of R' such that the matrix $M = (m_{ij})$ expressing the basis $e'_1, \ldots, e'_4$ in terms of the basis $e_1, \ldots, e_4$ satisfies the following integrality condition: For some $a \in U(d_L^{2/g}\sqrt{p})$ we have $a \cdot m_{ij} \in \mathcal{O}_L, \forall i, j$.*

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Proof. We view R and R'' as the endomorphisms rings of L-superspecial abelian varieties $\underline{A}$ and $\underline{B}$; say $R = \mathrm{End}_{\mathcal{O}_L}(\underline{A})$, $R'' = \mathrm{End}_{\mathcal{O}_L}(\underline{B})$. Let $f \in \mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ be an isogeny, supplied by our theorem, such that $\|f\|_{\underline{A},\underline{B}} \leqslant 2^2 d_L^{2/g}((2g)!)^{1/(2g)}\pi^{-1}p^{1/2}$. Let $a = \deg_L(f)$ (recall that $f^*\lambda_B = a \cdot \lambda_A$). Via f we may embed R'' in $R \otimes_{\mathcal{O}_L} L = B_{p,L}$ by

$$\psi : R'' \to B_{p,L}, \qquad g \mapsto \psi(g) := f^{-1}gf,$$

where by f^{-1} we mean $\frac{1}{\deg_L(f)}\lambda_A^{-1} f^t \lambda_B$. Clearly $a \cdot \psi(g)$ is an endomorphism of A commuting with $\mathcal{O}_L$ and hence lies in R.

Let R' denote the image of ψ. Then $a \cdot R' \subseteq R$ and that means that $a \cdot e_i'$ can be written as an $\mathcal{O}_L$-linear combination of the basis $e_1, \ldots, e_4$. It remains to estimate a. We have $\frac{1}{g}\mathrm{Tr}_{L/\mathbb{Q}}(a) = \frac{1}{2g}\|f\|_{\underline{A},\underline{B}} \leqslant 2 \cdot d_L^{2/g}((2g)!)^{1/(2g)}\pi^{-1}g^{-1}p^{1/2}$. Exactly the same estimate made in the proof of Corollary 4.4 gives $\frac{1}{g}\mathrm{Tr}_{L/\mathbb{Q}}(a) \leqslant d_L^{2/g}\sqrt{p}$. □

5. Proof of the theorem

5.1. The upper bounds

We shall apply a result of Chalk [Cha]: Let G be a gauge function on $\mathbb{R}^{mg}$, that is, a function $G : \mathbb{R}^{mg} \to \mathbb{R}$ satisfying:

(1) $G(x) \geqslant 0, x \in \mathbb{R}^{mg}$ and $G(x) = 0$ implies $x = 0$;
(2) $G(tx) = |t| \cdot G(x), x \in \mathbb{R}^{mg}, t \in \mathbb{R}$;
(3) $G(x + x') \leqslant G(x) + G(x'), x, x' \in \mathbb{R}^{mg}$.

(In modern terminology, G is simply a norm. In fact, our definition here is slightly more restrictive than Chalk's. His definition of a gauge function is what is called today a semi-norm.) Let $\Lambda \subset \mathbb{R}^{mg}$ be the lattice $\phi(\mathcal{O}_L^m)$, where ϕ is induced from the diagonal embedding $L \to \mathbb{R}^g, \ell \mapsto (\sigma_1(\ell), \ldots, \sigma_g(\ell))$. We may identify $\mathbb{R}^{mg}$ with $(L \otimes_{\mathbb{Q}} \mathbb{R})^m$ via this embedding. The discriminant of Λ is $d_L^{m/2}$. Let K be the unit ball of G, $K := \{v \in \mathbb{R}^{mg} : G(v) \leqslant 1\}$.

The successive minima $\mu_1, \ldots, \mu_m$ of G relative to Λ are defined as follows: Let μ_1 be the minimum of G over non-zero elements of Λ. Say $G(\lambda_1) = \mu_1$ for some $\lambda_1 \in \Lambda$. We define the other successive minima by the following recursive procedure. Suppose that $\mu_1, \ldots, \mu_r$ were already defined and we have $G(\lambda_i) = \mu_i$ for some λ_i then μ_{r+1} is the minimum of G taken over all lattice vectors in Λ not lying in the L-linear span of $\lambda_1, \ldots, \lambda_r$. Chalk proves a generalization of Minkowski's theorem (similar generalizations were given previously by H. Weyl):

$$(\mu_1\mu_2\cdots\mu_m)^g \leqslant 2^{mg} d_L^{m/2}\,\mathrm{vol}(K)^{-1}. \tag{5.1}$$

Given two L-superspecial abelian varieties $\underline{A}, \underline{B}$, the quadratic $\mathcal{O}_L$-module $\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ is a torsion-free $\mathcal{O}_L$-module and hence, since $\mathcal{O}_L$ has class number one, free of rank 4. Choose a basis for $\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ over $\mathcal{O}_L$ so that we can identify $\mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ with $\mathcal{O}_L^4$. The bilinear form we consider is given by the $\mathbb{R}$-linear extension of $[\cdot,\cdot]_{\underline{A},\underline{B}}$ and the gauge function G is

$$G(f) = \sqrt{\|f\|_{\underline{A},\underline{B}}}.$$

We remark that G is indeed a gauge function because it is associated with the positive definite quadratic form $\|f\|_{\underline{A},\underline{B}}$—see Lemma 2.2. It follows that the volume of the unit ball of G is $\frac{1}{p^g d_L^2} \cdot \frac{\pi^{2g}}{(2g)!}$ (recall that the volume of the unit ball in $\mathbb{R}^{4g}$ is $\frac{\pi^{2g}}{(2g)!}$). Applying inequality (5.1) for $m = 4$, we get

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

$$\mu_1\mu_2\mu_3\mu_4 \leqslant 2^4 d_L^{4/g}\big((2g)!\big)^{1/g}\pi^{-2}\cdot p. \tag{5.2}$$

We conclude that $\mu_1^2 \leqslant 2^2 d_L^{2/g}((2g)!)^{1/(2g)}\pi^{-1}p^{1/2}$. That means that for every pair of L-superspecial abelian varieties $\underline{A}, \underline{B}$, there is some non-zero $f \in \mathrm{Hom}_{\mathcal{O}_L}(\underline{A}, \underline{B})$ with $\|f\|_{\underline{A},\underline{B}} \leqslant 2^2 d_L^{2/g}((2g)!)^{1/(2g)}\cdot \pi^{-1}p^{1/2}$. This proves the first upper bound. We remark that the use of Chalk's result is not essential here but is made to streamline the presentation. Using Minkowski's theorem gives the same inequality in this case, however, in the applications we make use of Chalk's result to estimate μ_2.

Consider now the degree of such f as an isogeny, namely, consider the rank of the finite group scheme $\mathrm{Ker}(f)$. This degree is equal to $\mathrm{Norm}_{L/\mathbb{Q}}\deg_L(f)$. Making use also of Remark 3.4, we find

$$\begin{aligned}
\mathrm{Norm}_{L/\mathbb{Q}}\deg_L(f) &= \mathrm{Norm}_{L/\mathbb{Q}}\big(\lambda_A^{-1}f^t\lambda_B f\big)\\
&\leqslant \left[\frac{1}{g}\mathrm{Tr}_{L/\mathbb{Q}}\big(\lambda_A^{-1}f^t\lambda_B f\big)\right]^g\\
&= \left[\frac{1}{2g}\|f\|_{\underline{A},\underline{B}}\right]^g\\
&\leqslant (2g)^{-g}N(p)^g\\
&\leqslant (2g)^{-g}\big(2gd_L^{2/g}\sqrt{p}\big)^g\\
&= d_L^2 p^{g/2}.
\end{aligned}$$

We now consider the upper bound in the second part of the theorem. In the case $\underline{A} = \underline{B}$ and the lattice $\mathrm{End}_{\mathcal{O}_L}(\underline{A})$, we use the trivial inequality $\mu_1 \geqslant 1$. It follows from inequality (5.2) that $\mu_2^3 \leqslant 2^4 d_L^{4/g}((2g)!)^{1/g}\pi^{-2}p$ and so that

$$\mu_2^2 \leqslant 2^{8/3}d_L^{8/3g}\big((2g)!\big)^{2/3g}\pi^{-4/3}p^{2/3}.$$

Note also that $\mu_1^2 \leqslant \|\mathrm{Id}_{\underline{A}}\| = 2g$. If μ_1 is achieved for an element $f \notin \mathcal{O}_L$ then certainly we have for an element $f \notin \mathcal{O}_L$ that $\|f\|_{\underline{A}} \leqslant 2^{8/3}d_L^{8/3g}((2g)!)^{2/3g}\pi^{-4/3}p^{2/3}$, because $2g \leqslant 2^{8/3}d_L^{8/3g}((2g)!)^{2/3g}\cdot \pi^{-4/3}p^{2/3}$. If μ_1 is achieved for an element in $\mathcal{O}_L$, then for the element f realizing μ_2 we have the required bound.

This finishes the proof of the upper bounds in the theorem. After developing some tools, we shall prove the lower bound in Section 5.3.

5.2. Subgroup schemes

In this section we estimate the number of subgroups schemes H of given rank of an L-superspecial variety $\underline{A}$, such that $\underline{A}/H$ is also an L-superspecial variety and such that the isogeny $\pi_H : \underline{A} \to \underline{A}/H$ is of polarized abelian varieties with RM. Clearly H has to be $\mathcal{O}_L$-invariant. First remark that if λ is an $\mathcal{O}_L$-polarization of $\underline{A}/H$ then $\pi_H^*\lambda$ is an $\mathcal{O}_L$-linear polarization of $\underline{A}$ and is thus $\mathcal{O}_L$-proportional to λ_A. Thus, the condition about polarizations amounts to the existence of an $\mathcal{O}_L$-principal polarization λ. Using Mumford's theory [Mum, Proposition 1], this is the case if and only if H is $\mathcal{O}_L$-invariant and maximal isotropic in $\mathrm{Ker}(a)$ for some $a \in \mathcal{O}_L$.

Definition 5.1. Suppose that $(\sharp H, p) = 1$. Then H is étale and has a composition series as an $\mathcal{O}_L$-subgroup scheme $H = H_0 \supset H_1 \supset \cdots \supset H_t = \{0\}$, where each H_{i-1}/H_i is (over an algebraic closure) an $\mathcal{O}_L$-module of the form $\mathcal{O}_L/\mathfrak{a}_i$ with $\mathfrak{a}_i$ a prime ideal of $\mathcal{O}_L$ not dividing p. Define the degree of H, $\deg(H)$, to be the ideal of $\mathcal{O}_L$ equal to $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_t$.

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

Lemma 5.2. *Let $H \subset \underline{A}$ be an $\mathcal{O}_L$-invariant group scheme such that $(\sharp H, p) = 1$. Then $\underline{A}/H$ has a principal $\mathcal{O}_L$-polarization λ, unique up to $\mathcal{O}_L^{\times +}$, such that $\pi_H : \underline{A} \to \underline{A}/H$ satisfies $\pi_H^* \lambda = a \cdot \lambda_A$ for some $a \in \mathcal{O}_L$.*

Proof. Suppose that $(\sharp H, p) = 1$. Then, since $\underline{A}$ is principally polarized it satisfies the Rapoport condition (see, for example, [Gor, §5, proof of Lemma 5.5]) and since the isogeny $\underline{A} \to \underline{A}/H$ induces an isomorphism on tangent spaces (with the $\mathcal{O}_L$-structure) it follows that $\underline{A}/H$ also satisfies the Rapoport condition. Since the strict class number of $\mathcal{O}_L$ is one, it follows that $\underline{A}/H$ has a principal $\mathcal{O}_L$-linear polarization as well.

Another proof can be given by induction on the composition series length for $\mathrm{Ker}(\pi_H)$. One then easily reduces to the case where $\mathrm{Ker}(\pi_H)$ is a simple $\mathcal{O}_L$-module killed by a prime ideal $\mathfrak{l} \lhd \mathcal{O}_L$. It is easy to check then that $\mathrm{Ker}(\pi_H)$ is a maximal isotropic subgroup of $\underline{A}[\mathfrak{l}]$. Since $\mathcal{O}_L$ has class number one, $\mathfrak{l} = (a)$ for some $a \in \mathcal{O}_L$ and we are done, by the remarks above. □

Lemma 5.3. *We have $\deg(H) = (\deg_L(\pi_H))$, the principal $\mathcal{O}_L$-ideal generated by $\deg_L(\pi_H)$. In particular, $\mathrm{Norm}_{L/\mathbb{Q}} \deg(H)$ is the ideal of $\mathbb{Z}$ generated by the usual degree of the isogeny $\pi_H : \underline{A} \to \underline{A}/H$, namely, the rank of the group scheme $\mathrm{Ker}(\pi_H)$.*

Proof. Let λ be a principal $\mathcal{O}_L$-polarization on $\underline{A}/H$ making π_H a map of $\mathcal{O}_L$-polarized abelian varieties. Such a polarization exists by Lemma 5.2. Then $\deg(H)$ is the square root of $\deg(\mathrm{Ker}(\pi_H^* \lambda))$, because H is maximal isotropic in $\mathrm{Ker}(\pi_H^* \lambda)$ and so $H \cong [\mathrm{Ker}(\pi_H^* \lambda)/H]^t$ as $\mathcal{O}_L$-group schemes—the duality is with respect to the Mumford pairing and we use $(-)^t$ to denote the dual group scheme. On the other hand, by definition, $\deg_L(\pi_H) = \lambda_A^{-1} \pi_H^t \lambda \pi_H = \lambda_A^{-1} \pi_H^* \lambda = a$, where $\mathrm{Ker}(\pi_H^* \lambda) = A[a]$. So, $\deg(\mathrm{Ker}(\pi_H^* \lambda)) = a^2$. □

Definition 5.4. For an ideal $\mathfrak{a}$ of $\mathcal{O}_L$, relatively prime to p, let $\phi(\mathfrak{a})$ be the number of $\mathcal{O}_L$-subgroup schemes H of $\underline{A}$ such that $\deg(H) = \mathfrak{a}$.

Lemma 5.5. *The function $\phi(\mathfrak{a})$ is a multiplicative function. Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_L$ of residue degree $f(\mathfrak{l})$, then*

$$\phi(\mathfrak{l}^k) = 1 + \mathrm{Norm}(\mathfrak{l}) + \cdots + \mathrm{Norm}(\mathfrak{l})^k = \frac{\ell^{(k+1)f(\mathfrak{l})} - 1}{\ell^{f(\mathfrak{l})} - 1}.$$

Proof. We argue by induction on k. The case $k = 0$ is clear. We use that $A[\mathfrak{l}^k] \cong (\mathcal{O}_L/\mathfrak{l}^k)^2$ as $\mathcal{O}_L$-modules, over an algebraic closure. Since the number of $\mathcal{O}_L$-group schemes of $\deg_L = \mathfrak{l}$ is the number of lines in the $\mathbb{F}_\mathfrak{l} := \mathcal{O}_L/\mathfrak{l}$ vector space $A[\mathfrak{l}] \cong \mathbb{F}_\mathfrak{l}^2$ which is equal to $\sharp \mathbb{P}^1(\mathbb{F}_\mathfrak{l}) = \mathrm{Norm}(\mathfrak{l}) + 1$, we see that the case $k = 1$ holds as well.

Suppose the result for $k - 2 \geqslant 0$. Note that $\phi(\mathfrak{l}^k) - \phi(\mathfrak{l}^{k-2})$ is exactly the number of $\mathcal{O}_L$-subgroup schemes H of $\underline{A}$ such that $\deg_L(H) = \mathfrak{l}^k$ and $H \not\supseteq A[\mathfrak{l}]$. Passing to the Tate module $T_\mathfrak{l}(A)/(\mathfrak{l}^k)$, we see that this is the number of $\mathcal{O}_L$ modules of $(\mathcal{O}_L/\mathfrak{l}^k)^2$ that are cyclic of order $\mathfrak{l}^k$. This number is just the number of elements (a, b) of $(\mathcal{O}_L/\mathfrak{l}^k)^2$ such that at least one of a, b is not divisible by $\mathfrak{l}$, taken modulo $(\mathcal{O}_L/\mathfrak{l}^k)^\times$, a group of order $(\ell^{f(\mathfrak{l})} - 1)\ell^{(k-1)f(\mathfrak{l})}$. On the other hand the number of such generators (a, b) is clearly $\ell^{2kf(\mathfrak{l})} - \ell^{2(k-1)f(\mathfrak{l})}$. We conclude that there are $\frac{\ell^{2kf(\mathfrak{l})} - \ell^{2(k-1)f(\mathfrak{l})}}{(\ell^{f(\mathfrak{l})} - 1)\ell^{(k-1)f(\mathfrak{l})}} = \ell^{kf(\mathfrak{l})} + \ell^{(k-1)f(\mathfrak{l})}$ such $\mathcal{O}_L$-modules and we are done, using the induction hypothesis for $k - 2$. □

Two multiplicative functions agreeing on powers of prime ideals are equal; this gives the following Corollary.

Corollary 5.6. *The function ϕ on ideals prime to p is the function $\sigma_{1,L}$, where $\sigma_{1,L}(\mathfrak{a}) = \sum_{\mathfrak{b}|\mathfrak{a}} \mathrm{Norm}(\mathfrak{b})$.*

5.3. Lower bound

We now come to the proof of the lower bound in Theorem 3.3(1).

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

5.3.1. Counting isomorphism classes

Fix an L-superspecial variety $\underline{A} = (A, \iota_A, \lambda_A)$. Let us denote the isomorphism class of an L-superspecial variety $\underline{B}$ by $[\underline{B}]$, where an isomorphism $f : \underline{B} \to \underline{C}$ is an isomorphism of abelian varieties that is $\mathcal{O}_L$-equivariant and satisfies $f^*\lambda_C = \epsilon \cdot \lambda_B$ for some $\epsilon \in \mathcal{O}_L^{\times +}$. One gets the same isomorphism classes (since we assume L has strict class number one) by taking $\epsilon = 1$.

We want to calculate the cardinality $C(M)$ of the set

$$\left\{[\underline{B}]\colon\ \exists f : \underline{A} \to \underline{B},\ \frac{1}{2}\|f\|_{\underline{A},\underline{B}} \leqslant M\right\},$$

at least for $M < p$. In general, when we write $f : \underline{A} \to \underline{B}$ we mean that f is an isogeny of abelian varieties with RM. It follows that $f^*\lambda_B = \deg_L(f) \cdot \lambda_A$. The lower bound on $N(p)$ will come from the fact that we must have $C(\frac{1}{2}N(p)) \geqslant \hbar$, where $\hbar$ is the number of isomorphism classes of L-superspecial varieties in characteristic p.

Let us fix now representatives for the isomorphism classes of L-superspecial varieties, say,

$$\underline{B}_j = (B_j, \iota_j, \lambda_j), \quad j = 1, \ldots, \hbar.$$

where $\underline{B}_1 = \underline{A}$. Then $C(M)$ is also the cardinality of the set

$$S = \left\{\underline{B}_j\colon\ \exists f : \underline{A} \to \underline{B}_j,\ \frac{1}{2}\|f\|_{\underline{A},\underline{B}} \leqslant M\right\}.$$

(This is just the statement that such an f exists for one member of $[\underline{B}_j]$ if and only if it exists for every member of $[\underline{B}_j]$.)

Now, $\underline{B}_i \cong \underline{B}_j$ if and only if $(B_i, \iota_i) \cong (B_j, \iota_j)$ as abelian varieties with RM. Indeed, the "forgetful direction" is clear; for the other direction use that any $\mathcal{O}_L$-polarization on $\underline{B}_i$ is of the form $a\lambda_i$ for some $a \in \mathcal{O}_L^+$.

Lemma 5.7. *Assuming $M < p$, $C(M) = \#S'$, where*

$$S' = \left\{(B_j, \iota_j)\colon\ \exists f : (A, \iota) \to (B_j, \iota_j),\ \exists \alpha \in \mathcal{O}_L^+ \text{ such that } \deg\big(\mathrm{Ker}(f)\big) = (\alpha),\ \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \leqslant M\right\}.$$

Proof. Given an object $\underline{B}_j \in S$ we have $f : \underline{A} \to \underline{B}_j$ corresponding to it. We take $\alpha = \deg_{L,\underline{A},\underline{B}_j}(f)$, and it follows from Lemma 5.3 that $\deg(\mathrm{Ker}(f)) = (\alpha)$. Conversely, given (B_j, ι_j) in S' and $f : (A, \iota) \to (B_j, \iota_j)$, we have for some $\epsilon \in \mathcal{O}_L^\times$ that $\deg_{L,\underline{A},\underline{B}_j}(\epsilon f) = \alpha$. Then $\epsilon f : \underline{A} \to \underline{B}_j$ and $\frac{1}{2}\|\epsilon f\| \leqslant M$. □

Corollary 5.8. *Assume $M < p$, then*

$$C(M) \leqslant \sum_{\alpha \in \mathcal{O}_L^+,\, \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \leqslant M} \sigma_{1,L}\big((\alpha)\big).$$

Proof. Indeed, since the isomorphism class of (B_j, ι_j), appearing as an element of S' and so as the target of $f : (A, \iota_A) \to (B_j, \iota_j)$, is completely determined by the kernel of f, we get

$$\begin{aligned} C(M) &\leqslant \sharp\big\{H < A\colon\ \mathcal{O}_L\text{-invariant},\ \exists \alpha \in \mathcal{O}_L^+ \text{ s.t. } \deg(H) = (\alpha),\ \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \leqslant M\big\} \\ &= \sum_{\alpha \in \mathcal{O}_L^+,\, \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \leqslant M} \phi\big((\alpha)\big) \\ &= \sum_{\alpha \in \mathcal{O}_L^+,\, \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \leqslant M} \sigma_{1,L}\big((\alpha)\big). \qquad \square \end{aligned} \tag{5.3}$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

We remark that the inequality results from the fact we may have $H_1 \neq H_2$, yet $\underline{A}/H_1 \cong \underline{A}/H_2$ as principally polarized abelian varieties with RM.

5.3.2. Eisenstein series

There is an Eisenstein series $E_{2,L}$ of weight 2 on $\mathrm{SL}_2(\mathcal{O}_L)$, whose Fourier expansion is given by

$$E_{2,L}(z) = 2^{-g}\zeta_L(-1) + \sum_{\nu \in D_L^{-1,+}} \sigma_{1,L}(\nu D_L) q^{\nu} = 2^{-g}\zeta_L(-1) + \sum_{\nu \in \mathcal{O}_L^{+}} \sigma_{1,L}(\nu \mathcal{O}_L) q^{\delta^{-1}\nu}, \quad z \in \mathfrak{H}^g,$$

where $q^{\nu} = \exp(2\pi i \cdot \mathrm{Tr}(\nu z))$, $\mathfrak{H} = \{z \in \mathbb{C}\colon \mathrm{Im}(z) > 0\}$ and δ is a totally positive generator of the different ideal D_L. See, e.g., [vdG, §6]. Consider then the diagonal embedding $\mathfrak{H} \to \mathfrak{H}^g$; via this embedding $E_{2,L}$ pulls back to a modular form B_L on $\mathrm{SL}_2(\mathbb{Z})$ of weight $2g$ and Fourier expansion

$$B_L(q) = 2^{-g}\zeta_L(-1) + \sum_{n=1}^{\infty} \Bigg(\sum_{\{\nu \in \mathcal{O}_L^{+}\colon\ \mathrm{Tr}(\nu)=n\}} \sigma_{1,L}(\nu \mathcal{O}_L) \Bigg) q^n = \sum_{n=0}^{\infty} a(n) q^n.$$

(If $L = \mathbb{Q}$ we define $B_L(q)$ this way as a formal power series; the series is not convergent.) In general, we are not aware of a closed formula expressing B_L in terms of generators for the modular forms of weight $2g$. We therefore make coarser estimates (but see our discussion in Sections 5.4.1, 5.4.2 below for $g \leqslant 3$ and see also [Coh].) We have

$$B_L(q) = 2^{1-g} \cdot \frac{\zeta_L(-1)}{\zeta_{\mathbb{Q}}(1-2g)} E_{2g}(q) + h(q),$$

where $h(q) = \sum_{n=1}^{\infty} a'_n q^n$ is a *cusp* form of weight $2g$ and E_{2g} is the Eisenstein series for $\mathrm{SL}_2(\mathbb{Z})$ of weight $2g$, normalized as

$$E_{2g}(q) = 2^{-1}\zeta_{\mathbb{Q}}(1-2g) + \sum_{n=1}^{\infty} \sigma_{2g-1}(n) q^n.$$

The Fourier coefficients a'_n of $h(q)$ satisfy the bound

$$\sum_{n=1}^{M} |a'_n| \ll M^{g+\frac{1}{2}},$$

where the notation $\alpha(n) \ll \beta(n)$ for functions $\mathbb{N} \to \mathbb{R}_{\geqslant} 0$ means $\alpha(n)/\beta(n) \to 0$ as $n \to \infty$. (This estimate follows, of course, from Deligne's bound, but one needs less. See [Iwa, Corollary 5.2].) Combining Equation 5.3 with the above gives

$$C(M) \leqslant \sum_{n=1}^{M} a_n = 2^{1-g} \cdot \frac{\zeta_L(-1)}{\zeta_{\mathbb{Q}}(1-2g)} \left(\sum_{n=1}^{M} \sigma_{2g-1}(n) \right) + \sum_{n=1}^{M} |a'_n|.$$

Estimates for $\sum_{n=1}^{M} \sigma_k(n)$, $k \geqslant 1$, are classical, see e.g. [Apo, Theorems 3.4, 3.5]:

$$\sum_{n=1}^{M} \sigma_k(n) = \frac{\zeta_{\mathbb{Q}}(1+k)}{1+k} M^{k+1} + \begin{cases} O(M \log M), & k = 1, \\ O(M^k), & k > 1, \end{cases}$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

which, using the functional equation $\zeta_{\mathbb{Q}}(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\pi s/2)\zeta_{\mathbb{Q}}(s)$ (see [Apo, Theorem 12.7]), gives us

$$\sum_{n=1}^{M}\sigma_{2g-1}(n) = \frac{(-1)^g 2^{2g-1}\pi^{2g}}{(2g)!}\cdot\zeta_{\mathbb{Q}}(1-2g)\cdot M^{2g} + \begin{cases} O(M\log M), & g=1,\\ O(M^{2g-1}), & g>1.\end{cases}$$

All together, we have proven the following proposition.

Proposition 5.9. *Let* $C(M) = \sharp\{[\underline{B}]\colon \exists f : \underline{A}\to\underline{B},\ \frac{1}{2}\|f\|_{\underline{A},\underline{B}} \leqslant M\}$ *then, as* $M\to\infty$,

$$C(M) \lesssim \frac{2^g\pi^{2g}}{(2g)!}\cdot(-1)^g\zeta_L(-1)\cdot M^{2g}.$$

Recall that our definition of $N(p)$ allows the use of f with $\|f\|_{\underline{A},\underline{B}} \leqslant N(p)$, or $\frac{1}{2}\|f\|_{\underline{A},\underline{B}} \leqslant \frac{1}{2}N(p)$. Using that $C(\frac{1}{2}N(p)) \geqslant \hbar$, we therefore obtain the following conclusion.

Corollary 5.10. *Let* $\hbar$ *be the number of isomorphism classes of* L*-superspecial abelian varieties in characteristic* p*,* p *unramified in* L*. Then, as* $p\to\infty$,

$$N(p) \gtrsim \frac{\sqrt{2}\cdot((2g)!)^{\frac{1}{2g}}}{\pi}\left(\frac{\hbar}{(-1)^g\zeta_L(-1)}\right)^{\frac{1}{2g}}.$$

5.3.3. Class numbers and mass formulas

Using [Nic], $\hbar$ is the class number of an Eichler order R of discriminant $p\mathcal{O}_L$ in the quaternion algebra $B_{p,L}$ for right R-ideals. This number is of course $\sum_{\mathfrak{a}\in Cl(R)}1$ and is complicated to evaluate in closed form. An easier magnitude is the mass of R,

$$m(R) = \sum_{\mathfrak{a}\in Cl(R)}\frac{1}{[R_\ell(\mathfrak{a})^\times : \mathcal{O}_L^\times]},$$

where $R_\ell(\mathfrak{a})$ is the left order of $\mathfrak{a}$. (We remark, though this is not used in the sequel, that $R_\ell(\mathfrak{a})$ can be identified with the ring of endomorphisms of an L-superspecial variety that commute with $\mathcal{O}_L$.) One knows that

$$m(R) = 2^{1-g}\zeta_L(-1)\times\prod_{\{\mathfrak{p}\lhd\mathcal{O}_L\colon\ f(\mathfrak{p}/p)\equiv 1(2)\}}(1-\mathrm{Norm}_{L/\mathbb{Q}}\mathfrak{p})\prod_{\{\mathfrak{p}\lhd\mathcal{O}_L\colon\ f(\mathfrak{p}/p)\equiv 0\ (2)\}}(1+\mathrm{Norm}_{L/\mathbb{Q}}\mathfrak{p}).$$

(Cf. [Vig, Chapitre V, Corollaire 2.3].) Clearly, $m(R)\leqslant\hbar$.

5.3.4.

Our considerations now imply that

$$\begin{aligned} N(p) &\gtrsim \frac{\sqrt{2}((2g)!)^{1/(2g)}}{\pi}\left(\frac{\hbar}{(-1)^g\zeta_L(-1)}\right)^{1/(2g)}\\ &\geqslant \frac{\sqrt{2}((2g)!)^{1/(2g)}}{\pi}\left(\frac{m(R)}{(-1)^g\zeta_L(-1)}\right)^{1/(2g)}\\ &\geqslant \frac{2^{1/(2g)}((2g)!)^{1/(2g)}}{\pi}\prod_{\mathfrak{p}|p}\left|\mathrm{Norm}(\mathfrak{p})+(-1)^{f(\mathfrak{p}/p)}\right|^{1/(2g)}\end{aligned}$$

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

$$\geqslant 2^{1/(2g)}\big((2g)!\big)^{1/(2g)}\pi^{-1}\sqrt{p-1}$$

$$\gtrsim \frac{(2g)!^{\frac{1}{2g}}}{\pi}\sqrt{p}.$$

This concludes the proof of the lower bound.

5.4. Further remarks

If $g \leqslant 3$ then we can be more precise in identifying the Eisenstein series and more precise in our lower bound.

5.4.1. $g = 1$

In this case the Eisenstein series is not convergent. The whole discussion above simplifies though. Indeed, the number of subgroups of order N, $(N, p) = 1$, of an elliptic curve is $\sigma_1(N)$ and the number of supersingular elliptic curves is about $p/12$ and certainly not smaller than $(p-1)/12$. The bound $N(p)$ is at least the smallest even integer N such that

$$\sum_{n=1}^{N/2}\sigma_1(n) \geqslant \frac{p-1}{12}$$

(because $N(p)$ is twice the degree). Now, for large N we have $\sum_{n=1}^{N/2}\sigma_1(n) \sim \frac{\pi^2}{48}N^2$. One finds that

$$N(p) \gtrsim \frac{2}{\pi}\sqrt{p} \approx 0.63662\sqrt{p}.$$

This matches quite well our upper bound from Theorem 3.3 in the case $g = 1$:

$$N(p) \leqslant \frac{4\sqrt{2}}{\pi}\sqrt{p} \approx 1.8006\sqrt{p}.$$

As above, let p be a prime, $\hbar$ the class number of $B_{p,\infty}$. In Table 1, N is the minimal integer for which there exists an isogeny of degree less or equal to N between any two supersingular elliptic

Table 1

p	$\hbar$	$[\sqrt{p}]$	N	$N/\sqrt{p}$
101	9	10	6	0.600
211	18	15	9	0.600
307	26	18	11	0.611
401	34	20	12	0.600
503	43	22	15	0.682
601	50	25	14	0.560
701	59	26	17	0.654
809	68	28	18	0.643
907	76	30	19	0.633
1009	84	32	20	0.625
2003	168	45	30	0.667
3001	250	55	34	0.618
4001	334	63	44	0.698
5003	418	71	46	0.648
6007	501	78	51	0.654
7001	584	84	56	0.667
8009	668	89	60	0.674
9001	750	95	59	0.621
10007	835	100	70	0.700

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005

curves over $\overline{\mathbb{F}}_p$. Thus $N = \frac{1}{2}N(p)$, but it is more natural to use N in the context of elliptic curves. Because of running time and memory restrictions we did only sample calculations. For $p = 10007$, the total computation time was 22688.710 seconds, total memory usage was 1213.97 MB. The program ran on an Intel Pentium 4, 2.53 GHz, 1 GB memory using MAGMA.

5.4.2. $g = 2, 3$

We do not enter explicit calculations here. The idea is that since the spaces of modular forms on $\mathrm{SL}_2(\mathbb{Z})$ of weight 4 and 6 are one-dimensional, we have $B_L(q) = 2^{1-g} \cdot \frac{\zeta_L(-1)}{\zeta_{\mathbb{Q}}(1-2g)} E_{2g}(q)$. This was used in turn by Siegel to find formulas for $\zeta_L(-1)$. See [Coh].

Acknowledgment

We thank H. Kisilevsky for conversations regarding this project.

References

[Apo] T.M. Apostol, Introduction to Analytic Number Theory, Undergrad. Texts Math., Springer-Verlag, New York, 1976.
[Cha] J.H.H. Chalk, Algebraic lattices, C. R. Math. Acad. Sci. Soc. R. Can. 2 (1980/1981) 5–10.
[CGL] D.X. Charles, E.Z. Goren, K.E. Lauter, Families of Ramanujan graphs and quaternion algebras, in: AMS-CRM Volume "Groups and Symmetries" in Honor of John McKay, in press.
[Coh] H. Cohen, Variations sur un thème de Siegel et Hecke, Acta Arith. 30 (1976/1977) 63–93.
[Eic] M. Eichler, On theta functions of real algebraic number fields, Acta Arith. 33 (3) (1977) 269–292.
[dSG] M. du Sautoy, F. Grunewald, Analytic properties of zeta functions and subgroup growth, Ann. of Math. (2) 152 (3) (2000) 793–833.
[vdG] G. van der Geer, Hilbert Modular Surfaces, Ergeb. Math. Grenzgeb. (3), vol. 16, Springer-Verlag, Berlin, 1988.
[Gor] E.Z. Goren, Lectures on Hilbert Modular Varieties and Modular Forms. With the Assistance of Marc-Hubert Nicole, CRM Monogr. Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002.
[GL] E.Z. Goren, K.E. Lauter, Class invariants for quartic CM fields, Ann. Inst. Fourier (Grenoble) 57 (2) (2007) 457–480.
[Iwa] H. Iwaniec, Topics in Classical Automorphic Forms, Grad. Stud. Math., vol. 17, Amer. Math. Soc., Providence, RI, 1997.
[Mes] J.-F. Mestre, La méthode des graphes. Exemples et applications, in: Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields, Katata, 1986, Nagoya Univ., Nagoya, 1986, pp. 217–242.
[Mum] D. Mumford, On the equations defining abelian varieties, I. Invent. Math. 1 (1966) 287–354.
[Nic] M.-H. Nicole, Superspecial abelian varieties, Theta series and the Jacquet–Langlands correspondence, PhD thesis, McGill University, 2005.
[Piz] A.K. Pizer, Ramanujan graphs, in: Computational Perspectives on Number Theory, Chicago, IL, 1995, in: AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 159–178.
[Vig] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math., vol. 800, Springer-Verlag, Berlin, 1980.
[Yu] C.-F. Yu, The isomorphism classes of abelian varieties of CM-type, J. Pure Appl. Algebra 187 (1–3) (2004) 305–319.

Please cite this article in press as: E.Z. Goren, K.E. Lauter, The distance between superspecial abelian varieties with real multiplication, J. Number Theory (2008), doi:10.1016/j.jnt.2008.07.005