On certain reduction problems concerning Abelian surfaces.

Goren, Eyal Z.

pp. 33 - 44

manuscripta math. 94, 33–43 (1997)

manuscripta mathematica

On Certain Reduction Problems Concerning Abelian Surfaces

Eyal Z. Goren

Department of Mathematics, Harvard University, Science Center, One Oxford St., Cambridge, MA 02138, USA.
email: egoren@abel.math.harvard.edu

Received August 19, 1996;
in revised form April 25, 1997

1. Introduction

Let $\mathcal{E}$ be an elliptic scheme (i.e. an abelian scheme of relative dimension one) over Spec $\mathcal{O}_M$ where $\mathcal{O}_M$ is the ring of integers of some number field M. Assume that $\mathcal{E}$ has complex multiplication by the full ring of integers of some quadratic imaginary field K and that $M \supseteq K$. Then a well known criterion of Deuring states that given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_M$, the reduction of $\mathcal{E}$ mod $\mathfrak{p}$, $\mathcal{E}_\mathfrak{p}$, is supersingular if $p = \mathfrak{p} \cap \mathbb{Z}$ is either ramified or inert in K and ordinary if p splits in K.

Let X be an abelian variety over a finite field $\mathbb{F}$ and let $\mathbb{F}^a$ be an algebraic closure of $\mathbb{F}$. Let $f(X)$ be the p-rank of $X[p](\mathbb{F}^a)$, so that $p^{f(X)}$ is the number of geometric points in $X[p]$ - the kernel of multiplication by p on X. Let $\alpha_{p,\mathbb{F}^a}$ be the finite local-local group scheme Spec $\mathbb{F}^a[x]/(x^p)$. Let $a(X) = \dim_{\mathbb{F}^a} \mathrm{Hom}(\alpha_{p,\mathbb{F}^a}, X \otimes \mathbb{F}^a)$. The criterion above describes $(f(\mathcal{E}_\mathfrak{p}), a(\mathcal{E}_\mathfrak{p}))$ solely in terms of the decomposition of $p = \mathfrak{p} \cap \mathbb{Z}$ in K.

While in the case of elliptic curves E over $\mathbb{F}$ we have $(f(E), a(E)) \in \{(1, 0), (0, 1)\}$ (and both possibilities always occur), the situation for surfaces is more involved. If X is an abelian surface over $\mathbb{F}$ then $(f(X), a(X)) \in \{(2, 0), (1, 1), (0, 1), (0, 2)\}$ and all possibilities do occur. Let $\mathcal{X}$ be an abelian scheme of relative dimension two over Spec $\mathcal{O}_M$. Assume that $\mathcal{X}$ has complex multiplication by the full ring of integers of a quartic primitive C.M. field K (i.e. K does not contain a quadratic imaginary subfield). In the first part of this paper we determine $(f(\mathcal{X}_\mathfrak{p}), a(\mathcal{X}_\mathfrak{p}))$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_M$ such that $p = \mathfrak{p} \cap \mathbb{Z}$ is unramified in the Galois closure of K. For example:

Theorem 1. *Let $K/\mathbb{Q}$ be a cyclic quartic C.M. field. Let $A/\overline{\mathbb{Q}}$ be an abelian surface. Assume that A has complex multiplication by $\mathcal{O}_K$. Let $\bar{P}$ be a prime of $\overline{\mathbb{Q}}$, $\mathfrak{p}_1 = \bar{P} \cap \mathcal{O}_K$, $p = \mathfrak{p}_1 \cap \mathbb{Z}$. Assume that p is unramified in K. Then the reduction of A mod $\bar{P}$, $A_{\bar{P}}$, and $(f(A_{\bar{P}}), a(A_{\bar{P}}))$ are determined by the decomposition of p in $\mathcal{O}_K$ as follows:*

(1) *If* $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, *then* $A_{\bar{F}}$ *is ordinary and simple*, $(f(A_{\bar{F}}), a(A_{\bar{F}})) = (2, 0)$.

(2) *If* $p = \mathfrak{p}_1\mathfrak{p}_2$, *then* $A_{\bar{F}}$ *is isomorphic to the product of two supersingular elliptic curves*, $(f(A_{\bar{F}}), a(A_{\bar{F}})) = (0, 2)$.

(3) *If* $p = \mathfrak{p}_1$, *then* $A_{\bar{F}}$ *is isogenous, but not isomorphic, to a product of two supersingular elliptic curves*, $(f(A_{\bar{F}}), a(A_{\bar{F}})) = (0, 1)$.

Theorem 2 deals with the non-cyclic case which is a bit more complicated. These theorems may be known to the experts and some special cases are scattered in the literature. The usefulness of such theorems and the lack of references convinced us that it may be worthwhile to publish them.

These theorems do not take into account polarizations. Analogous results with polarizations are a complete mystery. They would have far reaching applications (see [DSG]). Consider a particular case: assume that $\mathcal{X}$ is an abelian scheme of relative dimension two over Spec $\mathcal{O}_M$ and that $\lambda\colon \mathcal{X} \longrightarrow \mathrm{Pic}^0(\mathcal{X}/\mathcal{O}_M)$ is a principal polarization. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_M$ and assume further that $a(\mathcal{X}_\mathfrak{p}) = 2$. Then by [O1] $\mathcal{X}_\mathfrak{p} \cong E_1 \times E_2$ (over some extension of $\mathcal{O}_M/\mathfrak{p}$) where the E_i's are supersingular elliptic curves. Assume that $\mathcal{C}$ is a stable curve of genus two over Spec $\mathcal{O}_M$ such that $(\mathcal{X}, \lambda) \cong (\mathrm{Pic}^0(\mathcal{C}/\mathcal{O}_M), \phi_\mathcal{L})$, $\mathcal{L} = \underline{\mathcal{O}}_\mathcal{X}(\mathcal{C})$ and $\phi_\mathcal{L}(x) = T_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$. Then it is easy to see that $(\mathcal{X}_\mathfrak{p}, \lambda_\mathfrak{p}) \cong (E_1 \times E_2, \lambda_1 \times \lambda_2)$, where λ_i is the unique principal polarization on E_i, if and only if, $\mathcal{C}_\mathfrak{p}$ is a reducible curve whose two components are isomorphic to E_1 and E_2 and intersect transversely at their zero points. This observation and its relevance to understanding the values of certain modular forms on Siegel's upper half space of genus two in special points (see [DSG]) led us to the second part of this paper.

The second part of this paper is concerned with establishing the existence of curves of genus two whose stable models have everywhere good reduction. As a corollary of our method we get

Corollary . *For every genus* $g \geq 1$ *there exist infinitely many stable curves over* $\mathcal{O}_\mathbb{Q}[\frac{1}{2}]$ *with everywhere good reduction.*[1]

We remark that this result follows easily from [MB] (see also [R]) - I thank the referee for bringing it to my attention. However, the method presented here has some virtues: it is elementary, explicit (at least to some extent) and yields information on the field of definition of the constructed curves.

Acknowledgments. I would like to thank E. DeShalit for many enlightening discussions regarding the content of this paper. I would like to thank the referee for his careful reading of the manuscript and for many interesting comments and corections which affected in various ways the final shape of this paper.

---

[1] The method can be extended to cover characteristic 2 as well.

2. Reduction of Abelian Surfaces with Complex Multiplication.

Let X be an abelian variety over a finite field $\mathbb{F}$ of characteristic p. We have the following results ([O1], [O2]): (i) $0 \le f(X) \le \dim X$; (ii) $0 \le a(X) \le \dim X$; (iii) $0 < a(X) \iff f(X) < \dim X$; (iv) X is $\mathbb{F}^a$-isomorphic to a product of supersingular elliptic curves if and only if $a(X) = \dim X$.

Let A be an abelian variety over a number field M, Galois over $\mathbb{Q}$. Assume that A has complex multiplication by the full ring of integers $\mathcal{O}_K$ of a C.M. field K and let Φ be its C.M. type. Assume that $M \supseteq K$, P is a prime ideal of M such that $p = P \cap \mathbb{Z}$ is unramified in M and that A extends to an abelian scheme $\mathcal{A}$ over Spec $(\mathcal{O}_M)_P$. Let σ be a generator, lifting Frobenius, of the decomposition group of P in M and denote the decomposition of Emb(M, $\mathbb{C}$) induced by Φ, $\overline{\Phi}$ by Φ, $\overline{\Phi}$ again. Put $\mathbb{F} = \mathcal{O}_M/\mathfrak{p}$. Then:

The product criterion ([E] Proposition 2.4). *$\mathcal{A}_P$ is isomorphic over $\mathbb{F}^a$ to a product of supersingular elliptic curves if and only if $\sigma\overline{\Phi} = \Phi$.*

Let Y be a scheme over a finite field $\mathbb{F}$. Let F_Y: $Y \longrightarrow Y^{(p)}$ the Frobenius morphism. We write F^2 for the composition $F_{Y^{(p)}} \circ F_Y$ etc. The same abuse of notation is used for the Verschiebung morphism. The following lemma will be used repeatedly.

Lemma. *Let A be an abelian variety over a finite field $\mathbb{F}$ of characteristic p. Assume that the Frobenius morphism F: $A \longrightarrow A^{(p)}$ satisfies $F^{2i} = \varepsilon p^i$ for some i and $\varepsilon \in$ Aut(A). Then, denoting the Verschiebung by V, we have $V^{2i} = \varepsilon^{-1}p^i$. In particular $A[p]$ is a local-local group scheme.*

Proof. Indeed, $V^{2i}\varepsilon p^i = V^{2i}F^{2i} = p^{2i}$. Hence $(V^{2i} - p^i\varepsilon^{-1})\varepsilon p^i = 0$. Therefore, since εp^i is surjective, we get $V^{2i} = \varepsilon^{-1}p^i$. This implies that both Frobenius and Verschiebung are nilpotent on $A[p]$ and therefore that $A[p]$ is a local-local group scheme ([Ma] Proposition 1.5 - note that A_n and A_p should be interchanged there). Q.E.D.

Proposition 2.1. *Let $X/\overline{\mathbb{Q}}$ be an abelian variety with complex multiplication by the full ring of integers $\mathcal{O}_K$ of a C.M. field K, ι_X: $\mathcal{O}_K \longrightarrow$ End(X). Let Φ be the C.M. type and assume that Φ is not induced. Let K^* be the reflex C.M. field obtained from (K, Φ) and let H be the Hilbert class field of K^*. Let P be a prime ideal of $\mathcal{O}_H$. Then there exists an abelian variety A and ι_A : $\mathcal{O}_K \longrightarrow$ End(A), both defined over H, $\overline{\mathbb{Q}}$-isomorphic to (X, ι_X) and having good reduction at P.*

Proof. Since Φ is not induced, X is simple ([L] Chapter I, Theorem 3.4) and therefore there exists a polarization κ on X compatible with ι_X: $\mathcal{O}_K \longrightarrow$ End(X) (see [S] §1). Using loc. cit. Theorem 11 and (use loc.cit. Proposition 7) we get that there exists a triple (A, λ, ι_A) which is $\overline{\mathbb{Q}}$-isomorphic to (X, κ, ι_X) and (A, λ, ι_A) is defined over M - the moduli field of (A, λ, ι_A). Moreover $H \supseteq M$ ([L] Chapter V, Theorem 4.1).

We claim that we may take A as to have good reduction at P. Indeed, since End(A) = $\mathcal{O}_K$, Proposition 7 in [S] holds trivially. The proof of this proposition implies that for every given prime $p \in \mathbb{Z}$ we can find a decomposition of $U = \prod_{v \in M_{K,f}} U(K_v)$ (where $U(K_v) = \mathcal{O}_{K_v}^{\times}$ and $M_{K,f}$ is the set of finite valuations of K) as $U = \mu \times W$ where μ is the

group of roots of unity in K embedded diagonally in the non-archimedian part of $\mathbb{A}_K^\times$ and where $W \supseteq U(K_v)$ for all $v \mid p$. One checks that the Grössencharacter of $\mathbb{A}_M^\times$ constructed in [S] Theorem 11 (ii) will be unramified at every $v \in M_{M,f}$ such that $v \nmid p$ (see the paragraph preceding the cited theorem). By [SeT] Corollary to Theorem 6, A has good reduction at such a v. Q.E.D.

Let $\mathcal{X} \longrightarrow S$ be an abelian scheme of relative dimension g. For every $b \in \mathrm{End}(\mathcal{X}/S)$ let $\mathcal{X}[b]$ be the closed S-sub-group-scheme $\mathrm{Ker}(b)$. It is a flat S-group-scheme whose formation commutes with base change. Given a set $B \subseteq \mathrm{End}(\mathcal{X}/S)$ let $\mathcal{X}[B] = \bigcap_{b \in B} \mathcal{X}[b]$ (a finite intersection in fact). It is also a flat S-sub-group-scheme whose formation commutes with base change. Now suppose that $\mathrm{End}(\mathcal{X}/S)$ is the ring of integers of a C.M. field K of degree $2g$. If $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2$ are ideals of $\mathrm{End}(\mathcal{X}/S)$ such that $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ and $\mathfrak{b}_1, \mathfrak{b}_2$ are relatively prime then $\mathcal{X}[\mathfrak{b}] = \mathcal{X}[\mathfrak{b}_1] \oplus \mathcal{X}[\mathfrak{b}_2]$. Indeed, the map $\mathcal{X}[\mathfrak{b}_1] \oplus \mathcal{X}[\mathfrak{b}_2] \longrightarrow \mathcal{X}[\mathfrak{b}]$ has kernel $\mathcal{X}[\mathfrak{b}_1 \cup \mathfrak{b}_2]$ which is trivial. One reduces to checking surjectivity after base change to an algebraically closed field where it follows from the fact that $\deg \mathcal{X}[\mathfrak{b}] = N_{K'/\mathbb{Q}}\mathfrak{b}$ for every ideal $\mathfrak{b}$ ([L] Chapter 3, §2).

Theorem 1. *Let $K/\mathbb{Q}$ be a cyclic quartic C.M. field. Let $A/\overline{\mathbb{Q}}$ be an abelian surface. Assume that A has complex multiplication by $\mathcal{O}_K$, ι_A: $\mathcal{O}_K \longrightarrow \mathrm{End}(A)$. Let $\bar{P}$ be a prime of $\overline{\mathbb{Q}}$, $\mathfrak{p}_1 = \bar{P} \cap \mathcal{O}_K$, $p = \mathfrak{p}_1 \cap \mathbb{Z}$. Assume that p is unramified in K. Then the reduction of A mod $\bar{P}$, $A_{\bar{P}}$, and $(f(A_{\bar{P}}), a(A_{\bar{P}}))$ are determined by the decomposition of p in $\mathcal{O}_K$ as follows*:

(1) *If $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, then $A_{\bar{P}}$ is ordinary and simple, $(f(A_{\bar{P}}), a(A_{\bar{P}})) = (2, 0)$.*

(2) *If $p = \mathfrak{p}_1\mathfrak{p}_2$, then $A_{\bar{P}}$ is isomorphic to the product of two supersingular elliptic curves, $(f(A_{\bar{P}}), a(A_{\bar{P}})) = (0, 2)$.*

(3) *If $p = \mathfrak{p}_1$, then $A_{\bar{P}}$ is isogenous, but not isomorphic, to a product of two supersingular elliptic curves, $(f(A_{\bar{P}}), a(A_{\bar{P}})) = (0, 1)$.*

Proof. We may assume that A and ι_A are as in Proposition 2.1 w.r.t. $P = \bar{P} \cap \mathcal{O}_H$ (note that $K = K^*$). We can assume that $\Phi = \{1, \tau\}$ where τ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Let $k = \mathcal{O}_H/P$ and F_P be the power of Frobenius fixing k. Let $p = \prod_{n=1}^{t} \mathfrak{p}_n$ be the decomposition of p into prime ideals in $\mathcal{O}_K$. Then $A[p] = \bigoplus_{n=1}^{t} A[\mathfrak{p}_n]$ as group schemes over $\mathrm{Spec}\,\mathcal{O}_{H,P}$. By [ST] III.13 Theorem 1, the ideal generated by F_P in $\mathrm{End}(A_P)$ is a power of $N_{\Phi^*}(\mathfrak{p}_1)$.

(1) We have $t = 4$. Say $\tau(\mathfrak{p}_i) = \mathfrak{p}_{i+1}$. Since $N_{\Phi^*}(\mathfrak{p}_1) = \mathfrak{p}_1 \cdot \tau^2(\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_3$ we conclude that F_P has trivial kernel in its action on $A[\mathfrak{p}_2] \oplus A[\mathfrak{p}_4]$. That is, in the algebraic closure of k, the étale part of $A_P[p]$ is of order p^2. Thus A_P is ordinary. Furthermore, A_P is not isogenous to a product of elliptic curves:

If A_P is isogenous to a product of elliptic curves, say $E_1 \times E_2$, then they must be ordinary. By looking at the endomorphism rings we conclude that E_1 is isogenous to E_2. Thus, $\mathrm{End}^0(E_1 \times E_2) \cong M_2(L)$, L an imaginary quadratic extension of $\mathbb{Q}$. We have $K \hookrightarrow M_2(L)$. If the image of K (still denoted by K) does not contain L then KL is a

commutative algebra of degree 8 over $\mathbb{Q}$, hence equal to $M_2(L)$ which is a contradiction. Therefore K contains L which is absurd because the unique quadratic sub-field of K is real.

(2) We have $t = 2$, $\tau(\mathfrak{p}_1) = \mathfrak{p}_2$. Therefore $N_{\Phi^*}(\mathfrak{p}_1) = \mathfrak{p}_1 \cdot \tau^3(\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_2 = p$. Using the lemma we get that $A_P[p]$ is local-local. Therefore, since for a commutative local-local k-group-scheme the a-number is always positive, we have $a(A_P[p]) \geq a(A_P[\mathfrak{p}_1]) + a(A_P[\mathfrak{p}_2]) \geq 2$. Hence, A_P is isomorphic to a product of supersingular elliptic curves.

(3) We have $A[p] = A[\mathfrak{p}_1]$. By the same arguments $A_P[p]$ is local-local and therefore $a(A_P[p]) \geq 1$, $f(A_P[p]) = 0$. Now, let σ be the Frobenius of P in $\mathrm{Gal}(H/\mathbb{Q})$. Then σ restricted to K is equal to τ or τ^3 (it is here that we use that we can find a model of X over a field in which p remains unramified). Hence $\sigma\overline{\Phi}\cap\Phi = \{1\}, \{\tau\}$, respectively. The product criterion shows that A_P is not a product of supersingular elliptic curves and in particular $a(A_P) = 1$. It follows that A_P is isomorphic to $E \times E/\alpha_p$ where E is a supersingular elliptic curve and α_p is suitably embedded (see [KO] Theorem 1.2.).Q.E.D.

Let K be a non-cyclic primitive quartic C.M. field. Then ([ST] II.8.4) the Galois closure L of K satisfies $\mathrm{Gal}(L/\mathbb{Q}) \cong \langle x, y: x^2, y^4\ xyxy\rangle$ - the dihedral group of order 8. The classification of C.M. types of K shows that by changing y to y^{-1} and by twisting by complex conjugation we can always assume that K is the fixed field of x and that the C.M. type is $\{1, y\}$. The situation we will be considering is the following: Let $X/\overline{\mathbb{Q}}$ be an abelian surface with $\iota_X : \mathcal{O}_K \longrightarrow \mathrm{End}(X)$ for K as above. Let H be the Hilbert class field of K^* and $\bar{P}$ a prime of $\overline{\mathbb{Q}}$. Put $M = HL$, $P = \bar{P}\cap M$, $\mathfrak{p}_1 = P\cap L$, $\mathfrak{p} = P\cap K^*$, $p = P\cap\mathbb{Z}$. We denote the decomposition group of $\mathfrak{p}_1$ in $\mathrm{Gal}(L/\mathbb{Q})$ by $D = D(\mathfrak{p}_1)$. We will have to consider all possible decompositions of p in K and K^*. This is completely determined by D. We will use the following notation: after D is fixed we can index the primes dividing p in L by representatives $\{g\}$ of the cosets $\{gD\}$ in $\mathrm{Gal}(L/\mathbb{Q})$. That is, if $\mathfrak{q} = g\mathfrak{p}_1$, we denote $\mathfrak{q}$ by $\mathfrak{p}_g$.

Theorem 2. *Let the notation be as above. Assume that p is unramified in L. Then the reduction of X mod $\bar{P}$, $X_{\bar{P}}$, is as follows*:

(1) *If $D = \{1\}$ then $X_{\bar{P}}$ is ordinary, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (2, 0)$.*
(2) *If $D = \{1, x\}$ then $X_{\bar{P}}$ is intermediate, i.e. $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (1, 1)$.*
(3) *If $D = \{1, xy\}$ then $X_{\bar{P}}$ is supersingular and isomorphic to the product of two supersingular elliptic curves, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (0, 2)$.*
(4) *If $D = \{1, xy^2\}$ then $X_{\bar{P}}$ is is intermediate, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (1, 1)$.*
(5) *If $D = \{1, xy^3\}$ then $X_{\bar{P}}$ is ordinary, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (2, 0)$.*
(6) *If $D = \{1, y^2\}$ then $X_{\bar{P}}$ is supersingular and isomorphic to the product of two supersingular elliptic curves, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (0, 2)$.*
(7) *If $D = \{1, y, y^2, y^3\}$ then $X_{\bar{P}}$ is supersingular, isogenous but not isomorphic to a product of two supersingular elliptic curves, $(f(X_{\bar{P}}), a(X_{\bar{P}})) = (0, 1)$.*

Moreover, $X_{\bar{P}}$ is simple if and only if $f(X_{\bar{P}}) \geq 1$.

Proof. We briefly explain some of the cases (the arguments are similar to those

appearing in Theorem 1). First we may assume that $X = A$ given with $\iota_A : \mathcal{O}_K \longrightarrow \mathrm{End}(A)$ defined over M as in Proposition 2.1. Consider the following easily verified data

Case 1

$D = D(\mathfrak{p}_1)$	$\{1\}$
Decomposition of p in L	$\prod_{g \in \mathrm{Gal}(L/\mathbb{Q})} \mathfrak{p}_g$
Decomposition of p in K	$(\mathfrak{p}_1\mathfrak{p}_x)(\mathfrak{p}_{y^3}\mathfrak{p}_{xy^3})(\mathfrak{p}_y\mathfrak{p}_{xy})(\mathfrak{p}_{y^2}\mathfrak{p}_{xy^2})$
*Decomposition of p in K**	$(\mathfrak{p}_1\mathfrak{p}_{xy^3})(\mathfrak{p}_y\mathfrak{p}_x)(\mathfrak{p}_{y^2}\mathfrak{p}_{xy})(\mathfrak{p}_{y^3}\mathfrak{p}_{xy^2})$
$\mathfrak{p}$	$(\mathfrak{p}_1\mathfrak{p}_{xy^3})$
$N_{\Phi^*}(\mathfrak{p})$	$(\mathfrak{p}_1\mathfrak{p}_x)(\mathfrak{p}_{y^3}\mathfrak{p}_{xy^3})$
$X[p]$	$X[\mathfrak{p}_1\mathfrak{p}_x]\oplus X[\mathfrak{p}_{y^3}\mathfrak{p}_{xy^3}]\oplus X[\mathfrak{p}_y\mathfrak{p}_{xy}]\oplus X[\mathfrak{p}_{y^2}\mathfrak{p}_{xy^2}]$

Case 2

$D = D(\mathfrak{p}_1)$	$\{1, x\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^2}\mathfrak{p}_{y^3}$
Decomposition of p in K	$\mathfrak{p}_1\mathfrak{p}_{y^2}(\mathfrak{p}_y\mathfrak{p}_{y^3})$
*Decomposition of p in K**	$(\mathfrak{p}_1\mathfrak{p}_y)(\mathfrak{p}_{y^2}\mathfrak{p}_{y^3})$
$\mathfrak{p}$	$(\mathfrak{p}_1\mathfrak{p}_y)$
$N_{\Phi^*}(\mathfrak{p})$	$\mathfrak{p}_1^2(\mathfrak{p}_y\mathfrak{p}_{y^3})$
$X[p]$	$X[\mathfrak{p}_1]\oplus X[\mathfrak{p}_{y^2}]\oplus X[\mathfrak{p}_y\mathfrak{p}_{y^3}]$

Case 3

$D = D(\mathfrak{p}_1)$	$\{1, xy\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^2}\mathfrak{p}_{y^3}$
Decomposition of p in K	$(\mathfrak{p}_1\mathfrak{p}_y)(\mathfrak{p}_{y^2}\mathfrak{p}_{y^3})$
*Decomposition of p in K**	$(\mathfrak{p}_1\mathfrak{p}_{y^2})\mathfrak{p}_y\mathfrak{p}_{y^3}$
$\mathfrak{p}$	$(\mathfrak{p}_1\mathfrak{p}_{y^2})$
$N_{\Phi^*}(\mathfrak{p})$	p
$X[p]$	$X[\mathfrak{p}_1\mathfrak{p}_y]\oplus X[\mathfrak{p}_{y^2}\mathfrak{p}_{y^3}]$

Case 4

$D = D(\mathfrak{p}_1)$	$\{1, xy^2\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^2}\mathfrak{p}_{y^3}$
Decomposition of p in K	$(\mathfrak{p}_1\mathfrak{p}_{y^2})\mathfrak{p}_y\mathfrak{p}_{y^3}$
*Decomposition of p in K**	$(\mathfrak{p}_1\mathfrak{p}_{y^3})(\mathfrak{p}_y\mathfrak{p}_{y^2})$
$\mathfrak{p}$	$(\mathfrak{p}_1\mathfrak{p}_{y^3})$
$N_{\Phi^*}(\mathfrak{p})$	$(\mathfrak{p}_1\mathfrak{p}_{y^2})\mathfrak{p}_{y^3}^2$
$X[p]$	$X[\mathfrak{p}_1\mathfrak{p}_{y^2}]\oplus X[\mathfrak{p}_y]\oplus X[\mathfrak{p}_{y^3}]$

Case 5

$D = D(\mathfrak{p}_1)$	$\{1, xy^3\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_y\mathfrak{p}_{y^2}\mathfrak{p}_{y^3}$
Decomposition of p in K	$(\mathfrak{p}_1\mathfrak{p}_{y^3})(\mathfrak{p}_y\mathfrak{p}_{y^2})$
*Decomposition of p in K**	$\mathfrak{p}_1\mathfrak{p}_{y^2}(\mathfrak{p}_y\mathfrak{p}_{y^3})$

$\mathfrak{p}$	$\mathfrak{p}_1$
$N_{\Phi^*}(\mathfrak{p})$	$(\mathfrak{p}_1\mathfrak{p}_{y^3})$
$X[p]$	$X[\mathfrak{p}_1\mathfrak{p}_{y^3}]\oplus X[\mathfrak{p}_y\mathfrak{p}_{y^2}]$

Case 6

$D = D(\mathfrak{p}_1)$	$\{1, y^2\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_x\mathfrak{p}_y\mathfrak{p}_{xy}$
Decomposition of p in K	$(\mathfrak{p}_1\mathfrak{p}_x)(\mathfrak{p}_y\mathfrak{p}_{xy})$
*Decomposition of p in K**	$(\mathfrak{p}_1\mathfrak{p}_{xy})(\mathfrak{p}_x\mathfrak{p}_y)$
$\mathfrak{p}$	$(\mathfrak{p}_1\mathfrak{p}_{xy})$
$N_{\Phi^*}(\mathfrak{p})$	p
$X[p]$	$X[\mathfrak{p}_1\mathfrak{p}_x]\oplus X[\mathfrak{p}_y\mathfrak{p}_{xy}]$

Case 7

$D = D(\mathfrak{p}_1)$	$\{1, y, y^2, y^3\}$
Decomposition of p in L	$\mathfrak{p}_1\mathfrak{p}_x$
Decomposition of p in K	p
*Decomposition of p in K**	p
$\mathfrak{p}$	p
$N_{\Phi^*}(\mathfrak{p})$	p^2
$X[p]$	$X[p]$

To indicate how one concludes the assertions of the theorem, first note that in any case where the decomposition of $N_{\Phi^*}(\mathfrak{p})$ into prime ideals does not contains *every* prime ideal appearing in the decomposition of p in K, we can conclude that $X_P[p]$ is not killed by any power of Frobenius and hence $X_P[p]_{\text{étale}}$ is non-trivial and its order can be read in this fashion from the decomposition of $X[p]$. Also note that if $X[p] = G_1 \oplus G_2$ then $a(X_P[p]) = a(G_{1P}) + a(G_{2P})$. This settles cases (1), (2), (4), (5). In cases (3), (6), (7) we get that $X_P[p]$ is local and in fact, by the Lemma, local-local. Therefore in cases (3), (6) the a-number is evidently 2 and from [O1], X_P is isomorphic to a product of two supersingular elliptic curves. Only in case (7) we need the product criterion. In this case the Frobenius σ of $\mathfrak{O}_M/P$ is induced from a generator δ of D, i.e. from either y or y^{-1}. But $\delta\overline{\Phi} \neq \Phi$ ($\Phi = \{1, y\}$). Therefore X_P is not isomorphic to a product of supersingular elliptic curves although by [KO] it is isogenous to such a product. The last assertion of the theorem follows from considering the endomorphism rings as in the proof of Theorem 1. Q.E.D.

Remark. Note that in case (5) above, and only in this case, $X_P[p]$ decomposes further than the decomposition coming from the decomposition of p in the C.M. field.

3. Curves with Good Reduction.

Let K be a field. Let C/K be a stable curve of genus 2. Then C is of one of the

following types (see [NU]):

(I) An irreducible smooth curve.

(II) Two smooth genus 1 curves intersecting transversely at one point.

(III)a) An irreducible curve with one node.

(III)b) A smooth genus 1 curve intersecting transversely at one point a rational curve with one node.

(IV)a) An irreducible rational curve with two nodes.

(IV)b) Two rational curves with a node intersecting transversely at one point.

(IV)c) Two smooth rational curves intersecting transversely at three points.

Let E/K be an elliptic curve and $P \in E(K) - E[2]$. Assume that $\mathrm{Char}(K) \neq 2$. Let $f \in K(E)$ be a rational function such that $\mathrm{div}(f) = [P] + [-P] - 2[0_E]$ ($[P]$ is the divisor associated to P). There exists a unique smooth curve $C = C(E, \pm P)$ whose function field is $k(E)(\sqrt{f})$ and we have a natural separable morphism of degree 2, $C \longrightarrow E$, ramified precisely at two points $\Pi, -\Pi$ of C which project to $P, -P$, respectively (in "$-\Pi$" the minus sign is a *formal* symbol). Let $\sigma \in \mathrm{Aut}(C)$ be the corresponding involution. Let ι be the hyperelliptic involution of C and $\tau = \sigma \circ \iota$. One can verify that $C/\langle\tau\rangle$ is again an elliptic curve (in fact we can assume that $(E, \pm P) = (y^2 = x^3 + Ax^2 + Bx + 1, \pm(0, 1))$. Then C: $y^2 = X^6 + Ax^4 + Bx^2 + 1$ where $C \longrightarrow E$ is given by $(x, y) \longmapsto (x^2, y)$ and $C/\langle\tau\rangle$ is $y^2 = x^3 + Bx^2 + Ax + 1$).

Let $(R', \mathfrak{p}')$ be a d.v.r. with quotient field K' such that $\mathrm{Char}(R'/\mathfrak{p}') \neq 2$[2]. Let E/K' be an elliptic curve and $P \in E(K') - E[2]$. Then there exists a d.v.r. $(R, \mathfrak{p}) \supseteq (R', \mathfrak{p}')$ with quotient field K such that E extends to a stable elliptic curve $\mathcal{E}$ [3] over Spec R. We assume that R is chosen so that $C(E, \pm P)$ extends to a stable curve $\mathcal{C}(E, \pm P)$ over Spec R. We use the subscript $-_{\mathfrak{p}}$ to denote reduction mod $\mathfrak{p}$.

Proposition 3.1. *Let* $\mathcal{C} = \mathcal{C}(E, \pm P)$. *Assume that* $\mathcal{E}_{\mathfrak{p}}$ *is smooth. Then:*

(*a*) *If* $P_{\mathfrak{p}} \notin \mathcal{E}_{\mathfrak{p}}[2]$ *then* $\mathcal{C}_{\mathfrak{p}}$ *is of type* (I) (*i.e., smooth*).

(*b*) *If* $P_{\mathfrak{p}} = 0_{\mathcal{E}_{\mathfrak{p}}}$ *then* $\mathcal{C}_{\mathfrak{p}}$ *is of type* (II).

(*c*) *If* $P_{\mathfrak{p}} \in \mathcal{E}_{\mathfrak{p}}[2] - \{0_{\mathcal{E}_{\mathfrak{p}}}\}$ *then* $\mathcal{C}_{\mathfrak{p}}$ *is of type* (III)a).

Proof. The involutions σ, τ, ι extend uniquely to involutions Σ, T, I of $\mathcal{C}$ ([DM] Lemma 1.2). Now, there are some points to keep in mind:

(i) There is a surjective homomorphism $\mathrm{Pic}^0(\mathcal{C}/R) \longrightarrow \mathcal{E}$;

(ii) The involutions $\Sigma_{\mathfrak{p}}$, $T_{\mathfrak{p}}$, $I_{\mathfrak{p}}$ do not act as the identity on any component of $\mathcal{C}_{\mathfrak{p}}$ (follow the argument of [B] p. 176).

(iii) The quotient $\mathcal{C}/\Sigma$ is proper and flat over R with reduced 1-dimensional geometric fibers and is of genus 1.

We see, using (i), that $\mathcal{C}_{\mathfrak{p}}$ can only be of types (I), (II), (III)a) or (III)b). It follows from (ii) that if $\mathcal{C}_{\mathfrak{p}}$ is of type (III)b) then $\mathcal{C}_{\mathfrak{p}}/\Sigma_{\mathfrak{p}}$ is of genus 0, which contradicts (iii). Therefore $\mathcal{C}_{\mathfrak{p}}$ is of type (I), (II) or (III)a). If $\mathcal{C}_{\mathfrak{p}}$ is of type (III)a) then (ii) and (iii)

[2] The method can be extended to include $\mathrm{Char}(K') \neq 2$, $\mathrm{Char}(R'/\mathfrak{p}') = 2$.

[3] By this we mean that $\mathcal{E}_{\mathfrak{p}}$ is either smooth or irreducible with one node.

compel Σ_p to exchange the two components. We see therefore that

(iv) The quotient $\mathcal{C}/\Sigma$ is proper and flat over R with reduced and irreducible one dimensional geometric fibers and with node singularities at worst (see [B] Lemma 3.1).

It follows that $\mathcal{C}/\Sigma$ is isomorphic to $\mathcal{E}$. Observe that

(v) If $\mathcal{C}_p$ is of type (I) then Σ_p has two fixed points; If $\mathcal{C}_p$ is of type (II) then Σ_p yields an isomorphism of the two components and has a unique fixed point - the intersection point of the two components; If $\mathcal{C}_p$ is of type (III)a) then Σ_p has a unique fixed point - the singular point (consider the induced map from the normalization of $\mathcal{C}_p$ to $\mathcal{E}_p$).

It follows from (v) that

(vi) The points $\Pi_p, -\Pi_p$ are the only fixed points of Σ_p and they project to $P_p, -P_p$ respectively.

Another point, needed to decide between the cases (b) and (c) is that the fixed points of τ, denoted by $\Pi^*, -\Pi^*$, both project to the zero point of E and hence

(vii) The fixed points $\Pi^*_p, -\Pi^*_p$, of T_p project to the zero point of $\mathcal{E}_p$.

Case (a). Follows immediately from (v), (vi).

Case (b). It follows from (v) and (vi) that $\mathcal{C}_p$ is not of type (I). Assume that $\mathcal{C}_p$ is of type (III)a). Denote by $\Delta_\Pi, \Delta_{-\Pi}, \Delta_{\Pi^*}, \Delta_{-\Pi^*}$ the closure of the points $\Pi, -\Pi, \Pi^*, -\Pi^*$ in $\mathcal{C}$. Consider the function $\sqrt{f} \in K(C)$ as a rational function on $\mathcal{C}$. Since $\mathcal{C}_p$ is irreducible, its divisor is $\mathrm{div}(\sqrt{f}) = \Delta_\Pi + \Delta_{-\Pi} - \Delta_{\Pi^*} - \Delta_{-\Pi^*} + n\cdot \mathcal{C}_p$. After extending K if necessary we can thus assume that $\mathrm{div}(\sqrt{f}) = \Delta_\Pi + \Delta_{-\Pi} - \Delta_{\Pi^*} - \Delta_{-\Pi}$. Therefore $\sqrt{f}$ defines a rational function on $\mathcal{C}$ whose restriction to $\mathcal{C}_p$ is a constant $s \neq 0$. Since $\Sigma^*\sqrt{f} = -\sqrt{f}$ we get that $-s = (-\sqrt{f})_p = (\Sigma^*\sqrt{f})_p = \Sigma_p{}^*\sqrt{f}_p = \Sigma_p{}^* s = s$. A contradiction.

Case (c). It follows from (v) and (vi) that $\mathcal{C}_p$ is not of type (I). If $\mathcal{C}_p$ is of type (II) then the only fixed point of both Σ_p and T_p is the intersection point of the two components. Then (vii) implies that $\Pi_p, -\Pi_p$ project to $0_{\mathcal{E}_p}$. A contradiction. Q.E.D.

Corollary. *For every genus $g \geq 1$ there exist infinitely many stable curves over Spec $\mathcal{O}_{\mathbb{Q}}\left[\frac{1}{2}\right]$ with everywhere good reduction.*

Proof. For $g = 1$ this is well known. In fact any elliptic curve with complex multiplication will do.

Let $g \geq 2$ and put $N = g - 1$. Let L be a quadratic C.M. field in which every prime dividing N splits. Let E/K be an elliptic curve with complex multiplication by the full ring of integers of a C.M field L where K is suitable number field containing L. We can assume that $K \subseteq \mathbb{C}$ and that the C.M. type of E is the identity.

Let $q > 2$ be any prime that splits in L, $q = \mathfrak{q}_1\mathfrak{q}_2$. We have $E[q] = E[\mathfrak{q}_1] \oplus E[\mathfrak{q}_2]$. Let α_1 be a generator of $E[\mathfrak{q}_1]$ and $P = \alpha_1 + \alpha_2$. Let $C = C(E, \pm P)$ and $\pi: C \longrightarrow E$ the associated double covering.

For any prime Q of $\mathcal{O}_K$, if $Q \nmid q$ then the reduction mod Q gives an isomorphism $E[q] \cong E_Q[q]$ and in particular $P_Q \notin E_Q[2]$. If $Q \mid \mathfrak{q}_1$ then by the theory of complex multiplication the reduction mod Q is injective on $E[\mathfrak{q}_2]$ (and the zero map on $E[\mathfrak{q}_1]$).

Thus P_Q is of order q. The same argument works for $Q \mid \mathfrak{q}_2$. Hence, it follows from Proposition 3.1 that after a suitable finite extension $K_1 \supseteq K$, C extends to a smooth curve $\mathcal{C}$ over Spec $\mathcal{O}_{K_1}$.

Let $S = \text{Spec } \mathcal{O}_{\mathfrak{V}}$, $\mathfrak{P} \in S$ a closed point, $S(\mathfrak{P})$ its residue field. Let $A = \text{Pic}^0(C)$ and $\mathcal{A} = \text{Pic}^0(\mathcal{C}/\mathcal{O}_{K_1})$ the abelian scheme extending A. We consider henceforth $\mathcal{A}$ as an abelian scheme over Spec $\mathcal{O}_{\mathfrak{V}}$. We claim that there exists an abelian scheme $\mathcal{B}/S$ and an isogeny Ψ: $\mathcal{B} \longrightarrow \mathcal{A}$ of degree N such that Ker Ψ is étale over S (equivalently $(\text{Ker } \Psi) \otimes_S S(\mathfrak{P})$ is étale for every $\mathfrak{P}$): Indeed, let $\mathcal{E}/S$ be the elliptic scheme extending E. Let $p_1, .., p_r$ be the prime divisors of N. Let $p_i = \mathfrak{p}_i^1 \mathfrak{p}_i^2$ be the decomposition of p_i in L. We have

$$E[N] = E\left[\prod_{i=1}^{r} \mathfrak{p}_i^1\right] \oplus E\left[\prod_{i=1}^{r} \mathfrak{p}_i^2\right].$$

Each summand is a cyclic group. Let α_1 (resp. α_2) be a generator of the first (resp. second) summand and let $\alpha = \alpha_1 + \alpha_2$. Let H' be the cyclic subgroup of E of order N generated by α and $\mathcal{H}'$ the unique flat subgroup-scheme of $\mathcal{E}$ whose generic fiber is H'. The same argument as above shows that $\mathcal{H}'$ is étale over S. The covering $\pi : \mathcal{C} \longrightarrow \mathcal{E}$ induces a homomorphism π^*: $\mathcal{E} \longrightarrow \mathcal{A}$ whose geometric fibers are closed immersions ([M]). It follows that π^*: $\mathcal{E} \longrightarrow \mathcal{A}$ is a closed immersion and we see that we can find a subgroup-scheme $\mathcal{H}$ of $\mathcal{A}$, étale over S. Let H be the generic fiber of $\mathcal{H}$ and choose a subgroup scheme T of A such that $H \oplus T = A[N]$. Then T extends to a unique flat subgroup-scheme $\mathcal{T}$ of $\mathcal{A}$ and $\mathcal{A}[N] = \mathcal{H} \oplus \mathcal{T}$. Let $\mathcal{B} = \mathcal{A}/\mathcal{T}$. The canonical homomorphism $\mathcal{A} \longrightarrow \mathcal{A}/\mathcal{A}[N] \cong \mathcal{A}$ factors through $\mathcal{B}$ and the induced homomorphism has kernel $\mathcal{A}[N]/\mathcal{T} \cong \mathcal{H}$.

Let $\mathcal{D} = \mathcal{C} \times_{\mathcal{A}} \mathcal{B}$. For every $\mathfrak{P}$, $\mathcal{D}_{\mathfrak{P}} \longrightarrow \mathcal{C}_{\mathfrak{P}}$ is étale and $\mathcal{D}_{\mathfrak{P}}$ is a smooth irreducible curve (see [Se] §IV.2) of genus $N \times (\text{genus}(\mathcal{C}_{\mathfrak{P}}) - 1) + 1 = g$. Moreover $\mathcal{D} \longrightarrow \mathcal{C}$ is clearly flat and of finite type. It follows that $\mathcal{D} \longrightarrow \mathcal{C}$ is étale and that $\mathcal{D}$ is a stable curve of genus g with everywhere good reduction. Q.E.D.

Remarks. 1) The referee pointed out that the corollary can also be derived from a theorem of Moret-Bailly ([MB], Theorem 1.3) and it also follows from Rumely's theory ([R] Theorem 1). The same is true for the corollary stated below. Note, however, that in both corollaries the construction is (in a certain sense) explicit and yields information on fields of definition.

2) One can use Proposition 3.1. to prove the following corollary:

Let M be a number field and let R, S be two disjoint sets of prime ideals of $\mathcal{O}_M$. Then there exists a finite extension $N \supseteq M$ and a stable curve $\mathcal{C}$ over Spec $\mathcal{O}_N$ such that for every prime $\mathfrak{p}$ of $\mathcal{O}_N$ we have: (i) *If $\mathfrak{p} \cap \mathcal{O}_N \notin R \cup S$ then $\mathcal{C}$ is of type* (I); (ii) *If $\mathfrak{p} \cap \mathcal{O}_N \in R$ then $\mathcal{C}$ is of type* (II); (iii) *If $\mathfrak{p} \cap \mathcal{O}_N \in S$ then $\mathcal{C}$ is of type* (III)a).

References

[B] Beauville, A.: *Prym Varieties and the Schottky Problem*, Inventiones. Math. **41**(1977), 149 - 196.

[DM] Deligne, P. and Mumford,D.: *The Irreducibility of the Space of Curves of Given Genus*, Publ. Math. I.H.E.S. **36**(1969), 75 - 109.

[DSG] DeShalit, E. and Goren, E.Z.: *On Special Values of Theta Functions of Genus Two*, Preprint, June 1996.

[E] Ekedahl, T.: *On Supersingular Curves and Abelian Varieties*, Math. Scand. **60**(1987), 151-178.

[KO] Katsura, T. and Oort, F.: *Families of Supersingular Abelian Surfaces*, Compositio Math. **62**(1987), 107 - 167.

[L] Lang, S.: *Complex Multiplication*, Grundlehren der mathematischen Wissenschaften, **225**, Springer-Verlag, New-York, 1983.

[M] Mumford, D.: *Prym Varieties I*, in: Contributions to Analysis, Academic Press, New York, 1974, 325 - 350.

[Ma] Manin, Y.I.: *The Theory of Commutative Formal Groups over Fields of Finite Characteristic*, Russian Math. Surveys **18**(1963), 1 - 80.

[MB] Moret-Bailly, L.: *Groupes de Picard et Problèmes de Skolem*, Ann. Scient. Éc. Norm. Sup., 4^{e} série, t. **22**, 1989, 181 - 194.

[NU] Namikawa, Y. and Ueno, K.: *The Complete Classification of Fibres in Pencils of Curves of Genus Two*, Manuscripta Math. **9**(1973), 143 - 186.

[O1] Oort, F.: *Which Abelian Surfaces are Products of Elliptic Curves?*, Math. Ann. **214**(1975), 35 - 47.

[O2] Oort, F.: *Moduli of Abelian Varieties in Positive Characteristic*, In: Barsotti Symposium in Algebraic Geometry, Perspectives in Math. **15**, Academic Press, 1994, 253 - 276.

[R] Rumely, R.S.: *Arithmetic over the ring of all algebraic integers*, J. Reine Angew. Math. **368**(1986), 127 - 133.

[S] Shimura, G.: *On the Zeta-function of an Abelian Variety with Complex Multiplication*, Ann. of Math. **94**(1971), 504 - 533.

[SeT] Serre, J.P. and Tate, J.: *Good Reduction of Abelian Varieties*, Ann. of Math. **88**(1968), 492 - 517.

[ST] Shimura, G. and Taniyama, Y.: *Complex Multiplication of Abelian Varieties and its Application to Number Theory*, Publ. Math. Soc. Japan **6**, 1961.