

Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j -invariant II

Claus Diem and Jasper Scholten

July 17, 2006

Abstract

We show that for all odd primes p , there exist ordinary elliptic curves over $\overline{\mathbb{F}}_p(x)$ with arbitrarily high rank and constant j -invariant. This shows in particular that there are elliptic curves with arbitrarily high rank over these fields for which the corresponding elliptic surface is not supersingular. The result follows from a theorem which states that for all odd prime numbers p and ℓ , there exists a hyperelliptic curve over $\overline{\mathbb{F}}_p$ of genus $(\ell - 1)/2$ whose Jacobian is isogenous to the power of one ordinary elliptic curve.

Key words: Elliptic curves of high rank, Jacobians

MSC2000: Primary: 11G05; Secondary: 11G20, 14H40, 14H52.

1 Introduction

The purpose of this work is to prove the following theorem and its corollary.

Theorem *Let p and ℓ be odd prime numbers. Then there exists an ordinary hyperelliptic curve H over $\overline{\mathbb{F}}_p$ of genus $(\ell - 1)/2$ whose Jacobian variety is isogenous to the power of one ordinary elliptic curve.*

Corollary *Let p be a fixed odd prime number. Then there exist ordinary elliptic curves over $\overline{\mathbb{F}}_p(x)$ with arbitrarily high rank and constant j -invariant.*

The corollary follows from the theorem and the following general fact which was first pointed out by Shafarevich and Tate ([17]): Let H be a hyperelliptic curve over some field k with a k -rational divisor of degree 1, and let E be an elliptic curve over k such that $J_H \sim E^r \times A$ for some

abelian variety A over k . Let $k(H)|k(x)$ be an extension of degree 2. Then the quadratic twist of $E_{k(x)}$ with respect to $k(H)|k(x)$ has rank at least r . For details we refer to the introduction of [2].

Using the construction in [5], we have shown in [2] that for every $r \in \mathbb{N}$ there exists an ordinary hyperelliptic curve over \mathbb{F}_{2^r} whose Jacobian variety is completely decomposable and contains up to isogeny a factor E^r for some ordinary elliptic curve E ([2, Theorem 1]). This implies that the corollary holds in fact for all primes p . We note that in [2] the corollary has already been proven under the assumption of Artin's Primitive Root Conjecture.

It is not known whether there exist non-constant elliptic curves over $\mathbb{C}(x)$ with arbitrarily high rank. On the other hand, as noted in [2], there are several known classes of non-constant elliptic curves with arbitrarily high rank over rational function fields in positive characteristic. Previous to our work [2], examples of both high-rank supersingular elliptic curves and high-rank elliptic curves with non-constant j -invariant (which are thus ordinary) have been given. But all these examples are related to supersingular varieties because the corresponding elliptic surfaces are supersingular (in the sense of Shioda, that is, the ℓ -adic second cohomology groups are generated by divisor classes, cf. [18, page 235]). This is somewhat of a weakness if one wants to view the positive characteristic examples as an indication of what should be true in characteristic 0.

Just as the elliptic curves of high rank in [2], the elliptic curves of high rank given in this work do not correspond to supersingular surfaces.

In [4] it was asked by Ekedahl and Serre whether there exist curves in characteristic zero of arbitrarily high genus with completely decomposable Jacobian. It is well-known that the corresponding question for any fixed positive characteristic can be answered affirmatively: In every positive characteristic there exist supersingular curves of arbitrarily high genus, and over an algebraically closed field, the Jacobians of these curves are completely decomposable. Together with [2, Theorem 1] our theorem shows that in every positive characteristic there also exist ordinary curves of arbitrarily high genus with completely decomposable Jacobian.

Outline of the proof of the theorem

We consider families of hyperelliptic curves which have already been studied by Brumer and Mestre (see [15] and reference [3] in [15]). Over an algebraically closed field, the Jacobian varieties of the members of these families have real multiplication. Via a degeneration argument we give a criterion under which the families are generically ordinary. If we consider certain members of these families such that the real multiplication is not defined over the ground field, we can conclude that the Jacobian varieties

are isogenous to Weil restrictions of ordinary elliptic curves (here we use [2, Proposition 2]). The existence of suitable curves is guaranteed by a density argument.

Terminology and notations

Throughout the work, we use the following terminology concerning curves: If not stated otherwise, a *curve* over a field is assumed to be proper and geometrically reduced but not necessarily smooth or irreducible. A (relative) curve over a locally noetherian connected base S is a proper and flat morphism $C \rightarrow S$ whose fibers are curves. A *semi-stable* curve over S is a curve over S such that the only singularities of the fibers are ordinary double points.

We denote a relative curve C over S by C/S . For $s \in S$ or a geometric point s of S , we denote the (geometric) fiber of C over s by C_s . If C/S and D/S are curves, we call a finite and flat S -morphism $C \rightarrow D$ a *cover*.

Note that the Euler-Poincaré characteristic of the fibers of a relative curve is constant (see the first corollary to the Theorem in [16, Chapter II, §5]), and thus so is the (arithmetic) genus; we define the *genus* of a relative curve to be the genus of any of its fibers.

If A is an abelian variety over a field k , we denote the ring of endomorphisms of A over k by $\text{End}(A)$.

2 The curves

In this section, we define the hyperelliptic curves in question as well as the real multiplication on the Jacobians of these curves.

Let $\ell > 1$ be an odd prime. Let us fix a ground field k of any characteristic $\neq 2$ with algebraic closure \bar{k} . All curves in this section are over the fixed field k (but the real multiplication we want to define might not be defined over k). We assume that we are given an étale isogeny of elliptic curves $f : \tilde{E} \rightarrow E$ over k of degree ℓ . Let $\rho : E \rightarrow \mathbb{P}_k^1, \tilde{\rho} : \tilde{E} \rightarrow \mathbb{P}_k^1$ be covers of degree 2 which are ramified at the 2-torsion points. As the covers $\rho, \tilde{\rho}$ are in fact geometric quotients of E and \tilde{E} respectively by the automorphisms $[-1]$ on these curves, we have an induced cover $u : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ of degree ℓ with $\rho \circ f = u \circ \tilde{\rho}$.

Let $P := \rho(0_E)$, where 0_E is the zero point of E . Let $a : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ be a cover of degree 2 which is ramified at P and some other point $P' \notin \rho(E[2])$.

Now let D be the normalization of the fiber product of $a : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ and $u : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$, and let $d : D \rightarrow \mathbb{P}_k^1, \tilde{a} : D \rightarrow \mathbb{P}_k^1$ be the covers which are induced by the projections to the first and second factor respectively.

We thus have the following commutative diagram.

$$\begin{array}{ccccc}
 D & & \tilde{E} & & \\
 \downarrow d & \searrow \tilde{a} & \downarrow f & \searrow \tilde{\rho} & \\
 \mathbb{P}_k^1 & & E & & \mathbb{P}_k^1 \\
 & \searrow a & \searrow \rho & & \downarrow u \\
 & & & & \mathbb{P}_k^1
 \end{array} \tag{1}$$

Obviously D is hyperelliptic. Let us calculate its genus:

By Abhyankar's Lemma (cf. [19, Proposition III.8.9]), the cover $\tilde{a}_{\bar{k}} : D_{\bar{k}} \rightarrow \mathbb{P}_{\bar{k}}^1$ is unramified outside the preimages of P and P' under $u_{\bar{k}}$. Over the point P there is the point $\rho'(0_{\tilde{E}})$ which is unramified and $(\ell-1)/2$ other points in $\mathbb{P}^1(\bar{k})$ which are ramified of order 2. The point P' is unramified with respect to $u_{\bar{k}}$.

Again by Abhyankar's Lemma, the cover $\tilde{a}_{\bar{k}} : D_{\bar{k}} \rightarrow \mathbb{P}_{\bar{k}}^1$ is ramified exactly at $\tilde{\rho}(0_{\tilde{E}})$ and at the preimages of P' . This means that there are exactly $\ell+1$ ramification points, and the genus of D is $(\ell-1)/2$.

To introduce the real multiplication, we first consider the normalization C of $\mathbb{P}_k^1 \times_{\mathbb{P}_k^1} E$, where the product is taken with respect to a and ρ . Note that C is a genus 2 curve. Let $\tilde{C} := C \times_E \tilde{E}$. Note that as $f : \tilde{E} \rightarrow E$ is an étale cover of degree ℓ , so is $\tilde{C} \rightarrow C$. In particular, \tilde{C} is smooth, that is, it is a smooth and irreducible curve (of genus $\ell+1$). We have the following commutative diagram in which we also introduce some names for the covers.

$$\begin{array}{ccccc}
 \tilde{C} & & & & \\
 \downarrow c & \searrow \tilde{\phi} & & & \\
 C & & D & \tilde{E} & \mathbb{P}_k^1 \\
 & \searrow \phi & \downarrow d & \downarrow f & \downarrow u \\
 & & \mathbb{P}_k^1 & E & \mathbb{P}_k^1 \\
 & & \searrow a & \searrow \rho & \\
 & & & & \mathbb{P}_k^1
 \end{array} \tag{2}$$

Let $K|k$ be a field extension such that \tilde{E}_K has a non-trivial translation $\tau_{\tilde{E}_K}$ (of order ℓ) which is an automorphism of the cover $f_K : \tilde{E}_K \rightarrow E_K$ induced by f . Then $\tau_{\tilde{E}_K}$ induces by base-change an automorphism of order ℓ of $\tilde{C}_K = (C \times_E \tilde{E})_K$. Note that $\tau_{\tilde{C}_K}$ generates the automorphism group of the cover $c_K : \tilde{C}_K \rightarrow C_K$.

Let A be the reduced connected component of the zero of $\ker(c_*) < J_{\tilde{C}}$. Note that $\text{id} + \tau_{\tilde{C}_K}^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1}$ is defined over k , and A is the reduced connected component of the zero of $\ker(c^*c_*) = \ker(\text{id} + \tau_{\tilde{C}_K}^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1})$. Obviously $\tau_{\tilde{C}_K}^*(A_K) \subseteq A_K$ and the minimal polynomial of $\tau_{\tilde{C}_K}^*|_{A_K}$ divides $X^{\ell-1} + \cdots + X + 1$. As the latter polynomial is irreducible in $\mathbb{Q}[X]$ and $\tau_{\tilde{C}_K}^*|_{A_K}$ operates non-trivially on A_K , we conclude:

Lemma 1 *The ring $\mathbb{Z}[\tau_{\tilde{C}_K}^*|_{A_K}] < \text{End}(A_K)$ is isomorphic to $\mathbb{Z}[\zeta_\ell]$ (with $\tau_{\tilde{C}_K}^*|_{A_K} \longleftrightarrow \zeta_\ell$).*

Lemma 2 *$\tilde{\phi}^*(J_D)$ is contained in A .*

Proof. We proof this after base-change to K . Let δ be the non-trivial automorphism of \tilde{C} over D (of order 2). Note that $\tau_{\tilde{C}_K}$ and δ_K generate the automorphism group of $\phi_K \circ c_K : \tilde{C}_K \rightarrow \mathbb{P}_K^1$ which is in fact a dihedral group. In particular, we have

$$\begin{aligned} & (\text{id} + \tau_{\tilde{C}_K}^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1}) \circ (\text{id} + \delta_K^*) = \\ & \text{id} + \tau_{\tilde{C}_K}^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1} + \delta_K^* + \tau_{\tilde{C}_K}^* \circ \delta_K^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1} \circ \delta_K^* = \quad (3) \\ & c_{K*}^* \circ \phi_K^* \circ \phi_{K*} \circ c_{K*} = 0. \end{aligned}$$

Now $\tilde{\phi}_K^*(J_{D_K}) = \tilde{\phi}_K^* \tilde{\phi}_{K*}(J_{\tilde{C}_K}) = (\text{id} + \delta_K^*)(J_{\tilde{C}_K})$. By (3), this lies in $\ker(\text{id} + \tau_{\tilde{C}_K}^* + \cdots + \tau_{\tilde{C}_K}^{*\ell-1})$. \square

Now let $\tau := \tilde{\phi}_{K*} \circ \tau_{\tilde{C}_K}^* \circ \tilde{\phi}_K^* \in \text{End}(J_{D_K})$.

Proposition 1 *$\mathbb{Z}[\tau] < \text{End}(J_{D_K})$ is isomorphic to $\mathbb{Z}[(\tau_{\tilde{C}_K}^* + \tau_{\tilde{C}_K}^{*\ell-1})|_{A_K}] < \text{End}(A_K)$ as rings and Galois modules (with $\tau \longleftrightarrow (\tau_{\tilde{C}_K}^* + \tau_{\tilde{C}_K}^{*\ell-1})|_{A_K}$). In particular, the ring $\mathbb{Z}[\tau]$ is isomorphic to $\mathbb{Z}[\zeta_\ell + \zeta_\ell^{-1}]$.*

Proof. This follows by an analogous argument to the one presented on the lower part of page 498 of [2]. \square

Remark 1 For the proof of the theorem, we do not need the real multiplication on J_D but merely the automorphism $\tau_{\tilde{C}_K}^*|_{A_K}$. This is similar to the situation in [2].

Remark 2 The automorphism group of $a \circ \phi : C \rightarrow \mathbb{P}_k^1$ is $(\mathbb{Z}/2\mathbb{Z})^2$, thus besides the quotients $C \rightarrow E$ and $\phi : C \rightarrow \mathbb{P}_k^1$ of degree 2, there is another quotient $C \rightarrow E'$ of degree 2 together with an induced cover $\rho' : E' \rightarrow \mathbb{P}_k^1$ of degree 2. Now, $\rho' : E' \rightarrow \mathbb{P}_k^1$ is ramified at $\rho(E[2] - \{0_E\}) \cup \{P'\}$, thus E' has genus 1. By fixing the preimage of P' as zero-point, E' is turned into an elliptic curve. Obviously C is also the normalization of $E \times_{\mathbb{P}_k^1} E'$. In the next section this observation serves as the starting point.

3 Generically ordinary families

In this section, we introduce families of curves (i.e., relative curves) \tilde{C}/S whose fibers are – except for some “degenerate” fibers – curves denoted by \tilde{C} in the previous section. We strive for proving that under some conditions, these families are generically ordinary, that is, their generic fibers are ordinary. Note that as “ordinariness” is an “open property” (cf. [1, Proposition 1.5]), this means that there exists a non-empty open subset $U \subset S$ such that the fibers over U are ordinary. To prove this, we force that some fibers are not irreducible.

The setting in this section is more general than what is actually needed for the proof of the theorem.

Let S be an integral, regular scheme over $\mathbb{Z}[1/2]$ of dimension 1, and let E/S and E'/S be two (relative) elliptic curves. Let $[0_E]$ be the Cartier divisor associated to the zero-section, and let $E[2]^\# := E[2] - [0_E]$. (Similar definitions for E' .)

We assume that we are furthermore given

- an isomorphism $\psi : E[2] \xrightarrow{\sim} E'[2]$ of group schemes over S ,
- an étale isogeny of elliptic curves $f : \tilde{E} \rightarrow E$ of some degree ℓ (which need neither be odd nor prime).

Let $\rho : E \rightarrow E/[-1]$, $\rho' : E' \rightarrow E'/[-1]$ be the canonical maps. Note that $E/[-1]$ and $E'/[-1]$ are both \mathbb{P}^1 -bundles (in fact if $q : E \rightarrow S$ is the structure map then $E/[-1] \simeq \mathbb{P}(q_* \mathcal{L}(2[0_E]))$). Furthermore, both $E[2]^\#$ and $E'[2]^\#$ are étale over S of degree 3 and $\rho|_{E[2]^\#}$ as well as $\rho'|_{E'[2]^\#}$ are closed immersions. By [3, Proposition B.4] there exists a unique S -isomorphism

$$\gamma : E/[-1] \xrightarrow{\sim} E'/[-1]$$

with $\gamma \circ \rho|_{E[2]^\#} = \rho' \circ \psi|_{E[2]^\#}$.

We identify $E/[-1]$ and $E'/[-1]$ via γ and let $\mathbf{P} := E/[-1] = E'/[-1]$, $P := \rho([0_E])$ and $P' := \rho'([0_{E'}])$.

We have the following easy lemma (see [3, Lemma A.1]).

Lemma 3 *Let s be a geometric point of S . Then the following are equivalent:*

- *There exists an isomorphism $\alpha : E_s \longrightarrow E'_s$ with $\alpha|_{E_s[2]} = \psi_s$.*
- *$P_s = P'_s$.*

We now make the following assumption:

Assumption The divisors P and P' are not equal (i.e., they are not equal at the generic point of S) but there exists some point $s \in S$ such that $P_s = P'_s$ and $E_s (= E'_s)$ is ordinary.

Remark 3 For the proof of the theorem we will deal with the special case where S is an affine curve over \mathbb{F}_q and E'/S is a constant family.

Lemma 4 *$E \times_{\mathbf{P}} E'$ is integral, and $\kappa(E \times_{\mathbf{P}} E') \simeq \kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E')$.*

Proof. The ring $E \otimes_{\kappa(\mathbf{P})} \kappa(E')$ is a field because by assumption, the generic points of $\rho'([0_{E'}])$ and $\rho([0_E])$ are distinct.

Let A be the coordinate ring of an affine open part U of \mathbf{P} , let B and B' be the coordinate rings of the preimages of U in E and E' . We claim that the canonical map $B \otimes_A B' \longrightarrow \kappa(B) \otimes_{\kappa(A)} \kappa(B') \simeq \kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E')$ is injective.

We have $\kappa(B) \otimes_{\kappa(A)} \kappa(B') \simeq (B \otimes_A \kappa(A)) \otimes_{\kappa(A)} (B' \otimes_A \kappa(A)) \simeq (B \otimes_A B') \otimes_A \kappa(A)$ as B and B' are finite over A . We thus have to show that the map $B \otimes_A B' \longrightarrow (B \otimes_A B') \otimes_A \kappa(A)$ is injective. Now, $A \longrightarrow \kappa(A)$ is injective and $B \otimes_A B'$ is flat over A . This implies that $B \otimes_A B' \longrightarrow (B \otimes_A B') \otimes_A \kappa(A)$ is injective. It follows that $B \otimes_A B'$ is reduced and that $\kappa(B) \otimes_{\kappa(A)} \kappa(B') \simeq \kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E')$ is its function field. \square

Let C be the normalization of $E \times_{\mathbf{P}} E'$, and let $\pi : C \longrightarrow E$ and $\pi' : C \longrightarrow E'$ be the maps which are induced by the projections to the factors.

Lemma 5 *The morphisms π and π' as well as the normalization morphism $C \longrightarrow E \times_{\mathbf{P}} E'$ are finite, in particular C/S is proper.*

Proof. We first note that as S is regular and E is smooth over S , E is also regular and in particular normal (see [7, Exposé II, Proposition 3.1], [14, Theorem 19.4]).

The projection $E \times_{\mathbf{P}} E' \longrightarrow E$ is finite because it is induced by base-change from the finite morphism $E' \longrightarrow \mathbf{P}$. This implies in particular that the normalization of $E \times_{\mathbf{P}} E'$ is equal to the normalization of E in $\kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E')$. As E is normal and the extension $\kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E') | \kappa(E)$ is separable,

this implies that $\pi : C \rightarrow E$ is finite (see [12, Chapter 4, Proposition 1.25]). As $E \times_{\mathbf{P}} E'$ is finite over E , implies that the normalization morphism $C \rightarrow E \times_{\mathbf{P}} E'$ is finite too. Clearly, π' is also finite. \square

Proposition 2 *C/S is a semi-stable genus 2 curve and π, π' are covers of degree 2.*

For $s \in S$ with $P_s \neq P'_s$, C_s is an irreducible smooth genus 2 curve. For $s \in S$ with $P_s = P'_s$, C_s is isomorphic to the union of two copies of $E_s (= E'_s)$ intersecting at 0_{E_s} . One can choose an isomorphism such that π_s restricts to id_{E_s} on both components and π'_s restricts to id_{E_s} on one component and to $-\text{id}_{E_s}$ on the other.

Proof. The field $\kappa(S)$ is algebraically closed in $\kappa(E) \otimes_{\kappa(\mathbf{P})} \kappa(E')$ and S is normal. By Grothendieck's results on "Zariski's Main Theorem", this implies that the geometric fibers of C over S are connected (see [8, (4.3.12)]).

Let W be the ramification locus of $E \times_{\mathbf{P}} E' \rightarrow \mathbf{P}$. Then $(E \times_{\mathbf{P}} E') - W$ is normal, because the domain of an étale morphism mapping to a normal scheme is normal (see [7, Exposé I, Corollaire 9.11]). It follows that $C \rightarrow E \times_{\mathbf{P}} E'$ induces an isomorphism between the complement of the preimage of W in C and $(E \times_{\mathbf{P}} E') - W$.

Let $s \in S$. Then W_s is zero-dimensional, and as the canonical morphism $C_s \rightarrow E_s \times_{\mathbf{P}_s} E'_s$ is finite (by the preceding lemma), the preimage of W_s in C is zero-dimensional too. Moreover, the irreducible components of $E_s \times_{\mathbf{P}_s} E'_s$ are 1-dimensional (there are one or two irreducible components depending on whether $P_s \neq P'_s$ or $P_s = P'_s$). As C_s is connected, this implies that $C_s \rightarrow E_s \times_{\mathbf{P}_s} E'_s$ is birational on the irreducible components of C_s . The fact that C/S is proper (see preceding lemma) now implies that C_s is proper too. This means that C_s is a curve.

As S is integral of dimension 1 and C is integral, C/S is flat (see [10, Proposition 9.7]). It follows that C/S is a curve.

By Abhyankar's Lemma ([7, Exposé X, Lemme 3.6]) and "purity of the branch locus" ([7, Exposé X, Théorème 3.1]), π is étale outside $(\pi')^{-1}([0_{E'}]) = (\rho' \circ \pi')^{-1}(P'_s)$ and π' is étale outside $\pi^{-1}([0_E]) = (\rho \circ \pi)^{-1}(P_s)$. This implies that C/S is smooth outside the preimage of $P \cap P'$.

This means in particular that for $s \in S$ with $P_s \neq P'_s$, the fiber C_s is a non-singular curve. From the assumption it follows now that the generic fiber is a smooth curve. Clearly it has genus 2. This means that C/S is a curve of genus 2.

Now let $s \in S$ with $P_s = P'_s$.

Note that the normalization of $E_s \times_{\mathbf{P}_s} E'_s = E_s \times_{\mathbf{P}_s} E_s$ is isomorphic to $E_s \dot{\cup} E_s$. The identification can be made such that the first projection map restricts to id_{E_s} on both components and the second projection map

restricts to id_{E_s} on one component and to $-\text{id}_{E_s}$ on the other. We thus have a canonical map $E_s \dot{\cup} E_s \longrightarrow C_s$ such that the restrictions to each of the two components are closed immersions.

As outside the preimage of P_s the curve C_s is smooth, we furthermore have an isomorphism outside the preimage of P_s . Now, the preimage of P_s in $E_s \times_{\mathbf{P}^s} E'_s$ is $\{(0_{E_s}, 0_{E'_s})\}$, and the preimage of this in $E_s \dot{\cup} E_s$ is the set consisting of the two zero points.

As C_s is connected (see beginning of the proof), this implies that set-theoretically C_s is obtained from $E_s \dot{\cup} E_s$ by identifying the two zero points, and that moreover, outside the intersection point C_s is smooth. We claim that the intersection point is an ordinary double point.

Note that the genus of C_s is 2 because the genus of the fibers of C/S is constant (see the first corollary to the Theorem in [16, Chapter II, §5]). Together with [12, Chapter 7, Proposition 5.4] this implies that the intersection point is an ordinary double point.

This implies that C_s is semi-stable, and hence C/S is semi-stable too.

Clearly the morphisms π and π' induce covers of degree 2 on the fibers. They are flat by [9, (11.3.11)], and we have already seen in the preceding lemma that they are finite. They are thus covers of curves of degree 2. \square

Let $\tilde{C} := C \times_E \tilde{E}$. Note that as f is étale, so is the induced map $c: \tilde{C} \longrightarrow C$. It follows that \tilde{C}/S is a semi-stable curve of genus $\ell + 1$.

The main result of this section is:

Proposition 3 *The curve \tilde{C}/S is generically ordinary.*

Proof. We assumed that there exists some point $s \in S$ with $P_s = P'_s$ such that E_s is ordinary. Let us fix such a point. Then the irreducible components of C_s are elliptic curves isomorphic to E_s . In fact, by the previous proposition, the preimage of such an irreducible component is isomorphic to the ordinary elliptic curve \tilde{E}_s . This implies that \tilde{C}_s is ordinary (cf. the text below Lemma 1.3 in [1]), thus the curve \tilde{C}/S is generically ordinary (cf. [1, Proposition 1.5]). \square

Remark 4 Let Ω be an algebraically closed field, and let $s \in S(\Omega)$ be a geometric point of S with $P_s = P'_s$. Let $Q_1, \dots, Q_\ell \in \tilde{E}_s(\Omega)$ be the preimages of 0_{E_s} under f_s . Then \tilde{C}_s is in fact the union of two copies of \tilde{E}_s where any point Q_i on one component is identified with the corresponding point on the other component. This means that the dual graph of \tilde{C}_s (cf. [1, Section 1]) consists of two vertices which are connected by ℓ edges. In particular it has $\ell - 1$ loops. This is consistent with the genus being $\ell + 1$.

Remark 5 By [13, Lemma 5.6], the covers π, π' both have automorphisms of order 2. Let σ_C be the composition of these two automorphisms. Then σ_C is also an involution, and we have an induced cover $a : C/\langle\sigma_C\rangle \rightarrow \mathbf{P}$ of degree 2 whose branch locus is $P \cup P'$ (see [3] for more information). If $s \in S$ such that $P_s \neq P'_s$, then $C/\langle\sigma_C\rangle \approx \mathbb{P}_{\kappa(s)}^1$. Note that this corresponds to the setup of the previous section.

Now let ℓ be odd. Let $\tilde{\mathbf{P}} := \tilde{E}/[-1]$. Then as in the previous section we have an induced cover $u : \tilde{\mathbf{P}} \rightarrow \mathbf{P}$ of degree ℓ . Let D be the normalization of the fiber product $C/\langle\sigma_S\rangle \times_{\mathbf{P}} \tilde{\mathbf{P}}$ (which is integral), and let $\tilde{a} : D \rightarrow \tilde{\mathbf{P}}$ be the canonical map. Let U be the open subscheme of S where P and P' do not meet. Then D_U/U is a hyperelliptic curve of genus $(\ell - 1)/2$ in the sense of [13].

For this, one has to show that D_U/U is smooth and that $\tilde{a}_U : D_U \rightarrow \tilde{\mathbf{P}}_U$ is a degree 2 cover. The smoothness follows with Abhyankar's Lemma and "purity of the branch locus" similarly to the proof of Proposition 2, and the statement on \tilde{a}_U is also proved analogously to the corresponding statement in Proposition 2.

Note that for $s \in U$ and prime ℓ , the curve D_s is a hyperelliptic curve called D in the previous section, i.e., the point of study of this work. We do not need the family D/S in the sequel, though.

4 Modular curves and proof of the theorem

Let p and ℓ be odd primes.

We want to apply [2, Proposition 2] to the abelian variety $A < J_{\tilde{C}}$ for some curve \tilde{C} as in Section 2 over some finite field of characteristic p .

For this, we first fix an ordinary elliptic curve E' over a finite field \mathbb{F}_q of characteristic p . By enlarging the base field if necessary, we assume that the two-torsion points are all rational, and that $\zeta_4 \in \mathbb{F}_q$. We fix a cover $\rho' : E' \rightarrow \mathbb{P}_{\mathbb{F}_q}^1$ of degree 2, ramified as always at the 2-torsion points.

Note that the moduli problem "étale isogenies of order ℓ of elliptic curves with rational 4-torsion and a fixed determinant over \mathbb{F}_q -schemes" is (finely) represented by an irreducible affine curve over \mathbb{F}_q . Let us call this curve Y_0 . Let Y_1 be the affine modular curve parameterizing elliptic curves with rational 4-torsion and a fixed determinant with an automorphism of order ℓ over \mathbb{F}_q -schemes. Note that we have a canonical étale Galois cover $Y_1 \rightarrow Y_0$ with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^*$. Thus in particular the cover is cyclic of order $\ell - 1$.

Let $f : \tilde{E} \rightarrow E$ be a universal étale isogeny of order ℓ over Y_0 . The curve Y_0 will play the role of the base-scheme, denoted S in the previous section. The isogeny f will play the same role as in the previous section.

The complementary elliptic curve for the construction is E'_{Y_0} , obtained by base-change from $\text{Spec}(\mathbb{F}_q)$ to Y_0 .

By definition of E and E' , both $E[2]$ and $E'_{Y_0}[2]$ are isomorphic to the group scheme $(\mathbb{Z}/2\mathbb{Z})^2$ over Y_0 . There thus exists an isomorphism between $E[2]$ and $E'_{Y_0}[2]$ as S -group schemes. Let us choose such an isomorphism. We are then in the situation of the previous section, and we define the curves C/Y_0 and \tilde{C}/Y_0 as in the previous section.

The ‘‘Assumption’’ of the previous section is obviously satisfied, and by Proposition 3, \tilde{C}/Y_0 is generically ordinary. Recall that this means that there are only finitely many geometric fibers which are not ordinary.

Now consider the cover $Y_1 \rightarrow Y_0$ of degree $\ell - 1$. Note that by definition of Y_1 , if $y \in Y_0$, y_1 is a preimage of y and $k := \mathbb{F}_q(y)$, $K := \mathbb{F}_q(y_1)$ are the corresponding residue fields, there exists a non-trivial translation $\tau_{\tilde{E}_K}$ (of order ℓ) on $(\tilde{E}_y)_K$ which is an automorphism of the cover $(f_y)_K : (\tilde{E}_y)_K \rightarrow (E_y)_K$, and K is the smallest extension of k over which $\tau_{(\tilde{E}_y)_K}$ is defined.

By the Chebotarev Density Theorem (see e.g. [11]), there exist infinitely many $y \in Y_0$ which are inert. In particular, there exists such a y such that $P_y \neq P'_y$ (which implies that C_y and \tilde{C}_y are smooth and irreducible) and \tilde{C}_y is ordinary. Let us fix such a y . Let y_1 be the unique preimage of y in Y_1 . Let $k := \mathbb{F}_q(y)$ and $K := \mathbb{F}_q(y_1)$. Note that by the choice of y , $[K : k] = \ell - 1$.

Now similarly to Section 2, let $A_y := \ker((c_y)_*) < J_{\tilde{C}_y}$. Let D_y be the hyperelliptic curve over k obtained via (1) (and Remark 2) applied to the fibers over k (D_y is thus the fiber at y of the curve D/S in Remark 5). The curve D_y is the hyperelliptic curve of genus g whose Jacobian we want to study.

Let $\tau_{(\tilde{E}_y)_K}$ be a non-trivial translation which is an automorphism of f_K , and as in Section 2, let $\tau_{(\tilde{C}_y)_K}$ be the automorphism of \tilde{C}_K obtained by base-change from $\tau_{(\tilde{E}_y)_K}$. Then K is still the smallest extension of k over which $\tau_{(\tilde{C}_y)_K}$ is defined.

We have $\dim(A) = [K : k] = \ell - 1$ and $\mathbb{Q}[(\tau_{\tilde{C}_K}^*)|_{A_K}] \simeq \mathbb{Q}[\zeta_\ell]$. Using [2, Proposition 2] we conclude that A_y is isogenous to the Weil restriction with respect to $K|k$ of one ordinary elliptic curve over K . It follows that $(A_y)_K$ is isogenous to a power of one ordinary elliptic curve. In particular, the Jacobian of the hyperelliptic curve $(D_y)_K$, which by Lemma 2 is isogenous to an abelian subvariety of $(A_y)_K$, is isogenous to a power of one ordinary elliptic curve.

This proves the theorem stated in the introduction.

5 Further examples of ordinary curves with completely decomposable Jacobian

In the article [4] mentioned in the introduction it is not only asked whether there exist curves with completely decomposable Jacobian of arbitrarily high genus but also whether there exist such curves for every genus. To the knowledge of the authors, the question is still open in any characteristic except 2, and it is therefore interesting to give conditions on p and g such that a curve of genus g over $\overline{\mathbb{F}}_p$ with completely decomposable Jacobian exists (for characteristic 2, see [6]). In this section, we outline how the proof of our theorem can be generalized to give further examples of ordinary curves with completely decomposable Jacobian.

By the proof of the theorem, ordinary curves with completely decomposable Jacobian exist under the following assumptions for arbitrary odd characteristic:

- $g = \ell + 1$, ℓ an odd prime
- $g = (\ell - 1)/2$, ℓ an odd prime
- $g = (\ell + 1)/2$, ℓ an odd prime

Indeed, if ℓ is an odd prime, then the curves \tilde{C}_y in the proof of the theorem have genus $\ell + 1$ and the curves D_y have genus $(\ell - 1)/2$. Moreover, the curves \tilde{C}_y have another canonical quotient $C_y \rightarrow D'_y$ of degree 2 such that $g(D'_y) = (\ell + 1)/2$. In the notation of Remark 5, the curves D'_y are the normalizations of the fiber product of $\rho'_y : E'_y \rightarrow \mathbf{P}_y$ and $u_y : \tilde{\mathbf{P}}_y \rightarrow \mathbf{P}_y$.

The three conditions given above can be generalized to ℓ a *power* of an odd prime. This follows from a generalization of the proof of the theorem. An outline is as follows: For arbitrary odd ℓ , we have a canonical decomposition

$$J_{\tilde{C}_y} \sim J_{C_y} \times \prod_{d|\ell, d \neq 1} (A_y)_d,$$

where $(A_y)_d$ is an abelian variety of dimension $\phi(d)$ with $\mathbb{Z}[\tau_{\tilde{C}_y}^* |_{(A_y)_d}] \simeq \mathbb{Z}[\zeta_d]$. Now, if ℓ is a prime power, the cover $Y_1 \rightarrow Y_0$ is still cyclic, and if one chooses a point $y \in Y_0$ which is inert under this map and for which \tilde{C}_y is smooth and ordinary, one can conclude with [2, Proposition 2] that each of the $(A_y)_d$ is isogenous to a Weil restriction of one ordinary elliptic curve.

So far, we have not used the real multiplication on $J_{(D_y)_{\overline{\mathbb{F}}_p}}$ explicitly. If one does so, one can prove that there exist examples of suitable curves of genus $(\ell - 1)/2$ and $(\ell + 1)/2$ provided that ℓ is odd and $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$ is *cyclic* (which implies that ℓ is an odd prime power or the product of two odd prime powers).

We outline the proof for the genus being $(\ell - 1)/2$. The case $(\ell + 1)/2$ is similar.

Let ℓ be odd. We have a canonical decomposition

$$J_{D_y} \sim \prod_{d|\ell, d \neq 1} (B_y)_d,$$

where $(B_y)_d$ is an abelian variety of dimension $\phi(d)/2$ with $\mathbb{Z}[\tau^*|_{(B_y)_d}] \simeq \mathbb{Z}[\zeta_d + \zeta_d^{-1}]$, where τ is defined as in Section 2.

Let us assume that $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$ is cyclic. Let σ_2 be the automorphism of $Y_1 \rightarrow Y_0$ corresponding to $-1 \in (\mathbb{Z}/\ell\mathbb{Z})^*$, and let $Y_2 := Y_1/\langle \sigma_2 \rangle$.

Then for all $y \in Y_0$, the automorphism group of $Y_2 \rightarrow Y_0$ operates canonically on all $\mathbb{Q}[\tau^*|_{(B_y)_d}]$. If y is inert, it generates the automorphism groups of all these groups. If one chooses an inert y such that \tilde{C}_y (and thus D_y) is irreducible and ordinary, then again by [2, Proposition 2] each $(B_y)_d$ is isogenous to a Weil restriction of an ordinary elliptic curve.

Acknowledgment

With great pleasure, we thank Irene Bouw and Everett Howe for discussions and comments.

References

- [1] I. Bouw. The p -rank of curves and covers of curves. In *Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998)*, Progr.Math., pages 267–277. Birkhäuser, Basel.
- [2] I. Bouw, C. Diem, and J. Scholten. Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j -invariant. *manuscripta math.*, 114:487–501, 2004.
- [3] C. Diem. Families of elliptic curves with genus 2 covers of degree 2. *Collect. Math.*, 57:1–25, 2006.
- [4] T. Ekedahl and J.-P. Serre. Exemples de courbes algébriques à Jacobienne complètement décomposable. *C. R. Acad. Sci. Paris Sér. I Math.*, 317(5):509–513, 1993.
- [5] P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
- [6] G. van der Geer and M. van der Vlugt. On the existence of supersingular curves of given genus. *J. reine angew. Math.*, 458:53–61, 1995.

- [7] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA I)*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris.
- [8] A. Grothendieck. *Eléments de Géométrie Algébrique III (seconde partie)*. *Publ. Math. Inst. Hautes Etud. Sci*, 17, 1963.
- [9] A. Grothendieck. *Eléments de Géométrie Algébrique IV (troisième partie)*. *Publ. Math. Inst. Hautes Etud. Sci*, 28, 1966.
- [10] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.
- [11] M. Jarden. The Čebotarev density theorem for function fields: an elementary approach. *Math. Ann.*, 261(4):467–475, 1982.
- [12] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, Oxford, 2001.
- [13] S. Lønsted and K. Kleiman. Basics on families of hyperelliptic curves. *Compos. Math.*, 38:83–111, 1979.
- [14] H. Matsumura. *Commutative ring theory*. Cambridge University Press, Cambridge, UK, 1986.
- [15] J.-F. Mestre. Familles de courbes hyperelliptiques à multiplications réelles. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 193–208. Birkhäuser Boston, Boston, MA, 1991.
- [16] D. Mumford. *Abelian varieties*. Tata Institute for Fundamental Research, Bombay, 1970.
- [17] I. Shafarevich and J. Tate. The rank of elliptic curves. *Dokl. Soviet Math. Dokl.*, 8(4):917–920, 1967.
- [18] T. Shioda. An example of unirational surfaces in characteristic p . *Math. Ann.*, 211:233–236, 1974.
- [19] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

Claus Diem, Universität Leipzig, Fakultät für Mathematik und Informatik, Augustusplatz 10/11, 04109 Leipzig, Germany. diem@math.uni-leipzig.de
Jasper Scholten, ESAT/COSIC, K.U. Leuven, Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium. jasper.scholten@esat.kuleuven.be