PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 143, Number 6, June 2015, Pages 2339–2345
S 0002-9939(2015)12483-5
Article electronically published on January 21, 2015

ABELIAN VARIETIES WITHOUT A PRESCRIBED NEWTON POLYGON REDUCTION

JIANGWEI XUE AND CHIA-FU YU

(Communicated by Matthew A. Papanikolas)

Abstract. In this article we construct for each integer $g \geq 2$ an abelian variety A of dimension g defined over a number field for which there exists a symmetric integral slope sequence of length $2g$ that does not appear as the slope sequence of $\widetilde{A}$ for any good reduction $\widetilde{A}$ of A.

1. Introduction

Let A be an abelian variety over a number field F. It is conjectured that A always has a good ordinary reduction and furthermore there is a finite field extension L of F and a density one set $V(A, L)$ of non-archimedean places of L such that the base change $A \otimes_F L$ has (good) ordinary reduction at every place $v \in V(A, L)$ (cf. Bogomolov-Zarhin [1]).

This conjecture is known to be true for elliptic curves (Serre [10]), abelian surfaces (Ogus [8]), and some abelian three-folds or four-folds (see Noot [6, 7] and Tankeev [13]). In [1] Bogomolov and Zarhin prove the analogous theorem for K3 surfaces.

Concerning non-ordinary reductions, Elkies [2] shows that under a mild condition on the number field F, any elliptic curve over F has good supersingular reductions at infinitely many places of F. Inspired by the work of Elkies and having no counterexample, one may naturally ask whether any abelian variety over a number field F admits infinitely many supersingular reductions. So far this is not known yet even for abelian surfaces (except for some special cases like CM abelian surfaces). In the function field analogue, Poonen [9] shows the existence of a Drinfeld module of rank two which does not admit any supersingular reduction.

Throughout this paper, p and ℓ denote primes in $\mathbb{Q}$. For abelian varieties of dimension g in positive characteristic, the attached p-divisible groups up to isogeny over an algebraically closed field are classified by their Newton polygons, or equivalently, by the associated slope sequences β (the Dieudonné-Manin theorem; see Manin [5]). This invariant is a sequence of $2g$ rational numbers

$$0 \leq \lambda_1 \leq \cdots \leq \lambda_{2g} \leq 1,$$

which satisfy the symmetric and integral conditions:

(i) $\lambda_i + \lambda_{2g+1-i} = 1$ for all $1 \leq i \leq 2g$, and
(ii) the multiplicity of each λ_i is a multiple of its denominator.

Received by the editors November 5, 2013 and, in revised form, January 13, 2014.
2010 *Mathematics Subject Classification.* Primary 11G15; Secondary 14K22.

An abelian variety defined over a field of characteristic $p > 0$ is said to be *supersingular* if all $\lambda_i = 1/2$; it is said to be *ordinary* if λ_i is either 0 or 1 for all $1 \le i \le 2g$. Then given an abelian variety A over F of dimension g and a symmetric integral slope sequence β of length $2g$, does A always admit a good reduction whose slope sequence coincides with β? In this article we give a negative answer to this general question.

We will restrict ourselves to the case where A is absolutely simple. Otherwise, one is reduced to studying the simple factors of A (by extending the base field if necessary). For example, if $A = E^g$, a g-fold product of an elliptic curve E, then the reductions of A are either ordinary or supersingular. In other words, its reductions miss almost all the symmetric integral slope sequences except the two "extremal" ones.

Theorem 1. *For any integer $g \ge 2$, there is a pair $(A/F, \beta)$ consisting of*

- *an absolutely simple abelian variety A of dimension g defined over a number field F,*
- *a symmetric integral slope sequence β of length $2g$,*

such that β does not occur as the slope sequence of any good reduction of A.

In our construction the number field F depends on the dimension g. However, we have the following theorem.

Theorem 2. *In Theorem 1, there are infinitely many g for which the number field F can be chosen to be $\mathbb{Q}$.*

The CM abelian varieties play an essential role in our construction. For a CM abelian variety A/F of type (K, Φ), the Newton polygon of the reduction of A over a "good" prime $\mathfrak{q} \mid p$ of F can be determined from the CM-type Φ by the Taniyama-Shimura formula. This allows us to prove Theorem 1 by choosing a special type of CM-abelian varieties. To obtain Theorem 2, we study Honda's examples [3]. They are the Jacobians of the smooth projective curves defined by the affine equations $y^2 = 1 - x^\ell$ for all odd primes ℓ. This gives a family of CM Jacobians whose dimensions are of the form $(\ell - 1)/2$.

2. Reduction of CM abelian varieties

First, we recall Tate's formulation of the Shimura-Taniyama formula in terms of p-divisible groups [14, Section 4], which describes the behavior of reductions of CM abelian varieties. With this tool in hand, we then show that when the CM-field is a cyclic extension of $\mathbb{Q}$, the types of Newton polygons arising from the reductions are quite limited. This leads to a proof of Theorem 1. At the end, we present Honda's examples [3] and give a proof of Theorem 2.

2.1. **Shimura-Taniyama theory for CM abelian varieties.** Let K be a CM-field of degree $2g$ over $\mathbb{Q}$, and Σ_K the set of embeddings of K into the algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$ of $\mathbb{Q}$:

$$\Sigma_K := \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}).$$

We fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, where $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$. It induces a bijection:

$$\iota : \Sigma_K \simeq \Sigma_{K,p} := \mathrm{Hom}_{\mathbb{Q}_p}(K \otimes_{\mathbb{Q}} \mathbb{Q}_p, \overline{\mathbb{Q}}_p), \qquad \varphi \mapsto \iota \circ \varphi.$$

On the other hand, we have $K \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ denotes the completion of K at the prime $\mathfrak{p}$ of K. If we put $\Sigma_{K_{\mathfrak{p}}} := \mathrm{Hom}_{\mathbb{Q}_p}(K_{\mathfrak{p}}, \overline{\mathbb{Q}}_p)$, then

$$\Sigma_{K,p} = \coprod_{\mathfrak{p}} \Sigma_{K_{\mathfrak{p}}}. \tag{2.1.1}$$

Let $\rho \in \Sigma_K$ be a fixed embedding of K into $\overline{\mathbb{Q}}$. When $K/\mathbb{Q}$ is Galois with $G := \mathrm{Gal}(K/\mathbb{Q})$, we may identify Σ_K (and in turn $\Sigma_{K,p}$ via ι) with G via ρ:

$$G \simeq \Sigma_K, \quad \sigma \leftrightarrow \rho \circ \sigma, \ \forall \sigma \in G. \tag{2.1.2}$$

The embedding $\iota \circ \rho : K \hookrightarrow \overline{\mathbb{Q}}_p$ induces a unique prime $\mathfrak{p}_0 \mid p$ of K. Let $D_{\mathfrak{p}_0}$ be the decomposition group of $\mathfrak{p}_0$. Then (2.1.1) corresponds to the partition of G into the disjoint union of right cosets of $D_{\mathfrak{p}_0}$. More explicitly,

$$\Sigma_{K_{\mathfrak{p}}} \simeq D_{\mathfrak{p}_0} \sigma_{\mathfrak{p}}^{-1}, \qquad \text{with} \quad \sigma_{\mathfrak{p}} \mathfrak{p}_0 = \mathfrak{p}. \tag{2.1.3}$$

In particular, $|\Sigma_{K_{\mathfrak{p}}}| = |D_{\mathfrak{p}_0}|$ for all $\mathfrak{p} \mid p$. If K is abelian over $\mathbb{Q}$, the decomposition group $D_{\mathfrak{p}_0}$ depends only on p and not on $\mathfrak{p}_0$, so it is denoted by D_p instead. In this case, the partition of G into cosets of D_p does not depend on the choice of ι nor ρ.

Let $c \in \mathrm{Aut}(K)$ be the unique automorphism of order 2 that is induced by the complex conjugation for any embedding $K \hookrightarrow \mathbb{C}$. A subset $\Phi \subset \Sigma_K$ is said to be a CM-type on K if $\Sigma_K = \Phi \coprod \Phi c$. Given a CM-type Φ on K, we write $\Phi_{\mathfrak{p}} := \iota(\Phi) \cap \Sigma_{K_{\mathfrak{p}}} \subset \Sigma_{K,p}$ for prime $\mathfrak{p}$ of K. Let $\bar{\mathfrak{p}} := c\mathfrak{p}$; then c induces an isomorphism between the completions $K_{\mathfrak{p}} \simeq K_{\bar{\mathfrak{p}}}$, which gives rise to a bijective map

$$c : \Sigma_{K_{\bar{\mathfrak{p}}}} \to \Sigma_{K_{\mathfrak{p}}}, \qquad \varphi \mapsto \varphi \circ c. \tag{2.1.4}$$

It follows from the definition of a CM-type that

$$\Phi_{\mathfrak{p}} \coprod \Phi_{\bar{\mathfrak{p}}} c = \Sigma_{K_{\mathfrak{p}}}. \tag{2.1.5}$$

In particular, if $c\mathfrak{p} = \mathfrak{p}$, then $|\Phi_{\mathfrak{p}}| = |\Sigma_{K_{\mathfrak{p}}}|/2$.

A complex abelian variety $A_{\mathbb{C}}$ of dimension g is said to have complex multiplication of type (K, Φ) if there is an embedding $K \hookrightarrow \mathrm{End}^0(A_{\mathbb{C}}) := \mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and the character of the representation of K on the Lie algebra $\mathrm{Lie}_{\mathbb{C}}(A_{\mathbb{C}})$ is given by $\sum_{\varphi \in \Phi} \varphi$. A CM abelian variety of type (K, Φ) is simple if and only if Φ is *primitive*, i.e., not induced from a CM-type of a proper CM-subfield of K.

Let $A_{\mathbb{C}}$ be a CM complex abelian variety of type (K, Φ). Then $A_{\mathbb{C}}$ has a model A defined over a number field $F \subset \overline{\mathbb{Q}}$ ([12, Section 6.2 and 12.4]). Enlarging the base field F if necessary, we may assume that A has a good reduction $A \otimes \kappa(\mathfrak{q})$ at every finite place $\mathfrak{q}$ of F (cf. [11]). Here $\kappa(\mathfrak{q})$ denotes the residue field of $\mathfrak{q}$. Since we are only concerned with the isogeny invariants, replacing A with its quotient by a suitable finite subgroup if necessary, we may further assume that $\mathrm{End}(A) \cap K = O_K$, the ring of integers of K. The p-adic completion of O_K decomposes into a product

$$O_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{\mathfrak{p}|p} O_{K_{\mathfrak{p}}}, \tag{2.1.6}$$

where $O_{K_{\mathfrak{p}}}$ denotes the ring of integers of $K_{\mathfrak{p}}$. Let $\mathfrak{q}$ be the prime of F corresponding to the embedding $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$, and

$$A \otimes \overline{\kappa(\mathfrak{q})}[p^\infty] = \prod_{\mathfrak{p}|p} H_{\mathfrak{p}} \tag{2.1.7}$$

be the decomposition of p-divisible groups induced from (2.1.6). Then each component $H_{\mathfrak{p}}$ is of height $|\Sigma_{K_{\mathfrak{p}}}|$, dimension $|\Phi_{\mathfrak{p}}|$, and isoclinic of slope $|\Phi_{\mathfrak{p}}|/|\Sigma_{K_{\mathfrak{p}}}|$ (see [12, Chapter III, Theorem 1], [14, Section 5] and [15, Section 4]). In particular, if K is abelian over $\mathbb{Q}$, then the slope sequence of $A\otimes\overline{\kappa(\mathfrak{q})}$ depends only on Φ and p. In other words, it is independent of the choice of $\iota:\overline{\mathbb{Q}}\to\overline{\mathbb{Q}}_p$, and thus independent of the prime $\mathfrak{q}\mid p$ of F for the reduction.

Example 2.1.1. Suppose that p splits completely in K. Then $K_{\mathfrak{p}}=\mathbb{Q}_p$ for all $\mathfrak{p}\mid p$. So $|\Sigma_{K_{\mathfrak{p}}}|=1$, and $\Phi_{\mathfrak{p}}$ either coincides with $\Sigma_{K_{\mathfrak{p}}}$ or is empty. Therefore, each $H_{\mathfrak{p}}$ has slope either 0 or 1. The reduction of A at any prime $\mathfrak{q}\mid p$ is ordinary.

Let L be the Galois closure of K over $\mathbb{Q}$, i.e., the compositum of all conjugates of $K/\mathbb{Q}$. It is again a CM-field with c in the center of $\mathrm{Gal}(L/\mathbb{Q})$. Let p be a prime unramified for $L/\mathbb{Q}$ such that the Artin symbol $(p,L/\mathbb{Q})=c\in\mathrm{Gal}(L/\mathbb{Q})$. By Tchebotarev density theorem ([4, Theorem 10, Section VIII.4]), such p exists and they have a positive density. Any prime $\mathfrak{p}\mid p$ in K is then fixed by c. By the remark below (2.1.5), the reduction of A at $\mathfrak{q}$ is supersingular.

2.2. **Proof of Theorem 1.**

Lemma 2.2.1. *For any integer $g\geq 1$, there is a CM field K which is a cyclic extension over $\mathbb{Q}$ with Galois group $G\simeq\mathbb{Z}/2g\mathbb{Z}$. Moreover, K admits a primitive CM-type Φ.*

Proof. By the Dirichlet theorem on arithmetic progressions (cf. Lang [4, Section VIII.4]), there is a prime number ℓ such that $\ell\equiv 1+2g \pmod{4g}$. Then the integer $m:=(\ell-1)/2g$ is odd. Let K be the fixed subfield of the ℓ-th cyclotomic field $\mathbb{Q}(\zeta_\ell)$ for the unique subgroup $H\subset(\mathbb{Z}/\ell\mathbb{Z})^\times$ of order m. Since $|H|$ is odd, the complex conjugation c on $\mathbb{Q}(\zeta_\ell)$ is not contained in H, and hence it induces a non-trivial automorphism of K. Therefore, K is a CM field which is cyclic over $\mathbb{Q}$ of degree $2g$. We claim that $\Phi=\{0,1,\cdots,g-1\}\subseteq\mathbb{Z}/2g\mathbb{Z}=\mathrm{Gal}(K/\mathbb{Q})$ is a primitive CM-type on K. Otherwise, Φ will be translation invariant under a non-trivial subgroup $\mathrm{Gal}(K/K')\subset\mathbb{Z}/2g\mathbb{Z}$ for some proper CM-subfield K' of K, but this is not the case. □

Now for any $g\geq 2$, let $K\subset\overline{\mathbb{Q}}$ be a CM-field cyclic over $\mathbb{Q}$ with Galois group $G=\mathbb{Z}/2g\mathbb{Z}$. Choose a primitive CM type $\Phi\subset\Sigma_K\simeq G$. The complex torus $\mathbb{C}^\Phi/\Phi(O_K)$ defines a complex abelian variety $A_{\mathbb{C}}$ of CM type (K,Φ). Let A be a model of $A_{\mathbb{C}}$ defined over a sufficiently large number field $F\subset\mathbb{C}$ such that A has good reduction everywhere. Let $\mathfrak{q}$ be a prime of F over p, and D_p be a decomposition group of p in K. Since $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, D_p is uniquely determined by its order $f:=|D_p|$. We claim that the slope sequence of the reduction $A\otimes\kappa(\mathfrak{q})$ is uniquely determined by f. Indeed, the slope of each component $H_{\mathfrak{p}}$ in (2.1.7) is of the form $\lambda:=|\Phi\cap(a+D_p)|/f$ for some coset $a+D_p$ of D_p in G. If f is even, the complex conjugation $c\in\mathrm{Gal}(K/\mathbb{Q})$ lies in D_p, hence every prime $\mathfrak{p}\mid p$ in K is fixed by c. It follows that every $H_{\mathfrak{p}}$ in (2.1.7) is isoclinic of slope 1/2, and thus $A\otimes\kappa(\mathfrak{q})$ is supersingular. For a non-supersingular reduction of A, f is necessarily odd, so all the slopes λ have odd denominators.

Let M_g be the number of all possible slope sequences arising from good reductions of A, and N_g be k the number of all symmetric integral slope sequences of length

$2g$. To prove Theorem 1, it is enough to show that $M_g < N_g$. By the previous arguments, we have an upper bound

(2.2.1) $$M_g \leq 1 + \text{ the number of positive odd divisors of } 2g = |G|.$$

Therefore, $M_g \leq g$ for any $g \geq 2$. On the other hand, for any $g \geq 1$, one easily sees $N_g \geq g + 1$ by counting the number of symmetric integral slope sequences taking values only in $\{0, 1/2, 1\}$. This shows that $M_g < N_g$ for all $g \geq 2$ and hence proves Theorem 1.

In fact, let β be a symmetric integral slope sequence of length $2g$ that takes values only in $\{0, 1/2, 1\}$, and β is neither ordinary nor supersingular. There are $g - 1$ such slope sequences. We have shown that β never coincides with the slope sequence of any good reduction of A.

Remark 2.2.2. Suppose that $g = 2^n$. By (2.2.1), $M_g \leq 2$, and hence it is 2 by Example 2.1.1. Varying n, we obtain an infinite family of absolutely simple abelian varieties whose reductions are either ordinary or supersingular. There are other classes of abelian varieties that enjoy this property. For example, let D be an indefinite quaternion division algebra over $\mathbb{Q}$, and A/F be an abelian surface over a number field F with quaternion multiplication (QM) by D. In other words, there exists an embedding $D \hookrightarrow \mathrm{End}^0(A)$. Then any reduction of A is either ordinary or supersingular. Indeed, let $\widetilde{A}$ be a good reduction of A over some prime $\mathfrak{q} \mid p$ of F. The quaternion algebra $D_p := D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ acts on $V_p\widetilde{A} := T_p\widetilde{A} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p\widetilde{A}$ is the Tate-module of $\widetilde{A}$. If $\widetilde{A}$ has slope sequence $(0, 1/2, 1/2, 1)$, then $V_p\widetilde{A}$ is a dimension one $\mathbb{Q}_p$-vectors space, which cannot admit any action by D_p. It is known that an abelian surface A with QM by D is absolutely simple if and only if it does not have CM (cf. [16]). If A has no CM, then $\mathrm{End}^0(A) = D$, otherwise, A is isogenous to the self-product of a CM elliptic curve. In particular, any good reduction $\widetilde{A}$ of A, which is an abelian surface with QM by D over a finie field, is always isogenous to the self-product of an elliptic curve.

We would like to thank the referee for the following stronger version of Theorem 1.

Theorem 3. *Let K be a CM-field with $K/\mathbb{Q}$ Galois and $[K : \mathbb{Q}] = 2g$ with $g \geq 2$. Let A/F be an abelian variety with CM by K. There exists a symmetric integral slope sequence β such that, for each prime $\mathfrak{q}$ of F, the slope sequence of reduction $A \otimes \kappa(\mathfrak{q})$ does not coincide with β.*

Proof. Since K is Galois over $\mathbb{Q}$, in the decomposition (2.1.7) of the p-divisible group of the reduction, each component $H_{\mathfrak{p}}$ is isoclinic of slope $|\Phi_{\mathfrak{p}}|/f$, where f is the order of the decomposition group at p in K. Suppose that $g \geq 4$, we pick $1 < f_0 < g$ such that $\gcd(f_0, 2g) = 1$. For example, if g is odd, we may choose $f_0 = g - 2$, and if g is even, we choose $f_0 = g - 1$. Then $\mathrm{Gal}(K/\mathbb{Q})$ has no subgroup of order f_0, and thus f_0 can never occur as the denominator of a slope of some $H_{\mathfrak{p}}$. Let $\lambda = 1/f_0$, and β be the following symmetric integral slope sequence:

$$\beta = (\underbrace{0, \cdots, 0}_{g-f_0} \quad \underbrace{\lambda, \cdots, \lambda}_{f_0}, \quad \underbrace{1-\lambda, \cdots, 1-\lambda}_{f_0}, \quad \underbrace{1, \cdots, 1}_{g-f_0}).$$

Then β never occurs as the slope sequence of any good reduction of A.

If $g = 3$, then $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 6 with an element of order 2 in its center. Therefore, $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$ and we are reduced to the proof of Theorem 1. If $g = 2$, then $\mathrm{Gal}(K/\mathbb{Q})$ is either $\mathbb{Z}/4\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. In the first case, once again we are reduced to the proof of Theorem 1. In the second case K contains two quadratic imaginary subfields; any CM-type on K is induced from one of them. Hence A is isogenous over $\bar{F}$ to a product of CM elliptic curves, so its reduction is either ordinary or supersingular. It never achieves the slope sequence $(0, 1/2, 1/2, 1)$ from its reductions. □

2.3. **Honda's examples.** We will describe some results of Honda [3] and prove Theorem 2.

Let ℓ be an odd prime, and $C = C_\ell$ be the smooth projective curve over $\mathbb{Q}$ defined by the affine equation

$$y^2 = 1 - x^\ell. \tag{2.3.1}$$

The genus $g := g(C)$ of C is $(\ell - 1)/2$. The curve C and its Jacobian $J = J_\ell$ have good reductions at all primes $p \neq 2, \ell$. For a fixed odd prime $p \neq \ell$, let $\widetilde{J}$ (resp. $\widetilde{C}$) be the reduction of J (resp. C) at p (over $\mathbb{F}_p$).

Let ζ_ℓ be a primitive ℓ-th root of unity in $\overline{\mathbb{Q}} \subset \mathbb{C}$, and $K := \mathbb{Q}(\zeta_\ell)$ be the ℓ-th cyclotomic field. Then K is a CM-field that's cyclic over $\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/\ell\mathbb{Z})^\times$, where each $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ corresponds to the automorphism of K that send ζ_ℓ to ζ_ℓ^a. Let $\rho : K \hookrightarrow \overline{\mathbb{Q}}$ be the natural inclusion. We will identify G with Σ_K via ρ as in (2.1.2).

The automorphism of $C \otimes_{\mathbb{Q}} K$ defined by $(x, y) \mapsto (x, \zeta_\ell y)$ induces an embedding $K \hookrightarrow \mathrm{End}^0_K(J)$. This realizes $J \otimes_{\mathbb{Q}} K$ as a CM-abelian variety of type (K, Φ), where $\Phi = \{1, 2, \cdots g - 1, g\} \subset G$ is a primitive CM-type on K. Let f be the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. The Artin symbol $(p, K/\mathbb{Q})$ equals $p \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, and f is the order of the decomposition group $D_p = \langle p \rangle \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times$ of p in K. By [3, Theorem 1, 2] or the proof of Theorem 1, the slope sequence of $\widetilde{J}$ depends only on f. Moreover, if f is even, $\widetilde{J}$ is supersingular.

Now Theorem 2 follows from Theorem 1 by noting that J is an absolutely simple CM abelian variety of dimension $(\ell - 1)/2$ defined over $\mathbb{Q}$, and the field K is cyclic over $\mathbb{Q}$.

Acknowledgments

The authors would like to thank the referee for suggestions on the exposition of the paper. The referee also made several insightful remarks about the results, and provided a stronger version of our main result, which became Theorem 3 of the current paper. The first named author was partially supported by the grant NSC 102-2811-M-001-090. The second named author was partially supported by the grants NSC 100-2628-M-001-006-MY4 and AS-98-CDA-M01.

References

[1] Fedor A. Bogomolov and Yuri G. Zarhin, *Ordinary reduction of K3 surfaces*, Cent. Eur. J. Math. **7** (2009), no. 2, 206–213, DOI 10.2478/s11533-009-0013-8. MR2506961 (2010h:14038)

[2] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567, DOI 10.1007/BF01388985. MR903384 (88i:11034)

[3] Taira Honda, *On the Jacobian variety of the algebraic curve $y^2 = 1 - x^l$ over a field of characteristic $p > 0$*, Osaka J. Math. **3** (1966), 189–194. MR0225777 (37 #1370)

[4] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723 (95f:11085)

[5] Ju. I. Manin, *Theory of commutative formal groups over fields of finite characteristic* (Russian), Uspehi Mat. Nauk **18** (1963), no. 6 (114), 3–90. MR0157972 (28 #1200)

[6] Rutger Noot, *Abelian varieties—Galois representation and properties of ordinary reduction*, Compositio Math. **97** (1995), no. 1-2, 161–171. Special issue in honour of Frans Oort. MR1355123 (97a:11093)

[7] Rutger Noot, *Abelian varieties with l-adic Galois representation of Mumford's type*, J. Reine Angew. Math. **519** (2000), 155–169, DOI 10.1515/crll.2000.010. MR1739726 (2001k:11112)

[8] A. Ogus, *Hodge cycles and crystalline cohomology*, Lecture Notes in Math., vol. 1, Springer-Verlag, **900** (1982), 357–414.

[9] Bjorn Poonen, *Drinfeld modules with no supersingular primes*, Internat. Math. Res. Notices **3** (1998), 151–159, DOI 10.1155/S1073792898000130. MR1606391 (99a:11074)

[10] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR0263823 (41 #8422)

[11] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488)

[12] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961. MR0125113 (23 #A2419)

[13] S. G. Tankeev, *On the weights of an l-adic representation and the arithmetic of Frobenius eigenvalues* (Russian, with Russian summary), Izv. Ross. Akad. Nauk Ser. Mat. **63** (1999), no. 1, 185–224, DOI 10.1070/im1999v063n01ABEH000233; English transl., Izv. Math. **63** (1999), no. 1, 181–218. MR1701843 (2000f:11072)

[14] John Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)* (French), Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 352, 95–110. MR3077121

[15] Chia-Fu Yu, *The isomorphism classes of abelian varieties of CM-type*, J. Pure Appl. Algebra **187** (2004), no. 1-3, 305–319, DOI 10.1016/S0022-4049(03)00144-0. MR2027907 (2004k:14077)

[16] Chia-Fu Yu, *Endomorphism algebras of QM abelian surfaces*, J. Pure Appl. Algebra **217** (2013), no. 5, 907–914, DOI 10.1016/j.jpaa.2012.09.022. MR3003315

Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), 6th Floor, Astronomy Mathematics Building, No. 1, Roosevelt Road Section 4, Taipei, Taiwan, 10617

Current address: Collaborative Innovation Centre of Mathematics, School of Mathematics and Statistics, Wuhan University, Luojiashan, Wuhan, Hubei, 430072, People's Republic of China

E-mail address: `xue_j@whu.edu.cn`

Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), 6th Floor, Astronomy Mathematics Building, No. 1, Roosevelt Road Section 4, Taipei, Taiwan, 10617

E-mail address: `chiafu@math.sinica.edu.tw`