Journal of Algebra 322 (2009) 3733–3743

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Mass formula for supersingular abelian surfaces

Chia-Fu Yu [a,b], Jeng-Daw Yu [c,*]

[a] Institute of Mathematics, Academia Sinica, Academia Rd. Sec. 2, Nankang, Taipei, Taiwan
[b] NCTS (Taipei Office), Taiwan
[c] Department of Mathematics, National Taiwan University, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 3 February 2009
Available online 1 September 2009
Communicated by Laurent Moret-Bailly

Keywords:
Mass formula
Hecke orbits
Abelian surfaces

ABSTRACT

We show a mass formula for arbitrary supersingular abelian surfaces in characteristic p.

1. Introduction

In [1] Chai studied prime-to-p Hecke correspondences on Siegel moduli spaces in characteristic p and proved a deep geometric result about ordinary ℓ-adic Hecke orbits for any prime $\ell \neq p$. Recently Chai and Oort gave a complete answer to what this ℓ-adic Hecke orbit can be; see [2]. In this paper we study the arithmetic aspect of supersingular ℓ-adic Hecke orbits in the Siegel moduli spaces, the extreme situation opposite to the ordinary case. In the case of genus $g = 2$, we give a complete answer to the size of supersingular Hecke orbits.

Let p be a rational prime number and $g \geqslant 1$ be a positive integer. Let $N \geqslant 3$ be a prime-to-p positive integer. Choose a primitive Nth root of unity $\zeta_N \in \overline{\mathbb{Q}} \subset \mathbb{C}$ and fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. Let $\mathcal{A}_{g,1,N}$ denote the moduli space over $\overline{\mathbb{F}_p}$ of g-dimensional principally polarized abelian varieties with a symplectic level-N structure with respect to ζ_N. Let k be an algebraically closed field of characteristic p. For each point $x = \underline{A}_0 = (A_0, \lambda_0, \eta_0)$ in $\mathcal{A}_{g,1,N}(k)$ and a prime number $\ell \neq p$, the ℓ-adic Hecke orbit $\mathcal{H}_\ell(x)$ is defined to be the countable subset of $\mathcal{A}_{g,1,N}(k)$ that consists of points $\underline{A}$ such that there is an ℓ-quasi-isogeny from A to A_0 that preserves the polarizations (see Section 2 for definitions). It is proved in Chai [1, Proposition 1] that the ℓ-adic Hecke orbit $\mathcal{H}_\ell(x)$ is finite if and only if x

* Corresponding author.
E-mail addresses: chiafu@math.sinica.edu.tw (C.-F. Yu), jdyu@math.ntu.edu.tw (J.-D. Yu).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.08.008

is supersingular. Recall that an abelian variety A over k is *supersingular* if it is isogenous to a product of supersingular elliptic curves; A is *superspecial* if it is isomorphic to a product of supersingular elliptic curves. A natural question is whether it is possible to calculate the size of a supersingular Hecke orbit. The answer is affirmative, provided that we know its underlying p-divisible group structure explicitly, through the calculation of geometric mass formulas (see Section 2). This is the task of this paper where we examine the p-divisible group structure of some non-superspecial abelian varieties.

Let $x = (A_0, \lambda_0)$ be a g-dimensional supersingular principally polarized abelian varieties over k. Let Λ_x denote the set of isomorphism classes of g-dimensional supersingular principally polarized abelian varieties (A, λ) over k such that there exists an isomorphism $(A, \lambda)[p^\infty] \simeq (A_0, \lambda_0)[p^\infty]$ of the attached quasi-polarized p-divisible groups; it is a finite set (see [7, Theorem 2.1 and Proposition 2.2]). Define the mass $\mathrm{Mass}(\Lambda_x)$ of Λ_x as

$$\mathrm{Mass}(\Lambda_x) := \sum_{(A,\lambda)\in\Lambda_x} \frac{1}{|\mathrm{Aut}(A,\lambda)|}. \tag{1.1}$$

The main result of this paper is computing the geometric mass $\mathrm{Mass}(\Lambda_x)$ for arbitrary x when $g = 2$.

Let $\Lambda^*_{2,p}$ be the set of isomorphism classes of polarized superspecial abelian surfaces (A, λ) with polarization degree $\deg\lambda = p^2$ over $\overline{\mathbb{F}_p}$ such that $\ker\lambda \simeq \alpha_p \times \alpha_p$ (see Section 3.1). For each member (A_1, λ_1) in $\Lambda^*_{2,p}$, the space of degree-p isogenies $\varphi : (A_1, \lambda_1) \to (A, \lambda)$ with $\varphi^*\lambda = \lambda_1$ over k is a projective line $\mathbf{P}^1$ over k. Write $\mathbf{P}^1_{A_1}$ to indicate the space of p-isogenies arising from A_1. This family is studied in Moret-Bailly [6], and also in Katsura and Oort [5]. One defines an $\mathbb{F}_{p^2}$-structure on $\mathbf{P}^1$ using the $W(\mathbb{F}_{p^2})$-structure of M_1 defined by $F^2 = -p$, where M_1 is the covariant Dieudonné module of A_1 and F is the absolute Frobenius. For any supersingular principally polarized abelian surface (A, λ) there exist an (A_1, λ_1) in $\Lambda^*_{2,p}$ and a degree-p isogeny $\varphi : (A_1, \lambda_1) \to (A, \lambda)$ with $\varphi^*\lambda = \lambda_1$. The choice of (A_1, λ_1) and φ may not be unique. However, the degree $[\mathbb{F}_{p^2}(\xi) : \mathbb{F}_{p^2}]$ of the point $\xi \in \mathbf{P}^1_{A_1}(k)$ that corresponds to φ is well defined.

In this paper we prove

Theorem 1.1. *Let $x = (A, \lambda)$ be a supersingular principally polarized abelian surface over k. Suppose that (A, λ) is represented by a pair $(\underline{A}_1, \xi)$, where $\underline{A}_1 \in \Lambda^*_{2,p}$ and $\xi \in \mathbf{P}^1_{A_1}(k)$. Then*

$$\mathrm{Mass}(\Lambda_x) = \frac{L_p}{5760},$$

where

$$L_p = \begin{cases} (p-1)(p^2+1) & \text{if } \mathbb{F}_{p^2}(\xi) = \mathbb{F}_{p^2}, \\ (p^2-1)(p^4-p^2) & \text{if } [\mathbb{F}_{p^2}(\xi) : \mathbb{F}_{p^2}] = 2, \\ (p^2-1)|\mathrm{PSL}_2(\mathbb{F}_{p^2})| & \text{otherwise}. \end{cases}$$

Theorem 1.1 calculates the cardinality of ℓ-adic Hecke orbits $\mathcal{H}_\ell(x)$, as one has (Corollary 2.3)

$$\left|\mathcal{H}_\ell(x)\right| = \left|\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})\right| \cdot \mathrm{Mass}(\Lambda_x).$$

We mention that the function field analogue of Theorem 1.1 where supersingular abelian surfaces are replaced by supersingular Drinfeld modules is established in [10].

This paper is organized as follows. In Section 2 we describe the relationship between supersingular ℓ-adic Hecke orbits and mass formulas. We develop the mass formula for the orbits of certain superspecial abelian varieties. In Section 3 we compute the endomorphism ring of any supersingular abelian surface. The proof of the main theorem is given in the last section.

2. Hecke orbits and mass formulas

Let $g, p, N, \ell, \mathcal{A}_{g,1,N}, k$ be as in the previous section. We work with a slightly bigger moduli space in which the objects are not necessarily equipped with principal polarizations. It is indeed more convenient to work in this setting. Let $\mathcal{A}_{g,p^*,N} = \bigcup_{m \geqslant 1} \mathcal{A}_{g,p^m,N}$ be the moduli space over $\overline{\mathbb{F}_p}$ of g-dimensional abelian varieties together with a p-power degree polarization and a symplectic level-N structure with respect to ζ_N. Write $\mathcal{A}_{g,p^*}$ for the moduli stack over $\overline{\mathbb{F}_p}$ that parametrizes g-dimensional p-power degree polarized abelian varieties. For any point $x = \underline{A}_0 = (A_0, \lambda_0, \eta_0)$ in $\mathcal{A}_{g,p^*,N}(k)$, the ℓ-adic Hecke orbit $\mathcal{H}_\ell(x)$ is defined to be the countable subset of $\mathcal{A}_{g,p^*,N}(k)$ that consists of points $\underline{A}$ such that there is an ℓ-quasi-isogeny from A to A_0 that preserves the polarizations. An ℓ-quasi-isogeny from A to A_0 is an element $\varphi \in \mathrm{Hom}(A, A_0) \otimes \mathbb{Q}$ such that $\ell^m \varphi$, for some integer $m \geqslant 0$, is an isogeny of ℓ-power degree.

2.1. Group theoretical interpretation

Assume that x is supersingular. Let G_x be the automorphism group scheme over $\mathbb{Z}$ associated to $\underline{A}_0$; for any commutative ring R, the group of its R-valued points is defined by

$$G_x(R) = \left\{h \in \left(\mathrm{End}_k(A_0) \otimes R\right)^\times \;\middle|\; h'h = 1\right\},$$

where $h \mapsto h'$ is the Rosati involution induced by λ_0. Let $\Lambda_{x,N} \subset \mathcal{A}_{g,p^*,N}(k)$ be the subset consisting of objects (A, λ, η) such that there is an isomorphism ϵ_p: $(A, \lambda)[p^\infty] \simeq (A_0, \lambda_0)[p^\infty]$ of quasi-polarized p-divisible groups. Since ℓ-quasi-isogenies do not change the associated p-divisible group structure, we have the inclusion $\mathcal{H}_\ell(x) \subset \Lambda_{x,N}$.

Proposition 2.1. *Notations and assumptions as above.*

(1) *There is a natural isomorphism $\Lambda_{x,N} \simeq G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f)/K_N$ of pointed sets, where K_N is the stabilizer of η_0 in $G_x(\widehat{\mathbb{Z}})$.*
(2) *One has $\mathcal{H}_\ell(x) = \Lambda_{x,N}$.*

Proof. (1) This is a special case of [7, Theorem 2.1 and Proposition 2.2]. We sketch the proof for the reader's convenience. Let $\underline{A}$ be an element in $\Lambda_{x,N}$. As A is supersingular, there is a quasi-isogeny $\varphi: A_0 \to A$ such that $\varphi^*\lambda = \lambda_0$. For each prime q (including p and ℓ), choose an isomorphism ϵ_q: $\underline{A}_0[q^\infty] \simeq \underline{A}[q^\infty]$ of q-divisible groups compatible with polarizations and level structures. There is an element $\phi_q \in G_x(\mathbb{Q}_q)$ such that $\varphi\phi_q = \epsilon_q$ for all q. The map $\underline{A} \mapsto [(\phi_q)]$ gives a well-defined map from $\Lambda_{x,N}$ to $G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f)/K_N$. It is not hard to show that this is a bijection.

(2) The inclusion $\mathcal{H}_\ell(x) \subset \Lambda_{x,N}$ under the isomorphism in (1) is given by

$$\left[G_x(\mathbb{Q}) \cap G_x\left(\widehat{\mathbb{Z}}^{(\ell)}\right)\right] \backslash \left[G_x(\mathbb{Q}_\ell) \times G_x\left(\widehat{\mathbb{Z}}^{(\ell)}\right)\right] / K_N \subset G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f)/K_N.$$

Since the group G_x is semi-simple and simply-connected, the strong approximation shows that $G_x(\mathbb{Q}) \subset G_x(\mathbb{A}_f^{(\ell)})$ is dense. The equality then follows immediately. $\square$

Corollary 2.2. *Let $\underline{A}_i = (A_i, \lambda_i, \eta_i)$, $i = 1, 2$, be two supersingular points in $\mathcal{A}_{g,p^*,N}(k)$. Suppose that there is an isomorphism of the associated quasi-polarized p-divisible groups. Then for any prime $\ell \nmid pN$ there is an ℓ-quasi-isogeny $\varphi: A_1 \to A_2$ which preserves the polarizations and level structures.*

Proof. This follows from the strong approximation property for G_x that any element ϕ in the double space $G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f)/K_N$ can be represented by an element in $G_x(\mathbb{Q}_\ell) \times K_N^{(\ell)}$, where $K_N^{(\ell)} \subset G_x(\widehat{\mathbb{Z}}^{(\ell)})$ is the prime-to-ℓ component of K_N. $\square$

Recall that we denote by Λ_x the set of isomorphism classes of g-dimensional supersingular p-power degree polarized abelian varieties (A,λ) over k such that there is an isomorphism $(A,\lambda)[p^\infty] \simeq (A_0,\lambda_0)[p^\infty]$, and define the mass $\mathrm{Mass}(\Lambda_x)$ of Λ_x as

$$\mathrm{Mass}(\Lambda_x) := \sum_{(A,\lambda)\in\Lambda_x} \frac{1}{|\operatorname{Aut}(A,\lambda)|}.$$

Similarly, we define

$$\mathrm{Mass}(\Lambda_{x,N}) := \sum_{(A,\lambda,\eta)\in\Lambda_{x,N}} \frac{1}{|\operatorname{Aut}(A,\lambda,\eta)|}.$$

Corollary 2.3. *One has $|\mathcal{H}_\ell(x)| = |\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \cdot \mathrm{Mass}(\Lambda_x)$.*

Proof. This follows from

$$\bigl|\mathcal{H}_\ell(x)\bigr| = |\Lambda_{x,N}| = \mathrm{Mass}(\Lambda_{x,N}) = \bigl|G_x(\mathbb{Z}/N\mathbb{Z})\bigr| \cdot \mathrm{Mass}(\Lambda_x)$$

and $|G_x(\mathbb{Z}/N\mathbb{Z})| = |\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})|$. $\square$

2.2. Relative indices

Write G' for the automorphism group scheme associated to a principally polarized superspecial point x_0. The group $G'_{\mathbb{Q}}$ is unique up to isomorphism. This is an inner form of Sp_{2g} which is "twisted at p and ∞" (cf. Section 3.1 below). For any supersingular point $x \in \mathcal{A}_{g,p*}(k)$, we can regard $G_x(\mathbb{Z}_p)$ as an open compact subgroup of $G'(\mathbb{Q}_p)$ through a choice of a quasi-isogeny of polarized abelian varieties between x_0 and x. Another choice of quasi-isogeny gives rise to a subgroup which differs from the previous one by the conjugation of an element in $G'(\mathbb{Q}_p)$. For any two open compact subgroups U_1, U_2 of $G'(\mathbb{Q}_p)$, we put

$$\mu(U_1/U_2) := [U_1\colon U_1 \cap U_2][U_2\colon U_1 \cap U_2]^{-1}.$$

Proposition 2.4. *Let x_1, x_2 be two supersingular points in $\mathcal{A}_{g,p^*}(k)$. Then one has*

$$\mathrm{Mass}(\Lambda_{x_2}) = \mathrm{Mass}(\Lambda_{x_1}) \cdot \mu\bigl(G_{x_1}(\mathbb{Z}_p)/G_{x_2}(\mathbb{Z}_p)\bigr).$$

Proof. See Theorem 2.7 of [7]. $\square$

2.3. The superspecial case

Let Λ_g denote the set of isomorphism classes of g-dimensional principally polarized superspecial abelian varieties over $\overline{\mathbb{F}_p}$. When $g = 2D > 0$ is even, we denote by Λ^*_{g,p^D} the set of isomorphism classes of g-dimensional polarized superspecial abelian varieties (A,λ) of degree p^{2D} over $\overline{\mathbb{F}_p}$ satisfying $\ker\lambda = A[F]$, where $F: A \to A^{(p)}$ is the relative Frobenius morphism on A. Write

$$M_g := \sum_{(A,\lambda)\in\Lambda_g} \frac{1}{|\operatorname{Aut}(A,\lambda)|}, \qquad M^*_g := \sum_{(A,\lambda)\in\Lambda^*_{g,p^D}} \frac{1}{|\operatorname{Aut}(A,\lambda)|}$$

for the mass attached to the finite sets Λ_g and Λ^*_{g,p^D}, respectively.

Theorem 2.5. *Notations as above.*

(1) *For any positive integer g, one has*

$$M_g = \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^{g} \zeta(1-2k) \right\} \cdot \prod_{k=1}^{g} \{p^k + (-1)^k\},$$

where $\zeta(s)$ is the Riemann zeta function.

(2) *For any positive even integer $g = 2D$, one has*

$$M_g^* = \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^{g} \zeta(1-2k) \right\} \cdot \prod_{k=1}^{D} (p^{4k-2} - 1).$$

Proof. (1) This is due to Ekedahl and Hashimoto and Ibukiyama (see [3, p. 159] and [4, Proposition 9], also cf. [8, Section 3]).

(2) See Theorem 6.6 of [8]. □

Corollary 2.6. *One has*

$$M_2 = \frac{(p-1)(p^2+1)}{5760} \quad \text{and} \quad M_2^* = \frac{(p^2-1)}{5760}.$$

Proof. This follows from Theorem 2.5 and the basic fact $\zeta(-1) = \frac{-1}{12}$ and $\zeta(-3) = \frac{1}{120}$. This is also obtained in Katsura and Oort [5, Theorem 5.1 and Theorem 5.2] by a method different from above. □

Remark 2.7. Proposition 2.1 is generalized to the moduli spaces of PEL-type in [9], with modification due to the failure of the Hasse principle.

3. Endomorphism rings

In this section we treat the endomorphism rings of supersingular abelian surfaces.

3.1. Basic setting

For any abelian variety A over k, the *a-number* $a(A)$ of A is defined by

$$a(A) := \dim_k \operatorname{Hom}(\alpha_p, A).$$

Here α_p is the kernel of the Frobenius morphism $F: \mathbb{G}_a \to \mathbb{G}_a$ on the additive group. Denote by $\mathcal{DM}$ the category of Dieudonné modules over k. If M is the (covariant) Dieudonné module of A, then

$$a(A) = a(M) := \dim_k M/(F, V)M.$$

Let $B_{p,\infty}$ denote the quaternion algebra over $\mathbb{Q}$ which is ramified exactly at $\{p, \infty\}$. Let D be the division quaternion algebra over $\mathbb{Q}_p$ and O_D be the maximal order. Let $W = W(k)$ be the ring of Witt vectors over k, $B(k) := \operatorname{Frac}(W(k))$ the fraction field, and σ the Frobenius map on $W(k)$. We also write $\mathbb{Q}_{p^2}$ and $\mathbb{Z}_{p^2}$ for $B(\mathbb{F}_{p^2})$ and $W(\mathbb{F}_{p^2})$, respectively.

Let A be an abelian variety (over any field). The endomorphism ring $\operatorname{End}(A)$ is an order of the semi-simple algebra $\operatorname{End}(A) \otimes \mathbb{Q}$. Determining $\operatorname{End}(A)$ is equivalent to determining the semi-simple algebra $\operatorname{End}(A) \otimes \mathbb{Q}$ and all local orders $\operatorname{End}(A) \otimes \mathbb{Z}_\ell$. Suppose that A is a supersingular abelian variety over k. We know that

- $\mathrm{End}(A) \otimes \mathbb{Q} = M_g(B_{p,\infty})$, and
- $\mathrm{End}(A) \otimes \mathbb{Z}_\ell = M_{2g}(\mathbb{Z}_\ell)$ for all primes $\ell \neq p$.

Therefore, it is sufficient to determine the local endomorphism ring $\mathrm{End}(A) \otimes \mathbb{Z}_p = \mathrm{End}_{\mathcal{DM}}(M)$, which is an order of the simple algebra $M_g(D)$.

3.2. The surface case

Let A be a supersingular abelian surface over k. There is a superspecial abelian surface A_1 and an isogeny $\varphi: A_1 \to A$ of degree p. Let M_1 and M be the covariant Dieudonné modules of A_1 and A, respectively. One regards M_1 as a submodule of M through the injective map φ_*. Let N be the Dieudonné submodule in $M_1 \otimes \mathbb{Q}_p$ such that $VN = M_1$. If $a(M) = 1$, then $M_1 = (F, V)M$ and hence it is determined by M. If $a(M) = 2$, or equivalently M is superspecial, then there are $p^2 + 1$ superspecial submodules $M_1 \subset M$ such that $\dim_k M/M_1 = 1$.

Now we fix a rank 4 superspecial Dieudonné module N (and hence fix M_1) and consider the space $\mathcal{X}$ of Dieudonné submodules M with $M_1 \subset M \subset N$ and $\dim_k N/M = 1$. It is clear that $\mathcal{X}$ is isomorphic to the projective line $\mathbf{P}^1$ over k. Let $\widetilde{N} \subset N$ be the $W(\mathbb{F}_{p^2})$-submodule defined by $F^2 = -p$. This gives an $\mathbb{F}_{p^2}$-structure on $\mathbf{P}^1$. It is easy to show the following.

Lemma 3.1. *Let $\xi \in \mathbf{P}^1(k)$ be the point corresponding to a Dieudonné module M in $\mathcal{X}$. Then M is superspecial if and only if $\xi \in \mathbf{P}^1(\mathbb{F}_{p^2})$.*

Choose a W-basis e_1, e_2, e_3, e_4 for N such that

$$Fe_1 = e_2, \qquad Fe_2 = -pe_1, \qquad Fe_3 = e_4, \qquad Fe_4 = -pe_3.$$

Note that this is a $W(\mathbb{F}_{p^2})$-basis for $\widetilde{N}$. Write $\xi = [a:b] \in \mathbf{P}^1(k)$. The corresponding Dieudonné module M is given by

$$M = \mathrm{Span}\langle pe_1, pe_3, e_2, e_4, v\rangle,$$

where $v = a'e_1 + b'e_3$ and $a', b' \in W$ are any liftings of a, b respectively.

Case (i): $\xi \in \mathbf{P}^1(\mathbb{F}_{p^2})$. In this case M is superspecial. We have $\mathrm{End}_{\mathcal{DM}}(M) = M_2(O_D)$.

Assume that $\xi \notin \mathbf{P}^1(\mathbb{F}_{p^2})$. In this case $a(M) = 1$. If $\phi \in \mathrm{End}_{\mathcal{DM}}(M)$, then $\phi \in \mathrm{End}_{\mathcal{DM}}(N)$. Therefore,

$$\mathrm{End}_{\mathcal{DM}}(M) = \bigl\{\phi \in \mathrm{End}_{\mathcal{DM}}(N);\ \phi(M) \subset M\bigr\}.$$

We have $\mathrm{End}_{\mathcal{DM}}(N) = \mathrm{End}_{\mathcal{DM}}(\widetilde{N}) = M_2(O_D)$. The induced map

$$\pi : \mathrm{End}_{\mathcal{DM}}(\widetilde{N}) \to \mathrm{End}_{\mathcal{DM}}(\widetilde{N}/V\widetilde{N}) \tag{3.1}$$

is surjective. Put

$$V_0 := \widetilde{N}/V\widetilde{N} = \mathbb{F}_{p^2}e_1 \oplus \mathbb{F}_{p^2}e_3 \quad \text{and} \quad B_0 := \mathrm{End}_{\mathbb{F}_{p^2}}(V_0).$$

We have

$$\mathrm{End}_{\mathcal{DM}}(\widetilde{N}/V\widetilde{N}) = \mathrm{End}_{\mathbb{F}_{p^2}}(V_0) = M_2(\mathbb{F}_{p^2}).$$

Put

$$B_0' := \bigl\{T \in B_0;\ T(v) \in k \cdot v\bigr\},$$

where $v = ae_1 + be_3 \in V_0 \otimes_{\mathbb{F}_{p^2}} k$. Therefore, $\mathrm{End}_{\mathcal{DM}}(M) = \pi^{-1}(B'_0)$. Since $\xi \notin \mathbf{P}^1(\mathbb{F}_{p^2})$, $a \neq 0$. We write $\xi = [1 : b]$, $v = e_1 + be_3$, and we have $\mathbb{F}_{p^2}(\xi) = \mathbb{F}_{p^2}(b)$. Write $T = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in B_0$, where $a_{ij} \in \mathbb{F}_{p^2}$. From $T(v) \in kv$, we get the condition

$$a_{12}b^2 + (a_{11} - a_{22})b - a_{21} = 0. \tag{3.2}$$

Case (ii): $\mathbb{F}_{p^2}(\xi)/\mathbb{F}_{p^2}$ is quadratic. Write $\xi = [1 : b]$. Suppose b satisfies $b^2 = \alpha b + \beta$, where $\alpha, \beta \in \mathbb{F}_{p^2}$. Plugging this in (3.2), we get

$$a_{11} - a_{12} + a_{12}\alpha = 0 \quad \text{and} \quad a_{12}\beta = a_{21}.$$

This shows

$$B'_0 = \left\{ t_1 I + t_2 \begin{pmatrix} 0 & 1 \\ \beta & \alpha \end{pmatrix};\ t_1, t_2 \in \mathbb{F}_{p^2} \right\} \simeq \mathbb{F}_{p^2}(\xi), \tag{3.3}$$

where $X^2 - \alpha X - \beta$ is the minimal polynomial of b.

Case (iii): $\xi \notin \mathbf{P}^1(\mathbb{F}_{p^2})$ and $\mathbb{F}_{p^2}(\xi)/\mathbb{F}_{p^2}$ is not quadratic. In this case $a_{12} = a_{21} = 0$ and $a_{11} = a_{22}$. We have

$$B'_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix};\ a \in \mathbb{F}_{p^2} \right\}.$$

We conclude

Proposition 3.2. *Let A be a supersingular surface over k and M be the associated covariant Dieudonné module. Suppose that A is represented by a pair (A_1, ξ), where A_1 is a superspecial abelian surface and $\xi \in \mathbf{P}^1_{A_1}(k)$. Let $\pi : M_2(O_D) \to M_2(\mathbb{F}_{p^2})$ be the natural projection.*

(1) *If $\mathbb{F}_{p^2}(\xi) = \mathbb{F}_{p^2}$, then $\mathrm{End}_{\mathcal{DM}}(M) = M_2(O_D)$.*
(2) *If $[\mathbb{F}_{p^2}(\xi) : \mathbb{F}_{p^2}] = 2$, then*

$$\mathrm{End}_{\mathcal{DM}}(M) \simeq \{\phi \in M_2(O_D);\ \pi(\phi) \in B'_0\},$$

where $B'_0 \subset M_2(\mathbb{F}_{p^2})$ is a subalgebra isomorphic to $\mathbb{F}_{p^2}(\xi)$.
(3) *If it is neither in the case (1) nor (2), then*

$$\mathrm{End}_{\mathcal{DM}}(M) \simeq \left\{ \phi \in M_2(O_D);\ \pi(\phi) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},\ a \in \mathbb{F}_{p^2} \right\}.$$

4. Proof of Theorem 1.1

4.1. The automorphism groups

Let $x = (A, \lambda)$ be a supersingular principally polarized abelian surfaces over k. Let $x_1 = (A_1, \lambda_1)$ be an element in $\Lambda^*_{2,p}$ such that there is a degree-p isogeny $\varphi : (A_1, \lambda_1) \to (A, \lambda)$ of polarized abelian varieties. Write $\xi = [a : b] \in \mathbf{P}^1(k)$ the point corresponding to the isogeny φ. We choose an $\mathbb{F}_{p^2}$-structure on $\mathbf{P}^1$ as in Section 3.2. Let $(M_1, \langle\,,\rangle) \subset (M, \langle\,,\rangle)$ be the covariant Dieudonné modules associated to $\varphi : (A_1, \lambda_1) \to (A, \lambda)$. Let N be the submodule in $M_1 \otimes \mathbb{Q}_p$ such that $VN = M_1$, and put $\langle\,,\rangle_N = p\langle\,,\rangle$. One has an isomorphism $(N, \langle\,,\rangle_N) \simeq (M_1, \langle\,,\rangle)$ of quasi-polarized Dieudonné modules. Put

$$U_x := G_x(\mathbb{Z}_p) = \mathrm{Aut}_{\mathcal{DM}}\big(M, \langle\, ,\rangle\big),$$
$$U_{x_1} := G_{x_1}(\mathbb{Z}_p) = \mathrm{Aut}_{\mathcal{DM}}\big(M_1, \langle\, ,\rangle\big) = \mathrm{Aut}_{\mathcal{DM}}\big(N, \langle\, ,\rangle_N\big).$$

Choose a W-basis e_1, e_2, e_3, e_4 for N such that

$$Fe_1 = e_2, \qquad Fe_2 = -pe_1, \qquad Fe_3 = e_4, \qquad Fe_4 = -pe_3,$$
$$\langle e_1, e_3\rangle_N = -\langle e_3, e_1\rangle_N = 1, \qquad \langle e_2, e_4\rangle_N = -\langle e_4, e_2\rangle_N = p,$$

and $\langle e_i, e_j\rangle = 0$ for all remaining i, j. The Dieudonné module M is given by

$$M = \mathrm{Span}\langle pe_1, pe_3, e_2, e_4, v\rangle,$$

where $v = a'e_1 + b'e_3$ and $a', b' \in W$ are any liftings of a, b respectively.

Case (i): $\boldsymbol{\xi \in \mathbf{P}^1(\mathbb{F}_{p^2})}$. In this case A is superspecial. One has $\Lambda_x = \Lambda_2$ and, by Corollary 2.6,

$$\mathrm{Mass}(\Lambda_x) = \frac{(p-1)(p^2+1)}{5760}.$$

In the remaining of this section, we treat the case $\xi \notin \mathbf{P}^1(\mathbb{F}_{p^2})$. One has

$$U_x = \big\{\phi \in U_{x_1};\ \phi(M) = M\big\},$$

and, by Proposition 2.4 and Corollary 2.6,

$$\mathrm{Mass}(\Lambda_x) = \mathrm{Mass}(\Lambda_{x_1}) \cdot \mu(U_{x_1}/U_x) = \frac{p^2-1}{5760}[U_{x_1} : U_x]. \tag{4.1}$$

Recall that $V_0 = \widetilde{N}/V\widetilde{N}$, which is equipped with the non-degenerate alternating pairing $\langle\, ,\rangle : V_0 \times V_0 \to \mathbb{F}_{p^2}$ induced from $\langle\, ,\rangle_N$. The map (3.1) induces a group homomorphism

$$\pi : U_{x_1} \to \mathrm{Aut}\big(V_0, \langle\, ,\rangle\big) = \mathrm{SL}_2(\mathbb{F}_{p^2}).$$

Proposition 4.1. *The map π above is surjective.*

The proof is given in Section 4.2.

Lemma 4.2. *One has* $\ker\pi \subset U_x$.

Proof. Let $\phi \in \ker\pi$. Write $\phi(e_1) = e_1 + f_1$, $\phi(e_3) = e_3 + f_3$, where $f_1, f_3 \in VN$. Since M is generated by VN and v, it suffices to check $\phi(v) = v + a'f_1 + b'f_3 \in M$; this is clear. $\square$

Case (ii): $\boldsymbol{[\mathbb{F}_{p^2}(\xi) : \mathbb{F}_{p^2}] = 2}$. By Proposition 3.2 and Lemma 4.2, we have $\pi\colon\ U_{x_1}/U_x \simeq \mathrm{SL}_2(\mathbb{F}_{p^2})/\mathbb{F}_{p^2}(\xi)^\times_1$, where

$$\mathbb{F}_{p^2}(\xi)^\times_1 = \mathbb{F}_{p^2}(\xi) \cap \mathrm{SL}_2(\mathbb{F}_{p^2})$$

via the identification (3.3). This shows

$$[U_{x_1} : U_x] = \big(p^4 - p^2\big).$$

Case (iii): $[\mathbb{F}_{p^2}(\xi):\mathbb{F}_{p^2}] \geqslant 3$. By Proposition 3.2 and Lemma 4.2, we have $\pi\colon U_{x_1}/U_x \simeq \mathrm{SL}_2(\mathbb{F}_{p^2})/\{\pm 1\}$. This shows

$$[U_{x_1}:U_x] = \left|\mathrm{PSL}_2(\mathbb{F}_{p^2})\right|.$$

From cases (i)–(iii) above and Eq. (4.1), Theorem 1.1 is proved.

4.2. Proof of Proposition 4.1

Write

$$O_D = W(\mathbb{F}_{p^2})[\Pi], \quad \Pi^2 = -p, \quad \Pi a = a^\sigma \Pi,\ \forall a \in W(\mathbb{F}_{p^2}).$$

The canonical involution is given by $(a+b\Pi)^* = a^\sigma - b\Pi$. With the basis $1, \Pi$, we have the embedding

$$O_D \subset M_2\big(W(\mathbb{F}_{p^2})\big), \qquad a + b\Pi = \begin{pmatrix} a & -pb^\sigma \\ b & a^\sigma \end{pmatrix}.$$

Note that this embedding is compatible with the canonical involutions. With respect to the basis e_1, e_2, e_3, e_4, an element $\phi \in \mathrm{End}_{\mathcal{DM}}(N)$ can be written as

$$T = (T_{ij}) \in M_2(O_D) \subset M_4\big(W(\mathbb{F}_{p^2})\big), \qquad T_{ij} = a_{ij} + b_{ij}\Pi = \begin{pmatrix} a_{ij} & -pb_{ij}^\sigma \\ b_{ij} & a_{ij}^\sigma \end{pmatrix}.$$

Since ϕ preserves the pairing $\langle\,,\rangle_N$, we get the condition in $M_4(\mathbb{Q}_{p^2})$:

$$T^t \begin{pmatrix} & J \\ -J & \end{pmatrix} T = \begin{pmatrix} & J \\ -J & \end{pmatrix}, \quad J = \begin{pmatrix} 1 & \\ & p \end{pmatrix}. \tag{4.2}$$

Note that

$$w_0 T_{ji}^* w_0^{-1} = T_{ji}^t, \quad w_0 = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \in M_2(\mathbb{Z}_{p^2}).$$

The condition (4.2) becomes

$$\begin{pmatrix} w_0 & \\ & w_0 \end{pmatrix} T^* \begin{pmatrix} w_0^{-1} & \\ & w_0^{-1} \end{pmatrix} \begin{pmatrix} & J \\ -J & \end{pmatrix} T = \begin{pmatrix} & J \\ -J & \end{pmatrix}. \tag{4.3}$$

Since

$$\begin{pmatrix} w_0^{-1} & \\ & w_0^{-1} \end{pmatrix} \begin{pmatrix} & J \\ -J & \end{pmatrix} = \begin{pmatrix} & -\Pi \\ \Pi & \end{pmatrix} = \Pi \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \in M_2(O_D),$$

we have

Lemma 4.3. *The group U_{x_1} is the group of O_D-linear automorphisms on the standard O_D-lattice $O_D \oplus O_D$ which preserve that quaternion hermitian form $\left(\begin{smallmatrix} 0 & -\Pi \\ \Pi & 0 \end{smallmatrix}\right)$.*

We also write (4.3) as

$$\Pi^{-1}T^*\Pi wT = w, \quad w = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \in M_2(O_D). \tag{4.4}$$

Notation. For an element $T \in M_m(D)$ and $n \in \mathbb{Z}$, write $T^{(n)} = \Pi^n T \Pi^{-n}$. In particular, if $T = (T_{ij}) \in M_m(\mathbb{Q}_{p^2}) \subset M_m(D)$, then $T^{(n)} = (T_{ij}^{\sigma^n})$. If $T \in M_m(O_D)$, denote by $\overline{T} \in M_m(\mathbb{F}_{p^2})$ the reduction of $T \bmod \Pi$.

Suppose $\bar{\phi} \in \mathrm{SL}_2(\mathbb{F}_{p^2})$ is given. Then we must find an element $T \in M_2(O_D)$ satisfying (4.4). We show that there is a sequence of elements $T_n \in M_2(O_D)$ for $n \geqslant 0$ satisfying the conditions

$$\left(T_n^*\right)^{(1)} wT_n \equiv w \pmod{\Pi^{n+1}}, \qquad T_{n+1} \equiv T_n \pmod{\Pi^{n+1}} \quad \text{and} \quad \overline{T}_0 = \bar{\phi}. \tag{4.5}$$

Suppose there is already an element $T_n \in M_2(O_D)$ for some $n \geqslant 0$ that satisfies

$$\left(T_n^*\right)^{(1)} wT_n \equiv w \pmod{\Pi^{n+1}}.$$

Put $T_{n+1} := T_n + B_n\Pi^{n+1}$, where $B_n \in M_2(O_D)$, and put $X_n := (T_n^*)^{(1)} wT_n$. Suppose $X_n \equiv w + C_n\Pi^{n+1}$ $(\bmod\ \Pi^{n+2})$. One computes that

$$\begin{aligned} X_{n+1} &\equiv T_n^{*(1)} wT_n + T_n^{*(1)} wB_n\Pi^{n+1} + \left(\Pi^{n+1}\right)^* B_n^{*(1)} wT_n \pmod{\Pi^{n+2}} \\ &\equiv w + C_n\Pi^{n+1} + T_n^{*(1)} wB_n\Pi^{n+1} + (-1)^{n+1} B_n^{*(n)} wT_n^{(n+1)}\Pi^{n+1} \pmod{\Pi^{n+2}}. \end{aligned}$$

Therefore, we require an element $B_n \in M_2(O_D)$ satisfying

$$\overline{C}_n + \overline{T}_n^t w\overline{B}_n + (-1)^{n+1}\overline{B}_n^{t(n+1)} w\overline{T}_n^{(n+1)} = 0.$$

Put $\overline{Y}_n := \overline{T}_n^t w\overline{B}_n$. As $\overline{Y}_n^t = -\overline{B}_n^t w\overline{T}_n$, we need to solve the equation

$$\overline{C}_n + \overline{Y}_n + (-1)^n\overline{Y}_n^{t(n+1)} = 0,$$

or equivalently the equation

$$\begin{cases} \overline{C}_n + \overline{Y}_n + \overline{Y}_n^{t(1)} = 0, & \text{if } n \text{ is even}, \\ \overline{C}_n + \overline{Y}_n - \overline{Y}_n^t = 0, & \text{if } n \text{ is odd}. \end{cases}$$

It is easy to compute that $X_n^* = -X_n^{(1)}$. From this it follows that

$$(-1)^{n+1} C_n^{*(n+1)}\Pi^{n+1} \equiv -C_n^{(1)}\Pi^{n+1} \pmod{\Pi^{n+2}},$$

or simply $(-1)^n\overline{C}_n^{t(n)} = \overline{C}_n^{(1)}$. This gives the condition

$$\begin{cases} \overline{C}_n^t = \overline{C}_n^{(1)}, & \text{if } n \text{ is even}, \\ -\overline{C}_n^t = \overline{C}_n, & \text{if } n \text{ is odd}. \end{cases}$$

By the following lemma, we prove the existence of $\{T_n\}$ satisfying (4.5). Therefore, Proposition 4.1 is proved.

Lemma 4.4. *Let C be an element in the matrix algebra $M_m(\mathbb{F}_{p^2})$.*

(1) *If $C^t = C^{(1)}$, then there is an element $Y \in M_m(\mathbb{F}_{p^2})$ such that $C + Y + Y^{t(1)} = 0$.*
(2) *If $-C^t = C$, then there is an element $Y \in M_m(\mathbb{F}_{p^2})$ such that $C + Y - Y^t = 0$.*

Proof. The proof is elementary and hence omitted. □

Remark 4.5. Theorem 1.1 also provides another way to look at the supersingular locus S_2 of the Siegel threefold. We used to divide it into two parts: superspecial locus and non-superspecial locus. Consider the mass function

$$M : S_2 \to \mathbb{Q}, \qquad x \mapsto \mathrm{Mass}(\Lambda_x).$$

Then the function M divides the supersingular locus S_2 into 3 locally closed subsets that refine the previous one. More generally, we can consider the same function M on the supersingular locus S_g of the Siegel modular variety of genus g. The situation definitely becomes much more complicated. However, it is worth knowing whether the following question has the affirmative answer.

(Question): Is the map $M : S_g \to \mathbb{Q}$ a constructible function?

Acknowledgments

The research of C.-F. Yu was partially supported by the grants NSC 97-2115-M-001-015-MY3 and AS-98-CDA-M01. The research of J.-D. Yu was partially supported by the grant NSC 97-2115-M-002-018.

References

[1] C.-L. Chai, Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli, Invent. Math. 121 (1995) 439–479.
[2] C.-L. Chai, Hecke orbits on Siegel modular varieties. Geometric methods in algebra and number theory, in: Progr. Math., vol. 235, Birkhäuser, Boston, 2005, pp. 71–107.
[3] T. Ekedahl, On supersingular curves and supersingular abelian varieties, Math. Scand. 60 (1987) 151–178.
[4] K. Hashimoto, T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo 27 (1980) 549–601.
[5] T. Katsura, F. Oort, Families of supersingular abelian surfaces, Compos. Math. 62 (1987) 107–167.
[6] L. Moret-Bailly, Familles de courbes et de variétés abéliennes sur P^1, in: L. Szpiro (Ed.), Sém. sur les pinceaux de courbes de genre au moins deux, Astérisque 86 (1981) 109–140.
[7] C.-F. Yu, On the mass formula of supersingular abelian varieties with real multiplications, J. Aust. Math. Soc. 78 (2005) 373–392.
[8] C.-F. Yu, The supersingular loci and mass formulas on Siegel modular varieties, Doc. Math. 11 (2006) 449–468.
[9] C.-F. Yu, Simple mass formulas on Shimura varieties of PEL-type, Forum Math., in press.
[10] C.-F. Yu, J. Yu, Mass formula for supersingular Drinfeld modules, C. R. Math. Acad. Sci. Paris Sér. I 338 (2004) 905–908.